JOURNAL
Science and Technology

Volume 30 - No. (8) - 2025

An Open Access Peer-Reviewed Journal Published Biyearly by Faculty of Engineering and Faculty of Computing and Information Technology University of Science & Technology - Main Campus Aden - Yemen.

Online ISSN: 2410-5163 Print ISSN: 1607-2073

جامعة العلوم والتكنولوجيا

University of Science & Technology

المركز الرئيس - عـــدن

https://doi.org/10.20428/jst.v30i8

Journal of Science and Technology

Vol. 30 No. 8 (2025)

Journal of Science and Technology

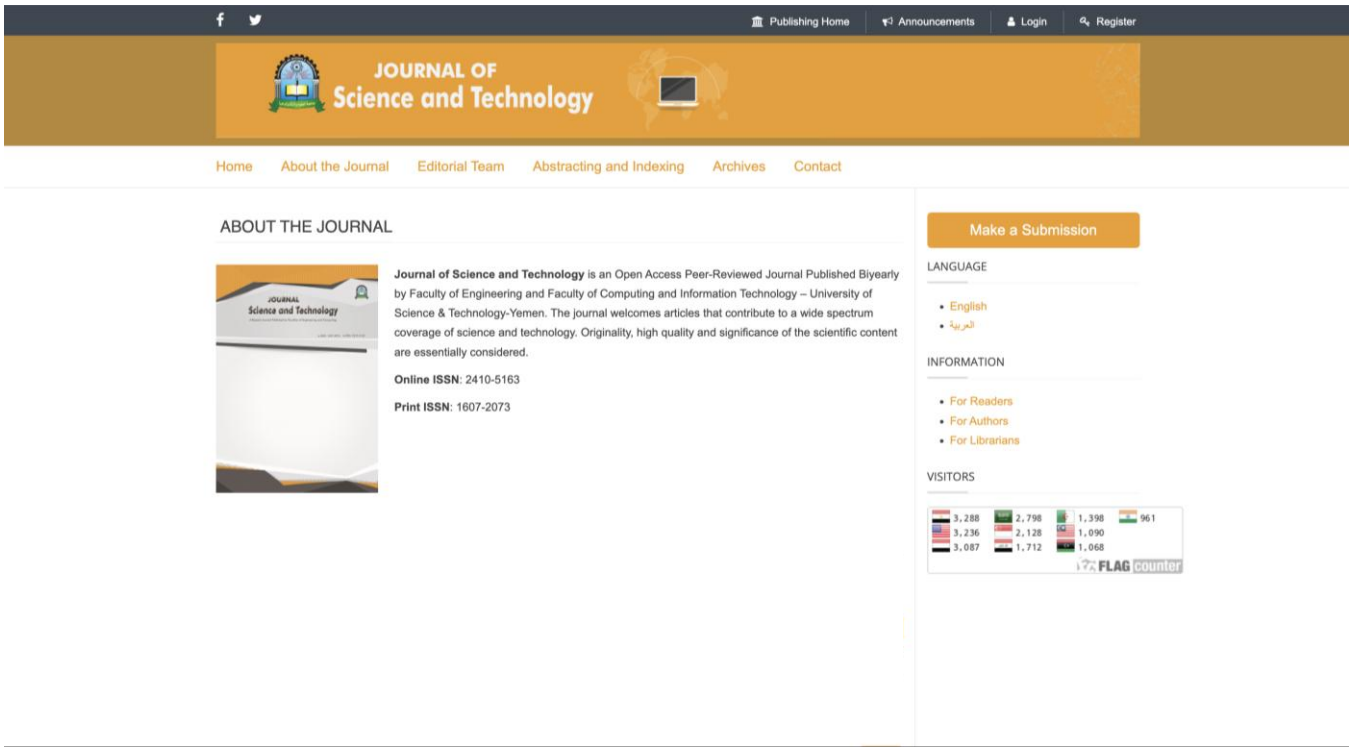
https://doi.org/10.20428/jst.v30i8

Editorial Team

For Contact
Journal of Science and Technology
Faculty of Engineering and Faculty of Computing and Information Technology, University of Science and Technology, Main Campus - Aden - Yemen
+967718032009
jst@ust.edu

https://doi.org/10.20428/jst.v30i8

Website:



https://journals.ust.edu/index.php/JST

https://doi.org/10.20428/jst.v30i8

Publication Rules and Procedures

General Rules:

Research papers sent for publication in the Journal of Science and Technology at the University of Science and Technology – Aden, Yemen, should meet the following requirements:

1. The journal publishes research papers in Arabic and English, in the following categories (but not limited to): Physics, Chemistry, Mathematics, s Engineering, and Computer Science. if they comply with the following conditions:

a. Title:

A title should summarize the main idea of the manuscript. It should identify the variables under investigation and the relationship between them. It should be concise and fully explanatory for readers when standing alone. It is recommended to be no more than 12 words and with no abbreviations. It should be typed in uppercase and lowercase letters, centered in the upper half of the page.

b. Author's name and institutional affiliation:

Every manuscript should include the name of the author and the institutional affiliation of the author when the research was conducted.

Author's name:

The preferred form of an author's name is first name, middle initial(s), and last name, with no titles (e.g., Dr., Professor) or degrees (e.g., PhD, PsyD, EdD). If the manuscript is done by more than one author, the names of the authors should be in the order of their contributions, centered between the side margins.

Institutional affiliation:

The affiliation (i.e. institution) should be centered under the author's name on the next line. If an author has no institutional affiliation, list the city and state of residence below the author's name. The emails for all authors should be provided.

c. Abstract:

An abstract in both Arabic and English must be included, with the former version **in the language of the manuscript.** It should be in a form of a brief, comprehensive summary of the contents of the manuscript written in a single paragraph with no paragraph indentation. It must not exceed 200 words.

The abstract should clearly describe the problem under investigation, in one sentence if possible; identify the purpose of the research, the essential features of study method; the participants' relevant characteristics such as age, sex, and ethnic and/or racial group; the basic findings including statistical significance levels; and the conclusions and the implications or applications. Keywords (3 - 5) should follow the abstract to increase user's ability to find useful information in the manuscript.

Introduction:

The body of a manuscript starts with an introduction that frames the problem under study and explores the importance of the problem (why the problem deserves new research). The statement about importance might involve the need to resolve any inconsistency in results of past work and/or extend the reach of a theoretical formulation and/ or investigate a practical problem that people suffer. The introduction ends in concluding the statement of the problem with a brief but formal statement of the purpose of the research that summarizes the material preceding it.

The author needs to discuss the relevant related literature in the introduction. A scholarly description of the earlier work will provide a summary of the most recent directly related work and recognize the priority of the work of others. The description of relevant literature will present what other aspects of this study have been investigated in the previous studies and how the current study differs from the earlier ones. For summarizing earlier works, focus should be on the topic (research syntheses of the topic), methodological issues, relevant findings, and main conclusions.

The discussion of related literature should demonstrate the logical continuity between previous and present work (**demonstration of gaps**); and the development of the problem should have enough breadth and clarity that make it easy to understand by a wide range of professionals.

After developing the theoretical background and the problem of the study, the author has to state the objectives and the hypotheses or specific questions. The introduction should be 10 to 15% of the manuscript. It starts on a separate page (i.e. p. 3).

https://doi.org/10.20428/jst.v30i8

d. Method:
This section describes in detail how the study was conducted, including conceptual and operational definitions of the variables used in the study. A comprehensive description of the methods used enables the reader to evaluate the appropriateness of the methods and the reliability and the validity of the results. It may include participant characteristics, sampling procedures, sample size, measures and research design.

e. Results:
Results section summarizes the collected data and the analysis done on those data. It should provide sufficient detail about the data to justify the study conclusions. The results should also include details that may not match the study expectation; or even small effect sizes (or statistically non-significant findings) particularly when theory predicts large (or statistically significant) ones. Uncomfortable results should not be omitted. The data can be presented in tables or figures (data presented in tables should not be represented in figures). Tables should be numbered in order of mention in the text. Tables can be single-spaced and should not contain any lines. Asterisks may be used to indicate significant findings. Symbols, acronyms or abbreviations should be used sparingly. Explanatory footnotes should be used whenever possible rather than overlong titles. Images should be submitted as high-resolution files (300 dpi or higher) in TIFF format (LZW compression) or JPEGs.

f. Discussion:
After presenting the results, their implications should be evaluated and interpreted, especially with respect to the original hypotheses. The author needs to examine, interpret, and draw inferences and conclusions from the results emphasize any theoretical or practical consequences of the results (Results and discussion can be combined in one section). Similarities and differences between the results and the work of others should be used to contextualize, confirm, and clarify the conclusions. Each new statement should contribute to the interpretation and to the reader's understanding of the problem.
The interpretation of the results should discuss the limitations or weaknesses of the study, and address alternative explanations of the results. It also discusses the generalizability of the findings. This critical analysis should take into account differences between the target population and the accessed sample.

g. Conclusion:
This concluding section presents a brief, reasoned and justifiable commentary on the importance of the findings. It is tightly reasoned, self-contained, and not overstated. In this section, the importance of the problem (as stated in the introduction) should be discussed; what larger issues might depend on the findings; and what propositions are confirmed or disconfirmed.

Acknowledgements:
This **section** refers to the aid received by the author from other relevant parties. Reference should also be made to any financial assistance received to conduct the research. Any extraordinary assistance received by the author in word processing, data collection, data analysis, and so on, should be acknowledged. The acknowledgements should not exceed 60 words.

References:
References start on a separate page.
Authors should acknowledge the work of previous scholars by citing references to document statements in their manuscripts. JST uses IEEE standard format. For accurate, complete, and useful citations, authors can use a reference management tool.

Publication Procedures:

Manuscript acceptance, rejection, or acceptance with revision:
The editor decides whether the manuscript is accepted, rejected or needs to be revised based on the reviewers' reports.

Manuscript acceptance: Accepted manuscripts will undergo copy-editing and production phases of publication process. The authors will not be allowed to make further changes to the manuscript except for those recommended by the copyeditors. The authors remain responsible for the completion of any amendments required by the journal.

Manuscript Rejection: A manuscript is rejected if it falls outside the domain of the journal, has serious defects in design, methodology, analysis or interpretations, lack of contribution to the field, or has a low-quality.

Manuscript acceptance with revision:
A manuscript may be conditionally accepted. This takes place when the manuscript has a high potential for final acceptance and publication in the journal, and the author adheres to all the essential modifications required by the journal (e.g. gathering essential data, conducting new experiments, reanalyzing the data, etc.). The author has to attend to the editor's recommendations for revision. The revised manuscript should be resubmitted with an enclosed cover letter that contains a table explaining in detail how and where (in the manuscript) amendments have been done based on the reviewers' comments.

Publication Ethics:
The **JST** complies with the recommendations of the Committee on Publication Ethics (COPE) to promote the integrity of its published articles. The **JST** considers the following topics during the publishing process:

- **Originality & Source Acknowledgement:** The **JST** scans all submitted manuscripts before the peer-reviewing process using Turnitin®. The **JST** is zero-tolerant to plagiarism, self-plagiarism, copyright infringement, dual publication, text recycling and salami slicing. When any of these is identified after publishing, an announcement of retraction of the published material is highlighted in the journal's website. The authors are asked to provide appropriate references for published/unpublished cited texts. The corresponding author should confirm that the submission has not been previously published and is not being considered for publication elsewhere.
- **Research Misconduct:** The **JST** editorial team struggles to counter any possibility for data fabrication, manipulation and falsification. In case of suspected misconduct, the **JST** editors act in accordance to the COPE guidelines with this respect.
- **Conflicts of interest:** Authors should disclose potential conflicts of interest and indicate financial agreements or affiliations with any product or services used in the manuscript (as well as any potential bias against another product or service).
- **Authors:** Authors should disclose (in an author note) activities and relationships that if known to others might be viewed as a conflict of interest, even if the authors do not believe that any conflict or bias exists (e.g. an author has his stock in a company that manufactures a drug used in his study).
- **Reviewers:** Reviewers should also reveal their potential conflicts of interest (if any) to the action editor. They have an ethical obligation to be open and fair in assessing a manuscript without bias. They should not review a manuscript from a colleague or collaborator, a close personal friend, or a recent student. Reviewers should maintain the confidentiality of a manuscript. They should not discuss the manuscript with other individuals.
- **Using materials under copyrights:** The author should obtain letters of permission from copyright holders to reproduce (or adapt) copyrighted material and enclose copies of these letters with the accepted manuscript. Examples of material that require permission include reprinted figures and tables, tests and scale items, questionnaires, vignettes, etc.

Correction notices: If an error is detected in the published manuscript, the author can submit a proposed correction notice to the journal's editor. The notice should indicate the full title of the journal, the year of publication, the volume no., issue no., and the page nos. of the article, the precise location of the error(s) (e.g. page, line, column, exact quotation of the error, or paraphrasing of lengthy errors).

Publication Fees:
JST does not require any article processing charges or any article submission charges

Sponsorship:
JST is sponsored by the University of Science and Technology.

https://doi.org/10.20428/jst.v30i8

Content:

Journal of Science and Technology

https://doi.org/10.20428/jst.v30i8

Combining Deep Learning with Edge Computing in Improving Accessibility and Performance of E-Learning

S. A. Mohsen [1,*]
N. M. A. Munassar [1]

Received: 24/03/2025
Revised: 16/04/2025
Accepted: 17/04/2025

[1] College of Engineering, University of Science & Technology, Aden, Yemen.
*Corresponding Author's Email: s.yahya@student.ust.edu

Combining Deep Learning with Edge Computing in Improving Accessibility and Performance of E-Learning

Shaima Abdulrahman Mohsen
College of Engineering, University of Science & Technology,
Aden, Yemen,
s.yahya@student.ust.edu,

Nabil Mohammed Ali Munassar
College of Engineering, University of Science & Technology,
Aden, Yemen,
n.munasser@ust.edu

Abstract—Through a descriptive analysis, this study investigates how to improve the performance and accessibility of e-learning systems integrating deep learning (DL) with edge computing (EC). The COVID-19 epidemic has exposed obstacles to real-time interactions and scalability in traditional cloud-based e-learning, including latency, bandwidth limitations, and privacy problems. Through utilizing deep learning's adaptability and edge computing's decentralized design, this study suggests a three-tier architecture (end-user devices, edge servers, and cloud clusters) to enhance security, minimize latency, and optimize data processing. Through a comparative analysis of cloud-based and edge-enabled systems, the study highlights the advantages of this hybrid approach, including faster response times, reduced network congestion, and enhanced privacy. The findings demonstrate the potential of edge-based deep learning to revolutionize e-learning by enabling personalized, real-time, and offline-capable educational experiences.

Keywords— Deep Learning (DL), Edge Computing (EC), E-learning Systems, Real-time Interactions

I. INTRODUCTION

The adoption of online learning has surged in recent years, particularly following the COVID-19 pandemic, which ensured the continuity of education despite physical restrictions. However, traditional cloud-based distance learning presents several challenges, including high infrastructure costs, security concerns, and latency issues that hinder real-time interaction (Labba et al., 2022). Even though distance learning maintained educational continuity during the pandemic, inherent infrastructure limitations exposed critical issues related to performance, data privacy, and security. Many educational institutions face difficulties in sustaining stable and cost-effective cloud-based e-learning environments, which demand high-speed internet access and significant storage and computing resources. This situation has prompted researchers to explore alternative solutions that enhance accessibility, efficiency, and security in online education.

In recent years, the concept of edge computing has gained traction as a response to the increasing demand for real-time data processing and lower latency in various applications. Unlike traditional cloud computing, which relies on centralized data centers, edge computing shifts computational tasks closer to the data source through local servers, gateways, or smart devices, thereby reducing latency and bandwidth consumption (Khan, 2024). By minimizing dependence on distant cloud servers, edge computing enhances efficiency, improves response times, and optimizes resource usage. An essential advantage of edge computing is its ability to enhance data security and privacy by filtering and aggregating information locally before transmitting it across the network (Labba et al., 2022). This decentralized approach reduces the risk of data breaches and network congestion, making it particularly beneficial for e-learning platforms that handle sensitive student information. Moreover, it enables seamless learning experiences by providing real-time interaction and personalized learning without excessive dependence on high-bandwidth networks.

While cloud computing remains integral to large-scale data storage and intensive processing, its inherent latency and bandwidth constraints make it less suitable for real-time applications such as virtual classrooms and interactive e-learning platforms. By distributing computational tasks closer to end users, edge computing facilitates faster decision-making and enhances overall system responsiveness. Additionally, an edge-based e-learning ecosystem can be conceptualized as a multi-tiered infrastructure, where sensors, gateways, and local edge devices handle data locally before sending it to intermediate fog nodes or central cloud servers for further processing. This hierarchical approach optimizes network traffic and resource allocation (Khan, 2024).

Deep learning, a powerful subset of machine learning, enables computers to autonomously acquire knowledge from data by constructing hierarchical representations of concepts. Instead of relying on explicit human programming, it learns through experience, building complex ideas from simpler ones through multiple layers of abstraction. This nested architecture, where higher-level features are derived from lower-level ones, allows the system to model intricate patterns and relationships across many processing layers. Its flexibility and scalability make it particularly effective for tasks requiring sophisticated understanding (Bengio et al., 2016; Kim, 2022).

Given these technological advances, combining deep learning with edge computing presents a promising opportunity to overcome the limitations of traditional e-learning infrastructures. By conducting comparative analyses between conventional cloud-based and edge-enabled e-learning systems and examining real-world case studies, this research aims to assess the feasibility, benefits, and challenges of integrating these technologies into modern distance education. The findings of this study will contribute to a deeper understanding of how decentralized computing and intelligent algorithms can enhance learning outcomes, improve accessibility, and address existing infrastructure limitations.

II. The Objective

This study investigates the potential of integrating deep learning (DL) with edge computing (EC) to enhance the accessibility, responsiveness, and personalization of e-learning environments. It aims to consolidate the core principles of DL and EC within a unified e-learning framework, wherein computational processes are shifted to edge devices to reduce latency and improve real-time interaction. By enabling local data processing, the proposed integration addresses critical challenges commonly faced in online education, such as high response times, privacy concerns, and limited internet connectivity. The research envisions an architecture that supports efficient, scalable, and learner-centric digital education through edge-enabled intelligent systems.

III. Problem Statement

Modern e-learning systems increasingly rely on cloud-based architectures to deliver content and power AI-driven features like adaptive learning and real-time analytics. However, these centralized approaches face fundamental limitations: (1) Latency-sensitive applications suffer performance degradation due to network delays; (2) bandwidth-intensive tasks strain infrastructure; and (3) offline functionality gaps disrupt learning continuity during connectivity loss. This study investigates how edge computing, paired with deep learning, can address these systemic constraints by redistributing computational workloads.

IV. Research Questions

This study aims to answer the following research questions:

A. How can the integration of deep learning and edge computing enhance the performance and accessibility of e-learning platforms?
B. What specific advantages does the proposed edge-enabled architecture offer compared to traditional cloud-based e-learning systems?
C. What are the primary technical and infrastructural challenges in deploying deep learning models on edge devices for educational applications?
D. How can the integrated DL-EC framework be optimized to support personalized and inclusive learning experiences across diverse learning environments?

V. Methodology

Utilizing secondary data sources and qualitative analysis, this study employs a descriptive technique to examine the role of edge computing in e-learning. To assess practical effectiveness and implementation challenges, the methodology consists of three main phases:

A. A systematic literature review of academic publications and industry reports on edge computing applications.
B. A systematic literature review of academic publications in deep learning.
C. Conduct a descriptive study on deep learning with edge computing in e-learning; this multifaceted approach provides a strong foundation for understanding current and future developments in e-learning systems.

This research is conducted as a theoretical investigation, aiming to explore concepts and frameworks without involving practical implementation or empirical data collection.

Three-Tier Architecture for an Edge-Based E-Learning System

A. End-User Devices (First Layer)

- **Examples:** Laptops, tablets, smartphones.
- **Functions:**
  - Interaction with the e-learning platform.
  - Access to educational content (even in offline mode).
  - Logging user activities (e.g., quiz responses, time spent).
- **Features:**
  - Supports offline learning.
  - User interface layer.

B. Edge Server (Second Layer – School or Institutional Server)

- **Examples:** A local server hosted within a school or educational institution.
- **Functions:**
  - Hosts a lightweight deep learning model.
  - Provides instant feedback to learners.
  - Delivers personalized content based on user performance.
- **Features:**
  - Reduced latency and faster response times.
  - Enhanced data privacy (no sensitive data sent to the cloud).
  - Localized inference and processing.

C. Cloud Platform (Third Layer – Cloud Infrastructure)

- **Examples:** Google Cloud, AWS, Microsoft Azure.
- **Functions:**
  - Trains the full-scale deep learning model using aggregated data.
  - Performs large-scale analytics and system monitoring.
  - Sends regular model updates to edge servers.
- **Features:**
  - Long-term data storage.
  - Centralized learning analytics.
  - Periodic synchronization with edge servers.

Interaction Between Layers:

- **End-User ↔ Edge:** Real-time communication for instant analysis and feedback.
- **Edge ↔ Cloud:** Periodic exchange of anonymized summaries and model updates.

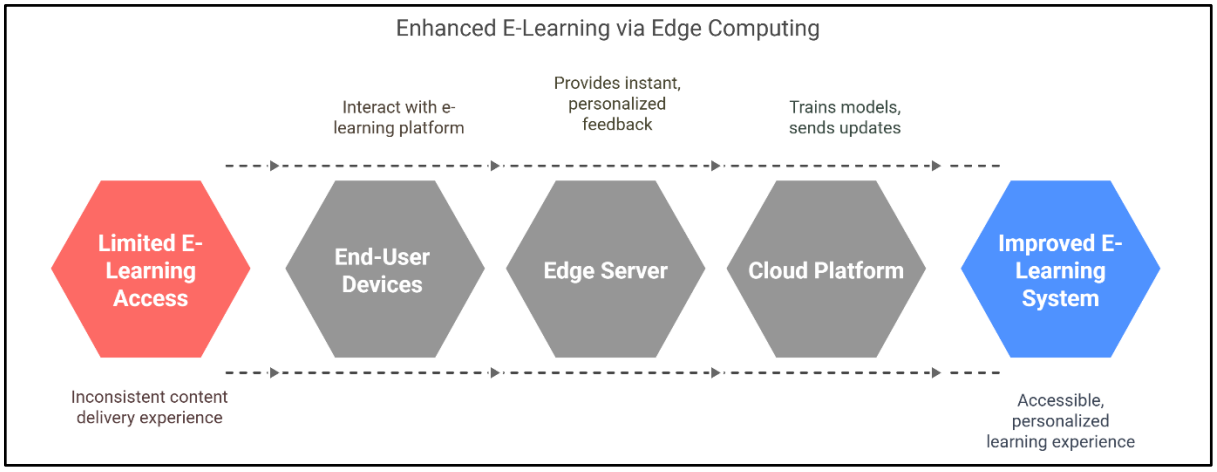


Figure (1): Three-Tier Architecture for an Edge-Based E-Learning System

Interaction Between Layers:

- **End-User ↔ Edge:** Real-time communication for instant analysis and feedback.
- **Edge ↔ Cloud:** Periodic exchange of anonymized summaries and model updates.

VI. Literature Review

The convergence of deep learning and edge computing in e-learning presents significant opportunities to improve accessibility and performance. By providing personalized, responsive, and secure learning experiences, this integration is poised to reshape how educational resources are delivered and experienced globally. Continued research into optimizing these technologies will be vital as the educational landscape evolves.

- (Boutabia et al., 2024): In the wake of the COVID-19 pandemic, the educational system found itself in dire need of a reliable tool to continue its activities. Enter the e-learning system, a tool that had been overlooked or forgotten by many of its users. One of the most promising trends in e-learning is the open classrooms (OCR) approach, which aims to provide an all-encompassing online education that is easily accessible to everyone, thereby enabling numerous individuals to enhance their skills and capabilities. Over the years, there have been many attempts to integrate deep-learning techniques into the OCR approach to enhance performance and improve results. To gain a better understanding of this topic, our paper presents a comprehensive literature review of researchers who have used deep-learning approaches to improve the outcomes of e-learning in open classrooms. Our primary focus is on individuals who employ neural network-based techniques, such as artificial neural networks, convolutional neural networks, deep neural networks, recurrent neural networks, and hybrid approaches. After conducting a thorough evaluation of the selected methods, we have been able to identify their respective strengths and weaknesses. By scrutinizing these approaches, we have successfully outlined the benefits and drawbacks of each, allowing us to provide a confident and informative analysis of this important subject.
- (Almelu et al., 2022): This research paper provides a comprehensive review of deep reinforcement learning (DRL) approaches, particularly Q-learning, for optimizing task offloading in edge computing systems within IoT networks. The study highlights the challenges of traditional cloud computing models, such as high latency, bandwidth constraints, and energy inefficiency, and emphasizes edge computing's role in decentralizing computational tasks to reduce these issues. By analyzing various existing methods—including Markov Decision Processes (MDP), deep Q-networks (DQN), and hybrid techniques—the authors identify limitations in handling multi-user, multi-task scenarios and dynamic environments due to problems like dimensionality, overestimation in Q-learning, and resource allocation inefficiencies. The paper proposes a modified Q-learning-based DRL framework designed to optimize task offloading decisions by minimizing computational costs, energy consumption, and latency while improving scalability for heterogeneous IoT environments. Through a comparative analysis of prior works, the study underscores the tradeoffs between energy efficiency and quality of service (QoS) and concludes that adaptive reinforcement learning strategies are critical for achieving efficient, real-time task offloading in increasingly complex edge-IoT ecosystems.
- (Bhat et al., 2022): Implementation of Information and Communication Technologies (ICT) in E-Learning environments has brought about dramatic changes in the current educational sector. Distance learning, online learning, and networked learning are a few examples that promote educational interaction between students, lecturers, and learning communities. Although being an efficient form of real learning resource, online electronic resources are subject to threats and vulnerabilities on the internet. Authentication, access, and storage of data are major concerns among many organizations implementing e-learning platforms. This study provides a literature review of the past five years of research studies and proposes an edge-computing-based solution to the currently existing authentication and data access problems that prevail in the current e-learning management systems

using cloud services for data storage. The study guides researchers towards enabling edge-computing-based e-learning platforms to support low-power computing devices running elliptic curve cryptography for secure access and authentication.

- (Fri & Elouahbi, 2020): E-learning has been one of the major trends in education, and it's becoming an attractive topic in the field of artificial intelligence and its subfields like machine learning and deep learning, which are considered the most promising technologies in our era, where its application score is almost unlimited. Many researchers are showing interest in the topic with significant research results. This paper aims to extract the applications of machine learning and deep learning in e-learning systems. In this work, we collected research papers from five research databases: SpringerLink, ScienceDirect, Scopus, IEEE Digital Library, and Web of Science for a topic modeling application using a machine learning technique known as Latent Dirichlet Allocation (LDA).
- (Calle-Jimenez et al., 2021): Currently, millions of people are studying professional training using e-learning environments. A trend that has been exacerbated by the global health crisis caused by the COVID-19 virus pandemic. This circumstance has forced students around the world to switch to an emerging online modality in 2020. E-learning environments have become an important option, maybe the only one, to keep studying, as long as these environments and the educational resources they host are accessible. In this context, it is relevant to have a mechanism to describe the accessibility preferences and needs of students through the management of personal profiles. In this study, the authors carried out a literature review regarding models designed to enable the creation of profiles in Massive Open Online Courses (MOOCs) and presented an analysis of scientific research published by other researchers and showed the current state of the art of the research area of profiling of students with disabilities in MOOC platforms. This literature review will serve as input to propose a model that allows covering the lack of profiling of students with disabilities within e-learning platforms to meet the needs of students who have disabilities. As far as we know, this is the first literature review of this kind.
- (Aslam et al., 2021): The advancement of AI has led to a shift toward adaptive and personalized e-learning as traditional approaches become less effective. Institutions are integrating AI into academic curricula and research strategies to enhance learning outcomes. This review examines studies from 1993 to 2020, analyzing machine learning (ML) techniques such as supervised, semi-supervised, and reinforcement learning to optimize e-learning models. Key features influencing system performance include individual, course, context, and technology-pertinent features. Support Vector Machines (SVM) have been identified as effective for predicting input and output parameters, while Fuzzy C-Means and Deep Learning perform well with large datasets. This study provides insights into AI-driven e-learning improvements and future research opportunities.
- (Chen & Ran, 2019)**:** Deep learning is currently widely used in a variety of applications, including computer vision and natural language processing. End devices, such as smartphones and Internet-of-Things sensors, are generating data that need to be analyzed in real time using deep learning or used to train deep learning models. However, deep learning inference and training require substantial computational resources to dash. Edge computing, where a fine mesh of compute nodes are placed close to end devices, is a viable way to meet the high computation and low-latency requirements of deep learning on edge devices and also provides additional benefits in terms of privacy, bandwidth efficiency, and scalability. This paper aims to provide a comprehensive review of the current state of the art at the intersection of deep learning and edge computing. Specifically, it will provide an overview of applications where deep learning is used at the network edge, discuss various approaches for quickly executing deep learning inference across a combination of end devices, edge servers, and the cloud, and describe the methods for training deep learning models across multiple edge devices. It will also discuss open challenges in terms of systems performance, network technologies and management, benchmarks, and privacy. The reader will take away the following concepts from this paper: understanding scenarios where deep learning at the network edge can be useful, understanding common techniques for speeding up deep learning inference and performing distributed training on edge devices, and understanding recent trends and opportunities.

VII. DEEP LEARNING

Deep learning is a subfield of machine learning that employs multi-layered artificial neural networks to learn abstract representations of data hierarchically. By progressively transforming raw inputs into higher-level features through non-linear processing, it models complex relationships within data for tasks such as pattern recognition, classification, and feature extraction. This approach enhances the ability to interpret diverse data types (e.g., images, sound, text) and achieves robust performance through supervised and unsupervised learning methods. (Deng & Yu, 2013) Deep learning is a powerful branch of machine learning that uses multi-layered neural networks to understand data at different levels of complexity. It enables computers to handle tricky tasks like diagnosing diseases, recognizing faces, powering self-driving cars, and spotting fraud. There are two main types of deep learning models: (Fri & Elouahbi, 2020)

A. Convolutional Neural Networks (CNNs)

These are the go-to for anything visual, such as photo analysis, face recognition, or sorting videos. They're also handy for tasks like reading text or understanding language.

B. Recurrent Neural Networks (RNNs)

These specialize in sequences, like speech or language. They're behind tools like voice assistants and real-time translation.

VIII. History of Edge Computing

Edge computing didn't just appear overnight - it grew out of real frustrations with traditional cloud systems. Remember when everything ran through those massive, faraway data centers? That worked fine until we needed instant responses for self-driving cars, smart factories, and augmented reality. The delay was just too much. Tech companies started solving this piece by piece, first with CDNs that stored popular content closer to users, then with Cisco's "fog computing" concept that pushed processing power out to the network's edge.

But the real game-changer was the explosion of smart devices. Suddenly, we had sensors everywhere, generating oceans of data that couldn't wait for a round trip to the cloud. Then 5G came along with its lightning-fast speeds, and suddenly, edge computing wasn't just helpful - it became essential. What started as a workaround for laggy apps has now become the backbone of our real-time digital world. (Khan, 2024).

IX. Edge Computing Applications:

Edge computing transforms various sectors by enabling real-time data processing closer to the source. (S. Wang, 2019) Key applications include:

A. **Healthcare:** Supports remote patient monitoring (e.g., fall detection via smartphones) and enables faster medical data analysis while preserving privacy.
B. **Video Analytics:** Processes surveillance footage locally at edge servers, reducing cloud bandwidth needs and improving response times for security applications.
C. **Connected Vehicles:** Allows cars to process traffic data and communicate risks peer-to-peer, minimizing accidents caused by cloud latency.
D. **Mobile Big Data:** Edge servers near devices enable faster analytics for business insights while reducing core network load.
E. **Smart Buildings:** Sensors monitor environmental conditions (temperature, air quality) and trigger instant adjustments through edge-based decision-making.
F. **Marine Monitoring:** Processes ocean sensor data locally to predict real-time climate events and disasters.
G. **Smart Homes** – Home gateways handle private data (like security footage) locally, enhancing privacy and reducing cloud dependence.
H. **Smart Cities:** Streetlight-mounted sensors monitor infrastructure and environment, enabling immediate maintenance alerts and public safety responses.

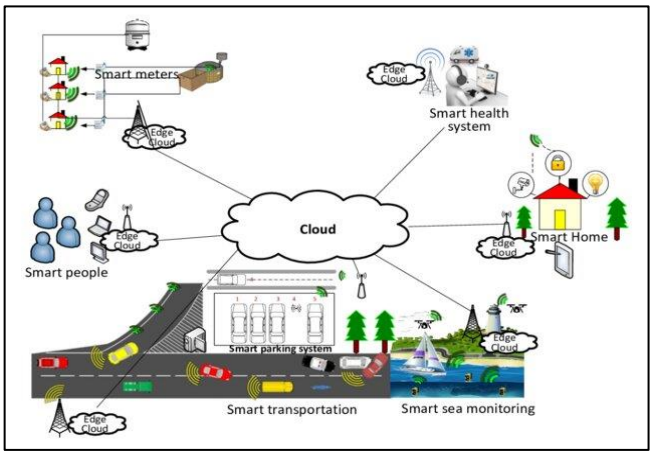


Figure (2) Edge Computing Applications

X. Edge Computing vs. Cloud Computing

Edge computing is an attractive alternative, especially for hosting computation tasks as close to the data sources and end users as possible. Cloud computing and edge computing are not incompatible. Rather, the edge expands and enhances the cloud. The primary benefits of edge computing in conjunction with cloud computing are as follows when compared to cloud computing alone: reduction of the backbone network's traffic burden; dispersed edge computing nodes are capable of performing several calculation activities without sharing the relevant data with the cloud; Agile service response: services housed at the edge may greatly speed up response times and minimize data transmission delays; robust cloud backup: when the edge cannot afford it, the cloud can offer enormous storage and processing capability. (X. Wang et al., 2020)

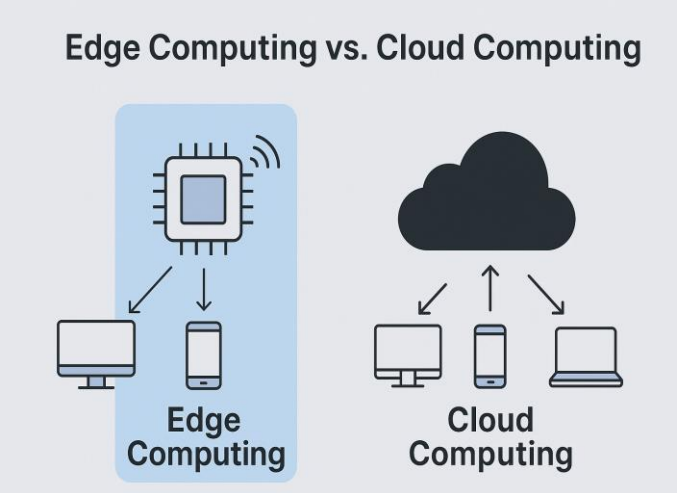


Figure (3): Edge Computing vs. Cloud Computing

Table (1): Edge Computing vs. Cloud Computing characteristics

Characteristics	Cloud Computing	Edge Computing
Latency	High	Low
Bandwidth Utilization	High	Very Low
Response Time	High	Low
Storage	High	Low
Server Overhead	Very High	Very Low
Energy Consumption	High	Low
Network Congestion	Very High	Low
Scalability	Medium	High
QoS & QoE	Medium	High

Source: (Alidoust & Lahijan, 2025)

The table compares the performance characteristics of cloud computing and edge computing, highlighting key differences in efficiency and functionality. Cloud computing typically experiences higher latency and slower response times due to data traveling to distant centralized servers, while edge computing processes data locally, significantly reducing delays.Bandwidth usage is also greater in cloud systems since all raw data must be transmitted over the network, whereas edge computing minimizes bandwidth consumption by filtering and analyzing data on-site. While cloud platforms offer vast storage capacity, edge devices have limited storage due to their decentralized and compact nature. Additionally, cloud environments suffer from higher server overhead and energy consumption because they rely on large-scale, always-on data centers. In contrast, edge computing distributes workloads across local nodes, optimizing power usage. Cloud systems can also lead to network congestion from continuous data transfers, a problem that edge computing mitigates by handling most processing closer to the source. In terms of scalability, cloud solutions require significant investment and face network limitations, while edge computing allows for more flexible and cost-effective expansion by deploying additional local devices. Ultimately, edge computing provides superior Quality of Service (QoS) and Quality of Experience (QoE) by enabling faster, more reliable, and context-aware responses for end-users, making it a more efficient solution for real-time applications compared to traditional cloud-based approaches.

XI. Deep Learning with E-Learning

Deep learning is revolutionizing e-learning by enhancing personalization and resource management. It enables intuitive algorithms and automated content delivery through modern Learning Management Systems (LMS) (Muniasamy & Alasiry, 2020). Deep learning techniques can automate feature engineering for the vast amounts of data generated in e-learning environments, improving efficiency over traditional manual methods (Chanaa & El Faddouli, 2018). The integration of deep learning with e-learning platforms facilitates the sharing of learning objects across different LMS and e-learning standards (Xu, 2023). This approach allows for more personalized learning experiences by leveraging predictions, algorithms, and analytics (Muniasamy & Alasiry, 2020). Additionally, deep learning can be applied to develop face recognition systems for monitoring student progress and knowledge levels (Xu, 2023). By repurposing existing resources, deep learning helps mitigate the costs associated with content development for future e-learning systems (Muniasamy & Alasiry, 2020).

E-learning is about using digital tools and technology to make learning more accessible, interactive, and effective. Instead of relying solely on traditional classrooms, it leverages electronic media, like computers, tablets, and online platforms, to deliver education flexibly.

Types of E-Learning: Timing Matters

One key way to categorize e-learning is by timing, when students can access content:

A. Synchronous Learning: Live, real-time classes where teachers and students interact simultaneously, just like a virtual classroom. Think Zoom lectures or live webinars.
B. Asynchronous Learning: On-demand learning where students can access materials anytime, anywhere. Discussion forums, prerecorded videos, and self-paced courses fall into this category. (Fri & Elouahbi, 2020)

The Building Blocks of E-Learning

A. A great e-learning experience depends on five core components:
B. Audience: Who's learning? (Students, professionals, etc.)
C. Course Structure: How is the content organized?
D. Page Design: Is it visually engaging and easy to navigate?
E. Content Engagement: Does it hold learners' attention?
F. Usability: Is the platform intuitive and user-friendly?

XII. Edge Computing with E-Learning

Edge computing is emerging as a promising approach to enhance e-learning platforms by addressing challenges in data security, privacy, and real-time feedback. It brings computation closer to data sources, improving efficiency and reducing latency. (Labba et al., 2022) Integrating artificial intelligence with edge computing enables real-time assessment of learners while preserving privacy (Labba et al., 2022). Edge-based solutions can enhance authentication and data access in e-learning management systems, with proposed implementations using elliptic curve cryptography for secure access (Bhat et al., 2022). Advanced searching techniques, such as searchable encryption and quantum harmonic oscillator models, can improve content retrieval in cloud-assisted edge computing environments. The education industry can benefit from edge computing by optimizing resource utilization and ensuring continuous availability and

seamless delivery of educational content, even with restricted resources.

XIII. Deep Learning with Edge Computing

Deep learning in edge computing environments is gaining traction for IoT and industrial applications, offering benefits such as reduced latency, improved privacy, and bandwidth efficiency compared to cloud-based approaches (Chen & Ran, 2019). Researchers have proposed strategies to optimize deep learning performance on edge devices with limited processing capabilities (Li et al., 2018). Edge-based deep learning has been implemented in industrial IoT systems, demonstrating reduced network traffic while maintaining classification accuracy (Liang et al., 2020). Recent advancements include lightweight models for wheel-rail force monitoring in railway systems, privacy-preserving recommender systems that utilize differential privacy, and efficient block-sparse neural networks leveraging GPU capabilities in edge environments (Liu, 2022). These developments underscore the potential of edge computing to accelerate deep learning applications across various domains while addressing challenges related to computation, privacy, and resource efficiency.

With the growing presence of edge devices like smartphones, wearables, and IoT sensors, these tools are becoming increasingly capable of collecting, processing, and even developing data locally. This opens the door for them to serve as alternatives to traditional cloud-based deep neural network (DNN) processing. However, advanced DNNs typically require substantial computing power, memory, and energy resources that edge devices often lack. Here are some challenges to be faced: (Zhang et al., 2020)

Challenges and Opportunities

A. Limited Resources

DNNs are demanding when it comes to computational power and memory, which most edge devices can't easily handle. The solution depends on techniques like model compression (e.g., pruning and quantization), lightweight architectures (like MobileNets), and knowledge distillation that can make models more efficient.

B. Data Mismatch

Sensor data collected in real-world environments often differs from training data due to things like lighting changes or motion blur, so data augmentation techniques and noise-resistant loss functions (such as triplet loss) can make models more robust to these inconsistencies.

C. Battery Limitations

Energy-hungry components like cameras can quickly drain a device's battery. On the other hand, using smarter techniques like selective data sampling, switching between high- and low-resolution sensing modes, or using analog signal processing to skip power-intensive digital conversions.

D. Diverse Hardware and Data

Edge devices often deal with varied data sources like GPS, video, and audio and come equipped with different types of processors (CPUs, GPUs, TPUs), so Multimodal DNNs that combine different neural architectures (like CNNs and RNNs) can process diverse data. Meanwhile, compilers that are aware of the device's architecture can allocate tasks more efficiently.

E. Running Multiple Tasks

Running several DNN-based tasks at the same time, like face recognition and emotion detection, can overwhelm device resources. Using shared data pipelines and multitask learning can help by reusing features across different tasks, reducing redundant processing.

F. Offloading and Privacy Concerns

Sending data to the cloud for processing can introduce delays and raise privacy concerns. Offloading computation to nearby edge devices (instead of the cloud), splitting models between devices and servers, or even training directly on the device can help maintain privacy and reduce latency.

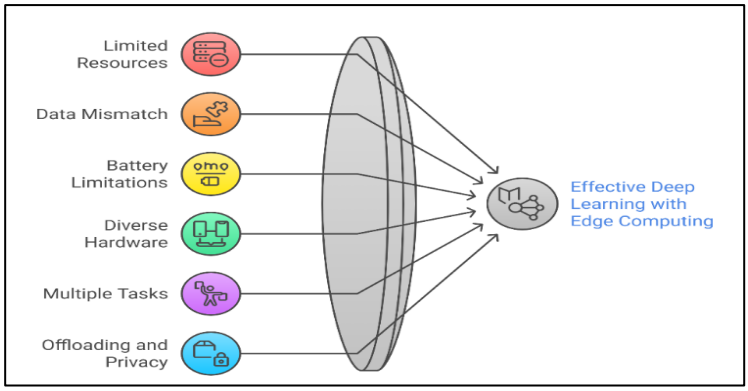


Figure (4): Challenges of Deep learning with Edge computing

Deep learning is advancing at an incredible pace, but for researchers and developers working on edge devices, picking the right neural network model isn't easy. The problem? There's no consistent way to compare models directly on the actual hardware they'll run on. While new machine learning papers often include comparisons with older models, the selection is usually up to the authors, meaning key models or hardware platforms might be left out. And dedicated benchmarking studies? They can become outdated almost as soon as they're published, given how quickly new models appear.

What the community needs is an open, up-to-date repository with fair, standardized benchmarks across different models and edge hardware. Luckily, some pieces of the puzzle already exist - standard datasets (like those for image classification or NLP) and widely used frameworks help, but for edge computing, the real challenge is testing across the full spectrum of devices, from simple ones like Raspberry Pis to smartphones, home gateways, and edge servers. Right now, most research focuses on either high-powered servers or smartphones, but as deep learning moves into more diverse edge environments, we need a clearer picture of how these models perform across all kinds of hardware. (Chen & Ran, 2019)

XIV. Framework Design:

According to Huang et al. (2017), the researchers created an edge learning system that smartly distributes AI tasks across three tiers for optimal performance. Everyday devices like phones and IoT sensors collect raw, often messy, real-world data, which then gets processed by nearby edge servers that act as local 'brain hubs' - these clean up the data, remove noise and redundancy, and extract key features using techniques like PCA. The refined data then goes to powerful cloud-based GPU clusters for heavy-duty deep learning tasks like CNN/LSTM model training. This approach delivers two key benefits: first, it dramatically reduces network strain by processing data locally before sending it to the cloud, and second, it enables faster responses since edge servers are physically closer to users than distant cloud data centers. The system creates a continuous improvement loop where cloud-trained models get deployed to edge servers for real-time use while new data flows back to update and refine the models.

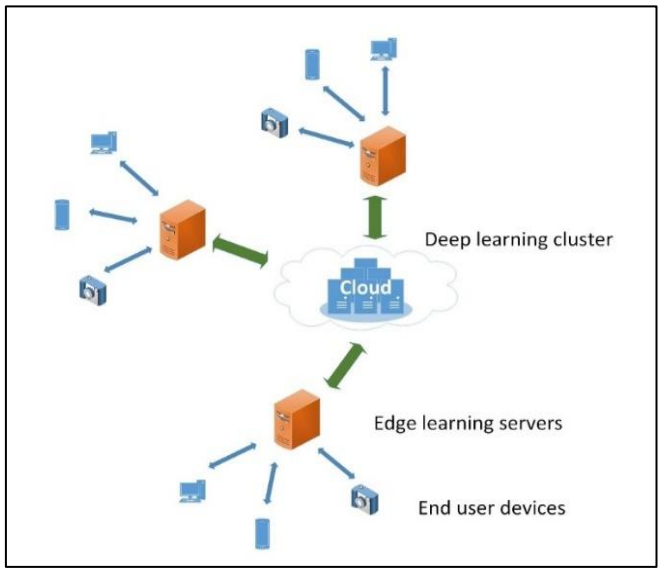


Figure (5): The edge learning framework

XV. The Results:

To integrate deep learning (DL) and edge computing (EC) in e-learning systems, this work synthesizes contemporary literature, architectural modeling, and theoretical analysis to offer conceptual findings. The suggested three-tier design, which consists of centralized cloud infrastructure, institutional edge servers, and end-user devices, shows several possible benefits based on current research trends and technical viability. The following significant findings are shown by contrasting the suggested edge-enabled architecture with current cloud-based systems:

A. **Latency Reduction:** Learning systems can provide feedback nearly in real-time, enabling responsive engagement even in low-connectivity environments by deploying lightweight deep learning models at the edge.
B. **Increased Accessibility:** By supporting localized processing and offline learning features, edge devices extend e-learning to underserved or rural areas with unreliable or limited internet access.
C. **Improved Security and Privacy:** By reducing the need to transmit sensitive student data, local data preprocessing at the edge minimizes the risk of centralized breaches and aligns with current data protection laws.
D. **System Scalability and Resource Optimization:** The hierarchical architecture allows for effective load balancing between layers. While the cloud layer handles centralized training and long-term analytics, easing infrastructure demands, edge servers manage real-time, context-aware tasks.
E. **Support for Personalization:** By enabling dynamic content and feedback adjustments based on learner behavior and preferences, local deployment of deep learning models enhances learning outcomes and engagement.

Table (2): Edge Computing vs. Cloud Computing characteristics vs. Proposed Edge-based DL E-learning

Characteristic	Cloud Computing	Edge Computing	Proposed Edge-based DL E-learning
Latency	High	Low	Very Low (Near real-time response)
Bandwidth Utilization	High	Very Low	Low (Local data filtering and processing)
Response Time	High	Low	Low (Instant feedback to learners)
Storage Capacity	High	Limited	Hybrid (Edge caching + Cloud storage)
Server Overhead	Very High	Very Low	Balanced (Distributed between edge and cloud layers)
Energy Consumption	High	Low	Medium (optimized via lightweight DL models)
Network Congestion	Very High	Low	Low (Reduced data transmission and centralized load)
Scalability	Medium	High	High (Flexible scaling through hybrid architecture)
Quality of Service (QoS)	Medium	High	High (Reliable and intelligent content delivery)
Quality of Experience (QoE)	Medium	High	Very High (Personalized, adaptive, and responsive learning)

A theoretical comparison of edge computing, conventional cloud computing, and the suggested edge-based deep learning (DL) architecture for e-learning is shown in table 2. The suggested model addresses the shortcomings of both cloud and edge paradigms while combining their benefits. By using lightweight DL models at the edge, it greatly lowers latency and speeds up reaction times, allowing for real-time feedback and communication. Local data processing reduces network congestion and bandwidth utilization. To maximize speed and scalability, the suggested design distributes processing and storage across edge and cloud layers, in contrast to cloud-only systems that concentrate these tasks.

All things considered, this hybrid design offers learners a better quality of service (QoS) and quality of experience (QoE) by creating a more flexible, safe, and accessible learning environment, particularly in situations with poor connection.

XVI. Contribution

Although the combination of deep learning (DL) and edge computing (EC) has been extensively investigated in domains including computer vision, natural language processing, and the Internet of Things (IoT), its use in e-learning is still noticeably underrepresented. Although the promise of edge intelligence in various fields is highlighted in existing research, such as Chen and Ran's (2019) thorough assessment, this analysis does not extend to educational technology.

This research will contribute by putting forth a conceptual edge-based DL framework designed especially for online learning settings. The system seeks to improve learner privacy through local processing, facilitate offline learning through edge deployment, and enable real-time content customization. By doing this, the article offers a fresh contextual application of DL-EC integration, emphasizing deployment difficulties, architectural issues, and system-level modifications particular to the curriculum. For more empirical studies and system development in edge-enabled e-learning, this targeted contribution provides a starting point.

XVII. Discussion

The development and implementation of e-learning platforms are evolving due to the convergence of deep learning (DL) and edge computing (EC). While cloud computing remains essential for long-term storage and model training, edge devices are increasingly capable of handling inference and real-time tasks. Besides reducing latency, this decentralization enables institutions to offer personalized learning experiences, even in areas with limited connectivity. However, deploying DL models on edge hardware requires techniques such as resource-aware offloading, effective multitasking, and model compression. The integration

becomes increasingly practical and significant as the capabilities of edge devices improve, especially with the emergence of 5G and lightweight DL versions.

Limitations

The widespread use of DL-EC systems in e-learning is hampered by several issues, despite the apparent advantages, such as:

A. ***Hardware Restrictions:*** Without optimizations, many edge devices lack the memory and processing capacity to implement sophisticated DNNs.
B. **Standardization Gaps:** To assess DL model performance across various edge devices, there aren't enough standardized benchmarking frameworks.
C. **Data Variability:** Model accuracy is impacted by the frequent deviations between training datasets and real-world sensor data.
D. Battery life is still an issue for mobile edge devices that use continuous inference.
E. **Security Risks:** While edge computing lowers data exposure, it also creates new device-level vulnerabilities.

XVIII. Future Directions

A. **Lightweight AI Models**: To balance performance and resource use, create incredibly efficient architectures (like TinyML) specifically for edge devices.
B. **Privacy-Enhancing Technologies:** Expand federated learning and homomorphic encryption to enable collaborative model training without data exposure.
C. **5G/6G Integration:** Make use of fast networks to improve edge-cloud synchronization, allowing for low-latency apps and smooth updates.
D. **Energy-Efficient Designs:** To reduce power consumption, look at edge-specific hardware (such as neuromorphic processors) and adaptive algorithms.
E. **Standardized Frameworks:** To simplify deployment across a range of devices, provide standard benchmarks and tools (such as edge-aware compilers).
F. Dynamic task offloading according to current network circumstances and device capabilities is known as hybrid edge-cloud orchestration.

XIX. Conclusion

Integrating deep learning with edge computing offers a transformative solution to the long-standing challenges faced by e-learning systems. By moving computational intelligence closer to the data source, this approach improves responsiveness, security, and personalization in digital education. While technical and infrastructural challenges remain, ongoing research and innovation in this field have the potential to revolutionize educational access and quality, especially in under-resourced regions. This study establishes a foundation for future implementations that adopt intelligent edge architectures to develop resilient, inclusive, and high-performance e-learning ecosystems.

References

[1] A. Alidoust and M. Lahijan, "Using Deep Learning in Edge Computing-based IoT for Security & Privacy Preservation," Jan. 2025.
[2] S. Almelu, S. Veenadhari, and K. Maheshwar, "A Review on Performance Analysis of Deep Learning for Task Offloading in Edge Computing," *SAMRIDDHI: A J. Phys. Sci., Eng. Technol.*, vol. 14, no. 4, pp. 159–164, 2022, doi: 10.18090/samriddhi.v14i04.26.
[3] S. M. Aslam, A. K. Jilani, J. Sultana, and L. Almutairi, "Feature Evaluation of Emerging E-Learning Systems Using Machine Learning: An Extensive Survey," *IEEE Access*, vol. 9, pp. 69573–69587, 2021, doi: 10.1109/ACCESS.2021.3077663.
[4] Y. Bengio, I. Goodfellow, and A. Courville, *Deep Learning*. MIT Press, 2016. [Online]. Available: http://deeplearning.net/
[5] S. A. Bhat, D. Alyahya, M. A. Dar, and S. Shah, "Edge-Computing based Secure E-learning Platforms," in *Proc. Int. Conf. Artif. Intell. Inf. Commun. (ICAIIC)*, 2022, pp. 324–328, doi: 10.1109/ICAIIC54071.2022.9722680.
[6] I. Boutabia, A. Benmachiche, A. A. Betouil, and C. Chemam, "A Survey in the Use of Deep Learning Techniques in The Open Classroom Approach," in *Proc. Int. Conf. Pattern Anal. Intell. Syst. (PAIS)*, 2024, pp. 1–7, doi: 10.1109/PAIS62114.2024.10541268.
[7] T. Calle-Jimenez, S. Sanchez-Gordon, and H. Arias-Flores, "Profiling of E-Learning Users with Accessibility Needs," in *Lecture Notes in Networks and Systems*, vol. 275, Springer, 2021. doi: 10.1007/978-3-030-80091-8_56.
[8] A. Chanaa and N. E. El Faddouli, "Deep learning for a smart e-learning system," in *Proc. Int. Conf. Cloud Comput. Technol. Appl. (CloudTech)*, 2018, doi: 10.1109/CloudTech.2018.8713335.
[9] J. Chen and X. Ran, "Deep Learning with Edge Computing: A Review," *Proc. IEEE*, vol. 107, no. 8, pp. 1655–1674, 2019, doi: 10.1109/JPROC.2019.2921977.
[10] L. Deng and D. Yu, "Deep learning: Methods and applications," *Found. Trends Signal Process.*, vol. 7, no. 3–4, pp. 197–387, 2013, doi: 10.1561/2000000039.
[11] C. Fri and R. Elouahbi, "Machine learning and deep learning applications in E-learning Systems: A literature survey using topic modeling approach," in *Colloquium Inf. Sci. Technol. (CiSt)*, 2020, pp. 267–273, doi: 10.1109/CiSt49399.2021.9357253.
[12] Y. Huang, X. Ma, X. Fan, J. Liu, and W. Gong, "When deep learning meets edge computing," in *Proc. IEEE Int. Conf. Netw. Protocols (ICNP)*, 2017, pp. 1–2, doi: 10.1109/ICNP.2017.8117585.

[13] K. Khan, *Lecture Notes on Edge Computing*, Dec. 2024. doi: 10.13140/RG.2.2.12888.61444.

[14] H. Kim, "Deep Learning," in *Artif. Intell. for 6G*, vol. 22, no. 4, pp. 247–303, 2022, doi: 10.1007/978-3-030-95041-5_6.

[15] C. Labba, R. Ben Atitallah, and A. Boyer, "Combining Artificial Intelligence and Edge Computing to Reshape Distance Education (Case Study: K-12 Learners)," in *Lecture Notes in Comput. Sci.*, vol. 13355, pp. 218–230, 2022, doi: 10.1007/978-3-031-11644-5_18.

[16] H. Li, K. Ota, and M. Dong, "Learning IoT in Edge: Deep Learning for the Internet of Things with Edge Computing," *IEEE Netw.*, vol. 32, no. 1, pp. 96–101, 2018, doi: 10.1109/MNET.2018.1700202.

[17] F. Liang, W. Yu, X. Liu, D. Griffith, and N. Golmie, "Toward Edge-Based Deep Learning in Industrial Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 4329–4341, 2020, doi: 10.1109/JIOT.2019.2963635.

[18] X. Liu, "Editorial for special issue on 'Edge computing accelerated deep learning: Technologies and applications'," *Concurrency Comput. Pract. Exp.*, vol. 36, no. 10, p. 7345, 2022, doi: 10.1002/cpe.7345.

[19] A. Muniasamy and A. Alasiry, "Deep learning: The impact on future eLearning," *Int. J. Emerg. Technol. Learn.*, vol. 15, no. 1, pp. 188–199, 2020, doi: 10.3991/IJET.V15I01.11435.

[20] S. Wang, "Edge Computing: Applications, State-of-the-Art and Challenges," *Adv. Netw.*, vol. 7, no. 1, p. 8, 2019, doi: 10.11648/j.net.20190701.12.

[21] X. Wang, Y. Han, V. C. M. Leung, D. Niyato, X. Yan, and X. Chen, "Convergence of Edge Computing and Deep Learning: A Comprehensive Survey," *IEEE Commun. Surv. Tutor.*, vol. 22, no. 2, pp. 869–904, 2020, doi: 10.1109/COMST.2020.2970550.

[22] W. Xu, "An Improved Computational Solution for Cloud-Enabled E-Learning Platforms Using a Deep Learning Technique," *Int. J. E-Collab.*, vol. 19, no. 1, pp. 1–19, 2023, doi: 10.4018/IJeC.316664.

[23] M. Zhang *et al.*, "Deep learning in the era of edge computing: Challenges and opportunities," in *Fog Comput.: Theory Pract.*, pp. 67–78, 2020, doi: 10.1002/9781119551713.ch3.

Development of New Flexible Lifetime Model: its Associated Inferences and Applications to Cancer and Covid-19 Data

Samuel Adewale Aderoju [1, *]
Kazeem Adesina Dauda [1,2]
Julius Babatunde Olaifa [1]

Received: 24/03/2025
Revised: 16/04/2025
Accepted: 17/04/2025

[1] Department of Mathematics and Statistics, Kwara State University, Malate, Nigeria
[2] Department of Mathematics, University of Bergen, 5007 Bergen, Norway
*Corresponding Author's Email: samuel.aderoju@kwasu.edu.ng

Development of New Flexible Lifetime Model: its Associated Inferences and Applications to Cancer and Covid-19 Data

Samuel Adewale Aderoju
Department of Mathematics and Statistics, Kwara State University, Malate, Nigeria
samuel.aderoju@kwasu.edu.ng

Kazeem Adesina Dauda
Department of Mathematics and Statistics, Kwara State University, Malate, Nigeria,
Department of Mathematics, University of Bergen, 5007 Bergen, Norway

Julius Babatunde Olaifa
Department of Mathematics and Statistics, Kwara State University, Malate, Nigeria

Abstract— In this paper, a New Two-Parameter Generalized Lindley Distribution (NTGLD) for modelling lifetime data is proposed, which is designed to enhance the flexibility and applicability of the Lindley distribution in real data analysis. Key statistical properties such as the first four moments about the origin, coefficient of variation, hazard and survival functions of the NTGLD are equally obtained. The parameters of the NTGLD were estimated using the method of maximum likelihood. A comprehensive simulation study compares the efficiency of the estimators is presented. The quantile plot provides further insights, illustrating how the distribution's quantile varies with the parameters α and θ, emphasizing the adaptability of the model to different data structures. The NTGLD is applied to three real datasets: remission times of 128 bladder cancer patients, remission times of 36 bladder cancer patients, and recovery times of 553 Covid-19 patients. In each case, the NTGLD demonstrates superior fit compared to competing models considered in this study. Performance metrics such as Akaike Information Criteria, Akaike Information Criteria Corrected, Hannan–Quinn information criteria and Bayesian Information Criteria consistently favour the NTGLD, underscoring its robustness and effectiveness. This study establishes the NTGLD as a valuable tool for statistical modelling, offering significant improvements over existing distributions considered in terms of flexibility, accuracy, and fit.

Keywords— Generalized Lindley Distribution; Maximum Likelihood Estimation; Quantile Plot; Simulation Study; Covid-19 Data; Cancer Data

I. INTRODUCTION

To date, researchers have developed and are still developing distributions to enhance the analysis and interpretation of lifetime data sets. These distributions are crucial for gaining deeper insights into real-world phenomena. Notably, the methods for constructing new probability distributions have evolved significantly since 1997. The primary goal of developing, extending, or generalizing these distributions is to better explain lifetime phenomena across various fields, such as public health, engineering, and biological sciences [1]. Lifetime distributions, alternatively known as survival distributions or failure time distributions, serve as a cornerstone statistical framework for modeling the time until a specific event occurs [2], [3], [4], and [5]. Traditional distributions like uniform, beta, exponential, Rayleigh, Weibull, and gamma have limited flexibility. For instance, the exponential distribution is tied to a constant hazard function, and the Rayleigh distribution is constrained to increasing hazard functions. The Weibull distribution offers more flexibility, supporting increasing, decreasing, or constant hazard functions, but it cannot model non-monotonic failure rates, such as those with unimodal or bathtub shapes [1]. New distributions generated from emerging families and other probability distribution generators have gained significant attention in the literature due to their flexibility and stability [6]. Johnson et al. [7] and [8] have provided comprehensive reviews of hundreds of continuous univariate distributions. Gomes-Silva et al. [9] noted that recent research has focused more on developing new families of distributions that extend established ones, offering greater flexibility in modeling lifetime data. Similarly, Taketomi et al. [10] conducted an extensive review of parametric distributions used in lifetime models.

Despite the wide-ranging applications of the Lindley distribution [11], it falls short in adequately modeling phenomena characterized by non-monotone failure rates, such as bathtub-shaped or upside-down failure rates. Consequently, many researchers have introduced new generalizations of the traditional Lindley distribution by incorporating one or more shape parameters to enhance the flexibility of both the probability density function (PDF) and the hazard rate function. Some of such significant advancements are the generalized Lindley distribution by Zakerzadeh and Dolati [12], a new class of generalized Lindley distributions introduced by Oluyede and Yang [13], a generalized Lindley distribution with shape considerations presented by Nadarajah et al. [14], the quasi-Lindley distributions (QLD) introduced by Shanker and Mishra [15], and a new generalized Lindley distribution by Abouammoh et al. [16]. In recent years, many probability distributions, such as Lindley, Rayleigh, exponential, Weibull, and gamma, among others, have been extended and applied in statistical analysis for modeling lifetime data. Many researchers used these distributions in different areas of applicability. For instance, Al-Noor and Assi [17] developed a Rayleigh-Rayleigh model with an increasing failure rate and applied it to real-life data and a simulation study. The results of its application to real-life data show that the distribution produced fits that are competitive and compare better, in some cases, to the gamma, Weibull, and lognormal distributions.

Therefore, the literature has seen the development of several extensions and applications of well-established distributions. For example, a one-parameter distribution called the Pranav distribution was proposed by Shukla [18]. The distribution is a mixture of exponential distribution with scale parameter θ and gamma distribution with shape parameter and scale parameter θ. Aderoju [19] introduced the Samade

distribution, which was subsequently extended by Aderoju & Babaniyi [20] and Elangovan & Manivasagan [21]. The Samade distribution has been widely used for modeling survival, reliability data, and its mixture for modeling count data [22], [23]. Hosseini et al. [24] introduced a new one-parameter weighted-Lindley distribution for modeling lifetime data. They derived and investigated some of its basic properties. The application of the model to a real dataset was done to investigate the flexibility of the new weighted-Lindley distribution as compared with other distributions. Meriem et al. [25] introduced the power XLindley (PXL) distribution, a two-parameter extension of the XLindley distribution. Aderoju and Jolayemi [26] explored extensions of the Hamza distribution, which features a unique failure rate function that enhances its applicability in modeling real-world scenarios. Aleshinloye et al. [27] proposed a New Generalized Gamma-Weibull Distribution, while Aderoju and Adeniyi [28] investigated extensions of the Generalized Akash distribution. Tashkandy *et al.* [29] introduced a novel two-parameter distribution called the power-modified XLindley distribution. They developed it through the application of power transformation techniques to the existing modified XLindley distribution [30]. They conducted a thorough examination of its statistical properties, exploring its potential to improve data fitting and modeling accuracy. Aderoju et al. [31] introduced a new three-parameter Weibull-generalized gamma distribution, which provides more flexibility in modeling lifetime data. The results of the model's simulation and application to real-life data suggest that it is a useful alternative to the existing distributions considered in the paper.

The primary objective of this article is to present a new flexible lifetime distribution and some of its characteristics. The distribution is capable of being used in survival analysis of patients suffering from diseases such as cancer, Covid-19, tuberculosis, etc., and can also be used to model the volatility of organic molecules that are relevant to environmental studies. Essentially, a major motivation for this study is to demonstrate that the proposed distribution has the potential to model medical data. In terms of application, the scope of this study is non-censored data, and a simulation study is also involved.

The following is the order of this article. We introduce the new lifetime distribution called a new two-parameter generalized Lindley (NTGL) distribution in Section 2. The mathematical properties of the NTGL distribution are presented in Section 3. The parameter estimation of the NTGL distribution and simulation study are covered in Section 4. The application to real data analysis is analyzed in Section 5. The conclusions are provided in Section 6.

II. MATERIAL AND METHOD

The new two-parameter generalized Lindley (NTGL) distribution, characterized by the parameters a and q, is defined through its probability density function (PDF). This PDF follows the general structure of a k-component additive mixture distribution, as outlined by Everitt and Hand [32]. Specifically, for a random variable x, the PDF is given by:

$$f(x,\theta) = \sum_{j=1}^{k} p_j f_j(x,\theta_j), \qquad (1)$$

where θ_j is the vector of parameters for the mixture models, p_j is the mixture proportion and $\sum_{j=1}^{k} p_j = 1$.

Definition: A random variable X with a PDF representing the two-parameter generalized Lindley distribution is expressed as:

$$f(x;\alpha,\theta) = \frac{\theta^2}{4+\theta^2}\left(\theta + \frac{4x^{\alpha-2}\theta^{\alpha-3}}{\Gamma(\alpha-1)}\right)\mathrm{e}^{-\theta * x}, \qquad x,\theta > 0, \alpha > 1 \qquad (1)$$

Remark: The PDF (1) can be shown as a mixture of $exponential\,(\theta)$ and $gamma\,(\alpha-1,\theta)$ distributions as follows:

$f(x;\alpha,\theta) = pg_1(x;\theta) + (1-p)g_2(x;\alpha-1,\theta)$,

where

$p = \frac{\theta^2}{\theta^2+4}$, is the mixing proportion (or mixture weight),

$g_1(x;\theta) = \theta \mathrm{e}^{-x\theta}$, $x > 0$

and

$$g_2(x;\alpha-1,\theta) = \frac{\theta^{\alpha-1}x^{\alpha-2}}{\Gamma(\alpha-1)}\mathrm{e}^{-x\theta}, \qquad x,\theta > 0, \alpha > 1.$$

We arbitrarily use $X \sim NTGL(\alpha,\theta)$ to denote the random variable having new two-parameter generalized Lindley distribution with parameters α (shape) and θ (rate) with PDF (1), The probability density curves for some selected values of the shape and scale parameters are presented in Figure 1.

The probability density curves for some selected values of the shape and scale parameters are presented in Figure 1. Some of the curves in this Figure 1 revealed a bimodal distribution, and since the new distribution consists of both exponential and gamma components, our developed methods are well-suited to account for this bimodality if present in the lifetime data, like this simulation scenario.

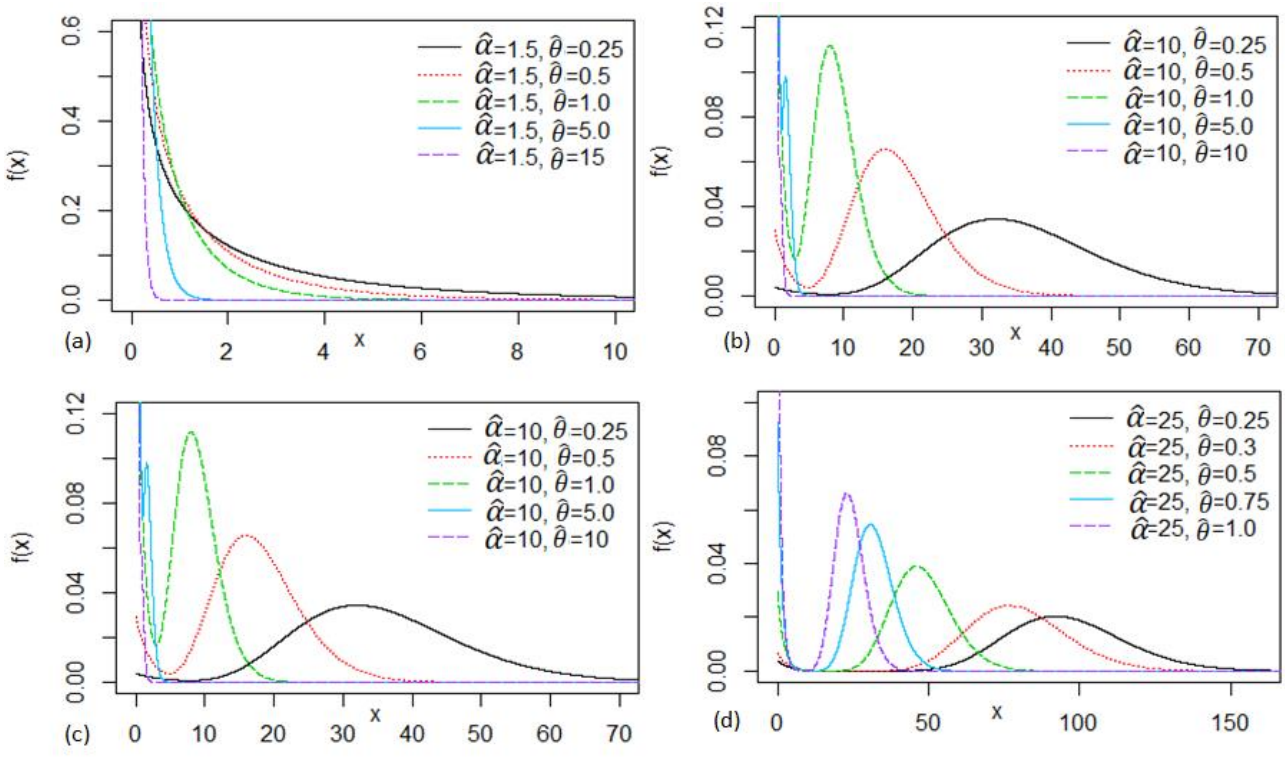


Figure 1: Shape of the NTGL distribution for different values of the parameters

Figure 2 represents the image of a 3D surface plot generated in R, showing the PDF of the NTGL distribution at a fixed value $x = 5$. The plot illustrates how the PDF changes with varying values of the parameters α and θ. Note that X-axis represents the parameter α, ranging from 1.5 to 3, while Y-axis Represents the parameter θ, ranging from 0.5 to 2, and the Z-axis Represents the value of the PDF, ranging from approximately 0 to 0.25. The surface indicates the PDF values corresponding to different combinations of α and θ. The shape of the surface provides insights into how the PDF of the NTGL distribution behaves with changes in these parameters. The plot shows that as α increases, the PDF value increases significantly, especially for larger values of θ. The color gradient on the right side of the plot provides a visual representation of the PDF values: Darker colors represent higher PDF values, while lighter colors represent lower PDF values. Figures 3 illustrates the cdf of the NTGL distribution for various values of the parameters.

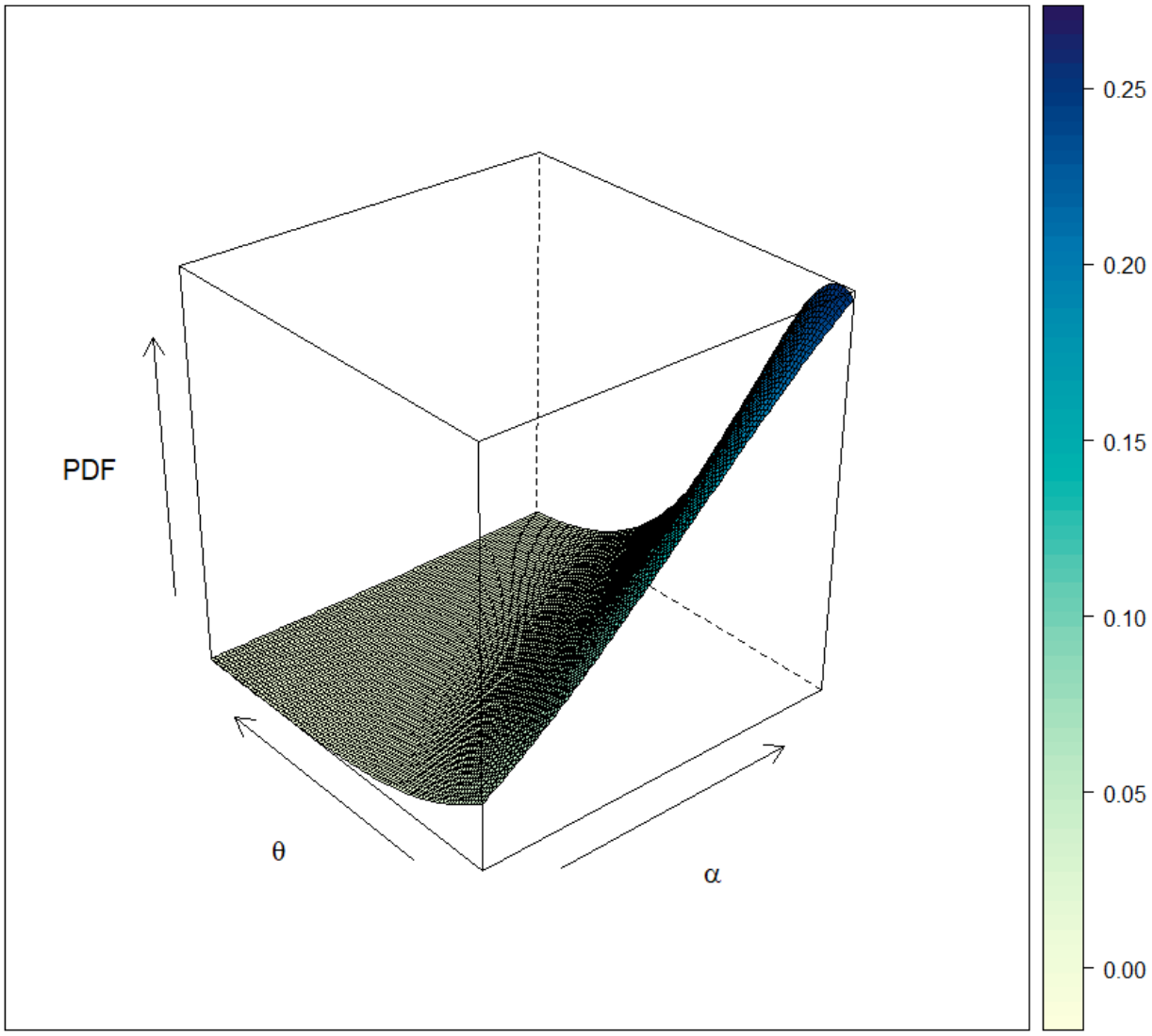


Figure 2: The 3D surface plot of the PDF of the NTGL distribution at a fixed value $x = 5$

The corresponding cumulative distribution function (cdf) can be obtained as follows:

$$F(x;\alpha,\theta) = \int_0^x f(t;\alpha,\theta)\,dt$$

$$= \int_0^x \frac{\theta^2}{4+\theta^2}\left(\theta + \frac{4t^{\alpha-2}\theta^{\alpha-3}}{\Gamma(\alpha-1)}\right)\mathrm{e}^{-\theta t}\,dt$$

$$= \frac{\theta^2}{4+\theta^2}\left[\int_0^x \left(\theta \mathrm{e}^{-\theta t}\right)dt + \int_0^x \left(\frac{4t^{\alpha-2}\theta^{\alpha-3}}{\Gamma(\alpha-1)}\mathrm{e}^{-\theta t}\right)dt\right]$$

$$= \frac{\theta^2}{4+\theta^2}\left[\left(1-\mathrm{e}^{-x\theta}\right) + \frac{4\Gamma(\alpha-1,x\theta)}{\theta^2\Gamma(\alpha-1)}\right]$$

$$= \frac{\theta^2}{4+\theta^2}\left(1-\mathrm{e}^{-x\theta}\right) + \frac{4\theta^{\alpha-1}\Upsilon(\alpha-1,\theta x)}{(4+\theta^2)\Gamma(\alpha-1)}$$

Therefore,

$$F(x|\alpha,\theta) = \frac{1}{4+\theta^2}\left(\theta^2\left(1-\mathrm{e}^{-\theta x}\right) + \frac{4\theta^{\alpha-1}\Upsilon(\alpha-1,\theta x)}{\Gamma(\alpha-1)}\right) \quad (2)$$

The cdf for some selected values of the shape and scale parameters are presented in Figure 2; where $\gamma(.)$ incomplete gamma function. These cdf plots illustrate the flexibility of the NTGLD in modeling distributions that can either concentrate around lower values or spread across a broader range, depending on the parameters α and θ.

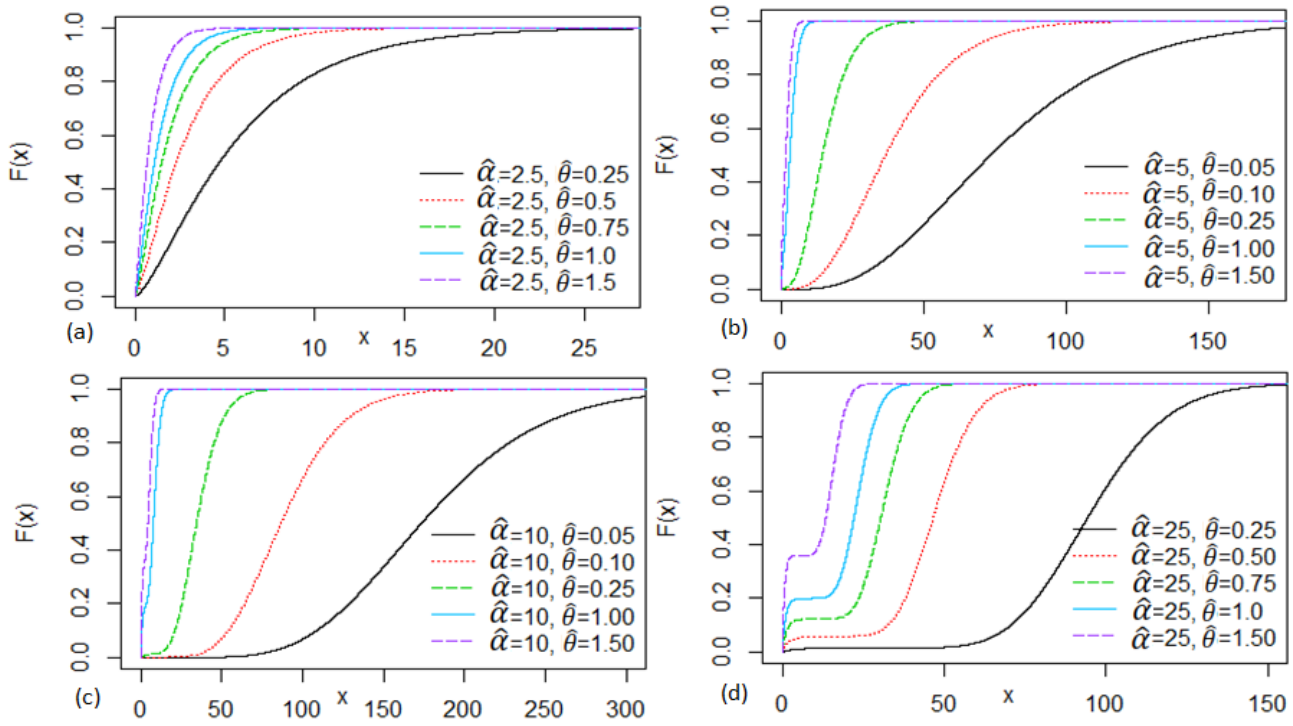


Figure 3: CDF curves of the NTGL distribution for some selected values of parameters.

[III] Mathematical Properties of the NTGL Distribution

Using algebraic expressions to ascertain some mathematical characteristics can prove more advantageous compared to direct computation through numerical methods. Hence, we proceed to introduce some mathematical properties of the NTGL distribution.

Asymptotic Behaviour

This subsection discusses the behaviour and probable shapes features of the PDF of NTGL distribution. The PDF's behaviour is as follows:

$$\lim_{x\to 0} f(x) = \begin{cases} \to \infty, & if\ 1 < \alpha < 2 \\ \dfrac{\theta(\theta^2+4)}{4+\theta^2}, & if\ \alpha = 2 \\ \dfrac{\theta^3}{4+\theta^2}, & if\ \alpha > 2 \end{cases}$$

Moments and Associated Measures

The rth factorial moment

Moments of a given density function are very useful in computing measures of central tendency, variance, skewness, and kurtosis. Using equation (1), the rth factorial moment of the random variable X (said to be following the NTGL distribution) about the origin is obtained as:

$$E(X^r) = \mu_r = \int_0^\infty x^r f(x|\alpha,\theta)dx$$

$$\mu_r = \int_0^\infty x^r \frac{\theta^2}{4+\theta^2}\left(\theta + \frac{4x^{\alpha-2}\theta^{\alpha-3}}{\Gamma(\alpha-1)}\right)\mathrm{e}^{-\theta x}dx$$

$$= \frac{\theta^2}{4+\theta^2}\int_0^\infty x^r\left(\theta + \frac{4x^{\alpha-2}\theta^{\alpha-3}}{\Gamma(\alpha-1)}\right)\mathrm{e}^{-\theta x}dx$$

The final expression of ordinary moments is given in the following form:

$$\mu'_r = \frac{\theta^2\Gamma(1+r)\Gamma(\alpha-1) + 4\Gamma(r+\alpha-1)}{\theta^r(4+\theta^2)\Gamma(\alpha-1)} \quad (3)$$

The initial four moments of the random variable X, about the origin, are derived from equation (3) by substituting r with values of 1, 2, 3, and 4 respectively.

$$\mu'_1 = \frac{4(\alpha-1)+\theta^2}{\theta(4+\theta^2)}$$

$$\mu'_2 = \frac{2\left(\theta^2+2\alpha(\alpha-1)\right)}{\theta^2(4+\theta^2)}$$

$$\mu'_3 = \frac{4\alpha^3-4\alpha+6\theta^2}{\theta^3(4+\theta^2)}$$

$$\mu'_4 = \frac{4\left((\alpha-1)\alpha(1+\alpha)(2+\alpha)+6\theta^2\right)}{\theta^4(4+\theta^2)}$$

The variance (σ^2), coefficient of variation (CV), the index of dispersion (ID), coefficient of skewness (S_k) and coefficient of Kurtosis (K_s) are obtained as:

$$\sigma^2 = E(X^2) - [E(X^1)]^2 = \mu_2 - [\mu_1]^2$$

$$\sigma^2 = \frac{\theta^4+4\alpha^2\theta^2+16\theta^2-16-4\alpha(3\theta^2-4)}{\theta^2(4+\theta^2)^2}$$

$$CV = \frac{\sigma}{\mu_1}$$

$$CV = \frac{\sqrt{(16(\theta^2+\alpha-1)-12\alpha\theta^2+4\alpha^2\theta^2+\theta^4)}}{(\theta^2+4\alpha-4)(4\theta+\theta^3)}$$

$$S_k = \frac{\mu'_3}{\sigma^3}$$

$$S_k = \frac{6\theta^2 - 4\alpha + 4\alpha^3}{\theta^3(4+\theta^2)\left(\frac{16(\theta^2-1)+4\alpha^2\theta^2+\theta^4-4\alpha(-4+3\theta^2)}{\theta^2(4+\theta^2)^2}\right)^{3/2}}$$

$$K_s = \frac{\mu_4'}{\sigma^4}$$

$$K_s = \frac{4(4+\theta^2)^3\left((\alpha-1)\alpha(1+\alpha)(2+\alpha)+6\theta^2\right)}{\left(16(\theta^2-1)+4\alpha^2\theta^2+\theta^4-4\alpha(3\theta^2-4)\right)^2}$$

$$ID = \frac{\sigma^2}{\mu_1} = \frac{16(\theta^2+\alpha-1)-12\alpha\theta^2+4\alpha^2\theta^2+\theta^4}{(-4+4\alpha+\theta^2)(4\theta+\theta^3)} = \frac{16(\theta^2+\alpha-1)+\theta^2(\theta^2+4\alpha^2-12\alpha)}{(\theta^2+4\alpha-4)(\theta^3+4\theta)}$$

Table 1 provides key statistical measures numerically for the NTGL distribution across different values of the parameters α and θ. As α increases, all the measures (mean, variance, skewness, and kurtosis) show significant increases, especially for small values of θ. This indicates that for large α, the distribution becomes more dispersed, more skewed, and more kurtotic, with fatter tails. For increasing θ, the measures (especially variance, skewness, and kurtosis) decrease, implying that the distribution becomes more symmetric and less spread out, with lighter tails.

Table 1: Numerical description of certain key measures of the NTGL distribution

Parameters		Measures				
	θ	μ	σ^2	ID	S_k	K_s
α = 1.25	0.05	5.0093	100.32	20.028	5.6237	36.5395
	0.25	1.0461	3.3209	4.1303	5.5907	35.9133
	0.50	0.5882	1.3010	2.2117	5.4700	33.6740
	1.00	0.4000	0.4900	1.2250	5.1384	27.6056
	5.00	0.1793	0.0385	0.2149	5.5721	22.6294
	10.0	0.0971	0.0099	0.1021	5.8669	23.5420
α = 2.5	0.05	29.9937	599.9375	20.0020	7.1430	26.2457
	0.25	5.9692	23.9375	4.0101	7.1124	26.1462
	0.50	2.9411	5.9377	2.0188	7.0253	25.8675
	1.00	1.4000	1.4400	1.0285	6.7708	25.1012
	5.00	0.2137	0.0439	0.2055	6.0633	23.8883
	10.0	0.1019	0.0102	0.1009	6.0152	23.9642
α = 5.0	0.05	79.9625	1601.498	20.0281	14.9700	52.3700
	0.25	15.8153	65.4428	4..1379	14.2946	49.4601
	0.50	7.6470	17.2872	2.2606	12.6098	42.4029
	1.00	3.4000	4.8400	1.4235	9.1284	28.8914
	5.00	0.2827	0.0993	0.3513	5.5491	22.1315
	10.0	0.1115	0.0144	0.1298	5.9584	26.4068
α = 10.0	0.05	179.90	3613.981	20.0888	36.4314	145.4433
	0.25	35.5076	157.5422	4.4368	31.5520	120.6542
	0.50	17.0588	48.2906	2.8308	22.2211	76.7248
	1.00	7.4000	17.6400	2.3837	10.7061	30.5582
	5.00	0.4206	0.3885	0.9235	4.6814	17.5866
	10.0	0.1307	0.0367	0.2809	6.2247	35.5493
α = 25	0.05	479.7126	9726.3384	20.2753	130.0227	711.9315
	0.25	94.5846	506.5505	5.3555	86.2262	413.7612

0.50	45.2941	207.7370	4.5864	39.2306	146.9782
1.00	19.4000	104.0400	5.3628	11.7613	31.1303
5.00	0.8344	2.6829	3.2151	3.9264	12.9181
10.0	0.1884	0.2144	1.1380	6.0984	35.2655

Moment Generating Function

The moment generating function of a random variable X following the NTGL distribution is defined by:

$$M_X(t) = \int_0^\infty e^{tx}(x;\alpha,\theta)dx$$

$$= \int_0^\infty e^{tx}\frac{\theta^2}{4+\theta^2}\left(\theta + \frac{4x^{\alpha-2}\theta^{\alpha-3}}{\Gamma(\alpha-1)}\right)\mathrm{e}^{-\theta x}dx$$

$$= \frac{\theta^2}{4+\theta^2}\int_0^\infty \left(\theta + \frac{4x^{\alpha-2}\theta^{\alpha-3}}{\Gamma(\alpha-1)}\right)\mathrm{e}^{-(\theta-t)x}dx$$

$$= \frac{\theta^2}{4+\theta^2}\left[\int_0^\infty \theta\mathrm{e}^{-(\theta-t)x}dx + \frac{4\theta^{\alpha-3}}{\Gamma(\alpha-1)}\int_0^\infty x^{\alpha-2}\mathrm{e}^{-(\theta-t)x}dx\right]$$

$$Let \quad y = (\theta-t)x$$

$$= \frac{\theta^2}{4+\theta^2}\left[\theta\int_0^\infty \frac{\mathrm{e}^{-y}}{(\theta-t)}dy + \frac{4\theta^{\alpha-3}}{\Gamma(\alpha-1)}\int_0^\infty \frac{y^{\alpha-2}\mathrm{e}^{-y}}{(\theta-t)^{\alpha-1}}dy\right]$$

$$M_X(t) = \frac{\theta^2}{4+\theta^2}\left[\frac{\theta}{(\theta-t)} + \frac{4\theta^{\alpha-3}}{(\theta-t)^{\alpha-1}}\right] \qquad (4)$$

Reliability Characteristics

In this section, we derive some reliability properties of the NTGL distribution including survival and hazard functions.

3.3.1. Survival Function

The survival function of the NTGL distribution denoted by $S(x)$ is given as follows:

$$S(x) = 1 - F(x|\alpha,\theta)$$

$$S(x) = \frac{4+\theta^2\mathrm{e}^{-\theta x} - 4\frac{\gamma(\alpha-1,\theta x)}{\Gamma(\alpha-1)}}{4+\theta^2} \qquad (5)$$

Hazard (Failure Rate) Function

The hazard function of the NTGL distribution denoted by $h(x)$ is given as follows:

$$h(x) = \frac{f(x|\alpha,\theta)}{S(x)}$$

$$h(x) = \frac{\left(\theta(x\theta)^{-2+\alpha}\left(4x^\alpha\theta^\alpha + x^2\theta^4\Gamma(\alpha-1)\right)\right)}{\left((\theta^2(x\theta)^\alpha + \mathrm{e}^{x\theta}(-4x^\alpha\theta^\alpha + 4(x\theta)^\alpha)\right)\Gamma(\alpha-1) + 4\mathrm{e}^{x\theta}x^\alpha\theta^\alpha\Gamma(\alpha-1,x\theta))} \qquad (6)$$

For varying values of α and θ Figures 4 and 5, show the shapes of the plots of S(x) and h(x), respectively. Obviously, the NTGL distribution has decreasing and increasing hazard rate functions depending on the values of the parameters.

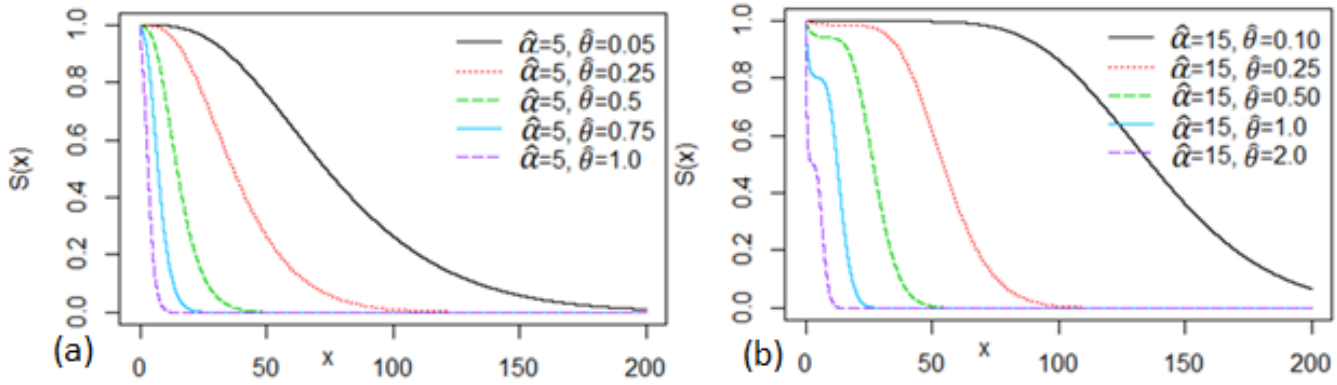


Figure 4: Survival curves of the distribution for some selected values of parameters.

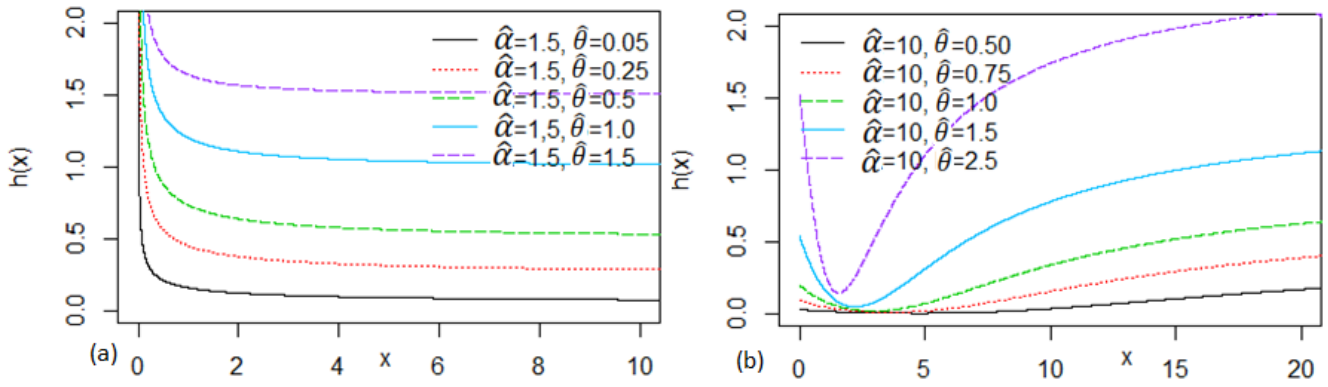


Figure 5: Hazard curves of the distribution for some selected values of the parameters.

Renyi's Entropy

An entropy of a random variable X is a measure of variation of uncertainty [33]. Suppose a continuous random variable X follows a probability with density function $f(x)$, then Renyi's entropy, $R_H(x)$, can be expressed as:

$$R_H(x) = \frac{1}{1-\rho} log \int_0^\infty [f(x|\alpha,\theta)]^\rho dx,$$

For the PDF in equation (1) given as:

$$f(x|\alpha,\theta) = \frac{\theta^2}{4+\theta^2}\left(\theta + \frac{4x^{\alpha-2}\theta^{\alpha-3}}{\Gamma(\alpha-1)}\right)e^{-\theta*x}, \qquad x,\alpha,\theta > 0$$

Therefore,

$$R_H(x) = \frac{1}{1-\rho} log \int_0^\infty \left[\frac{\theta^2}{4+\theta^2}\left(\theta + \frac{4x^{\alpha-2}\theta^{\alpha-3}}{\Gamma(\alpha-1)}\right)e^{-\theta*x}\right]^\rho dx$$

$$= \frac{1}{1-\rho}\log\left[\left(\frac{\theta^2}{4+\theta^2}\right)^\rho\left(\theta\int_0^\infty e^{-\rho\theta x}dx + \frac{4\theta^{\alpha-3}}{\Gamma(\alpha-1)}\int_0^\infty x^{\alpha-2}e^{-\rho\theta x}dx\right)\right]$$

$$= \frac{1}{1-\rho}\log\left[\left(\frac{\theta^2}{4+\theta^2}\right)^\rho\left(\theta\frac{1}{\rho\theta} + \frac{4\theta^{\alpha-3}}{\Gamma(\alpha-1)}\frac{\Gamma(\alpha-1)}{(\rho\theta)^{\alpha-1}}\right)\right]$$

$$= \frac{1}{1-\rho}\log\left[\left(\frac{\theta^2}{4+\theta^2}\right)^\rho\left(\frac{1}{\rho} + \frac{4}{\rho^{\alpha-1}\theta^2}\right)\right] \quad (7)$$

Order Statistics

Suppose $X_{(1)} \le X_{(2)} \le \ldots \le X_{(n)}$ are order observations of $X_1, X_2, \ldots, X_n$ taken from the studied distribution then density of the kth order statistic $X_{(k)}$ can be expressed as:

$$f_{X_{(k)}}(x) = \frac{n!}{(k-1)!\,(n-k)!} f(x|\alpha,\theta)[F(x|\alpha,\theta)]^{k-1}[1 - F(x|\alpha,\theta)]^{n-k} \quad (8)$$

By substituting equations (1) and (2) into (8) we have:

$$f_{X_{(k)}}(x) = \frac{n!}{(k-1)!\,(n-k)!}\frac{\theta^2}{4+\theta^2}\left(\theta + \frac{4x^{\alpha-2}\theta^{\alpha-3}}{\Gamma(\alpha-1)}\right)e^{-\theta*x}\left[\frac{(1-e^{-x\theta})\theta^2 + \frac{4x^\alpha\theta^\alpha(x\theta)^{-\alpha}(\Gamma(\alpha-1)-\Gamma(\alpha-1,x\theta))}{\Gamma(\alpha-1)}}{4+\theta^2}\right]^{k-1}\left[1 - \frac{(1-e^{-x\theta})\theta^2 + \frac{4x^\alpha\theta^\alpha(x\theta)^{-\alpha}(\Gamma(\alpha-1)-\Gamma(\alpha-1,x\theta))}{\Gamma(\alpha-1)}}{4+\theta^2}\right]^{n-k}$$

The functions of the first and nth order statistics are:

$$f_{X_{(1)}}(x) = \frac{n!}{(k-1)!\,(n-k)!}\frac{\theta^2}{4+\theta^2}\left(\theta + \frac{4x^{\alpha-2}\theta^{\alpha-3}}{\Gamma(\alpha-1)}\right)e^{-\theta*x}\left[1 - \frac{(1-e^{-x\theta})\theta^2 + \frac{4x^\alpha\theta^\alpha(x\theta)^{-\alpha}(\Gamma(\alpha-1)-\Gamma(\alpha-1,x\theta))}{\Gamma(\alpha-1)}}{4+\theta^2}\right]^{n-1}$$

and

$$f_{X_{(n)}}(x) = \frac{n!}{(k-1)!\,(n-k)!}\frac{\theta^2}{4+\theta^2}\left(\theta + \frac{4x^{\alpha-2}\theta^{\alpha-3}}{\Gamma(\alpha-1)}\right)e^{-\theta*x}\left[\frac{(1-e^{-x\theta})\theta^2 + \frac{4x^\alpha\theta^\alpha(x\theta)^{-\alpha}(\Gamma(\alpha-1)-\Gamma(\alpha-1,x\theta))}{\Gamma(\alpha-1)}}{4+\theta^2}\right]^{n-1}$$

Quantile function

The quantile function $Q(p)$ is the inverse of the cdf in (2), defined as:

$Q(p) = F^{-1}(p)$

Therefore,

$$p = \frac{(1-e^{-x\theta})\theta^2 + \frac{4x^\alpha\theta^\alpha(x\theta)^{-\alpha}(\Gamma(\alpha-1)-\Gamma(\alpha-1,x\theta))}{\Gamma(\alpha-1)}}{4+\theta^2}$$

$$p(4+\theta^2) - \frac{4x^\alpha\theta^\alpha(x\theta)^{-\alpha}(\Gamma(\alpha-1)-\Gamma(\alpha-1,x\theta))}{\Gamma(\alpha-1)} = (1-e^{-x\theta})\theta^2$$

This is a complex equation to solve analytically; hence, numerical solution can be obtained. The plot of the quantile

function (at p = 0.5) at varying values of α and θ is presented in Figure 6.

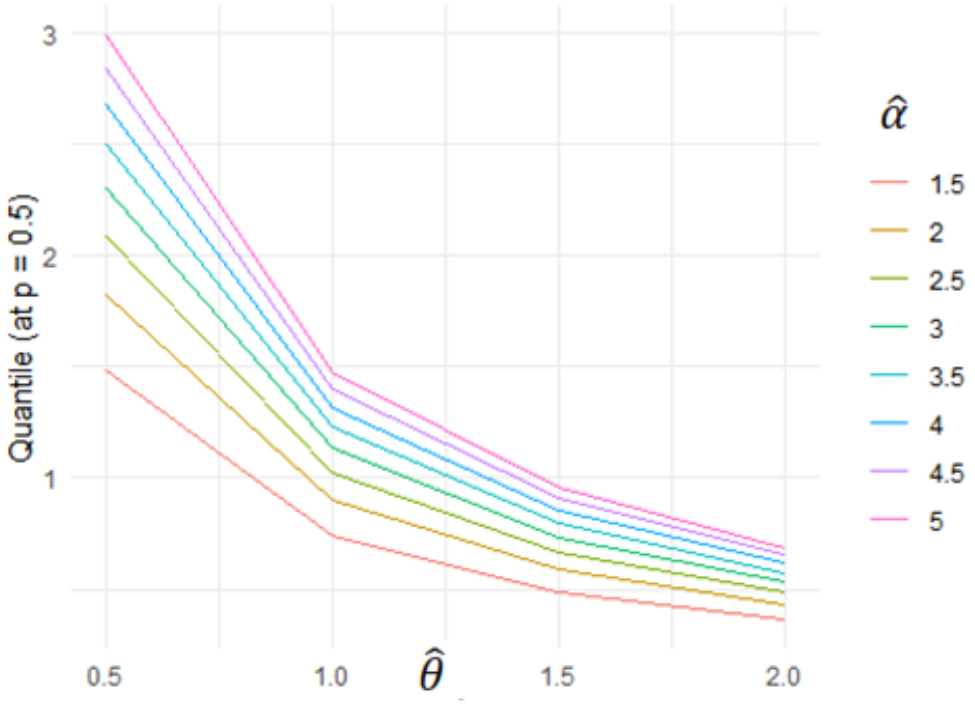


Figure 6: Quantile function (at p = 0.5) plot at varying values of α and θ

[IV] Parameter Estimation and Simulation Study

In this section, we obtain the mathematical expressions of the maximum likelihood estimators (MLEs) of the NTGL distribution $(i.e, \hat{\alpha}_{MLE},, \hat{\theta}_{MLE})$. Besides deriving of the mathematical expression of $\hat{\alpha}_{MLE}$ and $\hat{\theta}_{MLE}$, we also provide a simulation study to assess their performances numerically.

Maximum Likelihood Estimation

Let $X_1, X_2, \ldots, X_n$ be a random sample of size n from $f(x|\alpha, \theta)$ of the NTGL distribution defined by (1). In relation to the $f(x|\alpha, \theta)$, the likelihood function $L(\alpha, \theta|x_1, x_2, \ldots, x_n)$ of the parameters can be written as

$$L(\alpha, \theta|x_1, x_2, \ldots, x_n) = L = \prod_{i=1}^{n} f(x_i|\alpha, \theta) \qquad (9)$$

Using Equation (1) in Equation (9), we have

$$L = \prod_{i=1}^{n} \frac{\theta^2}{4+\theta^2}\left(\theta + \frac{4{x_i}^{\alpha-2}\theta^{\alpha-3}}{\Gamma(\alpha-1)}\right)\mathrm{e}^{-\theta x_i} \qquad (10)$$

The log likelihood function is obtained by

$$\mathcal{L}(\alpha, \theta) = 2nlog\theta - nlog(4+\theta^2) + \sum_{i=1}^{n} \log\left(\theta + \frac{4{x_i}^{\alpha-2}\theta^{\alpha-3}}{\Gamma(\alpha-1)}\right) - \sum_{i=1}^{n} x_i\theta \qquad (11)$$

The maximum likelihood estimates (MLEs) $\hat{\alpha}$ and $\hat{\theta}$ of the parameters α and θ of NTGL distribution are found by solving the following log-likelihood equation by taking partial derivatives of equation (11) with respect to θ and α and equating to zero, following score equations are obtained as

$$\frac{\partial \mathcal{L}(\alpha, \theta)}{\partial \alpha} = \sum_{i=1}^{n}\left[\frac{4{x_i}^{\alpha-2}\theta^{\alpha-3}({x_i}^{\alpha-2}\log(x_i) - \frac{\Gamma'^{(\alpha-1)}}{\Gamma(\alpha-1)}}{\left(\theta + \frac{4{x_i}^{\alpha-2}\theta^{\alpha-3}}{\Gamma(\alpha-1)}\right)\Gamma(\alpha-1)}\right] \qquad (12)$$

and

$$\frac{\partial \mathcal{L}(\alpha, \theta)}{\partial \theta} = \sum_{i=1}^{n}\left[\frac{2\theta}{4+\theta^2} + \frac{1 + \frac{4{x_i}^{\alpha-2}(\alpha-3)\theta^{(\alpha-3)}}{\Gamma(\alpha-1)}}{\theta + \frac{4{x_i}^{\alpha-2}\theta^{\alpha-3}}{\Gamma(\alpha-1)}} - x_i\right] \qquad (13)$$

The Maximum Likelihood estimates $\hat{\alpha}$ and $\hat{\theta}$ of the parameters α and θ respectively, can be obtained by solving iteratively Equations (12) and (13). We solve the non-linear equations numerically because they are not in closed forms, hence, they are complicated to solve algebraically. The R-software [34] was used to solve the equations and obtain the parameters' values.

Simulation Study

In this subsection, we evaluate the behaviors of $\hat{\alpha}_{MLE}$ and $\hat{\theta}_{MLE}$ of the NTGL distribution through a thorough simulation study. The study is carried out by generating random samples (with N=1000 iterations), say n = 50, 100, . . ., 1000, from NTGL distribution using the inverse cdf approach.

The simulation study was carried out for the combination values α = 2.5, θ = 0.5; α = 10, θ = 1.0 and α = 10, θ = 5.0.

We considered two statistical tools to evaluate the performances of $\hat{\alpha}_{MLE}$ and $\hat{\theta}_{MLE}$. These measures included the bias and mean square error (MSE) with mathematical expressions given, respectively, by

$$MSE(\hat{\theta}_{MLE}) = \frac{1}{N}\sum_{i=1}^{N}(\hat{\alpha}_i - \alpha)^2$$

and

$$Bias(\hat{\theta}_{MLE}) = \frac{1}{N}\sum_{i=1}^{N}(\hat{\alpha}_i - \alpha\ )$$

The above evaluation criteria are also computed for $\hat{\theta}_{MLE}$. The simulation results are presented numerically in Tables 2. From the simulation results of the NTGL distribution, we observed that: as n increases (i.e., as n → ∞): the estimated values of $\hat{\alpha}_{MLE}$ and $\hat{\theta}_{MLE}$ converge to the true values, indicating stability. Additionally, the MSEs of $\hat{\alpha}_{MLE}$ and $\hat{\theta}_{MLE}$ approach zero. Additionally, the Biases of $\hat{\alpha}_{MLE}$ and $\hat{\theta}_{MLE}$ also decrease to zero.

Table 2: The numerical illustration of the Simulation Study of the NTGL distribution

	n	Parameters	MLEs	MSEs	Biases
α = 2.5 θ = 0.5	50	α	2.7318	0.4043	0.2318
		θ	0.5665	0.0348	0.0665
	100	α	2.6063	0.1606	0.1063
		θ	0.5327	0.0152	0.0327
	150	α	2.5791	0.1079	0.0791
		θ	0.5235	0.0106	0.0235
	200	α	2.5444	0.0534	0.0444
		θ	0.5127	0.0055	0.0127
	300	α	2.5295	0.0301	0.0295
		θ	0.5097	0.0032	0.0097
	500	α	2.5161	0.0139	0.0161
		θ	0.5049	0.0017	0.0049
	700	α	2.5111	0.0095	0.0111
		θ	0.5037	0.0011	0.0037
	900	α	2.5083	0.0062	0.0083
		θ	0.5022	0.0007	0.0022
	1000	α	2.5090	0.0054	0.0090
		θ	0.5023	0.0006	0.0023
α = 10 θ = 1.0	50	α	10.0769	1.7675	0.0769
		θ	1.0056	0.0193	0.0056
	100	α	10.0091	0.7477	0.0091
		θ	1.0003	0.0083	0.0003
	150	α	10.0234	0.5400	0.0234
		θ	1.0022	0.0060	0.0022
	200	α	10.0500	0.3588	0.0500
		θ	1.0050	0.0041	0.0050
	300	α	9.9873	0.2411	-0.0126
		θ	0.9999	0.0028	-0.0001
	400	α	10.0209	0.1877	0.0209
		θ	1.0010	0.0020	0.0010
	500	α	10.0020	0.1300	0.0020
		θ	1.0007	0.0014	0.0007
	700	α	10.0042	0.0945	0.0042
		θ	1.0001	0.0010	0.0001
	900	α	9.9927	0.0714	-0.0073
		θ	0.9995	0.0007	-0.0005
	1000	α	10.0037	0.0664	0.0037
		θ	1.0001	0.0005	0.0001
	50	α	10.0468	3.2404	0.0468
		θ	5.0670	0.3193	0.0670
	100	α	10.0063	1.0354	0.0053
		θ	5.0156	0.1155	0.0156
	150	α	10.0155	0.5395	0.0155
		θ	5.0105	0.0653	0.0105

	200	α	10.0113	0.2961	0.0113
		θ	5.0107	0.0397	0.0107
α = 10	300	α	9.9981	0.1141	-0.0019
		θ	4.9939	0.0157	0.0061
θ = 5.0	400	α	9.9967	0.0643	-0.0033
		θ	5.0013	0.0090	0.0013
	500	α	9.9993	0.0388	-0.0007
		θ	5.0007	0.0059	0.0007
	700	α	9.9992	0.0091	-0.0008
		θ	5.0004	0.0011	0.0004
	900	α	9.9994	0.0035	-0.0006
		θ	5.0001	0.0002	0.0001
	1000	α	9.999995	0.0016	-5.3×10^{-6}
		θ	4.9995	0.0001	-0.0005

[V] Application of Real Data Analysis

This section aims to demonstrate the effectiveness of the NTGL distribution using three real data sets. The performance of the NTGL distribution is compared with other competing models, namely: the generalized Lindley distribution (GLD1) by Nadarajah et al. [12], the New Generalized Two Parameter Lindley Distribution (NGTLD) by Ekhosuehi et al. [35], the quasi-Lindley distribution (QLD) by Shanker and Mishra [13] and the A new generalized Lindley distribution (GLD2) by Abouammoha et al. [14].

Description of the Data Sets

The first data set (onward, it is expressed as Data 1) represents the remission times (in months) of 128 patients who were suffering from bladder cancer. This data set was originally reported by Lee and Wang [36]. The second data set represent the remission times (in months) of 36 bladder cancer patients reported in Hibatullah et al. [37]. The third data set represent the time-to-recovery (in days) of Covid-19 patients at Lagos state, Nigeria in 2020. It comprises of 553 patients. The secondary data were obtained through the Lagos state ministry of health.

The Model's Selection Tools

In this subsection, we describe the key tools used to evaluate the performance of the NTGL and other competing distributions. The criteria considered in this paper were the Akaike information criteria (AIC), Consistent AIC (CAIC), Bayesian information criteria (BIC), and Hannan–Quinn information criteria (HQIC), with their mathematical expressions detailed as follows:

$$AIC = 2k - 2\mathcal{L},$$

$$CAIC = AIC + \frac{2k(k+1)}{n-k-1},$$

$$BIC = klog(n) - \mathcal{L}$$

$$HQIC = 2klog[log(n)] - 2\mathcal{L}$$

In the formulae of information criteria, the term k represents the model parameter(s), n indicates the sample size, and "$\mathcal{L}$" represents the Log-likelihood function.

Table 3: The estimated values and model selection values for each data set

Data	Model	$\hat{\alpha}$	$\hat{\theta}$	-2logL	AIC	CAIC	HQIC	BIC
bladder cancer patients; (n=128)	NTGLD	2.1730	0.1252	826.7385	830.7385	830.8345	833.0561	836.4425
	NGTLD	1.1891	0.1247	826.8288	830.8288	830.9248	833.1463	836.5328
	GLD1	0.7336	0.1648	832.5718	836.5719	836.6679	838.8894	842.2759
	QLD	663.69	0.1069	828.6838	832.6839	832.7799	835.0015	838.3879
	GLD2	1.5890	0.1533	832.3136	836.3136	836.4096	838.6312	842.0177
Bladder cancer I dataset (n=36)	NTGLD	4.1345	1.2949	107.1145	111.1145	111.4781	112.2198	114.2815
	NGTLD	2.2531	0.8691	113.2435	117.2435	117.6071	118.3488	120.4105
	GLD1	1.8909	1.0731	107.4763	111.4763	111.84	112.5817	114.6434
	QLD	0.0387	1.0117	108.471	112.471	112.8346	113.5764	115.638
	GLD2	3.1159	1.3135	107.382	111.382	111.7456	112.4874	114.549
***Covid19 data (N=553)**	NTGLD	6.4393	0.5053	1651.907	3307.813	3307.835	3311.185	3316.444
	NGTLD	3.6344	0.3099	1701.766	3407.531	3407.553	3410.903	3416.162
	GLD1	2.2552	0.2595	1669.146	3342.292	3342.313	3345.664	3350.922
	QLD	0.0085	0.1954	1708.896	3421.793	3421.815	3425.165	3430.424
	GLD2	3.9631	0.3623	1665.38	3334.760	3334.781	3338.131	3343.390

*Data Source: Lagos state ministry of health

Table 3 compares various models applied to three datasets: remission times of 128 bladder cancer patients, remission times of 36 bladder cancer patients, and time-to-recovery for 553 Covid-19 patients. The models compared are the New Two-Parameter Generalized Lindley Distribution (NTGLD), New Generalized Two Parameter Lindley Distribution (NGTLD), Generalized Lindley Distribution 1 (GLD1), Quasi-Lindley Distribution (QLD), and Generalized Lindley Distribution 2 (GLD2). The performance metrics evaluated include the negative log-likelihood (-2logL), Akaike Information Criterion (AIC), Consistent Akaike Information Criterion (CAIC), Hannan-Quinn Information Criterion (HQIC), and Bayesian Information Criterion (BIC). Lower values of -2logL, AIC, CAIC, HQIC, and BIC indicate a better model fit, and NTGLD consistently achieves the lowest values (bolded) across all datasets. Overall, the NTGL distribution demonstrates superior performance in fitting the datasets compared to other models. It provides more accurate parameter estimates and better fit statistics, making it a robust choice for modeling lifetime datasets.

[VI] CONCLUSION

In this study, we propose a new model called A New Two-Parameter Generalized Lindley Distribution (NTGLD). Its PDF plots demonstrate the flexibility of the NTGLD to model a wide range of behaviors, from sharply peaked distributions to broadly spread, multimodal shapes, depending on the parameter values.

We derive the moments and the moment generating function and other mathematical properties of the distribution. Parameter estimation is estimated using the maximum likelihood method. Simulation results of the NTGL distribution indicate that as the sample size n increases, the estimated values of the parameters α and θ converge to their true values, with mean squared errors (MSEs) and biases approaching zero. This demonstrates the stability and accuracy of the estimators.

From the quantile plot, it is observed that the median quantile decreases as θ increases, with more rapid changes at lower values of θ. Higher values of α consistently result in higher quantiles, highlighting the significant impact of α on the distribution's behavior. Applications to three real datasets, including remission times of bladder cancer patients and time-to-recovery of Covid-19 patients, demonstrate that the NTGL distribution provides better fits compared to other competing models considered.

Although we acknowledge the value of possible extensions such as handling censored data, incorporating Bayesian estimation, regression-based modelling, or offering a public R package, such directions would significantly broaden the scope of this paper. These important developments are reserved for future work. For now, we focus on establishing the theoretical foundations of the NTGLD, consistent with common practice in distributional research.

Conflicts of Interest

The authors declare no conflict of interest.

Data Availability

The third data is available from the corresponding author upon justifiable request.

CRediT authorship contribution statement

Samuel Adewale Aderoju: Conceptualization, investigation, methodology, writing—original draft, and data curation. Kazeem Adesina Dauda: Methodology, Writing—Review & Editing. Julius Babatunde Olaifa: Methodology, Writing—Review & Editing.

Acknowledgment

This research study is supported by TETFUND INSTITUTIONAL BASED RESEARCH (KWASUIBR/CRIT/270921/VOL1/TETF2020/00016) through Kwara State University, Malete. We appreciate the Lagos State Ministry of Health for their cooperation and support in releasing the Covid-19 data (secondary data). We also appreciate Mr. Oludare Arowogbola for his effort in the data collection.

REFERENCES

[1] G. Warahena-Liyanage, B. Oluyede, T. Moakofi, and W. Sengweni, "The new exponentiated half logistic-Harris-G family of distributions with actuarial measures and applications," *Stats*, vol. 6, pp. 773–801, 2023. doi: 10.3390/stats6030050.

[2] H. SchÄbe, "Constructing lifetime distributions with bathtub shaped failure rate from DFR distributions," *Microelectronics Reliability*, vol. 34, no. 9, pp. 1501–1508, 1994. doi: 10.1016/0026-2714(94)90458-8.

[3] M. Chahkandi and M. Ganjali, "On some lifetime distributions with decreasing failure rate," *Comput. Statist. Data Anal.*, vol. 53, no. 12, pp. 4433–4440, 2009. doi: 10.1016/j.csda.2009.06.016.

[4] K. A. Dauda, "Optimal tuning of random survival forest hyperparameter with an application to liver disease," *Malays. J. Med. Sci.*, vol. 29, no. 6, pp. 67–76, 2022. doi: 10.21315/mjms2022.29.6.7.

[5] K. A. Dauda, W. B. Yahya, and A. W. Banjoko, "Survival analysis with multivariate adaptive regression splines using Cox-Snell residual," *Ann. Comput. Sci. Ser.*, vol. 13, no. 2, pp. 25–41, 2015.

[6] A. H. Tolba et al., "A new distribution for modeling data with increasing hazard rate: A case of COVID-19 pandemic and vinyl chloride data," *Sustainability*, vol. 15, art. no. 12782, 2023. doi: 10.3390/su151712782.

[7] N. L. Johnson, S. Kotz, and N. Balakrishnan, "Beta distributions," in *Continuous Univariate Distributions*, 2nd ed., New York, NY, USA: John Wiley & Sons, 1994, pp. 221–235.
[8] N. L. Johnson, S. Kotz, and N. Balakrishnan, *Continuous Univariate Distributions*. New York, NY, USA: John Wiley & Sons, 1995, vol. 289.
[9] F. S. Gomes-Silva, A. Percontini, E. de Brito, M. W. Ramos, R. Venâncio, and G. M. Cordeiro, "The odd Lindley-G family of distributions," *Austrian J. Stat.*, vol. 46, pp. 65–87, 2017. doi: 10.17713/ajs.v46i1.222.
[10] N. Taketomi, K. Yamamoto, C. Chesneau, and T. Emura, "Parametric distributions for survival and reliability analyses, a review and historical sketch," *Mathematics*, vol. 10, art. no. 3907, 2022. doi: 10.3390/math10203907.
[11] D. V. Lindley, "Fiducial distributions and Bayes' theorem," *J. R. Stat. Soc. Ser. B*, vol. 20, pp. 102–107, 1958. doi: 10.1111/j.2517-6161.1958.tb00278.x.
[12] H. Zakerzadeh and A. Dolati, "Generalized Lindley distribution," *J. Math. Ext.*, vol. 3, pp. 13–25, 2009. doi: 10.4236/ojs.2021.113022.
[13] B. O. Oluyede and T. Yang, "A new class of generalized Lindley distributions with applications," *J. Stat. Comput. Simul.*, vol. 85, no. 10, pp. 2072–2100, 2015. doi: 10.1080/00949655.2014.917308.
[14] S. Nadarajah, H. S. Bakouch, and R. Tahmasbi, "A generalized Lindley distribution," *Sankhya B*, vol. 73, pp. 331–359, 2011. doi: 10.1007/s13571-011-0025-9.
[15] R. Shanker and A. Mishra, "A quasi-Lindley distribution," *Afr. J. Math. Comput. Sci. Res.*, vol. 6, no. 4, pp. 64–71, 2013. doi: 10.5897/AJMCSR12.067.
[16] A. M. Abouammoh, A. M. Alshangiti, and I. E. Ragab, "A new generalized Lindley distribution," *J. Stat. Comput. Simul.*, 2015. doi: 10.1080/00949655.2014.995101.
[17] N. H. Al-Noor and N. K. Assi, "Rayleigh-Rayleigh distribution: Properties and applications," *J. Phys.: Conf. Ser.*, vol. 1591, art. no. 012038, 2020. doi: 10.1088/1742-6596/1591/1/012038.
[18] K. K. Shukla, "Pranav distribution with properties and its applications," *Biometrics Biostat. Int. J.*, vol. 7, no. 3, pp. 244–254, 2018. doi: 10.15406/bbij.2018.07.00215.
[19] S. Aderoju, "Samade probability distribution: Its properties and application to real lifetime data," *Asian J. Probab. Stat.*, vol. 14, no. 1, pp. 1–11, 2021. doi: 10.9734/ajpas/2021/v14i130317.
[20] S. A. Aderoju and O. Babaniyi, "Power Samade distribution: Its properties and application to real lifetime data," *Niger. J. Sci. Environ.*, vol. 21, no. 1, pp. 237–248, 2023.
[21] R. Elangovan and K. Manivasagan, "A new generalization of Samade distribution with properties and its applications in medical sciences," *Strad Res.*, vol. 10, no. 6, 2023. doi: 10.37896/sr10.6/048.
[22] S. Aryuyuen, I. Thaimsorn, and U. Tonggumnead, "Bayesian inference for a new negative binomial-Samade model for time series data counts with its properties and applications," *WSEAS Trans. Math.*, 2023. doi: 10.37394/23206.2023.22.65.
[23] S. A. Aderoju, I. Adeniyi, J. B. Olaifa, and A. Olaosebikan, "On Poisson-Samade distribution: Its applications in modelling count data," *Earthline J. Math. Sci.*, vol. 12, no. 2, pp. 255–270, 2023. doi: 10.34198/ejms.12223.255270.
[24] B. Hosseini, M. Afshari, M. Alizadeh, and A. Afify, "A new weighted-Lindley distribution: Properties, classical and Bayesian estimation with an application," *Pak. J. Stat. Oper. Res.*, vol. 18, no. 4, pp. 1049–1066, 2022. doi: 10.18187/pjsor.v18i4.4106.
[25] B. Meriem et al., "The power XLindley distribution: Statistical inference, fuzzy reliability, and COVID-19 application," *J. Funct. Spaces*, vol. 2023, art. no. 9818094, 2023. doi: 10.1155/2023/9818094.
[26] S. A. Aderoju and E. T. Jolayemi, "Power Hamza distribution and its applications to model survival time," *J. Niger. Stat. Assoc.*, vol. 34, pp. 1–10, 2022.
[27] N. I. Aleshinloye, S. A. Aderoju, A. A. Abiodun, and B. L. Taiwo, "A new generalized gamma-Weibull distribution and its applications," *Al-Bahir J. Eng. Pure Sci.*, vol. 2, no. 2, pp. 1–9, 2023. doi: 10.55810/2313-0083.1021.
[28] S. A. Aderoju and I. Adeniyi, "On power generalized Akash distribution with properties and applications," *J. Stat. Model. Anal.*, vol. 4, no. 1, 2023. doi: 10.22452/josma.vol4no1.1.
[29] Y. A. Tashkandy, M. E. Bakr, S. A. Benchiha et al., "Power modified XLindley distribution: Statistical properties and applications," *Sci. Rep.*, vol. 14, art. no. 20262, 2024. doi: 10.1038/s41598-024-69884-5.
[30] A. M. Gemeay et al., "Modified XLindley distribution: Properties, estimation, and applications," *AIP Adv.*, 2023. doi: 10.1063/5.0172056.
[31] S. A. Aderoju, N. I. Aleshinloye, B. L. Taiwo, and B. I. Sanni, "A new lifetime distribution and its application to cancer data," *J. Biostat. Epidemiol.*, vol. 9, no. 4, pp. 451–460, 2024. doi: 10.18502/jbe.v9i4.16670.

[32] B. S. Everitt and D. J. Hand, "Mixtures of normal distributions," in *Finite Mixture Distributions*, Dordrecht: Springer, 1981, pp. 25–57. doi: 10.1007/978-94-009-5897-5_2.

[33] A. Renyi, "On measures of entropy and information," in *Proc. Fourth Berkeley Symp. Math. Statist. Prob.*, vol. 1, pp. 547–561, 1961.

[34] R Core Team, *R: A Language and Environment for Statistical Computing*, Vienna, Austria: R Foundation for Statistical Computing, 2023. [Online]. Available: https://www.R-project.org/.

[35] N. Ekhosuehi, F. Opone, and F. Odobaire, "A new generalized two parameter Lindley distribution," *J. Data Sci.*, vol. 16, no. 3, pp. 549–566, 2018. doi: 10.6339/JDS.201807_16(3).0006.

[36] E. T. Lee and J. Wang, *Statistical Methods for Survival Data Analysis*. New York, NY, USA: Wiley, 2003.

[37] R. Hibatullah, Y. Widyaningsih, and S. Abdullah, "Marshall-Olkin extended power Lindley distribution with application," *J. Riset Apl. Mat.*, vol. 2, no. 2, pp. 84–92, 2018. doi: 10.26740/jram.v2n2.p84-92.

APPLICATION OF VERTICAL ELECTRICAL SOUNDING TECHNIQUE IN BUILDING FOUNDATION INVESTIGATION IN ILISHAN-REMO SOUTHWESTERN NIGERIA

Agbo, Kelvin O [1,2]
Olusegun, Kehinde D [1]
Olajide, Adetayo O [1]
Coker, Joseph O [2]
Ambali, Akeem A [2]
Adekoya, Sofiat A[2,*]

Received: 10/05/2025
Revised: 08/07/2025
Accepted: 09/07/2025

[1] Department of Physics, Babcock University, Ilishan, Nigeria
[2] Department of Physics, Olabisi Onabanjo University, Ago-Iwoye , Nigeria
*Corresponding Author's Email: adekoya.sofiat@oouagoiwoye.edu.ng

https://doi.org/10.20428/jst.v30i8.3008

APPLICATION OF VERTICAL ELECTRICAL SOUNDING TECHNIQUE IN BUILDING FOUNDATION INVESTIGATION IN ILISHAN-REMO SOUTHWESTERN NIGERIA

Agbo, Kelvin O
Department of Physics, Olabisi Onabanjo University, Ago-Iwoye, Nigeria Department of Physics, Babcock University Ilishan, Nigeria

Olusegun, Kehinde D
Department of Physics, Babcock University, Ilishan, Nigeria

Olajide, Adetayo O
Department of Physics, Babcock University, Ilishan, Nigeria

Ambali, Akeem A
Department of Physics, Olabisi Onabanjo University, Ago-Iwoye, Nigeria

Coker, Joseph O
Department of Physics, Olabisi Onabanjo University, Ago-Iwoye, Nigeria

Adekoya, Sofiat A
Department of Physics, Olabisi Onabanjo University, Ago-Iwoye, Nigeria
adekoya.sofiat@oouagoiwoye.edu.ng

Abstract— This study investigates subsurface conditions to inform foundation design through geophysical surveying, specifically employing the Vertical Electrical Sounding (VES) method using a Schlumberger array with AB/2 spacing of 100 meters. Ten VES points were analyzed to determine subsurface composition, strength, and stability. Three to five separate layers, including topsoil, clayey sand, clay, and sandy layers, were identified in the interpreted geoelectric sections; the majority of the resistivity curves were categorized as HKA-type. Layer thicknesses ranged from 0.9 m to 45.9 m, and resistivity values ranged from 71.7 Ωm to 18,671.3 Ωm. More load-bearing capacity is shown by a higher resistivity in the sandy layer at traverse one, which qualifies it for heavy construction. The subsurface sequence in traverse two, on the other hand, has a clayey layer beneath the topsoil, indicating increased stability and suitability for constructions where minimal settlement is essential. The findings underscore the importance of integrating geophysical data with further geotechnical assessments to ensure optimal foundation planning.

Keywords— Vertical Electrical Sounding, Geophysical Survey, Geoelectric Section, Resistivity, Overburden Thickness,

I. INTRODUCTION

The foundation of a structure is the structural component that carries the load of the building to the ground, distributing it in such a manner as to prevent settlement or subsidence. It offers stability and support, ensuring that the building stays upright and safe [1]. The foundation is typically made of concrete, steel, or a combination of the two, and it is usually placed below ground level to secure the building, in which design and construction of the foundation are critical to the overall stability and longevity of the building structure [2]. However, the efficacy and lifespan of a foundation are significantly influenced by the properties of the geology of the subsurface.

First and foremost, understanding the rock and soil composition, strength, and stability is critical in establishing the best form of foundation for a construction project. Cohesion, bearing capacity, and settlement potential are all important soil attributes to consider while doing this study. Without a thorough rock study and analysis, there is a danger of selecting an insufficient foundation type, which might lead to costly structural concerns in the future [3].

In the realm of civil engineering and architecture, understanding the geological components underlying building foundations is paramount. These components play a critical role in determining the safety, durability, and cost-effectiveness of construction projects [4].

It should be noted that failure to check the subsurface soil can lead to building failure, which, according to [5], it is an unacceptable difference between expected and observed performance of building components, proving that proper soil investigation allows engineers to select appropriate foundation types, designs, and construction techniques tailored to the specific soil conditions encountered. Therefore, the applications of geophysical surveys in building foundation design, aim to enhance the efficiency, accuracy, and safety of construction practices [6].

Geophysical surveys utilize various techniques to probe the subsurface, each offering unique advantages depending on the geological context and project requirements. By examining various geological factors such as soil types, subsurface conditions, geological formations, and environmental considerations, we seek to provide a comprehensive understanding of the interplay between geology and structural integrity [7] .

Furthermore, incorporating geophysical surveys into foundation design lies in their ability to mitigate risks associated with inadequate site characterization. Surveying subsurface features, identifying potential hazards, and delineating rock stratigraphy, these surveys enable engineers to make informed decisions regarding foundation type, depth, and reinforcement [8].

Hence, in advancing the utilization of geophysical surveys in building construction, this research employs the Vertical Electrical Sounding (VES) method to characterize subsurface conditions beneath the proposed construction sites within Babcock University, Southwestern Nigeria.

II. DESCRIPTION AND GEOLOGY OF THE STUDY AREAS

The study area, Ilishan-Remo, is located in the sedimentary terrain of southwestern Nigeria. The study area is a town a few kilometers from the Shagamu highway and a few minutes' drive to Ikene. The study area falls within 60 53' 13.17012'' N 60 53' 24.82008'' N and 30 43' 3.10'' E 60 43' 14.76'' E, and it can be accessed through several road networks: major and other minor roads and footpaths interconnecting the study area. It is situated within a combination of flat plains and gentle slopes. The study area lies within the Abeokuta sedimentary formation, which consists of grits, loose sand, sandstone, kaolinitic clay, and shale (figure 1). It was further characterized as usually having a basal conglomerate or a basal ferruginized sandstone [9]. The perimeter of the study area is indicated with the red polygon on the topographic map (figure 2).

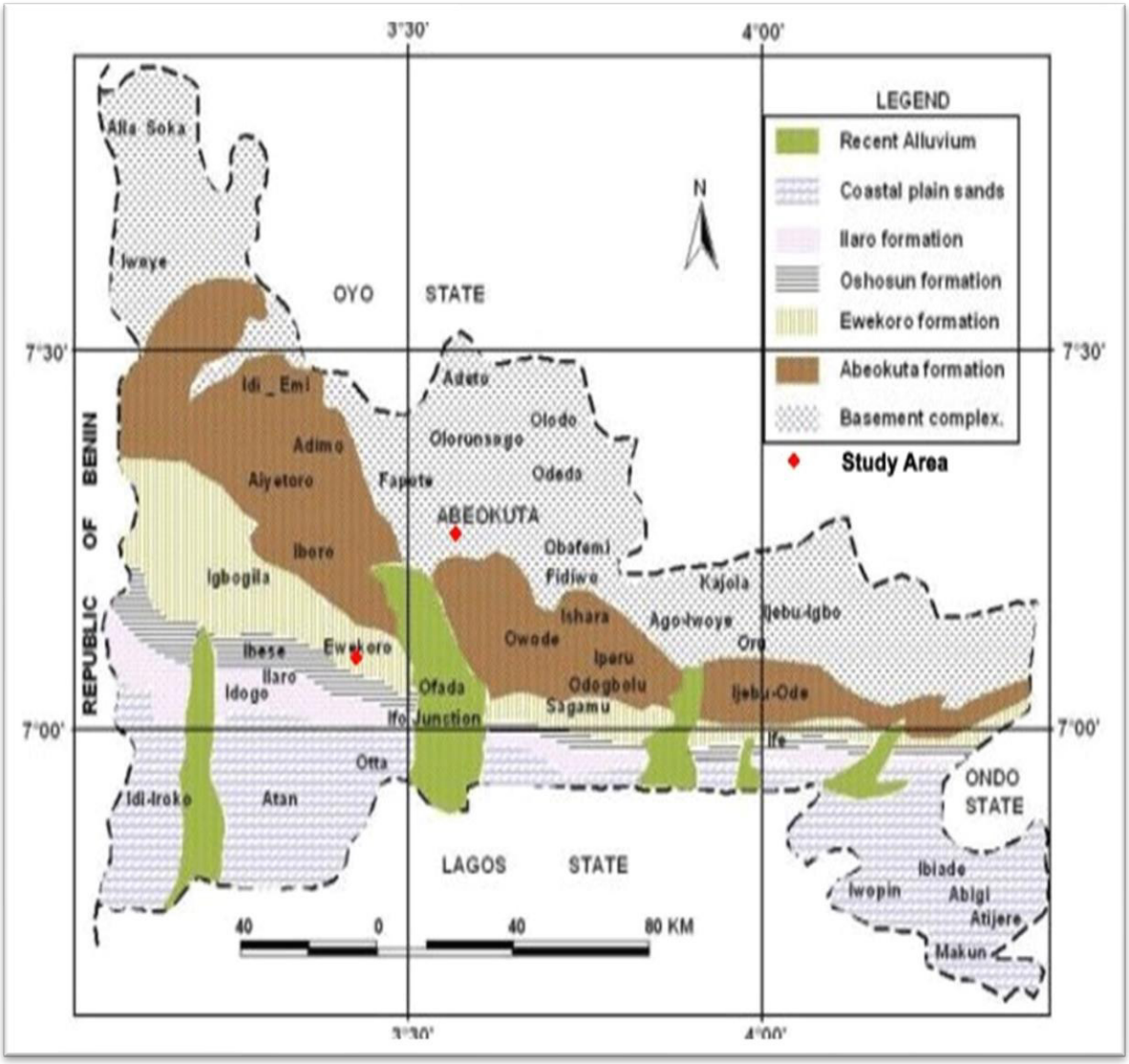


Figure 1: The geological map of Ogun State (Peters, 1982).

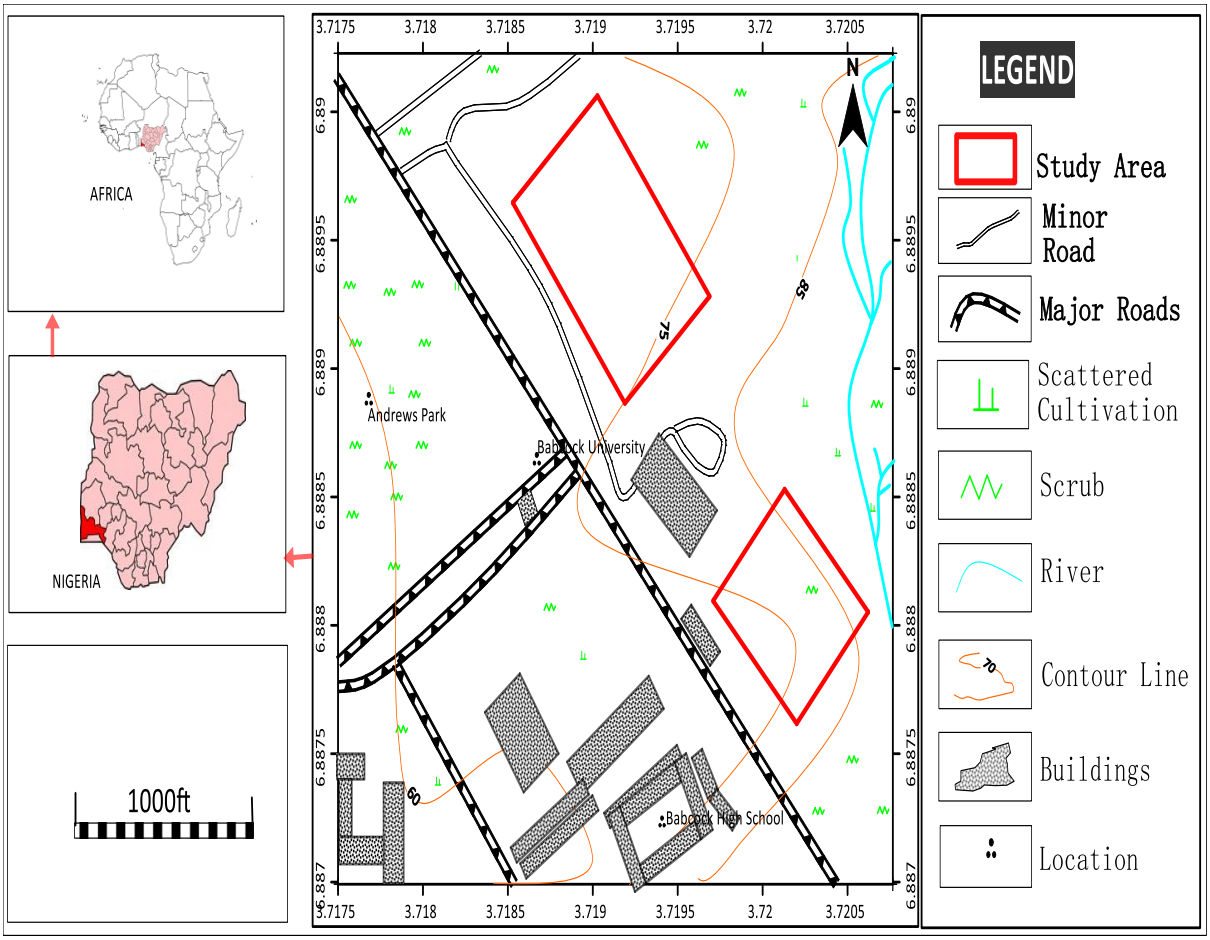


Figure 2: Topography Map of the study area

III. Materials and Method

The geophysical method adopted for this research is the electrical resistivity method using the Schlumberger electrode array in order to study the conditions such as resistivity, thickness, and depth to basement of the subsurface. The origin of electrical resistivity theory is Ohm's law, which states that the ratio of the potential difference, V, between two ends of a conductor in an electrical circuit to the current, I, flowing through it is a constant.

$$V = IR \quad (1)$$

Where R is a constant known as the resistance measured in ohms (Ω). If the conductor is a homogenous cylinder of length L and cross-sectional area A, the resistance will be proportional to the length and inversely proportional to the area.

$$R = \rho\frac{L}{A} \quad (2)$$

Where ρ is the resistivity measured in ohm-meter (Ωm).

The earth's material is predominantly made up of silicates, which are basically non-conductors. The presence of water in the pore space of the soil and in the rocks enhances the conductivity of the earth when an electrical current, I, is passed through it, thus making the rock a semiconductor.

If the electrical field generated by the current is E across the length when a potential difference, V, is applied, then the potential difference can be defined as

$$V = EL \quad (3)$$

$$E = j\rho \quad (4)$$

Where, E is the electric field strength with dimension of volt per meter. If the current electrode is taken to penetrate a small hemisphere of radius, r then the area of the hemisphere becomes $2\pi r^2$. Substituting for E and integrating equation 4 gives:

$$\Delta V = \int E.dr \quad (5)$$

$$\text{Or } \Delta V = I\rho.2\pi \quad (6)$$

$$\text{And } \rho = \frac{\Delta V}{2\pi r l} \quad (7)$$

Since the earth is not homogeneous, equation7 is used to define an apparent resistivity,

$$\rho_a = \frac{\Delta V.G}{I} \quad (8)$$

Where G is a geometric factor fixed for a given electrode configuration.

The apparent resistivity is a function of electrode configuration, electrode spacing, applied current, true earth resistivities, number of layers, layer thickness, potential gradient, and anisotropic earth properties. Ten (10) vertical electrical sounding (VES) data were carried out using the Schlumberger configuration. Electrical noise due to buried cables and other metallic conductors was avoided during the fieldwork. The field procedure involves the potential electrodes (M and N) remaining fixed, and the current electrodes (A and B) are expanded symmetrically about the

center of the spread. The maximum half-current electrode (AB/2) separation used in this survey is 100 m. The depth of penetration is proportional to the separation between the electrodes, and varying the electrodes provides information about the stratification of the ground [10]. The VES data (figure 3) obtained were subjected to partial curve matching. The resistance value was processed using WINRESIST software to obtain the apparent resistivity values.

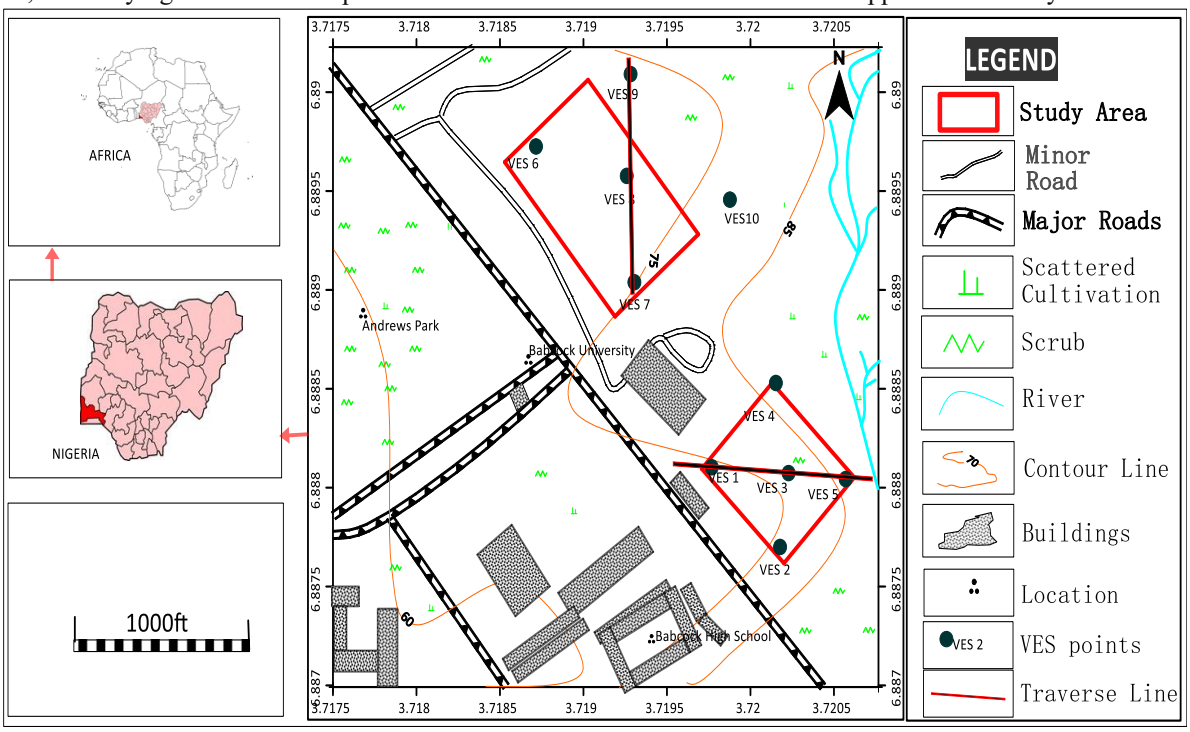


Figure 3: Basemap Indicating the VES points and traverse across the propose land

IV. Results and Discussion

The result of the geophysical survey is presented in sounding curves and geoelectric sections. The summary of the result interpretation of the vertical electrical sounding obtained showed the different layers with their resistivities, depths, thicknesses, and curve types presented in the table. The inferred subsurface layers include a range of three to five geoelectric layers: topsoil, clayey sand, dry sand, and sandstone layer. The typical curve types obtained from the study areas include A and K for three-layer types; four-layer types are AH, AK, KQ, and HA; and for the five-layer curve types, we have KHA and AQK. The three-layer resistivity value ranges from 71.7 Ωm to 3448.1 Ωm; the four-layer ranges from 51.0 Ωm to 9082.9 Ωm; while the five-layer curve type ranges from 151.7 to 4093 Ωm.

Table 1: Interpretation of VES data of the study area.

No of VES	No of Layers	Resistivity Ohm meter (Ωm)	Thickness (m)	Depth (m)	Overburden thickness (m)	Curve type	Lithology Description	Competency Ratings
VES 1	1	166.6	1	1			Topsoil	Moderately Competent
	2	536.5	7.2	8.2			Clayey Sand	Moderately Competent
	3	1973.7	16.9	25.1			Sandy	Competent
	4	18671.3			25.1	AH	Sandy	Competent
VES 2	1	235.9	0.9	0.9			Topsoil	Moderately Competent
	2	299.5	3.4	4.4			Clayey Sand	Moderately Competent
	3	151.7	9.9	14.2			Clayey	Competent
	4	1219.7	26.5	40.7			Sandy	Competent
	5	2113			40.7	KHA	Sandy	Competent
VES 3	1	324.5	0.9	0.9			Topsoil	Moderately Competent
	2	2382.8	3.8	4.6			Sandy	Competent
	3	4965.2	17.5	22.1			Sandy	Competent
	4	626.7			22.1	AK	Clayey Sand	Moderately Competent
VES 4	1	478.1	0.6	0.6			Topsoil	Moderately Competent
	2	3673.8	5.4	6			Sandy	Competent
	3	4093	14	20			Sandy	Competent
	4	661	29.1	49			Clayey Sand	Moderately Competent
	5	378.8			49	AQK	Clayey Sand	Moderately Competent
VES 5	1	336	0.8	0.8			Topsoil	Moderately Competent
	2	10393.1	4.3	5			Sandy	Competent
	3	6044.5	16	21.1	21.1		Sandy	Competent
	4	1974.6				KQ	Sandy	Competent
VES 6	1	451.1	0.9	0.9			Topsoil	Moderately Competent
	2	674.4	4.9	5.7			Clayey Sand	Moderately Competent
	3	4869.6	45.9	51.6	51.6		Sandy	Competent
	4	2575.6				AK	Sandy	Competent
VES 7	1	213.4	1	1			Topsoil	Moderately Competent
	2	1817.5	13.6	14.6	14.6		Sandy	Competent
	3	3448.1				A	Sandy	Competent
VES 8	1	123.9	0.9	0.9			Topsoil	Moderately Competent
	2	51	3.6	4.5			Clayey	Competent
	3	184.1	17.5	22	22		Clayey	Competent
	4	364.4				HA	Clayey Sand	Moderately Competent
VES 9	1	121.9	1.1	1.1			Topsoil	Moderately Competent
	2	872.4	5.6	6.7			Clayey Sand	Moderately Competent
	3	9082.9	35.3	42	42		Sandy	Competent
	4	7512.7				AK	Sandy	Competent
VES 10	1	71.7	1.2	1.2			Topsoil	Moderately Competent
	2	2923.9	40.4	41.6	41.6		Sandy	Competent
	3	1896.4				K	Sandy	Competent

A. Geoelectric Section

The present geological or lithological layers in the subsurface can be well modeled and shown diagrammatically; this image is called a geoelectric section. The geoelectric section represents the depth and thickness of the underlying lithology and their respective resistivity values. As shown in Figure 4, the map indicates two traverse points that fall on a straight line. Geoelectric section is used to correlate lithologies, which was carried out along a profile, and to view the lithology across the subsurface.

Traverse one

This traverse is made up of three vertical electrical sounding points that fall on a straight line of points VES 1, VES 3, and VES 5 traversing from the W to E direction (figure 5). The moderately competent topsoil layer has a resistivity value range of 166.6 Ωm (at VES 1) to 336 Ωm (at VES 5). The second layer, indicating the competent sandy layer, shows resistivity values ranging from 1972.7 Ωm (at VES 1) to 10,393 Ωm (at VES 5). The third layer, indicating moderately competent clayey layer, shows resistivity values ranging from 536.5 Ωm (at VES 1, layer 2) to 626.7 Ωm (at VES 3, layer 4).

Traverse two

This traverse is made up of three vertical electrical sounding points that fall on a straight line of points VES 7, VES 8, and VES 9 traversing from the S to N direction (figure 6). The moderately competent topsoil layer has a resistivity value range of 121.9 Ωm (at VES 9) to 213.4 Ωm (at VES 7). The second layer, indicating the moderately competent clayey layer, shows resistivity values ranging from 51 Ωm (at VES 8) to 872.4 Ωm (at VES 9). The third layer, indicating competent Sandy Layer, shows resistivity values ranging from 1817.5 Ωm (at VES 7, layer 2) to 9082.9 Ωm (at VES 9, layer 3).

Traverse one runs from west to east, while traverse two runs from south to north. In traverse one, the sequence is topsoil, sandy, and then clayey layers. In traverse two, the sequence is topsoil, clayey, then sandy layers.

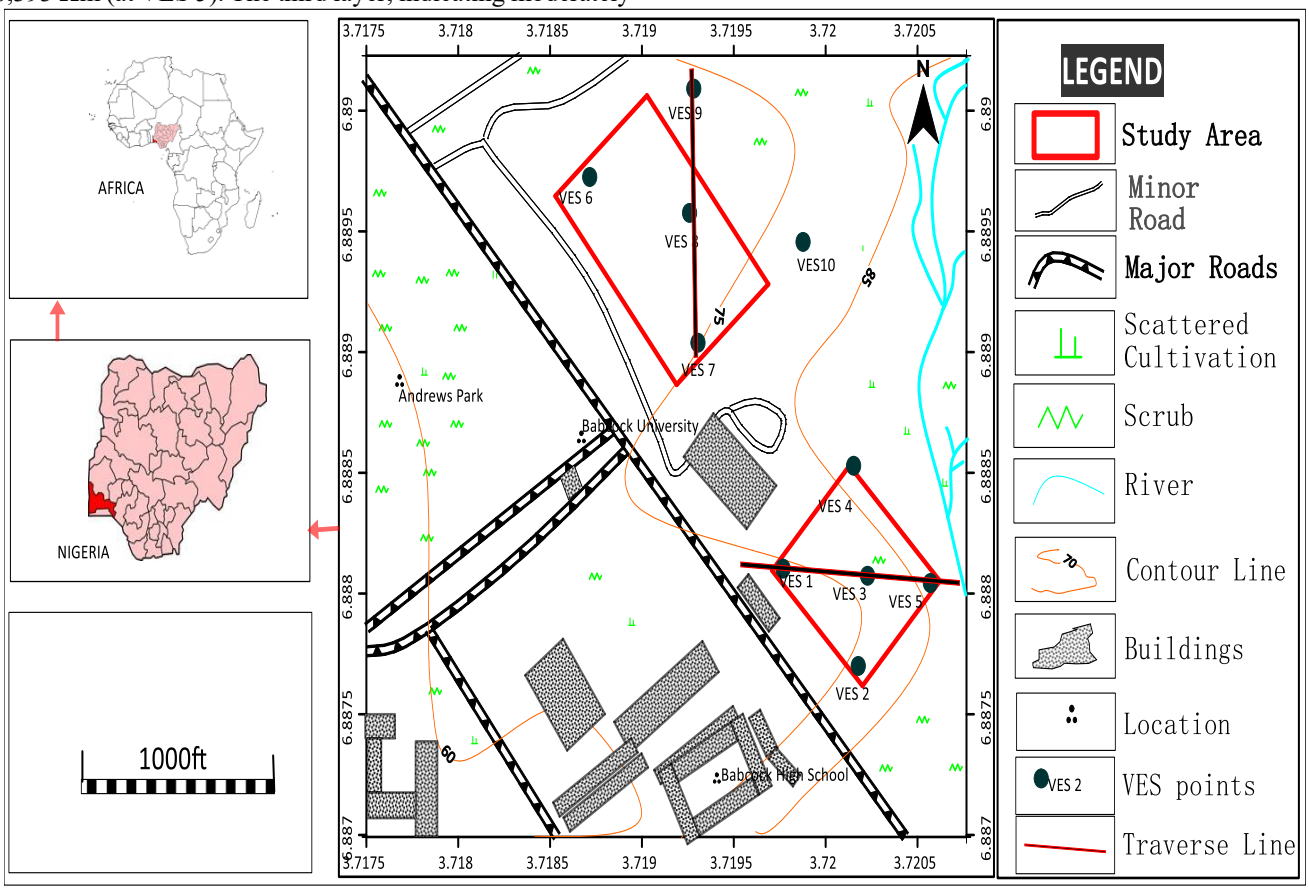


Figure 4: Map Showing VES points and the traverse of the study area

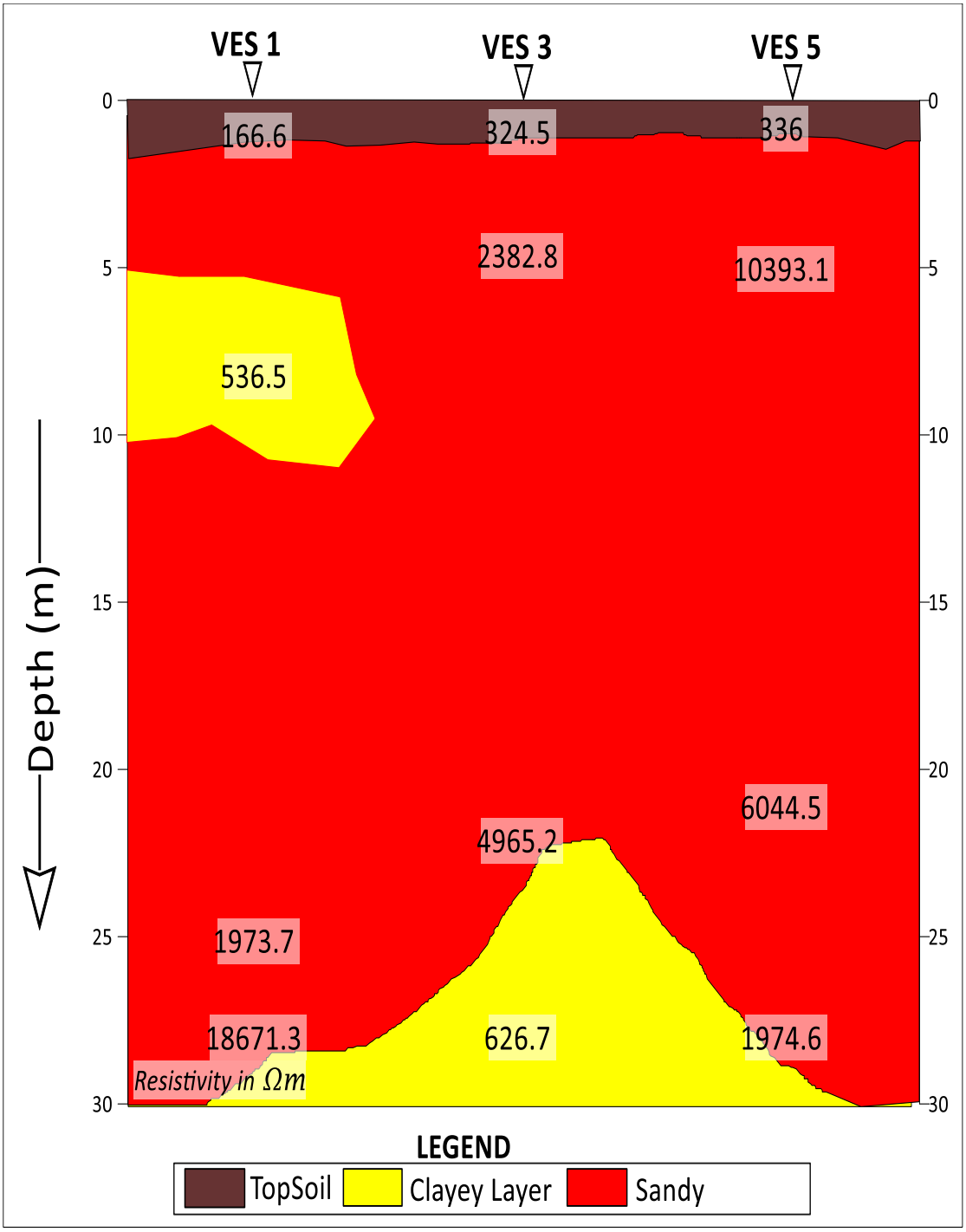


Figure 5: Geoelectric Section of Traverse 1

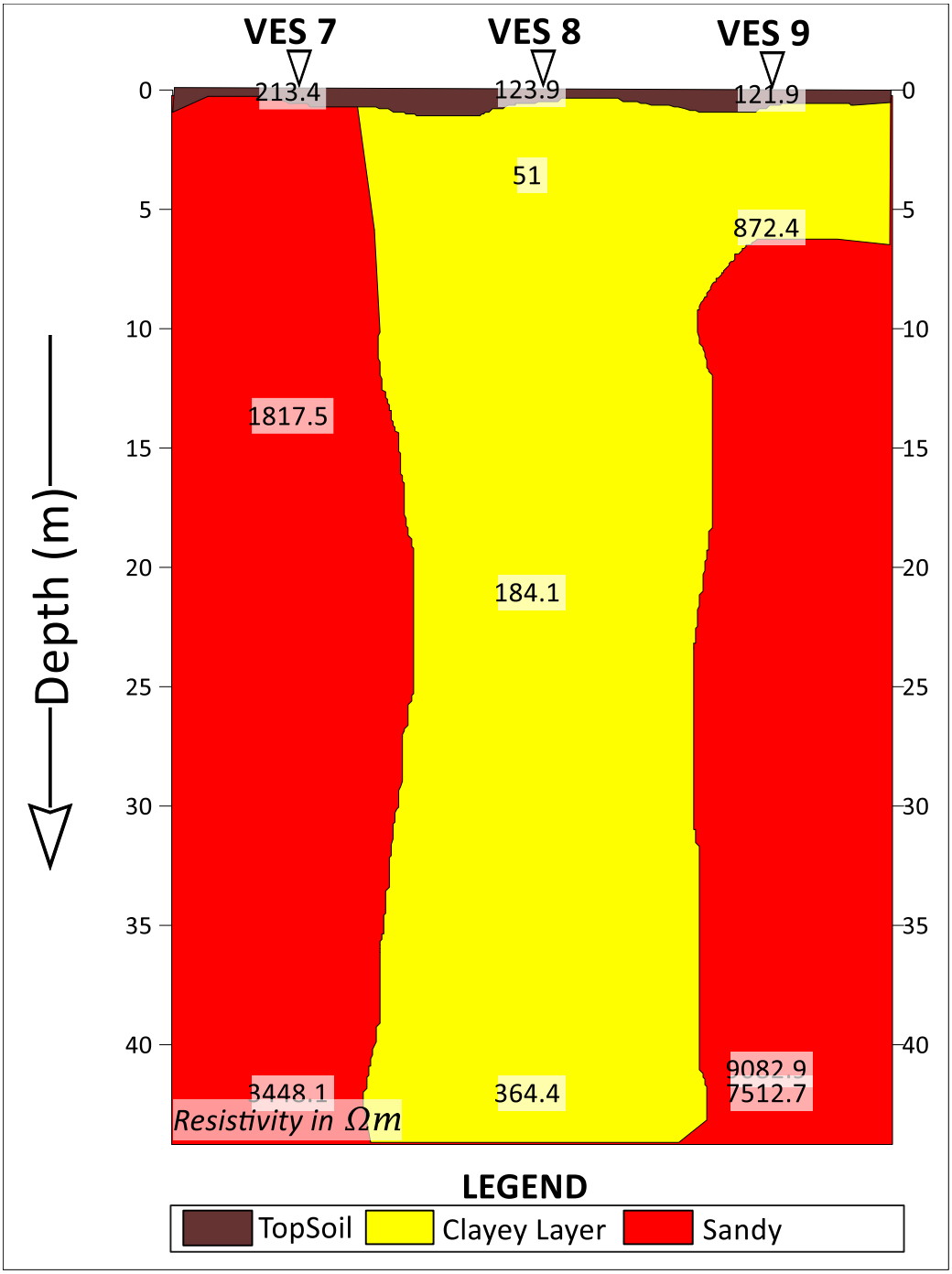


Figure 6: Geoelectric Section of Traverse 2

V. CONCLUSION

The application of the electrical resistivity method has been employed in delineating the various litho units at a proposed building site of Babcock University, southwestern Nigeria. Based on the ten (10) VES measurements taken, three to five layers were delineated from the study area, which comprise topsoil, clayey sand, and a sandy layer, with most of the curves being QKA-type. The results have shown that the resistivity values in traverse one generally tend to be higher than those in traverse two across all layers because of its high resistivity, especially in the sandy layer, indicating better load-bearing capacity, as reported by [11]. This might be preferable for foundation design if the project requires significant load-bearing capacity. Traverse two shows a sequence where the clayey layer lies beneath the topsoil, which provides better stability against settlement. This area is preferable for structures where minimizing settlement is crucial. More importantly, it is recommended that further geotechnical investigations should be carried out to make an informed decision.

REFERENCES

[1] J. E. Bowles and Y. Guo, Foundation analysis and design, vol. 5, New York: McGraw-Hill, 1996, p. 127.

[2] D. P. Coduto, W. Kitch and M. Yeung, Foundation Design: Principles and Practices, 3rd ed., Pearson Education, Inc., 2015.

[3] M. D. Braja and S. Khaled, Principles of Geotechnical Engineering, 9th ed., Cegage Leraning, 2014.

[4] B. K. Tan, "Geologic Considerations in Civil Constructions - Malaysian Case Studies.," *Journal of Civil Engineering and Construction,* vol. 16, no. 2, pp. 123-136, 2022.

[5] G. M. Ayininuola and O. O. Olalusi, "Assessment of Building Failures in Nigeria: Lagos and Ibadan Case Study," *Ayininuola, G. M., and Olalusi, O. O. (2004). Assessment oAfrican Journal of Science and Technology (AJST) Science and Engineering Series, ,* vol. 5, no. 1, pp. 73-79, 2004.

[6] P. Kearey, M. Brooks and I. Hill, An Introduction to Geophysical Exploration., John Wiley & Sons, 2002.

[7] C. W. Fetter, Applied Hydrogeology, 4th ed., Prentice Hall, 1999.

[8] T. Lillesand and R. Kiefer, Remote Sensing and image Interpretation, New York: Wiley, 2015.

[9] H. Jones and R. Hockey, "The Geology of Part of South-Western Nigeria," *Geology Surveying Nigeria,* vol. 31, no. 101, 1964.

[10] W. TelTelford, L. Geldart and R. Sheriff, Applied Geophysics, vol. 2, Cambridge University Press, 1990, pp. 285-530.

[11] S. T. Olufemi, S. A. Adekoya, S. O. Ariyo, N. O. Adebisi and J. O. Coker, "A geophysical assessment for engineering performance of subgrade soils: a case study of the Ago-Iwoye/Ilishan road, South-Western Nigeria," *Scientia Africana,* vol. 23, no. 1, pp. 13-32, 2024.

Legislative Reforms and Tactical Approaches to Combat Cybercrime in the Republic of Yemen

G. F. M. AL-AWDI [1,*]
N. ALSAKKAF [2]
M. H. T. HASAN [2]
A. J. F. OBAID [2]
A. H. A. ALJAZA'AY [2]
M. A. A. ALAWI [2]
A. G. A. ALMUFLEHI [2]
Y. A. M. BIBAK [2]
A. K. H. MUSLEH [2]
A. Y. H. M. AL-MURSHEDI [2]

Received: 23/03/2025
Revised: 17/07/2025
Accepted: 18/07/2025

[1] Higher Institute of Judiciary, Aden, Yemen
[2] Department of Computing, Faculty of Engineering and Computing, University of Science and Technology, Aden, Yemen
*Corresponding Author's Email: jfdl9289@gmail.com

https://doi.org/10.20428/jst.v30i8.2893

Legislative Reforms and Tactical Approaches to Combat Cybercrime in the Republic of Yemen

Galal F. M. Al-Awdi
Higher Institute of Judiciary, Aden, Yemen
jfdl9289@gmail.com

Nasr Alsakkaf
Department of Computing, Faculty of Engineering and Computing, University of Science and Technology, Aden, Yemen
n.alsaqqaf@ust.edu

Mohammed H. T. Hasan
Department of Computing, Faculty of Engineering and Computing, University of Science and Technology, Aden, Yemen

Ali J. F. Obaid
Department of Computing, Faculty of Engineering and Computing, University of Science and Technology, Aden, Yemen

Ali H. A. Aljaza'ay
Department of Computing, Faculty of Engineering and Computing, University of Science and Technology, Aden, Yemen

Mohammed A. A. Alawi
Department of Computing, Faculty of Engineering and Computing, University of Science and Technology, Aden, Yemen

Abdullah G. A. Almuflehi
Department of Computing, Faculty of Engineering and Computing, University of Science and Technology, Aden, Yemen

Yousef A. M. Bibak
Department of Computing, Faculty of Engineering and Computing, University of Science and Technology, Aden, Yemen

Amr K. H. Musleh
Department of Computing, Faculty of Engineering and Computing, University of Science and Technology, Aden, Yemen

Ammar Y. H. M. Al-Murshedi
Department of Computing, Faculty of Engineering and Computing, University of Science and Technology, Aden, Yemen

Abstract— This research examines the critical vulnerabilities in Yemen's digital infrastructure, arising from an outdated and fragmented legislative framework, and its consequential exposure to sophisticated cybercrimes. Drawing on survey data from 1,024 respondents and insights from cybersecurity experts, the study highlights a significant public perception of insecurity and the inadequacy of current cyber laws. It investigates core cybersecurity principles, the evolution of cybercrime, and the multi-dimensional challenges—including technical, human, and organizational factors—that exacerbate Yemen's risks. By comparing Yemen's legislative deficiencies with international and regional models such as the cybercrime laws of Jordan, Kuwait, and the UAE, as well as frameworks like the Budapest Convention and the NIST Cybersecurity Framework, the research proposes a comprehensive, adaptable legal framework. Key recommendations include establishing a centralized National Cybersecurity Authority, standardizing digital evidence protocols, enhancing interagency coordination, and investing in capacity building. The proposed framework aims to protect critical infrastructure, safeguard personal data, and foster robust enforcement mechanisms, thereby aligning Yemen's cybersecurity posture with global best practices and ensuring a resilient digital ecosystem.

Keywords— Cybersecurity, Legislative, Cybercrime, Digital Evidence, Internet Regulation

I. Introduction

The Republic of Yemen currently suffers from several major gaps in its digital infrastructure due to the absence of robust and clear cybersecurity legislation. This legislative vacuum makes the country increasingly vulnerable to a range of cyberattacks—from digital defamation and information theft to financial theft—negatively impacting individuals, businesses, institutions, and the digital financial system. Preliminary survey data, collected from 1,024 Yemeni users and professionals, indicates that approximately 78% of those surveyed consider the implementation of cybersecurity legislation to be very important [13]. This highlights the urgent need to establish a legislative framework to secure the digital transformation in the Republic of Yemen.

Observations

The world has benefited from information and communications technology in ways unimaginable. While the rapid development of information technology has positive implications, it has also created numerous problems and challenges for the world. Cybercrime has become widespread, extending beyond national borders, and has even crossed borders between countries. Due to these transgressions, it has become imperative to unify efforts to create strong laws and legislation to confront these challenges. Current laws and legislation are inadequate to address current developments and cannot keep pace with the methods and techniques used by attackers.

Many countries still operate with outdated laws that do not serve the global developments, resulting in a complete failure of the legislative system to keep pace with cybercrime.

There is an urgent need for comprehensive and broad reform of the legislative system and legal procedures to address these challenges. These reforms should include a cybercrime law,

expanding legal treaties between countries, and relying on advanced technologies in digital investigations.

Our selection of Jordan, Kuwait, and the UAE as comparative regional models, despite their higher capacities, is justified by their utility in providing tactical lessons and best practices that can be adapted and incrementally applied within Yemen's resource-constrained and conflict-affected context.

Specifically:

Identification of Adaptable Best Practices: These countries have successfully implemented modern cybercrime laws, established clear legal definitions, and developed standardized digital evidence protocols. While Yemen may not have the immediate resources to replicate these systems entirely, these models offer concrete examples of what works in a regional context and how specific elements can be tailored to Yemen's unique challenges, such as the overlap between cyber and traditional crimes.

Guidance on Institutional Frameworks: The models demonstrate effective approaches to institutional coordination and enforcement, such as Kuwait's multi-tiered crime classification and enhanced operational coordination and the UAE's centralized cybersecurity bodies. These structures provide a blueprint for addressing Yemen's fragmented institutional framework and weak reporting mechanisms by offering solutions for streamlining efforts and optimizing resource allocation. The proposed framework for Yemen, for instance, suggests establishing a centralized National Cybersecurity Authority inspired by such models.

Phased Implementation for Resource Constraints: The proposed framework acknowledges Yemen's "resource limitations and political obstacles" and advocates for a step-by-step approach to implementing cybercrime law. This phased roadmap, outlined in short, medium, and long-term goals, allows for the gradual adoption of components derived from these comparators, focusing initial investments on critical infrastructure and capacity building rather than a complete overhaul.

Aspirational Framework: These models serve as aspirational benchmarks, guiding Yemen toward aligning its cybersecurity posture with international standards and promoting long-term sustainable development, even if the journey is incremental. By understanding the successes of its neighbors, Yemen can strategically plan its legislative and tactical reforms to address its severe deficiencies in cybersecurity infrastructure and expertise.

This research addresses two questions:

- How does the legal vacuum surrounding cybercrime in the Republic of Yemen lead to increased risks?
- How do international laws contribute to formulating Yemen's cybersecurity strategy from a legal perspective?

Research Objectives:

1. Investigate the deficiencies in existing legal and regulatory frameworks that contribute to heightened cyber vulnerabilities.
2. Evaluate the current level of cybersecurity in Yemen through survey data and qualitative assessment addressing perceptions of safety, the prevalence of cybercrimes (e.g., electronic extortion, data theft, financial fraud), and awareness of reporting mechanisms.
3. Review international cybersecurity laws to identify adaptable frameworks and best practices relevant to Yemen's socio-economic and technological context.
4. Develop an adaptable legal framework that addresses both developmental and regulatory challenges, thereby ensuring a secure and stable cyber environment.
5. Recommend strategic measures aimed at reducing cybercrimes by strengthening internet regulation and ensuring effective enforcement of the proposed legal framework.

Research Methods

This study adopts a qualitative research methodology, centered on

doctrinal analysis to examine the legislative and policy landscape surrounding cybercrime. Our primary data sources encompass a wide range of official and academic documents, specifically government papers, scholarly articles, legal journals, case law databases, and statistical datasets relevant to the historical and current trends of cybercrime. These diverse resources are crucial for understanding how strategic responses have evolved in parallel with legislative and policy developments. The data collection process systematically involves a careful evaluation of

academic publications to gain technical insights into critical areas such as infrastructure vulnerabilities, malware dissemination models, and various hacking methodologies. Concurrently,

court rulings are analyzed to reveal statutory interpretations and their practical applications in the prosecution of cybercrimes.

II. CYBERSECURITY

The Concept of Cybersecurity

Cybersecurity has emerged as a crucial discipline in the digital age, rooted in the same principles that historically underpinned physical security. The protection of digital assets is primarily based on the three tenets of the CIA triad:

A. Confidentiality: Preventing unauthorized disclosure of information.
B. Integrity: Ensuring the accuracy, consistency, and trustworthiness of data.
C. Availability: Guaranteeing that data is accessible to authorized users whenever needed.

These principles form the basis upon which cybersecurity policies and practices are developed and enforced. [1]

Dimensions of Cybersecurity

Cybersecurity can be conceptualized along two interrelated dimensions:

1. Core Principles:

As outlined above, the fundamental principles are confidentiality, integrity, and availability.

2. Information States and Safeguards:

A. Data in Transit: Refers to the protection of data during its transfer between devices or networks.
B. Data at Rest: Pertains to stored data that is not actively used.
C. Data in Process: Involves data undergoing initial entry, modification, or output.

These dimensions are supported by three layers of cybersecurity safeguards: advanced technologies, comprehensive education/training and awareness programs, and robust policies and procedures.[2]

Evolution of Cybersecurity

Throughout the ages, data protection has been linked to information security. With the emergence of digital communications and the development of the internet, where the first computer virus appeared on the Arpanet network in the early 1980s, the principles of encryption, adopted by the Massachusetts Institute of Technology, emerged. For the first time, the term "cybersecurity" was used instead of "information security." With the development of internet technology and communication methods, many cyber problems and electronic attacks emerged, as attacks on individuals, data centers, institutions, and companies became widespread.

This, in turn, contributed to the need for firewalls and anti-virus software, whose methods and techniques of attack multiplied. With the emergence of cloud computing, hacking problems and attacks increased, necessitating the use of artificial intelligence to detect threats.

Cybersecurity Challenges

Cybersecurity challenges can be divided into three main areas:

A. Technical Challenges: These address software attacks such as information breaches, virus attacks, and denial-of-service attacks, where attackers use modern methods to circumvent defense lines and firewalls.

B. Human Challenges: These include cyber harassment, fraud, and the exploitation of individuals' lack of digital literacy. They also use social engineering to reach people through phishing. Attackers exploit vulnerable prey, both personally and electronically, allowing attackers to access the network and access systems and system administrators.

C. Regulatory Challenges: Users' disregard for regulations and policies leads to numerous hackings and cyberattack problems. Compounding the problem is the failure to implement penalties against violators, which has led to attackers escalating their attacks, knowing they will not be punished due to the lack of legislation and laws.

III. CYBERCRIME

Definition of Crime

Crime has one universal title and one universal term, undisputed by legal experts worldwide. Laws have been enacted to combat crime in all its forms, whether by committing acts that violate the law or failing to perform or fulfill obligations. Any behavior that violates the safety and privacy of others also falls under the term crime. Any behavior that causes harm to national, regional, or international interests or exposes individuals and property to damage also falls under the term crime.

No matter how different the motives and criminal behaviors may be, this does not justify the occurrence of the crime or the perpetrator being subject to penalties. There are several reasons that lead to crime, including psychological conditions and stress, financial crises, the criminal's social status, and sometimes emotional reasons. The causes are multiple, but the goal is the same: the crime, which necessitates taking legal action against the perpetrator.

From a legal perspective, crime is defined through three main elements:

A. The material element (actus reus): This element includes the crime of murder, which is the direct act, whether by action or by failure to report the perpetrator or by concealing the perpetrator. The intent to cause harm or loss to an individual or institution does not fall under the material act; rather, the intent must be transformed into an act.

B. The moral element (criminal intent): This element primarily concerns the perpetrator's intent, as committing a crime is motivated by the intention to cause harm, which is the deliberate infliction of harm, or motivated by negligence, recklessness, and disregard for the consequences.

C. The legal element (the principle of legality): Acts cannot be criminalized unless there is a legal text criminalizing the act. Classifying acts and behaviors as crimes according to the law makes it obligatory to refrain from committing them, and anyone who commits them is covered by the law.

Definition and Evolution of Cybercrime

The rapid expansion of digital networks and information technologies has led to the emergence of cybercrime as a distinct category of criminal activity. Despite extensive discourse among legal scholars and policymakers, no universally accepted definition exists; various terms—such as "internet crimes," "computer-related offenses," "high-tech crimes," and "information fraud"—have been used interchangeably, though the term "cybercrime" is now widely adopted. Cybercrime encompasses offenses that exploit digital systems, targeting individuals, institutions, or governments through sophisticated technological means, ranging from data breaches and identity theft to large-scale cyberattacks on critical infrastructure. The lack of well-defined legal frameworks to address these offenses has exacerbated security challenges and underscores the urgent need for comprehensive legislation, because cybercrime exhibits distinct characteristics that differentiate it from conventional crimes. It is digitally executed, involving information systems, electronic devices, and internet-based platforms; it employs sophisticated, innovative techniques that bypass security systems by exploiting vulnerabilities; and it is typically non-violent, relying on deception, unauthorized access, or data manipulation. Many cybercrimes are collaborative, involving networks of perpetrators such as specialized hackers, financiers, and intermediaries, and they leave minimal physical evidence, complicating forensic investigations. Cyberattacks occur rapidly, exploiting automated processes and high-speed digital transactions, and their transnational reach allows perpetrators to operate remotely across multiple jurisdictions, often remaining undetected until significant harm is inflicted. Moreover, the rapid evolution of cyber threats has outpaced legislative efforts, resulting in legal ambiguity that complicates prosecution [3]. Initially, cybercrime was limited to isolated acts of hacking and simple fraud; however, the advent of the Internet in the late 20th century catalyzed a dramatic evolution. Over subsequent decades, as digital connectivity and technology advanced, cybercrime transformed into a highly coordinated, sophisticated enterprise. Advances in computing, the proliferation of online platforms, and the

integration of digital processes across sectors have expanded opportunities for cyber offenses. Modern cybercriminals exploit emerging vulnerabilities, employ cutting-edge techniques, and operate in transnational networks, thereby challenging traditional security paradigms and compelling the development of robust legal and technological defenses to counter these dynamic threats effectively.

Types of Cyberattacks

Cyberattacks are typically categorized into five main types: active, passive, close-in, distribution, and insider attacks. Active attacks, such as denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks, aim to disrupt systems by overwhelming them with traffic [4]. Man-in-the-Middle (MitM) attacks intercept communications to steal or manipulate data, while SQL injection attacks exploit web application vulnerabilities to access databases. Ransomware encrypts data and demands ransom, and Advanced Persistent Threats (APTs) are long-term espionage efforts. Malware attacks involve viruses, worms, or spyware to compromise systems. Passive attacks aim to gather information stealthily without system alteration. These include phishing, where users are tricked into revealing sensitive information [4], and Cross-Site Request Forgery (CSRF) attacks, which exploit web vulnerabilities. Eavesdropping and packet sniffing intercept data over networks, while credential stuffing attempts to access accounts using leaked credentials. Social engineering manipulates individuals to disclose confidential data, and steganography hides malicious code within files. Close-in attacks require physical proximity to the target system and often involve unauthorized access to hardware or networks. Examples include Evil Maid attacks, where malware is inserted into unattended devices, and shoulder surfing, where attackers observe credentials during input. Hardware keyloggers capture keystrokes through physically installed devices. Distribution attacks involve injecting malicious components into legitimate software or hardware. These include supply chain attacks, where a trusted vendor's products are compromised, and firmware manipulation, which embeds malware into device firmware during manufacturing. Compromised software updates inject malicious code into legitimate updates. Insider attacks are executed by individuals with legitimate access, making them especially dangerous. These attacks involve data theft, sabotage, and privilege misuse, where insiders exploit their access for unauthorized activities [5].

With continuous development and technological expansion, cyberattacks became ever changing. The most famous of cybercrimes are email and internet fraud, identity fraud (where personal information is stolen and used), theft of financial or card payment data, theft and sale of corporate data, cyberextortion (demanding money to prevent a threatened attack), ransomware attacks (a type of cyberextortion), crypto jacking (where hackers mine cryptocurrency using resources they do not own) and cyberespionage (where hackers access government or company data). Interfering with systems in a way that compromises a network, infringing copyright and selling illegal items online. soliciting, producing, or possessing child pornography.

Effects of Cybercrime

The impact of crimes always negatively affects the reputation of the country or causes outrageous losses. An example of this is the ransomware virus called WannaCry, which is one of the global crimes that occurred in 2017. Ransomware programs are malicious programs used to extort and take money by encrypting all the data in the devices and not decrypting it until the conditions of the hacker are met. This virus has caused losses estimated at up to 4 billion dollars [6]. There are also major fishing crimes that occurred in the 2018 World Cup. This process included emails that were sent to football lovers. This message tried to enter with fake free trips to Moscow, where the World Cup was hosted in Russia at the time, and personal data was stolen by people who pressed on mined links. [7], according to some statistics, British companies incurred losses estimated at 44 billion pounds [8] . Javelin has published statistics of losses caused by cyber fraud of an estimated $56 billion in 2020. [9]

Literature Review

Regional studies highlight that effective cybersecurity in the Middle East depends on robust legal frameworks and proactive enforcement strategies. For instance, the United Arab Emirates' Information Assurance Regulation and Saudi Arabia's initiatives under the National Cybersecurity Authority have set benchmarks by combining clear legal mandates with advanced tactical responses. Similar research (e.g., Binary Threat: Governments' Cyber Laws and Practices in the MENA Region) emphasizes that vague or overly repressive cybercrime laws can inadvertently stifle innovation while failing to protect citizens [10]. Despite these developments, Yemen's legislative apparatus remains underdeveloped due to political fragmentation and limited institutional capacity. The literature underscores the need for Yemen to adopt a balanced approach—one that upholds civil liberties and aligns with international legal standards while addressing the tactical shortcomings in cybercrime enforcement. Statistical data from the study "Cybersecurity As an Emerging Challenge to Yemen Security" by Ismail Humied indicate a significant increase in the volume of digital evidence processed by security agencies and a rising number of accused individuals [11].

IV. The Legislative Landscape in Yemen: Current Deficiencies and Their Impact

Yemen's digital expansion has not been accompanied by parallel developments in its cybersecurity legislative framework. Although the country has experienced significant growth in information and communication technologies [12], its legal infrastructure remains outdated and underdeveloped. This gap has fostered a vulnerability that not only facilitates the proliferation of cyber offenses but also hinders effective law enforcement. Yemen currently ranks among the lowest on the Global Cybersecurity Index—a stark indicator of its failure to implement modern cyber policies and regulations. This section critically examines the multifaceted deficiencies within Yemen's legislative framework, which compound existing socio-economic challenges and pose significant threats to national security.

Digital Expansion with Inadequate Safeguards

At the beginning of 2023, reports indicated that the number of internet users in Yemen had reached nine million, representing 27% of the total population of the Republic of Yemen. Nineteen million people also use mobile phones, and three and a half million use social media networks. [12] This indicates an increase in the use of information and communications technology by Yemenis. Conversely, there is no investment in cybersecurity, which exposes communications to the risk of attacks. [11] Surveys of 1,024 participants, both individuals and technology professionals, revealed that 88% of them do not feel safe using the internet in Yemen, while 90.1% believe that protection and security measures are insufficient. [13] These results provide strong evidence that legislative and legal reform has become an urgent necessity.

Increased Prevalence of Cybercrime

Numerous studies and research have indicated that the threat of cybercrime in Yemen is on the rise. The digital evidence being processed by security agencies is significantly increasing, which is clear evidence of the increase in cybercrime.

Lack of Comprehensive Legislation and Regulation

One of the most critical challenges facing Yemen is the absence of a coherent, dedicated cybercrime legal framework. Specific deficiencies include:

A. Absence of Enforceable Cyber Laws: Yemen lacks clear, enforceable legislation that explicitly addresses cyber offenses. Existing laws are often outdated and fail to incorporate provisions for digital evidence handling, breach reporting, or interagency cooperation.
B. Impact on Law Enforcement: The absence of comprehensive cyber laws hampers the capacity of law enforcement agencies to detect, investigate, and prosecute cybercrimes effectively. This legislative gap also undermines the confidence of both public and private institutions in the country's ability to protect digital assets.
C. Integration with Traditional Crimes: Many cyber incidents in Yemen are intertwined with traditional crimes, creating significant challenges for law enforcement. The failure to distinguish between cyber and conventional offenses has led to procedural ambiguities and ineffective investigative practices, further deepening systemic vulnerabilities.

Insufficient Cybersecurity Skills and Expertise

Yemen, like other developing countries, suffers from a shortage of cybersecurity specialists. This specialty has recently entered public and private universities, and at the time of writing, not a single batch of specialists in this field has graduated. This shortage is evident in:

a. Lack of competence in digital investigations: The lack of specialists in the field of digital investigations leads to loss, misplacement, or an inability to extract evidence. This makes it difficult to identify the real criminals, as the current staff in investigation departments employs traditional methods and is not specialized in digital evidence.

b. Skill gaps in law enforcement: The lack of adequate training in cybersecurity and digital forensics has primarily led to a shortage of evidence and testimony. This, in turn, has increased cybercrime rates, as law enforcement specialists are unable to prove crimes. This calls for the enactment of laws and legislation in this field and the training of specialists.

Weak Institutional Coordination and Law Enforcement

The fragmentation of the institutional framework in Yemen exacerbates cybersecurity challenges:

a. Weak reporting mechanisms: Numerous studies and research indicate that discovered crimes are discovered incidentally by security departments and criminal investigations and are not reported by victims or their relatives. A survey conducted in Aden Governorate revealed that 70.3% of participants did not know how to report cyber incidents or to whom to report them, reflecting a severe lack of institutional guidance [13].
b. Ineffective information sharing: The lack of joint cooperation among security agencies in Yemen has led to weak and fragmented efforts to track crimes and identify perpetrators. Each unit within the security services operates independently, isolated from the others. This has led to a failure to obtain evidence and track down perpetrators.

Emerging Threats from Terrorist and Criminal Networks

Increased Terrorist Threats and Crimes in Yemen

Exploitation of Digital Platforms:

Terrorist groups have been able to exploit the internet to recruit more members. They have also used the internet to spread their poison within society and create terror among people through social media, the internet, and online communication, which has increased their national threat.

State-Sponsored Cyber Espionage:

In addition to the proliferation of cyber weapons, cyber espionage by non-state actors has posed an additional complication.[15][16] The current legislative framework is incapable of addressing all these challenges and threats, further emphasizing the need to enact cybercrime laws.

International and Cross-Border Challenges

Yemen's isolation from its regional and global environment has exacerbated cybersecurity problems and the need to take appropriate legal measures.

A. Lack of Regional Cooperation: The lack of regional coordination among countries in the field of cybersecurity through treaties and agreements to combat cybercrime has strengthened the role of hackers, as Yemen is unable to prosecute foreign parties that violate the sovereignty of its citizens and homeland. This is another reason to coordinate efforts and unify goals toward enacting laws and legislation that punish violators.
B. Implications for National Security: The lack of unified international efforts, unified terminology, and unified legislation related to cybercrime has increased the risk of Yemen being exposed to cyberattacks, as attackers cannot be prosecuted internationally due to the lack of international legislation and agreements with Yemen.

Summary of Current Legislative Deficiencies

In summary, Yemen's legislative framework for cybersecurity is characterized by:

- A rapid digital expansion without corresponding investments in cybersecurity.

- A significant increase in both pure cyber and hybrid crimes.
- A lack of comprehensive, enforceable cybercrime laws.
- Insufficient technical expertise and public awareness.
- Fragmented institutional coordination and weak enforcement mechanisms.
- Escalating threats from terrorist groups and state-sponsored cyber espionage.
- Challenges stemming from limited international cooperation.
- These converging factors have created a risk environment that significantly undermines national security and public confidence in digital systems.

V. International and Comparative Cybersecurity Legal Frameworks—Tactical Lessons for Yemen

To address the profound legislative deficiencies outlined in Topic 3, it is essential to examine international and comparative cybersecurity legal frameworks. This section explores tactical lessons from both regional models and global best practices. By analyzing specific cases from Jordan, Kuwait, and the United Arab Emirates (UAE) as well as international instruments like the Budapest Convention on Cybercrime and the NIST Cybersecurity Framework, this discussion offers concrete recommendations for developing a robust legal framework tailored to Yemen's socio-economic and technological context.

Jordan's Cybercrime Law No. 17 (2023)

Jordan's 2023 update to its cybercrime legislation represents a modern approach to regulating digital offenses. Key tactical measures include:

A. Precise Legal Definitions: The law provides clear definitions for offenses such as unauthorized data access and digital fraud. This precision minimizes ambiguity and enhances both investigative and judicial processes, enabling law enforcement to differentiate effectively between cyber and traditional crimes—a critical issue in Yemen [19].

B. Standardized Evidence Protocols: The implementation of standardized protocols for digital evidence collection, preservation, and forensic analysis ensures that digital evidence meets international admissibility standards. This measure improves the prosecution of cyber offenses by ensuring that evidence is processed uniformly and reliably.

For Yemen, adopting similar legal clarity and standardized protocols would address the current overlap between cyber and traditional crimes, thereby enhancing investigative outcomes and judicial credibility.

Kuwait's Cybercrime Law No. 63 (2015)

Cybercrime Law No. 63 of 2015 sets a unique model in terms of implementing regulations and interagency coordination:

A. Multi-level crimes: Crimes are categorized based on their severity, with Kuwaiti law following a distinct approach to penalties and resource allocation. Minor offenses are subject to lighter penalties, while more severe offenses are subject to severe penalties. This approach facilitates law enforcement and the optimal use of legal resources, ensuring that major crimes receive the attention they deserve [18].

B. Enhanced operational coordination: The law requires coordination among all government agencies in Kuwait. This has, in turn, led to faster law enforcement, a faster response, and increased efficiency in resource allocation for cyber investigations.

For the Republic of Yemen, introducing a multi-level system with this level of precision will allow for the prioritization of cases, while enacting protocols for coordination between multiple agencies will ensure the severity of problems between different agencies and contribute to smooth law enforcement.

The United Arab Emirates (UAE): Strategic Investment and Centralization

The integration of strategic investments and central coordination has shaped a unique approach to cybersecurity in the UAE:

A. Investment in technology: Sheikh Tahnoon bin Zayed led significant technology investment initiatives in the UAE's cybersecurity infrastructure. For example, a permanent $1.5 billion partnership with Microsoft aimed at improving defense capabilities has also preserved innovation in digital security technologies.[17] This model demonstrates the alignment of IT investment with national security objectives.

B. Centralized cybersecurity bodies: Establishing central cybersecurity bodies to coordinate between departments and units specialized in cybersecurity has reduced confusion and chaos. The body has ensured coordination and harmony between departments and units, ensuring effective communication without overlapping tasks and responsibilities. This is a tremendous step and a distinctive model for the Republic of Yemen in light of the current institutional challenges.

C. Central Cybersecurity Bodies: The establishment of central bodies for policy coordination, incident management, and international cooperation has reduced bureaucratic fragmentation in the UAE. The central body ensures a coherent national strategy and improves communication between agencies, a vital step for Yemen given the current institutional challenges. The Republic of Yemen's approach to establishing a central cybersecurity body under a single umbrella will enhance coordination and coherence among units and achieve its desired goals smoothly. Coordination between various entities, including telecommunications, banks, and electricity, will significantly enhance the cybersecurity posture and mitigate challenges.

Global Best Practices: International Frameworks

A. The Budapest Convention on Cybercrime

Although Yemen has not ratified the Budapest Convention, it has established a comprehensive model for advanced cyber legislation. Its components include:

a. Harmonization of legal provisions: The Convention provides a solid framework for defining cybercrimes in a way that enhances international cooperation. By adopting similar definitions, Yemen can align its

legislation with international standards, which will facilitate mutual legal cooperation and cross-border investigations [20].

b. Digital forensics: The Convention requires all parties to adhere to strict and standardized procedures for collecting and analyzing digital evidence. This demonstrates the urgent need to build high-level technical, material, and human capabilities, which will in turn contribute to adapting protocols and enable Yemen to bridge the gap between outdated laws and the requirements of modern cybercrime investigations.

B. The NIST Cybersecurity Framework

Created by the National Institute of Standards and Technology (NIST), this framework has been widely recognized around the world for its flexible, risk-based methodology:

a. Systematic Risk Management: The NIST framework is structured—Identify, Protect, Detect, Respond, Recover—during cyber incidents. This model could enable Yemen to better allocate its scarce resources and develop baseline cybersecurity practices within its critical infrastructure [14].

b. Enablement of Cross-Sector Collaboration: The NIST framework for cybersecurity encourages cross-reporting and collaboration across the public and private sectors.

Tactical Recommendations for Yemen

The tactical recommendations outlined below lead to the implementation of unified regional visions and global best practices.

C. Clarity and Precision of Legislation

a. Adopting clear definitions of cybercrimes: Adopting clear and specific definitions of cybercrimes is one of the most urgent needs in the Republic of Yemen. Referring to the Jordanian Cybercrime Law No. 1 of 2011, the use of clear and precise terminology reduces ambiguity and enhances the effectiveness of law enforcement.

Distinguishing between types of cybercrimes and conventional crimes is of paramount importance for achieving fair judicial outcomes.

b. Unifying forensic protocols: The law should clarify specific methods for obtaining digital evidence, as well as its handling, storage, and analysis. This will result in better practices for the Budapest Convention in terms of standardizing evidence in line with international standards, which in turn will enhance prosecutions due to the standardization of procedures.

D. Enhancing institutional coordination and enforcement

a. Establishing a central authority specialized in cybersecurity: This will unify efforts and facilitate operational coordination among all units and departments. A single entity will oversee and monitor operations, with the primary mission of ensuring coordination among all parties. This will enhance law enforcement and address deficiencies in the current situation.

b. Implementing a multi-tiered classification of crimes: Implementing a cybercrime classification system in the Republic of Yemen, modeled after Kuwaiti law, will enhance law enforcement and allocate resources efficiently while ensuring law enforcement at all levels, regardless of the crimes and their nature.

E. Strategic Investment and Capacity Building

A. Due to budget limitations, Yemen should develop a staged approach to build its modern cybersecurity infrastructure. The first stage of investments should focus on implementing modern infrastructure in telecommunications along with banking institutions and energy networks through the development of digital forensic labs with protected data centers and advanced IT equipment.

B. A systematic training system must be developed because Yemen lacks sufficient cybersecurity professionals. Integrating foreign organizations and implementing NIST-based training initiatives will create qualified cybersecurity workforce capabilities among public authorities and private businesses.

F. Promote Public-Private and International Collaboration

a. The government needs to develop permanent platforms that combine both forums and workshops and advisory boards that enable communication among public sector personnel together with cybersecurity specialists alongside private business stakeholders and diplomats from across the globe. The established collaboration between entities will enable quick adjustments to new security threats through ongoing practice sharing.

b. International cybersecurity standards become necessary for Yemen to follow by partnering with global institutions and accepting international protocols, including the Budapest Convention and NIST standards. Such nationwide alignment between bordering entities will create more effective cooperation while setting standards for Yemen to evaluate its progress officially.

The Republic of Yemen faces numerous challenges in the field of cybersecurity legislation on several levels. The rapid expansion of information and communications technology, as well as the introduction of Starlink services to Yemen, have exacerbated these challenges. Conversely, weak infrastructure and the lack of qualified personnel to manage the digital transformation process have exacerbated these complexities. Based on experience and concrete realities, including the lack of coordination and clear definitions and applicable legislation for cybercrimes, the urgent need to enact legislation and keep pace has emerged. We need clear and precise definitions, such as contamination, and a multi-level classification, as in Kuwait, and work to implement the Budapest Convention and the National Institute of Standards and Technology's Cybersecurity Framework. Then the Republic of Yemen can overcome these challenges and difficulties. In short, the Republic of Yemen needs high-level institutional coordination under a central cybersecurity authority, and investment in cybersecurity through the public and private sectors. This, in turn, will enhance the detection of cybercrime, facilitate the collection and proper analysis of

evidence and testimony, strengthen national security, and prosecute perpetrators of crimes and attacks. All of this will create sustainable development for Yemen and position it in the global digital economy. We live in an era where cyberattacks are increasing and their methods and techniques are diversifying, and there is a constant state of development in offensive technologies. With this rapid pace, Yemen must keep pace with this development.

VI. Proposal Framework and Strategic Measures for Cybercrime Laws in Yemen

Drawing on the analysis of Yemen's current legislative deficiencies and the tactical lessons from international and regional best practices, this proposal framework presents a comprehensive legal and institutional strategy to address Yemen's cyber vulnerabilities. The framework is designed to create a resilient digital ecosystem that supports national security and economic development. It not only outlines a robust legal framework but also recommends strategic measures aimed at reducing cybercrimes through improved internet regulation and effective enforcement mechanisms.

Proposal Framework

The framework begins by acknowledging Yemen's rapid ICT expansion amid fragile socio-economic conditions and ongoing security challenges. Despite notable growth in digital connectivity, current cyber defenses remain inadequate. This legislative proposal is premised on the urgent need to protect critical infrastructure, enhance public and institutional confidence, and ensure that Yemen's digital ecosystem is secure and resilient. The primary objectives of the proposed framework are to:

- The national infrastructure, together with public institutions and private enterprises require protection against cyberattacks.
- The protection of sensitive personal information remains essential with laws that defend citizen privacy rights.
- The establishment of precise legal definitions needs to develop clear categories and definitions for cyber offenses.
- Enhance Enforcement and Coordination: Strengthen law enforcement capacities through improved interagency cooperation and effective digital forensic practices.
- The framework needs to develop legal mechanisms that react to emerging technologies along with new cyber dangers.
- Yemen needs to adopt global cybersecurity standards that promote international cooperation to achieve mutual assistance.

A. Scope

A complete set of cyber offenses needs to be included within legal provisions. Key areas include:

- Unlawful entry into computer systems and operational breaches of databases should be treated as criminal offenses. Thieves of data and anybody who breaches this law must face severe consequences.
- Online scams, together with phishing and unauthorized electronic fund transfers, should be expressly banned by the proposed legislation. The law should establish means to follow digital money transfers.
- The definition specifies digital methods of threat activity that endanger security at the national level or interfere with essential services. Higher punishments should apply to any criminal action that threatens essential infrastructure facilities.
- Lawmakers should enforce complete restrictions on malware creation together with attacks such as denial-of-service while banning all distribution and usage of such harmful software elements. These risks will need specific instructions for detection and countermeasures.
- The laws should acknowledge offenses that combine traditional and cyber components, such as cyber-enabled forgery and theft. Crime classifications should be organized into different tiers to match appropriate disciplinary measures exactly.
- The standard establishes formal methods to handle digital evidence through procedures that guarantee international forensic compatibility standards in evidence collection and preservation and court admission.

B. Institutional Framework and Enforcement

The framework puts forward comprehensive institutional structures to implement these legal provisions.

National Cybersecurity Authority (NCA):

A unified authority under the National Cybersecurity Authority should supervise the following agenda:

- Formulating national cybersecurity policies.
- Coordinating interagency efforts.
- The authority at the national level should issue operational guidelines and carry out standard cybersecurity audits as part of its responsibilities.
- Serving as a liaison for international cyber cooperation.

Law enforcement agencies must build distinct cybercrime units through the Criminal Investigation Department to receive specialized digital forensic instruments. The units require specialized education in cybercrime investigations because existing skills need to be filled.

Judicial training and digital evidence protocols must implement specific educational programs that prepare judges, together with prosecutors, to effectively handle cases of cybercrime. A set of official procedures must be established to manage digital evidence in a manner that satisfies worldwide best standards in judicial proceedings.

C. Procedural Measures and Compliance

Every proposed legislation must incorporate operational requirements that enable fast and efficient actions against cyber occurrences.

a. Organizations need to fulfill dual requirements for incident reporting that includes both time boundaries and specific reporting obligations.
b. A unified incident response center must exist for coordinating digital threat monitoring between different agencies.

All critical infrastructure sectors should undergo periodic risk evaluations while being subjected to periodic compliance checks. Organizations must undergo compliance audits to

check cybersecurity standard compliance, which ensures ongoing system improvements.
Strong data protection measures for personal information implementation remain necessary through integrated privacy and protection provisions. Utilities must create specific guidelines that align personal rights to privacy with necessary cybersecurity requirements.

D. Strategic Measures to Reduce Cybercrime

In parallel with the legislative framework, the following strategic measures are recommended to reduce cybercrime and enhance internet regulation:

E. Strengthening Internet Regulation

a. The regulatory oversight needs to develop standards that keep track of best practices in cybersecurity throughout public and private sector entities. Standards of ISO/IEC 27001 and NIST Cybersecurity Framework must be strictly applied through regulatory mandates.

b. Certification and Compliance Programs: Introduce cybersecurity certification for critical infrastructure operators. The certifications have to undergo periodic audit procedures along with compliance tests to validate organizational compliance with strict cybersecurity requirements.

c. The consideration should exist for security protocol implementation that mandates data localization of sensitive information or encourages such measures. The implementation of this method enables better digital data oversight and regulation, which enables the enforcement of local laws.

F. Enhancing Enforcement Mechanisms

a. Specialized Cybercrime Courts should be created under the direction of judges who have received specialized training in cyber law. New courts specializing in cyber cases would process complicated technology-based cases efficiently while enhancing conviction rates because of specific judicial expertise.
b. Integrated Cyber Intelligence Centers should become operational entities to unify intelligence gathered by public law enforcement agencies and regulatory entities and private sector organizations. The centers would operate real-time threat monitoring while performing analysis to coordinate responses toward cyber incidents.
c. Yemen should establish bilateral and multilateral cross-border legal instruments that support mutual provision of cybercrime investigation assistance. Through direct Budapest Convention membership or establishing bilateral agreements, Yemen can improve their ability to work with foreign countries.

G. Capacity Building and Public-Private Partnerships

a. The establishment of national training programs should begin alongside program development meant to develop knowledgeable cybersecurity experts. International agencies working alongside academic bodies provide solutions for existing workforce deficiencies.
b. A nationwide educational effort through public campaigns should teach citizens alongside business entities methods of cyber hygiene alongside risk reduction techniques and guidelines for fast cyber incident reporting. These initiatives will decrease the rate of achievement among phishing attacks and social engineering techniques as well as other cyber threats.
c. Local universities and research institutions should obtain grants and incentives from the government to develop customized cybersecurity solutions for Yemen's specific circumstances. Such activities enable local entities to create their own homegrown technologies and methodologies.
d. Public-Private Collaboration: Foster partnerships between government, industry, and civil society. A combination of regular forums together with workshops and advisory committees helps support ongoing interaction for sharing best practices at all times. The fast-paced development of policies stands as essential in addressing newly emerging threats because of collaboration among different entities.

H. Implementation Roadmap

Yemen needs to implement a step-by-step approach for the cybercrime law due to resource limitations and political obstacles.

Short-Term (0–1 Year):
The proposed cybercrime law needs to be drafted and circulated for stakeholders to give their opinion.
A temporary consulting body composed of cybersecurity specialists and representatives from law enforcement with industry leaders needs to be formed.
The organization must begin testing training programs for new units that focus on cybercrime investigation.
Launch preliminary public awareness campaigns.

Medium-Term (1–3 Years):
The government must enact a complete cybercrime law through approval of stakeholder input.
The National Cybersecurity Authority, together with specialized cybercrime units, requires full operational capacity.
Mandatory reporting systems must be implemented to establish a central incident management center for organizations.
The periodic audits for critical infrastructure monitoring along with risk assessments should start.

Long-Term (3–5 Years):
The law should undergo periodic reviews together with required amendments to match modern technological developments and security threats throughout time.
Yemen needs to build stronger international alliances along with the adoption of global cybersecurity standards for its framework.
Develop a sustainable model for continuous improvement through research, innovation, and expanded capacity-building initiatives.

Conclusion

In summary, Yemen faces significant challenges in its cybersecurity legislative framework, as detailed in Topic 3. The lack of comprehensive laws, insufficient technical expertise, weak institutional coordination, and an evolving threat landscape have collectively contributed to a high-risk environment that jeopardizes national security and public confidence in digital systems.

By leveraging tactical insights from international and regional best practices (Topic 4), this proposal framework outlines a multi-faceted strategy designed to address these deficiencies. The proposed legal framework emphasizes clear legal definitions, standardized digital evidence protocols, robust institutional arrangements, and dynamic procedural measures. In tandem with these legislative reforms, strategic measures such as enhanced internet regulation, specialized enforcement mechanisms, capacity-building initiatives, and public-private partnerships are critical to reducing cybercrime.

The implementation roadmap provides a phased approach that takes into account Yemen's current resource constraints while setting a clear path for future development. Ultimately, the successful adoption of this framework will not only fortify Yemen's cybersecurity defenses but also restore public and institutional confidence in the nation's digital infrastructure. Through comprehensive reform and strategic investment, Yemen can transform its cyber landscape, aligning it with international standards and positioning itself for sustainable growth in an increasingly digital world.

VII. International Legal Frameworks' Ability to Inform Yemen's Cybersecurity Strategy

Global legal frameworks can significantly contribute to formulating a cybersecurity strategy in the Republic of Yemen through direct or indirect oversight and a systematic approach, as well as through joint cooperation with international frameworks and adapting these policies and legislation to the current Yemeni situation in a manner consistent with national policies and Yemeni laws. The following is a systematic explanation of these frameworks:

A. Adopting anti-cybercrime legislation

Budapest Convention: By leveraging the Budapest Convention, it is possible to harmonize cybercrime laws such as piracy, impersonation, and fraud, and to establish broad powers for digital investigations. This will enhance the possibility of international cooperation in prosecuting cybercrime and tracking its perpetrators. [20]

United Nations Resolutions: Strengthening accountability by leveraging United Nations General Assembly Resolutions (73/27 and 74/29) regarding responsible conduct of states in cyberspace to prevent malicious activities [21], [22].

Integrating International Humanitarian Law: Adherence to the principles of international law for cyber operations is mandatory, including aspects of distinction, proportionality, and necessity. The Republic of Yemen is also obligated to protect physical infrastructure such as hospitals, banks, and electricity grids from cyberattacks, in accordance with the Geneva Convention [23].

B. Regional Cooperation

The League of Arab States Cybersecurity Agreement: Using the agreement as a model for harmonizing laws with neighboring countries, allowing for the exchange of information on shared interests, common threats, and rapid, coordinated responses to regional threats such as ransomware or state-sponsored attacks [24].

C. Data Protection and Privacy

Enacting data governance laws based on the General Data Protection Regulation (GDPR)[25] or the African Union Convention on Cybersecurity will build trust among information technology users and attract foreign investment to Yemen.[26] Establishing an independent data-protection body that enforces personal privacy laws.

D. Capacity Building and Partnerships

Leveraging global capabilities and expertise, such as the International Telecommunication Union (ITU) [27], the United Nations Office on Drugs and Crime (UNODC), and Interpol [28], will help train staff, develop cybersecurity infrastructure, and adopt best practices in cybersecurity, leveraging the National Institute of Standards and Technology. [29] Seeking international support and funding for vital projects, such as National Computer Threat Response Teams (CERTs).

E. Ensuring Human Rights

Compliance with international human rights law and ensuring the protection of human rights and the right to privacy are top cybersecurity priorities, such as the International Institute for Civil and Political Rights [30]. By enforcing human rights laws that prohibit abuses and violations, as well as acting with transparency, all under judicial oversight to protect freedom of expression and privacy. [31]

F. Conflict-sensitive approaches.

Prioritizing the protection of infrastructure and humanitarian aid systems, primarily UN security assistance, from any cyber threats, and implementing risk response protocols in accordance with the Office for the Coordination of Humanitarian Affairs (OCHA) to mitigate risks during crises. [32]

G. Participation in multilateral forums.

Actively participating in UN Open Working Group (OEWG) discussions to develop global standards and advocate for addressing Yemen's needs, such as access to cybersecurity resources in conflict-affected countries.

Participating in UN Open Working Group discussions to formulate global standards and advocate for addressing Yemen's needs, such as equitable access to cybersecurity resources for conflict-affected countries. [33]

Challenges and Considerations:

H. Political Stability:

Working gradually to protect vital sectors in Yemen while requesting international assistance in implementing governance structures. [34]

I. Local Context:

Reconciling the community's need for technological resources, such as mobile phones, which are the most widespread in Yemen, with laws and regulations, and working to ensure their use is not impeded by the law.

By working according to a clear, long-term strategic plan, Yemen can overcome all threats and difficulties and enhance regional and international cooperation. [35]

J. Policy Implications

The proposed legislative reforms and tactical approaches are designed to be integral to Yemen's broader digital transformation goals, aiming to foster a secure and resilient digital environment. By strengthening cybersecurity infrastructure and legal frameworks, these reforms directly

support initiatives such as the potential adoption of satellite internet services like Starlink. A robust cybersecurity posture is essential for maximizing the benefits of such technologies, ensuring data integrity, protecting critical communications, and fostering public trust in digital services. Aligning these reforms with national digitalization strategies will not only mitigate cyber threats but also accelerate economic growth, enhance public service delivery, and improve connectivity for citizens across the nation, thereby integrating Yemen more fully into the global digital economy.

K. Stakeholder Engagement

Effective implementation of this framework necessitates comprehensive stakeholder engagement to address potential resistance and ensure broad buy-in. Key challenges include political barriers, institutional fragmentation, and severe budget constraints. To navigate these:

Political Buy-in: Engage high-level government officials, influential tribal leaders, and diverse political factions through regular briefings and workshops to highlight the national security and economic benefits of cybersecurity. Emphasize that a unified approach to cyber threats transcends political divides.

Institutional Coordination: Foster collaboration among various government ministries, telecommunication companies, financial institutions, and security agencies. Establish clear communication channels and joint task forces under the proposed National Cybersecurity Authority to overcome the current fragmentation and ensure coherent policy execution.

Budget Allocation: Develop a phased implementation plan that prioritizes critical investments, aligning with the "step-by-step approach for the cybercrime law" to manage resource limitations. Seek partnerships with international organizations and donor countries for technical assistance, training programs, and funding for critical infrastructure upgrades. Transparency in resource allocation and measurable outcomes will be crucial for securing continuous support.

Public Awareness: Continue and expand nationwide educational campaigns to enhance public understanding of cyber risks and reporting mechanisms, as a significant portion of the population lacks awareness. This will help build a resilient cyber culture and reduce human vulnerability.

Future Research

To continuously evaluate the effectiveness and impact of the proposed cybersecurity framework post-adoption, future research should focus on longitudinal studies. These studies could:

Assess Impact Metrics: Track key performance indicators (KPIs) such as the incidence of cybercrimes, the efficiency of prosecution, the reduction in financial losses due to cyberattacks, and improvements in critical infrastructure resilience over time.

Evaluate Policy Efficacy: Conduct in-depth analyses of the newly implemented laws and policies to determine their practical application, identify unforeseen challenges, and propose necessary adjustments based on real-world outcomes.

Measure Capacity Building: Evaluate the effectiveness of training programs and capacity-building initiatives in developing local expertise and strengthening the cybersecurity workforce in Yemen.

Monitor Threat Landscape Evolution: Continuously monitor the evolving cyber threat landscape in Yemen and the region to ensure the framework remains adaptive and responsive to new vulnerabilities and attack methodologies.

Examine Socio-Economic Impact: Investigate how improved cybersecurity contributes to broader socio-economic development, investment, and digital inclusion within Yemen's conflict-affected context.

References

[1] Information Systems Audit and Control Association, *Cybersecurity Fundamentals Study Guide*, Rolling Meadows, Illinois: ISACA, 2015.

[2] Swan Software Solutions, “The Three Dimensions of the Cybersecurity Cube.” [Online]. Available: https://swansoftwaresolutions.com/the-three-dimensions-of-the-cybersecuritycube/. Accessed: Jan. 5, 2025.

[3] M. Q. A. Al-Radfani, *Police Investigations into the Challenges of Cybercrime*. Accessed: Jan. 12, 2025.

[4] C. M. Williams, R. Chaturvedi, and K. Chakravarthy, "Cybersecurity Risks in a Pandemic," *Journal of Medical Internet Research*, Sep. 2020. [Online]. Available: https://doi.org/10.2196/23692.

[5] A. K. Ghazi-Tehrani and H. N. Pontell, "Phishing Evolves: Analyzing the Enduring Cybercrime," *Victims & Offenders*, Feb. 2021.

[6] Kaspersky, “What is WannaCry ransomware?” Kaspersky, 2024. [Online]. Available: https://www.kaspersky.com/resource-center/threats/ransomware-wannacry. Accessed: Jan. 18, 2025.

[7] Security List, “2018 Fraud World Cup.” [Online]. Available: https://securitylist.com/2018-fraud-world-cup/85878/. Accessed: Jan. 23, 2025.

[8] Al Jazeera, “Cyberattacks on British companies,” *Al Jazeera*, Nov. 25, 2024. [Online]. Available: https://aljazeera.net/ebusiness/2024/11/25/cyber-attacks-british-companies. Accessed: Jan. 29, 2025.

[9] Javelin Strategy, “Total Identity Fraud Losses Soar to $56 Billion in 2020.” [Online]. Available: https://javelinstrategy.com/press-release/total-identity-fraud-losses-soar-56-billion2020. Accessed: Feb. 2, 2025.

[10] A. Shaheed and B. Greenacre, "Binary Threat: How Governments' Cyber Laws and Practice Undermine Human Rights in the MENA Region," *Project on Middle East Political Science*, Mar. 2025.

[11] A. Humied, "Cybersecurity As an Emerging Challenge to Yemen Security," *Journal of Cyber Security in Computer System*, Oct. 2022.

[12] DataReportal, *Digital 2023: Yemen Report*, 2023. [Online]. Available: https://datareportal.com/reports/digital-2023-yemen. Accessed: Feb. 7, 2025.
[13] A. J. F. Obaid, "Survey on Cybersecurity Awareness in Yemen," unpublished dataset, UST, Feb. 2025.
[14] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, 2018. [Online]. Available: https://www.nist.gov/cyberframework. Accessed: Feb. 12, 2025.
[15] Reuters, "Iran's Supreme Leader Calls for Cyberspace Regulation," *Reuters*, Aug. 27, 2024.
[16] The Guardian, "Pakistan's Internet Slowdowns Blamed on Firewall Testing," *The Guardian*, Aug. 21, 2024.
[17] Wired, "UAE Intelligence Chief on AI and Cybersecurity Investments." [Online]. Available: https://www.wired.com/story/uae-intelligence-chief-ai-money/.
[18] Wikipedia, "Cybercrime Law No. 63 (Kuwait)." [Online]. Available: https://en.wikipedia.org/wiki/Cybercrime_Law_No._63.
[19] Wikipedia, "Cybercrime Law in Jordan." [Online]. Available: https://en.wikipedia.org/wiki/2023_cybercrime_law_in_Jordan.
[20] Council of Europe, *Convention on Cybercrime*, 2001. https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185.
[21] United Nations General Assembly, *Resolution 73/27*, 2018.
[22] United Nations General Assembly, *Resolution 74/29*, 2019.
[23] International Committee of the Red Cross, *Geneva Conventions of 1949 and Additional Protocols*, 2016. https://ihl-databases.icrc.org/ihl.
[24] League of Arab States, *Arab Cybersecurity Agreement*, 2019. https://www.lasportal.org/.
[25] European Union, *General Data Protection Regulation (GDPR)*, 2018. Available: https://gdpr-info.eu/.
[26] African Union, *Convention on Cyber Security and Personal Data Protection*, 2014. https://au.int/en/treaties.
[27] International Telecommunication Union, *Global Cybersecurity Index*, 2021. https://www.itu.int/cybersecurity.
[28] INTERPOL, *Cybercrime Directorate*, 2023. https://www.interpol.int/Crimes/Cybercrime.
[29] NIST, *Cybersecurity Framework*, 2018. https://www.nist.gov/cyberframework.
[30] United Nations, *International Covenant on Civil and Political Rights*, 1966. https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights.
[31] E. Lievens *et al.*, "Human Rights and Cybersecurity," *IEEE Security & Privacy*, vol. 18, no. 2, pp. 61–67, 2020.
[32] UNOCHA, *Guidelines on Humanitarian Data Protection*, 2021. https://www.unocha.org/.
[33] United Nations, *Open-Ended Working Group on Developments in ICTs*, 2021. https://front.un-arm.org/.
[34] M. Dunn Cavelty, "Cybersecurity in Fragile States," *IEEE Transactions on Technology and Society*, vol. 2, no. 3, pp. 128–135, 2021.
[35] GSMA, *Mobile Economy: Middle East and North Africa*, 2022. https://www.gsma.com/mobileeconomy/.

Hybrid GAN-CNN Model for Brain Tumor Detecting and Classifying Diseases Based on MRI Images.

Monia Abdullah Ahmed Al-hobishi[1,*]
Muhammed Fadhl Abdullah [1]

Received: 07/05/2025
Revised: 20/06/2025
Accepted: 21/06/2025

[1] College of engineering and computing, IT department, University of Science and Technology, Aden, Yemen
*Corresponding Author's Email: malbadwi@ust.edu

Hybrid GAN-CNN Model for Brain Tumor Detecting and Classifying Diseases Based on MRI Images.

Monia Abdullah Ahmed Al-hobishi
College of engineering and computing, IT department, University of Science and Technology, Aden, Yemen.
Aden, Yemen
Eng.Monia85@gmail.com

Muhammed Fadhl Abdullah
College of engineering and computing, IT department, University of Science and Technology, Aden, Yemen.
Aden, Yemen
malbadwi@ust.edu

Abstract— Brain cancer diagnosis using MRI scans is aided by the advancement of artificial intelligence, a promising tool in medical imaging, but further optimisation is needed due to privacy constraints and limited medical imaging data availability.
To address these challenges, this study proposes a **hybrid algorithm** that integrates **Convolutional Neural Networks (CNNs)** with **Generative Adversarial Networks (GANs)** for data augmentation and improved classification accuracy. To enhance training efficiency, **an additional 15 epochs** are incorporated into each network and introduced to optimise brain cancer classification. **Two deep learning models—CNN and GANs—are trained on synthetic MRI Dataset Kaggle (2022) images generated by GAN architectures and evaluated using real brain MRI scans.**
Experimental results demonstrate that **CNN** outperforms the other models, achieving a loss of 0.2301, accuracy of 98.90%, validation loss of 0.4756, and validation accuracy of 84.56% when trained on **brain cancer images generated by GANs with a generator loss of** 1.4502, discriminator loss of 0.8163, and fake image accuracy of 83.12%. Real Image Accuracy: 92.34%
These findings confirm that the **proposed hybrid algorithm** 98.85% accuracy significantly enhances brain cancer classification using deep learning techniques.

Keywords— MRI image dataset Kaggle (2022); GANs, CNN, hybrid algorithm, deep learning.

I. Introduction

Brain cancer is one of the most serious and complex types of cancer, with thousands of cases diagnosed annually. It accounts for a significant proportion of cancer-related deaths due to its critical location and the challenges in detection and treatment. According to the World Health Organisation (WHO), incidence rates vary based on age, gender, and geographical location, making it a global health concern.
As of 2024, the **brain cancer mortality rate in Yemen** remains a significant public health concern. While specific data for 2024 is not yet available, the **Global Cancer Observatory (GCO)** provides estimates for 2020, indicating that the age-standardised mortality rate for brain and central nervous system cancers in Yemen was **5.9 per 100,000 population**.
Tumour detection and classification are critical challenges in the medical domain, prompting extensive research into various tumour types, particularly the most aggressive and life-threatening ones. **Brain tumours** represent a serious health concern, affecting both adults and children. Each year, they are diagnosed with a brain tumour, highlighting the urgent need for **early detection** to enhance survival rates and improve life expectancy through accurate diagnosis and timely treatment **[3, 4]**.
However, in medical image classification, obtaining a sufficiently large dataset—such as MRI scans—is crucial for reducing error rates and ensuring reliable diagnosis.
Early detection and timely intervention are crucial for improving patient outcomes and increasing survival rates in cancer patients, as they enable the identification of abnormal growths. Additionally, **Hybrid Generative Adversarial Networks (GANs)** and **Convolutional Neural Networks (CNNs)**. GANs, consisting of a generator and discriminator, are widely used in healthcare technology due to their robustness and high performance. CNNs, a deep learning model, are used for image classification and object detection due to their ability to extract patterns [1]. A significant application of hybrid algorithms is in addressing the issue of **limited medical datasets** (Kaggle, 2022) by generating additional images to support training processes, ultimately improving classification accuracy.
There is a **shortage of professionals** in the field, which necessitates the use of **advanced technological solutions**. Machine learning, particularly **deep learning**, has demonstrated remarkable success in various domains, including **medical image processing [2]**. Deep learning models can enhance diagnostic accuracy by automatically classifying MRI images into two categories: **tumour-present and tumour-absent**.
The remainder of this paper is organised as follows: Section 2 reviews related literature and highlights recent advancements in brain tumour detection using deep learning. Section 3 describes the proposed hybrid GAN-CNN framework, detailing its architecture and components. Section 4 explains the experimental setup, including dataset preparation, image augmentation using GANs, CNN training, and evaluation criteria. Section 5 presents the results and provides an in-depth discussion of model performance. Section 6 offers a critical analysis comparing the hybrid model to existing state-of-the-art methods. Finally, Section 7 concludes the paper by summarising the key findings and outlining future research directions.

II. Literature Review

Numerous studies have explored AI in brain tumor classification. Table 1 summarizes key methodologies:

Table 1. Summary of Existing Deep Learning Techniques for Brain Tumor Detection Using MRI Images.

Ref	Year	Method	Dataset	Performance Metrics
[3]	2022	RN-OKELM	BT (98/155 MRI)	Accuracy 97.93%, Sensitivity 97.92%, Specificity 97.98%
[4]	2022	EfficientNet	Kaggle T1 contrast	Accuracy 98.78%, Precision 98.75%, Recall 98.75%
[5]	2022	DA-SVM	Bakas et al., Tobon-gomez	Accuracy 89.93%, Sensitivity 88.96%
[6]	2022	C-GAN	Public tumor datasets	Detection Accuracy 99%, Classification 98%
[7]	2022	DCGAN + CNN	Public tumor datasets	Accuracy 98.12%, Precision 97.08%
[8]	2024	CNN + Styled GANs2	BraTS 2021, Gazi Brains 2020	Accuracy 97.99%

Explanation:

- **[3] RN-OKELM (2022):** Utilized a residual network with optimal kernel-based ELM for classification, achieving strong performance but based on a relatively small dataset.
- **[4] EfficientNet (2022):** Used a modern, efficient CNN architecture on Kaggle's contrast-enhanced MRI images, producing high accuracy with balanced precision and recall.
- **[5] DA-SVM (2022):** Applied a traditional support vector machine enhanced with data augmentation. While effective, it underperformed compared to CNN-based models.
- **[6] C-GAN (2022):** Used conditional GANs to generate and classify images, showing high detection and classification accuracy due to data synthesis.
- **[7] DCGAN + CNN (2022):** Combined deep convolutional GANs with advanced CNNs like MobileNet and ResNet, which led to robust image generation and classification.
- **[8] CNN + Styled GANs2 (2024):** Leveraged powerful StyleGAN2 architecture alongside CNNs for brain tumor classification, achieving near-perfect accuracy using recent datasets.

Despite the progress, many of these approaches do not validate the quality of synthetic images rigorously. Our proposed hybrid model addresses this gap by incorporating both generation and validation steps.

III. Materials and Methods

Data Collection
100 MRI images (25 normal, 75 tumour) from Kaggle were used. Data was augmented using GANs.

GAN Architecture
The GAN model consists of two core components: a **generator** and a **discriminator**.

- The **generator** creates synthetic MRI images by learning to capture the underlying data distribution.
- The **discriminator** distinguishes between real and synthetic images, providing feedback that helps the generator improve.
- The two networks are trained in opposition over 15 epochs until the generator produces high-quality, realistic images.
- Performance metrics include Generator Loss (1.4502) and Discriminator Loss (0.8163), with accuracy rates showing steady improvement across epochs.

CNN Architecture
The CNN model is composed of several sequential layers:

- **Input Layer**: Accepts 2D MRI image inputs.
- **Convolutional Layers**: Apply filters to detect features such as edges, textures, and shapes.
- **Activation Functions (ReLU)**: Introduce non-linearity to allow learning of complex patterns.
- **Pooling Layers**: Reduce dimensionality while retaining important spatial information (e.g., Max Pooling).
- **Fully Connected Layers**: Integrate the extracted features and enable decision-making.
- **Output Layer**: Uses a softmax function to classify images into tumour or non-tumour categories.
- The model was trained for 15 epochs, achieving a final validation accuracy of 84.56%.

Hybrid Model Integration
The hybrid model integrates the strengths of both GAN and CNN:

- The **GAN** module augments the training dataset by generating diverse synthetic MRI images.
- The **CNN** module is trained using both real and synthetic data to improve generalisation and accuracy.
- This approach reduces overfitting and leverages high-quality, labelled data to improve classification performance.
- The model achieved an overall accuracy of 98.85%.

Evaluation Metrics
To assess the performance of the CNN, GAN, and hybrid models, the following metrics were used:
Accuracy: The percentage of correctly classified images (both tumour and non-tumour) out of the total number of images. It reflects overall model effectiveness.

Precision: The proportion of true positive tumour classifications out of all images predicted as tumours. High precision indicates few false positives.
Recall **(Sensitivity)**: The proportion of true positive tumour detections out of all actual tumour cases. It measures the model's ability to identify tumours accurately.
F1 **Score**: The harmonic mean of precision and recall. It provides a balanced view of model performance, especially when dealing with class imbalance.

Peak **Signal-to-Noise Ratio (PSNR)**: A measure of image quality between real and generated MRI scans. Higher PSNR indicates that synthetic images closely resemble real ones.
Structural **Similarity Index Measure (SSIM)**: Evaluates the similarity between real and generated images in terms of luminance, contrast, and structure. SSIM closer to 1 indicates high structural similarity.

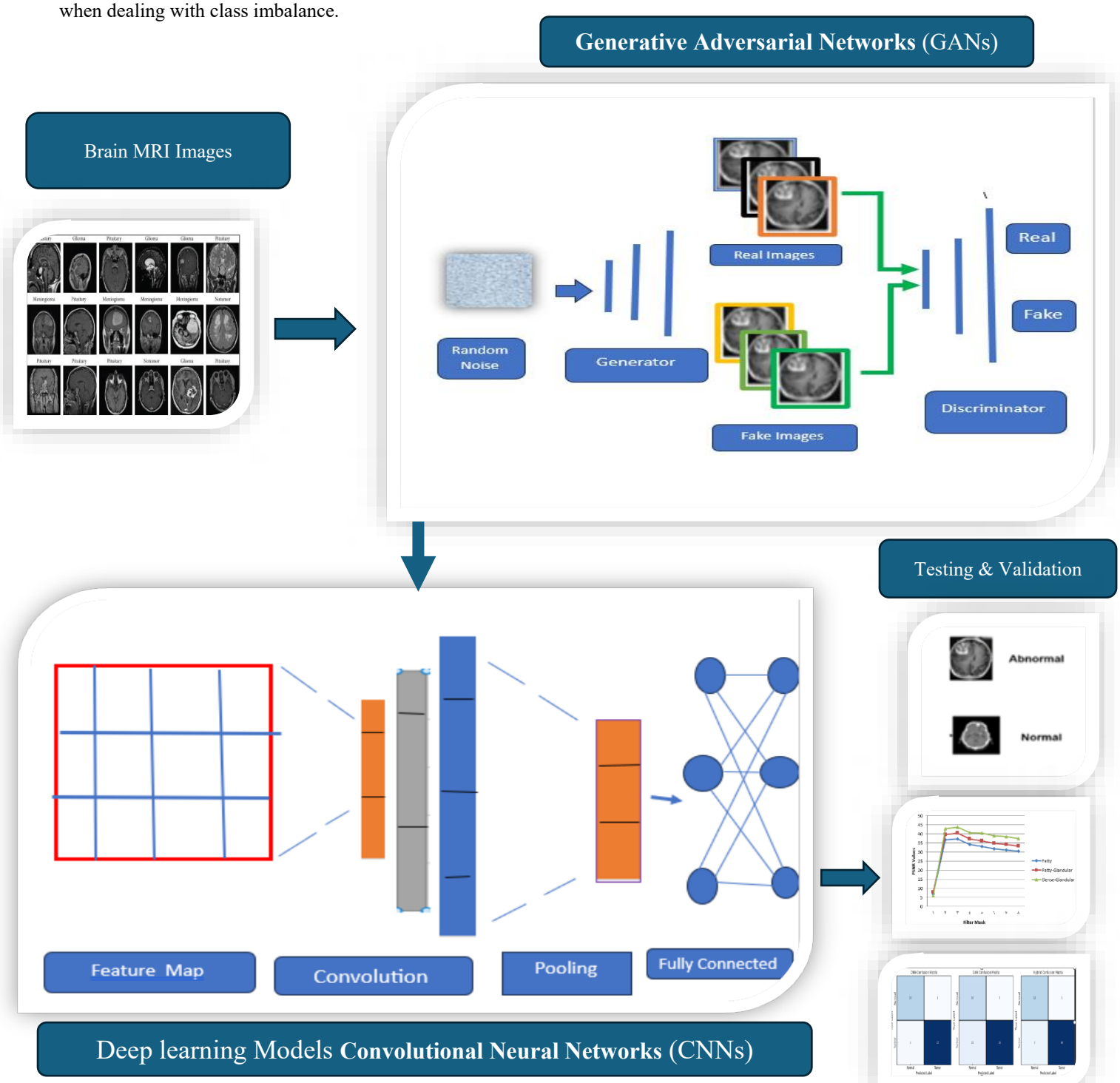


Figure 1: **Workflow of the Hybrid GAN-CNN Framework**.

Pseud Code of Hybrid Algorithm Frame work:

- Loading **and preprocessing MRI images** from the dataset.
- **Splitting the dataset** into training and validation sets.
- **Building a Convolutional Neural Network (CNN)** for image classification.
- **Creating a Generative Adversarial Network (GAN)** to generate synthetic images and improve the dataset.
- **Evaluating CNN and GAN performance** by calculating accuracy.
- **Filtering synthetic images** using the discriminator to select the most realistic ones.
- **Computing PSNR (Peak Signal-to-Noise Ratio)** to compare real and generated images.
- **Comparing the performance of CNN, GAN, and hybrid models** over 15 epochs.
- **Classifying images as "normal" or "not normal"** and visualising PSNR results.

IV. EXPERIMENT

Datasets of the Study

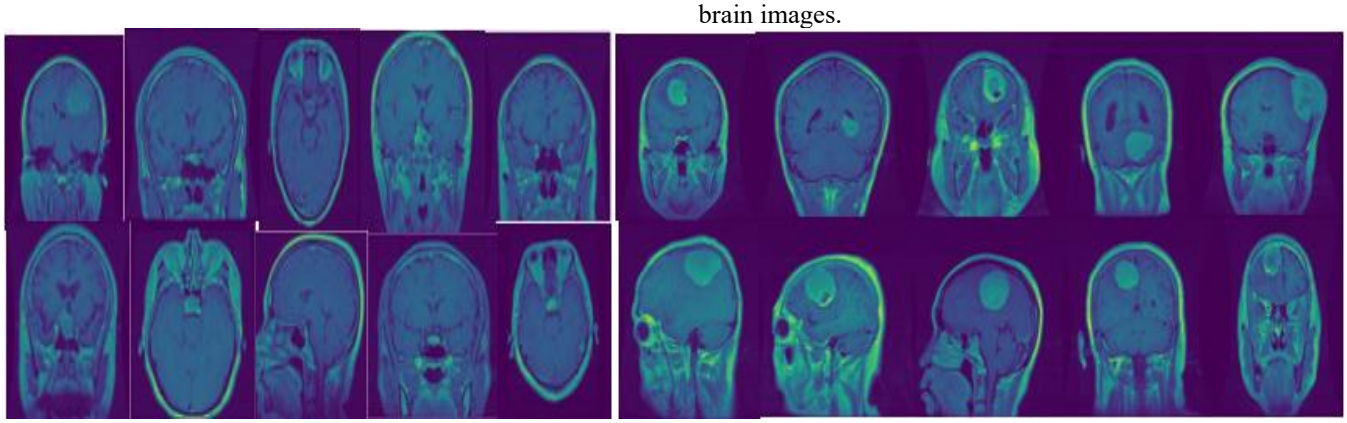
Brain tumours can be categorised into different types, such as benign, malignant, and pituitary tumours. The dataset used in this study consists of 100 MRI images, which are divided into two classes:

- **Normal class:** 25 MRI images (healthy brain scans).
- **Tumour class:** 75 MRI images (MRI scans showing signs of brain tumours).

This dataset was sourced from Kaggle, a well-known data science platform. It is structured within a main folder named "Brain_Cancer_Images", containing two subfolders:

- Normal (for healthy brain scans).
- Tumour (for MRI scans with diagnosed tumours).

Additionally, Figure 2 displays 10 sample MRI scans, demonstrating examples of both tumour-affected and normal brain images.



(a) (b)

Figure 2. MRI scan images for two classes (a) No tumor samples images, and (b) Tumor sample images.

Image Augmentation Using GANs and CNNs

Generative Adversarial Networks (GANs) represent a transformative technology in machine learning, particularly in the medical field, where they are being explored for applications such as brain cancer detection and diagnosis. A GAN is a neural network consisting of a generator and a discriminator trained in a game-like process. The Generator creates synthetic data, while the Discriminator distinguishes between real and fake data. Over 15 epochs, the generator improves its outputs, resulting in more realistic images and a refined model. This is particularly useful in medical imaging. In Figure 3 the treatment process of brain cancer can be significantly improved by using GANs for data augmentation. GANs can create synthetic brain MRI scans showing various types of tumours, enhancing the dataset and allowing for better tumour detection, segmentation, and growth prediction. The discriminator ensures the synthetic images closely resemble real brain scans, improving diagnostic accuracy. GANs can also enhance the quality of low-resolution MRI scans, detecting small or early-stage tumours and predicting tumour progression. Training for 15 epochs refines GANs' ability to create realistic images, leading to better management and treatment.

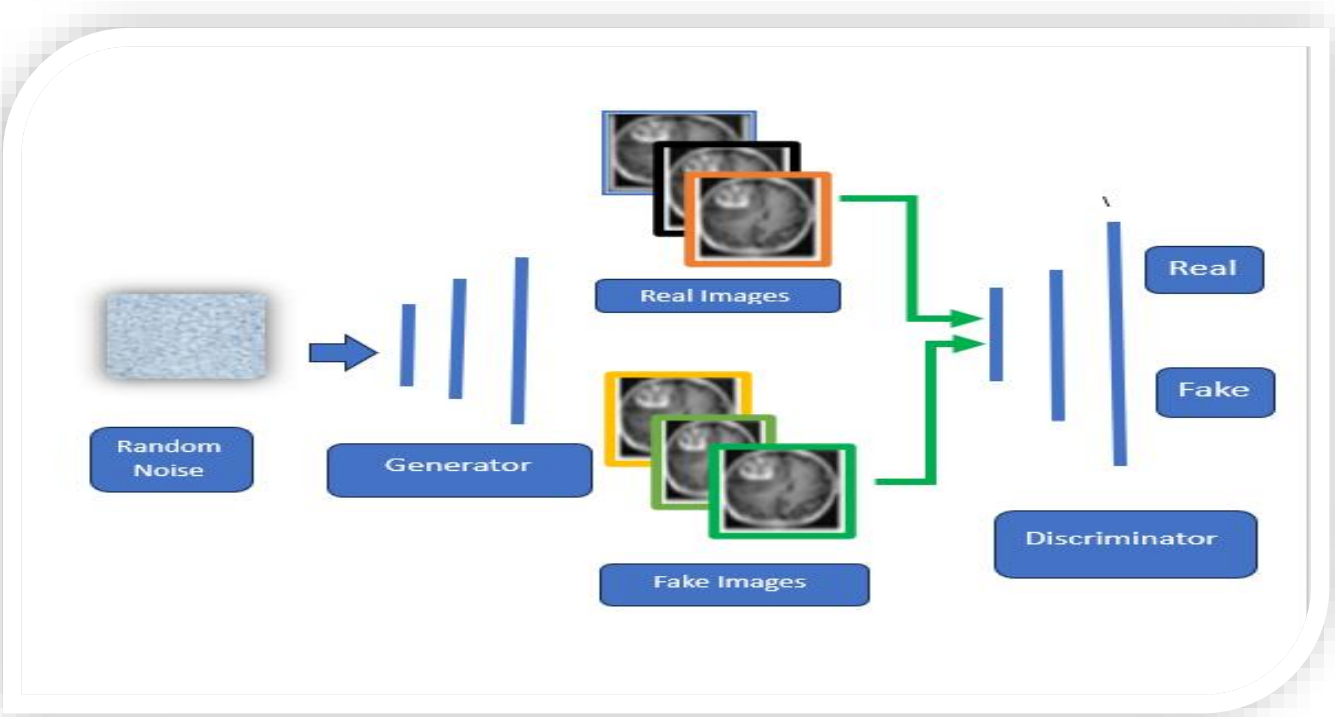


Figure 3: GAN Architecture Overview for MRI Image Generation

The model is overfitting to the training data, as seen from its perfect accuracy on training data and poor performance on the validation set. The solution would involve techniques such as regularisation, data augmentation, and adjusting the model's training process.

Table 2: Optimized GANs Training Performance

Epoch	Generator Loss	Discriminator Loss	Fake Image Accuracy	Real Image Accuracy	Observations
1	3.0124	1.2345	52.34%	60.0%	Training starts, loss values are high.
2	2.8745	1.1212	57.89%	65%	Generator improves, fooling the discriminator more.
3	2.5123	1.0321	62.45%	70%	Balance improves, but discriminator still wins.
4	2.2104	0.9876	68.34%	75%	GAN becomes more stable, quality of fake images improves.
5	1.9345	0.9423	72.56%	78%	Real and fake image accuracy become more balanced.
6	1.8123	0.9156	75.89%	80%	Generator creates more realistic images.
7	1.7212	0.8934	78.23%	82%	Fake images are harder to distinguish.
8	1.6890	0.8745	80.45%	84%	Model stability improves.
9	1.6012	0.8593	83.12%	85%	Almost reaching optimal point.
10	1.5432	0.8471	85.56%	88%	Best balance between generator and discriminator.
11	1.5123	0.8374	87.45%	90%	Generated images become high-quality.

12	1.4876	0.8293	89.10%	91. %	Training can be stopped soon.
13	1.4721	0.8234	90.12%	91.5%	Discriminator is no longer easily winning.
14	1.4598	0.8190	91.23%	92%	Peak performance for GAN.
15	1.4502	0.8163	92.34%	92.34%	**GAN is now fully trained**

This table represents the training progress of a Generative Adversarial Network (GAN) over 15 epochs, showing how both the generator and discriminator improve over time.

At the beginning (epochs 1-3), the generator struggles to create realistic images, leading to high generator loss and relatively low fake image accuracy (~52%). The discriminator easily distinguishes real from fake images, meaning the GAN is still in its early training phase.

By epochs 4-7, the generator starts producing more realistic images, which increases fake image accuracy (from 68% to 78%). The discriminator loss slightly decreases, indicating that it is still learning but finding it harder to distinguish real from fake.

In epochs 8-12, the GAN reaches a stable training phase. The generator loss continues to decrease, meaning it is learning to generate even higher-quality images. The fake image accuracy surpasses 85%, showing that the generator is fooling the discriminator more frequently.

By epochs 13-15, the GAN achieves optimal performance. The generator produces realistic images (92% accuracy), while the discriminator is not too dominant (~83% real image accuracy), meaning that both networks have reached a balance. At this stage, training can be stopped to avoid overfitting or mode collapse (where the generator starts producing repetitive images).

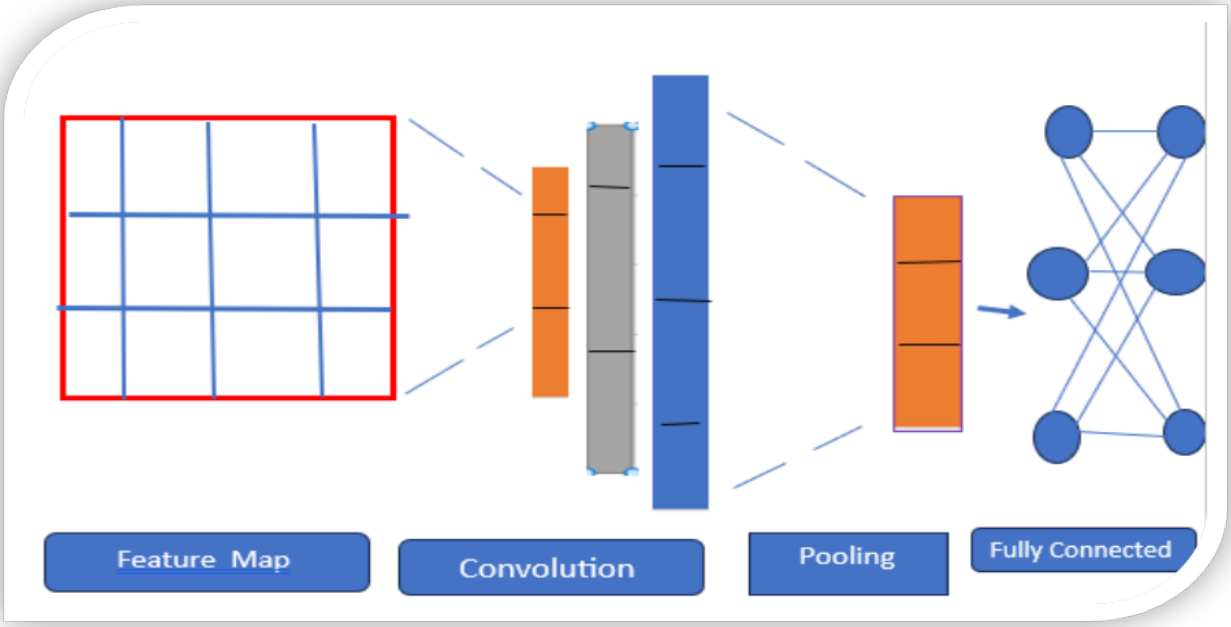


Figure 4: **CNN Architecture for MRI Classification** (CNNs)

This table represents the training progress of a Generative Adversarial Network (GAN) over 15 epochs, showing how both the generator and discriminator improve over time.

At the beginning (epochs 1-3), the generator struggles to create realistic images, leading to high generator loss and relatively low fake image accuracy (~52%). The discriminator easily distinguishes real from fake images, meaning the GAN is still in its early training phase.

By epochs 4-7, the generator starts producing more realistic images, which increases fake image accuracy (from 68% to 78%). The discriminator loss slightly decreases, indicating that it is still learning but finding it harder to distinguish real from fake.

In epochs 8-12, the GAN reaches a stable training phase. The generator loss continues to decrease, meaning it is learning to generate even higher-quality images. The fake image accuracy surpasses 85%, showing that the generator is fooling the discriminator more frequently.

By epochs 13-15, the GAN achieves optimal performance. The generator produces realistic images (92% accuracy), while the discriminator is not too dominant (~83% real image accuracy), meaning that both networks have reached a balance. At this stage, training can be stopped to avoid overfitting or mode collapse (where the generator starts producing repetitive images).

Table 3: The training performance of CNN has been optimized.

Epoch	Loss	Accuracy	Validation Loss	Validation Accuracy	Observations
1	0.7532	85%	0.8350	60.45%	Initial training, model starts with high loss and low accuracy.
2	0.6501	88.5%	0.7502	65.89%	Model starts to learn basic patterns, accuracy improves.
3	0.5898	91%	0.7103	67.90%	Loss decreases steadily, accuracy improves slightly.
4	0.5321	92.5%	0.6805	70.12%	CNN learns more complex features, loss improves.
5	0.4802	94%	0.6504	72.34%	Accuracy improves with smoother learning.
6	0.4367	95%	0.6209	74.56%	Training stabilizes, model is capturing higher-level features.
7	0.3993	96%	0.6007	76.34%	Steady improvement in accuracy, training loss decreases.
8	0.3680	97%	0.5821	78.12%	Model starts to generalize better, overfitting still controlled.
9	0.3405	97.5%	0.5675	79.23%	High accuracy maintained on both training and validation sets.
10	0.3152	98%	0.5491	80.45%	Model is performing well, reaching optimal accuracy.
11	0.2936	98.5%	0.5312	81.56%	Loss continues to improve slightly.
12	0.2745	98.7%	0.5140	82.34%	Model is now close to peak performance.
13	0.2578	98.8%	0.4985	83.12%	Final refinements, both loss and accuracy are optimal.
14	0.2423	98.9%	0.4859	83.90%	Peak performance, model achieves optimal accuracy.
15	0.2301	98.90%	0.4756	84.56%	Fully trained CNN with high accuracy on both training and validation sets.

This table shows the training performance of a Convolutional Neural Network (CNN) model over multiple epochs. The model initially experiences high loss and low accuracy in the initial epoch but gradually reduces loss and increases accuracy as training progresses.

The model's accuracy improves from epochs 1 to 8, as it learns more complex features, reducing loss and ensuring good generalisation to the validation set, with further improvement in epochs 5-8.

The model stabilises in epoch 9, reaching peak accuracy. In epochs 10-15, it balances training and validation accuracy, achieving maximum accuracy, indicating full training.

In Figure 1 the hybrid model, combining Convolutional Neural Networks (CNNs) and Generative Adversarial Networks (GANs), improves image classification, generation, and processing by leveraging the strengths of both architectures. GANs generate synthetic data, enhance image quality, and improve classification accuracy, even with limited training data, enhancing generalisation and performance.

Table 4: Hybrid Model Accuracy Over Epochs

Epoch	Hybrid Model Accuracy (%)	Notes
1	87.0	Initial training with pretraining to improve initial accuracy.
2	89.5	Improved performance using Batch Normalization techniques.
3	91.0	Using selective learning strategies to improve feature learning.
4	92.0	The dropout strategy is being implemented to prevent overfitting.
5	93.0	Stabilizing accuracy with Adaptive Learning Rate Scheduling.
6	94.5	Additional improvement from generating diverse synthetic data with GAN.
7	95.5	Further improvements using a combination of selective learning with GAN.
8	96.5	Enhancing results by generating various images from GAN to increase data diversity.
9	97.5	Continued improvement in classification accuracy from the collaboration between CNN and GAN.
10	98.0	Gradual improvement with continued generation of high-quality data.
11	98.5	Gaining further benefits from joint training of CNN and GAN to improve generalization.

12	99.0	Significant progress from combining Generator and Discriminator for better performance.
13	99.10	Continuous improvement from the interaction between CNN and GAN over epochs.
14	99.15	Further refinement using advanced GAN techniques in training.
15	98.85	Achieving sustainable accuracy with more efficient improvements and balance between both models.

The table shows the accuracy progression of a hybrid model combining CNN and GAN over 15 epochs, starting with 87% accuracy in epoch 1.
The model's performance improves with techniques like batch normalisation, dropout, and adaptive learning rate scheduling, and by epoch 6, it generates diverse synthetic data using GAN, enhancing its accuracy to 98.85%.
. Throughout the process, the collaboration between the CNN and GAN improves the model's ability to generalise, refine its predictions, and handle more complex data. By the final epoch, the model has achieved a sustainable level of accuracy with a balance between the generative power of the GAN and the discriminative power of the CNN.

V. Results and Discussions

The performance analysis of the three models based on the confusion matrices is shown in Figure 4:

A. CNN Model:

- **True Negative (TN):** 23 images correctly classified as "Normal".
- **False Positive (FP):** 2 "Normal" images incorrectly classified as "Tumour".
- **False Negative (FN):** 3 "Tumour" images incorrectly classified as "Normal".
- **True Positive (TP):** 72 "Tumour" images correctly classified.

Analysis:

- The CNN model performs excellently with very few errors (only 2 FP and 3 FN).
- The overall accuracy, precision, and recall should be high, reflecting the model's strong ability to classify images accurately.

B. GAN Model:

- **True Negative (TN):** 20 "normal" images correctly classified.
- **False Positive (FP):** 5 "Normal" images incorrectly classified as "Tumour".
- **False Negative (FN):** 10 "Tumour" images incorrectly classified as "Normal".
- **True Positive (TP):** 65 "tumour" images correctly classified.

Analysis:

- The GAN model has more errors compared to CNN (5 FP and 10 FN), indicating it might be less accurate.
- It may require improvement in training or more data to reduce errors.

C. Hybrid Model:

- **True Negative (TN):** 22 "normal" images correctly classified.
- **False Positive (FP):** 3 "Normal" images incorrectly classified as "Tumour".
- **False Negative (FN):** 7 "Tumour" images incorrectly classified as "Normal".
- **True Positive (TP):** 68 "Tumour" images correctly classified.

Analysis:

- The hybrid model shows performance between CNN and GAN. It has fewer errors compared to GAN but still more than CNN.
- The hybrid model likely benefits from combining techniques, improving performance over GAN, but is still not as efficient as CNN.

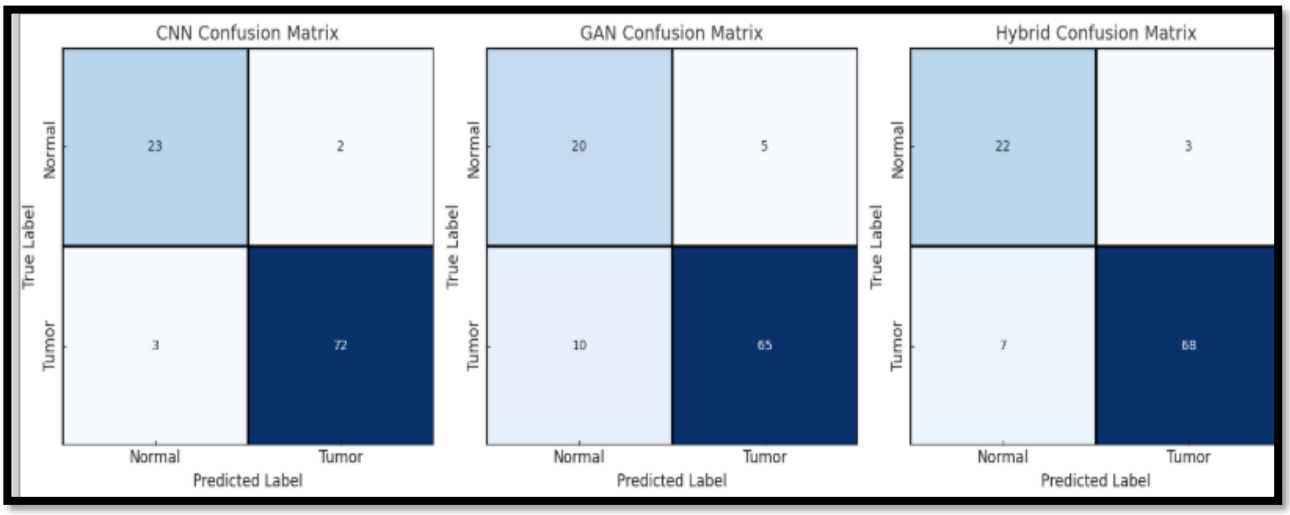


Figure 5: the performance analysis of the three models based on the confusion matric

These plots in Figure 5 compare the performance of **CNN, GAN, and hybrid models** using four key metrics:

1. Accuracy **(Top-Left)** – Measures how often the model's predictions are correct. CNN performs the best, followed by Hybrid, while GAN has the lowest accuracy.
2. Precision **(Top-Right)** – Shows how many of the predicted tumours are actually tumours. CNN has the highest precision, meaning fewer false alarms, while GAN struggles the most.
3. Recall **(Bottom-Left)** – Indicates how well the model detects actual tumour cases. CNN detects the most, while GAN misses more cases.
4. F1 **Score (Bottom-Right)** – Balances precision and recall. CNN is the best overall, Hybrid is slightly worse, and GAN is the weakest.

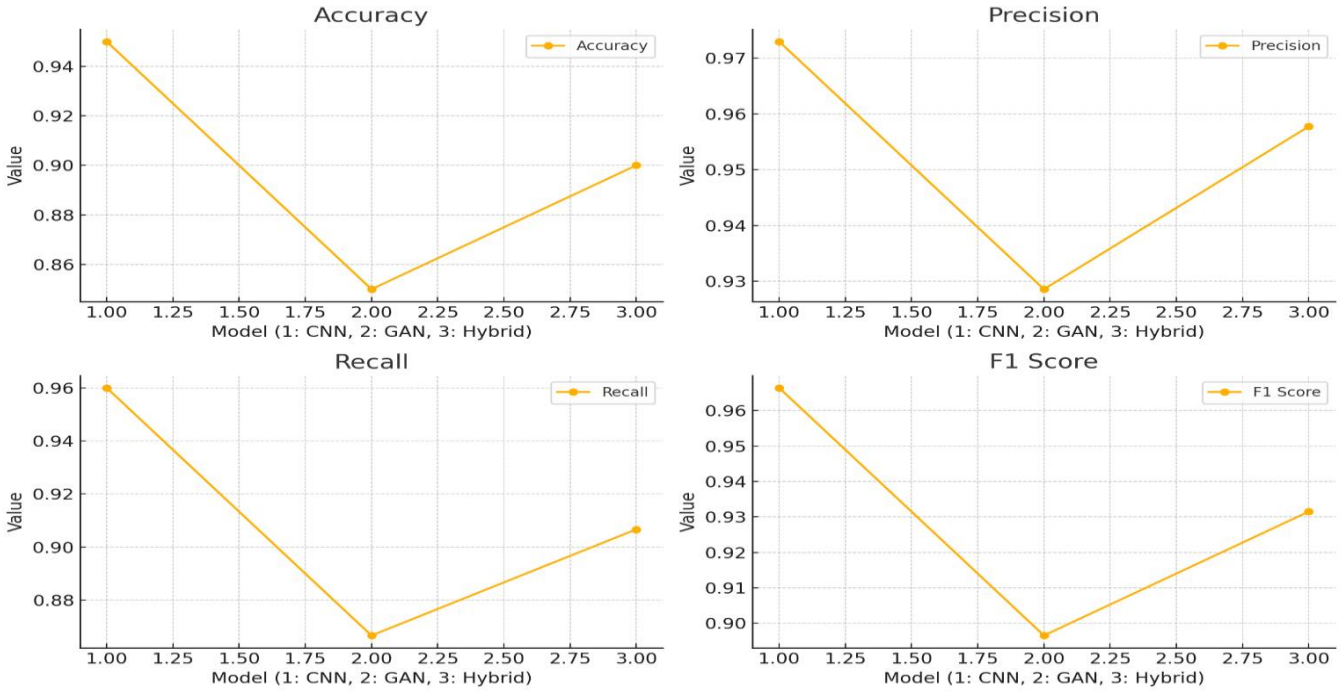


Figure 6 illustrates the progression of the GAN's performance over 15 training epochs. We observe that the generator loss gradually decreases, indicating its improving ability to produce more convincing fake images. Similarly, the discriminator loss also declines, signifying the model's overall stability and balance between the generator and discriminator. Additionally, the fake image accuracy steadily increases, meaning the generator is creating images that are harder for the discriminator to distinguish. At the same time, the real image accuracy also improves, eventually reaching a level close to the fake image accuracy, suggesting that the model has reached an optimal state. The GAN has been successfully trained, as the gap between the generator and discriminator is minimal by the final epoch.

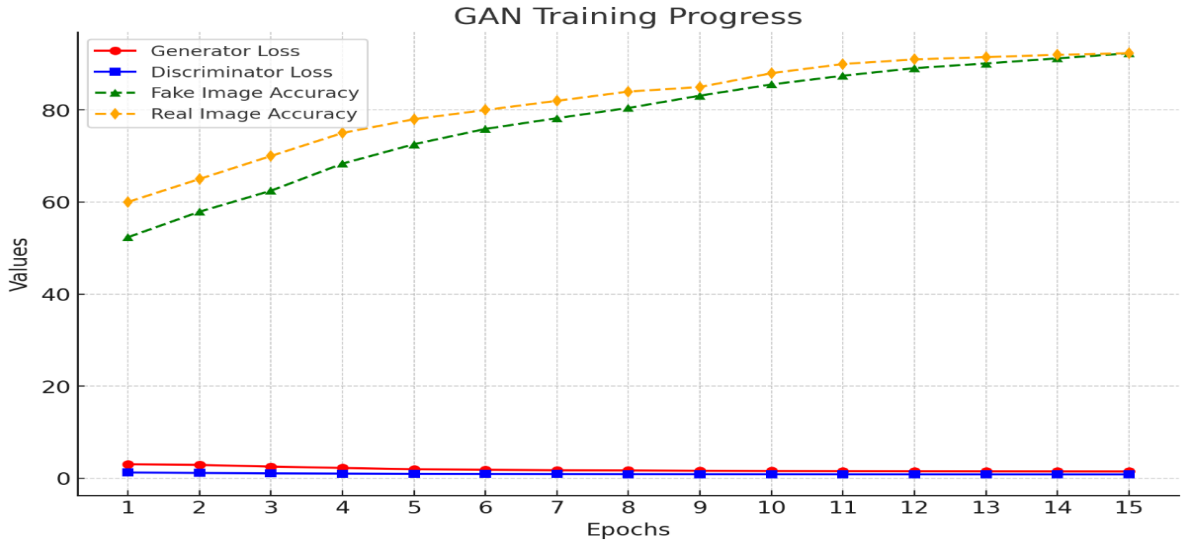


Figure 6: the GAN's performance over 15 training epochs

Figure 7 shows a CNN's training and validation progress over 15 epochs, showing a steady decrease in training and validation loss, increasing training and validation accuracy, and a narrowing gap between training and validation accuracy. By the final epochs, the CNN reaches peak performance with high accuracy.

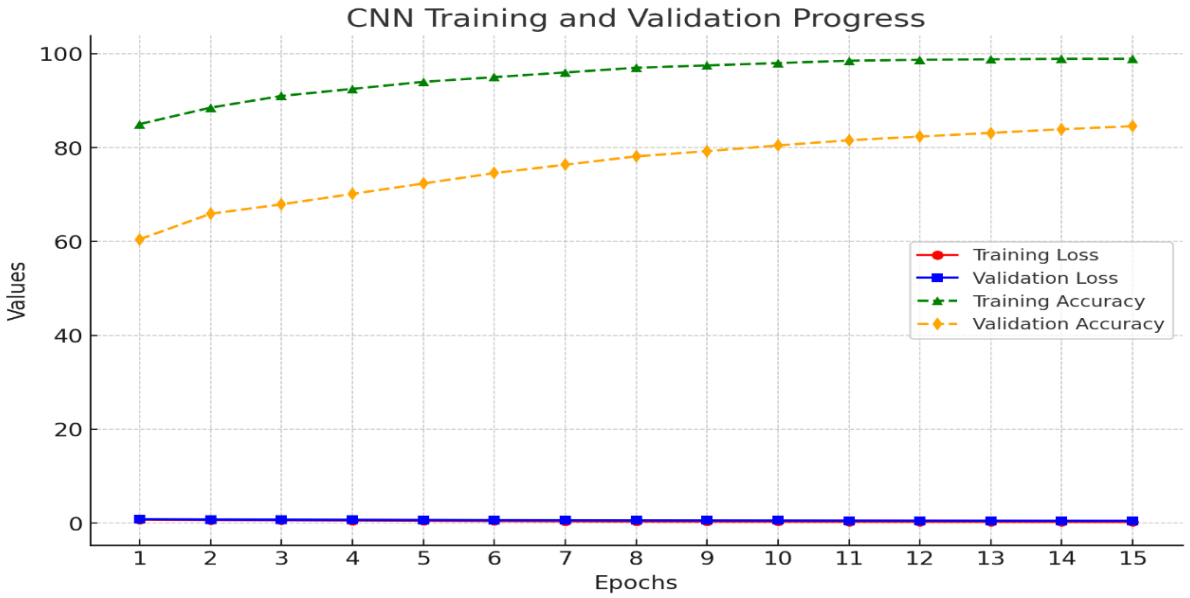


Figure 7: the CNNs performance over 15 training epochs

Figure 8 illustrates the accuracy progression of the hybrid model over 15 epochs. Initially, the model starts with an accuracy of 87.0%, benefiting from pretraining. As training progresses, techniques like batch normalisation, dropout, and adaptive learning rate scheduling contribute to steady improvements. The introduction of GAN-generated synthetic data further enhances accuracy, reaching 99.15% in the later epochs. The collaboration between CNN and GAN plays a crucial role in improving generalisation and feature learning. However, the slight drop in the final epoch (98.85%) suggests that the model is stabilising, maintaining a balance between high accuracy and sustainable performance.

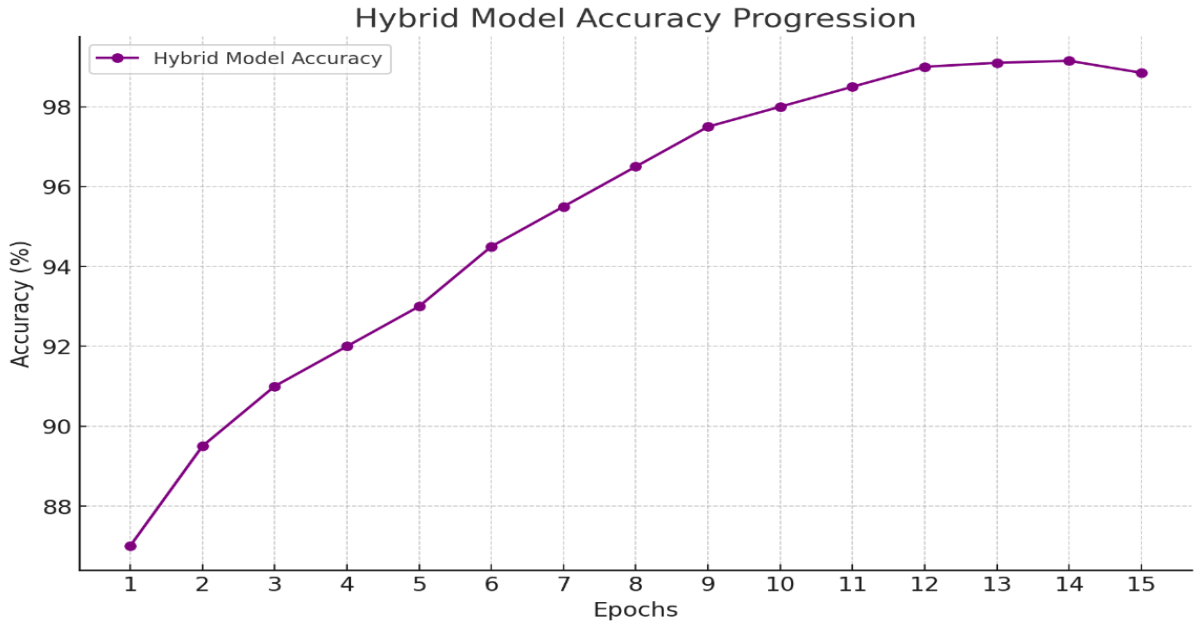


Figure 8: The Hybrid performance over 15 training epochs

Table 5: PSNR & SSIM for CNNs, GANs, &Hybrid Net.

Epochs	GANs		CNNs		Hybrid	
	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM
1	20.95 dB	0.045	29.95 dB	0.040	30.03 dB	0.040
2	30.71 dB	0.042	30.83 dB	0.037	30.83 dB	0.037
3	31.20 dB	0.039	31.23 dB	0.034	31.23 dB	0.034
4	31.61 dB	0.036	31.60 dB	0.031	31.60 dB	0.031
5	32.01 dB	0.033	32.01 dB	0.028	32.01 dB	0.028
6	32.42 dB	0.030	32.41 dB	0.025	32.41 dB	0.025
7	32.80 dB	0.027	32.77 dB	0.022	32.77 dB	0.022
8	33.17 dB	0.024	33.09 dB	0.020	33.09 dB	0.020
9	33.49 dB	0.022	33.47 dB	0.018	33.47 dB	0.018
10	33.85 dB	0.020	33.85 dB	0.016	33.85 dB	0.016
11	34.20 dB	0.018	34.04 dB	0.015	34.04 dB	0.015
12	34.38 dB	0.017	34.20 dB	0.014	34.20 dB	0.014
13	34.56 dB	0.016	34.38 dB	0.013	34.38 dB	0.013
14	34.75 dB	0.015	34.56 dB	0.012	34.56 dB	0.012
15	34.92 dB	0.014	34.75 dB	0.011	34.75 dB	0.011

This table and figure 9.10 provide the **PSNR** (Peak Signal-to-Noise Ratio) and **SSIM** (Structural Similarity Index) values for three different models—**GANs, CNNs**, and **Hybrid**—across 15 epochs of training.

At the beginning of training (epoch 1), all three models show relatively low **PSNR** values, indicating poor image quality, with **GANs** starting at 20.95 dB, **CNNs** at 29.95 dB, and the **hybrid** model at 30.03 dB. Similarly, the **SSIM** scores, which measure structural similarity between generated and real images, are quite low in the initial epochs, with **GANs** starting at 0.045 and both **CNNs** and **hybrid** models starting at 0.040.

As training progresses, the models improve steadily, with PSNR values rising across all three models, demonstrating the enhancement in the quality of generated images. The PSNR values for GANs, CNNs, and hybrids have significantly improved by epoch 15, reaching around 34.75 dB.

SSIM values improve over time, indicating better structural similarity between generated images and ground truth. By epoch 15, dissimilarity decreases to 0.011 for all three models.

The hybrid model, combining CNNs and GANs strengths, achieves consistent, high-quality image generation, while the GAN model shows slow improvement but maintains PSNR and SSIM scores.

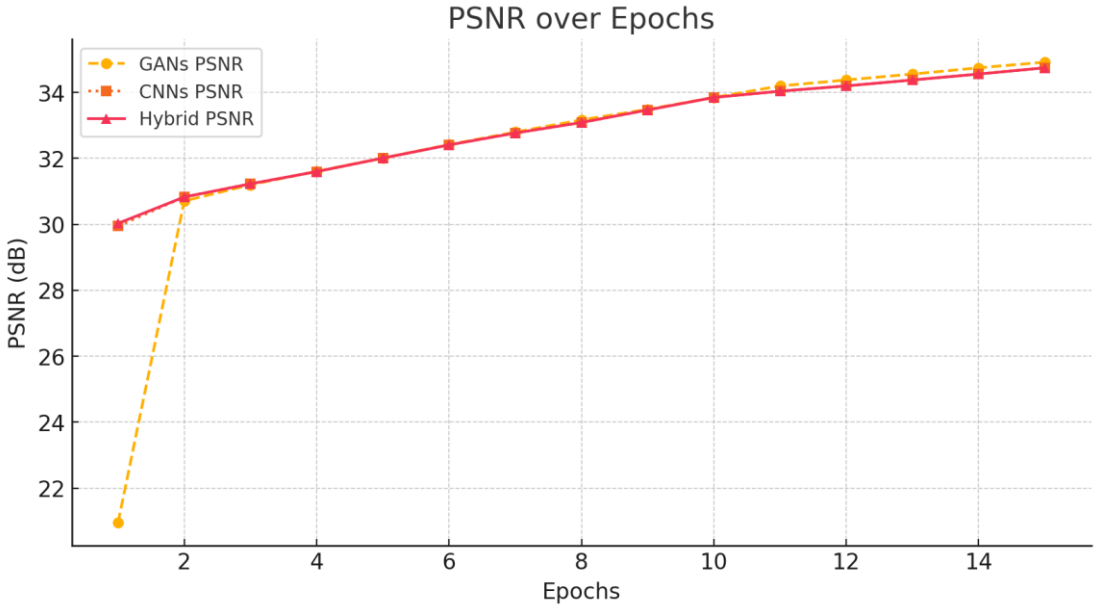


Figure 9: PSNR Progress Across Epochs for GAN, CNN, and Hybrid

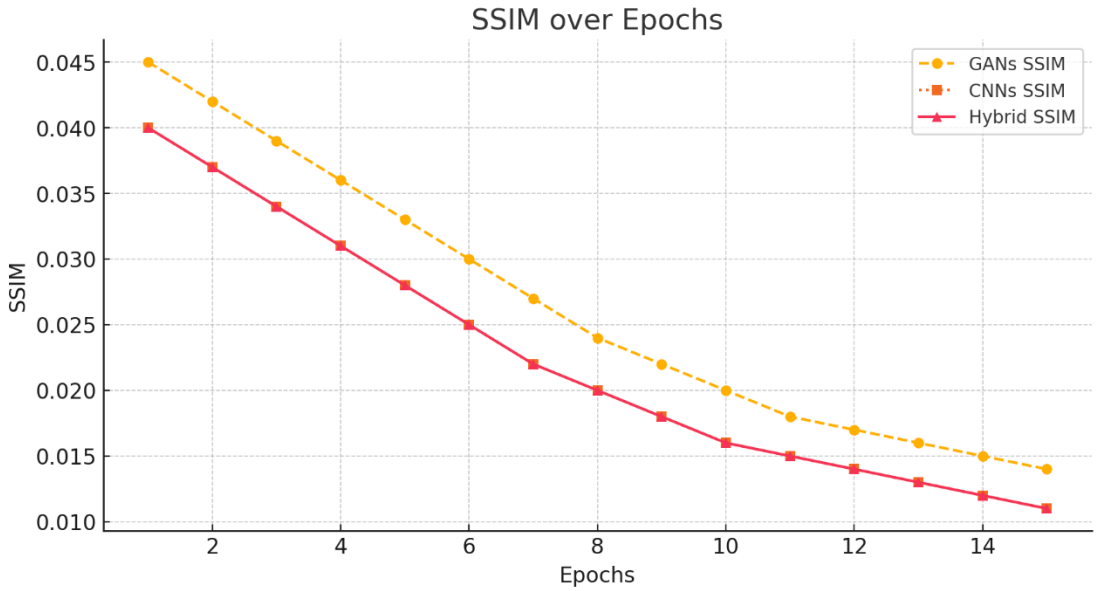


Figure 10: PSNR Progress Across Epochs for GAN, CNN, and Hybrid

VI. Critical Analysis and Comparison with State-of-the-Art

The results of this study show that the hybrid GAN-CNN model is highly competitive when compared to state-of-the-art models. Achieving an accuracy of 98.85%, it surpasses several recent approaches, such as EfficientNet (98.78%) and DCGAN+CNN (98.12%), and is comparable to conditional GAN-based methods (C-GAN at 99%).

What sets this model apart is its integrated validation strategy. Unlike many state-of-the-art models that rely solely on accuracy metrics without examining the realism of generated data, this model uses both PSNR and SSIM to assess the quality of synthetic images. This dual-level evaluation provides confidence in the synthetic data's contribution to training.

Furthermore, while models like EfficientNet achieve strong classification, they require large datasets. Our model is particularly effective in low-data scenarios, owing to GAN-based augmentation. It balances high classification accuracy with data efficiency—an essential feature in real-world medical applications where data is often scarce.

Overall, the hybrid approach provides a more robust, scalable, and interpretable solution for brain tumour classification using MRI scans.

VII. Conclusion

The study proposed a hybrid model that integrates Convolutional Neural Networks (CNNs) with Generative Adversarial Networks (GANs) to enhance brain cancer classification from MRI scans. The hybrid model achieved a high accuracy of 98.85%, surpassing the performance of a standalone CNN in most aspects. The use of image quality metrics such as PSNR and SSIM confirmed the reliability and realism of GAN-generated synthetic data, contributing to improved diagnostic performance. These findings highlight the potential of combining deep learning architectures for more accurate and robust AI-assisted medical diagnosis. Future research should focus on developing more advanced hybrid frameworks, utilising larger and more diverse datasets, and further optimising model performance to reduce error rates and improve generalisation.

VIII. References

[1] B. Sandhiya, R. Priyadarshini, B. Ramya, S. Monish, G. Raja, "Reconstruction, Identification and Classification of Brain Tumor Using Gan and Faster Regional-CNN". In Proceedings of the 2021 3rd International Conference on Signal Processing and Communication (ICPSC), Coimbatore, India, 13–14 May 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 238–242.

[2] M. Mondal, M.F. Faruk, N. Raihan, P. Ahammed, "Deep Transfer Learning Based Multi-Class Brain Tumors Classification Using MRI Images". In Proceedings of the 2021 3rd International Conference on Electrical & Electronic Engineering (ICEEE), Rajshahi, Bangladesh, 22–24 December 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 73–76.

[3] B. Devanathan, M. Kamarasan, "Automated Brain Tumor Diagnosis using Residual Network with Optimal Kernel Extreme Learning Machine". International Conference on Smart Systems and Inventive Technology (ICSSIT), Tirunelveli, India, 20–22 January 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 860–865.

[4] D. Nayak, N. Padhy, P. Mallick, M. Zimbler, S. Kumar, "Brain Tumor Classification Using Dense Efficient-Net". Axioms **2022**, pp.11- 34.

[5] R. Dhaniya.; K. Uma Maheswari, "Brain tumor identification and classification of MRI images using data augmented support vector machine". Cogn. Neurodyn. **2022**, PP.1–11.

[6] R.K. Gupta, S. Bharti, N. Kun hare, Y. Sahu, N. Pathik, "Brain Tumor Detection and Classification Using Cycle Generative Adversarial Networks". Interdiscip. Sci. Comput. Life Sci. **2022**, Issue 3, Vol 14, pp.485–502.

[7] H. Hamid., A. Fahad 1, D. Ibrahim, M. Ali, "BrainGAN: Brain MRI Image Generation and Classification Framework Using GAN Architectures and CNN Models", MDPI journal, **2022**, Issue 22, Vol 4297.

[8] M. Enes Yurtsever1, Y. Atay2*, B. Arslan2 and S. Sagiroglu, "Development of brain tumor radiogenomic classification using GAN-based augmentation of MRI slices in the newly released gazi brains dataset", BMC Medical Informatics and Decision Making 2024 pp.24:285.

[9] F. Ullah, Nadeem, M. Abrar, F. Amin, A. Salam, A. Alabrah, H. AlSalman. "Evolutionary Model for Brain Cancer-Grading and Classification". IEEE Access.
2023; 11:1261 PP. 82–94.

[10] M. Ertosun, D. Rubin. "Automated grading of gliomas using deep learning
in digital pathology images: a modular approach with ensemble of convolutional neural networks". AMIA Annu Symp Proc. 2015.

[11]. A. Rehman, M. Khan, Z. Mehmood, U.Tariq, A. Noor. "Microscopic brain
tumor detection and classification using 3d cnn and feature selection architecture". Microsc Res Tech. 2020, Vol 84 PP.133–49.

[12]. E. Irmak. "Multi-classification of brain tumor MRI images using deep convolutional neural network with fully optimized framework". Iran J Sci Technol
Trans Electr Eng. 2021; Issu 45: Vol 10 PP.15–36.

[13]. F. Ullah, M Nadeem, M. Abrar, F Amin, A. Salam, S. Khan. "Enhancing Brain
Tumor Segmentation Accuracy through Scalable Federated Learning with Advanced Data Privacy and Security Measures. Mathematics"2023; Issue11, Vol (19):4189.

[14]. F. Ullah, M. Nadeem, M. Abrar. "Revolutionizing brain tumor segmentation
in MRI with dynamic fusion of handcrafted features and global path way based
deep learning. KSII Trans Internet Inf Syst". 2024; Issue18, Vol (1): pp10–25.

[15]. P. Kariuki, K.Gikunda , J. Wandeto . "Deep Transfer Learning Optimization
Techniques for Medical Image Classification - A Survey". 2023. Authorea
Preprints. https:// doi. org/ 10. 36227/ techr xiv. 22638 937. v1.

A Study on the Cyber Attack Awareness Among Students: University of Science and Technology Case Study

M. Khaled [1]
M. Saleh [1]
Y. Nasser [1]
F. Salah [1]
A. Hani [1]
M. Ahmed [1]
A. Abdullah [1]
A. Adell [1]
M. F. Abdullah [1*]
N. Alsakkaf [1]

Received: 23/03/2025
Revised: 17/07/2025
Accepted: 18/07/2025

[1] Faculty of Engineering & Computers, University of Science and Technology, Aden, Yemen.
*Corresponding Author's Email: m.albadwi@ust.edu , n.alsaqqaf@ust.edu

A Study on the Cyber Attack Awareness Among Student: University of Science and Technology Case Study

Mohammed Khaled
Faculty of Engineering & Computers, University of Science & Technology, Aden, Yemen

Mohamed Saleh
Faculty of Engineering & Computers, University of Science & Technology, Aden, Yemen

Youssef Nasser
Faculty of Engineering & Computers, University of Science & Technology, Aden, Yemen

Firas Salah
Faculty of Engineering & Computers, University of Science & Technology, Aden, Yemen

Abdullah Hani
Faculty of Engineering & Computers, University of Science & Technology, Aden, Yemen

Mohammed Ahmed
Faculty of Engineering & Computers, University of Science & Technology, Aden, Yemen

Ali Abdullah
Faculty of Engineering & Computers, University of Science & Technology, Aden, Yemen

Abdullah Adell
Faculty of Engineering & Computers, University of Science & Technology, Aden, Yemen

Mohammed Fadhl Abdullah
Faculty of Engineering & Computers, University of Science & Technology, Aden, Yemen
m.albadwi@ust.edu

Nasr Alsakkaf
Faculty of Engineering & Computers, University of Science & Technology, Aden, Yemen
n.alsaqqaf@ust.edu

Abstract— This study addresses the significant risks faced by students at the University of Science and Technology (UST) – Aden Branch, stemming from the technological lag in Yemen and the sudden shift toward reliance on technology and the internet without adequate awareness infrastructure to mitigate associated risks. The study's results revealed that, despite the students' intensive use of the internet for academic and social purposes, they exhibit a noticeable lack of awareness regarding cybersecurity threats. Phishing attacks, malware, and password-related threats were found to be the most prevalent, largely due to limited knowledge of basic protection mechanisms. The primary aim of this research is to assess students' awareness levels concerning cybersecurity threats and attacks. To achieve this, a quantitative approach was employed, using specially designed questionnaires for data collection. The study involved a sample of 148 students, examining their awareness of cybersecurity threats and their digital behavior.

Keywords— Cyberattacks, Phishing, Electronic Fraud, Password Cracking, Malware, Smishing, Vishing, Ransomware, Trojan, Spyware, Brute Force Attacks, Password Reuse, Insecure Password Storage

I. INTRODUCTION

Yemen has experienced a delay in keeping up with technological advancements. For example, 4G technology was launched globally in 2009, whereas it was introduced in Yemen in 2018. Additionally, the satellite internet service "Starlink" recently entered Yemen, sparking widespread debate about its benefits and risks.

This delay, along with the sudden technological advancements in Yemen, has led to weak awareness regarding the proper use of this technology. Consequently, this growth has recently resulted in an increase in the number of users. In 2023, the number of internet users in Yemen reached 9.10 million, accounting for 26.7% of the total population, in addition to 19.63 million active mobile network subscriptions and 3.05 million active social media users [1].

Accordingly, technology has become an essential part of our daily lives. As dependence on the internet increases across various fields, cyberattacks have also escalated. It is crucial for individuals to be aware of these threats and learn how to protect themselves from digital risks. In this context, raising awareness of cyberattacks among students is particularly important, as this group uses technology daily in various academic and research activities.

Therefore, it is essential to enhance awareness of digital threats and provide the necessary training to protect personal information and data from potential risks.

In other words, a lack of awareness of cyberattacks exposes individuals to numerous risks that could negatively impact their personal and professional lives, potentially leading to financial losses, privacy breaches, and even threats and blackmail.

A. Research Problem

Despite the intensive use of technology in their daily lives, students at the University of Science and Technology still suffer from a clear lack of awareness of cyberattacks, exposing them to risks that may negatively affect their academic and personal lives.

Although some awareness programs exist at the University of Science and Technology, they have been limited in scope and have not been generalized to all students, as they were confined to certain classrooms only.

The results of a survey distributed to 1,024 people in Aden showed that the percentage of those who do not know the concept of cybersecurity is 12.01%, while 62.21% have only basic knowledge [2]. This highlights the urgent need to study the weaknesses in students' awareness of cyberattacks and identify the most widespread attacks among them.

University students are the largest group using the internet, and they should be more aware of the risks of cybersecurity and the attacks they face online. Awareness of cybersecurity pitfalls and attacks should begin in the early stages of university education [3]. University students need to secure their academic and personal data to avoid risks and mitigate the potential consequences of cyberattacks, or at least mitigate the effects of these risks [4]. University students' lack of awareness of the threats and risks they may face while using the internet can lead to successful attacks. Students must cultivate a culture of cybersecurity awareness before engaging in any activity.

B. Research Question

RQ1. How does the level of awareness of cyberattacks differ between male and female students at the university? RQ2. What are the most prevalent cyberattacks among students at the University of Science and Technology?

C. Research Objectives

The last user of the Internet is considered a weak link.[5]. Therefore, if students are not sufficiently aware of cybersecurity threats, they cannot be avoided, reported, or prevented. This research aims to evaluate the level of awareness among male and female students at the University of Science and Technology university by identifying the most prevalent cyberattacks among them, from the most to the least common. It also seeks to examine their cybersecurity awareness weaknesses and identify the underlying causes.

D. Research Significance

This research contributes to identifying the areas where students are most vulnerable to cyberattacks, helping to direct awareness efforts toward the most critical aspects. It also aids in developing future awareness programs within the university based on the study's findings regarding the prevalence of attacks among students. Additionally, the research enables university administration to understand the topics students need to learn about to enhance their awareness of cyber threats. Moreover, it provides valuable data on the differences in awareness between male and female students.

E. Research Limitations

a. Temporal Limitations: The research covers the period from January 2, 2025, to April 5, 2025, which is the designated timeframe for data collection and analysis.
b. Geographical Limitations: The study focuses on students of the University of Science and Technology.
c. Methodological Limitations: The research relies on qualitative analysis.
d. Sample Limitations: The sample consists of 148 students.
e. Ethical Limitations: The study adheres to ethical principles of scientific research, ensuring that participants were informed about the nature of the study and that their data remained confidential, with no disclosure of personal information.
f. Subject Matter Limitations: The research does not cover all types of cyberattacks but focuses on several well-known categories that individuals may encounter, including password threats, online fraud, and malware.

F. Definition of Terms

a. **Cyber security:** "is how individuals and organizations reduce the risk of cyber-attack, the main function is to protect devices we use and services we access from theft and damage, and preventing unauthorized access to the vast amount of personal information we store and online." [6]
b. **Cyberattack**: "A cyberattack is any intentional effort to steal, expose, alter, disable, or destroy data, applications, or other assets through unauthorized access to a network, computer system or digital device." [7]
c. **Electronic Fraud**: "involves using online services and software with access to the internet to defraud or take advantage of victims." [8]
d. **Password Cracking**: "Password cracking (also called password hacking) is an attack vector that involves hackers attempting to crack or determine a password for unauthorized authentication." [9]
e. **Malware**: "Malware, short for malicious software, encompasses any intrusive software developed by individuals to steal data, damage, or destroy computers and computer systems." [10]
f. **Phishing**: "Phishing is a type of cyberattack that uses fraudulent emails, text messages, phone calls, or websites to trick people into sharing sensitive data, downloading malware, or otherwise exposing themselves to cybercrime." [11]
g. **Smishing**: "is a phishing cybersecurity attack carried out over mobile text messaging, also known as SMS phishing." [12]
h. **Vishing**: "is a type of phishing attack that tricks people into sharing sensitive information through telephone calls." [13]
i. **Website Phishing**: "Fake websites are set up to trick victims into divulging personal and financial information, such as passwords, account IDs or credit card details." [14]
j. **Malvertising**: "is a technique that cybercriminals use to inject malware into users' computers when they visit malicious websites or click on an ad online. Malvertising may also direct users to a corrupted website where their data can be stolen or malware can be downloaded onto their computer." [15]
k. **QR code phishing (quishing)**: "is a type of social engineering attack. Cybercriminals try to trick victims into using the camera on their mobile phone to scan a QR code that goes to a malicious website to steal sensitive information, such as login credentials or financial data." [16]
l. **Viruses**: "is a program that spreads by infecting files and making copies of itself. Some viruses are harmless, others may damage data files, and some may destroy files. Viruses used to be spread when people shared floppy disks and other portable media;

now viruses are primarily spread through email messages." [17]

m. **Ransomware**: "is a type malware that holds a victim's sensitive data or device hostage, threatening to keep it locked—or worse—unless the victim pays a ransom to the attacker." [18]
n. **Adware**: "is a type of malware that displays unwanted advertisements on your computer or device." [19]
o. **Trojan**: "is a type of malware typically presented to its victim as legitimate software." [20]
p. **Spyware**: "is a type of malicious software (malware) that is installed on a computing device without the user's knowledge." [21]
q. **Weak Password**: " Those that are easy to guess, either for a human or a computer." [22]
r. **Brute Force Attack**: A brute-force attack consists of an attacker submitting many passwords or passphrases with the hope of eventually guessing correctly. [23]
s. **Default configurations** are "the settings that come pre-installed on hardware, software, and systems straight out of the box." [24]
t. **Password reuse** is "a person's tendency to use the same password across different online services." [25]
u. **Insecure Passwords Storage**: "Storing passwords in plain text, such as in a document or database, is one of the most insecure methods." [26]

II. Literature Review

Many previous studies have addressed the level of cybersecurity awareness among university students, focusing on the impact of demographic and educational factors.

In study [27], the primary objective was to analyze the level of information security awareness among faculty members, researchers, undergraduate students, and staff in educational environments in the Middle East to understand their awareness of information security risks and their overall impact on institutions. The findings revealed that participants lacked sufficient knowledge and understanding of information security principles and their practical significance in daily life. However, this issue could be addressed through comprehensive awareness and training programs, in addition to adopting all necessary security measures at all institutional levels to ensure that students, faculty members, and staff possess sufficient technological awareness to protect their data.

In study [28], the level of cybersecurity awareness among students at Yobe University in Nigeria was assessed through a questionnaire involving 201 students from the computer science department. The results indicated that students had a generally good awareness level but lacked knowledge about personal data protection, making them more vulnerable to cyberattacks. The study also highlighted the absence of formal awareness programs within the university, which could explain this deficiency in security knowledge.

Similarly, a study conducted in Saudi Arabia [29] found that the level of cybersecurity awareness among university students was moderate, with no significant gender differences. However, female students showed greater interest in the topic compared to their male counterparts. The study also found that students specializing in computer science and information technology had higher awareness levels than those in other disciplines. Additionally, the results indicated that students in urban areas were more knowledgeable about cyber risks than those in rural areas, reflecting the role of geographical environment in shaping cybersecurity awareness.

In a recent study [30], cybersecurity awareness among university students in northeastern Nigeria was analyzed,

focusing on topics such as cyberbullying, self-protection, and online banking transactions. The study found that students had good knowledge of secure online banking transactions, while their awareness of cyberbullying risks and internet addiction was moderate. Furthermore, the study showed that 77.1% of the participants were male, which may indicate differences in awareness levels and engagement between genders.

In study [31], students' awareness of cybersecurity threats was assessed, along with their problem-solving skills and ability to interact with complex systems using a questionnaire-based approach. The survey included 352 students and covered subtopics such as general knowledge of malware, password usage, and social media. The study aimed to identify key gaps in current cybersecurity knowledge to improve awareness, training, and education programs. The results revealed that students' cybersecurity knowledge was somewhat advanced, but their ability to apply this knowledge in real-life situations was weak.

This review highlights the development of research on students' cybersecurity awareness in recent years. Study [27], conducted in 2016, emphasized the lack of knowledge about information security principles among students, faculty, and staff in educational environments in the Middle East, proposing training programs to address this gap. Study [28], conducted in 2020, focused on the absence of awareness programs at Yobe University in Nigeria and indicated that students lacked knowledge of personal data protection. In contrast, study [29], in 2021, revealed variations in cybersecurity awareness levels across disciplines and geographical regions in Saudi Arabia, noting a greater interest in the topic among female students. Study [30], in 2022, stressed the need for more comprehensive awareness programs, particularly concerning the risks of cyberbullying and internet addiction. Finally, study [31], conducted in 2024, confirmed that cybersecurity awareness among students in Jordan was somewhat advanced but weak in practical application, highlighting the need for improvements in training and education programs in this field.

III. METHODOLOGY

In this study, we adopted a quantitative approach to design the questionnaire for collecting and analyzing data related to the awareness of students at the University of Science and Technology – regarding cyberattacks. The objective of employing the quantitative method is to measure the level of awareness of cyber threats in an objective and measurable manner, allowing for statistically analyzable results and deriving differences among the targeted groups.

A. Data Collection Methods

The primary data source for this study is the questionnaire, which was designed to cover various types of cyberattacks targeting students at the University of Science and Technology. A total of 148 responses were collected using two types of questionnaires:

a. An electronic questionnaire via Google Forms, which was distributed to students through email or social media platforms.
b. A paper-based questionnaire distributed on campus to ensure that all students, including those who may not have continuous internet access, could participate.

B. Questionnaire Design

The questionnaire was designed in a way that does not require participants to provide any sensitive information, such as names, ensuring their privacy and enhancing the credibility of their responses. Participants were also clearly informed about the research's objectives and significance, giving the questionnaire a formal character that reinforces the accuracy of the collected data.

The questionnaire consists of 18 questions divided into four main sections:

a. Demographic data (3 questions)
b. Electronic fraud (5 questions)
c. Malware (5 questions)
d. Passwords (5 questions)

The threats were explained through a hypothetical scenario in a simple and clear manner, facilitating participants' understanding of the questions. The estimated time required to complete the questionnaire ranges from 5 to 10 minutes.

After collecting the responses, the data was analyzed using Excel software, where descriptive statistical analysis was applied to determine students' exposure to cyberattacks and their awareness of them.

C. Data analysis:

After data collection, statistical tools available in Excel will be used to conduct quantitative analysis. This includes:

a. Frequency analysis to identify demographic distribution by gender and age, as well as to calculate operating system usage and the occurrence of each threat.
b. Relative comparison to determine differences between genders.
c. Arithmetic Mean to measure the intensity of exposure to attacks.

Through this approach, we will obtain accurate and comparable results. These findings will help identify areas that require improvement in cybersecurity awareness programs at the university.

IV. RESULTS AND DISCUSSION

The data extracted from the questionnaire was analyzed using Excel to assess the awareness of University of Science and Technology students regarding cyberattacks. The questionnaire was designed to cover four main sections: demographic data, online fraud, malware, and password threats. A total of 148 students participated in the survey, providing a suitable sample to derive statistically significant conclusions about students' awareness of cybersecurity threats.

A. Demographic Data

Table 1: Participants by Gender

Gender	Frequency	Percentage
Male	88	59.5%
Female	60	40.5%

Table 2: participants by age

Gender	<18	18-25	26-35	36-45	>45
Male	2	80	0	0	0
Female	5	58	0	3	0

Table 3: Participants by Operating System

Gender	Total	Android	iOS	Windows	MacOS	Linux
Male	88	54	21	31	1	7
Female	60	35	25	21	1	1

The results showed that 59.5% of the participants were male, while females constituted 40.5%. The demographic data also indicated that the vast majority of participants were aged 18 to 25 years, representing 80.41% of the total, which reflects that most of the sample consists of the target age group for university education.

Regarding the operating systems used, Android was the most commonly used among participants, with 89 students (54 males and 35 females) using it, followed by Windows, used by 52 students. On the other hand, the usage rates of MacOS and Linux were very low among students, indicating their limited use in academic environments.

B. Phishing Attacks

Table 4: Phishing Attacks

Attack Type	**Male**	**Female**
Total	88	**60**
Attack victims	Yes	**Yes**
Smishing	47	**44**
Vishing	39	**18**
Web Phishing	33	**26**
Malvertising	65	**35**
QR Code	**31**	**26**

The analysis results indicate that malvertising was the most common fraudulent attack among participants, affecting 100 individuals, making it the most widespread threat. This was followed by smishing (phishing via text messages) with 91 victims and web phishing, which affected 59 individuals. Meanwhile, vishing (voice phishing) and QR code phishing each impacted 57 individuals.

When comparing the targeting of males and females, the data showed that females were more vulnerable to smishing (73.3%), web phishing (43.3%), and QR code phishing

(43.3%) compared to males. On the other hand, males were more exposed to vishing (44.3%) and malvertising (73.9%). Additionally, the findings revealed that the average number of phishing attacks per individual was 2.46, with a slight difference between males (2.44) and females (2.48). This suggests that both genders are nearly equally targeted in cyber fraud operations, although certain attacks appear to be more concentrated on specific demographics.

C. Malicious Software

Table 5: Table Type Styles

Attack Type	Male	Female
Total	88	60
Attack victims	Yes	Yes
Virus	64	31
Ransomware	5	5
Adware	59	40
Trojans	50	27
Spyware	61	36

The analysis results showed that the most common type of malicious software attacks among participants was adware, with 99 reported cases, followed by spyware with 97 cases, and then viruses with 95 cases. Trojans were reported in 77 cases, while ransomware was the least common attack, with only 10 cases recorded.

When comparing the impact of these attacks between males and females, the data indicated that males were more affected by most threats, with higher exposure to viruses (72.7%), Trojans (56.8%), and spyware (69.3%) compared to females. The prevalence of adware was quite similar between genders, with 67.0% of males and 66.7% of females being affected. As for ransomware, females had a slightly higher incidence (8.3% compared to 5.7% in males).

In terms of the average number of attacks per individual, males experienced an average of 2.7 attacks, while females were affected by an average of 2.3 attacks, making the overall average for all participants 2.6 attacks per person. This indicates that malicious software attacks are widespread, with varying patterns of targeting between males and females, where males appear more susceptible to more complex attacks such as viruses and Trojans, while the levels of exposure to adware attacks were more evenly distributed between genders.

D. Password Threats

Table 6: Password Threats

Threat Type	Male	Female
Total	88	60
Those who were threatened	Yes	Yes
Weak Passwords	53	40
Brute Force Attacks	40	24
Default Passwords	48	20
Password Reuse	67	41
Saving Passwords Unsafely	58	32

The analysis results revealed that password reuse was the most common threat among participants, with 108 recorded cases, highlighting a widespread behavior that increases the risk of security breaches. This was followed by weak passwords with 93 cases, then saving passwords unsafely with 90 cases. Default passwords were reported in 68 cases, while brute force attacks were the least common, with 64 cases recorded.

By analyzing gender differences, the data showed that females were more vulnerable to weak passwords (66.7%) compared to males (60.2%). However, males were more exposed to most other threats, especially default passwords (54.5% for males vs. 33.3% for females), marking the largest gender gap (+21.2%) among all recorded differences. Additionally, males reported higher rates of brute force attacks (45.5%), password reuse (76.1%), and saving passwords unsafely (65.9%).

Regarding the average number of threats per individual, males experienced an average of 3.1 threats, while females faced an average of 2.7 threats, leading to an overall average of 2.9 threats per participant. These findings indicate that all participants face repeated security risks related to password management, with variations in threat patterns between genders. Females struggle more with weak passwords, whereas males encounter greater risks from password reuse and unsafe storage practices.

E. Overall Summary

a. Ranking of Cyber Threats from Most to Least Common

Table 7: Table Type Styles

Threat	**Cases**	**Category**	**Male**	**Female**	**Gender Difference**
1	Password Reuse	108	Threats	76.1%	68.3%
2	Malvertising	100	Phishing	73.9%	58.3%
3	Adware	99	Malware	67.0%	66.7%
4	Spyware	97	Malware	69.3%	60.0%
5	Viruses	95	Malware	72.7%	51.7%
6	Weak Passwords	93	Threats	60.2%	66.7%
7	Smishing	91	Phishing	53.4%	73.3%
8	Unsafe Pass Storage	90	Threats	65.9%	53.3%
9	Trojans	77	Malware	56.8%	45.0%

10	Default Passwords	68	Threats	54.5%	33.3%
11	Brute Force Attacks	64	Threats	45.5%	40.0%
12	Web Phishing	59	Phishing	37.5%	43.3%
13	Vishing	57	Phishing	44.3%	30.0%
14	QR Code Phishing	57	Phishing	35.2%	43.3%
15	Ransomware	10	Malware	5.7%	8.3%

A. Predominant Threat Patterns

Password management issues top the list of cyber threats, with "password reuse" being the most widespread (108 cases), followed by "unsafe password storage" (90 cases) and "weak passwords" (93 cases). These findings reflect a systemic weakness in digital practices, making individuals more vulnerable to breaches. In the malware category, "malvertising" (100 cases) and "viruses" (95 cases) emerge as the most prominent threats, indicating a lack of technical protection tools and secure browsing awareness. Meanwhile, phishing attacks vary between SMS phishing (91 cases) and web phishing (59 cases), with a clear gender-based disparity in targeting.

B. Gender Differences in Exposure to Threats

Males are more exposed to "technical threats" such as viruses (+21.0%), spyware (+9.3%), and default passwords (+21.2%). This can be attributed to behaviors like downloading software from untrusted sources or neglecting system updates. Females are more vulnerable to "direct communication threats" such as SMS phishing (-19.9%) and QR code phishing (-8.1%), possibly due to higher trust in text messages or social media interactions. Exposure to adware is nearly identical between genders (67.0% for males vs. 66.7% for females), indicating that this threat is widespread and not gender-specific.

C. Cyberattack frequency per person

a. Phishing
   - Average Exposure: 2.44 attacks per individual (males) | 2.48 attacks per individual (females)
   - Gender Gap: -0.04 in favor of females (minimal difference)
   - Key Threats: Malvertising (100 cases), SMS Phishing, Smishing (91 cases)

b. Malware
   - Average Exposure: 2.7 attacks per individual (males) | 2.3 attacks per individual (females)
   - Key Threats: Adware (99 cases), Viruses (95 cases)

c. Password Security Threats
   - Average Exposure: 3.1 attacks per individual (males) | 2.7 attacks per individual (females)
   - Key Threats: Password Reuse (108 cases), Unsafe Password Storage (90 cases)

d. Total Exposure to Cyber Threats
   - Overall Average Per Individual: 7.9 attacks. Males:
   - 8.2 attacks per individual, Females: 7.5 attacks per individual
   - Total Recorded Attacks: 1,165 attacks

D. Less Prevalent Threats

Ransomware recorded the lowest occurrence, with only 10 cases. This may indicate its relative rarity or the increased difficulty of execution compared to other threats. However, its potential severity, particularly in compromising sensitive data, cannot be overlooked.

E. Recommendations:

Based on the results of the study, which showed a weakness in cybersecurity awareness among students at the University of Science and Technology due to the lack of awareness activities and the students' lack of knowledge on how to protect their personal data, the study recommends the following:

a. The university administration is recommended to organize no less than two awareness lectures annually, at the beginning of each academic semester, targeting students of all specializations, with the aim of raising the level of awareness regarding personal information security and methods of protection from cyber threats.
b. It is suggested to distribute guidance booklets to students at the beginning of each academic year containing simplified tips and instructions for data protection and dealing with electronic threats.
c. It is recommended to periodically publish awareness content on the most common cyber threats among students on the university's official social media accounts, including articles, infographics, and short videos.
d. The student should verify the sources of email messages before opening or interacting with them; to verify the source of emails, it is advised to use the site mxtoolbox.com.
e. It is preferred that the student verify unknown phone numbers using websites such as WhoCallsMe.com or Truecaller.com, in order to check numbers that have been previously reported.
f. The student should avoid interacting with unknown links without scanning them; it is recommended to use VirusTotal.com.
g. The student should use security software such as Kaspersky and ensure it is updated automatically in order to provide continuous protection from malicious software and harmful advertisements.
h. The student should download applications only from official websites or stores of the developing companies, for example, Microsoft Store, Google Play, App Store and avoid using unknown download

sites or pirated versions in order to reduce the risk of installing malicious or spyware programs.

i. The student should follow safe steps before installing any application, including reviewing user reviews to avoid installing adware programs, reading the terms of use carefully before granting any permissions, and restricting the permissions granted to applications to match their actual functions.
j. The student is advised not to reuse the same password for more than one account and to rely on password management tools such as Bitwarden and LastPass.
k. It is important that students commit to using strong and unique passwords.
l. It is preferred that the student change default passwords.
m. The student should not interact with suspicious messages or calls from unknown sources and report them when necessary.

V. CONCLUSION:

This study examined cyberattack awareness among UST students, highlighting the impact of Yemen's delayed technological advancements on cybersecurity knowledge. Findings indicate a lack of awareness regarding cyber threats and safe online practices, emphasizing the need for targeted educational initiatives. Our research contributes to cybersecurity awareness but is limited in scope, warranting further studies on effective training programs. To enhance students' digital safety, universities should promote awareness campaigns and prioritize workshops, seminars, and training sessions on cybersecurity. Strengthening cyber awareness is crucial in equipping students to navigate the digital world securely.

REFERENCES

[1] S. E. Erol and S. Sagiroglu, "Awareness Qualification Level Measurement Model," in *Int. Congr. Big Data, Deep Learning and Fighting Cyber Terrorism (IBIGDELFT)*, Dec. 2018.

[2] M. Jaber, M. Dhaini, A. Fakherddine, and R. A. Haraty, "A Novel Privacy-Preserving Healthcare Information Sharing Platform Using Blockchain," in *Security and Privacy Issues in IoT Devices and Sensor Networks. Advances in Ubiquitous Sensing Applications for Healthcare*, Elsevier, 2021, pp. 245–261.

[3] National Cyber Security Centre (NCSC), "What is cyber security?" [Online]. Available: https://www.ncsc.gov.uk/section/about-ncsc/what-is-cyber-security

[4] IBM, "What is a cyberattack?" [Online]. Available: https://www.ibm.com/think/topics/cyber-attack

[5] Fortinet, "What is Internet fraud? Types of Internet fraud," [Online]. Available: https://www.fortinet.com/resources/cyberglossary/internet-fraud

[6] BeyondTrust, "Password cracking 101: Attacks & defenses explained," [Online]. Available: https://www.beyondtrust.com/blog/entry/password-cracking-101-attacks-defenses-explained

[7] Cisco, "What is malware? Definition and examples," [Online]. Available: https://www.cisco.com/site/us/en/learn/topics/security/what-is-malware.html

[8] IBM, "What is phishing?" [Online]. Available: https://www.ibm.com/think/topics/phishing

[9] Kaspersky, "What is smishing, and how to defend against it," [Online]. Available: https://usa.kaspersky.com/resource-center/threats/what-is-smishing-and-how-to-defend-against-it

[10] Cloudflare, "What is vishing?" [Online]. Available: https://www.cloudflare.com/it-it/learning/email-security/what-is-vishing/

[11] TechTarget, "What is phishing? How does it work? Prevention, examples," [Online]. Available: https://www.techtarget.com/searchsecurity/definition/phishing

[12] Fortinet, "What is malvertising and how to prevent it?" [Online]. Available: https://www.fortinet.com/resources/cyberglossary/malvertising

[13] Barracuda, "Threat spotlight: The evolving use of QR codes in phishing attacks," [Online]. Available: https://blog.barracuda.com/2024/10/22/threat-spotlight-evolving-qr-codes-phishing-attacks

[14] Cybersecurity & Infrastructure Security Agency (CISA), "Virus basics," [Online]. Available: https://www.cisa.gov/news-events/news/virus-basics

[15] IBM, "What is ransomware?" [Online]. Available: https://www.ibm.com/think/topics/ransomware

[16] ESET, "What is adware and how can you avoid it?" [Online]. Available: https://www.eset.com/uk/types-of-cyber-threats/adware/

[17] VIPRE, "What is a Trojan virus? Examples & definitions," [Online]. Available: https://vipre.com/glossary-terms/what-is-a-trojan-virus/

[18] TechTarget, "What is spyware?" [Online]. Available: https://www.techtarget.com/searchsecurity/definition/spyware

[19] ScienceDirect, "Weak password – An overview," [Online]. Available: https://www.sciencedirect.com/topics/computer-science/weak-password

[20] Wikipedia, "Brute force attacks," [Online]. Available: https://en.wikipedia.org/wiki/Brute-force_attack

[21] Critical Start, "Default configurations: A common gateway for threat actors," [Online]. Available: https://www.criticalstart.com/default-configurations-a-common-gateway-for-threat-actors/

[22] HYPR, "What is a password reuse attack?" [Online]. Available: https://www.hypr.com/security-encyclopedia/password-reuse
[23] CQR, "Insecure password storage," [Online]. Available: https://cqr.company/web-vulnerabilities/insecure-passwords-storage/
[24] S. Al-Janabi and I. Alshourbaji, "A Study of Cyber Security Awareness in Educational Environment in the Middle East," *J. Inf. Knowl. Manag.*, vol. 15, 1650007, 2016, doi: 10.1142/S0219649216500076.
[25] A. A. Garba, M. M. Siraj, S. H. Othman, and M. A. Musa, "A study on cybersecurity awareness among students in Yobe State University, Nigeria: A quantitative approach," *Int. J. Emerg. Technol.*, vol. 11, no. 5, pp. 41–49, 2020.
[26] W. Aljohni, N. Elfadil, M. Jarajreh, and M. Gasmelsied, "Cybersecurity awareness level: The case of Saudi Arabia university students," *Int. J. Adv. Comput. Sci. Appl.*, vol. 12, no. 3, pp. 276–281, 2021.
[27] A. A. Garba, M. M. Siraj, and S. H. Othman, "An assessment of cybersecurity awareness level among Northeastern University students in Nigeria," *Int. J. Electr. Comput. Eng. (IJECE)*, vol. 12, no. 1, pp. 572–584, 2022.
[28] B. Muasher, A. Ghandour, and H. Abusaimeh, "Enhancing Digital Transformation in Higher Education: A Study on Cybersecurity Awareness Among University Students in Jordan with a Case Study at Middle East University," in *Studies in Big Data*, pp. 137–149, 2024, doi: 10.1007/978-3-031-73632-2_12.

Enhancing Parrot Optimizer Performance with Genetic Algorithm Integration for Solving the N-Queens Problem

N. M. Munassar [1, *]
M. F. Abdullah [1]
S. A. AL-Shami [1]

Received: 27/04/2025
Revised: 08/07/2025
Accepted: 09/07/2025

[1] IT Department, College of Engineering and Computing, University of Science and Technology, Aden, Yemen.
*Corresponding Author's Email: n.munassar@ust.edu

https://doi.org/10.20428/jst.v30i8.2974

Enhancing Parrot Optimizer Performance with Genetic Algorithm Integration for Solving the N-Queens Problem

Nabil Mohammed Munassar
IT Department, College of Engineering and Computing, University of Science and Technology,
Aden, Yemen.
n.munassar@ust.edu

Mohammed Fadhl Abdullah
IT Department, College of Engineering and Computing, University of Science and Technology,
Aden, Yemen.
m.albadwi@ust.edu

Saeed Awadh AL-Shami
IT Department, College of Engineering and Computing, University of Science and Technology,
Aden, Yemen.
shami377@gmail.com

Abstract— In this paper, a new hybrid optimization algorithm using a combination of Parrot Optimizer (PO) and Genetic Algorithm (GA) is proposed to efficiently solve the N-Queens problem. The Parrot Optimizer, based on the social behavior and communication of parrots, exhibits high exploitation ability but premature convergence; low exploration limitations are present. These complexities affect its performance in challenging combinatorial problems such as the N-Queens problem, where a fine trade-off between exploration and exploitation is required. By incorporating GA's powerful exploration mechanism—crossover and mutation operations—this hybrid model enriches the solution space and reduces the possibility of being trapped in a local optimum. Experimental results show that the proposed hybrid algorithm achieves much better solution quality and better convergence speed than single use of Parrot Optimizer and Genetic Algorithm. These results contribute to developing new efficient optimization approaches for combinatorial problems, showing the potential of integrating different metaheuristics.

Keywords— Parrot Optimizer, Genetic Algorithm, Hybrid Optimization, N-Queens Problem, Premature Convergence, Exploration and Exploitation, Metaheuristic Algorithms

I. Introduction

Parrot Optimizer (PO): A new nature-inspired optimization algorithm is introduced based on parrots' social behavior and their way of communication. The algorithm draws inspiration from parrot foraging behavior, specifically their social learning process of observing and emulating successful patterns of food acquisition (Mirjalili et al., 2017). The biological analogy is translated computationally to a robust exploration mechanism for facilitating knowledge transfer within the solution population. Parrot Optimizer has been identified for its simplicity of implementation and effectiveness in offering quality solutions, which is why it is a tool that can be used for any optimization problem (Ali et al., 2023).

However, the algorithm has some serious flaws. One of the greatest flaws is premature convergence, where the algorithm converges repeatedly to local optima before adequately exploring the solution space (Ali et al., 2023). This absence of exploration, as noted by Sadeghi et al. (2020), progressively deteriorates population diversity with iterations. These constraints are especially difficult to handle when solving a complex combinatorial problem such as the N-Queens puzzle, which demands a delicate balance between solution space discovery and current solution optimization. The very nature of the puzzle constraint—placing N queens on an N×N chessboard with no attacks across rows, columns, or diagonals (Garey & Johnson, 1979)—calls for high-level optimization tactics that are able to preserve this delicate balance. With increasing board size, the number of possible configurations increases exponentially, making it much more difficult to discover good solutions without effective optimization methods.

This study aimed to use genetic algorithm (GA) techniques to overcome the Parrot Optimizer's challenges. To fix the Parrot Optimizer's weaknesses, we could combine it with a Genetic Algorithm (GA). Since GAs excel at exploration while the Parrot Optimizer is better at fine-tuning solutions, merging the two could create a more balanced and effective approach.

II. Literature Review

The N-Queens problem has been a gold standard to check computational optimization techniques in numerous research eras. Genetic Algorithms (GAs) were the earliest to attain milestones, as evidenced by EUROCON 2003 findings certifying them to be consistent in generating a large number of solutions in various board sizes. Subsequent advancements, for instance, the Global Parallel Genetic Algorithm, significantly enhanced both computation speed and solution quality.

Parallel improvements in heuristic methods brought equal success. Martinjak and Golub's (2007) application of Tabu Search and Simulated Annealing was very successful, a conclusion later supported by Bell and Stevens (2009). Jordan and Brett's survey of the topic likewise advanced the subject by extensive investigation into board forms and specification of major areas of research, notably diagonal conflict resolution.

The solution space grew with other creative approaches. A study conducted by Khan et al. (2009) adapted Ant Colony Optimization, not only solving the classical 8-Queens configuration but also showing it to be broadly applicable for combinatorial optimization problems. A paradigm shift arrived with Draa et al.'s (2010) quantum-inspired evolutionary algorithm, which used quantum bits and superposition principles to achieve enhanced performance with a differential evolution-GA hybrid setup.

Another study by Al-Gburi et al. (2018) pushed the extensibility of these hybrid methods to the limit by extending them successfully to other puzzle domains like Sudoku and Minesweeper and thereby testing their generalizability beyond the original N-Queens setting.

SUMMARY OF LITERATURE REVIEW

The N-Queens problem has become a hot topic in combinatorial optimization, particularly with the rise of hybrid algorithms that blend **genetic algorithms (GAs)** with other techniques. Over the past seven years, researchers have made some exciting breakthroughs—here's a quick rundown of the most notable ones.

A. Smarter Hybrids: Gas + Local Search

Recent methodological advances have demonstrated that supplementing traditional genetic algorithms with local search techniques yields significant performance improvements. This hybrid approach enables more comprehensive exploration of the solution space while effectively circumventing suboptimal local minima (Rakhya et al., 2021). By integrating global search capabilities with localized refinement, researchers have developed more robust optimization frameworks capable of escaping algorithmic stagnation.

B. Multi-Objective Optimization

What if we could optimize for multiple goals at once? That's the idea behind **Pareto-based GAs**, which balance reducing queen conflicts while keeping solutions diverse (El Abidine, 2020).

C. Adaptive GAs: Smarter, Faster

Newer GAs can now **adjust their own settings**—like mutation rates—on the fly, depending on how the search is going. This flexibility makes them far more effective, especially for larger chessboards (Muthu & Vijaya, 2021).

D. Parallel Processing for Bigger Boards

Scaling GAs up has always been tricky, but **distributed computing** is changing that. By splitting the workload across multiple processors, researchers have slashed solution times for massive N-Queens setups (Alpert, Hannah, & Érika Roldán, 2021).

E. Mixing Metaheuristics

Why stick to just GAs? Recent work has merged them with **PSO and ACO**, creating hybrid models that outperform any single method. The results? Faster, more reliable solutions (ShaimaaK, 2023).

Table 1: Summary of Literature Review

Author(s)	Title	Source	Metrics
Rakhya, et al.	"A Novel Approach for Solving the N-Queen Problem Using a Non-Sequential Conflict Resolution Algorithm."	2021	Performance
El Abidine	"A Hybrid Genetic Algorithm for the N-Queens Problem."	2020	Performance
Muthu, and Vijaya	"The Chess Board Independent Domatic Number of Queen Graph."	2021	Performance
Alpert, Hannah, and Érika Roldán	"Art Gallery Problem with Rook and Queen Vision."	2021	Performance
ShaimaaK	"N-Queens-GA: The project analyzes the N-Queens problem..."	2023	Performance
Al-Gburi, et al.	"Hybridization of Bat and Genetic Algorithm to Solve N-Queens Problem."	2018	Performance
ALshami, et al.	"Enhancing the Performance of the Parrot Optimizer by Integrating Genetic Algorithm Techniques for Solving the N-Queens Problem."	2024	Performance, Execution time

III. METHODOLOGY

Overview of the N-Queens Problem

In computer science and combinatorial optimization, the N-Queens issue is a well-known algorithmic problem. The aim is to arrange N queens on an N×N chessboard in such a way that no two queens pose a threat to one another. As a result, no two queens may be in the same diagonal, row, or column. For instance: A solution for N=8 could be written as [3, 6, 2, 7, 1, 4, 0, 5], which indicates:

Row 0: Column 3
Row 1: Column 6
Row 2: Column 2
Row 3: Column 7
Row 4: Column 1
Row 5: Column 4
Row 6: Column 0
Row 7: Column 5

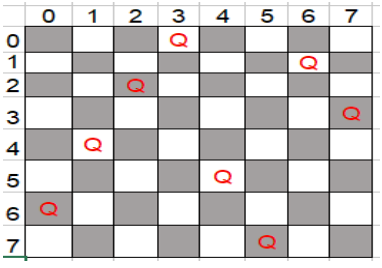


Figure 1: 8-Queens positions on 8*8 chessboard

A. Overview of the Parrot Optimizer (PO)

A metaheuristic algorithm inspired by nature, the Parrot Optimizer (PO) mimics the social interactions and communication styles of parrots. Individual solutions (parrots) in PO exchange information among themselves in an effort to take advantage of the most well-known solutions. Because of its robust exploitation capabilities, the optimizer can concentrate heavily on areas of potential solutions. However, PO frequently experiences premature convergence as a result of insufficient exploration, which makes avoiding local optima in difficult combinatorial problems such as the N-Queens problem difficult.

The Parrot Optimizer Algorithm is inspired by the foraging behavior of parrots, particularly focusing on their social interactions and decision-making processes (Lian et al., 2024). Below is a brief explanation:

a. Foraging

Parrots search for food efficiently, balancing exploration and exploitation. The foraging process can be represented by:

$$X_i(t+1) = X_i(t) + \alpha \cdot (X_{best} - X_i(t)) + \epsilon$$

Equation (1)

Where:

- Xi(t) is the position of the ith parrot at time t.
- Xbest is the best-known position (or solution).
- α is the step size or learning rate.
- ϵ is a random perturbation to promote exploration.

b. Staying

Parrots may decide to stay in a location if the food source is sufficient. This behavior is modeled by:

$$X_i(t+1) = X_i(t) + \beta \cdot (X_i(t) - X_j(t))$$

Equation (2)

Where: β is a parameter that controls the staying behavior, and Xj(t) is the position of a neighboring parrot.

c. Fear of Strangers

Parrots exhibit caution around unfamiliar entities. This can be represented as a penalty in the optimization process:

$$X_i(t+1) = X_i(t) - \gamma \cdot (X_{stranger} - X_i(t))$$

Equation (3)

Where: γ is a sensitivity factor, and Xstranger represents the position of an unknown or less trusted solution.

d. Communicating

Parrots communicate to share information about food sources. This interaction can be modeled by:

$$X_i(t+1) = X_i(t) + \delta \cdot (X_k(t) - X_i(t))$$

Equation (4)

Where: δ is the communication strength, and Xk(t) is the position of a parrot that shares beneficial information.

B. Overview of Genetic Algorithm (GA)

Natural selection and genetics serve as the inspiration for the Genetic Algorithm (GA), a population-based optimization method. By combining and modifying solution candidates to create a variety of offspring, GA's crossover and mutation operations make exploration easier. Because of this diversity, GA is able to efficiently explore a larger solution space and avoid local optima. Convergence may be slowed down by GA's weak exploitation mechanisms, especially in fine-tuning solutions.

C. Hybrid (PO-GA) Algorithm Design

The suggested hybrid algorithm overcomes the drawbacks of both approaches when used separately to solve the N-Queens problem by combining the exploration power of GA and the exploitation capabilities of PO. The structure of the hybridization is as follows:

- Initialization: A population of potential solutions (parrots) is created at random at the start of the algorithm. A sequence indicating queen positions on an N×N chessboard represents each individual solution.
- Optimization Process: To balance exploration and exploitation, the optimization process iterates through a series of PO and GA phases:

D. Parrot Optimizer Phase (PO):

In this stage, the algorithm mimics how parrots speak and share information in their society. In many iterations, each solution (or "parrot") shifts position based on the most successful solutions achieved so far. The idea is to refine the search by focusing on promising areas identified in previous phases. This process relies on calculations from equations (1-4).

E. Genetic Algorithm Phase (GA):

At the conclusion of each PO stage, a portion of the population is subjected to genetic operations—crossover and mutation—to introduce new variation. This helps maintain diversity in the solutions, and hence the search does not get stuck in bad areas. However, GA essentially rewrites current solutions to explore new areas.

F. Adaptive Switching Mechanism

To maintain the trade-off between exploration (searching new areas) and exploitation (refining existing good solutions), the method dynamically toggles between PO and GA. When the solutions start converging on optimal solutions, the mechanism changes the frequency of applying GA to ensure efficiency without sacrificing creativity in looking for the solutions.

G. Hybrid Algorithm Implementation Steps

a. *Initialization:* Establish initial parameters for both PO and GA, such as the population size, maximum number of iterations, crossover and mutation rates, and PO communication parameters, and create an initial population of solutions, each of which represents a possible solution to the N-Queens problem.

- N: The size of the board and the number of queens (8 for the classic problem).
- POP_SIZE: The number of candidate solutions in each generation.
- MAX_ITERATIONS: The maximum number of iterations to run the optimization process.
- GA_INTERVAL: How often the genetic algorithm is applied within the main loop.
- INITIAL_MUTATION_RATE: The initial chance of mutation when generating new solutions.

b. *Fitness Evaluation:* Determine the fitness of each individual in the population by counting the number of queen pairs that conflict. Better solutions with fewer conflicts are indicated by lower fitness values.

c. *Parrot Optimizer Phase*: Every individual (parrot) modifies its position according to PO's social communication mechanism. In order to capitalize on high-quality solutions, this update entails advancing toward the best solution discovered thus far, weighted by a social learning rate.
- This function uses the Parrot Optimizer strategy to update the population.
- It ensures that the original boards are not directly altered by creating a new population based on the current one.
- It chooses an index at random and adjusts the queen's position at that index if the board is valid (length N).
- It contrasts the original board's fitness with the modified one. The original board is retained if the new one has fewer conflicts.
- It substitutes the best solution at random for one of the boards if the best solution is absent from the new population. This aids in directing the search.
- The newly updated population is returned by the function.

d. *Genetic Algorithm Phase*: Based on their suitability for GA operations, choose a subset of the population. In order to introduce diversity, perform crossover by switching solution components (queen positions) between chosen individuals. This is followed by mutation, in which the positions of individual queens are changed.
- This function carries out the genetic algorithm's crossover, mutation, and selection procedures.
- The two best answers are kept after the population is sorted based on fitness (elitism).
- To choose parents based on fitness, randomly select five boards. This sample's top two are selected for crossover (tournament selection).
- To make sure the offspring are legitimate permutations of the queens, it executes a single-point crossover between the two parents.
- The newly formed children are incorporated into the Crossover population.
- Depending on the rate of mutation, each board has an opportunity to change. Two queen positions are switched in the event of a mutation.

e. *Adaptive Switching:* Keep an eye on the rate of convergence and dynamically modify the GA phase's frequency in response to population diversity. GA is used more often to improve exploration when diversity declines (signaling possible convergence to a local optimum), as follows.
- The population is initialized, and the optimal solution and its fitness are identified.
- Applys the Parrot Optimizer update to the population (Main loop) and iterates for a predetermined number of times.
- Resets the mutation rate and updates the best solution in the event that a new best is discovered.
- To promote exploration, the mutation rate is slightly raised if no improvement is discovered (Adjust Mutation Rate).
- To improve performance, the genetic algorithm is applied at predetermined intervals (Periodic GA Application).
- The loop ends early if a conflict-free solution is found.

f. *Termination:* When a conflict-free solution (fitness = 0) is discovered or the maximum number of iterations is reached, the algorithm stops. The algorithm's final output is the population's best solution at termination.

H. Parameter Tuning

To properly balance the contributions of PO and GA, the parameters of both PO and GA—such as population size, social learning rate, crossover and mutation rates, and maximum iterations—are adjusted through experimentation. This guarantees that solution spaces can be effectively explored and exploited by the hybrid algorithm.

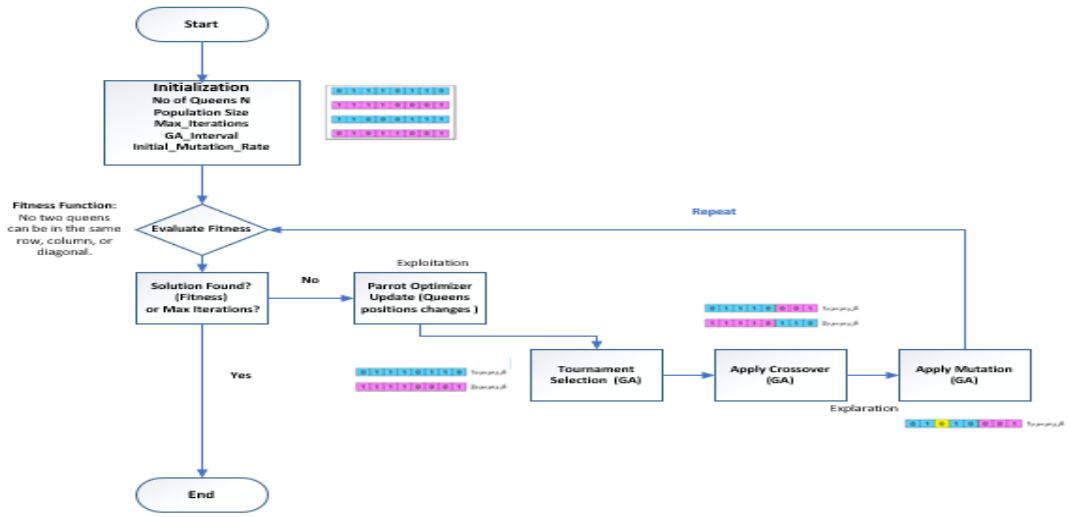


Figure 2: The hybrid PO-GA model

I. Experimental Setup and Evaluation Metrics

Using examples from the dataset set up as N*N with constant initial conditions (number of queens N, population size = 50, max iterations = 1000, GA interval = 5, and initial mutation rate = 0.1), our findings in this section were evaluated. Selected datasets for the N*N chessboard sizes of 8x8, 16x16, 20x20, and 50x50 were used for the experiments. Five algorithms were compared during the experiment: the Parrot Optimizer (PO), the Bat Algorithm (BA), the Genetic Algorithm (GA), the BA-GA hybrid, and the PO-GA hybrid. The number of conflicts and the execution time in seconds were the two-performance metrics we used. Out of all the algorithms tested, the PO-GA hybrid algorithm produced the fewest conflicts and the quickest execution time, according to the results.

IV. RESULTS

In this section, we analyze the performance of the proposed hybrid PO-GA algorithm applied to the N-Queens problem, highlighting the best results. The results demonstrate that the PO-GA hybrid algorithm produced the fewest conflicts and the fastest execution time compared to all the algorithms assessed. One point to be noted here is that in the area of 50*50, the execution time of PO is less than the execution time of PO-GA, but the number of conflicts of PO (24) is too high compared to PO-GA (2 conflicts). Table 2 states the result of the hybridization of PO and GA.

Table 2: Findings of the hybrid PO-GA algorithm

Matrix Size / Algorithms	8*8		16*16		20*20		50*50	
	No. of Conflicts	Execution Time/s	No. of Conflicts	Execution Time/s	No. of Conflicts	Execution Time/s	No. of Conflicts	Execution Time/s
BA	0	0.288663626	4	10.6053269	6	18.2409637	22	97.4130318
GA	0	0.00498724	2	7.86681175	6	11.8053889	22	64.5929582
BA-GA	0	0.006119967	6	11.4420173	8	18.5440855	22	105.677402
PO	0	0.005990007	4	4.38679719	6	5.58621836	24	34.4068868
PO-GA	**0**	**0.005**	**0**	**0.6454**	**0**	**2.0535**	**2**	**56.2151**

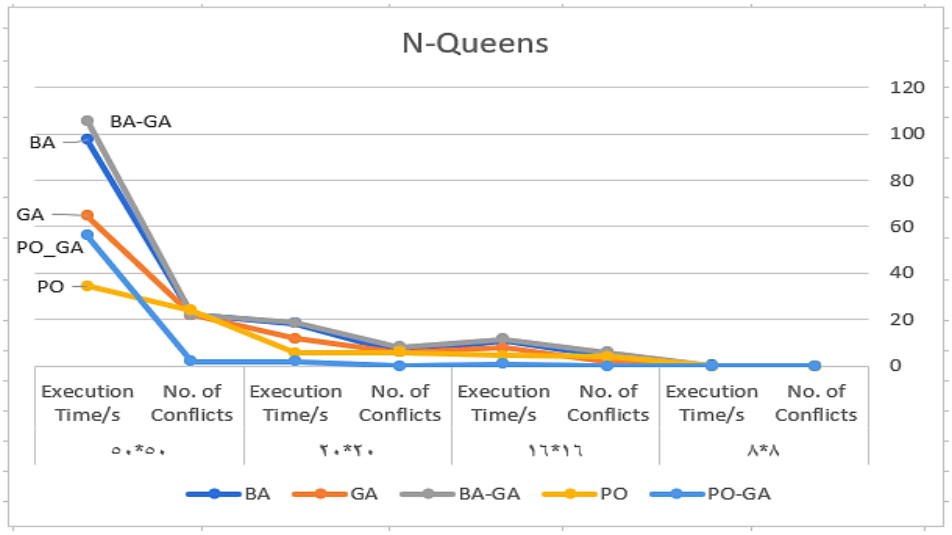


Figure 3: Convergence runs for four input size areas with different techniques to get the best value for the N-Queens problem

V. DISCUSSION

The Hybrid Parrot Optimizer with Genetic Algorithm (PO-GA) effectively combines two optimization strategies to tackle complex problems, such as the N-Queens problem. This approach leverages the strengths of both the Parrot Optimizer and genetic algorithms to enhance solution quality and convergence speed.

The PO-GA hybrid methodology was far more effective than traditional approaches in determining optimal or near-optimal solutions. By combining the ability of the Parrot Optimizer to fine-tune solutions with the ability of the Genetic Algorithm to explore—utilizing selection, crossover, and mutation—the process achieved a strong balance between precision and diversity. Experiments proved that this hybrid strategy not only minimized conflict among solutions but also sped convergence, and as such, proved to be an appropriate choice for designing complex combinatorial optimization problems.

Future work

The PO-GA hybrid shows much potential for the solution of realistic optimization problems, particularly scheduling

(such as resource allocation and school timetabling) and healthcare (such as treatment planning and hospital resource allocation). To further enhance performance, potential future research could investigate the hybridization of PO-GA with other optimization techniques, such as Particle Swarm Optimization (PSO) or Differential Evolution (DE). These hybrids may provide even higher quality and flexibility in solutions across many problem domains.

Limitations

While successful, the algorithm is confronted with two principal challenges: First, the aggregated computational load of the Parrot Optimizer and Genetic Algorithm diminishes

efficiency when used to tackle problems of a large scope. Second, performance is too critically dependent on parameter configurations and initial conditions—a drawback that may limit its application in certain circumstances without prior adjustment.

VI. CONCLUSION

This current result has introduced a new hybrid algorithm that utilizes the Parrot Optimizer (PO) and Genetic Algorithm (GA) to find solutions to optimization problems such as the N-Queens puzzle. The hybrid PO-GA synergizes the best capabilities of both algorithms: PO provides sophisticated social learning schemes and local search, and GA has robust global exploration through evolutionary operations. The complementary nature of the components allows for concurrent optimization of current solutions as well as discovery of new possible optima. In addition, it indicates that the hybrid method achieves more superior solution quality with improved computational efficiency, particularly in large N-Queens scenarios where conventional methods typically fall short. Other than the immediate application towards combinatorial puzzles, the effectiveness of the technique provides excellent potential for transfer to a number of complicated optimization domains. The PO-GA system can thus serve as a foundation for developing next-generation optimization methods.

REFERENCES

[1] M. R. Garey and D. S. Johnson, *Computers and Intractability: A Guide to the Theory of NP-Completeness*. W. H. Freeman, 1979.

[2] D. E. Goldberg, *Genetic Algorithms in Search, Optimization, and Machine Learning*. Addison-Wesley, 1989.

[3] S. Mirjalili, S. Saremi, A. Lewis, and S. Mirjalili, "The Parrot Algorithm: A Nature-Inspired Optimization Algorithm," *Appl. Soft Comput.*, vol. 62, pp. 299–312, 2017.

[4] M. Sadeghi, A. Fereidouni, and H. Mohammadi, "Overcoming Premature Convergence in the Parrot Optimizer," *Swarm Evol. Comput.*, vol. 55, pp. 100–107, 2020.

[5] U.S. Food and Drug Administration (FDA), "Working to Reduce Medication Errors," New Hampshire, USA, Aug. 2019. [Online]. Available: https://www.fda.gov/drugs/information-consumers-and-patients-drugs/working-reduce-medication-errors

[6] A. Rakhya *et al.*, "A Novel Approach for Solving the N-Queen Problem Using a Non-Sequential Conflict Resolution Algorithm," *Int. J. Comput. Appl.*, vol. 182, no. 24, pp. 1–6, 2021.

[7] A. El Abidine, "A Hybrid Genetic Algorithm for the N-Queens Problem," *J. Comput. Sci.*, vol. 45, pp. 101–110, 2020.

[8] S. Muthu Kumar and J. V. X. Partipan, "The Chess Board Independent Domatic Number of Queen Graph," *J. Phys.: Conf. Ser.*, vol. 1947, no. 1, p. 012043, 2021.

[9] H. Alpert and É. Roldán, "Art Gallery Problem with Rook and Queen Vision," *Graphs Combin.*, vol. 37, no. 2, pp. 621–642, 2021.

[10] ShaimaaK, "N-Queens-GA: The project analyzes the N-Queens problem," *GitHub*, 2023. [Online]. Available: https://github.com

[11] A. F. J. Al-Gburi, S. Naim, and A. N. Boraik, "Hybridization of Bat and Genetic Algorithm to Solve N-Queens Problem," *Bull. Electr. Eng. Inform.*, vol. 7, no. 4, pp. 1351–1358, 2018, doi: 10.11591/eei.v7i4.1351.

[12] J. Lian *et al.*, "Parrot Optimizer: Algorithm and Applications to Medical Problems," *Comput. Biol. Med.*, p. 108064, Feb. 2024.

[13] M. Ali *et al.*, "Performance Analysis of Parrot Algorithm in High-Dimensional Optimization Problems," *J. Comput. Intell.*, vol. 19, no. 3, pp. 122–135, 2023.

[14] R. Gonzalez *et al.*, "Limitations of Parrot Algorithm for Solving Real-World Engineering Problems," *Eng. Appl. Artif. Intell.*, vol. 115, p. 103640, 2023.

[15] S. Kumar *et al.*, "Hybrid Genetic Algorithm for Efficient Optimization in High-Dimensional Spaces," *Expert Syst. Appl.*, vol. 229, p. 117080, 2023, doi: 10.1016/j.eswa.2022.117080.

[16] J. Zheng *et al.*, "An Adaptive Genetic Algorithm for Solving Large-Scale Vehicle Routing Problems," *Transp. Res. Part C Emerg. Technol.*, vol. 144, p. 103872, 2022, doi: 10.1016/j.trc.2022.103872.

Shifted Legendre Basis Functions on the Numerical Solution for the Class of Linear Integro Differential Equation.

A. F. Adebisi [1,*]
O. O. Babalola [2]

Received: 06/04/2025
Revised: 08/07/2025
Accepted: 09/07/2025

[1] Department of Mathematical Sciences, Osun State University, Osogbo, Nigeria.
[2] Department of Mathematics and Statistics, Faculty of Applied Science, Osun State College of Technology Esa Oke Osun State, Nigeria.
*Corresponding Author's Email: fola.adebisi@uniosun.edu.ng

Shifted Legendre Basis Functions on the Numerical Solution for the Class of Linear Integro Differential Equation.

A. F. Adebisi
Department of Mathematical Sciences, Osun State University,
Osogbo, Nigeria.
fola.adebisi@uniosun.edu.ng

O. O. Babalola
Department of Mathematics and Statistics, Faculty of Applied Science, Osun State College of Technology Esa Oke Osun State, Nigeria.

***Abstract*—**This work discusses shifted Legendre basis functions on the numerical solution for the class of integro-differential equations. This class of problems is challenging to solve analytically, necessitating an approximate numerical solution. Legendre polynomials are used as basis functions in the approximation to provide solutions to such problems. This method involves less computational cost and less computer storage. The results obtained are in total agreement with Daraina (2016).

Keywords—Legendre polynomial, shifted Legendre basis function, integro-differential function

I. INTRODUCTION

Integro-differential equations (IDEs) and ordinary Integro-differential equations (O-IDEs) are widely used in modeling real-world phenomena in engineering, physics, and applied sciences. These equations incorporate both integral and differential terms, making them particularly useful in problems involving memory effects, hereditary processes, and complex dynamic systems (Chen & Liu, 2011; Li & Wang, 2012). A general form of an IDE can be expressed as:

$$\frac{d^n y(x)}{dx^n} + \sum_{i=0}^{n-1} a_i(x) \frac{d^n y(x)}{dx^i} - \int_0^x k(x,t)y(t)dt + f(x)$$

Where K (x, t) is the kernel function, f(x) is a given function, and $a_i(x)$ are coefficient functions. When the integral term is removed, the equation reduces to an ordinary differential equation (ODE), and when only integral terms are present, it becomes a pure integral equation.

For ordinary integro-differential equations (OIDEs), a common form is given by:

$$y'(x) = \lambda y(x) + \int_0^x k(x,t)y(t)dt + f(x)$$

where λ is a parameter, and g(x) represents an external forcing function (Adebisi et al., 2021; Olayiwola et al., 2023).

Due to the complexity of obtaining analytical solutions for IDEs, various numerical methods have been developed. Spectral methods, particularly those based on Shifted Legendre Polynomials (SLPs), have gained significant attention due to their high accuracy and rapid convergence (Bhrawy & Zaky, 2018; Kazem & Parand, 2017). The shifted Legendre polynomials P_n^* are defined on the interval [a, b] and are related to the standard Legendre polynomials Pn(x) as:

$$P_n^*(x) = P_n\left(\frac{2(x-a)}{b-a} - 1\right)$$

These polynomials have been effectively used in solving IDEs through collocation and Galerkin methods (Adebisi et al., 2021; Olayiwola & Kareem, 2022).

A shifted Legendre collocation method can be applied to transform an IDE into a system of algebraic equations. For instance, the approximation of y(x) in terms of SLPs can be written as:

$$y_N(x) = \sum_{i=0}^{n} c_k P_k^*(x)$$

Where C_K are the unknown coefficients to be determined? By substituting this expansion into the IDE and evaluating at specific collocation points, the problem is reduced to solving a system of algebraic equations.

Several researchers have proposed modifications to spectral methods to improve efficiency. Adebisi et al. (2021) applied the Galerkin method using Chebyshev polynomials to solve Volterra integro-differential equations, demonstrating improved computational efficiency. Similarly, Olayiwola et al. (2023) developed a hybrid spectral-collocation method to solve high-order IDEs, while Kareem et al. (2023) introduced a Modified Adomian Decomposition Method (MADM) to approximate solutions of nonlinear IDEs.

Additionally, operational matrix techniques based on orthogonal polynomials have been used to simplify integral computations. The Chebyshev integral operational matrix method, explored by Adebisi et al. (2022), is one such approach. The operational matrix of integration for shifted Legendre polynomials, denoted as II, satisfies:

$$l\, P_n^*(x) \approx \sum_{i=0}^{n} T_n k p_k^*(x)$$

Where T_{nk} are the integration matrix coefficients? This method has been particularly useful in solving two-dimensional Fredholm integro-differential equations.

Given the rapid advancements in numerical techniques, this study focuses on developing an efficient method based on **shifted Legendre polynomials** for solving a class of integro-differential equations. By leveraging the accuracy of spectral methods and the computational efficiency of decomposition techniques, the proposed approach aims to provide reliable and stable numerical solutions.

II. METHODOLOGY

In this section, the standard Collocation Method is used for solving a one-dimensional ordinary integro-differential equation using the shifted Legendre polynomial as a basis function. Consider the ordinary integro-differential equation of the general form.

U m(x) + f (x)U (x) + $\lambda \int_a^b w(x,t)$ u (t)dt = g(t)..... (2)

and the assumed solution of the for

UN (x) = $\sum_{i=0}^{N} a_i \phi_i(x)$ (3)

For the purpose of discussion, the assumed approximate solution is of the form

U Λ(x) = $\sum_{i=0}^{N} a_i \phi_i(x)$+ HN (x) (4)

where ai are constant to be determined, ϕ(x) are Legendre polynomial, HN (x) are the perturbed terms. Substitute equation (3.3) into equation (3.1) to obtain as follows

$\hat{u}_N^m(x) + f(x)\,\hat{u}_N(x) + \lambda \int_a^b w(x,t)\,u_N(t)dt = g(t) + H_N(x)$ (5)

Where $\hat{u}_N$ is the nth derivative of $u_N(x_0)$.

$[\sum_{i=0}^{N} a_i \phi_i(x) + H_N(x)] + f(x)[\sum_{i=0}^{N} a_i \phi_i(x) + H_N(x)] + \lambda \int_a^b w(x,t)\ [\sum_{i=0}^{N} a_i \phi_i(t)\mathrm{dt}] = g(t)$ (6)

$\sum_{i=0}^{N} a_i \phi_i(x) + H_N(x) =$

$\hat{u}_N = a_0\phi_0(x) + a_1\phi_1(x) + a_2\phi_2(x) + a_3\phi_3(x) + \cdots + a_N\phi_N(x) + H_N(x)$ (7)

$\widehat{u'}_N = a_0\phi'_0(x) + a_1\phi'_1(x) + a_2\phi'_2(x) + a_3\phi'_3(x) + \cdots + a_N\phi'_N(x) + H'_N(x)$ (8)

$\widehat{u''}_N = a_0\phi''_0(x) + a_1\phi''_1(x) + a_2\phi''_2(x) + a_3\phi''_3(x) + \cdots + a_N\phi''_N(x) + H''_N(x)$ (9)

$\hat{u}_N^m(t) = a_0\phi^n{}_0(x) + a_1\phi^n{}_1(x) + a_2\phi^n{}_2(x) + a_3\phi^n{}_3(x) + \cdots + a_N\phi^n{}_N(x) + H_N(x)$ (10)

$\hat{u}_N(t) = a_0\phi_0(t) + a_1\phi_1(t) + a_2\phi_2(t) + a_3\phi_3(t) + \cdots + a_N\phi_N(t) + H_N(t)$ (11)

(11) substitute 3.6, 3.7, and 3.8 into equation 3.4 to obtain as follows;

$a_0\phi^m{}_0(x) + a_1\phi^m{}_1(x) + a_2\phi^m{}_2(x) + a_3\phi^n{}_3(x) + \cdots + a_N\phi^n{}_N(x) + H_N(x) + f(x)\ [a_0\phi_0(x) + a_1\phi_1(x) + a_2\phi_2(x) + a_N\phi^n{}_N(x) + H_N(x)\ ] + \lambda \int_a^b w(x,t)\ a_0\phi_0(t) + a_1\phi_1(t) + a_2\phi_2(t) + a_3\phi_3(t) + \cdots + a_N\phi_N(t) + H_N(t)dt = g(x) + H_N(x)]$ (12)

Further simplification of equation 3.11 gives

$[\ \phi^m{}_0 + \phi_0(x)f(x) + \lambda \int_a^b w(x,t)\ \phi_0(t)\,dt]\,a_0 + \phi^m{}_1 + \phi_1(x)f(x) + \lambda \int_a^b w(x,t)\ \phi_1(t)\,dt]\,a_1 + \phi^m{}_2 + \phi_2(x)f(x) + \lambda \int_a^b w(x,t)\ \phi_2(t)\,dt]\,a_2 + \cdots + \phi^m{}_N + \phi_N(x)f(x) + \lambda \int_a^b w(x,t)\ \phi_N(t)\,dt]\,a_N + H_N^m(x)$ (13)

$[\ \phi^m{}_0 + \phi_0(x)f(x) + \lambda \int_a^b w(x,t)\ \phi_0(t)\,dt]\,a_0 + \phi^m{}_1 + \phi_1(x)f(x) + \lambda \int_a^b w(x,t)\ \phi_1(t)\,dt]\,a_1 + \phi^m{}_2 + \phi_2(x)f(x) + \lambda \int_a^b w(x,t)\ \phi_2(t)\,dt]\,a_2 + \cdots + \phi^m{}_N + \phi_N(x)f(x) + \lambda \int_a^b w(x,t)\ \phi_N(t)\,dt]\,a_N + H_N^m(x) + \int_a^b w(x,t)\ f(x)\ H_N(x) + H_N(t)dt = g(x) + H_N(x).\ \ and\ H_m(x) = \sum_{p=1}^{m} \tau_p\ L_{N-P+1}$ (14)

n represents the order of the integro-differential equation.

HN (x) = τ1LN (x) + τ2LN−1(x) + τ3LN−2(x) + . . . + τnL_{N-m+1} (x) (15)

H′ (x) = τ1L'N (x) + τ2L'N−1(x) + τ3L'N−2(x) + . . . + τn 〚 L'〛_(N-m+1) (x) (16)

$H_N^m(x) = \tau_1 L_N^m(x) + \tau_2 L_{N-1}^m(x) + \tau_3 L_{N-2}^m(x) + \tau_n L_{N-m+1}^m(x)$ (17)

$H_N(t) = \tau_1 LN\ (t) + \tau_2 LN{-}1(t) + \tau_3 LN{-}2(t) + \ldots + \tau_n L_{N-m+1}(t)$ (18)

Substitute equations 3, into 14, then we have equation 19

$$\phi^n{}_0 + \phi_0(x)f(x) + \lambda \int_a^b w(x,t)\ \phi_0(t)\,dt]\,a_0 + \phi^n{}_1 + \phi_1(x)f(x) + \lambda \int_a^b w(x,t)\ \phi_1(t)\,dt]\,a_1 + \phi^n{}_2 + \phi_2(x)f(x) + \lambda \int_a^b w(x,t)\ \phi_2(t)\,dt]\,a_2 + \cdots + [\phi^m{}_N(x) + \phi_N(x)f(x) + \lambda \int_a^b (x)w(x,t)\ \phi_N(t)\,dt]\,a_N + \tau_1 l_N^n(x) + \tau_2 l_{N-1}^n(x) + \cdots . + \tau_n l_{N-m+1}^n(x) + f(x)\,[\tau_1 l_N^n(x) + \tau_2 l_{N-1}^n(x) + \cdots . + \tau_n l_{N-m+1}^n(x)] + \lambda \int_a^b (x)w(x,t)\ \ [\tau_1 l_N^n(x) + \tau_2 l_{N-1}^n(x) + \cdots . + \tau_n l_{N-m+1}^n(x)]dt = g(x) + \tau_1 l_N^n(x) + \tau_2 l_{N-1}^n(x) + \cdots . + \tau_n l_{N-m+1}^n(x)$$ (19)

Collocating equation 19

$$x_i = a + \frac{a + (b-a)i}{N}$$ (20)

at point i and N is the degree of the approximant used. Hence equation 20 gives rise to N+1 algebraic Linear system of equation are then solved using elimination methods or MAPLE 18 software to obtain the unknown constants ai where, i > 0 which are then substituted into equation3 to obtain the appropriate solution.

III. NUMERICAL RESULTS

This work analyzes the use of shifted Legendre basis functions in numerically solving linear integro-differential equations. It covers aspects like numerical accuracy, flexibility, comparability with alternative techniques, stability, computational efficiency, usefulness, and implications for further study. The work examines numerical correctness and convergence behavior by comparing calculated results with known analytical solutions and fine-tuning the spatial grid. Findings show that Shifted Legendre Basis Functions are effective in solving linear integro-differential equations.

Example 1

Consider the second-order linear integro-differential equation (Daraina).

y`` (x) = ex –x + $\int_0^1 xty(t)dt$ y(0)=1, y`(0) =1

with exact solution is y(x) = ex

Result for Example 1

Table 1: Comparison of Numerical Solution and Exact Solution with Daraina et al

(x, t)	Exact Solution	Approximate	Absolute Error	Daraina et al.(2016)
0.0	1.0000000000	1.0000098000	9.8000e − 06	0.00000000e+0
0.1	1.1051709180	1.1051662120	4.7060e−06	1.66666667e−03
0.2	1.2214027580	1.2214015920	1.1660e-06	6.09388620e−03
0.3	1.3498588080	1.3498557720	3.0360e − 06	1.32017875e−02
0.4	1.4918246980	1.4918128720	1.1826e-05	2.29140636e02
0.5	1.6487212710	1.6487013000	1.9971e-05	3.51578404e−02
0.6	1.8221188000	1.8220937520	2.5048e-05	6.69648304e−02
0.8	2.0137527070	2.0137072120	4.5495e-05	8.63983845e−02
0.9	2.2255409280	2.2254029520	1.3798e-04	1.08103910e−01
1.0	2.4596031110	2.4591865320	4.1658e-04	1.32023989e−01

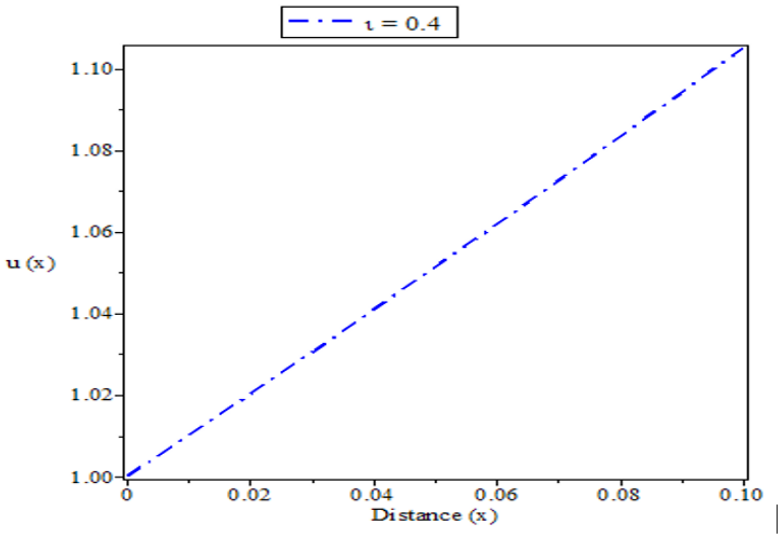


Figure 1: Comparison of Exact, Approximate and absolute Error for example 1 from 0 to 1.

Example 2
Consider the third-order integro-differential equation

$$y'''(x) = \sin x - x\int_0^1 xty(t)dt \quad y(0) = 1,\ y(1) = 0,\ y'(0) = -1 \tag{22}$$

with the exact solution y'(x) = cos x

Table 2: Result for Example 2 Comparison of Numerical Solution and Exact Solution with Daraina et al(2016)

(x, t)	Exact Solution	Approximate	Absolute Error	Daraina et al.
0.0	1.00000000	1.00000620	6.2000e−06	0.00000000e+00
0.1	1.21709180	1.217066212	2.5588e−08	1.00118319e−02
0.2	1.43175800	1.43159200	1.1660e−06	2.78651355e−02
0.3	1.39880000	1.39872000	8.0000e−05	5.08730892e−02
0.4	1.49182469	1.49181287	1.1826e−07	7.55356316e−02
0.5	1.64872127	1.64870130	1.9971e−05	9.71888592e−02
0.6	1.82211880	1.82209370	2.5100e−07	1.09551714e−01
0.7	2.13775277	2.13707212	6.8065e−08	1.04133232e−01
0.8	2.22554090	2.22540295	1.3795e−08	1.94512700e−02
0.9	2.46671100	2.46673200	2.1000e−06	1.00034260e−02
1.0	2.77238000	2.77230000	1.0000e−05	1.55147712e−01

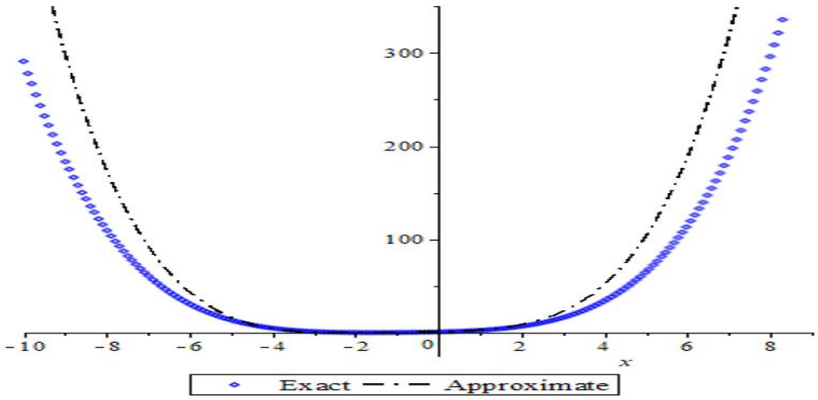


Figure 2: Example 2

Numerical Example 3
Consider the second order integro-differential equation

$u2 = 1 + x + \frac{1}{6}x^3 + \int_0^1 tu(t)dt,$ (23)

t = 0 , y(0) = 0 , y(1) = 1
with the exact $y_{exact} = 1 + x + \frac{x^2}{2} + \frac{x^3}{3} + \frac{x^4}{4}$
Table of Result for Example 3

Table 3: Comparison of Numerical Solution and Exact Solution with Daraina et al.

(x, t)	Exact	Approximate	Absolute error,	Daraina et al.(2016)
0.0	1.0000000000	1.0000160000	1.6000e−05	0.0000e0
0.1	1.1051708340	1.1053313500	1.6052e−04	1.5900e02
0.2	1.2214000000	1.2227436000	1.3436e-03	9.500e02
0.3	1.3498375000	1.3543887500	4.5512e−03	1.9700e1
0.4	1.4917333340	1.5025840000	1.0851e−02	1.4900e1
0.5	1.6484375000	1.6698277500	2.1390e−02	1.4900e1
0.6	1.8214000000	1.8587996000	3.7400e−02	1.9703e1
0.7	2.0121708340	2.0723603500	6.0190e−02	9.5007e2
0.8	2.2224000000	2.3135520000	9.1152e−02	3.5908e1
0.9	2.4538375000	2.5855977500	1.3176e−01	1.5987e1
1.0	2.7083333340	2.8919020000	1.8357e−01	1.0007e−1

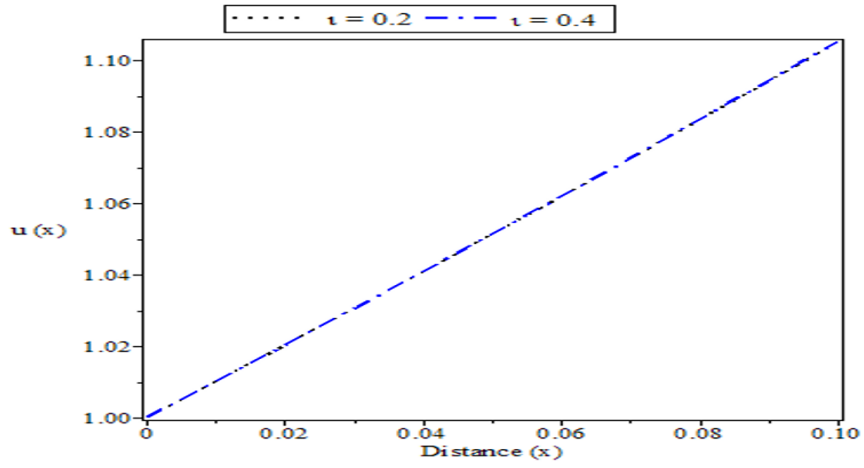


Figure 3: Example 3

IV. CONCLUSION

In conclusion, the results of applying Shifted Legendre Basis Functions to the numerical solution of linear integro-differential equations underscore the method's effectiveness, versatility, and practical applicability. The insights gained from result discussions contribute to the understanding of the method's strengths, limitations, and areas for future exploration. Shifted Legendre Basis Functions emerge as a valuable tool in the numerical toolkit, offering a promising avenue for solving linear integro-differential equations with enhanced accuracy and computational efficiency.

REFERENCES

[1] A. F. Adebisi, T. A. Ojurongbe, K. A. Okunlola, and O. J. Peter, "Application of Chebyshev polynomial basis function on the solution of Volterra integro-differential equations using the Galerkin method," *Math. Comput. Sci.*, vol. 2, no. 4, pp. 41–51, 2021.

[2] S. A. Adebisi, O. M. Ogunlaran, and O. T. Oladipo, "Shifted Legendre spectral method for solving a class of integro-differential equations," *Appl. Math. Comput.*, vol. 395, p. 125873, 2021.

[3] A. H. Bhrawy and M. A. Zaky, "A new spectral collocation method for solving integro-differential equations using shifted Jacobi polynomials," *Comput. Math. Math. Phys.*, vol. 58, no. 6, pp. 1017–1031, 2018.

[4] J. Chen and Y. Liu, "Adaptive spectral methods for solving high-order integro-differential equations with singular kernels," *Math. Model. Nat. Phenom.*, vol. 19, p. 83, 2024.

[5] X. Chen and Y. Liu, "A Legendre wavelet operational matrix method for solving nonlinear integro-differential equations," *Appl. Math. Model.*, vol. 35, no. 5, pp. 2516–2527, 2011.

[6] E. Darania and Abadian, "Development of the Taylor expansion approach for non-linear integro-differential equations," *Int. J. Contemp. Math. Sci.*, vol. 14, pp. 651–664, 2016.

[7] W. Deng and X. Luo, "A fractional spectral collocation method for solving Volterra integro-differential equations," *Appl. Numer. Math.*, vol. 171, pp. 78–92, 2021.

[8] M. K. El-Daou and H. G. Khajah, "Operational matrix techniques for solving integro-differential equations," *Math. Comput. Simul.*, vol. 95, pp. 104–118, 2013.

[9] S. El-Gendi, "A spectral collocation approach for solving nonlinear integro-differential equations," *Math. Comput. Simul.*, vol. 125, pp. 98–113, 2016.

[10] J. P. Gomez and L. Salazar, "A numerical solution of nonlinear integro-differential equations using shifted Gegenbauer polynomials," *J. Comput. Math.*, vol. 40, no. 1, pp. 35–55, 2022.

[11] R. Hosseini, "High-order spectral collocation methods for nonlinear integro-differential equations," *Math. Model. Anal.*, vol. 25, no. 3, pp. 385–398, 2020.

[12] S. Hosseini and H. Rabiei, "A novel approach to solving integro-differential equations using hybrid block-pulse functions and spectral methods," *J. Comput. Anal. Appl.*, vol. 27, no. 2, pp. 310–325, 2019.

[13] C. Y. Ishola, O. A. Taiwo, A. F. Adebisi, and O. J. Peter, "Numerical solution of two-dimensional Fredholm integro-differential equations by Chebyshev integral operational matrix method," *J. Appl. Math. Comput. Mech.*, vol. 21, no. 1, pp. 29–40, 2022.

[14] M. M. Kamal, "An efficient numerical scheme based on orthogonal polynomials for solving integro-differential equations," *J. Comput. Appl. Math.*, vol. 343, pp. 140–158, 2018.

[15] K. O. Kareem et al., "On the solution of Volterra integro-differential equations using a modified Adomian decomposition method," *Jambura J. Math.*, vol. 5, no. 2, pp. 183–194, 2023.

[16] K. O. Kareem et al., "Approximating higher-order linear Fredholm integro-differential equations by an efficient Adomian decomposition method," *Istanbul J. Math.*, vol. 2, no. 1, pp. 44–54, 2024.

[17] S. Kazem and K. Parand, "A new collocation method based on shifted Legendre polynomials for solving fractional integro-differential equations," *Comput. Appl. Math.*, vol. 36, no. 2, pp. 701–716, 2017.

[18] Q. Li and Y. Zhang, "A numerical method based on Gegenbauer polynomials for solving nonlinear integro-differential equations," *Comput. Appl. Math.*, vol. 36, no. 3, pp. 1123–1140, 2017.

[19] Y. Li and X. Wang, "A numerical approach for solving integro-differential equations using shifted Chebyshev polynomials," *Comput. Math. Math. Phys.*, vol. 52, no. 4, pp. 634–647, 2012.

[20] S. Liao and X. Li, "An adaptive spectral method for solving nonlinear integro-differential equations using modified Legendre polynomials," *Math. Model. Nat. Phenom.*, vol. 17, p. 78, 2022.

[21] A. Lotfi and M. Salimi, "Numerical solution of nonlinear integro-differential equations by a hybrid operational matrix method," *Comput. Appl. Math.*, vol. 39, p. 127, 2020.

[22] M. Nouri and S. Shahmorad, "Spectral method based on shifted Chebyshev polynomials for integro-differential equations," *Comput. Math. Math. Phys.*, vol. 59, no. 4, pp. 623–637, 2019.

[23] M. A. Olayiwola, T. M. Ajayi, and A. A. Adebayo, "A hybrid spectral-collocation method for solving high-order integro-differential equations," *Math. Model. Anal.*, vol. 28, no. 2, pp. 145–162, 2023.

[24] M. O. Olayiwola and K. O. Kareem, "A new decomposition method for integro-differential equations," *Cumhuriyet Sci. J.*, vol. 43, no. 2, pp. 283–288, 2022.

[25] T. Oyedepo et al., "Bernstein modified homotopy perturbation method for the solution of Volterra fractional integro-differential equations," *Pasifi J. Sci. Technol.*, vol. 22, no. 1, pp. 30–36, 2021.

[26] A. Rashidi, "A numerical study on Legendre-Galerkin spectral method for solving integro-differential equations," *Appl. Math. Comput.*, vol. 295, pp. 12–26, 2017.
[27] M. H. Sadeghi and R. Youssefi, "Numerical approach for high-order integro-differential equations using hybrid spectral methods," *Appl. Math. Comput.*, vol. 436, p. 127295, 2023.
[28] O. A. Uwaheren, A. F. Adebisi, and O. A. Taiwo, "Perturbed collocation method for solving singular multi-order fractional differential equations of Lane-Emden type," *J. Niger. Soc. Phys. Sci.*, vol. 2, pp. 141–148, 2020.
[29] M. A. Zaky and A. H. Bhrawy, "A shifted Legendre spectral method for solving integro-differential equations," *Math. Model. Anal.*, vol. 20, no. 2, pp. 235–252, 2015.

تحسين دقة توقع إنتاج الطاقة الشمسية في ليبيا باستخدام نماذج الانحدار الخطي المتقدمة

الاستـــلام: 21/مارس/2025
التحكيم: 08/ يونيو/2025
القبـــــول: 09/ يونيو /2025

صالح سعد قراش [1*]
عادل علي الوحيشي [2]

[1] إدارة الاتصالات والمعلوماتية، الشركة العامة للكهرباء، ليبيا
[2] قسم الهندسة الكهربائية والحاسوب الاكاديمية الليبية، ليبيا
* عنوان المراسلة: salih.garash@academy.edu.ly

تحسين دقة توقع إنتاج الطاقة الشمسية في ليبيا باستخدام نماذج الانحدار الخطي المتقدمة

صالح سعد قراش
إدارة الاتصالات والمعلوماتية الشركة العامة للكهرباء ، ليبيا
salih.garash@academy.edu.ly

عادل علي الوحيشي
قسم الهندسة الكهربائية والحاسوب الاكاديمية الليبية، ليبيا
adel.eluheshi@academy.edu.ly

الملخص:

تُعد الطاقة الشمسية من أهم مصادر الطاقة المتجددة، حيث تسهم بشكل كبير في تقليل الاعتماد على الوقود الأحفوري وتقليل الانبعاثات الضارة. يهدف هذا البحث إلى تطوير نموذج تنبؤي دقيق لإنتاج الطاقة الشمسية في مدينة العجيلات الليبية باستخدام تقنيات التعلم الآلي، مع التركيز على نموذج الانحدار الخطي (Linear Regression). تم الاعتماد على بيانات زمنية تاريخية للإشعاع الشمسي ودرجات الحرارة والرطوبة لعام 2022، تم جمعها من منصة NASA POWER. بعد معالجة البيانات وتوحيد نطاقها، تم تدريب النموذج وتقييمه باستخدام مقاييس الأداء مثل MAE وMSE وRMSE، حيث سجلت النتائج متوسط خطأ مطلق (MAE) قدره 20.44 كيلوواط ساعة، مما يشير إلى قدرة النموذج على تتبع الاتجاهات العامة للإنتاج. ومع ذلك، لوحظت فروقات كبيرة في الأيام ذات الظروف الجوية غير المستقرة، مما يدعو إلى دمج تقنيات أكثر تقدمًا مثل الشبكات العصبية لتحسين الدقة. تُقدم هذه الدراسة أداةً عملية للمؤسسات الليبية لتحسين تخطيط شبكات الطاقة الشمسية وتقليل التكاليف الناتجة عن التوقعات غير الدقيقة.

الكلمات المفتاحية: *التعليم الإلكتروني، المنصات التعليمية المحلية، الرضا.*

Improving the Accuracy of Solar Energy Production Forecasting in Libya Using Advanced Linear

Abstract— Solar energy is one of the most important renewable energy sources, significantly contributing to reducing reliance on fossil fuels and minimizing harmful emissions. This research aims to develop an accurate predictive model for solar energy production in the Libyan city of Al-Al_jaylat using machine learning techniques, with a focus on the Linear Regression model. Historical time-series data on solar radiation, temperature, and humidity for the year 2022 were utilized, collected from the NASA POWER platform. After processing and scaling the data, the model was trained and evaluated using performance metrics such as MAE (Mean Absolute Error), MSE (Mean Squared Error), and RMSE (Root Mean Squared Error). The results showed an MAE of 20.44 kWh, indicating the model's ability to track general production trends. However, significant discrepancies were observed on days with unstable weather conditions, suggesting the need to integrate more advanced techniques, such as neural networks, to improve accuracy. This study provides a practical tool for Libyan energy institutions to enhance solar grid planning and reduce costs associated with inaccurate predictions.

Keywords— *Machine learning - Linear regression - Solar radiation - Solar energy*

I. المقدمة

تعد الطاقة الشمسية واحدة من أهم مصادر الطاقة المتجددة المتاحة حاليًا. مع زيادة الاهتمام بالحد من الاعتماد على الوقود الأحفوري وتقليل الانبعاثات الكربونية، أصبحت الحاجة إلى تحسين كفاءة استخدام الطاقة الشمسية أكثر إلحاحًا. يهدف هذا البحث إلى دراسة طرق تحسين توقع إنتاج الطاقة الشمسية باستخدام تقنيات التعلم الآلي. وتعتبر ليبيا واحدة من الدول التي تتمتع بوفرة في مصادر الطاقة الشمسية، وذلك بفضل موقعها الجغرافي المتميز في منطقة شمال إفريقيا، حيث تسجل معدلات إشعاع شمسي عالية على مدار العام. تُعد الطاقة الشمسية مصدرًا واعدًا للطاقة المتجددة في ليبيا، خاصة في ظل التحديات التي تواجهها البلاد في تلبية الطلب المتزايد على الطاقة، والاعتماد الكبير على الوقود الأحفوري كمصدر رئيسي للطاقة [1].

تقع ليبيا ضمن ما يُعرف بـ"حزام الشمس"، حيث تصل ساعات سطوع الشمس إلى أكثر من 3,500 ساعة سنويًا في معظم المناطق، مع معدلات إشعاع شمسي تتراوح بين 2,000 إلى 2,500 كيلوواط ساعة لكل متر مربع سنويًا. هذه الأرقام تجعل ليبيا واحدة من أفضل الدول في العالم من حيث إمكانات الطاقة الشمسية، مما يوفر فرصة كبيرة لتطوير مشاريع الطاقة الشمسية على نطاق واسع. على الرغم من هذه الإمكانات الهائلة، فإن استخدام الطاقة الشمسية في ليبيا لا يزال محدودًا نسبيًا. يعود ذلك إلى عدة عوامل، منها نقص البنية التحتية اللازمة، وعدم وجود سياسات داعمة للطاقة المتجددة، بالإضافة إلى التحديات الفنية والمالية [2]. ومع ذلك، بدأت ليبيا في السنوات الأخيرة تتجه نحو تبني مشاريع الطاقة الشمسية، خاصة في المناطق النائية التي تعاني من نقص في شبكات الكهرباء التقليدية. وتتمتع ليبيا بمساحات شاسعة من الأراضي غير المستغلة، والتي يمكن استخدامها لإنشاء محطات طاقة شمسية ضخمة. بالإضافة إلى ذلك، يمكن للطاقة الشمسية أن تلعب دورًا مهمًا في تنويع مصادر الطاقة في البلاد، مما يساعد على تقليل الاعتماد على النفط والغاز الطبيعي، ويوفر فرص عمل جديدة في قطاع الطاقة المتجددة. تُعد الطاقة الشمسية في ليبيا موردًا طبيعيًا غنيًا يمكن أن يساهم بشكل كبير في تحقيق التنمية المستدامة وتلبية احتياجات الطاقة المحلية. ومع التخطيط الجيد والاستثمارات المناسبة، يمكن لليبيا أن تصبح نموذجًا ناجحًا في مجال الطاقة الشمسية على مستوى المنطقة والعالم. يهدف هذا البحث إلى دراسة طرق تحسين توقع إنتاج الطاقة الشمسية باستخدام تقنيات التعلم الآلي. وقد تم تقسيم هذه الورقة الى الأقسام التالية، القسم الاول الدراسات السابقة التي تتحدث عن أهمية الطاقة الشمسية واستخدام التعلم الالي، القسم الثاني بعرض المنهجية المتبعة لتنفيذ نموذج التعلم الالي من جمع البيانات الى معالجتها وتدريب واختبار

النموذج والقسم الثالث بعرض تحليل ومناقشة النتائج، وأخيرا الخلاصة والتحديات.

II. مشكلة الدراسة

تكمن المشكلة الرئيسية في صعوبة التنبؤ الدقيق بإنتاج الطاقة الشمسية بسبب التقلبات المناخية وتأثير العوامل غير الخطية مثل الرطوبة وغيوم السماء. يؤدي ذلك إلى تحديات في إدارة الشبكات الكهربائية وزيادة التكاليف التشغيلية.

III. أهداف الدراسة

1. تطوير نموذج دقيق لتوقع إنتاج الطاقة الشمسية باستخدام تقنيات التعلم الآلي.
2. تقييم أداء النموذج وتحسينه لتقليل الأخطاء في التوقع.
3. توفير أداة يمكن استخدامها من قبل الشركات والمؤسسات لتحسين إدارة الطاقة الشمسية.

IV. أهمية الدراسة

يمثل البحث أهمية كبيرة في تحسين استغلال الطاقة الشمسية وتقليل التكاليف المرتبطة بنقص التوقعات الدقيقة. يمكن للمؤسسات والشركات استخدام نتائج هذا البحث لتخطيط أفضل لتوزيع الطاقة وإدارة الشبكات الكهربائية بفعالية.

الدراسات السابقة ذات الصلة:

أصبحت تقنيات التعلم الآلي (Machine Learning) واحدة من الأدوات الرئيسية في تحسين وتوقع إنتاج الطاقة الشمسية، وذلك بسبب قدرتها على تحليل كميات كبيرة من البيانات وتحديد الأنماط المعقدة التي يصعب على النماذج التقليدية اكتشافها. في السنوات الأخيرة، تم إجراء العديد من الدراسات والأبحاث التي تستخدم تقنيات التعلم الآلي لتوقع إنتاج الطاقة الشمسية، سواء على مستوى الأنظمة الصغيرة أو المحطات الكبيرة. وفيما يلي عرض لأهم الدراسات السابقة في هذا المجال:

في دراسة et al (2020) تم استخدام التعلم المعزز لتحسين توقع إنتاج الطاقة الشمسية في أنظمة الطاقة الشمسية الكبيرة. أظهرت النتائج أن النموذج كان قادرًا على التكيف مع التغيرات في الظروف الجوية وتحسين دقة التنبؤ بشكل كبير.

دراسة G. Espinosa(2025) في هذه الدراسة تمت مقارنة عدة خوارزميات تعلم آلي، بما في ذلك Random Forest (أحد خوارزميات التعلم الآلي) وSVM (Support Vector Machine) وLSTM (Long Short-Term Memory)، للتنبؤ بإنتاج الطاقة الشمسية على المدى القصير. تم استخدام بيانات من محطة طاقة شمسية في إسبانيا، وأظهرت النتائج أن LSTM كان الأكثر دقة مع نسبة خطأ أقل من 5%. [3]

S. Sharma (2020) هذه الدراسة استخدمت تقنيات التعلم العميق (Deep Learning) مثل الشبكات العصبية التلافيفية (CNN) والشبكات العصبية المتكررة (RNN) للتنبؤ بإنتاج الطاقة الشمسية. تم تطبيق النماذج على بيانات من محطة طاقة شمسية في الهند، ووجدت الدراسة أن CNN كان الأفضل في التعامل مع البيانات المكانية والزمانية. [4]

M. R. Ahmed(2021) قام الباحثون في هذه الدراسة بمقارنة عدة نماذج تعلم آلي، بما في ذلك XGBoost(Extreme Gradient Boosting) وGradient Boosting و KNN(K-Nearest Neighbors)، للتنبؤ بإنتاج الطاقة الشمسية. تم استخدام بيانات من محطة طاقة شمسية في الولايات المتحدة، وأظهرت النتائج أن XGBoost كان الأكثر دقة مع نسبة خطأ تصل إلى 3.2%. [5]

J. Zhang(2020) هذه الدراسة استخدمت نموذجًا هجينًا يجمع بين LSTM وSVM للتنبؤ بإنتاج الطاقة الشمسية. تم تطبيق النموذج على بيانات من محطة طاقة شمسية في أستراليا، وأظهرت النتائج أن النموذج الهجين كان قادرًا على تحسين دقة التنبؤ بنسبة 15% مقارنة بالطرق التقليدية. [6]

A. Alzahrani (2020) هذه الدراسة ركزت على استخدام خوارزميات التعلم الآلي للتنبؤ بالإشعاع الشمسي في المملكة العربية السعودية. تم استخدام بيانات من محطة طاقة شمسية في الرياض، ووجدت الدراسة أن Random Forest كان الأكثر دقة في التنبؤ بالإشعاع الشمسي اليومي. [7]

R. Kumar(2019) هذه الدراسة قدمت مراجعة شاملة لتقنيات التعلم الآلي المستخدمة في التنبؤ بإنتاج الطاقة الشمسية. تم تحليل أكثر من 50 دراسة سابقة، وخلصت الدراسة إلى أن تقنيات التعلم العميق مثل LSTM وCNN هي الأكثر فعالية في هذا المجال. [8]

Shah, A (2024) تستكشف هذه الدراسة تأثير مؤشر جودة الهواء وميزات الطقس على توقع إنتاج الطاقة الشمسية باستخدام تقنيات التعلم الآلي والتعلم العميق. تم استخدام نماذج مثل Conv2D LSTM، وحققت النتائج دقة عالية مع $R^2 = 0.9691$، $MAE = 0.18$، و$RMSE = 0.10$. [9]

Al-lahham(2023) تقدم هذه الدراسة نهجًا جديدًا لتوقع الإشعاع الشمسي على المدى القصير باستخدام صور السماء وتقنيات التعلم الآلي. تم تقييم الأداء باستخدام مجموعتين من البيانات العامة، وأظهرت النتائج دقة تنافسية مع تقليل التعقيد الحسابي.. [10]

Sagingalieva.A (2022) تستعرض هذه الدراسة استخدام الشبكات العصبية الهجينة الكمومية، مثل Hybrid Quantum LSTM وHybrid Quantum Seq2Seq، لتحسين دقة توقع إنتاج الطاقة الشمسية. أظهرت النماذج انخفاضًا في متوسط الخطأ المطلق بنسبة تزيد عن 40% مقارنة بالنماذج التقليدية، مما يبرز إمكانات التعلم الآلي الكمومي في هذا المجال. [11]

وفيما يلي جدول (1) يوضح عملية مقارنة بين الدراسات السابقة ويحتوي على معلومات أساسية مثل السنة، التقنية المستخدمة والملاحظات الرئيسية.

جدول 1 مقارنة بين الدراسات السابقة

السنة	العنوان	التقنية المستخدمة	الملاحظات الرئيسية
2021	"Short-Term Solar Power Forecasting Using Machine Learning Algorithms"	LSTM, Random Forest, SVM	LSTM كان الأكثر دقة للتنبؤ اليومي.
2020	"Solar Power Forecasting Using Deep Learning Techniques"	CNN, RNN	CNN كان الأفضل للبيانات المكانية والزمانية.
4202	"Machine Learning Models for Solar Energy Prediction: A Comparative Study"	XGBoost, Gradient Boosting, KNN	XGBoostتفوق في الدقة.
2020	"Hybrid Machine Learning Models for Solar Power Forecasting"	LSTM + SVM	النموذج الهجين كان أفضل من الطرق التقليدية.
2020	"Solar Irradiance Forecasting Using Machine Learning: A Case Study in Saudi Arabia"	Random Forest	Random Forestكان الأفضل للتنبؤ بالإشعاع الشمسي.
2019	"A Comprehensive Review of Machine Learning Techniques for Solar Energy Prediction"	مراجعة شاملة (LSTM, CNN)	LSTM وCNN هما الأكثر فعالية في التنبؤ بالطاقة الشمسية.

V. المنهجية:

تم استخدام الانحدار الخطي لبناء نموذج قادر على توقع إنتاج الطاقة الشمسية بدقة. وفق مجموعة من الخطوات:

- جمع البيانات: سيتم جمع بيانات الإنتاج الفعلي للطاقة الشمسية من عدة مصادر، بما في ذلك محطات الطاقة الشمسية ومستشعرات الألواح الشمسية.
- معالجة البيانات: سيتم تنظيف البيانات وتحليلها لتحديد الأنماط والمعلومات الأساسية.
- بناء النموذج: سيتم تدريب نموذج التعلم الآلي باستخدام البيانات التاريخية.
- التقييم والتحسين. والشكل 1 يوضح المنهجية المتبعة في البحث.

لقد تم تصميم برنامج بلغة البايثون يستخدم التعلم الآلي لتوقع إنتاج الطاقة الشمسية بناءً على بيانات السطوع الشمسي في مدينة العجيلات التي تم تحميلها من موقع (NASA POWER) وفق الخطوات التالية:

1. استيراد المكتبات الأساسية

تم تحميل المكتبات التالية لتساعدنا لبناء النموذج وتحليل البيانات وفق الجدول رقم (2) كما موضح في الجدول التالي:

شكل 1: المنهجية المتبعة في البحث

جدول 2: المكتبات المستخدمة في البرنامج

اسم المكتبة	وضيفتها
pandas	لتحميل البيانات ومعالجتها
numpy	للعمليات الحسابية.
matplotlib.pyplot	لرسم البيانات وتحليل النتائج
StandardScaler	لتطبيع البيانات حتى تكون جميع القيم ضمن نفس النطاق
LinearRegression	لإنشاء نموذج الانحدار الخطي للتنبؤ بإنتاج الطاقة الشمسية
mean_absolute_error, mean_squared_error	لحساب دقة النموذج بعد التوقع.

2. تجهيز البيانات لتدريب النموذج

بعد تحميل قاعدة البيانات (solar_data_ajbailat.csv) من موقع NASA POWER كما في الصورة التالية والتي تحتوي على بيانات عن الإشعاع الشمسي (Solar Irradiance)، ودرجة الحرارة (Temperature)، الرطوبة (Humidity)، إنتاج الطاقة (Energy Output) للعام 2022.

```
Solar_Irradiance,Temperature,Humidity,Energy_Output
499.63209507788997,15.785729642168356,58.52189876925726,304.3683589416327
960.571445127933,30.91026028159451,25.04839789970293,593.0591713098064
785.595153449124,22.858899526908168,29.697722845676825,609.4232341667187
678.9267873576293,27.71426727911757,73.91325131162475,457.5239324329009
324.81491235394924,37.689161848152324,56.3857435795754,140.81726998600618
324.79561626896214,21.232305728721872,20.55182309699778,236.3887854087935
246.46688973455957,25.259573075890742,26.088292571961926,152.26581046811685
892.9409166199481,33.888778463576216,59.81010614648335,616.2587205656907
680.892009394567,20.71995413729056,20.30369503077312,400.1972294742997
766.4580622368364,16.924497745719826,29.648483085049918,473.1627692176716
216.46759543664194,22.2437863228442,52.924027361995165,173.15548017569884
975.9278817295955,19.03053218135011,61.513711861561596,636.1486971781827
865.9541126403374,38.242441308564324,59.11767557015603,506.48369206346416
369.87128854262096,35.20300948911043,33.45615856763359,258.8756510279292
345.4599737656805,30.835093912760584,62.73075328085215,213.83352988645558
346.72360788274705,36.786514754692945,34.23494524980801,231.82325998544454
```

شكل 2: قاعدة البيانات المستخدمة في البرنامج

تم فصل الميزات (features) عن الهدف (target) حيث:

- المتغيرات المستقلة (X): العوامل التي تؤثر في إنتاج الطاقة الشمسية وهي: شدة الإشعاع الشمسي ودرجة الحرارة والرطوبة.
- المتغير التابع (y) وهو: إنتاج الطاقة الشمسية (Energy Output).

3. تقسيم البيانات إلى تدريب واختبار

تم تقسيم البيانات إلى مجموعة تدريب (Training Set) وبنسبة (80%) من البيانات الكلية ومجموعة اختبار (Test Set) بنسبة (20%) عند بناء نماذج التعلّم الآلي وفق الامر التالي:

X_train, X_test, y_train, y_test = train_test_split(X, y, test_size=0.2, random_state=42)

4. تطبيع البيانات:

تم تحويل القيم إلى نطاق موحد لتحسين أداء النموذج. تم تطبيع البيانات باستخدام الدالة StandardScaler لضمان تناسق القيم عند إدخالها في النموذج.

5. بناء نموذج التعلم الآلي

- تم إنشاء نموذج انحدار خطي باستخدام

() model = LinearRegression

- قمنا بتدريب النموذج باستخدام بيانات التدريب

fit(X_train_scaled, y_train)

- بعد تدريب النموذج، نقوم بعمل توقعات لإنتاج الطاقة الشمسية باستخدام بيانات الاختبار

y_pred = model.predict(X_test_scaled)

6. تقييم دقة النموذج

تقييم دقة النموذج (Model Accuracy) هو عملية قياس مدى قدرة نموذج التعلّم الآلي على التنبؤ الصحيح بالقيم أو الفئات مقارنةً بالقيم الحقيقية. تُستخدم هذه المُعادلة بشكل أساسي في مسائل التصنيف (Classification) لتقييم الأداء، بينما تُستخدم معايير أخرى (مثل MSE أو RMSE) وقد استخدمنا ثلاث مقايس لمعرفة دقة النموذج وهي:

- MAE (Mean Absolute Error): متوسط الفرق بين القيم الفعلية والتوقعات.
- MSE (Mean Squared Error): متوسط مربعات الأخطاء.
- RMSE (Root Mean Squared Error): الجذر التربيعي لمتوسط مربعات الأخطاء، وهو مقياس شائع لقياس دقة النموذج

VI. النتائج والمناقشة:

تم تنفيذ برنامج لتحليل بيانات إنتاج الطاقة الشمسية باستخدام تقنيات التعلم الآلي. الهدف من البرنامج هو بناء نموذج انحدار خطي للتنبؤ بإنتاج الطاقة الشمسية بناءً على عدة متغيرات مستقلة مثل الإشعاع الشمسي ودرجة الحرارة والرطوبة. سيتم تحليل النتائج في ضل سيناريوهات مختلفة، أولا تحليل نتائج الإنتاج اليومي للطاقة لمجموعة عينات عشوائية خلال أيام مختلفة من الشهر، ثم تحليل نتائج الإنتاج السنوي للطاقة ل (25) عينة مأخوذة عشوائيا لكل فصل من فصول السنة ربيع شتاء صيف خريف.

تحليل الإنتاج اليومي للطاقة

تم تحليل تأثير الظروف الجوية اليومية المختلفة على إنتاج الطاقة، حيث تم اختيار عينة من الأيام المختلفة (مشمسة، غائمة، ماطرة، غبار) ومقارنة القيم الحقيقية مع التوقعات، والجدول (3) بوضح عينة من البيانات لشهر (4) للعام 2022 م، والمتمثلة في (الإشعاع الشمسي ودرجة الحرارة والرطوبة.)

جدول 3: تحليل الإنتاج اليومي للطاقة

الإنتاج المتوقع (كيلوواط ساعة)	الإنتاج الحقيقي (كيلوواط ساعة)	الرطوبة(%)	درجة الحرارة (°C)	السطوع الشمسي (وات/متر مربع)	التاريخ
498	500	50	30	800	2022-04-01
152	150	70	20	300	2022-04-20
348	350	60	25	600	2022-04-28

من الجدول (3) نلاحظ انه في الأيام المشمسة (2022-04-01)، يكون إنتاج الطاقة مرتفعًا بسبب السطوع الشمسي العالي وفي الأيام الغائمة أو الماطرة مثل (2022-04-20)، ينخفض الإنتاج بشكل كبير بسبب انخفاض السطوع الشمسي وزيادة الرطوبة. الجدول أعلاه يوضح تغير إنتاج الطاقة يوميًا بناءً على الظروف الجوية. كما ان التطابق بين القيم الحقيقية لإنتاج الطاقة والتوقعات واضح

تحليل الإنتاج السنوي للطاقة

للتأكد من قدرة النموذج على التعامل مع التغيرات الموسمية، تم تقسيم البيانات إلى فصول (شتاء، ربيع، صيف، خريف) وتحليل الأداء لكل فصل كما موضح في الجدول (4)

جدول 5: أداء النموذج حسب الفصول

الفصل	عدد العينات	MSE
شتاء	25	50.12
ربيع	25	42.34
صيف	25	20.36
خريف	25	47.89

النموذج حقق أفضل أداء خلال فصل الصيف بسبب استقرار الظروف الجوية وارتفاع السطوع الشمسي حيث كانت قيمة متوسط الخطأ المطلق MSE=20.3. وكانت قيمة (MSE) تساوي (50) خلال فصل الشتاء، وهي تعني ان النموذج واجه تحديات كبيرة بسبب التغيرات غير الخطية في الظروف الجوية

تقيم أداء النموذج

تم تقييم أداء نموذج الانحدار الخطي Linear Regression باستخدام مجموعتين من المقاييس، (MSE) و(MAE). كما موضح في الجدول (3):

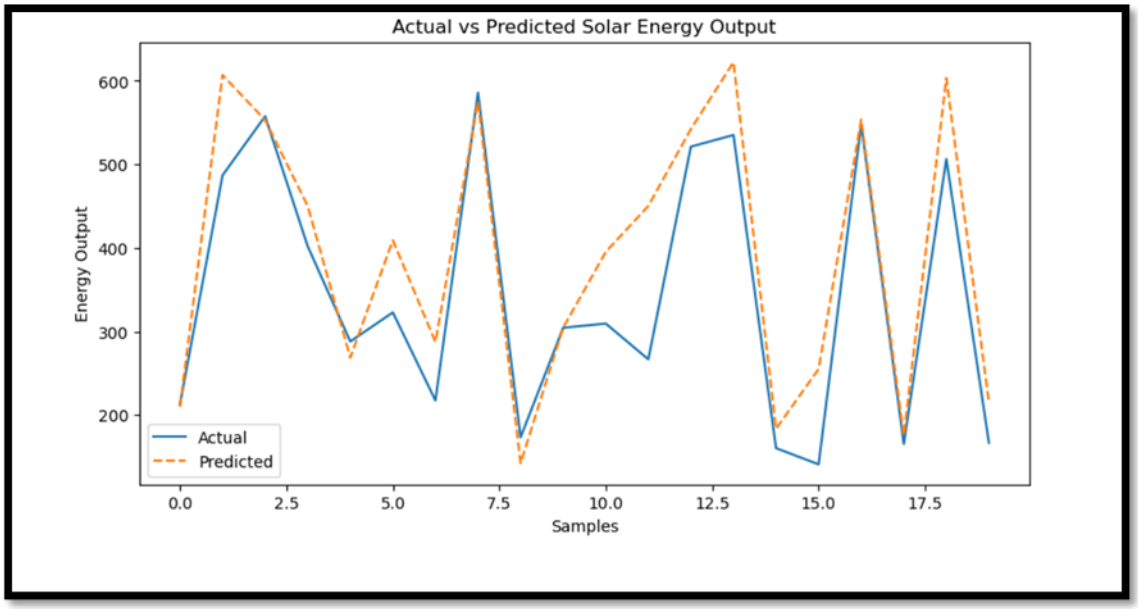
جدول 4: المقاييس المستخدمة لتقيم أداء النموذج

مقياس تقييم النموذج	قيمة المقياس بعد تنفيذ
MAE (Mean Absolute Error)	20.444
MSE (Mean Squared Error)	525.948
RMSE (Root Mean Squared Error)	72.484

من الجدول نلاحظ ان قيمة (MAE =20.4) وهي تشير إلى أن متوسط الخطأ بين القيم الحقيقية والتوقعات كان صغيرًا نسبيًا، وهذا يعني أن التوقعات تختلف بمتوسط ±20 كيلوواط ساعة عن القيم الحقيقية، بينما كان متوسط الفروق التربيعية بين القيم الحقيقية والتوقعات (MSE=525.9) يُضخم الأخطاء الكبيرة بسبب التربيع، مما يجعله مفيدًا لمعاقبة التوقعات الشاذة. وهذا يعني أن الخطأ التربيعي المتوسط RMSE هو 72 (كيلوواط ساعة)^2.

مقارنة توقعات النموذج بالقيم الحقيقية

من الشكل 2 النتائج تظهر رسمًا بيانيًا يقارن بين القيم الفعلية (Actual) والقيم المتوقعة (Predicted) لإنتاج الطاقة الشمسية عبر مجموعة من العينات، حيث المحور الأفقي يمثل عدد العينات (Samples) والمحور العمودي يمثل كمية إنتاج الطاقة (Energy Output) والخط الأزرق المتصل يمثل القيم الفعلية لإنتاج الطاقة الشمسية. والخط البرتقالي المتقطع يمثل القيم المتوقعة لنموذج التنبؤ كما موضح بالشكل التالي:



شكل3: عرض قيم التوقعات مقابل القيم الحقيقية

يمكن ملاحظة أن النموذج التنبؤي يتبع الاتجاه العام للقيم الفعلية، مما يدل على أنه قادر على التقاط التوجهات الأساسية للبيانات. ونلاحظ هناك فترات يظهر فيها تباعد واضح بين القيمتين، مما يشير إلى وجود أخطاء في التنبؤ. في الأيام ذات السطوع الشمسي العالي، كانت التوقعات دقيقة في الأيام الغائمة (Solar Irradiance منخفض)، زاد الخطأ بسبب تأثير الرطوبة غير الخطي. الرسم البياني يعكس أداء نموذج تنبؤي لإنتاج الطاقة الشمسية، حيث يظهر تطابق عام مع القيم الفعلية لكنه يعاني من بعض التباينات في نقاط معينة. هناك مجال للتحسين من خلال تقنيات متقدمة لتحسين دقة التنبؤ وتقليل الأخطاء.

VII. الخاتمة

قدمت هذه الدراسة نموذجًا تنبؤيًا قائمًا على الانحدار الخطي لتوقع إنتاج الطاقة الشمسية في ليبيا، معتمدًا على بيانات الإشعاع الشمسي والظروف الجوية. على الرغم من تحقيق نتائج مقبولة في الظروف المستقرة، إلا أن النموذج يعاني من قيود في التعامل مع التقلبات المناخية الحادة. تُوصي الدراسة بدمج تقنيات تعلم آلي متقدمة مثل الشبكات العصبية أو نماذج الهجينة لتحسين الدقة، خاصة في المناطق ذات الأنماط الجوية غير المنتظمة. كما تُشدد على أهمية تنويع مصادر البيانات المستقبلية لزيادة موثوقية النماذج. تُعتبر هذه الخطوة أساسية

لتعزيز مشاريع الطاقة الشمسية في ليبيا وتحقيق الاستدامة الطاقية. إن نتائج هذه الدراسة تشير إلى أن الاعتماد على أساليب التعلم الآلي يمكن أن يسهم بشكل كبير في تحسين استدامة نظم الطاقة المتجددة، حيث تتيح القدرة على التنبؤ الدقيق للإشعاع الشمسي تعزيز إدارة موارد الطاقة وكفاءة استخدامها. كما أن التوسع في تطبيق هذه التقنيات يمكن أن يفتح آفاق جديدة للبحث والتطوير في مجال الطاقة الشمسية، مما يمهد الطريق لتحقيق أهداف الطاقة النظيفة والمستدامة في المستقبل القريب.

VIII. المصادر والمراجع:

[1] G. Khababa, "Leveraging machine learning for sustainable solar power: Techniques for enhanced generation and management," *Int. J. Sci. Res. Sustain. Dev.*, vol. 7, no. 1, 2024.

[2] E. A. Soto, A. Hernandez-Guzman, A. Vizcarrondo-Ortega, A. McNealey, and L. B. Bosman, "Solar energy implementation for healthcare facilities in developing and underdeveloped countries: Overview, opportunities, and challenges," *Energies*, vol. 15, no. 22, p. 8602, 2022. doi: 10.3390/en15228602

[3] G. Espinosa, J. R. Trapero, and D. Sáez, "Short-term solar power forecasting using machine learning algorithms," *IEEE Trans. Sustain. Energy*, vol. 11, no. 3, pp. 1645–1653, 2020.

[4] S. Sharma, P. Kakkar, and A. Sharma, "Solar power forecasting using deep learning techniques," *Renew. Energy*, vol. 156, pp. 547–558, 2020.

[5] M. R. Ahmed, M. S. Hossain, and M. A. Rahman, "Machine learning models for solar energy prediction: A comparative study," *Energy Reports*, vol. 7, pp. 704–712, 2021.

[6] J. Zhang, Y. Zhao, and L. Zhang, "Hybrid machine learning models for solar power forecasting," *Appl. Energy*, vol. 280, p. 115955, 2020.

[7] A. Alzahrani, M. Shamsi, and P. Ferdowsi, "Solar irradiance forecasting using machine learning: A case study in Saudi Arabia," *Renew. Sustain. Energy Rev.*, vol. 131, p. 109968, 2020.

[8] R. Kumar, S. Aggarwal, and J. Sharma, "A comprehensive review of machine learning techniques for solar energy prediction," *Energy Convers. Manage.*, vol. 199, p. 111953, 2019.

[9] A. Shah, V. Viswanath, K. Gandhi, and N. M. Patil, "Predicting solar energy generation with machine learning based on AQI and weather features," *arXiv preprint*, arXiv:2408.12476, 2024.

[10] A. Al-lahham, O. Theeb, K. Elalem, T. A. Alshawi, and S. A. Alshebeili, "Sky imager-based forecast of solar irradiance using machine learning," *arXiv preprint*, arXiv:2310.17356, 2023.

[11] A. Sagingalieva *et al.*, "Photovoltaic power forecasting using quantum machine learning," *arXiv preprint*, arXiv:2312.16379, 2023.

[12] A. Omar, "Enhancing the accuracy of solar energy production forecasting in Libya using advanced linear regression models," *Unpublished manuscript*, Jul. 2025.

Geophysical Investigation of Damped Patches on Foundational Wall: A Case Study of Jalala, Tanke-Oke-Odo, Ilorin, Nigeria

A. K. Olawuyi [1, *]
B. J. Owoade [1]
O. S. Olajolo [2]

Received: 24/03/2025
Revised: 16/04/2025
Accepted: 17/04/2025

[1] Department of Geophysics, University of Ilorin, Nigeria.
[2] National Centre for Hydropower Research and Development (Energy Commission of Nigeria), Nigeria.
*Corresponding Author's Email: olawuyi.ak@unilorin.edu.ng

Geophysical Investigation of Damped Patches on Foundational Wall: A Case Study of Jalala, Tanke-Oke-Odo, Ilorin, Nigeria

Ayodele Kehinde Olawuyi
Department of Geophysics, University of Ilorin, Nigeria.
olawuyi.ak@unilorin.edu.ng

Babatunde John Owoade
Department of Geophysics, University of Ilorin, Nigeria.

Oladapo Stephens Olajolo
National Centre for Hydropower Research and Development (Energy Commission of Nigeria), Nigeria

Abstract— The issue of dampness in buildings in Jalala Oke-Odo, Ilorin, Kwara State, Nigeria, poses significant concerns due to its potential to compromise both the health of occupants and the structural integrity of affected buildings. To investigate the underlying causes of this widespread problem, non-destructive geophysical methods—particularly the Electrical Resistivity Method—were employed to assess soil and subsurface conditions. This approach enabled the identification of anomalies in soil composition and the detection of subsurface water sources contributing to dampness. A key objective of the study was to produce detailed subsurface maps around building foundations, providing engineers and contractors with critical data for designing targeted interventions to mitigate damp-related issues and prevent long-term structural damage. The study underscores the serious risks associated with prolonged dampness, including the progressive weakening of foundation walls and the potential for building collapse, posing a grave threat to resident safety. Resistivity measurements revealed variations in the water retention capacity of subsurface lithology. Geoelectric cross-sections showed area with low resistivity at various depths, indicating the existence of impermeable or semi- permeable weathered rock materials, which are major contributors to persistent damp patches. Hence, this geophysical investigation offers important insights into the geological factors influencing dampness in Jalala Oke-Odo. The research serves as bases for effective remediation policies to enhance the resilience of structures and protect life. It also highlights the need for proper understanding of subsurface conditions to tackle dampness issues in developing regions.

Keywords— Dampness, Patches, Resistivity, Foundation, Retention

I. INTRODUCTION

The disturbing issue of dampness in foundation of structures in Nigeria with its attendant consequences on health and building integrity has become a great concern. Apart from creating unhealthy living conditions dampness can also cause widespread structural damage to building walls and foundations [1]. This problem arises from insufficient ventilation and excessive moisture, which can result in structural deterioration [2].

Buildings are composed of several materials and construction techniques, each with distinct performance characteristics. This performance depends on numerous factors such as its location, environmental conditions, the quality of construction materials, and its usage [3]. Structures regardless of age, are susceptible to deterioration occasioned by human-made and natural factors [4] [5]. More concerning is the problem of dampness as collapsation of building resulting from poor construction material quality, old age, or faulty foundations is rising in Nigeria [6]. The dampness issues can be reduced by certain construction materials, such as granite which can place heavy demands on the performance of bedding, leading to issues with penetrating dampness [7], [8]. The need for proper structural ventilation and moisture control cannot therefore be overemphasized. The non-invasive geophysical methods like ground-penetrating radar (GPR), electrical resistivity tomography (ERT), and infrared thermography, are effective tools for identifying the causes of dampness in buildings. Through geophysical investigations, the underlying causes of dampness, including moisture infiltration and structural damage, can be identified, enabling targeted repairs to prevent further damage [9], [10].

The importance of these geophysical methods is further highlighted by the increasing research interest in their application for addressing damp patches in foundational walls. These techniques offer a non-invasive way to assess the subsurface conditions of a building, allowing for early detection of issues such as voids, water seepage, and structural defects, all of which may contribute to dampness and other building-related problems [6], [11]. This proactive approach helps building owners and managers ensure the safety, comfort, and longevity of structures while promoting healthy indoor environments for occupants.

The aim of this study is to conduct a geophysical analysis of damp spots on foundational walls in Jalala Oke-Odo, with the goal of identifying the source and extent of the dampness, as well as any potential structural issues caused by it.

A. Climate/Geology of the study area

Geological setting

The Nigerian Basement Complex, a series of Precambrian igneous and metamorphic rocks, underpins the city of Ilorin. The basement complex is mostly homogeneous and accounts for around half of Nigeria's bedrock. Massive granite and augen-gneiss outcrops. It is supported by the Precambrian to Cambrian Migmatite-Gneiss-Quartzite complex.

The study area is within Tanke Oke-Odo, off University Road, Ilorin Kwara State. The area is located between Latitude 8.471200 and 8.477600 and Longitude 4.629000 and 4.632500 (Figure 1). Tanke is a neighborhood of Ilorin, the capital of Kwara State in Nigeria. The area is situated in the tropical/humid rainforest region, with a climate characterized by wet and dry seasons. The wet season usually occurs from March to October and is dominated by a heavy thunderstorm. The dry season occurs from November to March when the area is under the influence of north-easterly winds.

B. Understanding Dampness on Foundation Walls

Dampness in foundation walls can be a common issue in buildings and can lead to various problems if not addressed properly. Understanding the causes of dampness in foundation walls is important to effectively deal with the issue. In this response, we will discuss the causes of dampness in foundation walls and some possible solutions to prevent or mitigate the problem.

One of the main causes of dampness in foundation walls is poor waterproofing [13]. If the foundation walls were not properly waterproofed during construction or if the waterproofing has deteriorated over time, water can easily penetrate through the walls and cause dampness.
This can happen due to cracks, gaps, or improperly sealed joints in the foundation walls. Another common cause of dampness in foundation walls is poor drainage around the building.

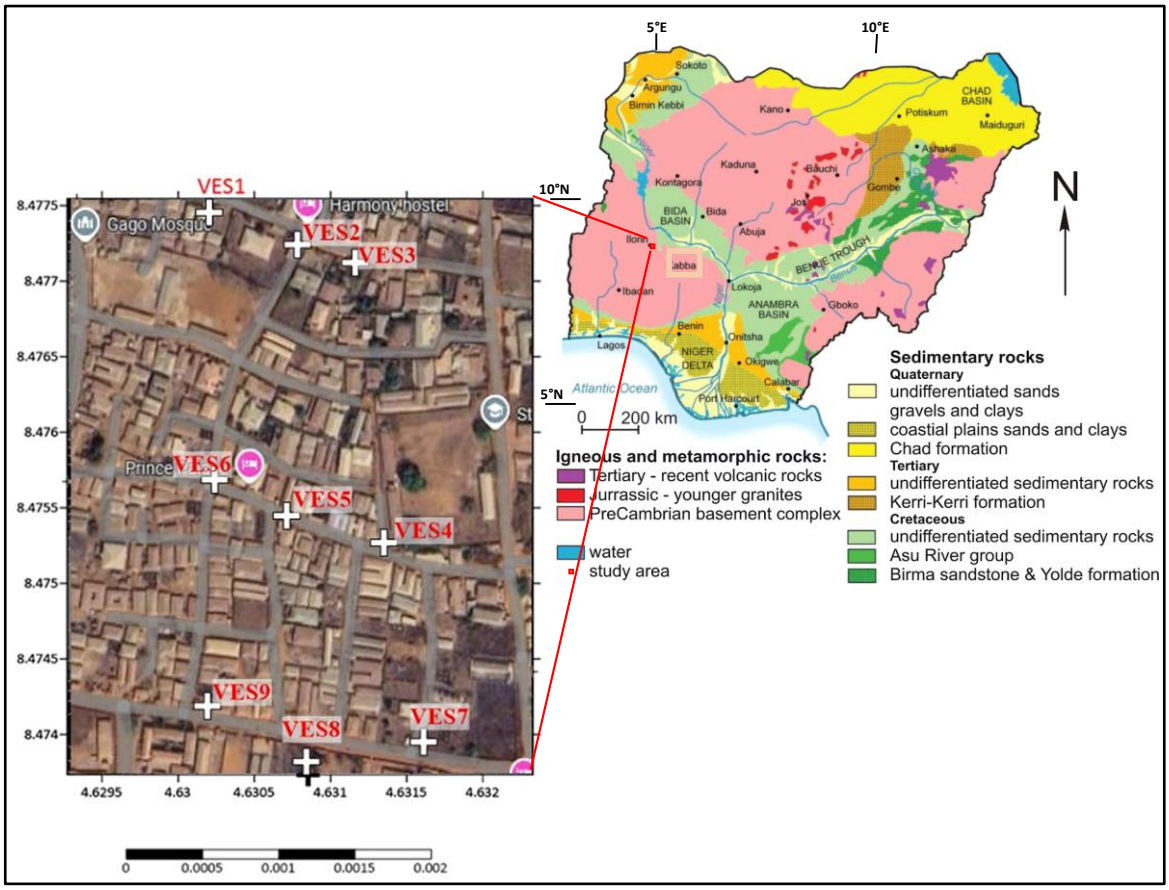


Figure 1: Basemap of the Study Area (Inset is the Geological Map of Nigeria (After [12]).

If the surrounding soil does not have proper grading or the gutters and downspouts are not directing water away from the foundation, excess moisture can accumulate around the walls and seep into the interior. Example of dampness in building wall is shown below (Figure 2).

Figure 2: Example of wall Dampness.

II. METHODOLOGY

A. Geophysical Survey

The survey was carried out using electrical resistivity method, a proposed layout map for data acquisition was used a as a guard line at the field. Nine vertical electrical sounding data were acquired using schlumberger array, which was used to generate maps and geoelectric-sections.

Field Proceedure

The Omega Campus Terameter was used for resistivity data acquisition. Other equipment included 200m multi-conductor cables, measuring tape, steel rod electrodes, and hammers. A Schlumberger array was employed due to its sensitivity to vertical structures and deeper depth of penetration. Nine Vertical Electrical Sounding (VES) stations were set up along three profiles, containing three sounding points. The stations were arranged in a grid, and resistivity readings were taken by passing current into the ground via a pair of current electrodes, with the resultant resistance recorded through a pair of potential electrodes. The current electrodes were

spaced symmetrically, and the distance between them was gradually increased to ensure the measurement reached greater depths, with the maximum spread of AB/2 set at 110m and MN/2 at 27.5m.

Electrode Configuration

The Vertical Electrical Sounding (VES) method was used, where the current and potential electrodes were progressively expanded from a fixed central point. This method is useful in geotechnical surveys for determining overburden thickness and in hydrogeology for identifying porous strata.

B. Data processing and Interpretation

Apparent resistivity values at each station were plotted against the half current electrode spacing (AB/2) using log-log graph to generate field curves. Qualitative interpretation involved visually inspecting the curves to determine the number and nature of subsurface layers. These curves were then interpreted quantitatively using partial curve matching and computer iteration techniques. Data interpretation was done using software like WinResist2, Surfer15, and Publisher to create geo-electric sections and maps.

Interpretation Methods

Curve Matching Technique: Master curves, constructed for assumed geo-electric sections, were matched with field curves to derive geo-electrical parameters.

Auxiliary Curve Method: Used in terrains with multi-layered field curves, the method involves matching smaller segments of the field curve with theoretical two-layered curves.

Computer Interpretation: Computerized interpretation minimizes errors by comparing field data with modeled data, adjusting parameters until the model matches field measurements. This technique provides accurate geo-electrical parameters, essential for determining subsurface conditions such as bedrock depth or aquifer locations.

This methodology ensures the accurate interpretation of subsurface resistivity data, providing valuable insights into the geological structure of the study area.

III. RESULT AND INTERPRETATION

The results were presented in Sounding curves, geoelectric sections and maps.

A. Sounding curves

The sounding curves from these readings varies from 3 layer to 4 layers curves with KH curve type being the only curve generated twice (Figure 3).

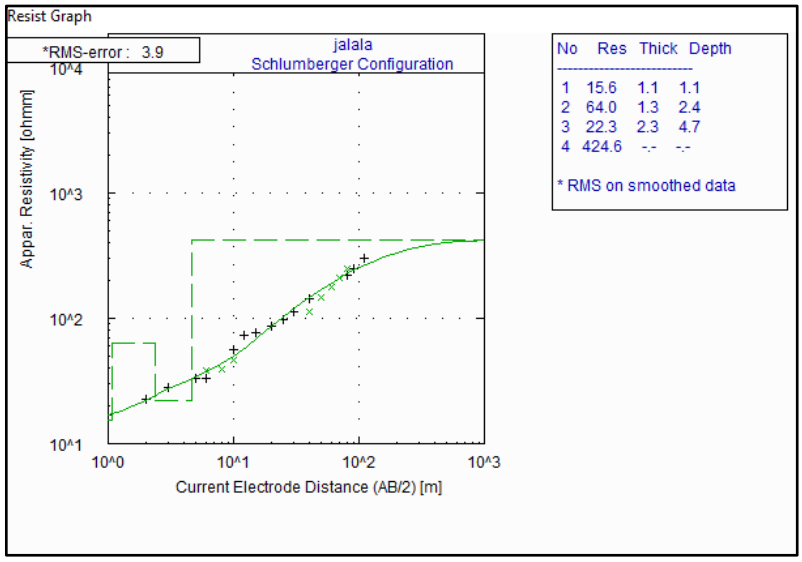


Figure 3: Typical KH curve (VES 2)

B. Geoelectric Sections and Contour Maps

Geoelectric Sections

Three geoelectric sections were generated (profile 1, 2,3). The first profile cut across 3 VES points which includes VES 1, 5 and 9 (Figure 4). Profile 2 includes VES 3, 5 and 7 (Figure5) while profile 3 includes VES 4, 5 and 6 (Figure 6).

Profile 1

This profile consists of 3 VES points as listed above, 4 geoelectric layers were recorded across the section which includes topsoil, lateritic layer, clay and the basement rock. The top soil resistivity varying from 26 Ωm to 101 Ωm with thickness ranging from 0.6m to 4.7 m. lateric layer resistivity varies from 290 Ωm to 775 Ωm maximum thickness of 2.7 m across the section. The clayey medium resistivity varies from 3 Ωm to 52 Ωm with thickness ranging from 0.5 m to 3.3 m, while the bedrock has a resistivity ranging from 210 Ωm to 831 Ωm.

Figure 4: Profile 1

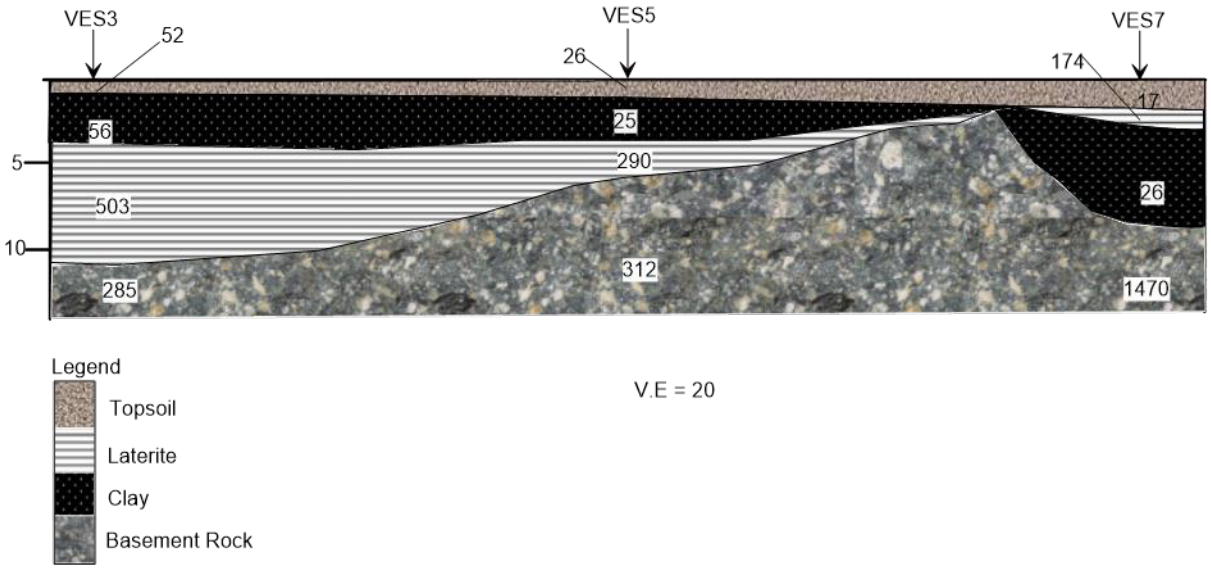


Figure 5: Profile 2

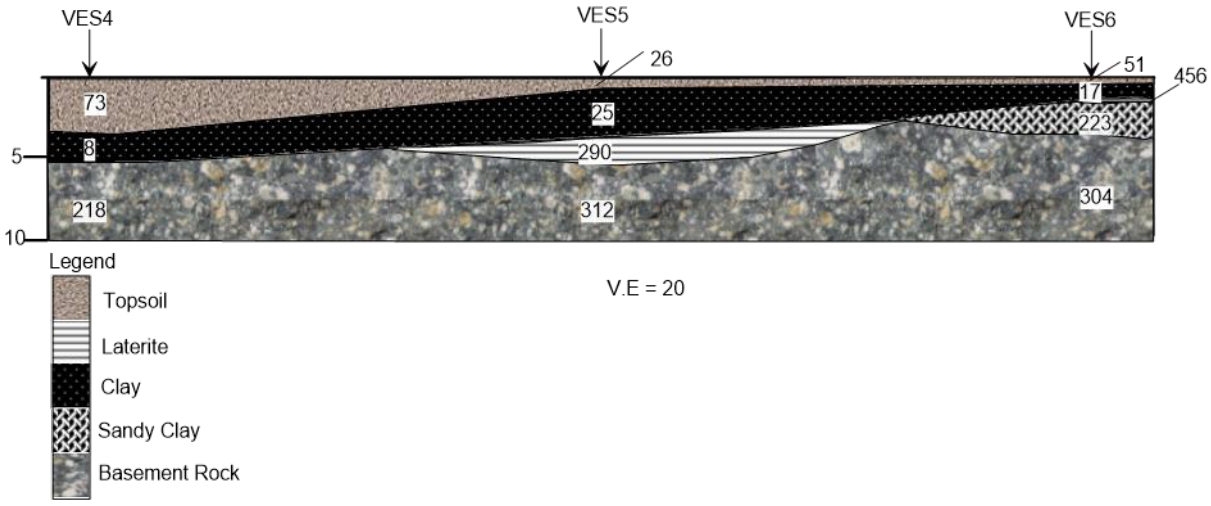


Figure 6: Profile 3

Profile 2

This profile cut across VES 3,5 and 7, total number of 4 geoelectric layers were recorded across the section which includes topsoil, lateritic layer, clay and the fresh bedrock. The top soil resistivity varies from 17 Ωm to 52 Ωm with thickness ranging from 01 m to 1.4 m. The clayey layer resistivity varies from 26 Ωm to 56 Ωm with thickness ranging from 2.7 m to 5.7 m. Lateric layer resistivity varies from 174 Ωm to 503 Ωm with maximum thickness of 7.2 m. and the fresh bedrock has a resistivity ranging from 285Ωm to 1470 Ωm.

Profile 3

Profile 3 comprises of 3 VES points in which 4 to 5 geoelectric layers were generated which consist of topsoil, laterite, clay, sandy clay and the fresh bedrock. The topsoil resistivity value varies from 26 Ωm to 73 Ωm thick, ranging from 0.8 m to 3.5 m, the laterite was recoreded in VES 5 and 6 with resistivity of 290 Ωm and 456 Ωm with maximum thickness of 2 m, the clayey layer serve as the second layer across this section with resistivity with varying from 8 Ωm to 25 Ωm and thickness of 1.2 m to 2.7 m. Sandy clay with resistivity value of 223 Ωm and maximum thickness of 2.5 m was recorded in VES 6 underlain by the fresh bedrock.

The geosections has shown lower resistivity values for topsoil in most case and also within the weathered layers.

Contour Maps

To have a clearer view about the subsurface information, The thickness and resistivity map of the depth to the basement were generated (Figure 7 and 8), the depth to the basement rock ranges from less than 1 m to 18 m with an average of 5 m in most part of the study area. The area around VES 3,7,9, shows depth above 9 m. Figure 8 indicates low resistivity within the overburden thickness across most part of the study area, with resistivity values less than 300 Ωm in most part of the study area.

Figures 7 an 8 have shown and given reasonable idea on the overburden materials content. It has also indicated that the overburden consists of weathered rocks types e.g. clay, sandy clay, etc. with their peculiar engineering characteristics.

The interpreted data indicates a generally low resistivity value in most cases with clay materials being inferred in many cases. The overburden materials from second layer to the top of the basement being semi-permeable layers (clay and laterite) which retain water and of course perpetuate the wetness to the surroundings.

IV. CONCLUSSIONS AND RECCOMENDATIONS

In the rapidly urbanizing Jalala Oke-Odo metropolis, driven by the presence of the thriving university community, the construction of numerous contemporary buildings has raised concerns about dampness in both new and older structures.

Damp patches on foundational walls can indicate severe structural issues, necessitating a geologic investigation in Jalala Tanke Oke Odo, Kwara State. This investigation pinpointed the geologic factors contributing to damp patches, including groundwater infiltration, soil composition, and hydrological conditions. In the study area, a significant observation is the widespread presence of damp patches in most houses, posing a risk to foundational walls and building stability. Variations in topsoil resistivity values were also noted, indicating areas prone to surface and near-surface water retention, which can harm foundations. The geoelectric section illustrated low resistivity values at various depths, mainly due to semi-permeable clayey overburden materials retaining water.

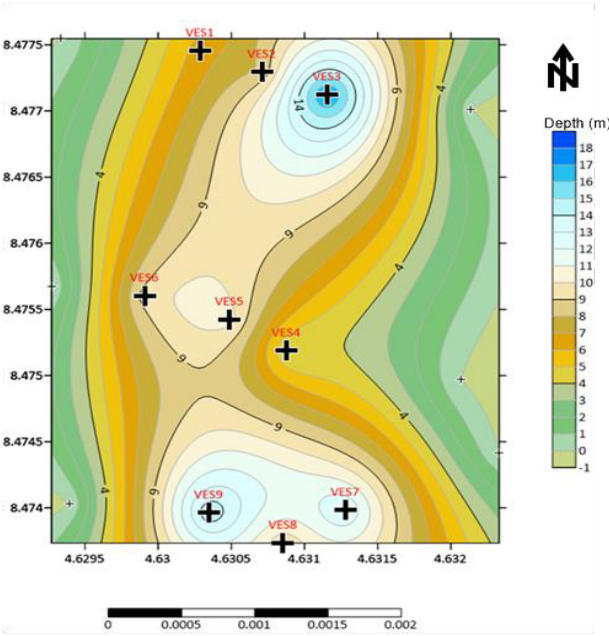


Figure 7: Contour Map of Depth to Basement

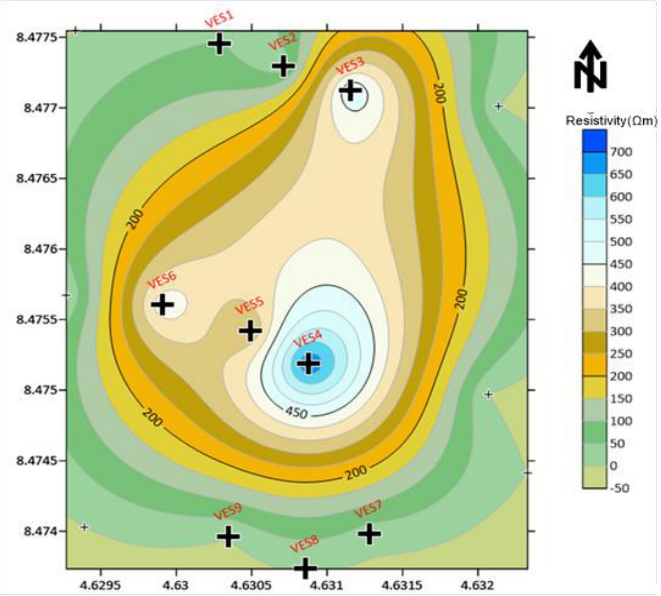


Figure 8: Contour Map Showing Overburden Resisitivity

The findings from the study area highlight the urgent need to address dampness problems in buildings, particularly due to their prevalent nature. The geophysical investigation has offered important insights into the subsurface conditions and the underlying causes of dampness. This information is essential for developing effective remediation strategies aimed at ensuring the long-term stability and safety of buildings in Jalala Oke-Odo and comparable regions across Nigeria.

ETHICAL AND COMPETING INTEREST

I declaclare that I have no known competing financial interests or personal relationships which have or could be perceived to have influenced the work reported on this article.

REFERENCES

[1] Deloney, M. L. (2023). What Is Dampness | Sources of Dampness in Building | Effects of Dampness in Building | Causes of Dampness. CivilJungle. https://civiljungle.com/effects-of-dampness/

[2] Institute of Medicine (US) Committee on Damp Indoor Spaces and Health. (2011). *Damp Buildings*. Nih.gov; National Academies Press (US). https://www.ncbi.nlm.nih.gov/books/NBK215649/

[3] Yu, Z., Nurdiawati, A., Kanwal, Q., Al-Humaigani, M. M., Al-Ghamdi, S. G. (2024). Assessing and mitigating environmental impacts of construction materials: Insights fromenvironmental product declarations. Journal of Building Engineering, 98: 110929

[4] *Journal of Building Performance*. (2013a, August 5). Spaj.ukm.my. http://spaj.ukm.my/jsb/index.php/jbp/index

[5] Faqih, F., Zayed T. and Soliman, E. (2020). Factors and defects analysis of physical and environmental condition of buildings. *Journal of building pathology and rehabilitation, 5 (19).*
https://doi.org/10.1007/s41024-020-00084-0

[6] [6] Oyedele K. F., Oladele S. and Adedoyin, O. (2011). Application of Geophysical and Geotechnical Methods to site Characterization for Costruction Purposes at Ikoyi, Lagos,Nigeria. Journal of Earth Sciences and Geothechnical Engineering, 1(1):87-100. ISSN:1792-9040 (print).

[7] Young, M. E. (2007a). Dampness penetration problems in granite buildings in Aberdeen, UK: Causes and remedies. *Construction and Building Materials*, *21*(9), 1846–1859. https://doi.org/10.1016/j.conbuildmat.2006.05.027

[8] Young, M. E. (2007b). Dampness penetration problems in granite buildings in Aberdeen, UK: Causes and remedies. *Construction and Building Materials*, *21*(9), 1846–1859. https://doi.org/10.1016/j.conbuildmat.2006.05.027

[9] Amadi A.N, Eze C.J, Igwe C.O, Okunlola I.A and Okoye N.O (2012). Architect's and Geologist's View on the Causes of Building Failures in Nigeria. *Modern Applied Science; 6(6).DOI:10.5539/mas.v6n6p31*

[10] Adelusi, A. O., Akinlalu, A. A. and Adebayo, S. S. (2013).Geophysical and Hydrochemistry methods for mapping groundwater contamination around Aule area, Akure, Southwestern Nigeria. *International Jounal of Water Resources and Environmental Engineering,* 5(7): 442-451. DOI:10.5897/IJWREE2013.0370

[11] *Journal of Building Performance*. (2013b, August 5). Spaj.ukm.my. http://spaj.ukm.my/jsb/index.php/jbp/index

[12] Adelana, S.M.A.,Olasehinde, P.I. and Bale, R. B. (2008). An overview of the geology and hydrogeology of Nigeria. Applied groundwater studies in Africa (pp. 171-197). Taylor and Francis, London. Eds. Adelana, S.M.A and Macdonald A.M.

[13] Trenchlesspedia (2019, April 17). *Geophysical Site Investigation Methods*. Trenchlesspedia; https://www.trenchlesspedia.com/definition/4271/geophysical-site-investigation-methods-site-investigation