Human Vulnerabilities in Cybersecurity: Analyzing Social Engineering Attacks and AI-Driven Machine Learning Countermeasures

Faotu Happy [(1)]*
Oghenekevwe N. Asheshemi[(2)]
Esite Jeremiah T[(3)]

Received: 02/10/2024
Revised: 11/10/2024
Accepted: 7/12/2024

[1] Department of Computer Science, Federal University of Petroleum Resources. Nigeria
[2] Department of Computer Science, Federal University of Petroleum Resources, Nigeria. nelson8life@gmail.com
[3] Department of Electrical and Electronic Engineering, Nigeria Maritime University. Nigeria. esite.jeremiah@nmu.edu.ng
* Corresponding Author's Email: faotuhappy@gmail.com.

https://doi.org/10.20428/jst.v30i1.2597

Human Vulnerabilities in Cybersecurity: Analyzing Social Engineering Attacks and AI-Driven Machine Learning Countermeasures

Faotu Happy
Department of Computer Science
Federal University of
Petroleum Resources,
Effurun Delta State, Nigeria
faotuhappy@gmail.com

Oghenekevwe N. Asheshemi
Department of Computer Science
Federal University of
Petroleum Resources,
Effurun Delta State, Nigeria
nelson8life@gmail.com

Esite Jeremiah T
Department of Electrical
and Electronic Engineering, Nigeria
Maritime University,
Delta State, Nigeria
esite.jeremiah@nmu.edu.ng

Abstract— Social engineering (SE) focuses on manipulating human behaviour to gain unauthorized access to sensitive information by exploiting errors, behavioural patterns, and psychological tendencies. This deceptive technique targets employees and consumers, often tricking them into revealing critical credentials. It looks at how attackers use cognitive biases, emotions, and trust to facilitate network hacks, data breaches, and other types of cybercrime. This paper highlights the growing prevalence and advanced nature of social engineering (SE) tactics in today's highly connected digital landscape. This paper presents how Artificial Intelligence (AI) and Machine Learning (ML) can serve as countermeasures against human-induced security mistakes, particularly in mitigating the financial and security impacts of social engineering attacks. The paper focuses on Artificial Intelligence (AI) based machine learning (ML) algorithms as a necessary countermeasure. The effectiveness of social engineering attacks will greatly decrease when these algorithms are integrated into cybersecurity. The study leverages the random forest algorithm, a robust machine learning technique, to predict and address social engineering (SE) attacks by mitigating human vulnerabilities. The paper also investigates emerging trends and hacking methods aimed at account compromise. The research focuses on addressing human vulnerabilities in cybersecurity and mitigating security breaches through the application of Artificial Intelligence (AI) and Machine Learning (ML) algorithms.

Keywords— Mechanism, Social Engineering, Cybersecurity, Vulnerability, Cyber intrusion, Machine Learning.

I. Introduction

Social engineering is focused on manipulating human behaviour to gain unauthorised access to sensitive information. This technique takes advantage of human errors, behaviours, and psychological tendencies, deceiving employees and consumers into disclosing their credentials. Attackers then use this information to infiltrate networks or accounts, relying on individuals' natural tendencies to trust, cooperate, or explore. Similar to human error, human vulnerability is the possibility of being exploited, which could lead to harm to a person or an organisation. The integrity of an entire system, program, or team can be jeopardised by a single weak point [1]. Social engineering (SE) remains the weakest link in cybersecurity, providing hackers with opportunities to exploit human errors and gain unauthorized access to accounts.

In the fields of cybersecurity and information security, this "weakest link" idea is especially important. Skilled hackers or clever malware can breach even the most sophisticated and well-defended security systems by identifying and taking advantage of the weakest point in the defence. Even the most advanced IT security systems often struggle to defend against social engineering attacks, as these intrusions can masquerade as legitimate access attempts. Individuals are especially vulnerable in the digital landscape, where their online presence and social media activities become prime targets for exploitation.

Cybercriminals frequently entice users into compromising their personal accounts and networks by directing them to parody websites or accounts [2]. They may trick victims into clicking on malicious links or encourage them to download harmful applications. As a result, the risk of falling victim to these deceptive tactics remains alarmingly high. Scams and identity theft have existed long before computers and the internet. In the cybersecurity domain, scams fall under social engineering (SE) attacks. These clever methods exploit human weaknesses, using deception, persuasion, and manipulation to steal personal information or break into security systems.

Social Engineering attacks are tricky because they don't follow a set pattern, making them harder to spot. Often, victims aren't even aware they are being tricked. Recent major security breaches have shown how much human vulnerability can affect cybersecurity. Even with advanced technology in place, people remain a key part of security and a top target for cyber attackers. In 2017, it was revealed that a 2014 data breach had exposed the personal details of all three billion

Yahoo user accounts. The attackers used a spear-phishing attack to steal employee login credentials, which allowed them to infiltrate Yahoo's network. As a result, sensitive information such as names, email addresses, phone numbers, birthdates, encrypted passwords, and security questions (both encrypted and unencrypted) was compromised [3].

Data and information security threats are becoming more alarming and widespread due to constant changes in storage methods and social interactions. Encryption and other countermeasures are essential skills in defending against these threats, particularly social engineering attacks. Unlike traditional cyberattacks that exploit technical vulnerabilities, social engineering targets human behaviour, using manipulation and deception to bypass security barriers and gain unauthorised access or steal confidential information. Training in digital security and techniques for recognising these attacks is critical in preventing such breaches.

II. Background & Literature review

A. Human Vulnerabilities in Cybersecurity

Human vulnerability, a crucial aspect of cybersecurity, refers to individuals' inclination towards errors, manipulation, or exploitation, often leading to security breaches [4]. Humans remain one of the weakest defenses against cyberattacks, despite the fact that systems and technology are becoming more complicated and resilient. Some of the common weaknesses are

1) *Lack of Awareness:* Many people are easy candidates for phishing emails, malware, and other social engineering assaults because they don't understand the fundamentals of cybersecurity.

2) *Trust:* To obtain sensitive information, attackers frequently take advantage of people's confidence by posing as trustworthy organisations, such as banks, government agencies, or coworkers.

3) *Fear and urgency:* By threatening to deactivate an account or take legal action, cybercriminals instil a sense of urgency or anxiety in their victims, leading them to make snap decisions without first confirming their legitimacy.

4) *Curiosity:* In order to propagate malware, malicious links or attachments with alluring titles or subjects (such as "Confidential Report" or "Breaking News") take advantage of people's curiosity.

5) *Negligence:* Carelessness can provide attackers the chance to obtain unauthorised access. Examples of this include sharing passwords, leaving devices open, and neglecting software updates.

6) *Weak Password:* Brute force or credential-stuffing attacks are made easier for attackers when simple, predictable passwords are used or reused across several accounts.

7) *Cognitive Biases:* cognitive biases are systematic patterns of deviation from rational decision-making. These biases arise as individuals simplify complex security information, leading to errors in threat assessment, risk evaluation, and response strategies.

B. Social Engineering and Attacks

Social engineering is not about sophisticated technical hacking; it manipulates human behaviour to breach security. As technology advances, the complexity of technical cyberattacks increases, making them harder to execute. However, social engineering remains highly effective, using deception to exploit human vulnerabilities and bypassing even the most advanced security systems. Attackers leveraging this tactic can infiltrate networks, bypass firewalls, implant malware, or establish backdoor access. The key to social engineering lies in exploiting cognitive biases and human error, rather than technical flaws, to obtain sensitive information or access. Social engineering is defined as one of the simplest ways to gather information about a target by exploiting human weaknesses present in every organization. Attackers use this technique to manipulate individuals into revealing confidential information, which is then used to compromise the organization's security [5]. This makes human vulnerability a critical weak point in cybersecurity.

While social engineering is often considered low-tech, it is highly successful because it preys on the psychological flaws of individuals. Security technologies may strengthen systems defenses, but human factors remain the most exploitable link. In essence, attackers use social engineering to circumvent security measures by deceiving human insiders, making it a powerful tool in modern cyberattacks.

https://doi.org/10.20428/jst.v30i1.2597

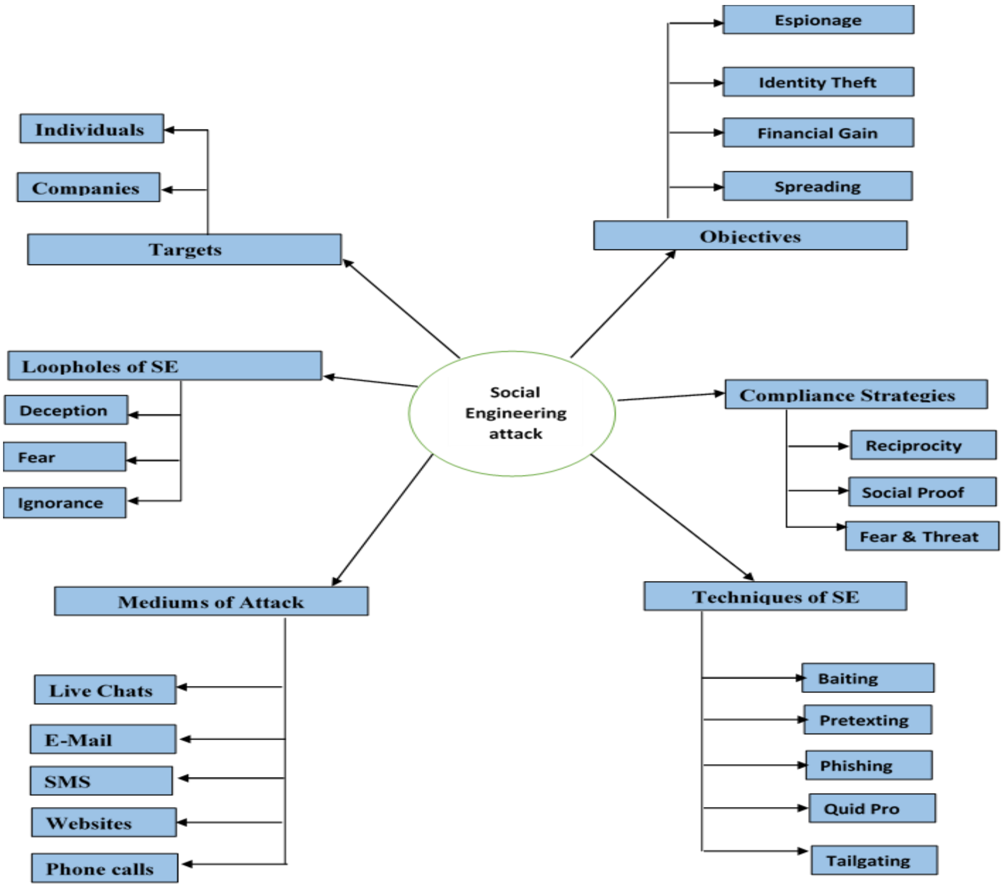

Fig. 1. Social Engineering

C. Social Engineering Attacking Mechanisms

Social engineering attack mechanisms are sophisticated tactics employed by cybercriminals to infiltrate targeted accounts by exploiting human vulnerabilities rather than relying solely on technical weaknesses. These deceptive methods often manipulate individuals into divulging sensitive information or granting unauthorized access to systems, making them highly effective. The attackers may pose as trusted entities or use psychological manipulation, such as creating a sense of urgency or fear, to trick their victims. By preying on emotions and trust, social engineering has become one of the most insidious and dangerous methods in the world of cybersecurity, posing significant threats to both individuals and organizations. Below are some of the mechanisms used in Social Engineering attacks: Phishing is an online scam where attackers send deceptive emails or messages that appear to come from trusted sources, such as banks or service providers. These emails typically ask recipients to provide sensitive personal information, such as passwords or credit card numbers, or trick them into clicking on malicious links or downloading harmful software [6] (Abdulrhman et al., 2023). By impersonating legitimate organizations, phishing aims to steal data or gain unauthorized access to users' accounts.

Baiting is a social engineering tactic where attackers entice victims with enticing offers or rewards, such as free software, media, or other desirable items. By appealing to curiosity or desire, baiting exploits human behavior, leading to unintentional security breaches, either through the download of malicious software or the disclosure of confidential data that attackers can exploit.

Quid pro quo is a social engineering tactic that poses significant risks to workplaces. In this method, attackers offer a service or benefit in exchange for sensitive information. For example, they may impersonate technical support staff, offering to help resolve an issue, and in return, trick victims into sharing confidential data. This approach exploits trust and creates vulnerabilities that can lead to security breaches, putting both personal and organizational information at risk. Tailgating is a physical or digital security breach in which an unauthorized person gains access to restricted areas by exploiting the trust or courtesy of authorized individuals. In physical tailgating, an attacker follows closely behind an authorized person into a secure building without proper credentials. In digital spaces, an attacker may gain access by using an employee's device or credentials to enter sensitive areas of the organization's network. This tactic bypasses security protocols and poses a serious risk to both physical and digital environments.

Pretexting is a social engineering tactic where attackers create a fabricated scenario to obtain private information, systems, or services. By posing as someone in authority or a trusted entity, attackers manipulate victims into sharing sensitive data. This method increases the chances of success for future attacks by building trust and making the deceptive scenario seem more legitimate. Pretexting is often used to gain access to confidential information, such as login credentials, banking details, or internal systems, by exploiting the victim's trust and compliance. According to data released by the Nigeria Inter-Bank Settlement System (NIBSS), the country recorded significant financial losses due to fraud between 2022 and 2023. The total amount lost to fraudulent activities during this period amounted to a staggering ₦9.7 billion. Also, from January to December 2023 alone, there was a reported total of 94,757 fraud cases across Nigeria, highlighting the pervasive nature of financial crimes and the urgent need for enhanced security measures within the financial sector.

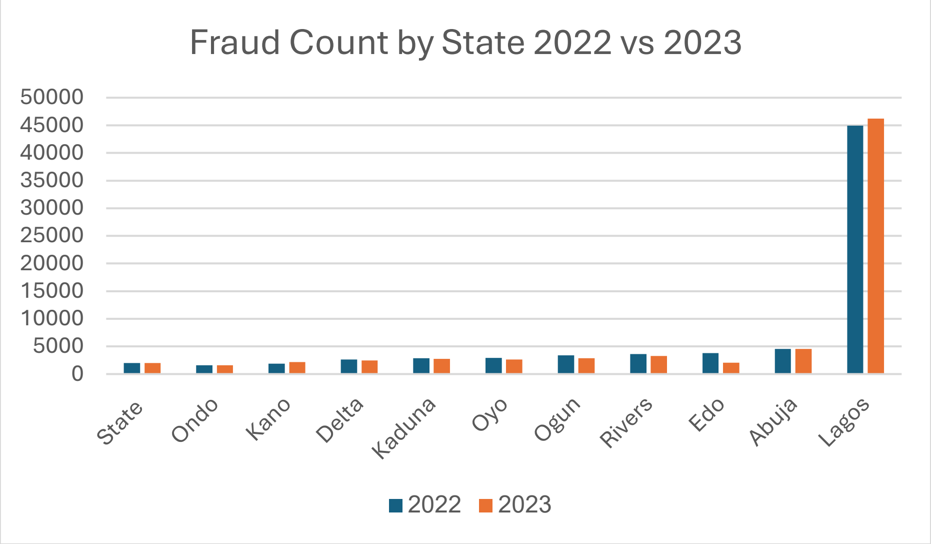

Fig. 2. Fraud count by state 2022 vs 2023

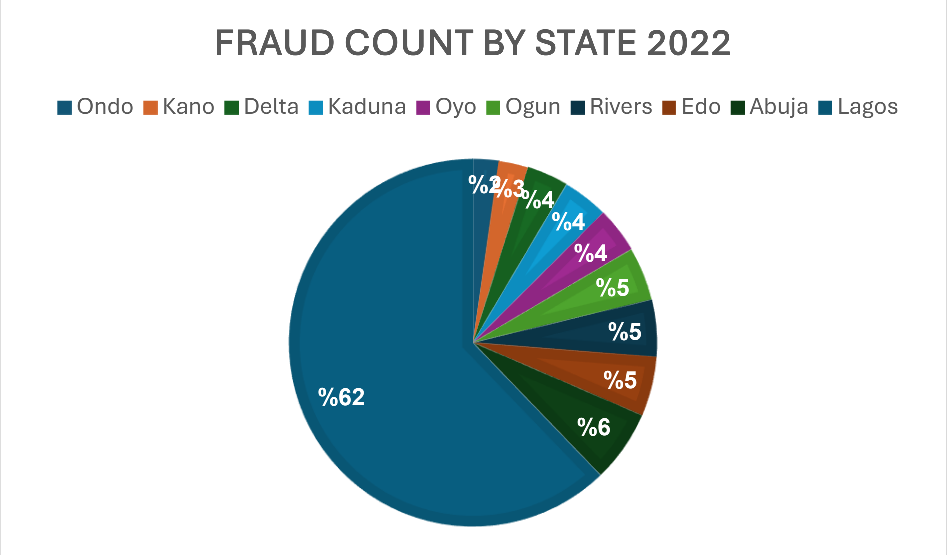

Fig. 3. Fraud count by state 2022

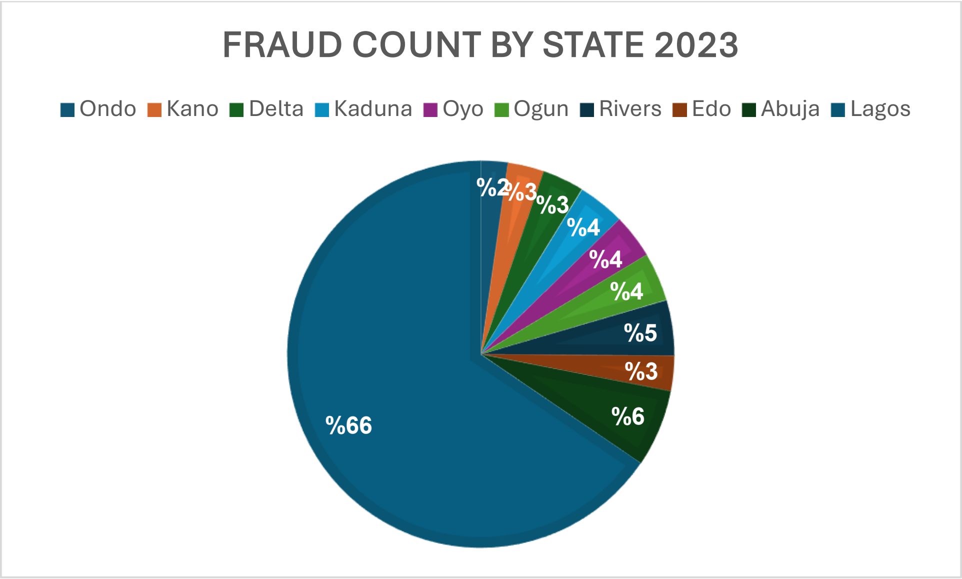

Fig. 4. Fraud count by state 2023

D. Artificial Intelligence as a countermeasure for security threats

AI-driven machine learning offers a highly effective solution for addressing threats such as social engineering and other cybersecurity risks. By analyzing vast amounts of data, these systems can predict patterns and identify common trends employed by potential hackers. AI systems excel at recognizing unusual activities or behaviors that may indicate an impending attack. Additionally, AI not only helps detect these threats in real time but also provides actionable recommendations to mitigate vulnerabilities and strengthen defenses. By continuously learning and adapting, AI-driven solutions are pivotal in combating ever-evolving cyber threats and ensuring robust security in an increasingly digital world.

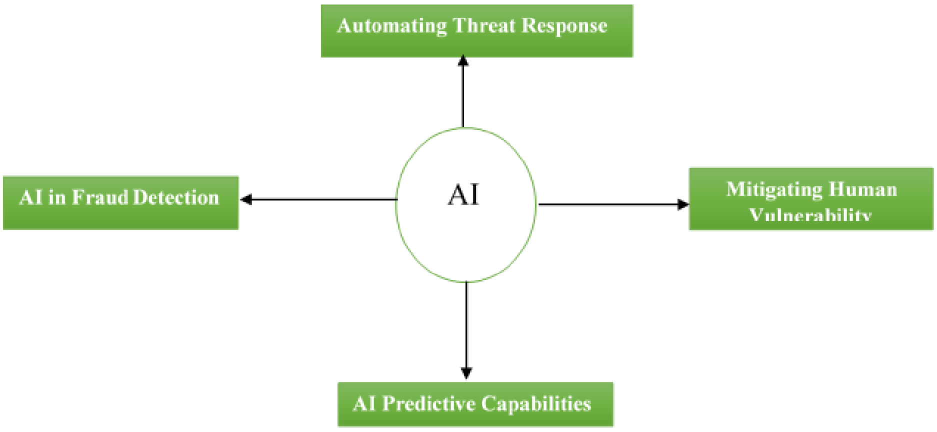
Automating Threat Response
AI in Fraud Detection
AI
Mitigating Human Vulnerability
AI Predictive Capabilities

Fig. 5. AI as a Countermeasure for security threats

1) *AI in thread/fraud detection:* Artificial Intelligence (AI) has greatly increased our thinking and problem-solving approaches, helping us overcome fears related to cybersecurity through its ability to detect and forecast threats. By leveraging large amounts of data, AI excels at identifying patterns and anomalies that may go unnoticed by traditional systems. AI-based systems are capable of continuously monitoring network activity, detecting unusual behaviours, and flagging potential cyberattacks like phishing and malware. These systems can analyze suspicious activities and unauthorized access attempts by studying the behavioral patterns and usage habits of their users. This proactive approach not only enhances security measures but also reduces the risk of successful cyberattacks, making AI an indispensable tool in modern cybersecurity frameworks.

2) *AI predictive capabilities:* Artificial Intelligence (AI) is very good at making predictions. It uses past data to predict possible risks and take action before they become serious problems. AI systems can identify anomalies, including odd transaction patterns that could point to fraud or security breaches, by examining enormous datasets. AI is also very good at spotting vulnerabilities and system breakdowns in vital infrastructure, generating early alerts that allow for preventative actions to lessen the risks. By guaranteeing prompt system optimisation and repair, this capability lowers downtime and boosts operational effectiveness. AI is essential to preserving the dependability and security of contemporary technological ecosystems by utilising its predictive capabilities.

3) *Mitigating Human Vulnerability:* Hackers often exploit human vulnerabilities through social engineering attacks—manipulating individuals to gain unauthorized access to sensitive data, compromise accounts, or commit fraud. These attacks rely on psychological manipulation, making them challenging to counter with traditional security measures alone. However, artificial intelligence (AI) provides effective countermeasures to mitigate these threats. AI can identify phishing attempts by analyzing email content, message patterns, and metadata to detect suspicious activities. Advanced algorithms are capable of flagging fraudulent emails and warning users about potential risks in real time. AI systems can provide automated responses to suspicious requests, minimizing human involvement in critical decision-making processes where errors are likely. By combining message analysis with intelligent automation, AI not only reduces the chances of successful attacks but also enhances overall cybersecurity resilience. This proactive approach helps organizations and individuals safeguard their data and accounts against increasingly sophisticated social engineering tactics.

4) *Automating Thread Response:* AI not only identifies threats but also actively responds to them through automated incident response systems. These systems can isolate compromised devices or networks to contain potential damage, ensuring threats do not spread further. Additionally, AI can deploy countermeasures in real time, such as blocking suspicious IP addresses or disabling access points linked to malicious activities. By acting swiftly and efficiently, AI-powered response systems reduce the reliance on manual interventions, minimize damage, and enhance overall security. This capability enables organizations to maintain robust defenses against evolving cyber threats, ensuring greater resilience and protection for critical systems and data.

E. Artificial Intelligence and Machine Learning in Cybersecurity

Artificial Intelligence (AI) and Machine Learning (ML) have greatly improved cybersecurity by improving security mechanisms and enhancing the detection, prevention, and response to threats more effectively and efficiently. Standard security approaches often depend on predefined rules and manual surveillance, which are insufficient to address the growing complexity and sophistication of modern cyberattacks. AI and ML overcome these limitations by analyzing massive datasets in real time, enabling them to detect patterns, anomalies, and emerging threats with remarkable speed and accuracy. These advanced technologies not only strengthen defense systems but also adapt to evolving attack methods, ensuring robust, proactive cybersecurity solutions. Below are some applications of AI and machine learning in cybersecurity:

1) *Thread Detection:* By analyzing network activity, system logs, and behavioural patterns, AI-Driven systems can effectively detect threats such as malware, phishing attempts, and unauthorized access. Machine learning models enhance this process by continuously adapting and improving their accuracy over time, ensuring more precise threat identification and better overall security. A supervised learning algorithm called Random Forest is applied to both classification and regression tasks. It builds many decision trees during training and combines their output to produce predictions. The tree ensemble improves overfitting, vastness, and accuracy. It is used for spam email detection and below is a brief classification of tree building using Gini Index (1).

$$G = 1 - \sum_{i=1}^{n} p_i^2 \qquad (1)$$

Where P_i is the proportion of samples belonging to class *i* as given node. If we have a binary classification problem such as ***threat vs no threat*** p_i represents the probability of ***threat*** and p_2 will represent ***no threat*** indications

p_i^2 Proportion help indicate the classes with higher concentration of samples.

$1 -$ This indicates that it is close to 0 so the dataset is pure

N is the total number of classes.

When building decision trees, the metrics above is used to determine which feature is optimal to split on. Despite their mathematical differences, they typically produce results that are comparable; nevertheless, in some implementations, such as the CART method, the Gini index is typically chosen because of its easier computation.

2) *Fraud Preventation:* One key factor of cybersecurity is fraud prevention, especially in industries like banking, e-commerce, and finance where fraudulent activity can result in large financial losses as well as harm to an organization's reputation. By spotting patterns and irregularities that point to questionable activity, artificial intelligence (AI) and machine learning (ML) have emerged as crucial instruments in the fight against fraud in recent years.

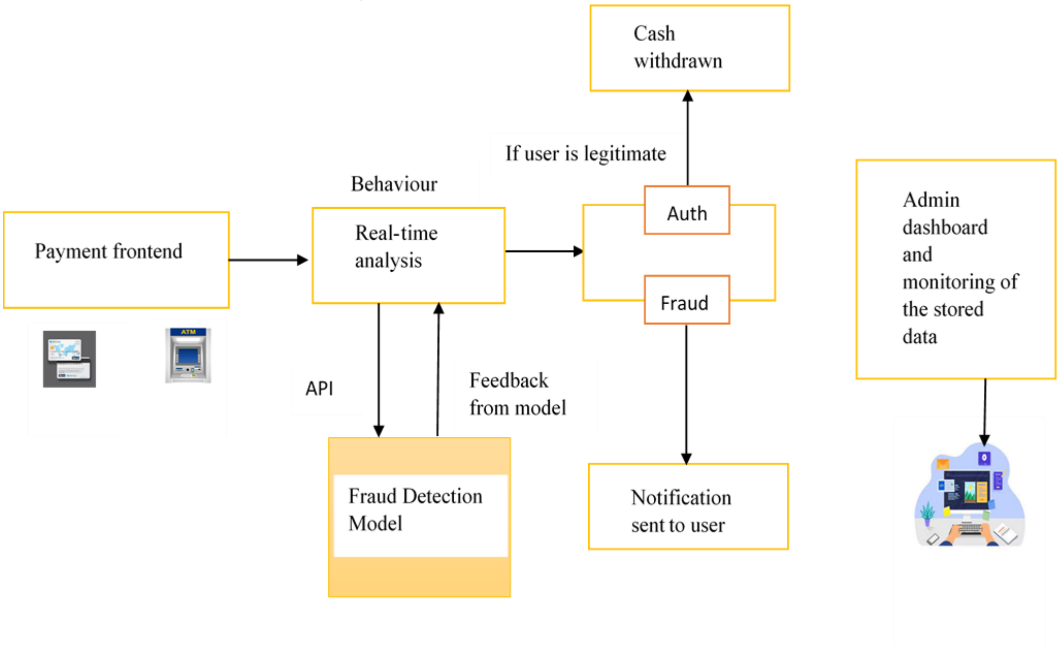

Fig. 6. Fraud Detection Model [7]

3) *Anomaly Detection:* Finding anomalous patterns or outliers in data that differ from expected behaviour is known as anomaly detection. Anomaly detection is essential in cybersecurity to spot possible fraud, system errors, or security breaches [8]. AI and ML can dynamically learn patterns from data, which makes them more successful in spotting risks that have not yet been identified. Some key domains of anomaly detection are Adaptive learning, Data collection, pattern recognition, and real-time analysis.

4) *Phishing & Spam Detaction:* Phishing and spam are dominant cybersecurity risks that are frequently used to deceive people into disclosing private information or downloading harmful files. By examining a variety of signs, including email content, sender behaviour, and communication patterns, AI and ML are integral in identifying and stopping spam and phishing attempts.

F. Challenges in implementing AI and ML Countermeasures

Although implementing machine learning (ML) and artificial intelligence (AI) countermeasures in cybersecurity is a promising strategy, there are several obstacles to overcome. The following is a list of some of the main challenges that organisations encounter:

1) *The availability and quality of data:* For AI and ML models to work well, huge datasets are essential. Inaccurate forecasts might result from biased datasets, poor data quality, or missing information, which reduces the systems' ability to identify hazards.

2) *High Costs of Implementation:* It takes a large investment in infrastructure, qualified staff, and tools to develop and implement AI-driven solutions. This can pose a significant obstacle, especially for small and medium-sized businesses (SMEs) with limited financial resources.

3) *Attacks by Adversaries:* Cybercriminals are increasingly using adversarial tactics to exploit weaknesses in AI models. For instance, someone might subtly alter data inputs to deceive the system and make it useless.

4) *Integration's Complexity:* It can be difficult and time-consuming to integrate AI and ML systems into current cybersecurity frameworks. Redesigning historical systems and making sure they function with the tools and processes in place now can be necessary.

5) *The absence of qualified experts:* Proficiency in both data science and cybersecurity is necessary for the effective implementation of AI and ML in cybersecurity. However, a global shortage of professionals with the necessary skills hinders implementation.

6) *Negative and false positive results:* Artificial intelligence (AI) models may generate false positives, reporting benign activity as a threat, or false negatives, missing real dangers. Both situations may result in operational inefficiencies and a decline in system trust.

G. How Cybersecurity benefits from AI and ML

Machine learning and Artificial Intelligence offers several key advantages in cybersecurity, including:

1) *Enhanced Accuracy:* As machine learning algorithms gain knowledge and adjust to new data, they gradually increase the precision of their detections. This reduces false negatives (missing real threats) and false positives (inaccurately labelled benign behaviour).

2) *Threat Prioritization:* It might be difficult to decide which responses to prioritise when there are so many possible dangers. Security teams can more efficiently deploy resources by using machine learning (ML) to evaluate alarms based on their likelihood and severity.

3) *Quicker Data Analysis:* Security teams handle enormous volumes of data from network traffic, firewalls, and other sources. ML systems analyse this data far more quickly than people do, finding trends and irregularities that can point to possible threats.

4) *Increased Automation:* Machine learning (ML) can be used to automate repetitive and time-consuming processes like screening false positives from alarms or analysing log files. Security analysts are able to concentrate on strategic initiatives as a result.

5) *Improved Threat Detection:* Attack techniques used by cybercriminals are always changing. Proactive defence is made possible by ML's ability to examine past attacks and identify minute behavioural shifts that can indicate new dangers.

III. METHODOLOGY

This study adopted the Agile Software Development Methodology to iteratively design and implement an AI-driven machine learning model, aimed at mitigating human vulnerabilities in cybersecurity. The Agile approach, known for its flexibility, fosters continuous collaboration between team members and stakeholders through cycles of planning, execution, and evaluation [9]. This methodological framework allows the study to assess both the technical and human factors in cybersecurity, with a particular focus on how social engineering attacks exploit human vulnerabilities and the role of encryption in preventing such attacks [10].

This approach promotes faster delivery of value, enhanced quality of outcomes, and increased adaptability to changing requirements. Facilitating a more responsive and iterative development cycle enables teams to continuously deliver and refine solutions that align with user needs and evolving priorities. We specifically chose Scrum among the various Agile frameworks for this study due to its well-defined structure, which includes distinct roles, clearly outlined artefacts, and time-boxed activities designed to optimise team collaboration and efficiency.

Scrum is particularly suited for managing complex and dynamic projects, as its iterative and incremental practices ensure continuous progress and adaptability. By breaking down work into manageable sprints, teams can focus on delivering functional increments of the product while regularly incorporating feedback to enhance the final output. This iterative nature not only boosts productivity but also significantly reduces delivery timelines when compared to traditional waterfall methodologies. We integrated Natural Language Processing (NLP) with the agile methodology in the development of the system architecture. This comWe chose this combination to ensure a flexible and iterative design process, which enables the architecture to effectively utilise training data. ary goal of this approach is to develop countermeasures against social engineering attacks by leveraging the NLP's ability to analyse and interpret human language patterns, thereby enhancing the system's security capabilities.

https://doi.org/10.20428/jst.v30i1.2597

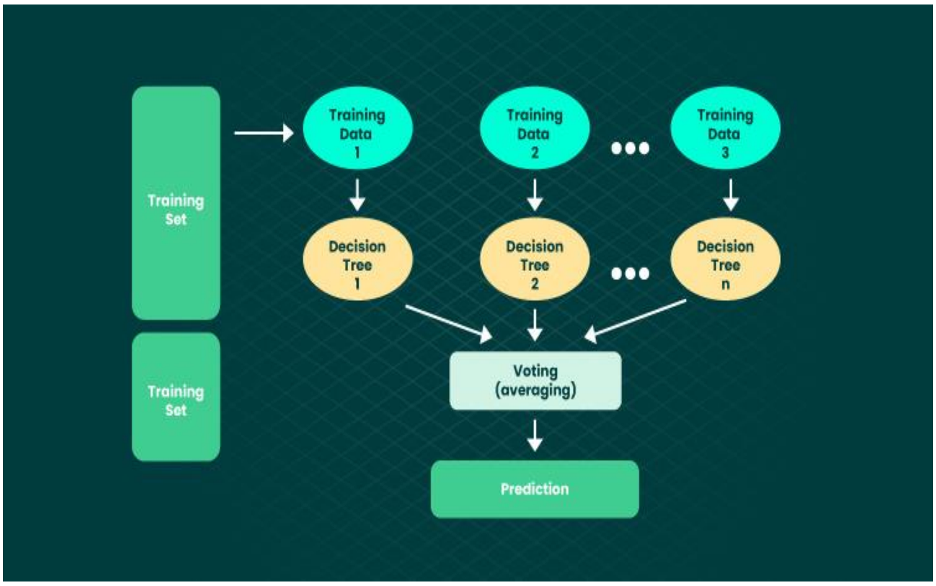

Fig. 7. Architecture of existing system [11]

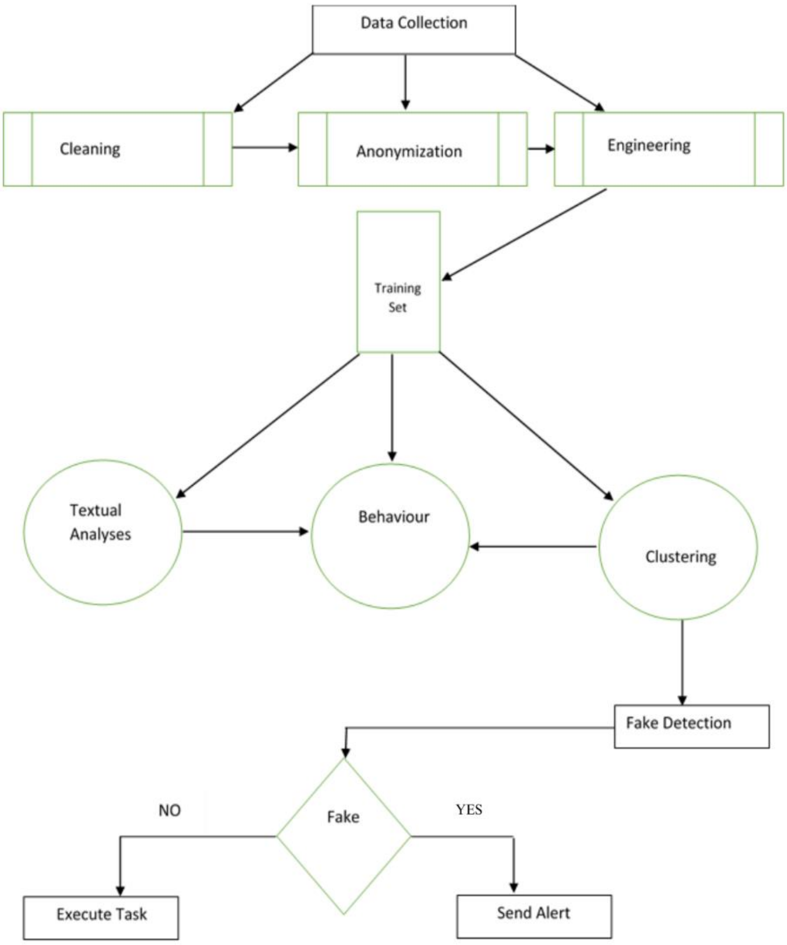

Fig. 8. Architecture of the proposed system

IV. Results and Discussion

This paper explores social engineering mechanisms and other security threats within the cybersecurity landscape, highlighting the strategies employed by malicious actors to bypass existing security frameworks. Social engineering attacks, in particular, exploit human psychological and emotional vulnerabilities by leveraging trust, fear, and urgency to manipulate individuals into divulging sensitive information or granting unauthorized access.

Employees and customers' lack of security awareness contributes significantly to fraudulent activities. To mitigate these threats, fostering a culture of security awareness is essential. This involves regularly sharing relevant resources and training programs that educate stakeholders about common attack vectors and preventive measures (Tahmasebi, 2024).

Also, utilizing artificial intelligence (AI) and machine learning (ML) offers a promising solution to combat fraudulent activities. These technologies excel in detecting anomalies, identifying evolving attack patterns, and automating responses to potential threats. However, implementing AI and ML in cybersecurity comes with financial and technical challenges. Organizations must invest in robust historical datasets and extensive modeling training to ensure the effectiveness of these tools. Despite the initial costs, these technologies provide long-term benefits by enhancing threat detection, reducing response time, and bolstering overall security resilience. This paper underscores the importance of combining human-centric approaches with technological advancements to address cybersecurity threats effectively. Promoting security awareness is vital and can be achieved through impactful initiatives like offering free lectures to university students on campus and educating market women about social engineering attacks, ensuring even those less familiar with technology are protected.

V. Recommendation and Conclusion

The integration of artificial intelligence (AI) and machine learning (ML) in cybersecurity represents a pivotal advancement in combating increasingly sophisticated cyber threats. With a notable rise in social engineering attacks and other malicious mechanisms, there is a critical need for robust, AI-driven systems capable of both detecting and preventing such activities. While awareness campaigns about social engineering have gained traction, they alone are insufficient to address the continually evolving tactics of attackers who leverage advancements in technology to refine their methods.

The future of AI in cybersecurity lies in advancing targeted research that expands the capabilities of current technologies while addressing their limitations. Strategic integration of AI in security frameworks demands vigilant oversight to balance the use of cutting-edge capabilities with adherence to system integrity and ethical standards. This requires rigorous testing, continuous monitoring of AI behavior, and the establishment of frameworks that ensure accountability for AI-driven decision-making. The creation of powerful systems that recognize and thwart complex manipulation efforts should be the main focus of future research. To achieve this, we need a multidisciplinary strategy that fosters cooperation between government, business, and academia to establish best practices and standards. The cybersecurity community can make use of AI's revolutionary potential to build a safer digital environment by focusing on ethical use, strong security, and technological innovation.

VI. References

[1] P. Do, R. Assaf, P. Scarf, and B. Iung, "Modelling and application of condition-based maintenance for a two-component system with stochastic and economic dependencies," Rel. Eng. Syst. Saf., vol. 182, pp. 86–97, 2018. doi: 10.1016/j.ress.2018.10.007.

[2] N. Z. Gorment, A. Selamat, L. K. Cheng, and O. Krejcar, "Machine Learning Algorithm for Malware Detection: Taxonomy, Current Challenges, and Future Directions," IEEE Access, vol. 11, pp. 141045–141089, 2023. doi: 10.1109/access.2023.3256979.

[3] M. Williams, “Inside the Russian hack of Yahoo: How they did it,” CSO, Oct. 4, 2017. [Online]. Available: https://www.csoonline.com/article/3222606/inside-the-russian-hack-of-yahoo-how-they-did-it.html. [Accessed: Apr. 21, 2017].

[4] V. Demertzi, S. Demertzis, and K. Demertzis, "An Overview of Cyber Threats, Attacks and Countermeasures on the Primary Domains of Smart Cities," Appl. Sci., vol. 13, no. 2, p. 790, 2023. doi: 10.3390/app13020790.

[5] R. Yash, “Beyond the code: Exploring the human factor in cybersecurity through social engineering,” *2023*.

[6] L. M. Abdulrahman, S. H. Ahmed, Z. N. Rashid, Y. S. Jghef, T. M. Ghazi, and U. H. Jader, “Web phishing detection using web crawling, cloud infrastructure and deep learning framework,” *J. Appl. Sci. Technol. Trends*, vol. 4, no. 1, pp. 54–71, 2023, doi: 10.38094/jastt401144

[7] H. Faotu and T. E. Jeremiah, “AI and SaaS Embedded System: Enhancing Content Creation through Contextual Language,” *J. Sci. Technol.*, vol. 29, no. 2, pp. 57–66, 2024, doi: 10.20428/jst.v29i2.2447

[8] N. Capuano, G. Fenza, V. Loia, and C. Stanzione, “Explainable Artificial Intelligence in CyberSecurity: A Survey,” IEEE Access, vol. 10, pp. 93575–93600, 2022, doi: 10.1109/ACCESS.2022.3204171.

[9] M. Bianchi, G. Marzi, and M. Guerini, "Agile, Stage-Gate and their combination: Exploring how they relate to performance in software development," J. Bus. Res., vol. 110, pp. 538–553, 2018. doi: 10.1016/j.jbusres.2018.05.003.

[10] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, "A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements, and Future Directions," IEEE Commun. Surv. Tutorials, vol. 22, no. 1, pp. 196–248, 2019. doi: 10.1109/comst.2019.2933899.

[11] A. Dmytriieva, “Leaving no chance for a scam: A brief guide into machine learning in fraud detection,” Forbytes, 2022. [Online]. Available: https://forbytes.com/blog/fraud-detection-in-machine-learning/

[12] M. Tahmasebi, “Beyond defense: Proactive approaches to disaster recovery and threat intelligence in modern enterprises,” *Journal of Information Security*, vol. 15, no. 2, pp. 106–133, 2024. [Online]. Available: https://doi.org/10.4236/jis.2024.152008

[13] S. Agostinelli *et al.*, “Geant4—a simulation toolkit,” *Nuclear Instruments and Methods in Physics Research Section A: Accelerators, Spectrometers, Detectors and Associated Equipment*, vol. 506, no. 3, pp. 250–303, 2003. [Online]. Available: https://doi.org/10.1016/s0168-9002(03)01368-8

[14] *AI and the Future of Skills, Volume 1*, *Educational Research and Innovation*, 2021. [Online]. Available: https://doi.org/10.1787/5ee71f34-en

[15] A. Bharadwaj, O. A. E. Sawy, P. A. Pavlou, and N. Venkatraman, “Digital business strategy: Toward a next generation of insights,” *MIS Quarterly*, vol. 37, no. 2, pp. 471–482, 2013. [Online]. Available: https://doi.org/10.25300/misq/2013/37:2.3

[16] P. Bourdieu, “The specificity of the scientific field and the social conditions of the progress of reason,” *Social Science Information*, vol. 14, no. 6, pp. 19–47, 1975. [Online]. Available: https://doi.org/10.1177/053901847501400602

[17] J. Boyle, *The public domain: enclosing the commons of the mind*, *Choice Reviews Online*, vol. 46, no. 11, pp. 46–6473, 2009. [Online]. Available: https://doi.org/10.5860/choice.46-6473

[18] P. Brey and J. H. Søraker, “Philosophy of computing and information technology,” in *Elsevier eBooks*, 2009, pp. 1341–1407. [Online]. Available: https://doi.org/10.1016/b978-0-444-51667-1.50051-3

[19] *Building an International Cybersecurity Regime*, Edward Elgar Publishing eBooks, 2023. [Online]. Available: https://doi.org/10.4337/9781035301546

[20] A. Cattaneo, A. Vitali, D. Regazzoni, and C. Rizzi, “A sustainable approach to telerehabilitation in Europe: Patients are ready, but caregivers are essential,” *Studies in Health Technology and Informatics*, 2024. [Online]. Available: https://doi.org/10.3233/shti240014

[21] M. Charfeddine, H. M. Kammoun, B. Hamdaoui, and M. Guizani, “ChatGPT’s security risks and benefits: Offensive and defensive use-cases, mitigation measures, and future implications,” *IEEE Access*, vol. 12, pp. 30263–30310, 2024. [Online]. Available: https://doi.org/10.1109/access.2024.3367792.

[22] K. W. Dam, “Some economic considerations in the intellectual property protection of software,” *The Journal of Legal Studies*, vol. 24, no. 2, pp. 321–377, 1995. [Online]. Available: https://doi.org/10.1086/467962

[23] M. Di Renzo, A. Zappone, M. Debbah, M. Alouini, C. Yuen, J. De Rosny, and S. Tretyakov, “Smart radio environments empowered by reconfigurable intelligent surfaces: How it works, state of research, and the road ahead,” *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 11, pp. 2450–2525, 2020. [Online]. Available: https://doi.org/10.1109/jsac.2020.3007211

[24] S. Iqbal, A. N. Qureshi, J. Li, and T. Mahmood, “On the analyses of medical images using traditional machine learning techniques and convolutional neural networks,” *Archives of Computational Methods in Engineering*, vol. 30, no. 5, pp. 3173–3233, 2023. [Online]. Available: https://doi.org/10.1007/s11831-023-09899-9

[25] D. Kreutz, F. M. V. Ramos, P. E. Verissimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, “Software-defined networking: A comprehensive survey,” *Proceedings of the IEEE*, vol. 103, no. 1, pp. 14–76, 2014. [Online]. Available: https://doi.org/10.1109/jproc.2014.2371999

[26] S. Morandini, F. Fraboni, M. De Angelis, G. Puzzo, D. Giusino, and L. Pietrantoni, “The impact of artificial intelligence on workers’ skills: Upskilling and reskilling in organisations,” *Informing Science: The International Journal*

of an Emerging Transdiscipline, vol. 26, pp. 039–068, 2023. [Online]. Available: https://doi.org/10.28945/5078

[27] K. Ooi *et al.*, “The potential of generative artificial intelligence across disciplines: Perspectives and future directions,” *Journal of Computer Information Systems*, pp. 1–32, 2023. [Online]. Available: https://doi.org/10.1080/08874417.2023.2261010

[28] J. Opara-Martins, “Perspective chapter: Cloud lock-in parameters – Service adoption and migration,” in *IntechOpen eBooks*, 2023. [Online]. Available: https://doi.org/10.5772/intechopen.109601

[29] G. D. Putnik, V. Shah, Z. Putnik, and L. Ferreira, “Machine learning in cyber-physical systems and manufacturing singularity – It does not mean total automation, human is still in the centre: Part II – In-CPS and a view from community on industry 4.0 impact on society,” Journal of Machine Engineering, pp. 133–153, 2021. [Online]. Available: https://doi.org/10.36897/jme/134245

[30] P. Scott, “The globalization of higher education,” in Routledge eBooks, pp. 101–118, 2005. [Online]. Available: https://doi.org/10.4324/9780203984581-13

[31] Y. K. Dwivedi *et al.*, “Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy,” *International Journal of Information Management*, vol. 66, p. 102542, 2022. [Online]. Available: https://doi.org/10.1016/j.ijinfomgt.2022.102542

[32] B. C. Stahl, *Artificial Intelligence for a Better Future*, SpringerBriefs in Research and Innovation Governance. Springer, 2021. [Online]. Available: https://doi.org/10.1007/978-3-030-69978-9

[33] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, and E. K. Markakis, “A survey on the Internet of Things (IoT) forensics: Challenges, approaches, and open issues,” *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1191–1221, 2020. [Online]. Available: https://doi.org/10.1109/comst.2019.2962586