The Effect of Using Social Engineering for Cybersecurity on the Internet of Things Environment

Meiad Jrad Hamood Aljrad [1,*]
Kawther Al-Dhlan[2]

[1] College of Computer science and Engineering. University of Ha'il.
[2] College of Computer science and Engineering. University of Ha'il. Email: k.aldahlan@uoh.edu.sa
* Corresponding Author Designation, Email: meiadjh@hotmail.com

https://doi.org/10.20428/jst.v27i2.2055

The Effect of Using Social Engineering for Cybersecurity on the Internet of Things Environment

Meiad Jrad Hamood Aljrad
College of Computer science and Engineering
University of Ha'il
Ha'il, KSA
meiadjh@hotmail.com

Kawther Al-Dhlan
College of Computer science and Engineering
University of Ha'il
Ha'il, KSA
k.aldahlan@uoh.edu.sa

***Abstract*— Although the Internet of Things (IoT) developers view human users as the weakest cybersecurity link and potentially a deciding factor in IoT security, IoT devices are exposed to a variety of security flaws and vulnerabilities, which most social engineers take advantage of to launch several data-collection attacks. For various purposes, this study looked at improving data security on MySQL databases and web pages by using TSL encryption protocols and the two algorithms (RSA & AES) that correlate with the Internet of Things environment and enable user authentication. The implementation was done on the proposed models and encryption methods used. This study aimed to protect the information that is shared on the Internet and connect IoT devices in a secure environment. The results revealed that the proposed study increased the level of protection with the help of complex conditions specified when registering the user and protecting it against attacks. As a result, one of the most important events that came true is the existence of cybersecurity. It is expected that this research will enhance the understanding of the IoT environment and exploit social engineering attacks to impose security on the IoT environment and preserve the rights of human users.**

***Keywords*—** *Internet of Things (IoT), Social Engineering, Encryption, Human Weakness*

I. INTRODUCTION

In the modern world, the internet of things technology is a very helpful technology that will continue to be widely adopted. However, as private networks of IoT devices are exposed to electronic attacks by social engineers, this research looked at some of the issues IoT devices face and developed solutions. Moreover, it offered a proposal for this problem by using encryption algorithms that protect data and information, as well as some studies related to this field in the world of cybersecurity and clarification of the results of this research after conducting various experiments to find ways to raise the level of protection and security.

II. RELATED WORK

[1] studied that the Internet of Things is developing rapidly due to new technologies. Still, on the other hand, there will be many problems related to privacy and failure to preserve the collected data. A review of some protocols used in IoT was also presented. It focused on problems and weaknesses related to confidentiality, discussed some major security issues and some proposed solutions to improve the security protocol. They explained that the MQTT protocol was vulnerable to DDS attacks. They also made it clear that it is susceptible to changes related to the environment, used AppKey for exchanging keys, establishing a secure connection, and exchanging keys when the counter exceeds a high value.

Recent technological developments and Internet of things devices are rapid [11]. The era now is the era of the Internet of things and interconnected intelligent devices. The exchange of data over the network without the need for humans brings convenience to the user and opens a vast world of intruders, such as social engineers. The study showed an overview of some old theoretical models, also what is new in the science of digital medical analysis and data extraction in a way that preserves privacy. Moreover, it made it clear that attackers do not target IoT devices directly. It showed some fundamental challenges and trends in forensic IoT and a look at issues of weakness within the Internet of things systems. It also discussed the significant lack of security in the world of cybersecurity because the expansion of the Internet of Things environment increases its development and accordingly increases security challenges and risks.

The uses of IoT devices are extensive [7], so sharing data poses an unlimited number of risks and privacy violations. With the growth of wireless technologies, the development and use of IoT devices have increased, and IoT devices use embedded sensor technology to collect personal data and information. That, in turn, poses tremendous privacy challenges. Furthermore, the research presented a specification for security gaps and an attempt to mitigate them by an intelligent software vendor. As it identifies the weaknesses in its database and provides them with a solution that mitigates their risks, using the (CVE) method to enumerate and identify widespread

https://doi.org/10.20428/jst.v27i2.2055

security vulnerabilities and then conduct a thorough analysis of them. The results showed that identifying security vulnerabilities for Internet of Things programs mitigated their attacks and were able to identify existing vulnerabilities accurately.

[10] studied the Internet of things technology depends on devices. Hence, the data collected and stored on these devices, such as name, location, and others, help in the activity of electronic attack. They offered a method to calculate the weight and determine the risks of each threat based on the users and, as a result, contribute to the creation of services and security in IoT systems. They used the AHP algorithm to detect threats and made decisions with multiple criteria such as price, colour, weight, or even psychological state, whether sadness or happiness. They said it could be converted into numbers as a relationship numeric (a method of measuring intangible factors through comparisons using judgments that give relative dominance to these factors). These concepts are essential to AHP. As mentioned earlier, this study applied the AHP approach to propose a specialized security classification against IoT threats.

The study by [14] touched on the importance of data privacy, and that data security is essential. All technology companies prefer their data to everything. No matter how advanced companies and others are in data security, every sector still has a security gap. This gap is called the human being, and the art of collecting sensitive information that called social engineering and its strong impact. The study also showed that some private information is sold on the dark web. That is very dangerous because of the lack of knowledge and awareness, social engineering is growing day by day, and the results came that it is impossible to stop social engineering attacks because it is related to human weakness. It depends on their education and knowledge of its harmful effects.

[15] proposed a conceptual model explaining how social engineering attacks work. Three basic entities have been identified: the mechanism of influence, human weakness, and the method of attack, after looking for 16 scenarios that have been presented, most of these were effective and have been theoretically validated in the field of social engineering, but they have not been verified experimentally, and the studies related to social engineering are still relatively few, and therefore will need more experimental research shortly. The results showed that many of the scenarios presented were effective. Still, some theoretical elements in social engineering that have not been investigated experimentally have also been shown to be affected by different environments. Experimental studies related to social engineering are still few, and some were not included in the survey so that they could be examined further in the future.

Learn about human activity in intelligent homes [2] clarified that technologies related to human activity in smart homes are advancing daily; they also introduced modern algorithms, procedures, challenges, and field classification in the intelligent home to recognize human activity through sensors in the Internet of Things. The algorithms here related to identifying human activity in smart homes are machine learning techniques and the development of hardware systems IoT with improved accuracy. Intelligent homes now contain devices that can be controlled remotely by connecting devices and sensors through communication protocols; the researchers have introduced Human Activity Recognition (HAR) technology. It consists of observing a person's behaviour and then analyzing it to infer the activity and dividing it into two categories—the activity recognition approach, which relies on vision (seeing cameras to track human behaviour) or algorithms. The study's results stated that human activity in intelligent homes is complex and changes from one inhabitant to another due to different lifestyles, habits, or abilities. This field still faces many technical challenges. Brilliant home builders need to provide a set of HARs to determine the required limit of sensors because sensors are more acceptable to users than cameras.

III. ERP Adoption Motivations and Benefits

With the presence and availability of electronic devices and the daily operations achieved on the Internet [6], users become more vulnerable to various types of electronic attacks, especially social engineering attacks that target the user and the computer instead of exploiting loopholes [5]. It is known that IoT devices are more vulnerable to electronic attacks, and one of their most prominent security risks is exposure to social engineering attacks that are on humans rather than the devices. In the field of cybersecurity [3], it is often assumed that the human user is the weakest link, and the need to develop protection in the wide area of attack has become more essential. We must know that human sensors can detect attacks across the platforms that have been developed. Taking advantage of the human sensing ability enables users to contribute directly to the discovery of social engineering attacks, which, in turn, will advance awareness. This research attempted to describe data security and protection from social engineering attacks within the IoT environment based on proposed models. It used some encryption algorithms to protect data from attacks. It developed their use to deal with social engineering attacks in the IoT environment based on the proposed application encryption algorithms and information protection strategies of IoT devices.

IV. Methodology

A particular methodology was used to enhance cybersecurity. It discussed enhancing protection for users by keeping their information entered on the sites confidential when registering. It showed how the use of social engineering algorithms has a significant impact in improving protection in the Internet of Things environment from phishing and fraud attacks, setting conditions for passwords where they help to increase the safety and security and store the data entered on the database, as the essential part of it was encrypting the security answers, date of birth and password, even the authorized reader, cannot read the information on the database because always encrypted. The main reason was that social engineering exploits human weaknesses, so humans are the best to confront social engineering risks. The encryption algorithms AES and RSA have been proposed based on their association with the IoT environment and social engineering, SQL injection attack has been repelled and protected the session phishing, and a new proposal has been developed to protect data when the social engineer tries to infiltrate the user account, whereby persistent cracks sent to the user email with an attempt to enter the version then shows the two-step authentication page. That protects data and information from social engineering attacks, which are now widely used worldwide.

V. Disscusion and Results

Discussion: With the rapid development and availability for using electronic devices, users here are more vulnerable to attacks, especially social engineering attacks and their fraud methods. IoT devices are more susceptible to electronic attacks, so it is necessary to protect servers and web pages connected to the Internet of things devices and store information encrypted. That is to prevent social engineers from reading the stored information, and even users who have authorized access cannot read the data stored in the central database, in the field of cybersecurity often imposes that the human user is the weakest link. Hence, it was necessary to develop protection methods in the attack area.

The study's main objective was to protect against social engineering attacks within the IoT environment based on proposed methods, as shown in figure 1, and to simulate some encryption algorithms to raise the level of security.

The results came here based on the objectives of the research, the most prominent of which was simulating algorithms in an IoT environment, where the AES algorithms were chosen because of their encryption for security and data protection on IoT devices, and the RSA algorithm because of their encryption based on servers on the Internet of Things environment. The above algorithms were selected based on some criteria, most notably:

1. It is connected to the Internet of Things environment.
2. The speed of encryption is high.
3. Data protection is very high, so it is difficult to damage.

Results: The analysis of the results came by relating them to the main objectives of the message, starting with the protection and security of data on the Internet of Things environment and the algorithms used in the Internet of Things environment. The proposed approach was simulated, so the algorithms were selected based on some basic criteria and their uses in the IoT environment, most notably speed, lightness, high level of data protection and ease of use against social engineering attacks. It uses the AES algorithm in the database since not even an authorized user can read all the information. Second, the RSA algorithm has been associated with protecting web pages with the support of one of the encryption protocols, protecting the session. At the same time, the user is present and repelling social engineering attacks that exploit human weaknesses. In contrast, the user is present and working on IoT devices to link them together in a single account. Therefore, I found that one of the main reasons to ensure that data within the IoT environment is protected from the threats of social engineers is that any form of authentication must be established; However, implementing security and protection in an IoT environment is not easy, as companies, government institutions and others are aware of the importance of information security and the damage caused by social engineering attacks that exploit human vulnerabilities.

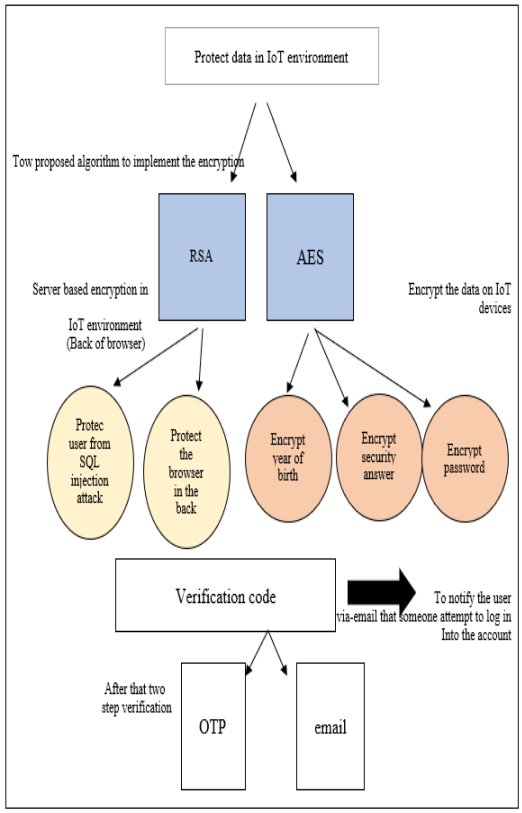

Figure1: Summary of the Proposed Method

VI. Conclusion

Internet of things technology is useful but has many risks that pose a danger to human users. On the other hand, it has facilitated many things and opened wide avenues that can be done in the world of cybersecurity.

This research considered social engineers' important factors in enforcing security in the Internet of Things environment. The goal was to raise the level of protection by using encryption algorithms with security protocols and to enhance authentication using a verification code that increases the level of protection in the IoT environment and protects data traffic while users are at the expense of linked devices and web pages on the Internet exploited by social engineering attacks, the research presented An upgrade in the knowledge of the Internet of Things environment and associated studies, an increase in the knowledge of social engineers and the use of encryption algorithms that were based on some standards to protect data from attacks and notify users of it.

VII. References

[1] Abdulghani, R. M., Alrehili, M. M., Almuhanna, A. A., & Alhazmi, O. H. (2020). Vulnerabilities and Security Issues in IoT Protocols. https://doi.org/https://ieeexplore-ieee-org.sdl.idm.oclc.org/document/9283795

[2] Bouchabou, D., Lohr, C., Kanellos, I., & Nguyen, S. M. (2021). *Human Activity Recognition (HAR) in Smart Homes*. https://doi.org/https://arxiv.org/abs/2112.11232

[3] Breda, F., Barbosa, H., & Morais, T. S. (2017). SOCIAL ENGINEERING AND CYBER SECURITY. https://doi.org/https://www.researchgate.net/publication/315351300_SOCIAL_ENGINEERING_AND_CYBER_SECURITY

[4] Harba, E. S. I. (2017). Secure Data Encryption Through a Combination of AES, RSA and HMAC. Engineering, Technology & Applied Science Research, 7(4), 1781–1785. https://doi.org/10.48084/etasr.1272

[5] Heartfield, R., & Loukas, G. (2018). Detecting Semantic Social Engineering Attacks with the Weakest Link: Implementation and Empirical Evaluation of a Human-as-a-Security-Sensor Framework. https://doi.org/https://www.researchgate.net/publication/323428827_Detecting_semantic_social_engineering_attacks_with_the_weakest_link_Implementation_and_empirical_evaluation_of_a_human-as-a-security-sensor_framework.

[6] Kandias, M., Stavrou, V., Bozovic, N., & Gritzalis, D. (2013, November). Proactive insider threat detection through social media: The YouTube case. In Proceedings of the 12th ACM workshop on Workshop on privacy in the electronic society (pp. 261-266).

[7] Lee, I. (2020). Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management. https://doi.org/https://www.mdpi.com/1999-5903/12/9/157

[8] Malik, V., & Singh, S. (2019). Security Risk Management in IoT Environment. https://doi.org/https://www.tandfonline.com/doi/abs/10.1080/09720529.2019.1642628

[9] Mohammed, A., & Varol, N. (2019). A Review Paper on Cryptography. https://doi.org/https://www.researchgate.net/publication/334418542_A_Review_Paper_on_Cryptography

[10] Mohamed, I., Aissa, A., & Hussein, L. (2020). *Classification For Iot Threats Based On The Analytic Hierarchy Process*. https://doi.org/https://www.researchgate.net/profile/Anis-Aissa-2/publication/344450526_Classification_for_IoT_Threats_Based_on_the_Analytic_Hierarchy_Process/links/5f7b003b458515b7cf67a90f/Classification-for-IoT-Threats-Based-on-the-Analytic-Hierarchy-Process.pdf

[11] Park, M., Oh, H., & Lee, K. (2019). Security Risk Measurement for Information Leakage in IoT-Based Smart Homes from a Situational Awareness Perspective. https://doi.org/https://eds-s-ebscohost-com.sdl.idm.oclc.org/eds/detail/detail?vid=6&sid=24588cad-0d6a-47dc-b4b4-3594d49675ed%40redis&bdata=JnNpdGU9ZWRzLWxpdmU%3d#AN=31075883&db=mdc

[12] Saveetha, P. And Arumugam, S. (2016) "Study on Improvement in Rsa Algorithm and Its Implementation," International Journal of Computer and Communication

[13] Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E., & Markakis, E. (2020). A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues. https://doi.org/https://ieeexplore-ieee-org.sdl.idm.oclc.org/document/8950109.

[14] Shivam, S., Kanellopoulos, A., Vamvoudakis, K., & Wardi, Y. (2019). *A Predictive Deep Learning Approach to Output Regulation: The Case of Collaborative Pursuit Evasion*. https://doi.org/https://ieeexplore.ieee.org/abstract/document/9028950

[15] Wang, Z., Zhu, H., & Sun, L. (2021). *Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities and Attack Methods*. https://doi.org/https://ieeexplore.ieee.org/abstract/document/9323026