

---

# Journal of Informatics and Web Engineering

Vol. 4 No. 3 (October 2025)

eISSN: 2821-370X

---

## Addressing IoT Security Challenges through Advanced Machine Learning and Encryption

Ahmad Aziem Khushairi Anuar<sup>1</sup>, Ahmad Anwar Zainuddin<sup>2\*</sup>, Ahmad Adlan Abdul Halim<sup>3</sup>, Dek  
Rina<sup>4</sup>

<sup>1,2,3</sup>Kulliyah of Information and Communication Technology, International Islamic University Malaysia, Jln Gombak, 53100  
Kuala Lumpur, Malaysia

<sup>4</sup>Department of Physics, Faculty of Mathematics and Natural Science, University of Syiah Kuala, Jl. Teuku Nyak Arief No.441,  
Kopelma Darussalam, Kec. Syiah Kuala, Kota Banda Aceh, Aceh 23111, Indonesia

\*corresponding author: (anwarzain@iium.edu.my; ORCID: 0000-0001-6822-0075)

*Abstract* - The rapid growth of Internet of Things (IoT) devices, including smartwatches, home assistants, and connected appliances, has brought significant convenience to daily life, but it has also introduced serious security challenges. These devices often transmit sensitive data, making them vulnerable to theft, misuse, and unauthorized access. Current security measures are insufficient to address the complex and evolving nature of IoT systems, leaving many of them exposed to potential breaches and cyberattacks. This review explores recent developments in IoT security, focusing on how advanced technologies, such as machine learning, can be utilized to enhance the protection of IoT systems. The main objective of this paper is to examine potential solutions to the security problems that arise in IoT environments. It includes a thorough analysis of recent research and technological innovations in the field, with a particular emphasis on how different security methods are applied across IoT systems. By identifying the most common security vulnerabilities and outlining their impact on IoT networks, the review suggests improved methods to safeguard IoT data and ensure privacy. The findings aim to support researchers, developers, and businesses in designing more secure IoT solutions, and contribute to the establishment of stronger data protection policies. Ultimately, the review serves as a resource for those seeking to enhance the security of IoT devices and systems in an increasingly interconnected world.

*Keywords*—Internet of Things, Smart Devices, IoT Security, Sensitive Data, Machine Learning, Advanced Security Tools, System Vulnerabilities, Data Safety.

Received: 6 February 2025; Accepted: 25 May 2025; Published: 16 October 2025

This is an open access article under the CC BY-NC-ND 4.0 license.



---

### 1. INTRODUCTION

The IoT is an innovative concept that can be defined as the integration of devices via the internet with the aim of the devices' interaction, data sharing, and cooperation [1]. Using sensors and communication technologies, these devices can do various jobs and even make decisions based on the data they collect. The current popular example of IoT applications in everyday life is the use of Smart Home Assistants, for instance Amazon Echo and Google Home. These

devices are central devices that allow the users to control other devices which are connected to their homes. They also have the capability of understanding voice commands, and can give information, as well as regulate smart devices. As these devices go into operation, the more a user utilizes them, the more adept they become in making suggestions and taking actions in the best interest of the user and hence more useful in his life [2].

One of the significant concerns in IoT security is the challenge posed by the diverse range of devices, which do not all operate under the same security protocols. Establishing a unified security framework is difficult due to the integration of various technological devices with different capabilities and security features [3]. Since IoT devices are ubiquitous and aim to provide enhanced user experiences, they constantly collect and analyse user data. This data is often shared across multiple platforms, increasing the risk of information disclosure. For example, in the healthcare sector, IoT devices can access sensitive patient information within a hospital. If an unauthorized individual gains access to this data, it could result in severe problems and dire consequences [4]. Statistics indicate that up to 98% of IoT devices may have security vulnerabilities [5]. This highlights the critical need to improve security protocols for managing multiple connected devices.

This paper aims to review potential solutions and strategies to improve IoT security. Some of these include using advanced technologies like blockchain to enhance data security in management and implementing federated learning, which allows devices to collaborate and improve security by sharing knowledge without exchanging raw data. Additionally, developing more effective methods to control access to devices can lead to safer environments [6]. In the future, establishing robust security systems from the outset can make devices more private and secure, enabling better access control, regular software updates, and educating users on safe practices for each device [7]. In conclusion, while IoT offers numerous advantages, it also poses significant privacy and data security challenges that require immediate attention.

The paper starts with a literature review, which explores earlier relevant research articles that revolve around IoT, machine learning, and security. The methodology is inspired from earlier review papers and explains the special contributions of the present paper towards minimizing present problems. In the result section, typical IoT security threats are explained, which are followed by the discussion, introducing adequate security measures.

## 2. LITERATURE REVIEW

Advances in technology today have made various devices easily accessible at any place [8]. The introduction of the IoT has transformed the way humans interact with computers, enabling a faster and more convenient way of life [9]. The advancement of the IoT has introduced significant challenges in ensuring data security, making it imperative to protect sensitive information from unauthorized access [10]. [9] presented a comprehensive review of security and privacy challenges in cloud-based IoT ecosystem. He also separated the ecosystem into several categorical classifications, which focused on several IoT domains such as consumer IoT, healthcare IoT which showed unique vulnerabilities for each domain [11]. This further adds to our understanding that IoT devices are vulnerable to threats. Security measures need to be taken appropriately to enable each of these problems to be successfully addressed.

Table 1 provides a comprehensive overview of IoT privacy and security in perspective of change and solutions for the future on existing literature from 2020 onwards.

## 3. RELATED WORKS

From the paper titled, “A secure framework for the IoT anomalies using machine learning”, it discusses an IoT anomaly-detection framework that uses a machine learning models such as Classification and Regression Trees and Gaussian Naive Bayes. It achieves 91-98% accuracy in validation and emphasizes real-time monitoring with the help of AWS Infrastructure [20]. As we step into future, which will bring more challenges in maintaining IoT security, we need to improve the quality of existing machine learning. In our paper, we suggest usages of the advanced machine learning and deep learning techniques, which have the advantage of identifying data patterns that help in identifying unknown intruders making more easier to alert with any invasion.

Other than that, paper with titled “A new adaptive XOR, hashing and encryption-based authentication protocol for secure transmission of the medical data in IoT”, proposed a protocol that can enhance the security of data transmission process in IoT. It based three functions, one of it is encryption key exchange (AXHE). AXHE have lacks in several

IoT security for instance AXHE use a simple XOR-based “encryption function”. This simple XOR-based obfuscation is cryptographically weak, leading to not unreadable intercepted data. Our paper is advocating for mature and message-authentication codes like Hash-based MACs (HMAC) that have been formally analysed for resistance against cryptanalysis [21].

Table 1. Summary of Literature Review

Article	Key Finding/ Argument	Supporting Evidence/Sample/ Characteristics/ Methods	Strength/Limitation	Significance/Implication
Research Question: How can advanced machine learning techniques be effectively applied to enhance intrusion detection and cybersecurity in IoT and cloud-based environments?				
[12]	The study emphasizes the need for new solutions to address security issues especially in the digitalizing the medical field. This is through integrating technologies like machine and deep learning using the IoT-23 dataset which is vital to improve the security of IoT devices.	The paper studies the ways to improve the security of the Social Medical System through effective technologies such as blockchain and IoT, and learning algorithms such as SVM, Random Forest (RF), and Convolutional Neural Network (CNN).	The study uses the IoT-23 dataset which is majority used for IoT security research to ensure reliable findings. The study also provides a detailed analysis of security flaws in healthcare systems through integrating diverse learning algorithm.	The research highlights the urgent need to strengthen security in the healthcare systems as they increasingly depend on digital technologies. It adds valuable insights into innovative approaches and technologies to help mitigate risks like data breaches and cyber threats.
[13]	The paper proposes a hybrid data mining model where Grey Wolf Optimization is integrated with Convolutional Neural Networks for Intrusion Detection System (IDS) in IoT networks. It recognizes the problems that IoT systems encounter including low power consumption, use of multiple protocols and others mentioned above. These factors make the IoT systems to be prone to different forms of intrusions	The authors discuss the various threats to IoT devices such as eavesdropping and Man in the Middle attacks. The hybrid algorithm that the authors propose enhances the efficiency of IDSs and effectively mitigates threats to IoT devices.	The integration of Grey Wolf Optimization and CNNs has the potential of enhancing the accuracy of intrusion detection in real time through the integration of the two algorithms' strengths.	The research addresses key security challenges in IoT systems which steadily increased in use in smart homes, agriculture, and urban infrastructure. By improving intrusion detection, it enhances the security of IoT networks.
[14]	The study shows that deep learning algorithms like CNN and Multilayer Perceptron (MLP) can effectively detect and classify attacks in IoT networks. It emphasizes	The paper evaluates the performance of algorithms like RF, MLP, and CNN using a confusion matrix. This shows that deep learning models can	The paper highlights the use of deep learning technologies which significantly boost the rate of intrusion detection	The research is significant as it focuses on the problem of security of IoT networks that are becoming popular among study to helps attackers in

	the importance of performance metrics such as accuracy, true positive rate, and true negative rate in assessing model effectiveness which are crucial to evaluate the success of machine learning models.	get high accuracy in detecting intrusion. It references datasets such as KDD, NSL-KDD, and BoT-IoT, which is used to train the models to ensure a thorough and robust testing of the algorithms.	as compared to traditional ways. Not only that, it also evaluate the model by using multiple performance metric to have a much more clear view on the model's effectiveness	due to the evolution the of rising more number efficient of intrusion cybers detection threats. systems Through that the application improve of the deep security learning, of the IoT environments.
[15]	The research suggests that improving the accuracy of classifying traffic problems is tackled by the proposed data collection method. The system effectively overcomes the obstacle of collecting network traffic data and provides a level of precision in detecting irregularities.	The research showed that the suggested method was effective, by achieving enhancements in assessment criteria when compared to datasets identified beforehand. The approach was based on a structure involving data organization feature development and classification the outcomes demonstrated the dependability and replicability of the method. By correlating with the increasing interest in flow based data techniques for detecting network attacks the study emphasized the need for investigation, in this area to tackle challenges and boost detection abilities.	The research provides an assessment of how the model performs by considering various measurements to ensure dependable and comprehensive outcomes. By combining learning methods, with a stacked technique, for cybersecurity is a new and innovative approach. Moreover, using datasets that're publicly enhances the reproducibility of the study and makes it easier for other researchers to validate the findings.	This study plays a role, in the field of cybersecurity by improving methods for detecting network behaviour that is essential for protecting important data and critical infrastructure assets. The study highlights the effectiveness of machine learning approaches such as learning in improving the identification of online threats. The results have significance as they provide a model that can be put into practice in real world security systems to strengthen protections, against cyber-attacks.
[16]	The suggested system shows an astonishing attack detection accuracy of around 99.72%, which is a clear advantage over already existing methods. Effective feature selection has contributed to the success by enhancing the learning accuracy and improving	The proposed methodology used the NSL-KDD dataset for evaluation, resulting in improved detection accuracy with reasonable testing times, suitable for delay-sensitive applications. It also draws on prior studies that emphasize the	A comprehensive approach to intrusion detection, considering the aspects of supervised and unsupervised learning, and achieving a trade-off between detection accuracy and computation time efficiency, is	This research represents a valuable contribution to the growing base of knowledge on IoT security through the introduction of an advanced machine learning-based intrusion detection model. The work brings to light the pressing need for effective security

	the quality of intrusion detection. The fresh Semi-Supervised Training Unit (SSTU) brings together deep learning and K-means clustering to achieve efficient intrusion detection in IoT networks. Further, the system is extremely efficient even against unknown attacks, which contributes to closing a vital research gap concerning detecting adversaries beyond predefined attack types.	importance of feature extraction in threat identification, thus strengthening the support for the robustness of the proposed method.	presented in the paper. The design is for real-time applicability, which is a prerequisite for environments requiring swift responses to threats in the IoT. The fusion of deep learning and clustering techniques imparts an innovative approach to this realm.	protocols that protect IoT networks ever more targeted by cyber-attacks. Accordingly, these findings indicate several interesting directions that could inspire future research-for example, optimization of the computational time complexity of approaches like SSTU and improvement of attack detection accuracy.
[17]	This study summarizes a new data-oriented taxonomy for classifying IDS from data sources such as logs, packets, flows, and sessions. It provides some insight into how various machine learning algorithms perform well in IDS, thereby improving detection capabilities and reducing false positives. There is also mention of the increasing importance of interpretability in machine learning models for IDS, while addressing the fact that most of these models function as "black boxes."	The survey points toward advancement in machine learning applications in IDS. Important studies such as Uwagbole et al. is celebrated for their high accuracy within the SQL-injection detection domain, showcasing the efficacy of feature extraction followed by classification techniques.	This taxonomy thereby provides a way of systematically approaching the variety of uses of machine learning in IDSs with an aim to better research and development in the field at large. A limitation of this, however, is the lack of training and testing datasets for machine learning models.	The results give emphasis to the vital implementation of machine learning in IDS to boost cybersecurity in the battle against evolving threats. This focus on interpretability is critical for building user trust while making the security decision-making process comprehensible and explainable.
[18]	This paper demonstrates the significant improvement of intrusion detection for IoT environments by combing machine learning and network traffic analysis. This reduces false positives from 12.3% to a mere 4.2%, easily surpassing the conventional signature-based IDS systems, with the precision, accuracy,	The system showed a great improvement in the detection of new threats and complex threats compared to the existing IDS. It was able to detect network intrusion and unauthorized access effectively with less false positive when applied in real-world scenarios like smart homes and industrial environments.	The system has better scalability and effectiveness with a high detection accuracy in IoT scenarios but heavily depends on the high-quality labelled datasets compared with traditional IDS approaches. Otherwise, the labelling might not be as good or even poor, which	This research work shows how machine learning-enhanced IDS frameworks can strengthen the cybersecurity of IoT and, in turn, increase the dependability of IoT systems by increasing detection accuracy and reducing false positives. The study calls for the optimization of methods for real-time detection on resource-

	and recall values estimated to be around 96.5%, 94.2%, and 95.8%, respectively. More interestingly, the proposed framework showed a high adaptability with detection accuracy between 95% and 97% under different IoT applications in smart homes and industrial automation.		will cause issues with this system. Further, as the IoT environment changes, so does the baseline profiling. updating it regularly implies high operational complexity.	constrained IoT devices and combining dynamic profiling with machine learning for enhanced security. Future research could focus on unsupervised and semi-supervised learning to reduce the requirement for labelled data and further explore how to automatically update IDS systems to keep up with the fast-changing IoT environment.
[19]	This study pointed that less important features such as Node info, Protocol and humidity was dropped from the dataset to make analysis of the dataset manageable at features reduced from 31 to 17. Other than that, data normalization techniques are performed to scale numerical data between the ranges of 0 and 1, hence reducing bias and improving model performance. The proposed clustering algorithm was of high performance since the samples were classified very successfully with optimal results at 50 clusters.	The reliability of the model is ensured by the 199,537 samples of the training and testing dataset with a balanced distribution of normal and attack occurrences. One of the systematic ways of selecting important features are to use the Feature Probability Estimation (FPE) technique for supervised feature selection. Also, performance analysis on the KDD dataset shows that the proposed intrusion detection methods outperform the existing methods.	The capability of detection is increased with features such as temperature, battery life, and packet loss. On the other hand, micro-clustering approaches provide high accuracy and precision for real-time intrusion detection; data normalization ensures that model training is reliable. However, this may reduce the generalizability of the approach due to some features' lack of variability.	The framework addresses the requirement for better security in IoT systems, especially in sensitive applications where data integrity is utmost important, such as cold storage. It enhances intrusion detection and sets a new landmark for further research using the AI or machine learning techniques. The results potentially enhance the security in a range of Internet of Things applications including industrial systems and smart home.

## 4. RESEARCH METHODOLOGY

### 4.1. Literature Review and Data Collection

This research paper is based on qualitative research and analysis of the challenges related to privacy and security on the IoT. It aims to enhance security by conducting a comprehensive literature review, followed by proposing several solutions to address these issues. The literature review for this study aims to identify and explore the challenges related to the security of the IoT by analysing relevant works, including scholarly journals, conference proceedings, and research papers. Initial searches for international scientific articles were conducted using key terms such as “IoT security”, “machine learning for IoT”, “IoT Encryption” and “IoT”.

The research papers and studies selected for this review were sourced from reputable platforms. These sources were rigorously examined to extract relevant data, conclusions, and insights. The findings provided valuable information on proposed strategies and enhancements for securing edge IoT devices, with a particular focus on employing advanced security measures.

#### 4.2. Proposed Technique: Review Paper of Addressing IoT Security Challenges through Advanced Machine Learning and Encryption

To achieve the objective of this study, a reading of security challenges from other papers has been done, and the contents from the previous papers have been analysed, and several challenges and solutions have been selected. Emphasis is given to how to solve security problems by providing several advanced solutions that offer significant improvements over previous methods.

## 5. RESULTS AND DISCUSSIONS

### 5.1. Security Challenges of Implementing Machine Learning and Deep Learning in Resource-Constrained IoT Environments

This section will discuss more on the current security issues faced by the security of the IoT. The IoT faces unique security challenges in utilizing advanced machine learning and deep learning techniques to safeguard data as depicted in Figure 1. These challenges primarily arise due to the limited computational resources of IoT devices. Currently, the main constraints stem from processing power, memory, and energy supply, which significantly impact the implementation of critical security functions. As a result, achieving robust security in IoT environments becomes increasingly difficult. [22] further emphasizes that IoT differs fundamentally from cloud-based systems. While cloud-based systems can leverage substantial resources to handle data security effectively, IoT devices are constrained by their hardware limitations. These limitations hinder their ability to detect and respond security threats as quickly as needed.

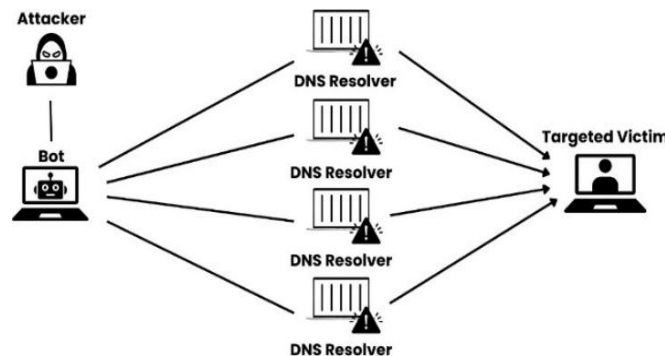


Figure 1. Domain Name System Amplification Attack Workflow

Beyond hardware limitations, Distributed Denial of Service (DDoS) attacks represent another significant challenge in IoT security. This issue is often attributed to the increasing prevalence of IoT devices, which are commonly known for their limited security features. Devices with resource constraints are particularly vulnerable to being hijacked by malicious actors. The proliferation of insecure IoT devices is worsening daily, as there are no clear security standards that can serve as a universal reference for all devices in the IoT ecosystem [23]. Another critical concern is packet injection, where malicious actors exploit vulnerabilities in encryption protocols to introduce unauthorized packets into network traffic. For example, in Software-Defined Networking (SDN), the lack of robust verification tools allows attackers to inject, drop, or alter packets, often using compromised switch nodes. This can disrupt network rules, misdirect legitimate traffic, and compromise the integrity of the network [24].

### 5.2. Vulnerabilities and Artificial Intelligence Driven Countermeasures for Network-Level IoT Security Threats

IoT systems are exposed to man-in-the-middle (MITM) and hacking attempts at the network level because of unsecured communication routes [25]. In addition to IoT devices being regularly controlled out into botnets for massive DDoS attacks, static rule-based IDS frequently fall short in identifying complex threats [26]. Data in transit can be protected from detection by using advanced encryption protocols like TLS/SSL [27]. Also, real-time network traffic analysis is possible with AI-driven anomaly detection systems which may detect unusual trends that could be

signs of DDoS attacks or other harmful activity. IoT devices often have limited access controls and authentication, which enables unauthorized access using static password-based systems that are accessible to physical attacks. Besides, attackers can alter or retrieve sensitive data from devices through physical damage [28]. It is important to use end-to-end encryption to communicate to reduce these weaknesses and guarantee that intercepted data cannot be read. To monitor device behaviour, anomaly detection systems can identify unusual activity which could lead to continuous attacks. Figure 2 shows the comparison between key aspects and differences of privacy and security.

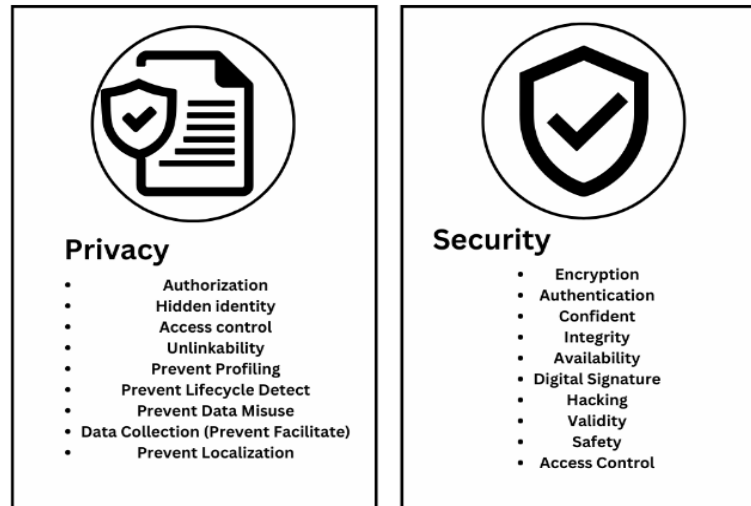


Figure 2. Privacy vs. Security: Key Aspects and Differences

### 5.3. Enhancing IoT Security Through Natural Language Processing (NLP) and Transformer- Based Real-Time Anomaly Detection

Real-time monitoring is essential in cybersecurity to promptly detect and mitigate threats. Traditional methods often struggle with the vast amounts of unstructured data and the sophistication of modern attacks. Integrating NLP into real-time monitoring systems offers a solution by enabling the analysis of textual data, such as network logs and user activities, to identify anomalies indicative of security breaches [29]. NLP techniques process and analyse human language data, allowing systems to understand and interpret textual information. In cybersecurity, NLP can be applied to parse network traffic, analyse system logs, and monitor communications for suspicious patterns. By converting unstructured text into structured data, NLP facilitates the detection of anomalies that may signify intrusion attempts or malicious activities. One method involves using NLP to preprocess network data, including tokenization and normalization, followed by employing machine learning algorithms to detect anomalies. For example, Transformer models, as discussed in the article Network Intrusion Detection Using Transformer Models and NLP for Enhanced Web Application Attack Detection, can be used to analyse the communications between IoT devices [30]. Transformers, due to their self-attention mechanism, are particularly effective in identifying subtle patterns or irregularities in long sequences of data, such as device logs or communication messages. This ability allows the model to detect previously unseen issues, ensuring that IoT systems run smoothly and securely by identifying and resolving problems in real-time. The proposed model mentioned is illustrated in Figure 3.

### 5.4. Advanced Machine Learning and Deep Learning Techniques

A most efficient approach toward the challenge of security problems at the device-level is the use of deep learning models. Deep learning models have emerged as powerful tools in anomaly detection, specifically with the IoT. The capability of deep learning models in examining intricate patterns in data helps in recognizing unauthorized tries for access. Furthermore, the integration of deep learning models with other advanced models enhances their ability to detect anomalies more precisely. For instance, Farooq proposed a hybrid model by integrating Graph Neural Networks (GNNs) and CNNs. In this integrated approach, the features related to both spatial and temporal characteristics can be extracted, and thus, the accuracy in anomaly detection is improved immensely [31]. GNNs are adept at modelling relational data and the communications between it can be viewed as graphs. GNNs can effectively detect anomalies that manifest as unusual patterns by capturing both the features of nodes (devices) and the topology of the network. Then, CNNs in the context of IoT, they can analysis traffic data to identify spatial correlations that distinguish between



normal operations and potential anomalies, thereby it can enhance real-time threat detection and system reliability [32]. Figure 4 indicates the machine learning cycle.

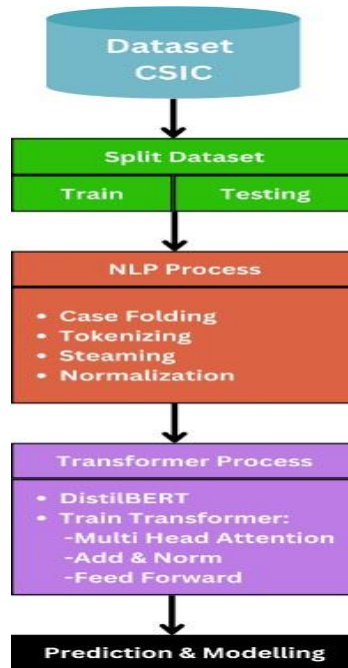


Figure 3. Intrusion Detection Architecture

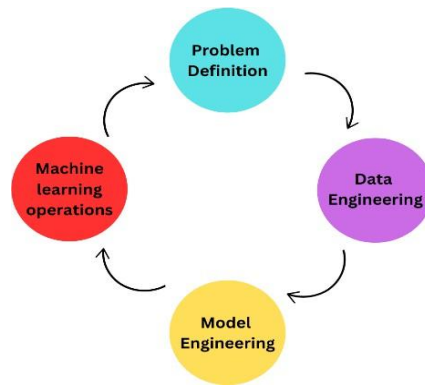


Figure 4. The Machine Learning Lifecycle

### 5.5. Encryption and Anomaly Detection

Encryption and anomaly detection have many advantages for IoT security systems. Data encryption helps to ensure confidentiality and data integrity, meaning any intercepted data would appear unreadable [33]. Immediate identification and action of potential risks is possible due to real-time anomaly detection. The scalability and adaptability of these systems would also accommodate a wide range of IoT applications. Finally, anomaly detection mechanisms can adapt to effectively deal with new attack scenarios and forthcoming threats by ingesting new data [34]. Many IoT endpoints use stream ciphers for instance ChaCha20 because they require less silicon area and less power [35]. This makes them particularly suitable for constrained environments where computational efficiency and low energy consumption are crucial. By combining lightweight encryption with real time anomaly detection, IoT framework not only ensures that data in transit remains unintelligible to adversaries, but at the same time, it provides immediate and adaptive defences against any exploitation. Other than that, to ensure data authenticity and integrity in IoT environment is by using Message Authentication Code such as HMACs. HMACs are cryptographic primitives

that have undergone extensive formal analysis and are proven to be resistant against various form of cryptanalysis. Their standardization and maturity, make them highly reliable for authenticating messages, especially in systems where data integrity is confidentiality, as highlighted in blockchain platforms like Ethereum and Hyperledger Fabric, which emphasize secure communication and data integrity mechanism in their ecosystems [36].

## 6. CONCLUSION

The IoT is a technological revolution that has brought unparalleled convenience and connectivity to many fields. However, besides the advantages, IoT also faces serious privacy and security issues that must be solved to guarantee further growth and reliability. These are challenges regarding the lack of defined security protocols, restricted computational resources, and heightened exposure to complex cyber-threats such as DDoS and MITM attacks. This work shows important gaps in current security frameworks within contexts where conventional security measures are impracticable and accentuates risks in IoT ecosystems. The paper presents only a few of the challenges despite the great potential these methods have. First, the computing needs of advanced machine learning models can stress simple IoT devices. Second, both the lack of common security protocols and the shortage of diverse datasets somewhat restrict the effectiveness and generalizability of the solutions proposed to date. In summary, future research efforts should focus on resource-efficient solutions and encourage collaboration among researchers, industry stakeholders, and regulators to enhance the security of IoT ecosystems. This will be a major factor in addressing the privacy and security concerns by establishing strong security standards, user education, and promotion of best practices. Only with advanced techniques like machine learning, encryption, and NLP can IoT systems really become resilient and trustworthy to face an era of secure and reliable technologies.

## ACKNOWLEDGEMENT

This work is supported by the Department of Computer Sciences, KICT, IIUM, Centre of Excellence Cybersecurity, KICT, IoTeams, KICT and Silverseeds Lab Network.

## FUNDING STATEMENT

The authors received no funding from any party for the research and publication of this article.

## AUTHOR CONTRIBUTIONS

Ahmad Aziem Khushairi Anuar: Conceptualization, Methodology and Writing – Original Draft Preparation;  
Ahmad Anwar Zainuddin: Mentor;  
Ahmad Adlan Abdul Halim: Proofreader;  
Dek Rina: Writing – Review & Editing.

## CONFLICT OF INTERESTS

No conflict of interests were disclosed.

## ETHICS STATEMENTS

Our publication ethics follow The Committee of Publication Ethics (COPE) guideline. <https://publicationethics.org/>





## REFERENCES

- [1] Y. Badr, X. Zhu, and M. N. Alraja, "Security and privacy in the Internet of Things: threats and challenges," *Serv. Oriented Comput. Appl.*, vol. 15, no. 4, pp. 257–271, Dec. 2021, doi: 10.1007/s11761-021-00327-z.

- [2] A. Sarango, G. Vásquez, and R. Torres, “A Vehicle-to-Vehicle Communication System using ZigBee,” *IOP Conf. Ser. Earth Environ. Sci.*, vol. 1370, no. 1, pp. 012008, Jul. 2024, doi: 10.1088/1755-1315/1370/1/012008.
- [3] Md. Tauseef, M.R. Kounte, A.H. Nalband, and M. R. Ahmed, “Exploring the Joint Potential of Blockchain and AI for Securing Internet of Things,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 14, no. 4, 2023, doi: 10.14569/IJACSA.2023.0140498.
- [4] H. Alrubayyi, G. Goteng, and M. Jaber, “AIS for Malware Detection in a Realistic IoT System: Challenges and Opportunities,” *Network*, vol. 3, no. 4, pp. 522–537, Nov. 2023, doi: 10.3390/network3040023.
- [5] H. Alrubayyi, G. Goteng, M. Jaber, and J. Kelly, “Challenges of Malware Detection in the IoT and a Review of Artificial Immune System Approaches,” *J. Sens. Actuator Netw.*, vol. 10, no. 4, pp. 61, Oct. 2021, doi: 10.3390/jsan10040061.
- [6] C.A. Teodorescu, A.-N. Ciucu Durnoi, and V.M. Vargas, “The Rise of the Mobile Internet: Tracing the Evolution of Portable Devices,” *Proc. Int. Conf. Bus. Excell.*, vol. 17, no. 1, pp. 1645–1654, Jul. 2023, doi: 10.2478/picbe- 2023-0147.
- [7] R. Rawat, “Harnessing the Power of IoT and AI for Human Evolution,” *Int. J. Res. Sci. Eng.*, no. 33, pp. 58– 68, May 2023, doi: 10.55529/ijrise.33.58.68.
- [8] Z. Nie, Y. Long, S. Zhang, and Y. Lu, “A controllable privacy data transmission mechanism for Internet of things system based on blockchain,” *Int. J. Distrib. Sens. Netw.*, vol. 18, no. 3, pp. 155013292210884, Mar. 2022, doi: 10.1177/15501329221088450.
- [9] N. Singh, R. Buyya, and H. Kim, “Securing Cloud-Based Internet of Things: Challenges and Mitigations,” *Sensors*, vol. 25, no. 1, pp. 79, Dec. 2024, doi: 10.3390/s25010079.
- [10] R. Mutha, R.R. Borhade, S.S. Barekar, S.S., Dari, D. Dhabliya, and M. Patil, “Enhancing Public Healthcare Security: Integrating Cutting-Edge Technologies into Social Medical Systems,” *South East. Eur. J. Public Health*, 2024, doi: 10.52710/seejph.483.
- [11] B. R. Kikissagbe and M. Adda, “Machine Learning-Based Intrusion Detection Methods in IoT Systems: A Comprehensive Review,” *Electronics*, vol. 13, no. 18, pp. 3601, Sep. 2024, doi: 10.3390/electronics13183601.
- [12] B. Susilo and R.F. Sari, “Intrusion Detection in IoT Networks Using Deep Learning Algorithm,” *Information*, vol. 11, no. 5, pp. 279, May 2020, doi: 10.3390/info11050279.
- [13] V. Dutta, M. Choras, M. Pawlicki, and R. Kozik, “A Deep Learning Ensemble for Network Anomaly and Cyber-Attack Detection,” *Sensors*, vol. 20, no. 16, pp. 4583, Aug. 2020, doi: 10.3390/s20164583.
- [14] H. Naeem, “Analysis of Network Security in IoT-based Cloud Computing Using Machine Learning: Analysis of Network Security in IoT-based Cloud Computing Using Machine Learning,” *Int. J. Electron. Crime Investig.*, vol. 7, no. 2, Jul. 2023, doi: 10.54692/ijeci.2023.0702153.
- [15] H. Liu and B. Lang, “Machine Learning and Deep Learning Methods for Intrusion Detection Systems: A Survey,” *Appl. Sci.*, vol. 9, no. 20, pp. 4396, Oct. 2019, doi: 10.3390/app9204396.
- [16] E. M. Campos et al., “Evaluating Federated Learning for intrusion detection in Internet of Things: Review and challenges,” *Comput. Netw.*, vol. 203, pp. 108661, Feb. 2022, doi: 10.1016/j.comnet.2021.108661.
- [17] M. Prasad, P. Pal, S. Tripathi, and K. Dahal, “AI/ML driven intrusion detection framework for IoT-enabled cold storage monitoring system,” *Security and Privacy*, 7(5), e400, doi: 10.21203/rs.3.rs-2190363/v1.
- [18] M. Riegler, J. Sametinger, and M. Vierhauser, “A Distributed MAPE-K Framework for Self-Protective IoT Devices,” in *2023 IEEE/ACM 18th Symposium on Software Engineering for Adaptive and Self-Managing Systems (SEAMS)*, May 2023, pp. 202–208, doi: 10.1109/SEAMS59076.2023.00034.
- [19] V. Prakash, O. Odedina, A. Kumar, L. Garg, and S. Bawa, “A secure framework for the Internet of Things anomalies using machine learning,” *Discover Internet of Things*, vol. 4, no. 33, 2024, doi: 10.1007/s43926-024-00088-z.

- [20] D.A. Chaudhari, and E. Umamaheswari, “A new adaptive XOR, hashing and encryption-based authentication protocol for secure transmission of the medical data in Internet of Things (IoT),” *Biomedical Engineering / Biomedizinische Technik*, vol. 66, no. 1, pp. 91–105, Aug. 2020, doi: 10.1515/bmt-2019-0123.
- [21] Y.K. Beshah, S.L. Abebe, and H.M. Melaku, “Drift Adaptive Online DDoS Attack Detection Framework for IoT System,” *Electronics*, vol. 13, no. 6, pp. 1004, Mar. 2024, doi: 10.3390/electronics13061004.
- [22] P. Wu, C.-W. Chang, Y.-Y. Ma, and Z.-B. Zuo, “Constant-Size Credential-Based Packet Forwarding Verification in SDN,” *Secur. Commun. Netw.*, vol. 2022, pp. 1–12, Oct. 2022, doi: 10.1155/2022/2270627.
- [23] S. Kavianpour, B. Shanmugam, S. Azam, M. Zamani, G. Narayana Samy, and F. De Boer, “A Systematic Literature Review of Authentication in Internet of Things for Heterogeneous Devices,” *J. Comput. Netw. Commun.*, vol. 2019, pp. 1–14, Aug. 2019, doi: 10.1155/2019/5747136.
- [24] A. Rocha, H. Adeli, G. Dzemyda, F. Moreira, and A.M. Ramalho Correia, “Trends and Applications in Information Systems and Technologies,” *Advances in Intelligent Systems and Computing*, Vol. 1367, 2021, doi:10.1007/978-3-030-72660-7.
- [25] Y. Zheng, Y. Cao, and C.-H. Chang, “UDhashing: Physical Unclonable Function-Based User-Device Hash for Endpoint Authentication,” *IEEE Trans. Ind. Electron.*, vol. 66, no. 12, pp. 9559–9570, Dec. 2019, doi: 10.1109/TIE.2019.2893831.
- [26] A. Babaei, and G. Schiele, “Physical Unclonable Functions in the Internet of Things: State of the Art and Open Challenges,” *Sensors*, vol. 19, no. 14, pp. 3208, Jul. 2019, doi: 10.3390/s19143208.
- [27] A. Golczynski, and J. A. Emanuella, “End-To-End Anomaly Detection for Identifying Malicious Cyber Behavior through NLP-Based Log Embeddings,” *arXiv*. 2021, doi: 10.48550/ARXIV.2108.12276.
- [28] Z. Long, H. Yan, G. Shen, X. Zhang, H. He, and L. Cheng, “A Transformer-based network intrusion detection approach for cloud security,” *J. Cloud Comput.*, vol. 13, no. 1, pp. 5, Jan. 2024, doi: 10.1186/s13677-023-00574-9.
- [29] M. Farooq, M. Khan, and R. A. Khan, “Graph-CNN Hybrid Advance Model for Accurate Anomaly Detection in Multivariate Time Series IoT Streams,” Feb. 28, 2024, doi: 10.21203/rs.3.rs-3977682/v1.
- [30] W.W. Lo, S. Layegby, M. Sarhan, M. Gallagher, and M. Portmann, “E-GraphSAGE: A Graph Neural Network based Intrusion Detection System for IoT,” in *IEEE/IFIP Network Operations and Management Symposium (NOMS)*, 2022. doi: 10.1109/NOMS54207.2022.9789878.
- [31] A. Hangan, D. Lazea, and T. Cioara, “Privacy Preserving Anomaly Detection on Homomorphic Encrypted Data from IoT Sensors,” *arXiv preprint arXiv:2403.09322*, Mar. 14, 2024.
- [32] F. Sabrina, N. Li, and S. Sohail, “A Blockchain Based Secure IoT System Using Device Identity Management,” *Sensors*, vol. 22, no. 19, p. 7535, Oct. 2022, doi: 10.3390/s22197535.
- [33] T. Janssen, R. Berkvens, and M. Weyn, “Benchmarking RSS-based localization algorithms with LoRaWAN,” *Internet of Things*, vol. 12, pp. 100235, Dec. 2020, doi: 10.1016/j.iot.2020.100235.
- [34] F. Mazlan, N.F. Omar, N.N.M.S.N. Mohd, and A.A. Zainuddin, “Comprehensive insights into smart contracts: Architecture, sectoral applications, security analysis, and legal frameworks,” *Journal of Informatics and Web Engineering*, 4(1), pp. 1-17, 2025, doi: 10.33093/jiwe.2025.4.1.1.
- [35] M. H. Z. H. Nizam, M. A. A. Nizam, M. H. H. Jumjadi, N. N. M. S. N. Mohd, and A.A. Zainuddin, “Hyperledger Fabric blockchain for securing the edge Internet of Things: A review,” *Journal of Informatics and Web Engineering*, 4(1), pp. 81-98, 2025, doi: 10.33093/jiwe.2025.4.1.7.
- [36] N. N. M. S. N. Mohd, S. Afiqah, S. Khadeja, A. Nasuha, W. M. H. N. I. Wan, M. Azman, ... and A.A. Zainuddin, “Surveys on the Security of Ethereum and Hyperledger Fabric Blockchain Platforms,” *International Journal on Perceptive and Cognitive Computing*, 11(1), pp. 16-40, 2025, doi: 10.31436/ijpcc.v11i1.526.

## BIOGRAPHIES OF AUTHORS

	<p><b>Ahmad Aziem Khushairi Anuar</b> is a student in Kulliyyah of Information and Communication Technology, International Islamic University Malaysia. His research focuses on general overview and recommendations for security on the Internet of Things (IoT). He can be contacted via email at <a href="mailto:Khushairi.anuar@student.iium.edu.my">Khushairi.anuar@student.iium.edu.my</a>.</p>
	<p><b>Ahmad Anwar Zainuddin</b> is an Assistant Professor at the International Islamic University Malaysia (IIUM), with a Ph.D. in Computer Engineering. His research interests include IoT, AI, Blockchain, and acoustic wave electrochemistry biosensors, with a focus on interdisciplinary technology applications. He emphasises AI, problem-solving skills, and adaptability in the fast-paced tech field. His academic work significantly contributes to the field of ICT, particularly in the areas of biosensors and AI integration. He can be contacted at <a href="mailto:anwarzain@iium.edu.my">anwarzain@iium.edu.my</a>.</p>
	<p><b>Ahmad Adlan Abdul Halim</b> is a student at the Kulliyyah of Information and Communication Technology, International Islamic University Malaysia (IIUM). His academic focus is on Business Intelligence and Analysis. His research involves full-stack web systems integrated with Internet of Things (IoT) technologies. His work reflects a strong interest in combining data analytics and system development to enhance IoT security. He can be contacted at email: <a href="mailto:a.adlan@live.iium.edu.my">a.adlan@live.iium.edu.my</a>.</p>
	<p><b>Dek Rina</b> is a Physics student at the University of Syiah Kuala, specializing in Applied Physics, IoT, AI, Medical Physics, Geophysics, Optics, and Material Physics. Her research focuses on smart devices and sensors for analysing Patchouli Oil purity and characterization, with an emphasis on solving counterfeit issues using NIR Spectroscopy methods. She can be contacted email at <a href="mailto:dekrina@mhs.usk.ac.id">dekrina@mhs.usk.ac.id</a>.</p>