

# Security challenges and strategies for CNN-based intrusion detection model for IoT networks

Wan Fariza Wan Abdul Rahman, Nurul Taqiah Ab Aziz

Department of Computer Science, Faculty of Computer and Mathematical Sciences,  
Universiti Teknologi MARA Kelantan Branch, Kelantan, Malaysia

## Article Info

### Article history:

Received Aug 21, 2024

Revised Apr 20, 2025

Accepted Jul 3, 2025

### Keywords:

CNN

Deep learning

IDS

IoT

Security

## ABSTRACT

The rapid proliferation of internet-of-things (IoT) networks has revolutionized various industries but has also exposed them to a myriad of security threats. These networks are particularly vulnerable to sophisticated cyber-attacks due to their distributed nature, resource constraints, and the diverse range of connected devices. To safeguard IoT systems, intrusion detection systems (IDS) have emerged as a critical security measure. Among these, convolutional neural network (CNN)-based models offer promising capabilities in recognizing and mitigating malicious activities within IoT environments. This paper addresses the security challenges specific to IoT networks and explores the critical aspects of identifying malicious packets that threaten their integrity. It also delves into the general challenges associated with implementing IDS in IoT settings, such as the need for real-time detection, resource efficiency, and adaptability to evolving threats. The discussion extends to potential strategies for enhancing CNN-based IDS. The paper concludes by summarizing the key findings and proposing directions for future research to overcome the identified challenges, ultimately contributing to the development of more robust and effective IDS solutions for securing IoT networks.

This is an open access article under the [CC BY-SA](#) license.



## Corresponding Author:

Wan Fariza Wan Abdul Rahman

Department of Computer Science, Faculty of Computer and Mathematical Sciences

Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA Kelantan Branch

18500 Machang, Kelantan, Malaysia

Email: wfariza@uitm.edu.my

## 1. INTRODUCTION

Internet-of-things (IoT) is a system of connected objects embedded with sensors, software, and control systems. The IoT is an emerging communication paradigm in which devices serve as objects or 'things' that can sense their environment, connect, and exchange data over the Internet. IoT can be defined as an automated machine-to-machine (M2M) communication system that makes decisions and processes data operations without direct human intervention, improving the quality of human life in terms of comfort and efficiency.

Numerous practical IoT applications can be found in various domains, including healthcare, smart home, smart industry, and environmental monitoring. Recently, the IoT has played a vital role in the transformation of fields such as education, healthcare, and agriculture into better management. In agriculture, the traditional way of farming has been transformed into better water management and soil monitoring. Wearables, telemedicine, and remote patient monitoring have facilitated the healthcare sector. IoT has become an integral part of everyday life. However, the integration of real-world objects with IoT brings a range of cybersecurity

threats. Commonly found attacks in IoT are denial of service (DoS), man-in-the-middle (MITM) and so on. Such attacks can cause considerable damage to the IoT services. The intrusion detection system (IDS) is crucial in the IoT security framework to detect known and unknown attacks. The frequency and variety of security threats to these systems have increased in several ways, demonstrating the value of an effective intrusion detection system [1]. Due to the limited computing and storage capabilities of IoT devices and the specific protocols used, conventional IDSs may not be an option for IoT environments [2].

Security issues in IoT, with the extensive demand and continuous growth of various IoT applications, the vast amount of invaluable data produced makes IoT vulnerable to various security attacks. The security challenges in IoT systems are related to security issues arising in the different IoT layers. Physical damage, hardware failure, and power limitations are challenges faced in the physical layer. DoS attacks, sniffing, gateway attacks and unauthorized access are challenges relevant to the network layer. Malicious code attacks, application vulnerabilities, and software bugs are challenges faced in the application layer [3].

Unlike conventional internet technology infrastructure, IoT networks are deployed in hostile, heterogeneous, and dynamic environments, with potentially numerous types of networks and devices. There is no standard in the security protocols since the security solution for each device depends on the vendor and the heterogeneity of the devices in the IoT network. Due to the small processors in IoT devices, traditional security methods become impractical. The additional challenge includes mobility and resource constraints in terms of processor, memory, power, and size of the devices [4].

Vital information may be tampered with when IoT devices are compromised by malicious attackers exploiting their resource constraints and relevant vulnerabilities. An attack against IoT devices could lead to sensitive information leakage and can cause interruptions in workflows [5]. Accounting for the wide adoption of IoT, security threats can cause severe privacy problems and economic damage. Security is vital in IoT to maintain the customers' trust. Failure to maintain security will consequently make the IoT network vulnerable to security attacks, ultimately causing enormous financial and reputational losses [4].

Intrusion detection system, IDS can be classified as host-based, network-based, or hybrid IDS, based on the target location. Host-based IDS is specific to a system, and it is expensive as one IDS is required per host. Network-based IDS can well detect outside intrusion but require too much traffic to analyze. Hybrid IDS combines features of both host-based and network-based IDS. Thus, provides more security and flexibility. Centralized IDS use individual monitors for monitoring each host, as it does not scale according to requirement, thus providing less flexibility. Moreover, centralized IDS is prone to a single point of failure. Distributed IDS, on the other hand, works as a peer-to-peer (P2P) architecture, and in this case, each monitoring unit doubles up as an analysis unit as well [4].

In general, the IDS detects malware based on two main approaches: signature-based detection and anomaly-based detection [6]. The signature-based detection technique is not reasonably effective in real-world situations when the target is to detect new variants of malware, as the malware keeps on mutating, and the signature also keeps on changing. Anomaly-based detection techniques, on the other hand, presume that the malware traffic will be behaviorally different from normal traffic.

IDS for IoT; anomaly detection is a key technique used in IDS for IoT. It involves analyzing the collected data to identify deviations from normal behavior. Statistical methods, machine learning (ML) algorithms, and pattern recognition techniques are often employed for anomaly detection. For example, sudden spikes in network traffic, unusual device behavior, or unexpected communication patterns could indicate potential intrusions.

Although intrusion detection has been a considerable field of work for more than three decades, there are still open-ended research issues of the IDS for the IoT environment. The ML-based approach is advantageous for a wide range of malware classification. ML techniques are mainly used for feature engineering as they are lightweight and less complicated, making them a suitable candidate for developing security solutions for IoT [4]. ML versus deep learning (DL) solutions. In almost all areas including intrusion detection, learning-based approaches have been extensively used due to their distinctive nature of resolving real-time problems. ML as well as DL methods learn from existing data and predict the future behaviour of a system. By classifying the normal or abnormal behaviour of a system, various security attacks and intrusions in the IoT system for the application, network, and physical layers can be countered [7].

DL has been improved over ML in many computing domains due to current developments in hardware and powerful DL algorithms. DL algorithms, a subset of ML, are characterized by the complexity (or depth) of the hidden layers of neural networks (NN). ML contains either linear or nonlinear algorithms as a single layer.

In ML, the feature extraction (selection) is the first step that precedes the implementation of the model, while in DL, the feature extraction is embedded within the model. In IoT security, DL architectures are a powerful method of data exploration to learn about normal and abnormal behaviours. DL techniques are used in IoT security because they can perceptively predict future unknown attacks [8].

The efficiency of learning-based approaches depends on attack detection accuracy, true and false-positive rates, F1-score, and some other performance matrix. DL algorithms can be trained on devices with relatively high processing and memory capabilities because they require large datasets and the structure of neural networks is complex. ML algorithms, on the other hand, can be trained on devices with somewhat lower processor and memory properties. In terms of performance, the DL approaches provide higher accuracy and reliability compared to ML algorithms. The structure of DL algorithms is more complex than that of ML algorithms and requires larger dataset to be trained on [7]. Among DL NNs the convolutional neural network (CNN) is a well-known structure designed to process complex data. The CNN overcomes the typical limitations of conventional ML approaches and is mainly used in IDSs [9].

## **2. KEY ASPECTS IN RECOGNIZING MALICIOUS PACKET**

Common attacks in IoT networks include distributed denial of service (DDoS), eavesdropping, probe, side-channel, botnet, MITM, phishing, malware, port scan, brute force, flooding and spoofing [10], [11]. Distinguishing between malicious and normal packets is crucial for ensuring the security and stability of IoT networks. Malicious packets often contain harmful payloads designed to exploit vulnerabilities, disrupt network operations, or steal sensitive data. By accurately identifying these packets, IDS can mitigate potential attacks before they cause significant damage. Additionally, understanding the differences in packet behavior and intent allows for the development of more effective detection models, enhancing the network's resilience against evolving cyber threats. This proactive approach not only protects connected devices and data but also ensures the reliability and trustworthiness of the IoT ecosystem. Malicious packets typically differ from normal packets of data in several key aspects, including their payload content, behavior, and intent [12], [13].

### **2.1. Payload content**

Malicious packets often contain payload content that deviates from the expected or normal data patterns. The content may include exploit code, malware payloads, command-and-control (C2) instructions, or malicious scripts designed to compromise or manipulate target systems [14], [15]. In contrast, normal packets typically carry legitimate data relevant to the intended communication or application, such as HTTP requests, DNS queries, or sensor data in IoT environments.

### **2.2. Protocol violations**

Malicious packets may exploit vulnerabilities or weaknesses in network protocols to perform unauthorized actions or bypass security controls. For example, they may contain malformed headers, invalid protocol commands, or unusual packet sequences that violate protocol specifications [16], [17]. Normal packets adhere to established protocol standards and exhibit expected behaviors, such as following the prescribed communication sequence and structure.

### **2.3. Anomalous behavior**

Malicious packets often exhibit abnormal behavior that deviates from typical network traffic patterns [18]. This behavior may include scanning activities [19], port probing [20], brute-force attacks [21], or reconnaissance attempts [22] aimed at identifying and exploiting vulnerabilities in target systems. Normal packets, on the other hand, adhere to expected communication patterns and exhibit predictable behaviors based on the application or service they represent.

### **2.4. Source and destination information**

Malicious packets may originate from suspicious or unauthorized sources, such as known malicious IP addresses, botnet nodes, or compromised devices [23]. They may also target vulnerable or sensitive destinations, such as high-value servers, critical infrastructure components, or IoT devices with known security vulnerabilities. Normal packets typically originate from legitimate sources and target authorized destinations within the network or across the internet.

### 2.5. Payload encryption or obfuscation

Malicious packets may employ encryption, obfuscation, or encoding techniques to conceal their true intent or payload content [24]. This can make it challenging to detect and analyze malicious activity solely based on packet inspection. Normal packets may or may not use encryption but typically do not attempt to obfuscate their content in a manner designed to evade detection.

### 2.6. Frequency and volume

Malicious packets may exhibit unusual frequency or volume characteristics compared to normal traffic patterns. For example, they may generate a high volume of requests or connections in a short period, engage in rapid scanning activities, or exhibit bursts of traffic indicative of DoS attacks [25]. Normal packets are typically distributed more evenly over time and do not display abnormal spikes or surges in activity. By analyzing these differences, intrusion detection systems can identify and classify packets as either normal or malicious, enabling timely detection and mitigation of security threats in network environments.

## 3. GENERAL CHALLENGES OF IDS IMPLEMENTATION IN IOT

An IDS is a security mechanism that works mainly in the network layer of an IoT system. An IDS deployed for an IoT system should be able to analyze packets of data and generate responses in real-time, analyze data packets in different layers of the IoT network with different protocol stacks, and adapt to different technologies in the IoT environment [26]. An IDS that is designed for IoT-based smart environments should operate under stringent conditions of low processing capability, fast response, and high-volume data processing [2]. Therefore, conventional IDSs may not be fully suitable for IoT environments.

IoT security requires an up-to-date understanding of the security vulnerabilities of IoT networks. Zero-day attacks are inevitable in real-world networks, and introducing new devices to the IoT system is expected. Furthermore, network traffic distribution is subject to change as these new devices join the network [27].

The implementation of a strong security mechanism for IoT systems depends on the strength of the power and memory factors of IoT devices. However, IoT devices are known to be constrained devices in terms of processor, power, memory, and size. With constraints in place, maintaining security is a challenge. Since IoT devices are computationally less powerful and embedded with limited memory, lightweight, yet robust solutions should be considered while designing, developing, and implementing security protocols for IoT. This is to ensure that the protocol is compatible with the device's limited capabilities [2], [4], [7]. Apart from the challenges mentioned earlier, several CNN-specific challenges need to be focused on including data diversity, limited adaptation to IoT characteristics, high computational complexity, dataset issues and so on. These ideas are portrayed in the following subsections.

### 3.1. Data diversity

Today, with the expansion of IoT different applications, IoT heterogeneous devices produce various heterogeneous data with different scales according to the type of application. The data often contains a mixture of structured and unstructured information. The diversity and heterogeneity of generated data with large volumes from various applications pose challenges in designing effective feature extraction methods that capture relevant patterns for intrusion detection. Thus, managing the produced data is one of the crucial challenges [27].

### 3.2. Limited adaptation to IoT characteristics

Traditional CNN architectures are often designed and trained on large-scale image datasets like ImageNet, which may not fully capture the characteristics of IoT network traffic data. IoT data, such as network packets or sensor readings, exhibit different patterns and distributions compared to natural images. Therefore, CNN architectures need enhancements to better adapt to the unique features of IoT data [11], [28].

CNN architectures, such as AlexNet, VGG, and ResNet, have been widely used in various computer vision tasks, including image classification, object detection, and segmentation [29]. These architectures typically consist of convolutional layers followed by pooling layers for feature extraction, followed by fully connected layers for classification. While these architectures have demonstrated impressive performance on tasks like image classification, they may not be directly suitable for intrusion detection in IoT networks without enhancements.

### 3.3. High computational complexity

Traditional CNN architectures are typically designed for high accuracy and may contain a large number of parameters and computations. The training time and computational complexity of DL methods depend on how complex the structure is. For example, ensemble-based [30] and stack-based DL algorithms are computationally costly [31]. The deployment of these methods may create bottlenecks. It can be prohibitive for real-time implementation on resource-constrained IoT devices, which often have limited processing power, memory, and energy resources. Therefore, reducing the computational burden while maintaining or improving detection accuracy must be considered while designing and developing a learning-based algorithm for enhancement [7].

### 3.4. Datasets issue

Learning-based methods depend on the existing data or information from where the models learn and classify the incoming traffic as normal or abnormal. However, finding real-world IoT-dedicated datasets to train learning-based algorithms is challenging due to the limited datasets available on public platforms. Since network activities (normal and malicious) are changing frequently, newer and more comprehensive datasets which consist of a broad spectrum of malware activities are required to guarantee the effectiveness of the developed model over time [11].

Moreover, ML and DL algorithms may produce a higher false-positive rate if the dataset used in training is not realistic. High-quality real-world and comprehensive IoT training datasets are required to train these methods to produce better and smarter decisions [32]. Generating high-quality training datasets remains a challenge for contemporary scholars in the field of IoT-related academic investigations [7].

DL is a new type of ML in which the model itself can govern the prediction accuracy. IoT systems with contextual and adapted assistance, DL models are best fit for classification and prediction due to self service nature. ML and DL can provide promising results for IoT networks in several ways e.g., huge amount of data is produced by IoT systems which can be utilized by ML and DL techniques to enable IoT systems a better and smart decision [32].

### 3.5. Data quality and availability

CNN model development process requires more realistic and diverse IoT datasets which represent various types of attacks. Unfortunately, the existing datasets may not capture the full range of potential attacks and normal behavior in real-world IoT networks. High-quality labelled datasets are essential for training effective CNN models. However, obtaining comprehensive and well-labelled IoT intrusion datasets is challenging. There is a lack of extensive, labelled, and diverse datasets specific to IoT environments.

### 3.6. Class imbalance

Intrusion detection datasets often suffer from imbalanced classes, with a disproportionate amount of normal traffic compared to attack traffic. This imbalance can lead to biased models that perform poorly on minority classes [33]. Techniques for data augmentation and synthetic data generation can be considered to enhance training datasets [34].

### 3.7. Non-image data handling

While CNNs excel at processing image data, adapting them to handle non-image data, such as network traffic, sensor readings, or log files, requires innovative approaches. The main challenges involve feature representation and domain adaptation. Feature representation refers to a situation where the non-image data requires effective preprocessing and transformation into a format suitable for CNN [35]. This transformation process however can be complex and may not always capture the intrinsic characteristics of the data. Domain adaptation, on the other hand, refers to the techniques proposed in [36] to adapt CNN for non-image data without losing the advantages of its deep architecture. This approach is still under research.

### 3.8. Resource constraint

IoT devices are often resource-constrained, operating with limited memory, processing power, and energy supply. Traditional CNN architectures may not be optimized for resource efficiency, leading to challenges in deploying them on IoT devices. Enhancements are needed to develop lightweight architectures that can operate efficiently within the constraints of IoT environments. One example of the research is in [37]. CNN models can be computationally intensive, requiring significant processing power and memory. IoT devices, however, are typically resource-constrained, making it challenging to deploy these models on edge devices.

### 3.9. Real-time detection and processing constraint

Intrusion detection in IoT networks often requires real-time or near-real-time processing to promptly identify and respond to security threats. However, traditional CNN architectures may not be optimized for low-latency inference, which is crucial for real-time applications. Enhancements are necessary to reduce inference time and ensure timely detection of intrusions in IoT networks. Some of the proposed works to tackle this issue can be seen in [38], [39]. Achieving real-time detection with CNN models can be difficult due to their computational complexity. Thus, ensuring low latency in processing and classifying data is crucial for effective real-time intrusion detection.

### 3.10. Adversarial robustness

CNN-based IDS might correctly classify normal and attack traffic under standard conditions but fail to detect sophisticated adversarial attacks that subtly alter the traffic patterns [40]. IoT networks are vulnerable to various security threats, including adversarial attacks aimed at fooling ML models. Traditional CNN architectures may lack robustness against such attacks, as they are primarily optimized for accuracy on clean data. Enhancements are needed to improve the robustness of intrusion detection models against adversarial manipulations in IoT environments.

## 4. METHOD

This study follows a structured approach to investigate the security challenges in IoT networks, with a particular focus on intrusion detection and malicious packet identification. The methodology is divided into three main phases: literature review and problem identification, analysis of intrusion detection challenges, and summary of CNN-based IDS strategies. The transformation from the literature review to the summary of CNN-based IDS strategies occurs as researchers systematically analyze and synthesize the findings from previous studies. By evaluating the strengths and weaknesses of existing CNN-based IDS approaches, a comprehensive summary can be formed, highlighting effective strategies, architectural choices, and optimization techniques. This progression ensures that the proposed research is well-grounded and aligned with current advancements in the field. The methodology used for this research has been illustrated in Figure 1.

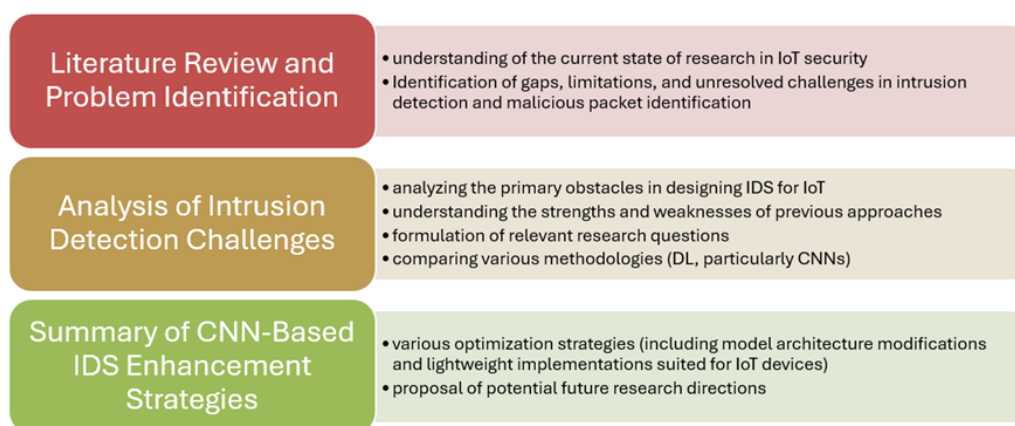


Figure 1. Three main phases in the research methodology

### 4.1. Literature review and problem identification

A comprehensive review of existing literature on IoT security threats, intrusion detection techniques, and ML-based solutions was conducted. This helped identify the key challenges in implementing IDS in resource-constrained IoT environments and the limitations of traditional approaches. A literature review is essential as it provides a comprehensive understanding of the current state of research in IoT security. Examining existing studies helps identify gaps, limitations, and unresolved challenges in intrusion detection and malicious packet identification. This foundational knowledge allows researchers to understand the strengths and weaknesses of previous approaches, leading to the formulation of relevant research questions.

#### 4.2. Analysis of intrusion detection challenges

The study analyzed the primary obstacles in designing IDS for IoT, including limited computational resources, high network traffic volume, and evolving attack patterns. Different IDS methodologies, such as signature-based and anomaly-based approaches, concerning IoT constraints were identified. The role of DL, particularly CNNs, in enhancing detection accuracy was explored by reviewing recent studies. Comparing various methodologies and findings facilitates the identification of recurring issues, emerging trends, and effective strategies, which are crucial for precisely defining the research problem and justifying the need for further investigation.

#### 4.3. Summary of CNN-based IDS enhancement strategies

To address the identified challenges, various optimization strategies for CNN-based IDS were examined. This included model architecture modifications and lightweight implementations suited for IoT devices. The findings were presented to propose potential future research directions in IoT intrusion detection.

### 5. RESULTS-POTENTIAL STRATEGIES FOR COMMON ISSUES IN CNN-BASED IDS

As previously discussed in section 3., several challenges in the implementation of IDS in IoT networks involve the heterogeneity of the data and devices in the network itself. From a CNN point of view, the challenges are more related to the dataset issues and CNN architectures in making it suitable for the IoT environment. Based on examination and analysis performed on previous studies, Table 1 below summarizes the challenges and potential solutions to tackle the issues of CNN-based IDS.

Table 1. The strategies/possible solutions to common issues in CNN-based IDS

Challenges	Issues	Strategies/Possible solutions
Lack of high-quality labelled datasets	Limited comprehensive and well-labelled IoT intrusion datasets	Data augmentation [41]. Synthetic data generation [34].
Non-image data handling	Complex non-image data pre-processing and transformation into a CNN suitable format	Non-image-to-image data conversion
Imbalanced datasets	A significant class imbalance, with normal traffic vastly outnumbering anomalous or malicious traffic	Advanced techniques for handling imbalanced datasets, such as SMOTE (synthetic minority over-sampling technique) [42] and other resampling methods
Real-time detection	Due to resource constraints and the need for low-latency processing	Optimization of CNN architectures for real-time performance [39]. Leveraging edge computing and distributed processing to offload computation and reduce latency
Adversarial attacks	Vulnerability to adversarial attacks – small perturbations in input data may lead to incorrect classifications	Adversarial training [43].
Resource constraints	Limited computational and power resources of the IoT devices – restrict the deployment of complex CNN models	Lightweight CNN architectures that can run on resource-constrained IoT devices [44]. Model compression and optimization techniques to reduce the computational footprint of CNN models
Adaptability to new threats	Generalization to new and unknown attacks that were not present in the training data, making them less effective for detecting zero-day attacks	Adaptive residual blocks [45], [46]. Lightweight convolutional filters [47], [48].

### 6. DISCUSSION

The inherent vulnerabilities of IoT devices, such as limited computational resources and heterogeneous protocols, pose significant challenges for the development of effective IDS solutions. CNN-based models, while powerful in recognizing patterns and anomalies, face obstacles in terms of detection accuracy, real-time processing, and adaptability to new and evolving threats.

Key aspects in recognizing malicious packets (involving feature extraction) and the classification of normal versus abnormal behavior remain central to the success of CNN-based IDS. However, the balance between detection accuracy and computational efficiency is a critical consideration, especially given the resource constraints typical of IoT devices. Moreover, the development of CNN-based IDS in IoT networks must account for the diversity of devices and the dynamic nature of network traffic. Strategies such as data augmentation, adversarial training, and lightweight architectures are promising avenues to enhance detection performance. However, these strategies must be carefully tailored to the specific characteristics of IoT environments to ensure their practical applicability.

Intrusion detection in IoT networks faces several critical challenges, starting with the lack of high-quality labelled datasets. The limited availability of well-labelled IoT intrusion datasets hinders the training of robust models, making data augmentation and synthetic data generation essential solutions to enhance dataset quality. Another challenge lies in non-image data handling, as IoT traffic data is typically in non-image formats, requiring complex preprocessing before it can be fed into a CNN model. One proposed solution is converting non-image data into image representations to better leverage CNN capabilities.

Additionally, imbalanced datasets pose a significant issue, where normal traffic vastly outnumbers malicious traffic, leading to biased model performance. Techniques such as SMOTE and resampling methods can be employed to balance datasets and improve detection accuracy. The need for real-time detection further complicates the deployment of CNN models, as resource constraints demand low-latency processing. Optimizing CNN architectures for speed and efficiency, along with leveraging edge computing, can help meet real-time requirements.

Another pressing concern is the vulnerability of CNN models to adversarial attacks, where small perturbations in input data can lead to incorrect classifications. Adversarial training has been suggested as a potential solution to improve model robustness. Moreover, resource constraints on IoT devices limit the feasibility of deploying complex DL models. This challenge can be addressed by designing lightweight CNN architectures and applying model compression techniques to reduce computational demands.

Lastly, adaptability to new threats, especially zero-day attacks, remains a major hurdle. Since intrusion detection models struggle to generalize to unseen threats, adaptive residual blocks and lightweight convolutional filters can enhance their ability to detect new and evolving attack patterns. Addressing these challenges is crucial for developing more effective and efficient CNN-based IDS systems for IoT networks.

One promising area of future research is the development of efficient non-image-to-image conversion techniques to transform network traffic data into image representations while preserving crucial patterns and relationships. Optimizing these conversion methods can improve the effectiveness of CNN-based IDS.

Addressing data imbalance remains a significant challenge. Future research could focus on exploring novel approaches for handling imbalanced data and generating synthetic samples of rare attack types. This could improve model performance in detecting underrepresented attack patterns. Similarly, there is a need for a research ultra-low latency CNN architectures for IoT that can operate in real-time environments with minimal computational overhead. This research could focus on optimizing network architectures, reducing redundant computations, and leveraging specialized hardware for edge-based processing.

Given the growing threat of adversarial attacks, it is essential to investigate the robustness against adversarial attacks by exploring defense mechanisms such as self-supervised learning, anomaly detection techniques, or adversarial training strategies. Strengthening CNN models against adversarial perturbations can enhance their reliability in real-world IoT deployments. Moreover, the development of the DL model in resource-constrained IoT devices requires research on energy-efficient CNNs through techniques that can significantly reduce computational requirements while maintaining high detection accuracy.

Finally, ensuring adaptability to new and unknown threats is critical in cybersecurity. Research into generalization for zero-day attacks could focus on meta-learning, continual learning, or self-evolving models that can adapt to emerging threats without extensive retraining. By enabling models to learn from a limited number of new attack instances, future IDS could become more resilient to evolving cyber threats.

## 7. CONCLUSION

In conclusion, securing IoT networks through CNN-based IDS presents both significant challenges and opportunities. While CNN models are well-suited for the task of pattern recognition in complex datasets, their deployment in resource-constrained and dynamic IoT environments requires innovative approaches to



overcome limitations related to computational efficiency, real-time processing, and adaptability. The paper has identified key security issues, general challenges in IDS implementation, and potential strategies that can enhance the effectiveness of CNN-based models in detecting malicious activities within IoT networks. The significance of our findings lies in their potential to enhance real-time intrusion detection in IoT networks while maintaining computational efficiency. Given the increasing deployment of IoT devices in critical sectors such as healthcare, smart cities, and industrial automation, improving intrusion detection is essential to mitigate cyber threats. Failure to strengthen IDS mechanisms could lead to widespread IoT-based cyberattacks, compromising critical infrastructure. Without adaptive CNN models, attackers can exploit zero-day vulnerabilities, leading to severe financial and operational disruptions.

Future research should focus on refining the strategies previously stated, particularly through the development of more lightweight CNN architectures and the exploration of hybrid approaches that combine the strengths of CNNs with other methodologies. A comparative study among different strategies should be conducted to determine the most effective approach for IoT security. Real-time deployment of CNN-based IDS should be conducted in real IoT environments to evaluate their performance under live network conditions, against various types of attacks. Continuous updates and improvements in the training datasets used for IDS will be essential to maintain the relevance and accuracy of detection models as IoT threats continue to evolve. By addressing these challenges, it is possible to advance the development of robust, efficient, and scalable IDS solutions that can provide a critical layer of security for the ever-expanding IoT ecosystem.

## FUNDING INFORMATION

This research is funded by Ministry of Higher Education Malaysia under Fundamental Research Grant Scheme (FRGS/1/2023/ICT07/UITM/02/2).

## AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Wan Fariza Wan Abdul Rahman	✓	✓		✓	✓	✓	✓		✓	✓		✓	✓	✓
Nurul Taqiah Ab Aziz		✓	✓		✓	✓	✓	✓		✓	✓			

C : Conceptualization

M : Methodology

So : Software

Va : Validation

Fo : Formal Analysis

I : Investigation

R : Resources

D : Data Curation

O : Writing - Original Draft

E : Writing - Review & Editing

Vi : Visualization

Su : Supervision

P : Project Administration

Fu : Funding Acquisition

## CONFLICT OF INTEREST STATEMENT

The authors declare no conflict of interest.

## DATA AVAILABILITY

All data used in this study are derived from previously published sources, which are cited within the manuscript.

## REFERENCES




- [1] J. C. S. Sicato, S. K. Singh, S. Rathore, and J. H. Park, "A comprehensive analyses of intrusion detection system for IoT environment," *Journal of Information Processing Systems*, vol. 16, no. 4, pp. 975–990, 2020, doi: 10.3745/JIPS.03.0144.
- [2] M. F. Elrawy, A. I. Awad, and H. F. A. Hamed, "Intrusion detection systems for IoT-based smart environments: a survey," *Journal of Cloud Computing*, vol. 7, no. 1, p. 21, Dec. 2018, doi: 10.1186/s13677-018-0123-6.
- [3] S. A. Kumar, T. Vealey, and H. Srivastava, "Security in internet of things: challenges, solutions and future directions," in *2016 49th Hawaii International Conference on System Sciences (HICSS)*, 2016, pp. 5772–5781, doi: 10.1109/HICSS.2016.714.
- [4] N. Mishra and S. Pandya, "Internet of things applications, security challenges, attacks, intrusion detection, and future visions: a systematic review," *IEEE Access*, vol. 9, pp. 59353–59377, 2021, doi: 10.1109/ACCESS.2021.3073408.

- [5] M. Bagaa, T. Taleb, J. B. Bernabe, and A. Skarmeta, "A machine learning security framework for IoT systems," *IEEE Access*, vol. 8, pp. 114066–114077, 2020, doi: 10.1109/ACCESS.2020.2996214.
- [6] Y. Otoum and A. Nayak, "AS-IDS: anomaly and signature based IDS for the internet of things," *Journal of Network and Systems Management*, vol. 29, no. 3, p. 23, Jul. 2021, doi: 10.1007/s10922-021-09589-6.
- [7] S. Khanam, I. Bin Ahmedy, M. Y. Idna Idris, M. H. Jaward, and A. Q. Bin Md Sabri, "A survey of security challenges, attacks taxonomy and advanced countermeasures in the internet of things," *IEEE Access*, vol. 8, pp. 219709–219743, 2020, doi: 10.1109/ACCESS.2020.3037359.
- [8] K. Albulayhi, A. A. Smadi, F. T. Sheldon, and R. K. Abercrombie, "IoT intrusion detection taxonomy, reference architecture, and analyses," *Sensors*, vol. 21, no. 19, p. 6432, Sep. 2021, doi: 10.3390/s21196432.
- [9] L. Mohammadpour, T. C. Ling, C. S. Liew, and A. Aryanfar, "A survey of CNN-based network intrusion detection," *Applied Sciences*, vol. 12, no. 16, p. 8162, Aug. 2022, doi: 10.3390/app12168162.
- [10] N. Islam *et al.*, "Towards machine learning based intrusion detection in IoT networks," *Computers, Materials & Continua*, vol. 69, no. 2, pp. 1801–1821, 2021, doi: 10.32604/cmc.2021.018466.
- [11] A. Khraisat and A. Alazab, "A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges," *Cybersecurity*, 2021, doi: 10.1186/s42400-021-00077-7.
- [12] I. Hafeez, M. Antikainen, A. Y. Ding, and S. Tarkoma, "IoT-KEEPER: detecting malicious IoT network activity using online traffic analysis at the edge," *IEEE Transactions on Network and Service Management*, vol. 17, no. 1, pp. 45–59, Mar. 2020, doi: 10.1109/TNSM.2020.2966951.
- [13] L. Deri and F. Fusco, "Using deep packet inspection in cybertraffic analysis," in *2021 IEEE International Conference on Cyber Security and Resilience (CSR)*, Jul. 2021, pp. 89–94, doi: 10.1109/CSR51186.2021.9527976.
- [14] I. Dube and G. Wells, "An analysis of the use of DNS for malicious payload distribution," in *2020 2nd International Multidisciplinary Information Technology and Engineering Conference (IMITEC)*, Nov. 2020, pp. 1–12, doi: 10.1109/IMITEC50163.2020.9334104.
- [15] Z. Ismail, A. Jantan, and M. Najwadi, "A framework for detecting botnet command and control communication over an encrypted channel," *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 1, pp. 319–326, 2020, doi: 10.14569/IJACSA.2020.0110140.
- [16] P. C. Amusuo, R. A. C. Méndez, Z. Xu, A. Machiry, and J. C. Davis, "Systematically detecting packet validation vulnerabilities in embedded network stacks," in *2023 38th IEEE/ACM International Conference on Automated Software Engineering (ASE)*, Sep. 2023, pp. 926–938, doi: 10.1109/ASE56229.2023.00095.
- [17] Ö. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin, "A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions," *Electronics*, vol. 12, no. 6, p. 1333, Mar. 2023, doi: 10.3390/electronics12061333.
- [18] A. A. Bahashwan, M. Anbar, I. H. Hasbullah, Z. R. Alashhab, and A. Bin-Salem, "Flow-based approach to detect abnormal behavior in neighbor discovery protocol (NDP)," *IEEE Access*, vol. 9, pp. 45512–45526, 2021, doi: 10.1109/ACCESS.2021.3066630.
- [19] M. Kallitsis, R. Prajapati, V. Honavar, D. Wu, and J. Yen, "Detecting and interpreting changes in scanning behavior in large network telescopes," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 3611–3625, 2022, doi: 10.1109/TIFS.2022.3211644.
- [20] A. Mirza, "Port scanning: techniques, tools and detection." Jun. 19, 2023, doi: 10.31224/3053.
- [21] J. Luxemburk, K. Hynek, and T. Cejka, "Detection of HTTPS brute-force attacks with packet-level feature set," *2021 IEEE 11th Annual Computing and Communication Workshop and Conference, CCWC 2021*, pp. 114–122, 2021, doi: 10.1109/CCWC51732.2021.9375998.
- [22] W. Mazurczyk and L. Cavaglione, "Cyber reconnaissance techniques," *Communications of the ACM*, vol. 64, no. 3, pp. 86–95, 2021, doi: 10.1145/3418293.
- [23] N. Sharma, M. Sharma, and D. P. Sharma, "A trust based scheme for spotting malicious node of wormhole in dynamic source routing protocol," in *2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, Oct. 2020, pp. 1232–1237, doi: 10.1109/I-SMAC49090.2020.9243369.
- [24] D.-P. Pham, D. Marion, M. Mastio, and A. Heuser, "Obfuscation revealed: leveraging electromagnetic signals for obfuscated malware classification," in *Annual Computer Security Applications Conference*, Dec. 2021, pp. 706–719, doi: 10.1145/3485832.3485894.
- [25] M. Moure-Garrido, C. Campo, and C. Garcia-Rubio, "Real time detection of malicious DoH traffic using statistical analysis," *Computer Networks*, vol. 234, p. 109910, Oct. 2023, doi: 10.1016/j.comnet.2023.109910.
- [26] A. A. Gendreau and M. Moorman, "Survey of intrusion detection systems towards an end to end secure internet of things," *Proceedings - 2016 IEEE 4th International Conference on Future Internet of Things and Cloud, FiCloud 2016*, pp. 84–90, 2016, doi: 10.1109/FiCloud.2016.20.
- [27] A. Ghaffari, N. Jelodari, S. Pouralish, N. Derakhshanfard, and B. Arasteh, "Securing internet of things using machine and deep learning methods: a survey," *Cluster Computing*, vol. 27, no. 7, pp. 9065–9089, Oct. 2024, doi: 10.1007/s10586-024-04509-0.
- [28] A. Thakkar and R. Lohiya, "A review on machine learning and deep learning perspectives of IDS for IoT: recent updates, security issues, and challenges," *Archives of Computational Methods in Engineering*, vol. 28, no. 4, pp. 3211–3243, Jun. 2021, doi: 10.1007/s11831-020-09496-0.
- [29] I. Singh, G. Goyal, and A. Chandel, "AlexNet architecture based convolutional neural network for toxic comments classification," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 9, pp. 7547–7558, Oct. 2022, doi: 10.1016/j.jksuci.2022.06.007.
- [30] A. Mohammed and R. Kora, "A comprehensive review on ensemble deep learning: Opportunities and challenges," *Journal of King Saud University - Computer and Information Sciences*, vol. 35, no. 2, pp. 757–774, Feb. 2023, doi: 10.1016/j.jksuci.2023.01.014.
- [31] J. Wang *et al.*, "StackRec," in *Proceedings of the 44th International ACM SIGIR Conference on Research and Development in Information Retrieval*, Jul. 2021, pp. 357–366, doi: 10.1145/3404835.3462890.
- [32] W. Iqbal, H. Abbas, M. Daneshmand, B. Rauf, and Y. A. Bangash, "An in-depth analysis of IoT security requirements, challenges, and their countermeasures via software-defined security," *IEEE Internet of Things Journal*, vol. 7, no. 10, pp. 10250–10276, Oct. 2020, doi: 10.1109/IIOT.2020.2997651.




- [33] F. Thabtah, S. Hammoud, F. Kamalov, and A. Gonsalves, "Data imbalance in classification: experimental evaluation," *Information Sciences*, vol. 513, pp. 429–441, Mar. 2020, doi: 10.1016/j.ins.2019.11.004.
- [34] N. Jaipuria *et al.*, "Deflating dataset bias using synthetic data augmentation," *IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops*, vol. 2020-June, pp. 3344–3353, 2020, doi: 10.1109/CVPRW50498.2020.00394.
- [35] M. Azizjon, A. Jumabek, and W. Kim, "1D CNN based network intrusion detection with normalization on imbalanced data," in *2020 International Conference on Artificial Intelligence in Information and Communication (ICAIIIC)*, Feb. 2020, pp. 218–224, doi: 10.1109/ICAIIIC48513.2020.9064976.
- [36] A. Singla, E. Bertino, and D. Verma, "Preparing network intrusion detection deep learning models with minimal data using adversarial domain adaptation," *Proceedings of the 15th ACM Asia Conference on Computer and Communications Security, ASIA CCS 2020*, pp. 127–140, 2020, doi: 10.1145/3320269.3384718.
- [37] S. Rizvi, M. Scanlon, J. McGibney, and J. Sheppard, "Deep learning based network intrusion detection system for resource-constrained environments," *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*, vol. 508 LNICST, pp. 355–367, 2023, doi: 10.1007/978-3-031-36574-4\_21.
- [38] M. Jouhari and M. Guizani, "Lightweight CNN-BiLSTM based intrusion detection systems for resource-constrained IoT devices," in *2024 International Wireless Communications and Mobile Computing (IWCMC)*, May 2024, pp. 1558–1563, doi: 10.1109/IWCMC61514.2024.10592352.
- [39] I. Idrissi, M. Azizi, and O. Moussaoui, "A lightweight optimized deep learning-based host-intrusion detection system deployed on the edge for IoT," *International Journal of Computing and Digital Systems*, vol. 11, no. 1, pp. 209–216, Jan. 2022, doi: 10.12785/ijcds/110117.
- [40] X. Fu, N. Zhou, L. Jiao, H. Li, and J. Zhang, "The robust deep learning-based schemes for intrusion detection in internet of things environments," *Annals of Telecommunications*, vol. 76, no. 5–6, pp. 273–285, Jun. 2021, doi: 10.1007/s12243-021-00854-y.
- [41] Y. Zhang and Q. Liu, "On IoT intrusion detection based on data augmentation for enhancing learning on unbalanced samples," *Future Generation Computer Systems*, vol. 133, pp. 213–227, Aug. 2022, doi: 10.1016/j.future.2022.03.007.
- [42] R. Mohammad, F. Saeed, A. A. Almazroi, F. S. Alsubaei, and A. A. Almazroi, "Enhancing intrusion detection systems using a deep learning and data augmentation approach," *Systems*, vol. 12, no. 3, p. 79, Mar. 2024, doi: 10.3390/systems12030079.
- [43] C. Zhang, X. Costa-Perez, and P. Patras, "Adversarial attacks against deep learning-based network intrusion detection systems and defense mechanisms," *IEEE/ACM Transactions on Networking*, vol. 30, no. 3, pp. 1294–1311, Jun. 2022, doi: 10.1109/TNET.2021.3137084.
- [44] K. K. S. R. Aleti, S. R. Aleti, K. Kurakula, and P. Goswami, "Evaluation of lightweight CNN architectures for multi-species animal image classification," 2024, [Online]. Available: [www.bth.se](http://www.bth.se).
- [45] C. Dong, L. Liu, Z. Li, and J. Shang, "Towards adaptive residual network training: a neural-ODE Perspective," *37th International Conference on Machine Learning, ICML 2020*, vol. PartF168147–4, pp. 2594–2604, 2020.
- [46] K. Park, J. W. Soh, and N. I. Cho, "A dynamic residual self-attention network for lightweight single image super-resolution," *IEEE Transactions on Multimedia*, vol. 25, pp. 907–918, 2023, doi: 10.1109/TMM.2021.3134172.
- [47] Q. Xia, S. Dong, and T. Peng, "An abnormal traffic detection method for IoT devices based on federated learning and depthwise separable convolutional neural networks," in *2022 IEEE International Performance, Computing, and Communications Conference (IPCCC)*, Nov. 2022, pp. 352–359, doi: 10.1109/IPCCC55026.2022.9894354.
- [48] G. Bao, M. B. Graeber, and X. Wang, "Depthwise multiception convolution for reducing network parameters without sacrificing accuracy," in *2020 16th International Conference on Control, Automation, Robotics and Vision (ICARCV)*, Dec. 2020, pp. 747–752, doi: 10.1109/ICARCV50220.2020.9305369.

## BIOGRAPHIES OF AUTHORS



**Wan Fariza Wan Abdul Rahman**    is a senior lecturer at the Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA (UiTM) Kelantan, Malaysia. She earned her Ph.D. in Computer Engineering from International Islamic University of Malaysia, specializing in computer networking and the IoT. Her research expertise spans computer networking protocols, computer security, IoT, and CNN-based pattern recognition. At UiTM Kelantan, Dr. Wan Fariza serves as the Industrial Training Coordinator for the Diploma in Computer Science students. She is a recipient of several prestigious awards from UiTM Kelantan, including the Teaching Award in the Science and Technology category, the Excellence Service Award, and the Exemplary Lecturer Award. As a project leader, she has also secured funding through the Fundamental Research Grant Scheme (FRGS) from Ministry of Higher Education Malaysia. Her research interests continue to focus on computer security, IoT, and pattern recognition. She can be contacted at email: [wfariza@uitm.edu.my](mailto:wfariza@uitm.edu.my).



**Nurul Taqiah Ab Aziz**    is a dedicated postgraduate student pursuing a Master's degree in Computer Science at Universiti Teknologi MARA (UiTM) Kelantan, Malaysia. Her passion for Computer Science was sparked during her high school years, leading her to pursue studies in this dynamic field. She earned her Bachelor's degree in Computer Science from Universiti Teknologi Malaysia (UTM) Johor Bahru in 2015. Following her graduation, Nurul gained practical experience working in her hometown before embarking on her current Master's research. Her research interests include computer networking, the IoT, and CNN-based architectures. She can be contacted at email: [nurultaqiah.abaziz@gmail.com](mailto:nurultaqiah.abaziz@gmail.com).