INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION

journal homepage : www.joiv.org/index.php/joiv

IoT Attack Detection Using Machine Learning and Deep Learning in Smart Home

Sharifah Nabila binti S Azli Sham [a,*], Khairul Khalil Ishak [b], Noor Afiza Mat Razali [a], Normaizeerah Mohd Noor [a], Nor Asiakin Hasbullah [a]

[a] *Defence Science and Technology Faculty, National Defence University of Malaysia, Sungai Besi, Kuala Lumpur Malaysia*
[b] *Center of Cyber Security and Big Data Management and Science University Shah Alam, Selangor, Malaysia*
Corresponding author: [*]sharifahnabila99@gmail.com

***Abstract*—The Internet of Things (IoT) has revolutionized the traditional Internet, pushing past its former boundaries by implementing smart linked gadgets. The IoT is steadily becoming a staple of everyday life, having been implemented into various diverse applications, such as cities, smart homes, and transportation. However, despite the technological advancements that the IoT brings, various new security risks have also been introduced due to the development of new types of attacks. This prevents current intelligent IoT applications from adaptively learning from other intelligent IoT applications, which leaves them in a volatile state. In this paper, we conducted a structured literature review (SLR) on Smart Home's IoT attack detection using machine learning and deep learning. Four journal databases were used to perform this review: IEEE, Science Direct, Association for Computing Machinery (ACM), and SpringerLink. Sixty articles were selected and studied, where we noted the various patterns and techniques present in the framework of the selected research. We also took note of the different machine learning and deep learning methods, the types of attacks, and the Network layers present in Smart Home. By conducting an SLR, we analyzed the numerous techniques of IoT attack detection for smart homes proposed by various theoretical studies. We enhanced the studied literature by proposing a new solution for better IoT attack detection in smart homes.**

***Keywords*— Cybersecurity framework; IoT; detection; attacks; smart home; machine learning.**

Manuscript received 2 Oct. 2023; revised 17 Jan. 2024; accepted 23 Feb. 2024. Date of publication 31 Mar. 2024.

I. INTRODUCTION

The Internet of Things (IoT) has recently extended into many parts of daily life. Smart cities and connected rural environments are examples of locations connected to networked technology, such as Internet of Things (IoT) devices and sensors, which help to improve the efficiency of services and the quality of citizens' lives. IoT devices have revolutionized the home automation sector, forming smart homes, which then, in part, make up smart cities. They have also helped enhance the personal home lifestyle, making monitoring and operating home appliances and systems more accessible and convenient [1].

However, as this technology is still in its infancy, it is still very volatile and vulnerable to potential threats. Based on research conducted by [2], IoT – Home Advanced Security System has stated that the critical issue in smart homes is their lack of security. Attacks are typically described by the layer of IoT infrastructure attacked, but because IoT infrastructure isn't standardized, it can be categorized into the following layers instead.

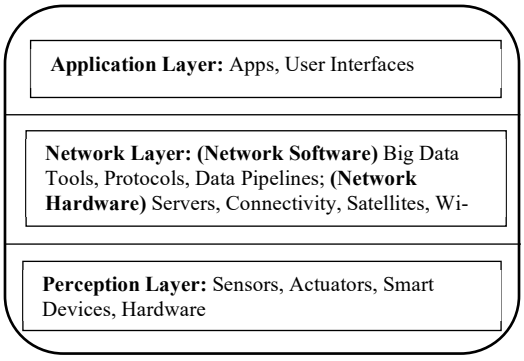

Fig. 1 IoT architecture [3]

Figure 1 shows the IoT architecture, including the perception, network, and application layers [3]. The perception layer stores the data of a physical environment

collected by a sensor [3]. This layer collects a large amount of data from the smart devices, which then circulates in the IoT. The data from all the smart devices and objects will then be delivered through a shared network, which requires the adoption of specific standards and protocols.

The second layer is the network layer, which defines the protocols that smart objects use to communicate with one another, including traditional and IoT-specific protocols. The network layer can also transmit data even when network connectivity is low. Before reaching their destination or a data storage place, the data may be transferred and re-transmitted multiple times between numerous intermediary relay nodes. Some data analytics are used on this layer to keep track of this traffic.

Next is the application layer, which comprises user interfaces, frameworks, and other components. Consumers can use the APIs of this layer to process the system's data. The perception layer and the application layer represent physical devices. Lastly, the network layer serves as the link between the IoT physical device and the IoT application.

Most attackers will target the network layer, as it is the most accessible layer of Smart Home to break into. Even though most IoT devices use encrypted network transmission, side-channel information leakage to on-path external adversaries can still occur because user in-home activities are highly connected at any time [4]. Examples of attacks that often appear in the network layer are traffic attacks, sniffing, DoS, wormholes, man-in-the-middle attacks, eavesdropping, intrusions, and DDoS [4], [5], [6], [7], [8], [9], [10], [11], [12], [13], [14], [15], [16].

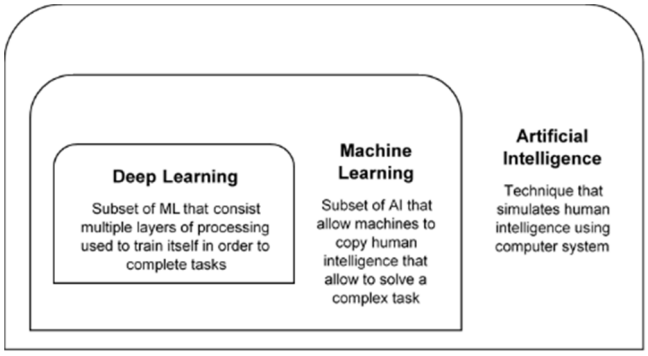

Fig. 2 The relationship between the concepts of AI, ML, and DL [17]

Machine learning is being used in smart homes to enhance attack detection accuracy and predict future attacks [18]. Figure 2 displays the relationship between AI, ML, and deep learning (DL) techniques. According to [1], DL is a promising machine-learning method for detecting and preventing attacks against IoT systems. ML can process and analyze massive quantities of data. As a result, ML can deliver better and faster data analysis that cannot be analyzed using traditional methods.

This paper consists of the following sections: The first is a brief introduction to the Internet of Things (IoT), Machine Learning, and Smart Home implementation. The second section then deliberates on the methods utilized in this study, and the third section presents the results derived from the reviewed articles. The fourth section is the discussion section, which will explain the suitable models and frameworks that can be used to implement Smart Home while also explaining the types of attacks that can occur in the Network Layer. Lastly, the conclusion section will summarize both derived results and the accompanying discussion. It will state the importance of the varying ideas of IoT attack detection using Machine Learning and Deep Learning in Smart Homes.

To help guide the development of this SLR, four research questions (RQ) were created. The proposed research questions are as follows:

- RQ1: What are the models and frameworks relating to IoT Smart Home Cybersecurity that are currently being researched?
- RQ2: What kind of attack and anomaly detection are being researched for IoT Smart Home Cybersecurity?
- RQ3: What Machine Learning (ML) techniques are used for attack anomaly detection in IoT Smart Home Cybersecurity?
- RQ4: What are the challenges, evaluation approach, used datasets, and results of IoT attack detection in Smart Home?

II. Materials and Method

To observe the literature relating to IoT Attack detection using machine learning and deep learning in Smart Homes, we conducted an SLR consisting of six phases: problem identification, research question development, literature searching, literary analysis, results and discussion, and conclusion, as shown in Figure 3.

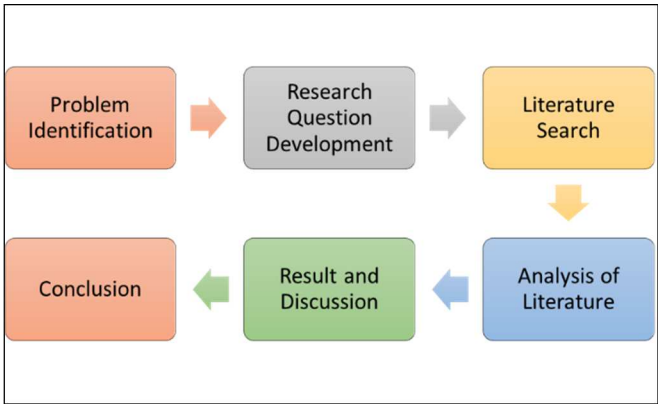

Fig. 3 The process of conducting a structural literature review

The first phase is problem identification, establishing the research objective and the systematic review's structure. The identified problem by the review must be clearly stated to propose a way to improve it. The next phase is research question development. The research questions must be constructed appropriately to ensure the findings remain relevant and accurate. The validity and significance of the research questions are crucial for the SLR's target audience. The third and fourth phases are literature searching and literary analysis, which will identify the existing algorithms, techniques, and models used in IoT attack detection using machine learning and deep learning in a smart home. These phases will be constructive when later selecting suitable machine learning (ML) or deep learning (DL) methods for IoT attack detection in Smart Homes [19]. The fifth phase is the result and discussion, clarifying the results collected from the literature review. Lastly, the conclusion will be presented,

where we will propose the various ideas developed from our SLR and justify the advantages of these ideas.

This Systematic Literature Review was conducted to answer all the proposed research questions and review the literature spanning four platforms: IEEE (Advancing Technology for Humanity), SCIENCE DIRECT, ACM (Association for Computing Machinery), and SpringerLink. Figure 4 presents the research methodology used to find the relevant articles.

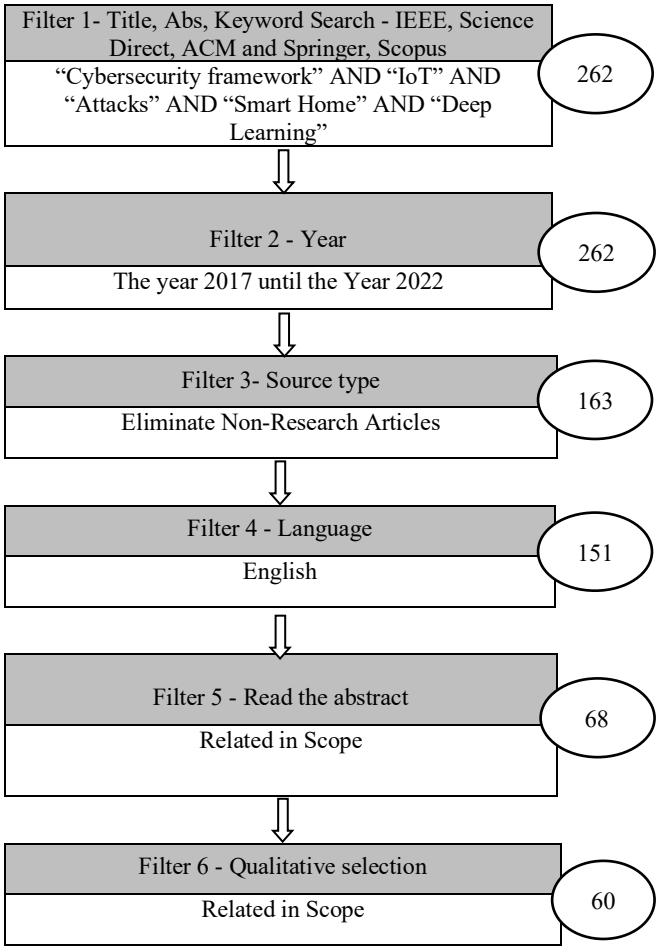

Fig. 4 Filters of the SLR strategy

III. Results and Discussion

From the 60 selected articles, we outlined and classified their various descriptive statistics, such as subject-wise analysis and year-wise analysis. The chart in Figure 5 shows the subject-wise classifications, revealing that Computer Science and Engineering are the significant areas in which research relating to IoT Attack detection using machine learning and deep learning in Smart Home has been published.

Figure 6 illustrates the year–wise analysis, which shows that research in IoT Attack detection using machine learning and deep learning in the Smart Home began in 2017. The increasing use of Smart Homes and IoT devices has made them a target for cyberattacks. The lack of security measures in many IoT devices and the growing interconnectedness of home systems make them vulnerable to attack. As a result, there has been a rise in research and studies focusing on IoT security and the protection of Smart Homes.

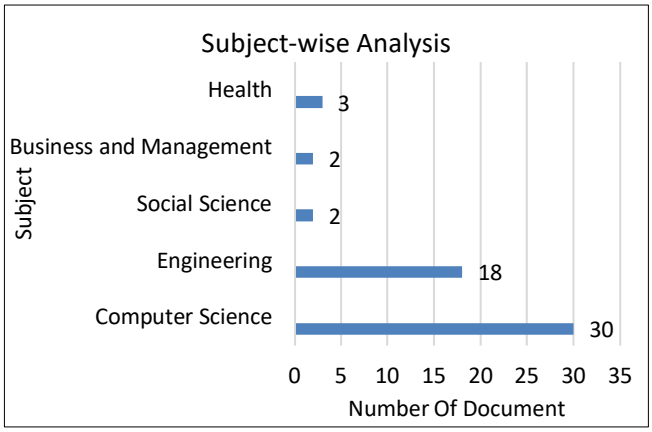

Fig. 5 Subject–wise analysis

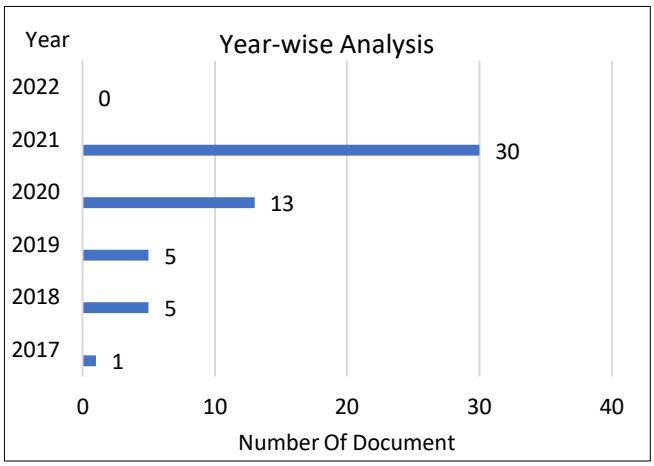

Fig. 6 Year–wise analysis

A. Models and Frameworks addressed in previous research

Research is an iterative process; new findings and advancements often build upon the work of previous researchers. By identifying gaps or limitations in earlier research, new researchers can contribute to the field by proposing new solutions and improving existing models and frameworks. To answer Research Question 1, we will discuss the models and frameworks that other researchers have proposed. Based on the SLR result for IoT Attack detection using machine learning and deep learning in smart homes, we found that some frameworks can be enhanced to solve the issue of Smart Home security and that every study described essential components for improving the framework of IoT detection in Smart Home, each with their varying styles and advantages.

Study [4] proposed a Smart Attack framework that could help identify user activity using Machine Learning techniques. For the framework to achieve the proposed expectation, they used the UNSW dataset for testing, which consisted of 22 IoT device packets from network traffic. Cross-validation was implemented into the framework to ensure that the ML/DL techniques being used were accurate. The performance evaluation of the cross-validated ML/DL techniques showed that their Smart Attack framework could detect 12 user activities accurately, each detected by a different ML/DL technique. Random Forest is a popular machine-learning algorithm that can be used for activity recognition. It has been shown to have high accuracy in detecting various activities, such as control switch usage,

voice commands through a smart assistant and condition monitoring. Random Forest is a decision tree-based algorithm that creates an ensemble of trees to make predictions. This approach can handle complex, non-linear relationships between features and the target variable, making it well-suited for activity recognition tasks.

TABLE I
MODELS AND FRAMEWORK ADDRESSED IN SLR

Model/Framework	Details
Proposed Deep learning-based adversarial attack model framework-SmartAttack [4]	• A framework that can collect user activity data for the Network Layer and perform analysis using ML/DL methods to determine network activity in smart homes (Decision Tree, Logistic Regression, K-Nearest Neighbors (kNN), Naive Bayes, Random Forest, and Support Vector Machines (SVMs)). • The framework can detect 12 user activity data in the smart home. • Can be employed to evaluate the potential security and privacy-preserving approach in smart home IoT devices.
Proposed three frameworks, which are as follows: • Data analytics system framework • Game theory framework. • Cloud-based framework [20]	• Framework that is being combined to apply in the Lean 4.0 system. • It detects and reduces the threats that occur in cybersecurity
Proposed Particle Deep Framework (PDF) for network forensics [10]	• A framework that captures network data using Particle Swarm Optimization (PSO) to adapt the parameters of a Deep Neural Network (DNN). This framework uses MLP to identify traffic attacks. • It provides high performance in detection accuracy and time.
COSMOS architecture [21]	• It's an enhancement from the previous framework, which increases the performance of cyber defense in IoT devices. • Frameworks consist of four extra modules in COSMOS sentinel (Dynamic Rule Loader (DRL), Vulnerability Detection System (VDS), Event Processing Module (EPM), and Mitigation Module (MM)).
Adversarial Model [22]	• This model calculates the number of MAC addresses since it can capture device activities at the network layer. • To strengthen the network device, they propose a cryptographically secure token.
Proposed SenseGan Framework [23]	• Framework that combines three neural network components: generator, classifier, and discriminator. • It can help to increase the prediction level by supporting unlabeled data.
Proposed ILLIAD (Intelligent Invariant and Anomaly Detection) System Architecture [24]	• The network data will be trained using the Kalman Filter and Factor analysis. Then, it will filter using KASE invariant Learning to analyze whether it has a threat, and the graph will be generated in the Front-End Dashboard. • The system has been tested with various datasets and estimates anomalies with higher accuracy.
The proposed general solution architecture can analyze intrusion detection in a smart home [25]	• The architecture will analyze the z-wave network using the Raspberry Pi as the home controller. • The data collected using the CTF event will undergo data processing, making it easier to analyze the intrusion. Alerts will be raised if intrusion occurs in a smart home.
Proposed IoT- HASS Framework [2]	• Framework of combining three engines: anomaly-based network intrusion detection, device management engines, and privacy monitoring engines. • It can help to secure entire homes from attacks. • It stated that IoT-HASS can be implemented but on a small scale of data.

Meanwhile, the authors of [20] proposed the implementation of three different frameworks for IoT attack detection: a data analytics system framework, a game theory framework, and a cloud–based dynamic resource allocation framework. Each of these frameworks has its advantages; for example, the game theory framework can identify the type of attack and respond to it. These proposed frameworks would be used to enhance the Lean 4.0 System for detection guidelines and will be able to support the emergence of Lean 4.0 systems.

Many researchers have proposed frameworks that based themselves on the network layer [10], [22], [24]. However, although the studies based their frameworks on the same layer, each proposition differed. The framework proposed in [10] identified attacks that occurred in network testing and was shown to have high detection accuracy and time performance. This varies from the framework proposed in [22], which focused on strengthening the overall network using cryptographically secure tokens that calculated the MAC addresses and captured network activities. Meanwhile, the framework proposed in [24] had its system continually update the state estimate of the Kalman filter using raw data instances while occasionally retraining the Kalman filter and the factor analysis model using historical data. These differing proposals illustrate the diverse variety of possible methods that can be adopted for IoT attack detection. Additionally, some researchers had built their frameworks from previous ones proposed by other researchers [21]. They enhanced the strengths of a previously existing framework by adding four modules, improving its performance in cyber defense, which was shown and proven through testing.

Some frameworks were semi-supervised, such as the SenseGan framework [23]. This framework was divided into three sections: the generator, the classifier, and the

discriminator, which all comprise its neural network. Its neural network helps to prevent the system from discriminating against unlabeled data. It enables the system to identify and classify data according to the behavior of the data generated through input sensing. Because of this, this framework has an increased level of forecasting analyzed data.

Furthermore, a study [25] produced an architecture that could detect intrusions. It consisted of four different types of engines: trace collection, data processing, automated analysis, and alert raising. In the trace collection engine, data collected from tracers are equipped with a minimal overhead rate using LTTng tracers [26], which allows the device to detect intrusions and leave a spell to enable the production of the Common Trace Format (CTF). Then, the CTF will go through a phase of data processing where the data will be processed using machine learning and converted into its metric form [27], [28] to become more accessible to comprehend. For the CTF traces to be read, the Babeltrace API [29] is used, and after that, the process identifiers (PID) are passed until a metric form contains several arrays. After that, the data will undergo an automated analysis, where machine learning will compare the data with standard data and check whether it followed good behavior, or an intrusion had occurred. [30]. If an intrusion has happened, it will alert the user and give the information of the suspicious event [31].

Lastly is the IoT-HASS framework, which consists of three main engines: an anomaly-based network intrusion detection engine (IDS), a device management engine, and a privacy monitoring engine. The framework works by having the IDS analyze the data sent from an Internet Service Provider (ISP) and check whether a packet contains an attack. If an attack is detected, the IoT-HASS will block it and notify the user about the intrusion [2]. If the IDS detects nothing suspicious, the packet is sent to the device management engine, where it will confirm the IoT device used to prevent a man-in-the-middle attack. If the device management engine detects nothing suspicious, the packet will be connected to the Home Network and inspected for plaintext before being sent to the internet. The existing frameworks produced by other researchers still have loopholes, as they cannot effectively secure the smart home environment from attacks. Therefore, there is a pressing need to enhance the framework to better protect the smart home environment against such vulnerabilities.

B. Type of Attacks and Anomalies Detected in The Network Layer

The IoT architecture comprises three main layers: the application, network, and perception. Every layer is responsible for ensuring the proper functioning of the IoT system, and each has its varying characteristics. The Network layer has three layers that can be attacked: the fog, the cloud, and the edge. To answer Research Question 2, we will discuss the types of attacks that target the Network Layer, as shown in Table II. The fog layer, as discussed in Table II, is widely recognized as having deficient security. Numerous researchers have concluded that hackers often target the fog layer [5], [7], [9], [12], [15], [16], [19], [33], [35], [38]due to its nature as a distributed network situated between cloud computing and the Internet of Things (IoT). This positioning makes breaching information and executing attacks easier compared to targeting the edge[12], [32], [34], [36] and cloud layers [12], [13], [37]. Despite previous research efforts, the fog layer remains vulnerable to IoT attacks.

TABLE II
TYPE OF ATTACK AND ANOMALY DETECTION OCCUR IN THE NETWORK LAYER

Articles	Computing	Threat
[5]	Fog	• Botnet attack – DDoS attack • Mirai Botnet Attack – auto scanning for vulnerable devices • Gafgyt Botnet attack – sending spam data
[32]	Cloud	• DOS attack
[9]	Fog	• DDOS attack • IoT botnet
[12]	Edge, Fog, Cloud	• Denial of Service (DoS) • Distributed DoS (DDoS) • ransomware • other botnet attacks
[13]	Edge	• DOS • Remote to Local (R2L) • User to Root (U2R) • Probe • Reconnaissance • Analysis • Worm • Generic • Fuzzer • Shellcode • Exploit
[33]	Fog	• Mirai • Scan • DoS • MTM • ARP Spoofing
[34]	Cloud	• Using threat model, KGC
[15]	Fog	• DDoS • ICMP • Smurf • HTTP-flood • TCP-Sync • UDP-flood.
[16]	Fog	• DDoS
[35]	Fog	• DDoS
[36]	Cloud	• Botnet attack
[7]	Fog	• DOS • Data Type Probing • Malicious Control (M.C) • Malicious Control (M.O) • Scan • Spying • Wrong Setup
[37]	Edge	• Changing system setpoints • Falsifying sensor measurement • Falsifying control signals
[38]	Fog	• DDOS attack • Phishing • botnet
[19]	Fog	• White-box (WB) attack • Black-box (BB) attack

Several types of attacks specifically target the fog layer exist. One prominent example is Distributed Denial of Service (DDoS) attacks [5], [7], [9], [12], [15], [16], [35], [38], which can also be categorized as botnet attacks. DDoS attacks can be concealed within standard network packets, making them

difficult to detect. Moreover, the methods employed in DDoS attacks continually adapt and evolve alongside technological advancements. Therefore, Smart home environments must establish robust network layer security measures to safeguard against these attacks.

Another form of attack directed at the fog layer is botnet attacks [5], [9], [12], [36], [38], [39]. In these attacks, a bot herder, an attacker, injects malware into a targeted network [40] to infect the network layer [41] and disrupt services. Two standard models employed in botnet attacks are the centralized client-server and decentralized peer-to-peer models. The centralized client-server model enables an attacker to control and command a server, while the peer-to-peer model requires the attacker to gain access to the target devices. Botnet attacks manifest in three primary forms: phishing, DDoS attacks, and spambots [42], [43], [44], [45].

In summary, the fog layer faces significant security challenges and is a preferred target for hackers due to its position as an intermediate layer between cloud computing and the IoT. DDoS attacks and botnet attacks pose substantial threats to the fog layer's integrity. Robust security measures are vital to protect the network layer of Smart Home environments from these evolving and adaptive attacks.

C. Types of Machine Learning Techniques Used for Attack Detection

We need to utilize suitable machine-learning techniques to strengthen the detection of IoT attacks in Smart Homes. Machine Learning, a subset of Artificial Intelligence (AI), can oversee overall threat patterns and trends in smart homes. To answer Research Question 3, we presented the most suitable machine-learning techniques for attack detection in Table III.

TABLE III
TYPE OF MACHINE LEARNING TECHNIQUES THAT BEING USED FOR DETECTION ATTACK

REFERENCES	MACHINE LEARNING	DETAILS
[6]	LSTM & CNN	LSTM can detect ransomware faster and more accurately compared to CNN.
[7]	Logistic Regression, SVM, Decision tree, Random Forest, ANN	Random Forest produces a high accuracy compared to other Machine Learning.
[8]	Logistic Regression, Random Forest, Multi-Layer Perceptron, kNN, LSTM	LSTM is the better solution to evaluate the VIDS
[46]	RNN, LSTM, BLSTM	CNN-BLSTM has a lower false positive rate and produces a better result compared to others.
[10]	MLP, RNN	MLP being used to make the Particle Deep Learning (PDF)
[47]	Naive Bayes (NB), Nearest Neighbor (NN), Decision Trees (J48, LMT, and RF), Support Vector Machines (SVM)	PSO algorithm produces the overall accuracy.
[38]	Distributed Convolutional Neural Network (DCNN) and Long-Short Term Memory (LSTM).	LSTM has a higher accuracy compared to others
[48]	Feed-forward neural networks (FNN) model and SVM model	MFNN produces better results in a large-scale area
[49]	Decision Tree, Naive Bayes, extra tree, KNN, Random Forest, and XGBoost	Decision Tree has the best performance.
[19]	CNN, DNN	DNNs are more suitable for audio-intelligent
[50]	LSTM, Neural Network, Random Forest, XGBoost and SVM	XGBoost produces higher accuracy
[51]	Random Forest (RF), Convolutional Neural Network (CNN), and Multi-Layer Perceptron (MLP)	MLP classification model provides good results for four performance measures
[52]	SVM	Federated Learning combination MLP produces high accuracy
[53]	LSTM and Multi-Layer Perceptron (MLP)	LSTM has a better result
[54]	Cross-device Deep Learning, SNR, and DNN	SNR has a better accuracy than DNN
[55]	random forest (RF), support vector machine (SVM), and artificial neural network (ANN)	SVM has a higher accuracy

Table III highlights LSTM as the most efficient technique for detecting anomalies in the context of anomaly detection. LSTM's effectiveness can be attributed to its advanced Recurrent Neural Network (RNN) architecture, which enables it to capture long-term dependencies in sequences of detection and process data quickly and accurately compared to other machine learning approaches. One of the advantages of LSTM in anomaly detection is its ability to handle temporal information effectively.

It's worth noting that LSTM belongs to deep learning, a subset of machine learning that incorporates sophisticated techniques. This characteristic distinguishes LSTM from traditional machine learning methods such as Decision Trees, Multilayer Perceptron (MLP), and Random Forests. Conventional approaches may need help to capture complex patterns and relationships in data, whereas LSTM, with its deep learning foundation, excels in this regard.

However, researchers have proposed an alternative approach to improve further the accuracy of detecting IoT attacks at the Network Layer. Some studies suggest combining two deep learning techniques [52]. For example, in [46], the fusion of Convolutional Neural Networks (CNN) and Bidirectional LSTM (BLSTM) showcased enhanced performance compared to LSTM alone. By leveraging the

strengths of both CNN and BLSTM, this hybrid model achieved superior accuracy in detecting IoT attacks.

In summary, while LSTM stands out as the most efficient technique for anomaly detection due to its advanced RNN architecture and deep learning foundation, researchers have explored the potential of combining deep learning techniques to enhance accuracy further. The combination of CNN and BLSTM, as demonstrated in [46], shows promise in achieving superior results in detecting IoT attacks at the Network Layer. This explains the ongoing efforts to improve anomaly detection techniques and adapt them to specific domains and challenges.

D. Challenges, Evaluation Approaches, Used Datasets, and Results for IoT Smart Home attack detection

Many of the selected articles had reported their techniques, dataset, challenges, and outcomes. Table IV was constructed to organize these inputs better, which is used to answer Research Question 4.

TABLE IV
CHALLENGES, EVALUATION APPROACHES, USED DATASETS, AND RESULTS FOR IOT SMART HOME ATTACK DETECTION

Articles	Technique	Dataset	Outcome	Challenges
[6]	LSTM & CNN	Locky (200), Cerber (220), TeslaCrypt (220), Crypto Wall (99), Torrent Locker (28), and Saga (77) ransomware datasets.	LSTM with eight units result in a more powerful binary compared to CNN	Proposed DRTHIS need enhancement to improve the speed of malware classification.
[7]	Logistic Regression, SVM, Decision tree, Random Forest, ANN	DS20S	Random Forest	The data that is gained from this experiment will not be valid to be used for big data cases.
[8]	Logistic Regression, LDA, Decision Tree, MLP, KNN, and LSTM	• Modbus • TCP, IEC • BACNET • MQTT • CSE CIC-IDS2018	LSTM	combined LSTM with potential machine learning to increase the performance
[46]	RNN, LSTM, BLSTM	• National Vulnerability Database (NVD) • NIST	CNN-BLSM model	NA
[10]	MLP, RNN	UNSW-NB15	Particle Deep Learning (PDF) using MLP	Need to improve using PSO to estimate multiple hyperparameters
[47]	Naive Bayes (NB), Nearest Neighbor (NN), Decision Trees and (SVM)	CICAndMal2017	PSO algorithm shows the best overall results	NA
[11]	DIGFuPAS-	NSL-KDD and CICIDS2018 datasets.	remarkable drops in the detection proportion of IDS	NA
[38]	DCNN and LSTM	Detection of IoT botnet attacks N-Balot	LSTM	Proposed a new approach to detect attacks on IoT environment
[48]	Use feed-forward neural networks (FNN) model and SVM model	BoT–IoT dataset	It is warranted for IoT network intrusion detection system design.	Only consider for four categories and it may cause the large scale of malware.
[56]	Use sFlow adaptive polling	Barnyard2 is used for creating a database to store datasets inside the Ryu SDN controller.	The sFlow achieved a higher detection rate.	NA
[13]	The evaluation criteria are accuracy, Detection Rate (DR), False Positive Rate (FPR), and processing time.	NSL-KDD and UNSW-NB15	DAD produces high performance	NA
[49]	Decision Tree, Naive Bayes, extra tree, KNN, Random Forest and XGBoost, accuracy, and F1 score	Kyoto 2006+, CICIDS, Bot-IoT, UNSW-NB15, Ton-IoT, CRÈME datasets for IoT security research.	The Decision Tree has a best detection	Need to leverage the potential of attack
[19]	CNN, DNN	Speech Command (SC) and Ambient (A)	training that compressed models with high resistance	NA
[14]	Promising for computation-intensive applications.	NA	study the separate attacks and propose a different defense	NA
[50]	LSTM, Neural Network, Random Forest, XGBoost and SVM	the dataset was collected over a short period	XGBoost has high accuracy	Need to enhance the security framework.

Articles	Technique	Dataset	Outcome	Challenges
[51]	Random Forest (RF), Convolutional Neural Network (CNN), MLP	ES File downloader, Hangman, Hangman 2, One Cleaner, and VPN master	MLP classification model provides good results	NA
[53]	LSTM and Multi-Layer Perceptron (MLP)	BreathPrint	LSTM models offer a compelling, lightweight authentication solution	Need to use GPU in order to improve inference time
[57]	Disguising Real Machines: The delay modification technique makes real machines resemble VMs.	Experiment: 1,000,000 packets sent, timestamp analysis, significant differences observed.	VMs and real machines distinguish, and protection is provided to real machines.	Malware behavior in VMs, security policy framework development
[58]	Machine learning, lexicon-based, hybrid, Kansei.	Social media (Twitter, Facebook, Tumblr), cyberspace websites (IMDB, Amazon).	Sentiment and emotion extraction from text, classification of opinions	Lack of domain-specific emotion words, dependency on existing libraries, and need for systematic evaluation.
[59]	TAM 3 and TRI 2 were used to evaluate blockchain acceptance in the intelligence community.	30 respondents from the intelligence community in Malaysia were surveyed	The findings showed positive influences on job relevance, optimism, and innovative	Small sample size and the need for training and education are challenges.
[60]	Combined username/password, biometric authentication, IoT device authentication, and one-time authorization code.	It was not specified.	It enhanced multi-factor authentication for the intelligence community's critical surveillance data access.	They are protecting intelligence data and resources, developing secure and efficient authentication processes.
[61]	Remote detection using IP timestamps in full virtualization.	Experiments conducted in a private cloud computing environment with full-virtualization VMs	Distinguishable differences in timestamp reply to characteristics between para-virtualization VMs and non-VM machines.	Security risks associated with virtualization technology and potential vulnerabilities in cloud computing environments.

Table IV provides insights into IoT smart home attack detection. One notable finding is the effectiveness of combining LSTM and CNN techniques, with LSTM outperforming CNN in binary classification tasks [6]. These holds promise for accurately detecting attacks in smart home environments. However, a challenge in terms of malware classification speed requires further improvement. Researchers have explored other machine learning algorithms, such as Logistic Regression, SVM, Decision Trees, Random Forests, and ANN, but concerns remain about data validity in high-volume cases [7]. Researchers propose combining LSTM with other approaches to enhance detection to leverage their strengths and create more robust models capable of detecting a more comprehensive range of attacks [8].

Another significant aspect highlighted in Table IV is the impact of adversarial attacks on intrusion detection systems (IDS) [11]. Adversarial attacks lead to a substantial drop in IDS detection proportion, emphasizing the need to develop robust defense mechanisms to effectively detect and mitigate these sophisticated attacks in smart home environments [38]. Distributed convolutional neural networks (DCNN) and LSTM show potential for detecting IoT botnet attacks and leveraging GPUs can improve inference time for faster and more efficient detection [53]. Overall, accurate and reliable detection of IoT smart home attacks is essential, and addressing challenges such as malware classification speed and adversarial attacks is crucial for developing resilient detection systems.

IV. Conclusion

Smart homes currently face significant vulnerabilities due to a lack of consistent enhancement and security upgrades. This unfortunate situation has made the IoT systems within smart homes a prime target for intruders and hackers. We conducted a systematic literature review (SLR) to address this issue to analyze existing papers on the subject. Our findings revealed a common trend in IoT attacks targeting the fog layer of the network.

Although prior researchers have developed frameworks to secure smart homes against attacks, these frameworks still exhibit specific vulnerabilities. To address this gap, we propose a novel solution that involves a hybrid deep learning approach. Our framework incorporates two distinct types of deep learning models: Long Short-Term Memory (LSTM) and K-Nearest Neighbors (KNN).

Previous research highlights the superior accuracy of LSTMs in detecting IoT attacks compared to other machine learning algorithms. LSTMs' ability to handle sequential, long-term data, their resilience to noise, and their capacity to generalize to new data position them as a promising choice for IoT attack detection. On the other hand, KNN is a swift algorithm suitable for real-time detection of rapidly evolving IoT threats, making it an ideal candidate for countering fast-moving attacks.

Acknowledgment

We acknowledge the National Defense University of Malaysia (UPNM) and the Ministry of Higher Education Malaysia (MOHE) for the approved fund that made this research viable and effective. This research is supported by the Fundamental Research Grant FRGS/1/2021/ICT07/ UPNM/02/1 and UPNM/2023/GPPP/ICT/2.

REFERENCES

[1] A. N. Muhammad, A. M. Aseere, H. Chiroma, H. Shah, A. Y. Gital, and I. A. T. Hashem, *Deep learning application in smart cities: recent development, taxonomy, challenges and research prospects*, vol. 33, no. 7. Springer London, 2021. doi: 10.1007/s00521-020-05151-8.

[2] T. Mudawi, "IoT-HASS: A Framework for Protecting Smart Home Environment," 2020, [Online]. Available: https://scholar.dsu.edu/theses

[3] S. Tsimenidis, T. Lagkas, and K. Rantos, *Deep Learning in IoT Intrusion Detection*, vol. 30, no. 1. Springer US, 2022. doi:10.1007/s10922-021-09621-9.

[4] K. Yu and D. Chen, "SmartAttack: Open-source Attack Models for Enabling Security Research in Smart Homes," *2020 11th International Green and Sustainable Computing Workshops, IGSC 2020*, 2020, doi:10.1109/IGSC51522.2020.9290797.

[5] M. Mafarja, A. A. Heidari, M. Habib, H. Faris, T. Thaher, and I. Aljarah, "Augmented whale feature selection for IoT attacks: Structure, analysis and applications," *Future Generation Computer Systems*, vol. 112, pp. 18–40, 2020, doi: 10.1016/j.future.2020.05.020.

[6] S. Homayoun *et al.*, "DRTHIS: Deep ransomware threat hunting and intelligence system at the fog layer," *Future Generation Computer Systems*, vol. 90, pp. 94–104, 2019, doi: 10.1016/j.future.2018.07.045.

[7] M. Hasan, M. M. Islam, M. I. I. Zarif, and M. M. A. Hashem, "Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches," *Internet of Things (Netherlands)*, vol. 7, p. 100059, 2019, doi: 10.1016/j.iot.2019.100059.

[8] P. Radoglou-Grammatikis *et al.*, "SPEAR SIEM: A Security Information and Event Management system for the Smart Grid," *Computer Networks*, vol. 193, no. September 2020, p. 108008, 2021, doi: 10.1016/j.comnet.2021.108008.

[9] G. L. Nguyen, B. Dumba, Q. D. Ngo, H. V. Le, and T. N. Nguyen, "A collaborative approach to early detection of IoT Botnet," *Computers and Electrical Engineering*, vol. 97, no. October, p. 107525, 2022, doi:10.1016/j.compeleceng.2021.107525.

[10] N. Koroniotis, N. Moustafa, and E. Sitnikova, "A new network forensic framework based on deep learning for Internet of Things networks: A particle deep framework," *Future Generation Computer Systems*, vol. 110, pp. 91–106, 2020, doi:10.1016/j.future.2020.03.042.

[11] P. T. Duy, L. K. Tien, N. H. Khoa, D. T. T. Hien, A. G. T. Nguyen, and V. H. Pham, "DIGFuPAS: Deceive IDS with GAN and function-preserving on adversarial samples in SDN-enabled networks," *Comput Secur*, vol. 109, p. 102367, 2021, doi: 10.1016/j.cose.2021.102367.

[12] N. Moustafa, "A new distributed architecture for evaluating AI-based security systems at the edge: Network TON_IoT datasets," *Sustain Cities Soc*, vol. 72, no. May, p. 102994, 2021, doi:10.1016/j.scs.2021.102994.

[13] N. Moustafa, M. Keshk, K. K. R. Choo, T. Lynar, S. Camtepe, and M. Whitty, "DAD: A Distributed Anomaly Detection system using ensemble one-class statistical learning in edge networks," *Future Generation Computer Systems*, vol. 118, pp. 240–251, 2021, doi:10.1016/j.future.2021.01.011.

[14] P. Yellu, L. Buell, M. Mark, M. A. Kinsy, D. Xu, and Q. Yu, "Security threat analyses and attack models for approximate computing systems," *ACM Transact Des Autom Electron Syst*, vol. 26, no. 4, 2021, doi: 10.1145/3442380.

[15] K. S. Sahoo and D. Puthal, "SDN-Assisted DDoS Defense Framework for the Internet of Multimedia Things," *ACM Transactions on Multimedia Computing, Communications and Applications*, vol. 16, no. 3s, 2021, doi: 10.1145/3394956.

[16] Y. J. Lee, N. K. Baik, C. Kim, and C. N. Yang, "Study of detection method for spoofed IP against DDoS attacks," *Pers Ubiquitous Comput*, vol. 22, no. 1, pp. 35–44, 2018, doi: 10.1007/s00779-017-1097-y.

[17] A. Yahyaoui, H. Lakhdhar, T. Abdellatif, and R. Attia, "Machine learning based network intrusion detection for data streaming IoT applications," *Proceedings - 2021 21st ACIS International Semi-Virtual Winter Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, SNPD-Winter 2021*, pp. 51–56, 2021, doi:10.1109/SNPDWinter52325.2021.00019.

[18] E. Adi, A. Anwar, Z. Baig, and S. Zeadally, "Machine learning and data analytics for the IoT," *Neural Comput Appl*, vol. 32, no. 20, pp. 16205–16233, 2020, doi: 10.1007/s00521-020-04874-y.

[19] S. Bhattacharya, Di. Manousakas, A. G. C. P. Ramos, S. I. Venieris, N. D. Lane, and C. Mascolo, "Countering Acoustic Adversarial Attacks in Microphone-equipped Smart Home Devices," *Proc ACM Interact Mob Wearable Ubiquitous Technol*, vol. 4, no. 2, 2020, doi:10.1145/3397332.

[20] M. Shahin, F. Frank Chen, H. Bouzary, and A. Zarreh, "Frameworks proposed to address the threat of cyber-physical attacks to lean 4.0 systems," *Procedia Manuf*, vol. 51, no. 2019, pp. 1184–1191, 2020, doi: 10.1016/j.promfg.2020.10.166.

[21] P. Nespoli, D. Díaz-López, and F. Gómez Mármol, "Cyberprotection in IoT environments: A dynamic rule-based solution to defend smart devices," *Journal of Information Security and Applications*, vol. 60, no. May, p. 102878, 2021, doi: 10.1016/j.jisa.2021.102878.

[22] N. Panwar, S. Sharma, G. Wang, S. Mehrotra, and N. Venkatasubramanian, "Canopy: A verifiable privacy-preserving token ring-based communication protocol for smart homes," *ACM Transactions on Cyber-Physical Systems*, vol. 5, no. 1, 2021, doi:10.1145/3390859.

[23] S. Yao *et al.*, "SenseGAN: Enabling Deep Learning for Internet of Things with a Semi-Supervised Framework," *Proc ACM Interact Mob Wearable Ubiquitous Technol*, vol. 2, no. 3, pp. 1–21, 2018, doi:10.1145/3264954.

[24] N. Muralidhar *et al.*, "Illiad: InteLLigent invariant and anomaly detection in cyber-physical systems," *ACM Trans Intell Syst Technol*, vol. 9, no. 3, pp. 1–20, 2018, doi: 10.1145/3066167.

[25] R. Gassais, N. Ezzati-Jivan, J. M. Fernandez, D. Aloise, and M. R. Dagenais, "Multi-level host-based intrusion detection system for Internet of things," *Journal of Cloud Computing*, vol. 9, no. 1, 2020, doi: 10.1186/s13677-020-00206-6.

[26] S. S. Murtaza, A. Hamou-Lhadj, W. Khreich, and M. Couture, "Total ADS: Automated software anomaly detection system," *Proceedings - 2014 14th IEEE International Working Conference on Source Code Analysis and Manipulation, SCAM 2014*, no. June 2016, pp. 83–88, 2014, doi: 10.1109/SCAM.2014.37.

[27] M. Feurer, "OUTROS - NIPS-2015-efficient-and-robust-automated-machine-learning-Paper," 2015, [Online]. Available: https://papers.neurips.cc/paper/2015/hash/11d0e6287202fced83f79975ec59a3a6-Abstract.html

[28] A. Pinna, S. Ibba, G. Baralla, R. Tonelli, and M. Marchesi, "A Massive Analysis of Ethereum Smart Contracts Empirical Study and Code Metrics," *IEEE Access*, vol. 7, no. 1993, pp. 78194–78213, 2019, doi:10.1109/access.2019.2921936.

[29] N. Ezzati-Jivan and M. R. Dagenais, "A Stateful Approach to Generate Synthetic Events from Kernel Traces," *Advances in Software Engineering*, vol. 2012, pp. 1–12, 2012, doi: 10.1155/2012/140368.

[30] D. Wagner and P. Soto, "Mimicry attacks on host-based intrusion detection systems," *Proceedings of the ACM Conference on Computer and Communications Security*, vol. 2, pp. 255–264, 2002, doi:10.1145/586110.586145.

[31] M. Moore and M. D. Moore, "Penetration Testing and Metasploit," no. April 2017, [Online]. Available: https://www.researchgate.net/publication/318710609

[32] J. Chen, L. Ramanathan, and M. Alazab, "Holistic big data integrated artificial intelligent modeling to improve privacy and security in data management of smart cities," *Microprocess Microsyst*, vol. 81, no. September 2020, p. 103722, 2021, doi:10.1016/j.micpro.2020.103722.

[33] D. K. K. Reddy, H. S. Behera, J. Nayak, B. Naik, U. Ghosh, and P. K. Sharma, "Exact greedy algorithm based split finding approach for intrusion detection in fog-enabled IoT environment," *Journal of Information Security and Applications*, vol. 60, no. June, p. 102866, 2021, doi: 10.1016/j.jisa.2021.102866.

[34] X. Ma, J. Ma, S. Kumari, F. Wei, M. Shojafar, and M. Alazab, "Privacy-Preserving Distributed Multi-Task Learning against Inference Attack in Cloud Computing," *ACM Trans Internet Technol*, vol. 22, no. 2, pp. 1–24, 2022, doi: 10.1145/3426969.

[35] M. Bhatia, "Intelligent System of Game-Theory-Based Decision Making in Smart Sports Industry," *ACM Trans Intell Syst Technol*, vol. 12, no. 3, pp. 1–23, 2021, doi: 10.1145/3447986.

[36] C. U. Om Kumar and P. R. K. Sathia Bhama, "Detecting and confronting flash attacks from IoT botnets," *Journal of Supercomputing*, vol. 75, no. 12, pp. 8312–8338, 2019, doi:10.1007/s11227-019-03005-2.

[37] M. Elnour, N. Meskin, K. Khan, and R. Jain, "Application of data-driven attack detection framework for secure operation in smart buildings," *Sustain Cities Soc*, vol. 69, no. September 2020, p. 102816, 2021, doi: 10.1016/j.scs.2021.102816.

[38] G. De La Torre Parra, P. Rad, K. K. R. Choo, and N. Beebe, "Detecting Internet of Things attacks using distributed deep learning," *Journal of*

Network and Computer Applications, vol. 163, no. April, 2020, doi:10.1016/j.jnca.2020.102662.

[39] A. Abbas, M. A. Khan, S. Latif, M. Ajaz, A. A. Shah, and J. Ahmad, "A New Ensemble-Based Intrusion Detection System for Internet of Things," *Arab J Sci Eng*, 2021, doi: 10.1007/s13369-021-06086-5.

[40] M. T. Banday, J. A. Qadri, and N. A. Shah, "Study of Botnets and their threats to Internet Security," *Working Papers on Information Systems*, no. January 2009, 2009.

[41] M. Eslahi, R. Salleh, and N. B. Anuar, "Bots and botnets: An overview of characteristics, detection and challenges," *Proceedings - 2012 IEEE International Conference on Control System, Computing and Engineering, ICCSCE 2012*, no. November, pp. 349–354, 2012, doi:10.1109/ICCSCE.2012.6487169.

[42] A. Kak, "Lecture Notes on ' Computer and Network Security ' Goals : Section Title," pp. 1–82, 2020.

[43] C. Douligeris and A. Mitrokotsa, "DDoS attacks and defense mechanisms: A classification," *Proceedings of the 3rd IEEE International Symposium on Signal Processing and Information Technology, ISSPIT 2003*, no. June 2014, pp. 190–193, 2003, doi:10.1109/ISSPIT.2003.1341092.

[44] M. A. Raza, T. F. N. Bukht, M. Ali, A. U. Rehman, and M. Idrees, "Analyzing the Behaviour of DDoS Cyber Attack," *Technical Journal*, vol. 26, no. 4, pp. 46–55, 2021.

[45] K. K. Brahma, S. Sarmah, C. Kalita, and R. Ghosh, "Detection of Multi-Vector DDoS Attack International Journal of Computer Sciences and Engineering Open Access Detection of Multi-Vector DDoS Attack," no. December, 2019.

[46] W. Niu, X. Zhang, X. Du, L. Zhao, R. Cao, and M. Guizani, "A deep learning based static taint analysis approach for IoT software vulnerability location," *Measurement (Lond)*, vol. 152, p. 107139, 2020, doi: 10.1016/j.measurement.2019.107139.

[47] M. A. Azad, F. Riaz, A. Aftab, S. K. J. Rizvi, J. Arshad, and H. F. Atlam, "DEEPSEL: A novel feature selection for early identification of malware in mobile applications," *Future Generation Computer Systems*, vol. 129, pp. 54–63, 2022, doi: 10.1016/j.future.2021.10.029.

[48] M. Ge, N. F. Syed, X. Fu, Z. Baig, and A. Robles-Kelly, "Towards a deep learning-driven intrusion detection approach for Internet of Things," *Computer Networks*, vol. 186, no. January, p. 107784, 2021, doi: 10.1016/j.comnet.2020.107784.

[49] H. K. Bui, Y. D. Lin, R. H. Hwang, P. C. Lin, V. L. Nguyen, and Y. C. Lai, "CREME: A toolchain of automatic dataset collection for machine learning in intrusion detection," *Journal of Network and Computer Applications*, vol. 193, no. August, p. 103212, 2021, doi:10.1016/j.jnca.2021.103212.

[50] M. Chowdhury, B. Ray, S. Chowdhury, and S. Rajasegarar, "A Novel Insider Attack and Machine Learning Based Detection for the Internet of Things," *ACM Transactions on Internet of Things*, vol. 2, no. 4, pp. 1–23, 2021, doi: 10.1145/3466721.

[51] F. Ullah, M. R. Naeem, A. S. Bajahzar, and F. Al-Turjman, "IoT-based Cloud Service for Secured Android Markets using PDG-based Deep Learning Classification," *ACM Trans Internet Technol*, vol. 22, no. 2, pp. 1–17, 2022, doi: 10.1145/3418206.

[52] Y. S. Can and C. Ersoy, "Privacy-preserving Federated Deep Learning for Wearable IoT-based Biomedical Monitoring," *ACM Trans Internet Technol*, vol. 21, no. 1, 2021, doi: 10.1145/3428152.

[53] J. Chauhan, J. Rajasegaran, S. Seneviratne, A. Misra, A. Seneviratne, and Y. Lee, "Performance Characterization of Deep Learning Models for Breathing-based Authentication on Resource-Constrained Devices," *Proc ACM Interact Mob Wearable Ubiquitous Technol*, vol. 2, no. 4, pp. 1–24, 2018, doi: 10.1145/3287036.

[54] J. Danial, D. Das, A. Golder, S. Ghosh, A. Raychowdhury, and S. Sen, "EM-X-DL: Efficient Cross-device Deep Learning Side-channel Attack With Noisy EM Signatures," *ACM J Emerg Technol Comput Syst*, vol. 18, no. 1, pp. 1–17, 2022, doi: 10.1145/3465380.

[55] Z. Lv, L. Qiao, A. Kumar Singh, and Q. Wang, "AI-empowered IoT Security for Smart Cities," *ACM Trans Internet Technol*, vol. 21, no. 4, 2021, doi: 10.1145/3406115.

[56] R. M. A. Ujjan, Z. Pervez, K. Dahal, A. K. Bashir, R. Mumtaz, and J. González, "Towards sFlow and adaptive polling sampling for deep learning based DDoS detection in SDN," *Future Generation Computer Systems*, vol. 111, pp. 763–779, 2020, doi:10.1016/j.future.2019.10.015.

[57] N. M, M. H, and K. T, "Virtual Machines Detection Methods Using IP Timestamps Pattern Characteristic," *International Journal of Computer Science and Information Technology*, vol. 8, no. 1, pp. 1–15, 2016, doi: 10.5121/ijcsit.2016.8101.

[58] N. A. M. Razali *et al.*, *Opinion mining for national security: techniques, domain applications, challenges and research opportunities*, vol. 8, no. 1. Springer International Publishing, 2021. doi: 10.1186/s40537-021-00536-5.

[59] W. N. W. Muhamad *et al.*, "Evaluation of Blockchain-based Data Sharing Acceptance among Intelligence Community," *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 12, pp. 597–606, 2020, doi: 10.14569/IJACSA.2020.0111270.

[60] R. Wahyudi, "Metadata of the chapter that will be visualized in Online," *Springer Nature Singapor*, no. August, pp. 1–8, 2023, doi: 10.1007/978-3-030-34032-2.

[61] M. Noorafiza, H. Maeda, R. Uda, T. Kinoshita, and M. Shiratori, "Vulnerability analysis using network timestamps in full virtualization virtual machine," *ICISSP 2015 - 1st International Conference on Information Systems Security and Privacy, Proceedings*, no. January 2015, pp. 83–89, 2015, doi: 10.5220/0005242000830089.