SEMARAK ILMU
PUBLISHING
202103268166(003316878-P)

Journal of Advanced Research in Applied Sciences and Engineering Technology

Journal homepage:
https://semarakilmu.com.my/journals/index.php/applied_sciences_eng_tech/index
ISSN: 2462-1943

Enhanced Readiness Forensic Framework for the Complexity of Internet of Things (IoT) Investigation Based on Artificial Intelligence

Randi Rizal[1,2], Siti Rahayu Selamat[1,*], Mohd. Zaki Mas'ud[1], Nur Widiyasono[2,3]

[1] Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka, 76100 Durian Tunggal, Melaka, Malaysia
[2] Department of Informatics, Faculty of Engineering, Siliwangi University, Tasikmalaya 46115, Indonesia
[3] PT Forensika Digital Nusantara, Kota Bekasi, Jawa Barat 17144, Indonesia

ARTICLE INFO

Article history:
Received 22 November 2023
Received in revised form 15 June 2024
Accepted 20 June 2024
Available online 10 August 2024

Keywords:

Internet of things; digital forensics readiness; IoT attack; investigation forensics; artificial intelligence (AI); ISO/IEC 27043

ABSTRACT

The growing versatility of Internet of Things devices increases the possibility of multiple attacks occurring and being carried out continuously. The limited processing capabilities and memory capacity of Internet of Things devices pose challenges for security and forensic analysis in collecting and documenting various attacks targeting these devices during the forensic investigation process. Thus, forensic investigative analysis goes beyond expectations, offering a holistic understanding of the complex consequences arising from IoT device attacks that have occurred. These issues and challenges provide important insights into vulnerabilities, potential future threats, and steps to effectively increase the resilience of the IoT ecosystem against the evolving cyber-attack risk landscape. Apart from that, the large amount of IoT attack data generated raises several problems. Such as the difficulty of quickly identifying threats and in-depth forensic analysis of each very diverse attack. The implementation of artificial intelligence is a very useful solution in overcoming the forensic investigation challenges that arise due to IoT attacks with the enormous increase in data volume and complexity. Therefore, this research aims and proposes to improve the IoT forensic readiness framework by collecting and analyzing digital evidence in detecting various attacks from various IoT devices automatically based on an artificial intelligence approach and functioning as an early warning system. Enhanced the proposed IoT forensic readiness framework based on ISO/IEC 27043 serves as a prototype for detecting and collecting various types of attacks as potential digital evidence from various IoT devices, as well as effective forensic investigation of digital evidence with the utilization of smart repository.

1. Introduction

The Internet of Things (IoT) introduces many intelligent device infrastructures where the interconnection of smart nodes creates a dynamic and versatile network [1] that supports various applications, services, and platforms with the aim of intelligent collaboration and communication between devices, systems, and people through various protocols, technologies, and internet

[*] *Corresponding author.*
E-mail address: sitirahayu@utem.edu.my

https://doi.org/10.37934/araset.50.1.121135

utilization [2,3]. For example, many developed countries have adopted and implemented IoT as a technological solution that promises to increase the comfort and convenience of human life, one of which has an impact on smart home infrastructure and the smart health sector for disease monitoring, tracking, detection, and prevention [4]. Nonetheless, the high level of acceptance and application of IoT in various fields results in a very large platform that is gaining attention from attacks, threats, and security issues [5].

At present, cyber security in IoT networks is very important and attracts attention, so it is the main target that attracts many intruders [6]. In Symantec's 2020 report, more than 57,000 attacks targeted IoT devices and networks. Attackers use a variety of attack strategies, including Denial of Services (DoS), Distributed DoS (DDoS), ransomware, and others. DoS and DDoS attacks are the most prevalent and regular types of attacks occurring threats of malicious attacks on IoT devices and networks [7]. According to Cloudfare's report on cyber threats, DDoS attacks increased by almost 1/3 between 2020 and 2021, with a spike of 75% in the last three months. In addition, the Neustar report explains that DDoS attacks have increased with a frequency of 200% while the volume increased by 73% when comparing the first six months of 2019 to the same time in 2018. Cisco's annual internet report, 2018-2023, provides an overview of the increasing trend of DDoS attacks. Based on observations in 2023, there has been an increase of two times the total, namely 15.4 million compared to 2018, as the impact of many incidents related to security on IoT devices is getting worse with the amount of data generated. A report issued by the International Data Corporation (IDC) in 2020 estimates that by 2025 so, many IoT devices are connected to generate 79 zettabytes of data. Such data has the potential to be highly prioritized for generating and informing digital forensic investigative processes.

Forensic investigations on IoT devices with standard digital forensic readiness techniques are ineffective due to memory capabilities and limited computing resources [8]. The forensic investigation process is compatible with standard devices electronic such as personal computers, laptops, servers, and smartphones, but forensic investigations with characteristics of IoT need to be carried out in a much more comprehensive manner in comparison with standard digital forensics [9,10]. For instance, many potential digital tokens of IoT devices communicate with the marketplace, making them extremely vulnerable and dangerous security holes. Internet of Things (IoT) devices produce significant amounts of data and digital records that lack traceability due to network disconnection, limited resources, and memory capabilities. Digital information and recordings assume an important part as crucial evidence in the event of undesirable occurrences, but when the IoT device is no longer connected, there is no other way to obtain the digital evidence needed for the forensic investigation process. Thus, the identification and collection of digital evidence is very important as a readiness for digital forensic investigations.

The digital forensic readiness process has been discussed in previous research such as [11-16] and also in the international standard ISO/IEC 27043 [17]. This standard emphasizes how important it is to use a standardized process when carrying out the forensic readiness process. One of the challenges when implementing digital forensic readiness is that this standard is presented in general terms, not specifically using technical methods for Internet of Things (IoT) forensic investigations. Therefore, in this research, we proposed the enhanced Forensic Readiness framework based on previous research with a combined artificial intelligence approach.

This research makes the following contributions. First, the enhanced forensic readiness framework for IoT investigation based on previous research, which is the technical readiness stages to address challenges in identification from collecting digital evidence which preserving it in a trusted, smart repository. The collected and stored attack logs are generated and analysed in the smart repository to collect information regarding the type of attack and trace patterns. The identification of these attacks is automated through an artificial intelligence approach based on a dataset that was generated from these attack logs. Second, the enhancement of this readiness forensic framework can help investigators to be very specific and more focused on identification attack type domains in IoT environment. In addition, using a smart repository as a container for IoT evidence can facilitate investigators to an effective and efficient digital evidence forensic investigation, also serves as early warning system.

2. Background and Related Work

This particular section provides a comprehensive overview of IoT forensic challenges, as well as the significance of digital forensic readiness in the IoT domain and IoT digital forensic readiness frameworks. The proposed forensic readiness framework in this research also adheres to the International Standard ISO/IEC 27043, which outlines the process of implementing digital forensic readiness in the context of a digital forensic investigation. Optimizing and adapting artificial intelligence is critical in improving the effectiveness of forensic investigations, especially as the amount of data generated by IoT devices and the complexity of attacks increase rapidly. According to this, forensic readiness framework must adapt to current developments that are combined with artificial intelligence approaches.

2.1 IoT Forensic Challenges

Internet of Things (IoT) forensic is a specialized branch within the realm of digital forensic investigation that focuses on identifying and extracting legally admissible digital information as digital evidence from the Internet of Things (IoT) environment [18]. Several challenges related to forensic investigations on IoT devices have also been highlighted by researchers [19,20]. For example, Zhang *et al.,* research [21] explained that one of the difficulties is keeping up with the advancement of IoT devices and networks, which greatly impacts the collection of digital evidence and highlights the importance of sharing knowledge to support forensic investigative activities.

In addition, Atlam *et al.*, [22] stated that IoT devices have limited computing resources and memory capabilities. Thus, these conditions make the main limitations that cause security problems in the collection of digital evidence by investigators untraceable. That means investigators cannot capture, monitor, and analyse various communications that occur between IoT devices. The characteristics possessed by IoT devices like this make it challenging for forensic analysts to document the numerous incidents on these devices. Also, the data that is created and kept on Internet of Things (IoT) devices exhibits a limited lifespan and temporary existence, and ultimately, the data intended to function as digital evidence is easily erased and rewritten. Due to such limitations, causing the collection of digital evidence is also a major problem for forensic IoT analysis [23]. In order to conduct research and investigations involving IoT devices, it is crucial to develop and employ forensic techniques that can enhance effectiveness [24]. Additionally, specific tools and methodologies are required to bolster the resilience and security of IoT networks against potential attacks. Thus, becoming a security challenge for investigators in the collection of IoT forensic evidence.

According to Atlam *et al.*, [22], the level of reinforcement and development of the introduction of IoT devices into society brings about a significant level of intricacy in forensic investigations due to the wide array of functional variations and diverse operating systems employed across numerous Internet of Things (IoT) devices. The current tools for forensic investigation encounter difficulties in effectively accommodating the diverse attributes exhibited inside the IoT environment. The various challenges mentioned and described above require intervention from various forensic communities. In this scenario, digital forensic measures and proactive strategies are employed in response to illegal activities or cyberattacks. Also known as cyber forensics, involves the systematic collection, analysis, and preservation of digital evidence to investigate and prevent cybercrimes. It encompasses a wide range of techniques and tools designed to uncover, trace, and understand the nature of security incidents. In the continuously developing landscape of cybersecurity, this approach is essential for maintaining the integrity and security of digital systems and sensitive data.

2.2 IoT Forensic Readiness Based on ISO/IEC 27043

Based on the ISO/IEC 27043 standard, the forensic readiness process consists of 4 process groups, as shown in Figure 1. The next section will discuss the readiness process groups by referring to words taken from the ISO/IEC 27043 standard.

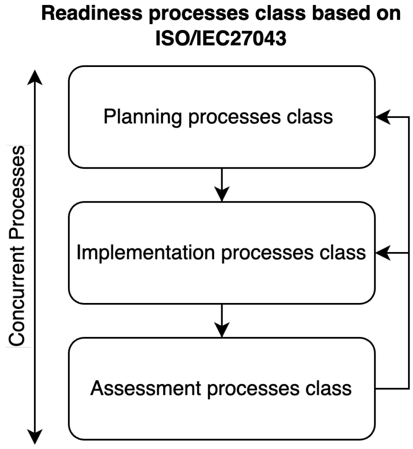
Readiness processes class based on ISO/IEC27043
Concurrent Processes
Planning processes class
Implementation processes class
Assessment processes class

Fig. 1. Readiness processes class

i. The Planning Processes Class, as defined by ISO/IEC 27043 involves planning activities for the pre-incident collection, storage, analysis, and presentation of digital forensic (DF) evidence. It encompasses the identification of actions to be taken upon incident detection and ensures that legal and specific requirements are considered in the overall Digital Forensic Readiness (DFR) process.

ii. The Implementation Processes Class puts into action the processes planned earlier, focusing on establishing the necessary system architecture and deploying systems and policies for effective digital forensic evidence collection, including incident logging, storage, and change-tracking tools and hardware across the organization.

iii. The Assessment Processes Class evaluates the outcomes of the Implementation Process Class, aiming to align them with Digital Forensic Readiness (DFR) objectives. The findings guide enhancements to the overall DFR process and ensure compliance with legal requirements and digital forensic principles for the admissibility of evidence in a court of law.

iv. Concurrent Processes, such as the chain of custody preservation, operate simultaneously with digital investigation processes, offering cross-functional applicability to various stages. The focus is on maintaining the integrity of the chain of custody as digital evidence is handled by different parties within the digital investigation process.

Conceptually, forensic readiness is an anticipatory strategy employed to apprehend prospective digital evidence before criminal activity or action can be investigated. Digital forensic readiness works and has been widely used to bail out and solve countless crime problems by providing a wide range of support and preserving digital evidence with great potential for digital forensic investigations. Research Venter and Ivans and Zulkipli *et al.*, [25,26] contributes to providing suggestions for six-component requirements and factors that must be owned by digital forensic readiness. The six components consist of Capabilities (Cap), Resources (Res), Operability (Op), Strategic Planning (SP), Knowledge (Kn) and Awareness (Aw). According to Collie [27], the digital forensic readiness process can be successfully achieved in two different ways. First, implement organizational data security policies and procedures. Second, by utilizing technical methods to track and preserve digital evidence.

Several other studies, involving [26,28,29], have actualization forensic readiness for IoT forensic investigations with organizational policy and procedure methods. The application of this method is because collecting digital evidence is a complex forensic investigation, particularly in the IoT environment. Thus, this research objectives are to develop technical methods for identification digital evidence with high accuracy and classification attack type from many IoT devices, also collection them into a smart repository effectively and efficiently as the development of forensic readiness for the IoT forensic environment for early warning system.

2.3 Readiness Forensic Based on Artificial Intelligence (AI) Approach

Conceptually, this term refers to artificial intelligence (AI) methodologies in enhancing an entity's readiness forensic to respond effectively to a variety of IoT challenges, such as cybersecurity incidents, legal investigations, disaster recovery, and operational disruptions. This innovative approach leverages AI's capabilities to identify, analyse, predict and optimize readiness strategies, ultimately ensuring a level of resilience and responsiveness. The primary objective of incorporating artificial intelligence (AI) into readiness forensic strategies is to cultivate a robust sense of resilience and responsiveness within an IoT entity. Through perpetual learning from data patterns, adept adjustments to emerging challenges, and the fine-tuning of responses, organizations can construct a proactive and adaptive framework. This framework significantly enhances the overall level of readiness IoT forensic. In a period characterized by dynamic and evolving any IoT type attack, the integration of AI with readiness strategies embodies an innovative approach to fortifying an capacity to adeptly and effectively navigate challenges.

3. Enhanced Readiness Forensic Framework for IoT Investigation

In retrospect, ISO/IEC 27043 was designed intentionally at an abstract level, enabling its application to digital investigations in a variety of contexts and types of digital evidence. The forensic readiness process described in ISO/IEC 27043 involves four main groups, namely planning, implementation, assessment, and concurrent processes. The purpose of this research is to discuss the planning and implementation of the four process classes, because this is abstract and does not fully reflect the unique characteristics of IoT technology. Therefore, the enhancement of the proposed AI-based IoT-FR Framework seeks to address DFR in the planning and implementation process class to meet the weaknesses and limitations in the characteristics of IoT technology. The assessment processes class is adopted as is in ISO/IEC 27043 and the concurrent process is replaced because it indicates preservation processes. Figure 2 illustrates the differences between the readiness process in the international standard ISO/IEC 27043 and the AI-based approach IoT-Forensic Readiness framework.

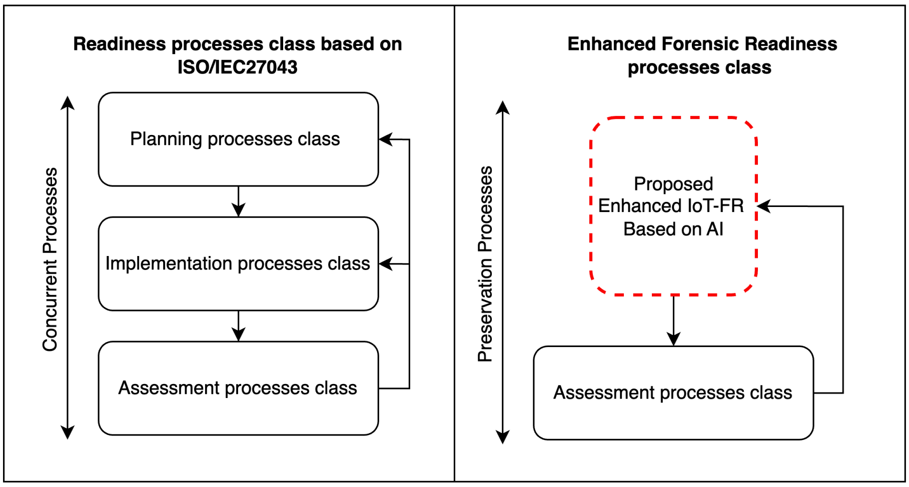
Readiness processes class based on ISO/IEC27043
Concurrent Processes
Planning processes class
Implementation processes class
Assessment processes class
Enhanced Forensic Readiness processes class
Preservation Processes
Proposed Enhanced IoT-FR Based on AI
Assessment processes class

Fig. 2. Consideration enhanced readiness processes class from ISO/IEC 27043

According to Abidin *et al.*, [30], the objective of the readiness processes is to guarantee the preparation, collection, examination and analysis, also reporting of all pertinent data and potential digital forensic data in accordance with the specifications outlined before investigation processes. These processes encompass tasks related to pinpointing crucial data sources, identify and managing forensic digital evidence, implementing tools forensic, also handling incident response and monitoring real-time with function as early warning system. The readiness processes are depicted in Figure 3 below, where all digital evidence data is enhanced and consolidated into a smart repository integrated with artificial intelligence.

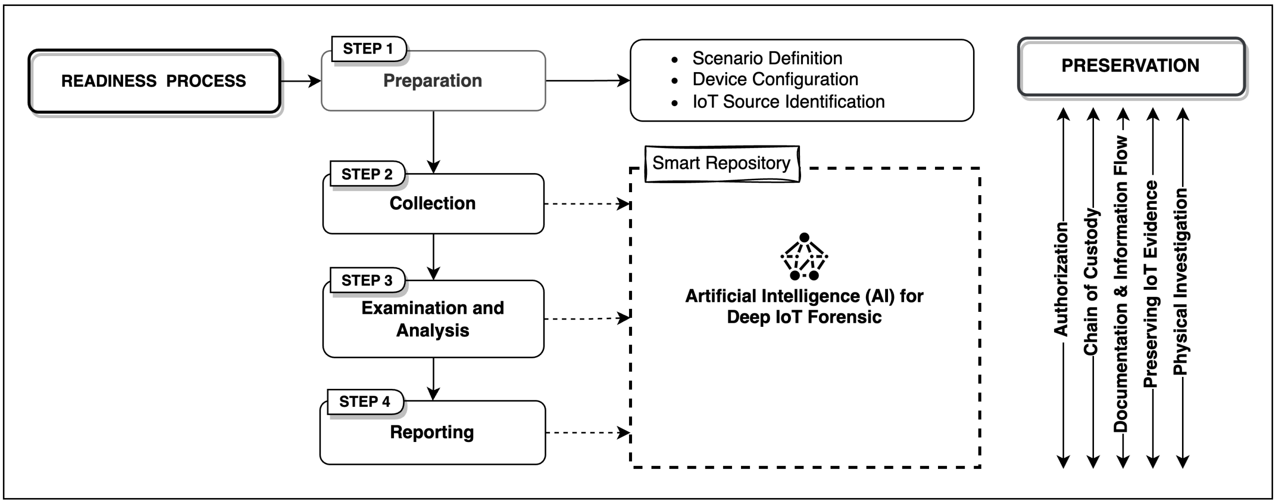

Fig. 3. Overview of enhanced IoT readiness forensic framework integrated AI-based

Although there are a number of frameworks for readiness forensic in an IoT environment, such as in research [11-15]. However, there is no forensic readiness framework to identify and classify types of attacks from various IoT devices directly by storing digital evidence in a smart repository integrated with artificial intelligence (AI) algorithms that aim for high accuracy analysis and an early warning system. Therefore, this research proposes the enhancement of readiness forensic framework to optimize the forensic investigation process on IoT devices which is carried out effectively and efficiently by investigators. During the readiness forensic process, digital evidence identification using artificial intelligence from various potential sources related to Internet of Things (IoT) devices is collected and stored while maintaining the integrity and accuracy the digital evidence. This process can reduce the time, effort, and costs required in the forensic investigation process for subsequent incidents.

Figure 3 shows five main processes (Step 1 – Step 4) of the readiness forensic: Preparation, Collection, Examination and Analysis, Presentation. Which step 2, 3, 4 into Smart Repository integrated AI-based approach. Each step has its sub-process. Moreover, the preservation process has become a critical and systematic procedure within the realm of legal and investigative activities aimed at safeguarding and maintaining the integrity of potential evidence relevant to a case, dispute, or inquiry in the overall digital forensic readiness framework.

3.1 Step 1: Preparation

First, the sub-processes of the Internet of Things (IoT) evidence preparation stage are as follows:

3.1.1 Scenario definition

In this process, we define all possible forensic investigation scenarios in the form of event sequences while being attuned to particular IoT applications to collect potential digital evidence with proper risk assessment. For example, unusual interactions with devices and unsuccessful authorization endeavours during the process of gaining access to those services. Within the application layer, scenarios are formulated to encompass the management of configuration and data. This entails considerations such as determining data accessibility and authorization privileges. Every individual scenario delineates events that induce alterations in the operational status of IoT devices. These alterations in the state are meticulously recognized in tandem with the corresponding attributes of the involved devices.

3.1.2 Device configuration

Before an Internet of Things (IoT) device operates, this procedure aims to detect and document every newly introduced device within the forensic ecosystem, along with its associated attributes. It involves configuring device-specific settings for IoT devices and securely storing all pertinent regulatory details in dedicated storage, ensuring their availability for future utilization.

3.1.3 IoT source identification

This process identifies the source of attack events on IoT devices forensically in accordance with the scenario established during the scenario definition step. Procedures are defined to validate network traffic interactions on IoT devices and identify potential sources. For example, at the application layer, a system can be formulated to oversee security facets concerning system configuration and the validation of access requests.

3.2 Step 2: Collection

The acquisition of digital evidence is a key point in the forensic process. This process includes the identification, acquisition, and collection of evidence from multiple IoT devices. For example, logging every attack activity directed at the device along with its timestamp. Command sources and attacks on devices will be logged. It is important to note that collaboration with service providers may very well be required to collect case-related data. The collection of digital evidence will be easier when tools and device operating systems support forensics to collect relevant evidence information.

The main goal of this process is to unify all incoming Internet of Things (IoT) network activity and filter rules based on predefined to determine known attack patterns. These rules update regularly to stay abreast of emerging threats. Additionally, it compares incoming IoT attacks against these rules and acts when a match is found.

3.3 Step 3: Examination and Analysis

This particular step refers to a specific stage within a comprehensive readiness designed for handling digital forensic activities in the IoT domain. This stage involves the careful examination of digital elements followed by a detailed analysis of the gathered digital evidence, contributing to a robust response and mitigation strategy in the context of IoT-related security incidents and rapidly evolving landscape of IoT technology.

3.4 Step 4: Reporting

This step in a forensic readiness framework is a critical component that focuses on the documentation, communication, and presentation of findings derived from IoT forensic investigation activities. This step plays a crucial role in ensuring transparency, accountability, and the effective sharing of insights with relevant stakeholders.

3.5 Smart Repository

The concept of smart repository suggests the development of an intelligent and integrated storage system specifically designed to enhance digital forensic readiness in the realm of the Internet of Things (IoT). The repository may utilize metadata and contextual information to organize digital evidence systematically, making it easily accessible for forensic analysis. The integration of artificial intelligence (AI) within the repository signifies the incorporation of deep learning algorithms and predictive analytics. AI enhances the repository's capabilities by automating tasks, recognizing patterns, and providing intelligent insights.

The smart repository, integrated with AI, becomes a proactive component in this readiness strategy, enabling swift and intelligent responses to emerging threats. AI-driven capabilities streamline the collection, identification, and analysis of IoT digital evidence, contributing to a more effective and timely forensic response.

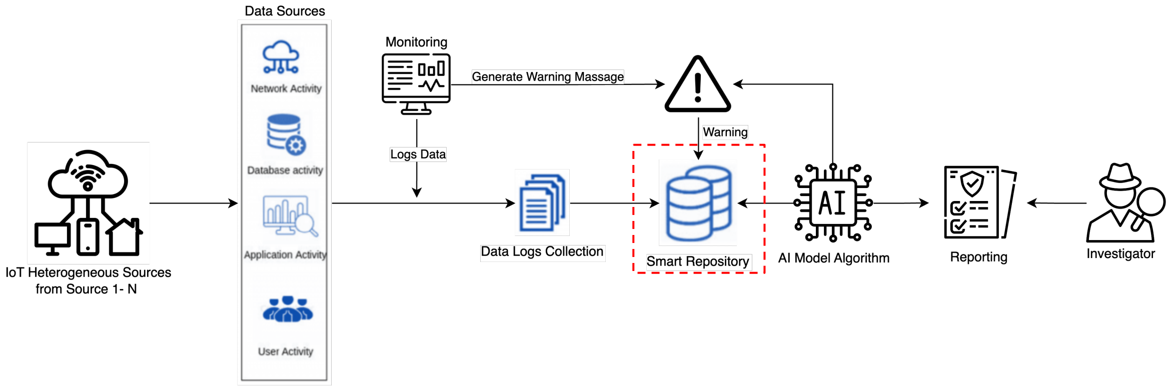

Fig. 4. Flow diagram smart repository integrated AI approach

3.6 Preservation Processes

This process can increase the acceptance of the IoT environment without difficulty. Authorization is involved with the entire forensic investigation framework process, which contains authority, user, and owner information. In addition, the concept of the chain of custody is harnessed to enhance the effectiveness of storing information pertinent to IoT forensic investigations. Its application extends to delineating the flow of information and fortifying security within an IoT-centric setting. Moreover, the preservation of forensic evidence stands as a pivotal facet within the framework of forensic investigation. Once evidence is amassed, it becomes imperative to uphold its integrity through secure encryption keys, assuring that it remains inviolate and unaltered.

4. Experimental Result and Discussion

At this stage, a comprehensive overview of the utilized the dataset used is described in detail, and the results of the discussion found are presented based on findings from research during the research. The findings presented in this stage serve to elucidate the significance of the dataset in shaping the research outcomes, offering valuable insights into the intricacies and nuances discovered during the investigative process.

4.1 Dataset Validation

This research involves collecting normal traffic after configuration of IoT devices in the network. Next, it infects the device with various types of botnet attacks, such as Mirai and Bashlite, and captures attack traffic on the IoT network. This approach enables in-depth analysis of IoT devices' responses to botnet attacks, aiding the understanding and identification of potential vulnerabilities in network security. A total of 115 features were extracted from the captured traffic after installation and configuration of IoT devices. A snapshot is taken of the host and protocol communicating with each captured packet, then extracted 23 summary statistical information on each traffic flow from 5 different time intervals.

Table 1 records the quantity of occurrence for each type of attack on each type of device. However, the dataset does not include information about Mirai attacks originating from Webcam devices. The right part of the table shows the proportion of data related to each type of attack in the dataset. This information provides a more detailed picture of the extent to which certain types of attacks affect specific devices in the context of the dataset forensic investigation.

Table 1
The quantity every attack category associated with each type of device

Botnet	Attack	Doorbell	Thermostat	Baby Monitor	Security Camera	Portion of Data
Benign		88,648	13,113	175,240	226,781	8%
	Combo	112,732	53,012	58,152	232,591	7%
	Junk	58,865	30,312	28,349	115,958	4%
Bashlite	Scan	57,969	27,494	27,859	114,091	4%
	TCP	193,677	95,021	92,581	380,788	12%
	UDP	209,807	104,791	105,782	415,369	13%
	ACK	102,195	113,285	91,123	337,218	9%
	Scan	107,685	43,192	103,621	283,481	8%
Mirai	SYN	112,573	116,807	118,128	375,791	10%
	UDP	237,665	151,481	217,034	623,819	17%
	UDP-Plain	81,892	87,368	80,808	273,146	8%
Total		1,373,798	835,876	1,098,677	3,379,033	100%

The constructed deep learning model utilizes a classification report, which is a performance assessment tool in artificial intelligence. Also evaluating and comparing the performance of trained models. This report presents crucial metrics, including precision, recall, F1 Score, and support, providing insights into the performance of a classification model.

4.2 Result and Discussion

Dataset in experimental results used as evaluation for deep learning models show that the performance of these models has been evaluated and compared with various neural network architectures. The evaluation process uses relevant evaluation metrics, and the results provide insight into the performance of this network in the context of the proposed deep learning model used in this research. The GRU deep learning model illustrated in Figure 5, outlines its structure and data flow across various layers.

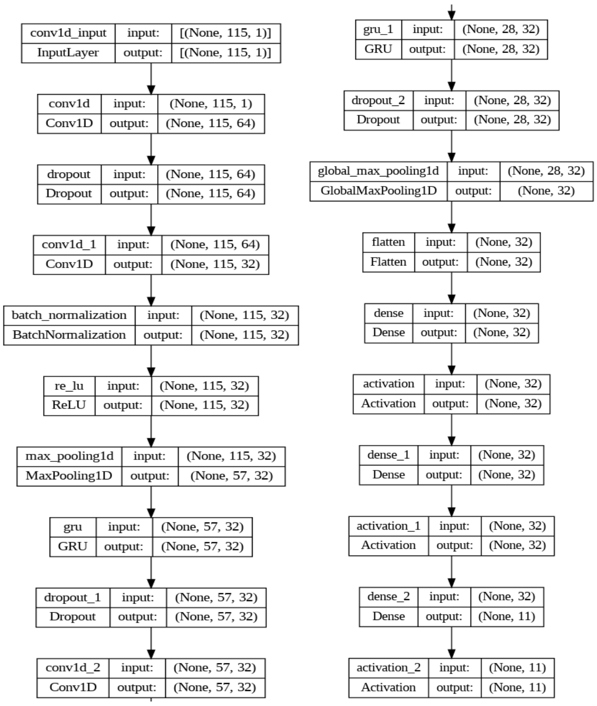
conv1d_input InputLayer input: [(None, 115, 1)] output: [(None, 115, 1)]
conv1d Conv1D input: (None, 115, 1) output: (None, 115, 64)
dropout Dropout input: (None, 115, 64) output: (None, 115, 64)
conv1d_1 Conv1D input: (None, 115, 64) output: (None, 115, 32)
batch_normalization BatchNormalization input: (None, 115, 32) output: (None, 115, 32)
re_lu ReLU input: (None, 115, 32) output: (None, 115, 32)
max_pooling1d MaxPooling1D input: (None, 115, 32) output: (None, 57, 32)
gru GRU input: (None, 57, 32) output: (None, 57, 32)
dropout_1 Dropout input: (None, 57, 32) output: (None, 57, 32)
conv1d_2 Conv1D input: (None, 57, 32) output: (None, 57, 32)
gru_1 GRU input: (None, 28, 32) output: (None, 28, 32)
dropout_2 Dropout input: (None, 28, 32) output: (None, 28, 32)
global_max_pooling1d GlobalMaxPooling1D input: (None, 28, 32) output: (None, 32)
flatten Flatten input: (None, 32) output: (None, 32)
dense Dense input: (None, 32) output: (None, 32)
activation Activation input: (None, 32) output: (None, 32)
dense_1 Dense input: (None, 32) output: (None, 32)
activation_1 Activation input: (None, 32) output: (None, 32)
dense_2 Dense input: (None, 32) output: (None, 11)
activation_2 Activation input: (None, 11) output: (None, 11)

Fig. 5. GRU deep layer model for baby monitor device

The model includes convolutional layers, activation layers, max pooling layers, and dense layers, as visualized in Figure 6. The model takes data with dimensions (None, 115, 1) and produces output with dimensions (None, 11). This model uses a combination of utilizing convolutional and dense layers for the purpose of analysing input data and extracting relevant details. A max pooling layer is used to reduce the dimensionality of the data and an activation layer introduces non-linearity into the model.

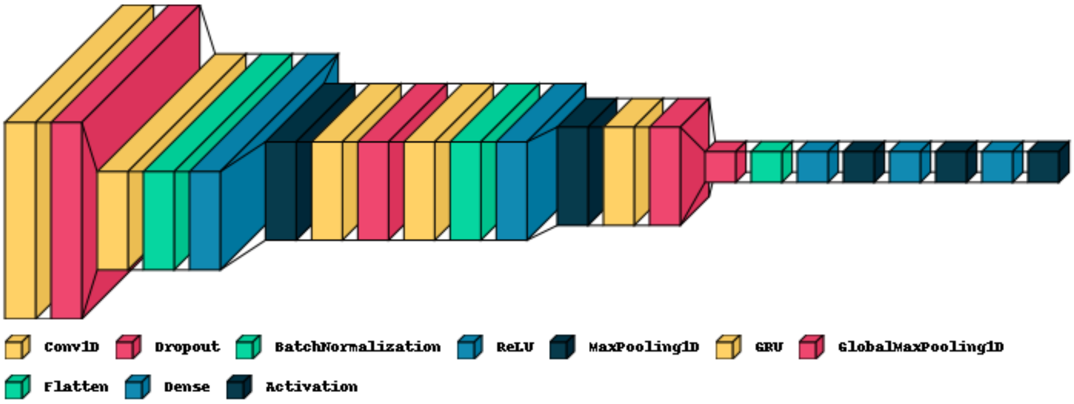

Fig. 6. GRU deep learning model visualization for baby monitor device

Figures 7 present the results of training and validation accuracy of the GRU model trained using PSO (Particle Swarm Optimization). The model has undergone 5 iterations, with each iteration consisting of 10 particles. The resulting accuracy scores for the model are 0.94 for highest score baby monitor device. In the visual representation graph, it shows the accuracy of the model for 30 epochs. The x-axis represents the number of epochs, ranging from 0 to 30, while the y-axis represents the accuracy score. The graph shows a gradual increase in accuracy as the number of epochs increases. The model also has a very low loss rate of 0.1027, indicating that the model has undergone a good training process and can provide more accurate predictions.

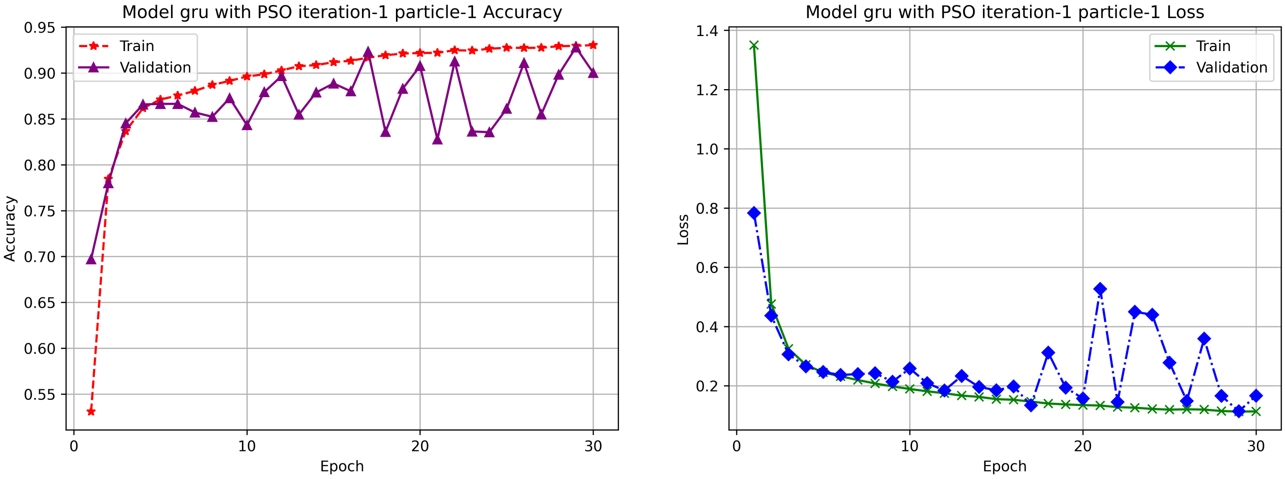

Fig. 7. Accuracy and loss graphs of training and validation data

Table 2
Comparison accuracy with previous model

No.	Model	Doorbell	Baby Monitor	Security Camera
1	RNN [31]	0.41	0.44	0.37
2	LSTM [31]	0.62	0.54	0.25
3	CNN [31]	0.91	0.91	0.85
6	GRU	0.86	0.94	0.91

Table 3 provides a comparison of the average accuracy scores between the previous model and the proposed model. We succeeded in creating model that is optimized for various IoT devices with higher accuracy results than the previous model, namely 0.94 for baby monitor device. For Security camera device get score 0.91 and the last score 0.86 for doorbell device. This significant improvement in accuracy across different devices underscores our commitment to delivering cutting-edge solutions tailored to the unique requirements of IoT environments.

Table 3
The results for each attack type for highest score

Index	Label (Benign / Attack Type)	Precision	Recall	F1-Score	Support
0	Benign	1.00	1.00	1.00	8678
1	Gafgyt_combo	1.00	0.96	0.98	2869
2	Gafgyt_junk	0.96	1.00	0.98	2874
3	Gafgyt_scan	1.00	1.00	1.00	2790
4	Gafgyt_tcp	1.00	0.00	0.00	2749
5	Gafgyt_udp	0.54	1.00	0.70	3236
6	Mirai_ack	0.99	1.00	1.00	4504
7	Mirai_scan	1.00	1.00	1.00	3026
8	Mirai_syn	1.00	1.00	1.00	6026
9	Mirai_udp	1.00	0.99	1.00	4314
10	Mirai_udpplain	1.00	1.00	1.00	4451
	Accuracy			0.94	45517
	Macro avg	0.86	0.90	0.88	45517
	Weighted avg	0.90	0.94	0.91	45517

5. Evaluation of Forensic Readiness Framework

Internet of Things devices is getting a lot of attention and widespread adoption across various industries development which begins from smart home, which are currently combined with the Artificial Intelligence approach. However, due to a security flaw or the vulnerabilities within these devices, numerous systems have been breached, yet no conclusive evidence has been uncovered. This can be attributed to the insufficient processing capabilities and severe memory limitations. To solve this problem, we have proposed the enhancement this IoT forensic readiness framework that keeps collect and identify logs data as IoT evidence of the attacks on smart repository integrated with an AI approach that can automatically perform forensic investigation analysis. By quickly identifying and detecting attacks, AI-based analysis increases the efficiency of the readiness framework. When traffic complies with these rules, real-time alerts and logs are created as early warning system. Attacks are identified with high accuracy to facilitate investigators in forensic investigations. Table 4 illustrates a comparison of the proposed framework with existing frameworks. AI-based smart repositories and generating rules deep learning model the parameters that differentiate our research from previous work.

Table 4
Comparison phase of IoT forensic readiness framework

		Preparation			Collection			Smart Repository			
Year	Author / Research Framework	Scenario Definition	Device Configuration	Identification	Generated Rules	Acquisitions	Realtime Monitoring	Integrity	Detection	Classification	Analyze
2023	Randi *et al.,* : Enhanced Readiness Forensic Framework for IoT forensic Based on AI	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2022	Mazhar *et al.,* : Machine to Machine (M2M) for IoT Forensic Framework [32]	✓	✓	✓	x	✓	✓	✓	x	x	x
2022	Fagbola *et al.,* : Smart Digital Forensic Readiness Model [12]	✓	✓	✓	x	✓	✓	x	x	x	x
2022	Alotaibi *et al.,* : Drone Forensics with A Novel Forensic Readiness Framework [15]	✓	✓	✓	x	✓	✓	x	x	x	x
2021	Sadineni *et al.,* : Ready-IoT Model for Internet of Things Forensic [13]	✓	✓	✓	x	✓	✓	x	x	x	x
2021	Ahmad Saleh *et al.,* : Common IoT Forensic Investigation Process Model [33]	✓	✓	✓	x	✓	✓	x	x	x	x
2020	Koroniotis *et al.,* : A particle deep framework for IoT networks [34]	✓	✓	✓	x	✓	✓	x	x	x	x
2020	Noura *et al.,* : DistLog scheme model for IoT forensics [35]	✓	✓	✓	x	✓	✓	x	x	x	x
2020	Scheidt *et al.,* : Identification IoT Devices for Forensic Investigation [36]	✓	✓	✓	x	✓	x	x	x	x	x
2019	Qatawneh *et al.,* : DFIM: A New Model for IoT Digital Forensics Investigation [37]	✓	✓	✓	x	✓	✓	x	x	x	x
2019	Sadineni *et al.,* : A Holistic Model for IoT Forensic Investigation [11]	✓	✓	✓	x	✓	x	x	x	x	x
2019	Jahidul Islam *et al.,* : A Comprehensive Framework for IoT Digital Forensic [16]	✓	✓	✓	x	✓	✓	x	x	x	x

6. Conclusions and Future Work

This research proposes the enhancement of a framework for implementing forensic readiness in IoT devices' forensic investigation. Forensic readiness development overcomes the low and memory limitations and is able to identify and collect potential digital evidence by considering the specific functionality and behaviour of IoT devices. Smart repository become the main step in this framework for forensic readiness purposes in a manner that facilitates the forensic investigation process in the IoT device environment to become more efficient and reliable. Also, the smart repository for forensic readiness is critical as a complementary approach to characteristic IoT devices. As part of the research, the authors have implemented this smart repository integrated deep learning algorithm for the process of investigating attacks on IoT environments with high accuracy detection as early warning system.

Acknowledgment

The authors wholeheartedly acknowledge the profound impact that the JKF research group at the Department of Informatics Siliwangi University and FTMK UTeM with the INSFORNET research group have had on this research. Their support, shared knowledge, and guidance have been pivotal, and the authors are deeply grateful for the privilege of working alongside such esteemed colleagues.

References

[1] Kaur, Rasmeet, B. L. Raina, and Avinash Sharma. "Internet of things: architecture, applications, and security concerns." *Journal of Computational and Theoretical Nanoscience* 17, no. 6 (2020): 2468-2474. https://doi.org/10.1166/jctn.2020.8917

[2] Kumar, Sachin, Prayag Tiwari, and Mikhail Zymbler. "Internet of Things is a revolutionary approach for future technology enhancement: a review." *Journal of Big data* 6, no. 1 (2019): 1-21. https://doi.org/10.1186/s40537-019-0268-2

[3] Ding, Jie, Mahyar Nemati, Chathurika Ranaweera, and Jinho Choi. "IoT connectivity technologies and applications: A survey." *IEEE Access* 8 (2020): 67646-67673. https://doi.org/10.1109/ACCESS.2020.2985932

[4] Umair, Muhammad, Muhammad Aamir Cheema, Omer Cheema, Huan Li, and Hua Lu. "Impact of COVID-19 on IoT adoption in healthcare, smart homes, smart buildings, smart cities, transportation and industrial IoT." *Sensors* 21, no. 11 (2021): 3838. https://doi.org/10.3390/s21113838

[5] Deogirikar, Jyoti, and Amarsinh Vidhate. "Security attacks in IoT: A survey." In *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)*, pp. 32-37. IEEE, 2017. https://doi.org/10.1109/I-SMAC.2017.8058363

[6] Butun, Ismail, Patrik Österberg, and Houbing Song. "Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures." *IEEE Communications Surveys & Tutorials* 22, no. 1 (2019): 616-644. https://doi.org/10.1109/COMST.2019.2953364

[7] Nguyen, Tri Gia, Trung V. Phan, Binh T. Nguyen, Chakchai So-In, Zubair Ahmed Baig, and Surasak Sanguanpong. "Search: A collaborative and intelligent nids architecture for sdn-based cloud iot networks." *IEEE access* 7 (2019): 107678-107694. https://doi.org/10.1109/ACCESS.2019.2932438

[8] Son, Jihun, Gyubin Kim, Hyunwoo Jung, Jewan Bang, and Jungheum Park. "IF-DSS: A forensic investigation framework for decentralized storage services." *Forensic Science International: Digital Investigation* 46 (2023): 301611. https://doi.org/10.1016/j.fsidi.2023.301611

[9] Ghosh, Atonu, Koushik Majumder, and Debashis De. "A systematic review of digital, cloud and iot forensics." *The" Essence" of Network Security: An End-to-End Panorama* (2021): 31-74. https://doi.org/10.1007/978-981-15-9317-8_2

[10] Kim, Jieon, Jungheum Park, and Sangjin Lee. "An improved IoT forensic model to identify interconnectivity between things." *Forensic Science International: Digital Investigation* 44 (2023): 301499. https://doi.org/10.1016/j.fsidi.2022.301499

[11] Sadineni, Lakshminarayana, Emmanuel Pilli, and Ramesh Babu Battula. "A holistic forensic model for the internet of things." In *Advances in Digital Forensics XV: 15th IFIP WG 11.9 International Conference, Orlando, FL, USA, January 28–29, 2019, Revised Selected Papers 15*, pp. 3-18. Springer International Publishing, 2019. https://doi.org/10.1007/978-3-030-28752-8_1

[12] Fagbola, Funmilola Ikeolu, and Hein S. Venter. "Smart digital forensic readiness model for shadow IoT devices." *Applied Sciences* 12, no. 2 (2022): 730. https://doi.org/10.3390/app12020730

[13] Sadineni, Lakshminarayana, Emmanuel S. Pilli, and Ramesh Babu Battula. "Ready-iot: A novel forensic readiness model for internet of things." In *2021 IEEE 7th World Forum on Internet of Things (WF-IoT)*, pp. 89-94. IEEE, 2021. https://doi.org/10.1109/WF-IoT51360.2021.9595902

[14] Riedler, Melanie. "Digital Forensic Readiness." Bachelor's thesis, 2018.

[15] Alotaibi, Fahad Mazaed, Arafat Al-Dhaqm, and Yasser D. Al-Otaibi. "A novel forensic readiness framework applicable to the drone forensics field." *Computational Intelligence and Neuroscience* 2022 (2022). https://doi.org/10.1155/2022/8002963

[16] Islam, Md Jahidul, Md Mahin, Ayesha Khatun, Biplab Chandra Debnath, and Sumaiya Kabir. "digital forensic investigation framework for internet of things (IoT): A Comprehensive Approach." In *2019 1st International Conference on Advances in Science, Engineering and Robotics Technology (ICASERT)*, pp. 1-6. IEEE, 2019. https://doi.org/10.1109/ICASERT.2019.8934707

[17] Valjarević, Aleksandar, Hein Venter, and Ranko Petrović. "ISO/IEC 27043: 2015—Role and application." In *2016 24th Telecommunications Forum (TELFOR)*, pp. 1-4. IEEE, 2016. https://doi.org/10.1109/TELFOR.2016.7818718

[18] Janarthanan, T., M. Bagheri, and S. Zargari. "IoT forensics: an overview of the current issues and challenges." *Digital Forensic Investigation of Internet of Things (IoT) Devices* (2021): 223-254. https://doi.org/10.1007/978-3-030-60425-7_10

[19] MacDermott, Aine, Thar Baker, and Qi Shi. "Iot forensics: Challenges for the ioa era." In *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, pp. 1-5. IEEE, 2018. https://doi.org/10.1109/NTMS.2018.8328748

[20] Li, Shancang, Kim-Kwang Raymond Choo, Qindong Sun, William J. Buchanan, and Jiuxin Cao. "IoT forensics: Amazon echo as a use case." *IEEE Internet of Things Journal* 6, no. 4 (2019): 6487-6497. https://doi.org/10.1109/JIOT.2019.2906946

[21] Zhang, Xiaolu, Kim-Kwang Raymond Choo, and Nicole Lang Beebe. "How do I share my IoT forensic experience with the broader community? An automated knowledge sharing IoT forensic platform." *IEEE Internet of Things Journal* 6, no. 4 (2019): 6850-6861. https://doi.org/10.1109/JIOT.2019.2912118

[22] Atlam, Hany F., and Gary B. Wills. "IoT security, privacy, safety and ethics." *Digital twin technologies and smart cities* (2020): 123-149. https://doi.org/10.1007/978-3-030-18732-3_8

[23] Rughani, Parag H. "IoT evidence acquisition—Issues and challenges." *Advances in Computational Sciences and Technology* 10, no. 5 (2017): 1285-1293.

[24] Karabiyik, Umit, and Kemal Akkaya. "Digital forensics for IoT and WSNS." *Mission-Oriented Sensor Networks and Systems: Art and Science: Volume 2: Advances* (2019): 171-207. https://doi.org/10.1007/978-3-319-92384-0_6

[25] Venter, H. S., and Ivans Kigwana. "A digital forensic readiness architecture for online examinations." *South African Computer Journal* 30, no. 1 (2018): 1-39. https://doi.org/10.18489/sacj.v30i1.466

[26] Zulkipli, Nurul Huda Nik, and Gary B. Wills. "An exploratory study on readiness framework in IoT forensics." *Procedia Computer Science* 179 (2021): 966-973. https://doi.org/10.1016/j.procs.2021.01.086

[27] Collie, Jan. "A strategic model for forensic readiness." *Athens Journal of Sciences* 5, no. 2 (2018): 167-182. https://doi.org/10.30958/ajs.5-2-4

[28] Kebande, Victor R., Phathutshedzo P. Mudau, Richard A. Ikuesan, H. S. Venter, and Kim-Kwang Raymond Choo. "Holistic digital forensic readiness framework for IoT-enabled organizations." *Forensic Science International: Reports* 2 (2020): 100117. https://doi.org/10.1016/j.fsir.2020.100117

[29] Kebande, Victor R., and Indrakshi Ray. "A generic digital forensic investigation framework for internet of things (iot)." In *2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud)*, pp. 356-362. IEEE, 2016. https://doi.org/10.1109/FiCloud.2016.57

[30] Abidin, Z. Z., S. R. Selamet, and S. Anawar. "Multi-Layered based Digital Forensic Investigation for Internet-of-Things: Systematic Literature Review." *International Journal of Computer and Science and Network Security* 19, no. 9 (2019): 156-175.

[31] Kim, Jiyeon, Minsun Shim, Seungah Hong, Yulim Shin, and Eunjung Choi. "Intelligent detection of iot botnets using machine learning and deep learning." *Applied Sciences* 10, no. 19 (2020): 7009. https://doi.org/10.3390/app10197009

[32] Mazhar, Muhammad Shoaib, Yasir Saleem, Ahmad Almogren, Jehangir Arshad, Mujtaba Hussain Jaffery, Ateeq Ur Rehman, Muhammad Shafiq, and Habib Hamam. "Forensic analysis on internet of things (IoT) device using machine-to-machine (M2M) framework." *Electronics* 11, no. 7 (2022): 1126. https://doi.org/10.3390/electronics11071126

[33] Saleh, Muhammed Ahmed, Siti Hajar Othman, Arafat Al-Dhaqm, and Mahmoud Ahmad Al-Khasawneh. "Common investigation process model for Internet of Things forensics." In *2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE)*, pp. 84-89. IEEE, 2021. https://doi.org/10.1109/ICSCEE50312.2021.9498045

[34] Koroniotis, Nickolaos, Nour Moustafa, and Elena Sitnikova. "A new network forensic framework based on deep learning for Internet of Things networks: A particle deep framework." *Future Generation Computer Systems* 110 (2020): 91-106. https://doi.org/10.1016/j.future.2020.03.042

[35] Noura, Hassan N., Ola Salman, Ali Chehab, and Raphaël Couturier. "DistLog: A distributed logging scheme for IoT forensics." *Ad Hoc Networks* 98 (2020): 102061. https://doi.org/10.1016/j.adhoc.2019.102061

[36] Scheidt, Nancy, and Mo Adda. "Identification of iot devices for forensic investigation." In *2020 IEEE 10th international conference on intelligent systems (is)*, pp. 165-170. IEEE, 2020. https://doi.org/10.1109/IS48319.2020.9200150

[37] Qatawneh, Mohammad, Wesam Almobaideen, Mohammed Khanafseh, Ibrahim Al Qatawneh, and P. Al-Ain. "Dfim: A New digital forensics investigation model for internet of things." *Journal of Theoretical and Applied Information Technology* 97, no. 24 (2019): 3850-3867.