Survey on Intrusion Detection System in IoT Network- A Review

Syed Ali Mehdi[†] **and Syed Zeeshan Hussain**[††],

Jamia Millia Islamia, New Delhi, India

Summary
Internet of Things (IoT) has emerged as a powerful communication and networking system for smart and automation processing. With the increasing usage of the Internet of Things in numerous critical activities, it is essential to ensure that the communication among these devices is safe and secure. The biggest threat to safe and secure communication is from cyber-attacks. Cyber-attacks have evolved and become more complex henceforth posing increased challenges to the data integrity, communication security, and confidentiality of the data. With its success in detecting security vulnerabilities in a communication network, intrusion detection systems are best integrated for securing IoT-based devices. But the integration of an intrusion detection system in an IoT-based network is a challenging task. This paper investigates the state of the art of IoT and intrusion detection system, the technology in use, and the technology challenges by reviewing notable existing works. A systematic literature review of 25 sources comprising 22 research papers and articles covering the threat models, intrusion detection system key challenges in IoT, Proposed models, and implementation of models, reviews, and evaluations are reviewed. The findings explore the needs and the best ways of integrating artificial intelligence-based intrusion detection systems in IoT networks for ensuring security and safety of communication.

Keywords:
The intrusion detection system, Internet of Things (IoT), Computer Security, Artificial Intelligence.

1. Introduction

Internet of Things (IoT) is the technology that makes communication and control among an various devices connected in a network. IoT allows for distributed communication through devices, like sensors, and other communication devices, along with data processing units. It enables autonomous decision making and intelligent data processing and analysis. The biggest technology that helps IoT devices in establishing communication and data transfer are wireless communication and Cloud computing.

IoT usages have increased over the years, and today they are in automation applications like health care services, industries, smart home applications, etc. These devices are in use in these critical areas and thus are more under the attacker lists. Hackers aim to gain access to the network for financial gains and other gains. Security is thus of utmost importance for IoT-based devices as they are primarily used in automated applications. Thus, there is a need to have a reliable security mechanism, and an intrusion detection system is one such effective mechanism.

Intrusion detection is the process wherein the objective is to detect intruder actions. These intruder actions main objectives are to gain unauthorized access to the network and thereby interfere with data integrity or network security. The intrusion into the network can be carried out from inside the network i.e. internal intruders or from outside the network i.e. external intruders. Thus, the intrusion detection system (IDS) aims to identify the intruder actions and trigger an alarm in the network for quick response towards intruder actions. A general IDS comprises of sensors, an analytical engine for processing and analyzing intruder patterns or actions and a reporting mechanism. The sensors of the IDS are placed in the network at various host positions. The task of a sensor is to collect the host data that includes packer headers, network service requests, file exchanges, statistics of traffic etc. All this collected data is sent to the analytical engine that investigates the data and detects any intrusion. If in case any intrusion is detected the reporting mechanisms sends the report to the network admin and an alarm is triggered for the intrusion. Millions of money is spent securing the network, and the devices and IDS are such effective devices.

With emphasis on IoT Security, intrusion detection systems have been proposed for IoT environment. Before aiming to come up with efficient IDS for IoT it is essential to understand IDS in context with IoT environment. Thus, there is a need to examine the current state of art, the basic requirements of IDS in IoT, the best strategies and the best ways to have efficient IDS for IoT environment. This literature review aims to examine all these aspects by addressing following questions:

RQ1: What key cyber threats are faced by IoT devices that require the need of IDS?

RQ2: What are the IDS systems used so far in IoT based environment? Can they be classified? If Yes, on what basis?

RQ3: What are the critical challenges of IDS in the IoT environment? Can AI address these challenges?

Manuscript received December 5, 2024
Manuscript revised December 20, 2024
https://doi.org/10.22937/IJCSNS.2024.24.12.11

2. Methodology

2.1 Search and Selection strategy

The data for this literature work is obtained from various reputed sources in the form of research articles, literature reviews, case studies, web articles, and books in online printed form. The articles were extracted through search from search engines like Google, Google scholar, Sci-Hub, sciencedirect.com, and the university library. Apart from it the other useful research material was obtained from reputed books and student thesis documents. The search relied on the query of the Intrusion detection system in IoT; it was then further refined with keywords like Artificial intelligence, security threats in IoT, challenges, etc.

2.2 Data Analysis

Quick abstract reviews and the article summary review were opted as the preliminary paper selection method. For theoretical frameworks, reviewed surveys, and case studies full paper or abstract. Only papers with implementation models, their challenges, and experimentations are selected. The review findings shall be listed in the table, and the analysis shall be done based on the listing to come up with a conclusion.

2.3 Quality Appraisal

The research paper and articles quality were highly dependable on the following factors:

- Relevance: Whether the information is relevant to the topic of research

- Credibility: Whether the information in the paper, a book, or article is supported with facts and figures

- Transferability: Whether the information in paper or book can be generalized to other settings.

2.4 Result

Fifty-eight papers related to the topic were selected through abstract reviews from the year 2013 to 2020. These 58 papers were filtered out based on a full article review and topics related to IoT. This resulted in 25 relevant papers. When evaluation, research works, or surveys-based papers were searched, the search resulted in 22 papers and articles. The rest papers were filtered because either they are proposal or literature surveys. Finally, only implementation models and frameworks are selected. This resulted in 10 papers with implementation models and 12 for related works.

3. Discussion

3.1 Types of Security Threats in IoT based environment

Numerous researches have classified the various threats present in the IoT network. The broad classifications are passive attacks and active attacks.

1. Passive attacks: The passive attacks are mainly hindering confidentiality and are very hard to detect. In these attacks, the attackers are hidden and affect the communication lines. These include eavesdropping,

node tampering, node outage, analysis of traffic patterns, etc. [1].

2. Active attacks: These attacks not only affect confidently but also have an impact on data integrity. The attacker in active attack aims to gain access into the system through unauthorized means and affects the network's operations. Wireless sensor networks and IoT currently employ five different OSI models, namely the physical layer, the data link layer, the network layer, the transport layer, and the application layer. Research has classified attacks based on each layer. The summary of these attacks are as follows:

   - Denial of Service (DoS) – This security threat is known to deny or prevent the authorized users' to access the resources on a network. It does by sending unwanted traffic. This attack can affect the network order by sending data packets or by simply flooding the packets in the network. Some IoT devices thus shall be denied service [2].
   - Malware – In this attack an executable code known as malware is used to disturb the IoT devices in communication network. With this executable code the access into the network is gained. [1].
   - Sybil attack: Attacker sends fake identities to authorized nodes, and by doing so, these legitimate authorized nodes become disabled permanently from the network. This can lead the IoT devices to accept inaccurate reports and accept spam and thus lose privacy [3].
   - Replay attacks: This attack reproduces the signal which is used for controlling any device. Different modulation methods are used to capture this signal and then collect the data for this signal. This signal is then again retransmitted to gain access to the system [3].
   - Selective forwarding attack: The malicious nodes in the network behave like the normal nodes and thus refuse to forward a packet selectively or drop the packet selectively. By selective dropping or reject forwarding, the nodes do not come into the picture quickly [15].
   - Sinkhole attack: In this attack, the malicious node advertises through broadcasting to its entire neighbor that it is the next hop for them. All nodes start sending packets to this sinkhole. It does not drop the packet and thus remains undetected by the intrusion detection system [2;3].
   - Wormhole attack: In this attack, the attacker can get the data packets on one side of the tunnel, and through this tunnel, it can send to another malicious user. These are the toughest attacks to be detected and impact on localization, data fusion of the network[3].
   - Blackhole attack: in this attack, the malicious user listens to the packet request with the help of routing protocols and then drops all the packets, thus stopping the packets near the black hole [15].
   - Jamming attack: In this attack, the attacker monitors the operational frequency of the node signals from the receiver to sender and vice versa. It captures it and then transmits a signal on the same frequency to hinder the receptor [1].

3.2 Classification of the Intrusion Detection System (IDS) for IoT

Numerous Intrusion detection mechanisms have been proposed in existing research. These intrusion detection systems are classified as statistical methods, knowledge-based, data-mining methods, and machine learning-based methods [26]. Statistical-based IDS techniques, relies on stochastic behavior of the captured network traffic. The statistical patterns give information on good action and bad actions. The bad actions are marked and intrusion is triggered [9]. On the other hand knowledge-based techniques, makes use of prior knowledge of the user behaviour. These Knowledge-based Intrusion detection systems are known to encode the expert's knowledge of already known patterns of previous cyber-attack and any sort of system vulnerabilities in the form of if-then database rules [16]. These IDS build a knowledge base from the knowledge gained from various kinds of attacks and the loopholes that exist in the network. When any action that is not recognized as normal behaviour is detected, such action is not considered acceptable, and the alarm is triggered. The detection approach is based on measuring the distance based on the Gaussian function modified to function as a similarity function [26]. The approach uses the K-Means algorithm for clustering based on the distance measures over both the training and testing data[21]. The training and testing data are then converted to a single-dimensional feature vector through the distance measure and the k-means [21]. The existing research work concludes that the accuracy of such an intrusion detection system is good, and it generates very low false alarm rates [26]. But the limitation of the system is that it is complicated to gather information on the known attacks and update the data with the new set of vulnerabilities [26]. It is essential to have a thorough analysis of all the vulnerabilities for the maintenance of the knowledge base of the intrusion detection system, which is a very time-consuming job.

Classification of IDS based on technique: Various studies have categorized intrusion detection systems for IoT based on their preferences. For example, based on their technique applied for intrusion detection, these systems are classified as follows:

- Signature-based intrusion detection system: In these IDS systems, the attacks are detected when the attack signature matches the internal database signature of any existing attack. When such an attack signature is found, then an alert is signaled. Numerous research has found that these are more accurate and effective [8;17;21]. These are also easy to understand and use. The key challenge in this method is that the database should be updated regularly for enhancing efficiency. [21].
- Anomaly-based intrusion detection system: These IDS are generally used to detect intrusion in the network and monitor the misuse in the network. The system categorizes the activities into normal and abnormal activities based on a threshold value [18]. Such IDs in IoT monitor the behaviour of the node and compute its threshold. It then compares it with the defined threshold for the network, and any deviation from it is considered abnormal, thereby resulting in an anomaly [12;18;24].
- Specification-based intrusion detection system: These IDS are based on rules. The rules define the expected behaviour of the network, the nodes, and the protocols [10;13]. When any node behaviour or communication differs from the specification, a trigger is raised. It differs from the anomaly-based system because the human user makes the rules. These IDs are prone to more false-positive rates due to human-based rules [10;13].
- Hybrid intrusion detection system: These IDS employ the best ways of all three approaches to capture intrusion in a more effective manner.

Classification of IDS based on placement strategy: In another classification of an intrusion detection system, these systems are classified based on the placement of the IDS in the IoT network. These are classified as follows:

- Centralized IDS: In this placement strategy, the IDS is placed in the central most component of the network, like a border router or any specific central host. The total traffic passes through this border router or the central host and can be analysed for any intrusion activities.
- Distributed IDS: This is a placement strategy of IDS wherein the IDS are placed in every network entity. Thus IDS are deployed in each node. The biggest challenge in using these kinds of IDS is that the IoT devices are resource constraints, and thus researchers have proposed lightweight IDS for the distrusted placement strategies.
- Hybrid IDS: In this placement strategy, the entire network is divided into clusters. For each cluster, the main node has the IDS to monitor the neighbouring node traffic [20].

From the existing research work of intrusion detection systems in the IoT environment, the key findings are summarized in Table 1 and Table 2. Table 1 summarizes the IDS methodology and the placement strategy of IDS in the IoT environment.

Table 1: Summary of Methodology and strategy of placement of IDS

Paper	***Methodology***	***Strategy of placement***
Kasinathan et al. (2013)[8]	IDS in IoT are built over IPv6 over a low-power personal area network (6LoWPAN) devices. The proposed IDS framework has a monitoring system and a detection engine integrated into the network framework developed within the EU FP7 project 'ebbits.'	The IDS is placed centrally[8] .
Raza et al. (2013) [20]	Real-time intrusions detection in IoT named SVELTE. [20]	Not Available
Ham et al. (2014) [4]	Made use of linear Support vector machine method for anomaly detection in android machines [4].	Not Available
Lee et al. (2014) [11]	Lightweight intrusion detection model based on energy consumption analysis of nodes consumed in 6LowPAN. The sensor nodes with irregular energy consumptions are identified as malicious attackers[11]	Distributed
Oh et al. (2014) [17]	Makes use of a pattern matching engine that detects the signature of the intrusion and signals an alarm [17].	Distributed

Le., A. et al. (2016) [10]	Routing protocol for low power network protocol based IDS [10]	Hybrid placement
Hodo et al. (2016)[5]	Made use of the artificial neural network, supervised learning for detecting DoS-based attacks [5].	Not Available
Thanigaivelan et al. (2016)[24]	Each node monitors its neighbors at the data link layer. If in any node behvaiour is abnormal, the monitoring neighbor node will block the packets from this abnormally behaving node. It will then report the abnormality to the parent node [24]	Hybrid placement
Li Jet al. (2018) [12]	Makes use of AI for IDS. It is two-stage IDS with Software-Defined Network (SDN) to support[12]	Not Available
Liu, L., et al. (2018) [13]	Made use of principal component analysis algorithm for intrusion detection [13]	Not Available
Sicato, J.C.S et al. (2020)[22]	Software-defined IDS for distributed cloud [22].	Centrally placed

From Table 1 it is evident that the most preferable strategy for placing the intrusion detection system is central. The total traffic passes through the centrally placed IDS and thus the entire system is monitored. The IDS technique, the advantages of each technique, and the challenges are summarized in table 2.

Table 2: Summary of IDS technique, advantages, and Issues in IDS

Paper	***IDS detection technique***	***Advantages***	***Issues***
Kasinathan et al. (2013) [8]	Signature-based detection technique	Easy to use, stable and scalable [8]	Need further refinement for more attacks detection requires an updated database [8].
Raza et al. (2013) [20]	Hybrid IDS technique	Real-time applicability	Low rates of detection [20]
Ham et al. (2014) [4]	Anomaly-based	High precision and low false alarms [4].	Greater overhead time [4].
Lee et al. (2014) [11]	Anomaly-based	Lightweight, effective [11]	Requires high time for computation [11].
Oh et al. (2014) [17]	Signature-based	High accuracy rates and uses less memory [17]	It cannot detect in a real-time scenario and has the lesser capability of intrusion detection [17]
Lee et al. (2016) [10]	Specification-based	More effective	Requires more rules for being effective [10].
Hodo et al. (2016) [5]	Anomaly-based	Good accuracy with low false-positive values, Excellent energy efficiency [5]	Consumes more time for perfect result computation [5]
Thanigaivelan et al. (2016) [24]	Anomaly-based detection [24]	Uses network fingerprinting for network changes [25]topology, Effective.	Requires high computing resources [24].
Li J. et al (2018) [12]	Anomaly-based	Very good accuracy with low false rates [12]	More time consuming & needs more computational resources [12].

Liu, L., et al (2018) [13]	Specification-based	The detection rates are high and the false alarms are low [13]	As the volume of data increases, efficiency decreases [13].
Sicato, J.C.S et al. (2020) [22]	Anomaly-based integrated with machine learning	SDN-based IDS makes use of IDS controller at Fog layer [22].	High risk to IoT application layer security

From Table 2 the key findings are :

- IoT networks are resource constraint devices. Thus, there is a shortage of extensive databases for known attack detection, especially in signature-based detection methods. Thus, signature-based methods are less effective in an IoT-based environment[18].
- Most of the existing IoT-based IDS employ an Anomaly-based intrusion detection technique followed by a hybrid detection technique. It is mainly because the anomaly-based detection technique enables dynamic behavior intrusion detection. It is also capable of detecting unknown threats and vulnerabilities. The key challenge with such intrusion detection techniques is that these have high false-positive rates and require high time for processing and computation.
- Moreover, it has been found that the usage of the traditional Intrusion detection system techniques in the IoT-based network is challenging due to particular characteristics such as device based resource constrain, challenges related to protocol stack and other communication standards

3.3 Challenges in IDS in IoT

From the analysis of the existing literature work, the key challenges of IDS in IoT based environment are as follows:

In general an intrusion detection system working on LAN based network raises several intrusion triggers [19]. Thus there are a large number of false-positive rates and a sometimes large number of low priority alerts. In such a scenario network, the admin cannot compute these alerts manually to find out which false-positive attack is and what mitigation steps are needed. The same problems are a challenge in the IoT environment. This challenge becomes more complex because most IoT devices are used for automation and significantly less human interaction [26]. Therefore there is a need to address this issue in IoT-based IDS systems. Thus, alert processing methods are needed. Furthermore, IoT-based devices cannot be flooded with many alerts and data due to resource constraints. Thus these issues must be addressed.

- IoT-based networks are more used for automation devices and thus have less human intervention. Thus, IDS administration cannot have frequent human intervention in the IoT environment. Therefore there is a need to have an automated IDS mechanism with minimal intervention of humans. Research works are on automated mitigation of threats paradigms for IoT. Such mechanisms are well-needed for IoT-based networks. This is where Artificial intelligence has a promising role to play. Early works on Artificial intelligence-based Intrusion detection systems in general and in IoT by [6;7;22;23;25] show the promising result on artificial intelligence and machine learning as the best technique for enhancing existing intrusion detection system efficiency.
- The needs of IoT are different as they require real-time monitoring of the data, require an automated system to detect anomalies, have different sets of protocols, etc. Thus, Midi et al[14]. proposed Kalis, an intrusion detection system for IoT which was protocol independent. Kalis IDS relies on "network-based, hybrid signature/anomaly-based technology that has placement strategy of hybrid centralized/distributed, and is capable of adapting to different environments." This system can be used as a standalone tool or as an external agent device. It is based on a knowledge-based system and thus automatically detects the data based on the network features. Furthermore, Kalis was able to detect the type of prevention techniques, such as cryptographic functions deployed by the network. Thus, it happened to be an effective and efficient system. The system's detection rate was found to be 91% with 100% accuracy, 0.19% CPU usage, and 13978.62 KB memory consumption. The system promised to be an effective tool for IoT-based intrusion detection [14].
- IoT networks are resource constraint devices. Thus, there is a shortage of extensive databases for known attack detection, especially in signature-based detection methods[23]. Thus, signature-based methods are less effective in an IoT-based environment [23]. This has to be addressed for signature-based IDS in IoT.

- The IoT devices are small, having small resources, and thus, in such a scenario, anomaly-based detection methods are better than the other approaches[21;23]. It is also found that these anomaly-based detection requires more computational needs, efforts, time and this emerges as a key challenge [23].

- The current security mechanism in IoT adapts the virtual local area network paradigm to secure the communication between two nodes and the IDS component [22;23]. Moreover completely securing the data communication lines in IoT network is not possible due to IoT characteristics. Any weak attack can be used to eavesdrop or passively monitor the communication lines and intrude on the network. Thus, there is a need to look at the IoT sensor and node communication[22;23].

- Placement strategies of IDS in IoT are still a challenge and require further research.

4. Recommendation

IoT security requires two main aspects: the security architecture aspect and the security by design aspect. To achieve these aspects, the systems must have the following things:

- To have an automatic detection mechanism to enhance the incident response during any attack. Artificial Intelligence is a powerful tool that can make use of its learning algorithms to help in achieving automation.

- The automation algorithms should be self-learning and adaptable. This can be achieved with the help of artificial intelligence, and some of its adaptive self-learning algorithms are machine learning by neural networks, artificial immune systems, etc.

- There is a need to have faster and enhanced decision-making abilities. Moreover, to effectively mitigate the intrusion, there is a need to understand the attacker's behavior and the data behavior. These understandings can be done through the use of computational intelligence systems. Thus, it can be concluded that an effective automated intrusion detection system can be made with the help of artificial intelligence tools.

5. Conclusion

This review is a summary of the methods used for designing the intrusion detection system for the IoT. Preliminary findings from the literature review revealed that an intrusion detection system is highly essential for IoT devices to ensure safe and secure communication. Widely used IDS for IoT rely most on anomaly-based detection methods due to its effectiveness. Moreover, the anomaly-based detection method is efficient due to IoT devices being small, with limited resources. It is found that anomaly-based intrusion detection technique requires more computational technology and this emerges as the key challenge in its usage. To overcome this challenge automated IDS is the need of the hour. This, in turn, looks towards Artificial Intelligence as the game-changer. Artificial intelligence could be a powerful tool in designing an efficient intrusion detection system for IoT-based systems. Finally, the literature on the placement strategy of IDS in IoT and its effectiveness is limited. Henceforth, there is a need to address the placement strategy for IDS in the IoT environment for more reliable and secure IDS in near future.

References

[1] Benkhelifa, E., Welsh, T. and Hamouda, W.: A critical review of practices and challenges in intrusion detection systems for IoT: Toward universal and resilient systems. IEEE communications surveys & tutorials, 20(4), pp.3496-3509 (2018).

[2] Borgohain, T., Kumar, U., Sanyal, S.: *Survey of security and privacy issues of internet of things*. arXiv preprint arXiv:1501.02211(2015).

[3] Hameed, S., Khan, F. I., and Hameed, B.:*Understanding security requirements and challenges in the Internet of Things (IoT): a review*. Journal of Computer Networks and Communications, (2019).

[4] Ham, H.S., Kim, H.H., Kim, M.S., Choi, M.J.: *Linear SVM-based android malware detection for reliable IoT services*, Journal of Appl. Math. 2014, pp 1–10 (2014).

[5] Hodo, E., Bellekens, X., Hamilton, A., Dubouilh, P. L., Iorkyase, E., Tachtatzis, C., & Atkinson, R.: *Threat analysis of IoT networks using artificial neural network intrusion detection system*. In 2016 International Symposium on Networks, Computers and Communications (ISNCC) (pp. 1-6). IEEE, May 2016.

[6] Hosseinpour, F., Amoli, P. V., Farahnakian, F., Plosila, J., &Hämäläinen, T.: *Artificial immune system based intrusion detection: Innate immunity using an unsupervised learning approach*. International Journal of Digital Content Technology and its Applications, 8(5), pp.1(2014).

[7] Javaid, A., Niyaz, Q., Sun, W., & Alam, M.: *A deep learning approach for network intrusion detection system*. In Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies (formerly BIONETICS), pp. 21-26(2016).

[8] Kasinathan, P., Costamagna, G., Khaleel, H., Pastrone, C., Spirito, M.A.: *DEMO: an IDS framework for the internet of things empowered by 6LoWPAN*. In: Proceedings of the 2013 ACM

SIGSAC Conference on Computer & Communications Security, CCS '13, ACM, New York, NY, USA, pp. 1337–1340(2013b).

[9] Kumar, S., Dutta, K.: *Intrusion detection in mobile ad hoc networks: techniques, systems, and future challenges*. Secure. Commun. Netw. 9 (14), pp. 2484–2556 (2016).

[10] Lee, J. Loo, K.K. Chai, M., Aiash, A.*: Specification-Based IDS for Detecting Attacks on RPL-Based Network Topology*, Information, vol- 7 (2),pp25 (2016).

[11] Lee, T.H., Wen, C.H., Chang, L.H., Chiang, H.S., Hsieh, M.C.: *A lightweight intrusion detection scheme based on energy consumption analysis in 6LowPAN.* In: Huang, Y.-M., Chao, H.-C., Deng, D.-J., Park, JJJH (Eds.), Advanced Technologies, Embedded, and Multimedia for Human-centric Computing, Lecture Notes in Electrical Engineering 260. Springer, Netherlands, pp.1205–1213(2014).

[12] Li, J., Zhao, Z., Li, R., Zhang, H., Zhang, T.: *AI-based two-stage intrusion detection for software-defined IoT networks.* IEEE Int. Things J. (2018).

[13] Liu, L., Xu, B., Zhang, X., Wu, X.: *An intrusion detection method for the internet of things based on suppressed fuzzy clustering*. EURASIP J. Wirel. Commun. Netw. (1) (2018) 113 2018.

[14] Midi, D., Rullo, A., Mudgerikar, A., &Bertino, E.:*Kalis—A system for knowledge-driven adaptable intrusion detection for the Internet of Things.* In 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS), pp. 656-666 (2017).

[15] Nawir, M., Amir,A., Yaakob, N., and. Lynn, O. B.: *Internet of Things (IoT): taxonomy of security attacks*. In Proceedings of 2016 3rd International Conference on Electronic Design (ICED), Phuket, Thailand, 2016, pp.321-326 (2016).

[16] Nobakht, M., Sivaraman, V., and Boreli, R.: *A Host-Based Intrusion Detection and Mitigation Framework for Smart Home IoT Using OpenFlow*. In 2016 11th International Conference on Availability, Reliability, and Security (ARES), pp. 147–156 (2016).

[17] Oh, D., Kim, D., Ro, W., W: *A malicious pattern detection engine for embedded security systems in the Internet of Things*. Sensors 14 (12), pp.24188–24211(2014).

[18] Pajouh, H. H., Javidan, R., Khayami, R., Ali, D., and Choo, K. K. R.:*A Two-layer Dimension Reduction and Two-tier Classification Model for Anomaly-Based Intrusion Detection in IoT Backbone Network.* IEEE Transactions on Emerging Topics in Computing, vol. PP, no. 99, pp. 1–1, (2016).

[19] Pongle, P., Chavan, G.: *Real-time intrusion and wormhole attack detection in the Internet of Things*. Int. J. Comput. Appl., Vol.121 (9), pp.1–9 (2015).

[20] Raza, S., Wallgren, L., Voigt, T.: *SVELTE: real-time intrusion detection in the Internet of Things*. Ad Hoc Network. 11 (8), pp.2661–2674 (2013).

[21] Sicato, J.C.S., Singh, S.K., Rathore, S. and Park, J.H.: *A comprehensive analyses of intrusion detection system for IoT environment*. Journal of Information Processing Systems, 16(4), pp.975-990 (2020).

[22] Song, M., Zhong, K., Zhang, J., Hu, Y., Liu, D., Zhang, W., & Li, T.: *In-situ ai: Towards autonomous and incremental deep learning for IoT systems*. In 2018 IEEE International Symposium on High-Performance Computer Architecture (HPCA), IEEE, pp. 92-103(2018).

[23] Summerville, D.H., Zach, K.M., Chen, Y.*: Ultra-lightweight deep packet anomaly detection for Internet of Things devices*. In: 2015 IEEE Proceedings of the 34th International Performance Computing and Communications Conference (IPCCC), IEEE, pp. 1–8(2015).

[24] Thanigaivelan, N.K., Nigussie, E., Kanth, R.K., Virtanen, S., Isoaho, J.:*Distributed internal anomaly detection system for Internet-of-Things*. In: 2016 Proceedings of the 13th IEEE Annual Consumer Communications Networking Conference (CCNC), pp. 319–320 (2016).

[25] Xiao, L., Wan, X., Lu, X., Zhang, Y. and Wu, D.: *IoT security techniques based on machine learning: How do IoT devices use AI to enhance security?*. IEEE Signal Processing Magazine, 35(5), pp.41-49(2018).

[26] Zarpelão, B. B., Miani, R. S., Kawakani, C. T., & de Alvarenga, S. C.: *A survey of intrusion detection in Internet of Things*. Journal of Network and Computer Applications, 84, pp. 25-37 (2017).

Syed Ali Mehdi received a Bachelor of Technology in Computer Science and Engineering degree from UP Technical University, Lucknow in 2012 and a Master of Technology in Computer Science and Engineering degree from Amity University Noida in 2015. He is currently pursuing a doctorate in Computer Science from Jamia Millia Islamia, New Delhi. He is also working as Assistant Professor at Jamia Hamdard, New Delhi. His research interest includes Artificial intelligence, Machine Learning, Digital Image processing, Computer Security and Algorithms.

Dr. Syed Zeeshan Hussain received B.Sc (Hons) and M.Sc in physics from Bhagalpur University, Bihar. He also received an MCA degree from IGNOU, New Delhi, and Doctorate in Computer Science from Jamia Millia Islamia, New Delhi. He is currently working as Associate Professor at Jamia Millia Islamia, New Delhi. His research interest includes Computer Networks, Network Security, Web Technology, and Applications.