

# A review of intrusion detection system and security threat in internet of things enabled environment

Nisha, Nasib Singh Gill, Preeti Gulia

Department of Computer Science and Applications, Maharshi Dayanand University, Rohtak, India

## Article Info

### Article history:

Received Oct 22, 2023

Revised Feb 20, 2024

Accepted Mar 20, 2024

### Keywords:

Anomaly detection

Internet of things

Intrusion detection system

Machine learning

Security threats

## ABSTRACT

Thousands of devices communicate globally to share data and information without any human intervention. A network of physical objects with numerous sensors and other network hardware to exchange data with servers and additional devices that are linked is referred to as the "internet of things (IoT)". The actions hurting the communication system are known as intrusions. Security features such as (integrity, and confidentiality) within IoT networks are compromised when any kind of intrusion occurs. To identify multiple infiltration types in an environment where IoT is enabled, an intrusion detection system (IDS) is required. In environments where IoT is enabled, security vulnerabilities are now more prevalent than ever. In this study, the IoT architecture is reviewed, and potential security risks at each tier are investigated. It is also hoped that this research will stimulate thought about the expanding risks posed by unprotected IoT devices. The paper also intends to provide an in-depth analysis of intrusion detection systems for identifying and classifying security threats in an IoT-enabled environment. Furthermore, this study investigates a variety of efficient machine learning-based methods for detecting cyberattacks on IoT devices.

*This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.*



## Corresponding Author:

Nisha

Department of Computer Science and Applications, Maharshi Dayanand University

Rohtak, Haryana, India

Email: nisha.rs.dcsa@mdurohtak.ac.in

## 1. INTRODUCTION

Because of the abundance of services available on the internet, the term internet and its related aspects play an important role in the field of research. The term IoT refers to the internet of things, which is a novel invention that allows many electrical devices connected to the internet to share information without the need for human intervention. The IoT is a rapidly expanding field of computer science that is expected to have 50 billion linked devices by the end of 2020 [1]. The rapid growth of the IoT industry is the foundation for this forecast. These connected devices produce a huge amount of data traffic, which feeds big data analytics, which is also used to discover previously unseen patterns and anomalies in network traffic. These connected computers can be controlled remotely from anywhere, which may cause different kinds of security threats. In addition, because IoT gadgets are often left unattended, bad actors can obtain access to them to harm [2]. Nowadays, IoT applications are used in many sectors like education, healthcare, agriculture, transportation, banks, and offices. But, network security has become a critical issue in IoT-enabled environments. Different kinds of intrusions may cause danger to IoT security. Any unwanted actions to the system that may be hurting IoT security are known as intrusions. An intrusion detection system (IDS) is used to handle security threats at all layers of IoT architecture. Security features (integrity, and confidentiality) of IoT networks are compromised when an intrusion occurs. IDSs have become a climacteric zone of security in IoT. Usually, an

intruder may be any human being or any software who tries to perform any illegal action on the network. The system, which is used to detect intrusions on the network is known as IDS. Ayyagari *et al.* [3] presented a thorough analysis of the literature on different intrusion detection methods designed for IoT-enabled environments. The authors presented many benefits and drawbacks of different kinds of IDS techniques. They also addressed various threats at each layer of IoT architecture. This paper mentions several IoT datasets, including NSL-KDD, KDD Cup 99, and others. This paper not only presents the comparison of existing IDS methods but also presents the latest contributions of IDSs in network security. The primary goal of this paper is to pique researchers' interest in further study opportunities [3]. Any electrical software component that detects malicious network activity is considered an IDS. It can identify simple as well as complex attacks at the initial stage of data transmission. The IDS also keeps the information of previously detected attacks for future reference. Keserwani *et al.* [4] proposed a model named grey wolf optimization-particle swarm optimization-random forest GWO-PSO-RF to attain more accurate results for detecting intrusions in IoT environments. RF classifier is implemented in Python programming language to achieve a high attack detection rate. This model achieved an average of 99.66% accuracy for different datasets like KDDCup 99 and CICIDS-2017. In the future, the proposed model can be implemented for intrusion detection in a real-time IoT environment. According to the most recent IDC report, approximately 41.6 billion connected IoT devices are expected to generate 79.4 zettabytes of data by the year 2025. Kalnoor and Gowrishankar [5] provide an overview of intrusions in the IoT environment; the authors also developed a smart IDS that employs machine learning (ML) techniques to find breaches in the IoT network. The work provides a high level of security to IoT-enabled environments by using a probabilistic Markov model and by implementing various ML approaches. With a high precision value, this model produced results with a 100% intrusion detection accuracy and a 19% false positive rate. Singh and Khare [6] conducted a survey and described freely released intrusion data sources such as the KDD Cup '99, and the data security laboratory-KDD (dataset).

**2. IOT AND ITS ARCHITECTURE**

The term IoT, first used in 1999, refers to the next generation of the internet [7]. IoT is now used in many real-world applications such as home automation, automated traffic control, smart cities, intelligent healthcare systems, intelligent farming, and so on. IoT brings out a broader change in information technology, the corporate sector, the healthcare system, energy stocks, and our daily activities. A wide range of application areas are covered by IoT but on the other hand, it also increases security vulnerabilities. Therefore, the solution to each security problem should be made. Because IoT devices are heterogeneous and have high processing power, they make an easy target for attackers. Various attacks like sinkhole attacks, eves-dropping, and denial of service attacks have become motivating factors for implementing security in IoT networks [8]. IoT enables the interconnection of different kinds of objects to communicate with one another without the need for human intervention. IoT networks have become an easy target for intruders with the increasing number of connected heterogeneous devices. As a result, a flexible layered architecture is required. The primary goal of Internet of Things architecture is data collection and processing via various sensors and devices. After that processed data is transferred to the application by using Bluetooth, and Zigbee. Intrusions of various types can occur in different layers of IoT architecture, but the network layer is the most susceptible [9]. The three-layered architecture is the basic IoT model, which incorporates application, network, and perception layers as shown in Figure 1.

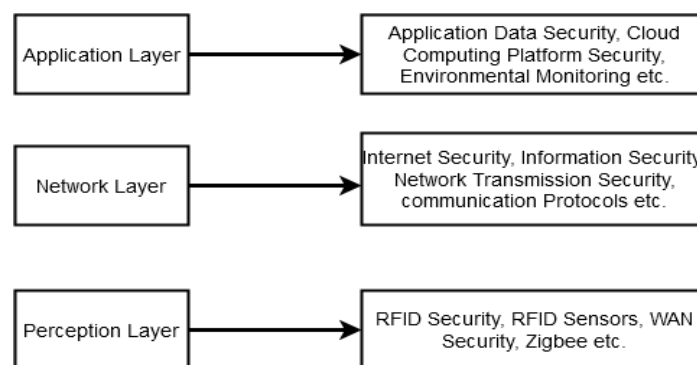


Figure 1. Layered IoT architecture

IoT indeed makes many applications possible to create a smart world for people but on the other hand, various risk factors are also increasing day by day. High-security risks in IoT systems are due to less defined parameters and the highly dynamic and heterogeneous nature of IoT devices. Many kinds of attacks take place in an IoT environment. These are mainly classified as internal and external attacks. In an external attack, an intruder is not a part of the network, whereas attacks within the network are initiated by harmed nodes that are part of the network [10]. Confidential information may be leaked at any time if security issues are not addressed properly. Thus, security issues must address privacy, integrity, accessibility, authenticity, and non-repudiation, among others. The main components of an IoT-enabled environment are sensors, actuators, and network connectivity. IoT environment needs to fulfill the countermeasures as given in Figure 2, to improve its security system [11].

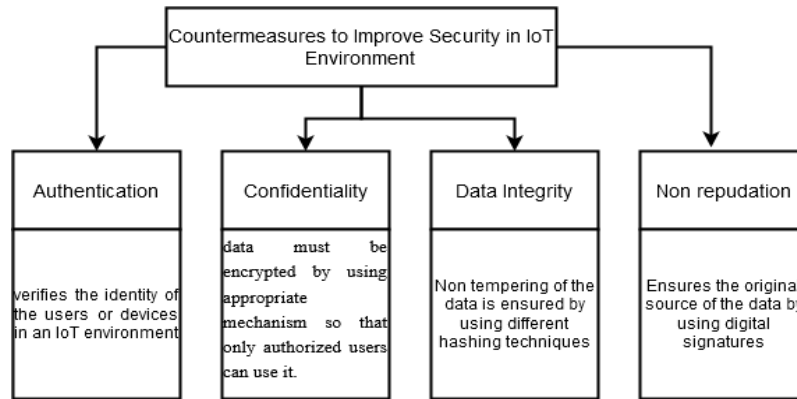


Figure 2. Security measures in the IoT environment

### 3. INTRUSION DETECTION SYSTEM

Any kind of hardware or software component is known as an IDS, which is used to monitor network connections along with system activities and creates prompts when anything departs from appropriate activity [12]. With IDS models, many issues such as high network transmission load, low detection performance, and poor data processing capability may exist. Conventional methods of intrusion detection systems are failing to secure the IoT environment because types of network attacks are changing and increasing day by day. An intrusion detection system is needed, which is self-healing and self-correcting in nature. There are three main stages to IDS operations. The initial stage helps to keep track of system and network actions [13]. Stage two is assessment, which is based on the extraction of features and pattern identification techniques. Finally, all kinds of intrusions are detected in the last stage. All IDS operations are shown in Figure 3.

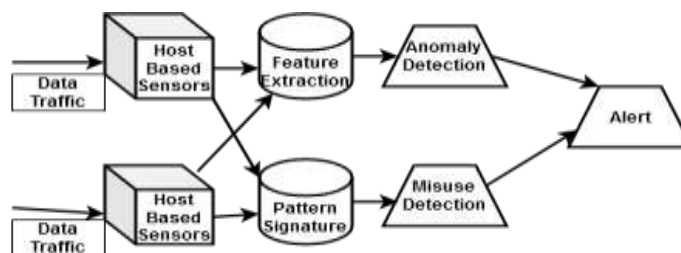


Figure 3. Operations of intrusion detection system [14]

IDS monitors system behavior and recognizes threats by analyzing traffic data using host-based sensors using some ML techniques. Sensors continuously monitor all kinds of happenings like temperature, noise, weather, and humidity, in the IoT environment and an alert is generated if any threat is detected. Four approaches of IDS are used to detect attacks in the IoT environment are shown using Figure 4.

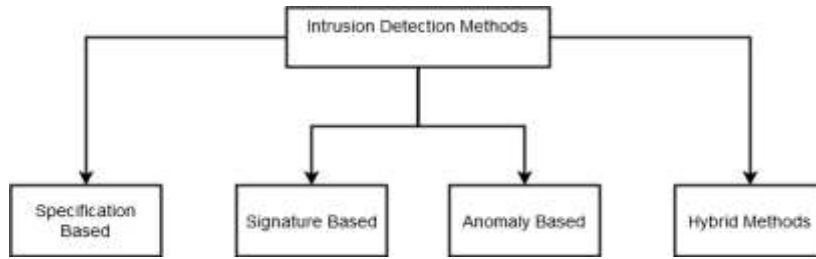


Figure 4. Types of intrusion detection system

There are two categories of intrusion detection systems: one for detecting network intrusions (NIDS), which monitors the network for policy violations and illegal activities, and the other category is to detect host intrusions (HIDS).

- Anomaly-based detection system: it detects both network and computer intrusions and generates an alert when anything deviates from its normal behavior. This is the best method to detect unknown attacks but sometimes it generates false alarms.
- Signature-based detection system: it monitors the behavior of known attacks finds out the patterns and generates an alarm if any match is found.
- Specification-based detection system: it is used to detect and verify only specific types of vulnerabilities in the network.
- Hybrid-based detection system: it combines the best results from all other IDS.

Table 1 shows the advantages and limitations of signature based intrusion detection system (SIDS) and anomaly based intrusion detection system (AIDS) methods.

Table 1. Methods for detecting intrusion: a comparison [15]

Detection methods	Advantages	Limitations
SIDS	Effective in detecting intruders while generating a few false positives (FA). Finds the security breaks right away. Exceptional at seeing the typical threats. Easy design.	A new signature is required regularly. SIDS is built to identify attacks with specific signatures. A system's inability to detect a variant of a previously identified intrusion occurs when the intrusion is modified in any way. Failed to identify the zero-day vulnerability. Incapable of spotting attacks that involve multiple phases. The attacks' subtlety was not fully grasped.
AIDS	It might help identify novel attacks. Potentially useful for generating an attack fingerprint.	Since AIDS is incapable of decrypting packets, an attack can go unnoticed and continue to pose a risk. There are lots of unneeded alarms. A highly adaptable computer system makes it challenging to construct a typical user profile. Warnings that aren't secret. It requires introductory instruction.

#### 4. STUDY OF EXISTING LITERATURE

This section deals with the review of existing work related to the identification of security threats in IoT-enabled environments. This section also presents widely used datasets and methodologies adopted related to security issues in IoT. The whole process of compilation of the works considered in this survey is called “systematic literature review” (SLR).

Saravanan *et al.* [16] investigate conventional ML techniques and NIDS, as well as future directions. ML algorithms are both secure and efficient for IoT network intrusion detection systems. A model uses classifier algorithms like Nave Bayes (NB), support vector machines (SVM), and decision trees (DT) for training. In addition to other renowned research about popular frames, a systematic investigation of NIDSs is utilized for many different aspects of learning perspectives of IoT. The examination started by identifying IoT threats and issues and then it initiated its IoT NIDS and over time developed cutting-edge, knowledgeable methodologies that help with IoT vulnerabilities. Kumar *et al.* [17] presented a unified intrusion detection system (UIDS) to ensure data security from the latest attacks like denial-of-services (DoS), generic, and probe attacks. In the UIDS model, the UNSW-NB15 dataset is analyzed to detect harmful threats in the network. This model improves the network's attack detection rate when compared to existing models ENADS and Dendron, which also take into account conventional data sets UNSWNB15. K-means clustering recognizes similarities in various types of data by discarding labels from the dataset. Kiran *et al.* [18] developed a system to identify data intrusions using ML approaches. The dataset must contain both normal and attack instances for this model

to work. To analyze traffic data patterns in IoT, there are many publicly accessible datasets. A testing platform using a DHT11 sensor, wireless router, and Node MCU ESP8266 is implemented to visualize the IoT infrastructure. The laptop is then used to create adversarial mechanisms that result in network attacks. In the final stage, ML systems are required to track and characterize network threats, and classifier performance is measured using performance metrics. Qureshi *et al.* [19] used random neural networks to build an innovative heuristic IDS for IoT environments (RNN-IDS). The effects of RNN-IDS were evaluated using NSL-KDD datasets which is a more complex version of the KDD-CUP'99 dataset. The effectiveness of RNN-IDS was examined against that of SVM, NB, RF, multi-layer perception, and other ML techniques. Because KDDTrain20 has a large number of anomalous records, it is used in this study to train the classifier.

The overall productivity of RNN-IDS is calculated using various performance matrices (precision value, accuracy, and false alarm rate). With a precision rate of 99.02%, RNN-IDS increased the accuracy of identifying novel attacks from 85.5% to 95.25%. A network of interconnected objects that can manage their cloud platforms is named IoT, according to research by Zhou *et al.* [20]. These devices produce a staggering amount of data. Over the years, a variety of attacks have been used by hackers to compromise devices that perform poorly. DoS attacks are the most frequent type of attack on an IoT network. Because it requires so little knowledge and software resources compared to other attacks, DoS accessibility is a serious security concern. The main aim of DoS attacks is to deny access to intended users. A lightweight intrusion detection system was developed by Fananir *et al.* [21] to enhance IoT security. The feature selection and feature classification ML techniques are the foundation of these IDS. The feature selection method is used because it has a low computational cost. The best classification technique was found when comparing NB, RF, logistic regression (LR), and SVM, among other methods. This is implemented using the Scikit-Learn Tool. The impact of feature selection techniques on various classification techniques is compared using three datasets (KDD99, UNSW-NB15, and NSL-KDD). To present IoT security concerns and identify unusual behavior of IoT devices on the network, Mridha *et al.* [22] develop a novel methodology. This process operates in two phases. In the first stage, the network administrator sets up and keeps up a rule-based methodology that uses ML approaches to learn the proper behavior of an IoT network. Supervised ML techniques are used to train the machine and to successfully detect irregularities in the network activities. Classification experiments are done using the ML tool Weka. The proposed method gives the best results in identifying scanning attacks. This paper's approach is an attempt to make a significant contribution to the field of the IoT for a brighter tomorrow.

Table 2. Comparative analysis of review work

References	Techniques	Datasets	Accuracy
Azizjon <i>et al.</i> [23]	system for detecting malware using deep neural systems	Mailing dataset	This technique produces a cutting-edge with 98.93% accuracy, but it hasn't yet been tested on an APT dataset
Huang and Zhu [24]	A multi-layered, game-theoretic paradigm for developing proactive cyber barriers by autonomous devices.		When compared to a rudimentary defense mechanism, the method's payout is 56% larger.
Ghafir <i>et al.</i> [25]	Method for autonomously detecting APTs in a broad setting.	Customized machine learning dataset	An accuracy rate of 84.8% is obtained.
Yu <i>et al.</i> [26]	BERT is a technique used by the APT detection system to automatically recognize APT assault sequences.	Los Almos Laboratory APT dataset.	This scheme has a 99% accuracy rate.
Siniosoglou <i>et al.</i> [27]	MENSA stands out from the competition due to its (anomaly detection and classification), cutting-edge Auto-encoder-generative adversarial network (GAN) architecture.	There is also real-time series data from power meters, data from Modbus/TCP networks, and data from DNP3 networks.	TPR and FPR of 0.947%, 0.812 and 0.036 respectively.
Kumar and Thing [28]	To track the development of an APT campaign and take appropriate countermeasures, a compact and comprehensive APT campaign graph is constructed using the interconnected phases of the attack.	For this method, we artificially add an APT campaign to the CSE-IDC2018 intrusion detection dataset.	Precision accuracy rate 0.993%. is achieved.

## 5. COMPARATIVE ANALYSIS OF RELATED REVIEW

In this section, we present a comparative analysis of a review of works related to identifying security threats in IoT-enabled environments. A comparison of widely used datasets and methodology adopted along with accuracy in papers related to security issues in IoT are presented in Table 2. The capacity of intrusion detection systems to derive features from each packet's context and intent is crucial to their success. Among the billions of packets transferred every day, the majority are harmless connections seeking to reach a server,

while a small percentage are malicious and designed to start assaults [29]. These attributes can be difficult to extract from IoT network traffic because of the overlap of packets from different subnet networks, the possibility of several network connections at once, and the high speed of the connection [30]. A fully connected feed-forward network is the most typical kind of neural network used for easy tasks. The capability of each neuron in one layer to communicate with a neuron in the upper layer is a requirement for full connectivity. Communication between neurons in the same layer is limited by feed-forward networks. Feature extraction is performed using fast convolutional neural networks (FCNNs) [31]. Because it is built of convolutional layers first, followed by fully connected layers, convolutional neural networks (CNNs) are multilayer neural networks [32]. Among these layers, the input and output layers make up a CNN. In most cases, the hidden layers in CNNs are convolutional layers, which multiply inputs collectively. Because they utilize spatial data, CNNs outperform earlier generations of neural networks [33]. Most IDS today make use of spatial characteristics as their primary traffic feature. Network traffic is converted into traffic images using geographic features, and then categorized using an image classification technique, allowing for the successful detection of intrusion traffic. While this method is relatively new, it has shown remarkable promise in multiple recent studies. For instance, Vasan *et al.* [34] CNNs algorithms were used to modify CNN architecture to transform the original malware binary into gray-scale and color images.

It is critical to assess machine learning strategies using relevant datasets because they are widely used in the fight against various kinds of threats. Table 3 demonstrates the IDS's tabulated properties. Our research indicates that numerous protocols and conventional data sets, such as KDD'99, were created to assist in the design of efficient IDS for the IoT.

Table 3. Evaluating the study's findings in light of developing IoT-based (IDS systems)

Survey Reference	Architecture	Protocols	Threats	IoT IDS aspects			Datasets
				IDS design choices	IDS-ML techniques	IDS-DL techniques	
[35]	✓	✓	✓	✓	×	×	×
[36]	×	×	✓	×	✓	×	×
[37]	×	×	✓	×	✓	✓	✓
[38]	✓	×	×	✓	✓	✓	✓
[39]	×	×	✓	✓	×	×	×
[40]	✓	✓	✓	✓	✓	✓	✓

## 6. CONCLUSION

This paper presents a systematic literature review on intrusion detection systems in IoT-enabled environments. The study incorporates a comprehensive investigation of different kinds of IoT attacks and their solutions. A taxonomy and table detailing detection tactics, NIDS deployment options, security threats, and validation procedures were supplied. A variety of dataset sources of IoT networks are detailed in this paper. The paper also presents different techniques, which may be applied for achieving security in IoT-enabled environments and specifically for intrusion detection. All conceivable challenges concerned with intrusion detection systems have been discussed, which will be of great significance and helpful for further research work to determine specific objectives in the related field and their achievement.

## REFERENCES





- [1] J. Teichmann, K. Heineke, T. Reinbacher, and D. Wee, "The internet of things: how to capture the value of IoT," Technical Report, Technical Report, 2018.
- [2] N. Moustafa, K.-K. R. Choo, I. Radwan, and S. Camtepe, "Outlier dirichlet mixture mechanism: adversarial statistical learning for anomaly detection in the fog," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 8, pp. 1975–1987, Aug. 2019, doi: 10.1109/TIFS.2018.2890808.
- [3] M. R. Ayyagari, N. Kesswani, M. Kumar, and K. Kumar, "Intrusion detection techniques in network environment: a systematic review," *Wireless Networks*, vol. 27, no. 2, pp. 1269–1285, Feb. 2021, doi: 10.1007/s11276-020-02529-3.
- [4] P. K. Keserwani, M. C. Govil, E. S. Pilli, and P. Govil, "A smart anomaly-based intrusion detection system for the internet of things (IoT) network using GWO-PSO-RF model," *Journal of Reliable Intelligent Environments*, vol. 7, no. 1, pp. 3–21, Mar. 2021, doi: 10.1007/s40860-020-00126-x.
- [5] G. Kalnoor and S. Gowrishankar, "IoT-based smart environment using intelligent intrusion detection system," *Soft Computing*, vol. 25, no. 17, pp. 11573–11588, Sep. 2021, doi: 10.1007/s00500-021-06028-1.
- [6] G. Singh and N. Khare, "A survey of intrusion detection from the perspective of intrusion datasets and machine learning techniques," *International Journal of Computers and Applications*, vol. 44, no. 7, pp. 659–669, Jul. 2022, doi: 10.1080/1206212X.2021.1885150.
- [7] P. Maniriho, E. Niyigaba, Z. Bizimana, V. Twiringiyimana, L. J. Mahoro, and T. Ahmad, "Anomaly-based intrusion detection approach for IoT networks using machine learning," in *2020 International Conference on Computer Engineering, Network, and Intelligent Multimedia (CENIM)*, Nov. 2020, pp. 303–308. doi: 10.1109/CENIM51130.2020.9297958.

- [8] J. C. S. Sicato, S. K. Singh, S. Rathore, and J. H. Park, "A comprehensive analyses of intrusion detection system for IoT environment," *Journal of Information Processing Systems*, vol. 16, no. 4, pp. 975–990, 2020.
- [9] D. Rani and N. C. Kaushal, "Supervised machine learning based network intrusion detection system for the internet of things," in *2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, Jul. 2020, pp. 1–7. doi: 10.1109/ICCCNT49239.2020.9225340.
- [10] N. F. Syed, Z. Baig, A. Ibrahim, and C. Valli, "Denial of service attack detection through machine learning for the IoT," *Journal of Information and Telecommunication*, vol. 4, no. 4, pp. 482–503, Oct. 2020, doi: 10.1080/24751839.2020.1767484.
- [11] N. N. Thilakarathne, "Security and privacy issues in IoT environment," *International Journal of Engineering and Management Research*, vol. 10, no. 01, pp. 26–29, Feb. 2020, doi: 10.31033/ijemr.10.1.5.
- [12] Khraisat, Gondal, Vamplew, Kamruzzaman, and Alazab, "A novel ensemble of hybrid intrusion detection system for detecting internet of things attacks," *Electronics*, vol. 8, no. 11, Oct. 2019, doi: 10.3390/electronics8111210.
- [13] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki, "A novel ensemble of hybrid intrusion detection system for detecting internet of things attacks," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2671–2701, 2019, doi: 10.1109/COMST.2019.2896380.
- [14] M. F. Elrawy, A. I. Awad, and H. F. A. Hamed, "Intrusion detection systems for IoT-based smart environments: a survey," *Journal of Cloud Computing*, vol. 7, no. 1, Dec. 2018, doi: 10.1186/s13677-018-0123-6.
- [15] A. Khraisat, I. Gondal, and P. Vamplew, "An anomaly intrusion detection system using C5 decision tree classifier," in *PAKDD 2018: Trends and Applications in Knowledge Discovery and Data Mining*, 2018, pp. 149–155. doi: 10.1007/978-3-030-04503-6\_14.
- [16] L. Saravanan, H. Sharma, K. Sreenivasulu, and M. Deivakani, "WITHDRAWN: detection of software intrusion based on machine learning techniques for IoT systems," *Materials Today: Proceedings*, Apr. 2021, doi: 10.1016/j.matpr.2021.03.138.
- [17] V. Kumar, A. K. Das, and D. Sinha, "UIDS: a unified intrusion detection system for IoT environment," *Evolutionary Intelligence*, vol. 14, no. 1, pp. 47–59, Mar. 2021, doi: 10.1007/s12065-019-00291-w.
- [18] K. V. N. L. S. Kiran, R. N. K. Devisetty, N. P. Kalyan, K. Mukundini, and R. Karthi, "Building an intrusion detection system for IoT environment using machine learning techniques," *Procedia Computer Science*, vol. 171, pp. 2372–2379, 2020, doi: 10.1016/j.procs.2020.04.257.
- [19] A.-H. Qureshi, H. Larijani, J. Ahmad, and N. Mtetwa, "A heuristic intrusion detection system for internet-of-things (IoT)," in *CompCom 2019: Intelligent Computing*, 2019, pp. 86–98. doi: 10.1007/978-3-030-22871-2\_7.
- [20] W. Zhou, Y. Jia, A. Peng, Y. Zhang, and P. Liu, "he effect of IoT new features on security and privacy: new threats, existing solutions, and challenges yet to be solved," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1606–1616, Apr. 2019, doi: 10.1109/JIOT.2018.2847733.
- [21] S. Fenanir, F. Semchedine, and A. Baadache, "A machine learning-based lightweight intrusion detection system for the internet of things," *Revue d'Intelligence Artificielle*, vol. 33, no. 3, pp. 203–211, Oct. 2019, doi: 10.18280/ria.330306.
- [22] M. F. Mridha, M. A. Hamid, and M. Asaduzzaman, "Issues of internet of things (IoT) and an intrusion detection system for IoT using machine learning paradigm," in *Proceedings of International Joint Conference on Computational Intelligence*, 2020, pp. 395–406. doi: 10.1007/978-981-13-7564-4\_34.
- [23] M. Azizjon, A. Jumabek, and W. Kim, "1D CNN based network intrusion detection with normalization on imbalanced data," in *2020 International Conference on Artificial Intelligence in Information and Communication (ICAIIIC)*, Feb. 2020, pp. 218–224. doi: 10.1109/ICAIIIC48513.2020.9064976.
- [24] L. Huang and Q. Zhu, "A dynamic games approach to proactive defense strategies against advanced persistent threats in cyber-physical systems," *Computers & Security*, vol. 89, p. 01660, Feb. 2020, doi: 10.1016/j.cose.2019.101660.
- [25] I. Ghafir *et al.*, "Detection of advanced persistent threat using machine-learning correlation analysis," *Future Generation Computer Systems*, vol. 89, pp. 349–359, Dec. 2018, doi: 10.1016/j.future.2018.06.055.
- [26] K. Yu *et al.*, "Securing critical infrastructures: deep-learning-based threat detection in IIoT," *IEEE Communications Magazine*, vol. 59, no. 10, pp. 76–82, Oct. 2021, doi: 10.1109/MCOM.101.2001126.
- [27] I. Sinioglou, P. Radoglou-Grammatikis, G. Efsthopoulos, P. Fouliras, and P. Sarigiannidis, "A unified deep learning anomaly detection and classification approach for smart grid environments," *IEEE Transactions on Network and Service Management*, vol. 18, no. 2, pp. 1137–1151, Jun. 2021, doi: 10.1109/TNSM.2021.3078381.
- [28] A. Kumar and V. L. L. Thing, "RAPTOR: advanced persistent threat detection in industrial IoT via attack stage correlation," *Preprint arXiv.2301.11524*, Jan. 2023.
- [29] Y. Mirsky, T. Doitshman, Y. Elovici, and A. Shabtai, "Kitsune: an ensemble of autoencoders for online network intrusion detection," *Prepr. arXiv.1802.09089*, Feb. 2018, [Online]. Available: <http://arxiv.org/abs/1802.09089>
- [30] S. P. R.M. *et al.*, "An effective feature engineering for DNN using hybrid PCA-GWO for intrusion detection in IoMT architecture," *Computer Communications*, vol. 160, pp. 139–149, Jul. 2020, doi: 10.1016/j.comcom.2020.05.048.
- [31] X. Wang, Y. Han, V. C. M. Leung, D. Niyato, X. Yan, and X. Chen, "Convergence of edge computing and deep learning: a comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 869–904, 2020, doi: 10.1109/COMST.2020.2970550.
- [32] D. Vasam, M. Alazab, S. Venkatraman, J. Akram, and Z. Qin, "MICHAEL: cross-architecture IoT malware detection based on neural network advanced ensemble learning," *IEEE Transactions on Computers*, vol. 69, no. 11, pp. 1654–1667, Nov. 2020, doi: 10.1109/TC.2020.3015584.
- [33] D. Vasam, M. Alazab, S. Wassan, B. Safaei, and Q. Zheng, "Image-based malware classification using ensemble of CNN architectures (IMCEC)," *Computers & Security*, vol. 92, May 2020, doi: 10.1016/j.cose.2020.101748.
- [34] D. Vasam, M. Alazab, S. Wassan, H. Naem, B. Safaei, and Q. Zheng, "IMCFN: image-based malware classification using fine-tuned convolutional neural network architecture," *Computer Networks*, vol. 171, Apr. 2020, doi: 10.1016/j.comnet.2020.107138.
- [35] E. Benkhefifa, T. Welsh, and W. Hamouda, "A critical review of practices and challenges in intrusion detection systems for IoT: toward universal and resilient systems," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 3496–3509, 2018, doi: 10.1109/COMST.2018.2844742.
- [36] L. Xiao, X. Wan, X. Lu, Y. Zhang, and D. Wu, "IoT security techniques based on machine learning: how do IoT devices use AI to enhance security?," *IEEE Signal Processing Magazine*, vol. 35, no. 5, pp. 41–49, Sep. 2018, doi: 10.1109/MSP.2018.2825478.
- [37] P. Mishra, V. Varadharajan, U. Tupakula, and E. S. Pilli, "A detailed investigation and analysis of using machine learning techniques for intrusion detection," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 686–728, 2019, doi: 10.1109/COMST.2018.2847722.
- [38] B. B. Zarpelão, R. S. Miani, C. T. Kawakani, and S. C. de Alvarenga, "A survey of intrusion detection in internet of things," *Journal of Network and Computer Applications*, vol. 84, pp. 25–37, Apr. 2017, doi: 10.1016/j.jnca.2017.02.009.





- [39] M. A. Lawal, R. A. Shaikh, and S. R. Hassan, "Security analysis of network anomalies mitigation schemes in IoT networks," *IEEE Access*, vol. 8, pp. 43355–43374, 2020, doi: 10.1109/ACCESS.2020.2976624.
- [40] J. Asharf, N. Moustafa, H. Khurshid, E. Debie, W. Haider, and A. Wahab, "A review of intrusion detection systems using machine and deep learning in the internet of things: challenges, solutions, and future directions," *Electronics*, vol. 9, no. 7, Jul. 2020, doi: 10.3390/electronics9071177.

## BIOGRAPHIES OF AUTHORS







**Nisha**     received her BCA degree in computer science from Maharshi Dayanand University, Rohtak (Haryana), and received her MCA degree from Guru Gobind Singh Indraprastha University Delhi. She is a Ph.D. scholar at the Department of Computer Science and Applications, Maharshi Dayanand University, Rohtak, Haryana, India. She has qualified National Eligibility Test for Assistant Professor in India. She can be contacted at email: nisha.rs.dcsa@mdurohtak.ac.in.



**Dr. Nasib Singh Gill**     is currently Head of, the Department of Computer Science and Applications, M. D. University, Rohtak, India. He is also working as Director of, the Directorate of Distance Education as well as Director of Digital Learning Centre, M. D. University, Rohtak, Haryana. He earned his Doctorate in Computer Science in the year 1996 and carried out his Post-Doctoral research at Brunel University, West London during 2001-2002. He is a recipient of the Commonwealth Fellowship Award of the British Government for the Year 2001. Besides, he also has earned his MBA degree. He is an active professional member of IETE, IAENG, and CSI. He has published more than 304 research papers and authored 5 popular books He has guided so far 12 Ph.D. scholars as well as guiding about 5 more scholars. His research interests primarily include–IoT, machine and deep learning, information and network security, data mining and data warehousing, NLP, and measurement of component-based systems. He can be contacted at email: nasib.gill@mdurohtak.ac.in.



**Dr. Preeti Gulia**     is currently working as an Associate Professor at the Department of Computer Science and Applications, M.D. University, Rohtak, India. She has been serving the Department since 2009. She earned her doctoral degree in 2013. She has published more than 65 research papers and articles in journals and conferences of national/international repute including ACM, and Scopus. Her area of research includes data mining, big data, machine learning, deep learning, IoT, and software engineering. She is an active professional member of IAENG, CSI, and ACM. She is also serving as an editorial board member active reviewer of international/ national journals. She has guided four research scholars as well as six Ph.D. research scholars from various research areas at present. She can be contacted at email: preeti@mdurohtak.ac.in.