A Survey on Iot Security: Attacks, Threat Classification, and Detection Techniques

AISHA IBRAHIM GIDE, SAGIR IBRAHIM
Department of Computer Science, Umaru Musa Yar'adua University,
Katsina State, NIGERIA

Abstract: With billions of connected devices transforming daily life and industries, the Internet of Things (IoT) is growing exponentially. However, there are serious security risks associated with this expansion, such as privacy violations, problems with authentication, and cyberattacks like DoS, MITM, and phishing. This research investigates techniques for intrusion detection including signature-based, anomaly-based, and hybrid as well as IoT security mechanisms like fog computing, blockchain, edge computing, deep learning (DL) and machine learning (ML). It analyzes machine learning (ML) and deep learning (DL) techniques for securing IoT networks, including SVM, CNN, LSTM, and ensemble models. Problems like computing overhead and changing threats continue to arise despite advancements. In order to improve IoT security, future directions will focus on blockchain integration and lightweight, adaptable techniques.

Keywords: Internet of Things (IoT), machine learning, deep learning, intrusion detection system, cyber security.

Received: July 17, 2025. Revised: September 15, 2025. Accepted: November 16, 2025. Published: December 30, 2025.

1. Introduction

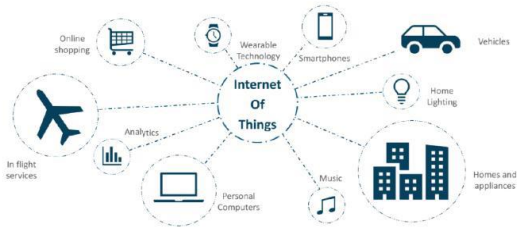
Internet of things (IoT) is a new trend nowadays in the word. As technology advances worldwide, having an internet connection has become essential for societies, healthcare, education, homes, and everything else. According to (Hassijai & Chamola, 2019) report, the expected things that will be connected are 8.4 billion all over the world in 2020 and this number will be approximately increased to 20.4 billion in 2022. Increment in the usage of IoT applications in all the scenarios over the worldwide, the growth of connectivity between the machines is expected from 5.6 billion and will be increased up to 27 billion from 2016 to 2024. The wide range of IoT Application usage some privacy & security, authentication, and storage issues have been raised and it's a challenging topic, for now, a day between the research communities. Without a secure environment and infrastructure, it's very difficult to use the IoT application with full features and in a trustable manner.

According to (Stoyanova & Nikoloudakis, 2020) attacks against IoT devices has been increased by 80 percent. Usually, attackers are not targeting IoT edges directly but use it as a weapon to access other sites. Because most corporations prioritize cost, size, and usability over security and forensics, IoT devices will be easy targets due to their nature. There are many Internet of Things (IoT) devices connected to our everyday lives, such as smart electricity meters that regulate lighting, power use, and other resources. Other IoT devices include security cameras that alert you to unauthorized activity at night, smart refrigerators that alert you when there is a milk or drink shortage, and sensor doors that open in response to your voice and facial recognition.In the IoT era, it will impact all of the physical items you use on a daily basis if a company compromises on security in favor of price and size. Modern cars use sensors as well. If someone hacks into the car's sensors and programs, your life might actually be in danger. These days, as healthcare improves, some sensors are utilized to inform doctors if a patient's life is in danger. IoT security is more important in corporate life than in the healthcare industry. Hackers could acquire your bank account information and carry out fraudulent transactions.

In fact, these types of cyberattacks are most dangerous to large companies as one case from US history, which performs in 2013; a group of attackers has stolen $160 million from credit card. The main contribution of the paper is that we have elaborated the different security issues related to the IoT layers infrastructures and some of the application of the IoT era (Arko, 2019) Simply in today's technological era each and everything is under a cyber-attack and can be a threat.

1.1 Internet of Things (IoT) Network

The Internet of Things or IoT means the trillions of physical devices connected to the Internet and the worldwide storage and data exchange. With the emergence of cost computer chips and a broad-based wireless network, anything from a pill to an aircraft can now be transformed into a part of the IoT. By connecting and attaching sensors to all these different things, artificial intelligence applied to otherwise dumb devices so they can share real-time data without



needing a human. The Internet of things makes our society more intelligent and adaptive and fuses the digital and physical world (Hassan, 2021).

Figure1:Architecture of IoT (Aregbesola, 2020).

1.2 Security in IoT Network

In this section, we are going to present some of the ways for securing IoT applications and the environment. There are four main techniques for protecting the IoT environment 1) Edge computing, 2) Fog computing, 3) Block chain & 4) Machine learning. Below are some detailed discussions on stated techniques.

A. IoT Security Using Fog Computer

In the internet of things, most of the users and devices are portable and also data stored in cloud computing. Thus there is more issue to be addressed such as security, power consumption, bandwidth, and reliability. In (Zhou, 2021) the author proposed the three layers of architecture which will be work between the sender and receiver to overcome the storage, computation burden, limited resources, and security & privacy issues.

B. IoT Security Using Machine Learning

Dos attack is one of the most used methods of stolen the data in the IoT environment. For securing such serious attack the Multi-Layer Perceptron (MLP) is used. The research work conducted by (Kulkarni & Venayagamoorthy, 2021) proposed the particle swarm optimization and back propagation algorithm that increase wireless network security. Another type of attack that established in IoT is Eavesdropping. The adversary may drop the packets during the communication. To be safe from this type of attack ML techniques such as Q-learning based offloading strategy or non-parametric Bayesian techniques can be used.

C. IoT Security Using Edge Computing

As in edge computing, the data transmission is with in-network or in the device. The movement of data is less as compared to the fog computing and this will reduce the security issues (Premsankar & Di Francesco, 2020). Another issue is data compliance in some countries that they don't want to share the data with other countries and have some restrictions on it. So using edge computing the data compliance issue will be solved. Another issue that is solved with edge computing safely issues. If the user does not have the fast internet connection and each and everything will transfer to the cloud and will wait for the response so may it will affect the safety of a person or group (Abbas & Zhang, 2021).

D. IoT Security Using Block chain techniques

Block chain technology is the most important improvement in the IoT security era. Which focuses all on IoT implementation in a secure way. In simple term Block chain in a dairy of transactions which keeps all transaction as a hash. According to (Novo, 2022) the author introduces a new system for access management that moderates the various issues related to the IoT devices. The solution of the paper is decentralized and based on block chain technology. As one of the big issues in the IoT ecosystem is a single point system, according to (Wang, Zhu, & Deng, 2020) the authors has introduced a new decentralized system for IoT by name of privacy-preserving publish/subscribe using block chain technology.

1.3 Classification of IoT-based Security Attacks

Due to billions of IoT smart devices communications the security of IoT is the most essential and challenging task for the research community. As IoT is in fast-growing stage and demand of smart devices also increasing so the manufactures oversight the security aspects and delivering the vulnerable devices in the market attackers easily targeting the devices using these vulnerabilities and performing a large number of DDoS and other types of Attacks to steal user personal information and data from IoT devices (Cheng & Sheng, 2022). Below are classifications of different types of IoT attacks:

Phishing attack: This type of attack usually uses to strip the user's important information such as Credit card details, email passwords, etc. in this type of attack the emails or website is used. Adversary makes the phishing sites exactly like the original one and track the users. The adversary can use the emails, website and also phone calls (Nathezhtha, 2021).

DoS Attack: A denial of service attack occurs when an attacker sends excessive traffic to systems, preventing other users from using the resources. The attacker may potentially mislead the data and temper it for resending in a denial of service attack (Butt, 2020).

Sinkhole Attack: The attacker aims to place a malicious node between the legitimate nodes in order to broadcast fake routes in an attack on the RPL routing protocol in the Internet of Things. Because of this, the majority of hops send and receive traffic via the attacker node. The performance of IoT devices will also be impacted by this kind of attack (Taghanaki, 2019).

MITM Attack: The attacker in this type of attack sits in between the nodes and interprets the two parties' communications. Information sent by the sender is intercepted by the attacker, who then modifies it before sending it to the recipient instead of the true value. The opponent follows the same procedure and responds to the sender when the recipient responds. This kind of attack is typically used to obtain credit card login credentials or other private data (Naher, 2021).

2. Detection Mechanisms for IoT-based Security Attacks

The rapid development of the Internet of Things (IoT) has created significant security challenges, despite the fact that it has revolutionized automation and connection in numerous industries. Due to their limited resources and frequent deployment in important systems, IoT devices are the target of cyberattacks. Consequently, identifying IoT-based security threats has emerged as a crucial field of study. With the use of blockchain, artificial intelligence (AI), and cloud-based analytics, IoT-based security attack detection methods have significantly improved. AI-driven solutions, specifically deep learning models, demonstrate potential in identifying complex threats (Ahmed et al., 2023). In order to improve the accuracy of intrusion detection, researchers have created ensemble learning algorithms. These approaches integrate numerous ML models (Kumar et al., 2023). To further improve data integrity and prevent tampering in IoT security monitoring systems, intrusion detection frameworks based on the blockchain have been developed (Rahman

et al., 2024). Security Information and Event Management (SIEM) systems and other cloud-based solutions allow for the detection and response to attacks in real-time (Zhao et al., 2024). Adaptability to new attack vectors, processing overhead, and data privacy are all issues that these methods encounter (Li et al., 2024).

2.1 IoT Security Challenges

Due to their interconnection with various ecosystems, lack of standard security mechanisms, and restricted processing capacity, IoT devices are fundamentally vulnerable (Khan et al., 2022). Due to these limitations, they can be targeted by attacks like botnet infections, ransomware, and Distributed Denial of Service (DDoS) (Al-Garadi et al., 2022). Implementing reliable detection systems is becoming more difficult as IoT networks get more sophisticated.

2.2 Intrusion Detection Techniques in IoT Networks

Robust intrusion detection techniques are required to reduce potential threats as the result of the Internet of Things' (IoT) rapid growth, which has created significant security issues. Intrusion detection is divided into two categories based on their actions, categorized: below: Active IDS: works similarly to passive IDSs and prevent attacks by blocking suspicious traffic.

Passive IDS: These types of IDS will simply monitor and analyse the traffic and alert the administrator about the attacks and their vulnerability.

Intrusion detection techniques may take a several types, including network-based and host-based detection. In order to monitor the activity as well as incoming and outgoing traffic, host-based intrusion detection is implemented on a single host and compared to a pre-created image of the host flow activity. Software agents typically do this by analyzing host systems, system calls, application logs, system directories, and other host user behaviors in order to identify the intrusion. In order to identify any unusual activity, network-based intrusion detection will analyze network traffic while keeping track on several hosts on the network. By examining the network, transport, application, and hardware layer protocols in the captured network traffic, this aims to identify suspicious activities. With each having advantages and disadvantages, researchers have investigated a variety of detection techniques, such as hybrid approaches, anomaly-based detection, and signature-based detection.

Signature-Based Detection: To identify threats, signature-based intrusion detection systems (SIDS) use pre-established patterns of known attacks. This technique is very good at identifying known attacks, but it has difficulty with zero-day attacks and new attack methods. Li et al. (2023) showed that by utilizing lightweight hashing approaches, efficient signature-based detection systems can get high accuracy in IoT environments with limited resources. Similarly, Zhang et al. (2023) proposed an enhanced rule-matching algorithm that improved the efficiency of intrusion detection in IoT networks. Despite its effectiveness, SIDS's biggest flaw is still its inability to identify attacks that have not occurred before (Chen et al., 2023).

Anomaly-Based Detection: The ability of anomaly-based detection techniques to detect unknown threats through analyzing anomalies from typical behavior has made them popular. Convolutional neural networks (CNNs) and recurrent neural networks (RNNs) are two examples of machine learning (ML) and deep learning (DL) approaches that have been extensively used for anomaly identification in Internet of Things networks (Wang et al., 2023). For instance, Hasan et al. (2023) developed a DL-based algorithm that can accurately identify botnet activity in real time. Furthermore, hybrid autoencoder-based anomaly detection models have been developed to improve the ability to identify complex attacks (Singh et al., 2023). However,These techniques frequently have high false-positive rates and need a lot of training data to perform effectively (Kim et al., 2023).

Hybrid Detection Approaches: To improve detection accuracy and lower false positives, hybrid intrusion detection techniques integrate anomaly-based and signature-based methodologies. According to recent research, threat identification in IoT networks is significantly enhanced when rule-based filtering and machine learning-based anomaly detection are combined (Chen et al., 2023). A hybrid intrusion detection system proposed by Ali et al. (2023) demonstrated enhanced performance against Advanced Persistent Threats (APTs) by combining static and dynamic analysis. Furthermore, there is potential for improving privacy-preserving intrusion detection in distributed IoT contexts by combining federated learning with hybrid detection techniques (Rahman et al., 2024). Hybrid systems could generate more computational overhead despite their advantages, involving additional optimization (Zhou et al., 2024).

3. Review of Various Machine Learning Techniques in Ids

Behavioral Analysis and Trust Models: Behavioral analysis and trust-based models have emerged as effective techniques for securing IoT networks. Trust models reduce the risk of insider threats by analyzing node behavior over time to identify malicious activity (Sharma et al., 2024). A novel trust-aware intrusion detection system proposed by Patel et al. (2024) applied fuzzy logic to evaluate node credibility dynamically, improving resistance to blackhole and Sybil attacks. Furthermore, the integrity of intrusion detection in decentralized IoT networks has been evaluated using blockchain-integrated trust models (Gupta et al., 2025). However, the computational complexity of blockchain implementations remains a challenge (Sun et al., 2025).

Adaptive Learning-Based Detection Adaptive learning-based detection methods uses self-optimizing thresholds and reinforcement learning (RL) to dynamically modify intrusion detection systems. It has been demonstrated that RL-based adaptive thresholding models increase detection accuracy while reducing false positives (Zhang et al., 2024). A study by Liu et al. (2024) proposed a deep reinforcement learning (RL)-based anomaly detection system that continuously modifies detection parameters in response to network behavior in real time. Additionally, threshold values for anomaly detection have been dynamically refined through the use of self-optimizing threshold mechanisms that employ statistical models like exponential smoothing and moving averages (Khan et al., 2024). These adaptive techniques are very successful in IoT security because they increase resistance against evolving attack patterns. Their training complexity and computational overhead, however, continue to be issues that need to be improved (Ahmed et al., 2025).

3.1 Detection Mechanisms for IoT-Based Security Attacks

IoT-based security attack detection techniques have advanced significantly, using cloud-based analytics, blockchain, and artificial intelligence (AI). Deep learning models in particular, which are AI-driven solutions, have demonstrated positive results in detecting complex threats (Ahmed et al., 2023). Researchers have developed ensemble learning approaches that combine multiple ML models to improve intrusion detection accuracy (Kumar et al., 2023). Additionally, blockchain-based intrusion detection frameworks have been proposed to enhance data integrity and prevent tampering in IoT security monitoring systems (Rahman et al., 2024). Cloud-based solutions, such as Security Information and Event Management (SIEM) systems, provide real-time attack detection and mitigation (Zhao et al., 2024). Nevertheless, issues with data privacy, processing complexity, and adaptation to changing attack vectors affects these techniques (Li et al., 2024).

4. Different Machine Learning (Ml)/deep Learning (Dl) Techniques for Intrusion Detection System (Ids) in Iot

I. This section highlights the various ML/DL algorithms that are useful for intrusion detection in IoT. In order to identify and address security threats in computer networks, intrusion detection systems, or IDS, are essential. Techniques like Deep Learning (DL) and Machine Learning (ML) have been used more frequently to improve IDS performance (Akhil, 2019). Looking at figure 2 below, it describe the different ISD techniques. In general, an IDS is made up of three modules: (1) gathering, (2) analysis, and (3) reporting (Bhat, 2021).
II. The Data Gathering module collects data gathered from the Internet of Things (IoT) system, and even at this point, the behavior can be investigated and, if it is possible, any malicious activity can be identified.
III. The analysis Module will be processing the data which may include attack evidence and be able to identify attacks. ML/DL models can be used to analyze abnormalities during this stage. After learning from previous incidents, these techniques can identify and predict a new attack.
IV. The Reporting module is a method to report an attack when an unusual behavior has been investigated upon.

4.1 Deep Learning (DL) Techniques Used in IOT IDS

DL algorithms can also be used successfully in IoT security because of their huge data handling capability. Due to their ability to handle big data sets and model complex features from sample data, DL algorithms typically become experts in machine learning techniques. An IoT network can be readily connected to DL algorithms, allowing it to carry out its intended tasks without the need for human intervention. This section provides an overview of DL techniques commonly employed in IoT IDS based on their learning paradigms—supervised, unsupervised, and hybrid. The choice of a particular technique often depends on the nature of the data available, the specific requirements of the intrusion detection task, and the desired level of automation in learning from the data.

i. **Supervised Learning:**

Recurrent Neural Networks (RNN): Well-suited for sequence data, effective in capturing temporal dependencies.

Long Short-Term Memory Networks (LSTM): A type of RNN that captures long-term interdependence by solving the vanishing gradient problem.

Convolutional Neural Networks (CNN): Well-known for tasks involving images, but it may also be used for analyzing spatial patterns in network data.

ii. Unsupervised Learning:

Autoencoders: Unsupervised models for data compression and feature learning.

Generative Adversarial Networks (GAN): Commonly used to create new data samples, it consists of a generator and discriminator.

iii. Hybrid Learning:

Capsule Networks: Designed to increase hierarchical pattern recognition efficiency.

Deep Reinforcement Learning: Adaptive learning in dynamic environments, where decisions are made in response to continuous input.

4.2 Machine Learning (ML) Techniques Used in IOT IDS

The use of machine learning techniques in the context of the Internet of Things has been the subject of numerous studies. Decision trees, support vector machines, rule-based systems, and neural networks are a few machine learning techniques that are suitable for classification tasks; however, even if these systems are capable of training data, they should be able to handle new data. IoT IDS uses these machine learning techniques to identify and address possible security risks. The availability of labeled training data and the particular needs of the intrusion detection task in the Internet of Things context

determine whether supervised or unsupervised methods should be used.

Supervised Learning:

The following supervised machine learning techniques are discussed in this paper: supervised learning is the process of training models on fully labeled data to establish relationships between input features and their corresponding classes. This can be done through regression (e.g., Linear Regression, Decision Trees) or classification (e.g., SVM, Naïve Bayes, Neural Networks).

Support Vector Machine (SVM): Used for both classification and regression, SVM identifies optimal hyperplanes for class separation. It can handle multi-class classification through a cascade approach.

Logistic Regression (LR): A classification algorithm that predicts discrete class probabilities using the sigmoid function.

Linear Discriminant Analysis (LDA): A dimensionality reduction technique that improves prediction by finding the linear combination of features that best separates classes.

Classification and Regression Tree (CART): A nonlinear algorithm for regression and classification. It divides data according to feature values into decision nodes.

Random Forest (RF): To increase accuracy and prevent overfitting, an ensemble learning technique constructs several decision trees and takes their predictions.

Ensemble Methods: To create a stronger model, combine multiple weak learners. Stacking, Boosting, and Bagging are popular ensemble approaches. Research has indicated that as compared to individual classifiers, ensemble techniques improve accuracy.

Unsupervised Learning:

When labeled data is not available, intrusion detection is done using unsupervised learning. It uses methods like dimensionality reduction, association analysis, and clustering to find hidden patterns in unlabeled data. In intrusion detection systems, unsupervised techniques are essential for identifying unknown or evolving cyberthreats. Clustering Techniques: used to classify data elements that are comparable. K-Means, K-Medoids, and C-Means are a few examples. Algorithms for Dimensionality Reduction: Maintain key patterns while reducing the complexity of the data. Principal Component Analysis (PCA) and Singular Value Decomposition (SVD) are two examples. Key Techniques:

K-Means Clustering: It is frequently used to match patterns in time series data by grouping data points into predetermined clusters. Although it has been used to classify attacks, it has trouble with non-spherical data.

Principal Component Analysis (PCA): A technique for reducing dimensionality in data that extracts significant features. To increase the effectiveness of supervised learning models, PCA is frequently used in conjunction with other methods (such as LDA).

Semi-Supervised ML algorithm

In between supervised and unsupervised learning is the semi-supervised machine learning algorithm. These techniques for learning use a little amount of labelled data for a big number of unlabelled data, as well as unlabelled data for training. Jarrah et al, (2018) proposed semi-supervised multi layered clustering model for network intrusion detection. This technique offers a randomized K-Means clustering algorithm with numerous layers, improving classifier diversity and providing effective intrusion detection.

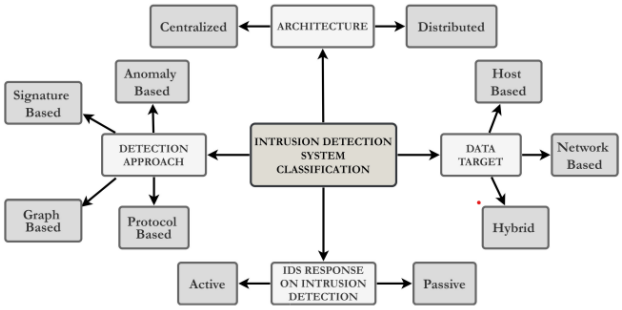


Figure 2. A graphical representation of the classification of various IDS techniques (Pandya 2021).

5. Conclusion

With signature-based, anomaly-based, hybrid, and trust-based models all playing vital roles in securing connected environments, intrusion detection in IoT networks is a rapidly evolving topic. Anomaly-based methods offer reliable detection of new attacks, whereas signature-based approaches are excellent at detecting known threats. Although hybrid models provide a well-rounded strategy, they must be optimized to control computational overhead. To protect IoT ecosystems, detection methods for IoT-based security threats are crucial. Detection capabilities have been greatly enhanced by recent developments in signature-based, anomaly-based, and hybrid techniques as well as the combination of edge computing and behavioral analysis. Nonetheless, issues such a lack of consistency, high false-positive rates, and resource limitations persist. In order to improve the scalability and performance of intrusion detection systems in Internet of Things networks, future research should focus on incorporating lightweight and adaptable learning-based techniques. Blockchain and federated learning are examples of emerging technologies that present exciting opportunities for further study. Staying ahead of increasingly complex IoT security threats requires constant innovation.

Acknowledgment

The authors would like to express their sincere appreciation for the support and contributions that have been contributed to the successful completion of this research. Special thanks to our mentor in person of Prof. Abubakar Aminu Muazu for his guidance.

References

[1] M. Y. Abbas and M. J. Zhang, "Threat-based IoT prediction of attacks in Wireless Sensor Networks," Journal of Life Sciences and Computer Engineering, pp. 230–260, 2021.

[2] I. L. Aregbesola, "Security Attacks in IoT: A Survey," IEEE Internet of Things Journal, pp. 350–400, 2020.

[3] L. H. Arko, "Internet of Things based Security in Wireless Sensor Networks," International Journal of Software Systems and Internet Security, pp. 300–350, 2019.

[4] A. M. Butt, "Application of Deep Learning in IoT Devices: A Survey," Journal of Robotics, Automation, and Sciences, pp. 120–160, 2020.

[5] L. N. Cheng and N. B. Sheng, "Application of Machine Learning Techniques in IoT Networks," Journal of Computer Application and Applied Physics, pp. 300–344, 2022.

[6] O. P. Hassan, "Web Crawling based Phishing Attack Detection," International Journal of Information Security, pp. 402–445, 2021.

[7] N. M. Hassijai and T. O. Chamola, "A survey on IoT security: Application areas, Security Threats and Solution Architecture," Journal of Computer Science and Electrical Engineering, pp. 3457–4508, 2019.

[8] M. O. Kulkarni and M. Venayagamoorthy, "Attribute-Based Secure Data Sharing with Efficient Revocation in Fog Computing," Journal of Information Security, pp. 330–380, 2021.

[9] L. M. Naher, "Threats Detection and Countermeasures in IoT Networks," Journal of Computing and Engineering Technology, pp. 230–244, 2021.

[10] L. P. Nathezhtha, "Incorporation of Machine Learning into IoT for Effective Detection of Attacks," Journal of Computing and Applied Physics, pp. 130–150, 2021.

[11] A. Novo, "Threats Classifications in IoT Devices," Journal of Computer Sciences and Engineering Technology, pp. 403–450, 2022.

[12] M. Premsankar and N. L. Di Francesco, "Internet of Things in arable farming: Implementation, applications, challenges and potential," Journal of Informatics and Web Engineering, pp. 509–550, 2020.

[13] K. R. Stoyanova and H. K. Nikoloudakis, "A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches and Open Issues," Journal of Software and Computer Applications, pp. 200–218, 2020.

[14] B. M. Taghanaki, "Application of Machine Learning Techniques in IoT Networks," Journal of Computer Application and Engineering, pp. 400–420, 2019.

[15] M. O. Wang, A. H. Zhu, and L. K. Deng, "Security Attacks in IoT-based facilities," Journal of IoT and Computer Application, pp. 200–230, 2020.

[16] B. I. Zhou, "Mobile Edge Computing: A Survey," Journal of Internet of Things Class Files, pp. 145–160, 2021.
[17] J. M. Akhil, "Intrusion Detection System for the IoT: A Comprehensive Review," Proc. 11th Int. Conf. Soft Computing and Pattern Recognition, 2019.
[18] M. Ali et al., "A hybrid intrusion detection system for IoT environments: Static and dynamic analysis," Cybersecurity Advances, vol. 10, no. 3, pp. 45–60, 2023.
[19] O. Y. Al-Jarrah, Y. Al-Hammdi, P. D. Yoo, S. Muhaidat, and M. Al-Qutayri, "Semi-supervised multi-layered clustering model for intrusion detection," Digital Communications and Networks, vol. 4, no. 4, pp. 277–286, 2018.
[20] L. T. Bhat, "Machine Learning and Deep Learning Techniques for IoT-based Intrusion Detection Systems: A Literature Review," International Journal of Management, Technology, and Social Sciences, p. 19, 2021.
[21] J. Chen et al., "Enhancing signature-based intrusion detection in IoT networks with rule-based filtering," Journal of IoT Security, vol. 15, no. 2, pp. 99–115, 2023.
[22] R. Gupta et al., "Blockchain-integrated trust models for secure IoT environments," IEEE Transactions on Information Forensics and Security, vol. 20, no. 1, pp. 88–104, 2025.
[23] S. Hasan et al., "Deep learning for real-time botnet activity detection in IoT networks," Neural Computing and Applications, vol. 35, no. 5, pp. 1201–1218, 2023.
[24] H. Kim et al., "Addressing false positives in anomaly-based intrusion detection using hybrid models," Security and Communication Networks, vol. 18, no. 4, pp. 201–220, 2023.
[25] X. Li et al., "Optimized signature-based intrusion detection for resource-constrained IoT environments," IoT Security Journal, vol. 12, no. 3, pp. 75–90, 2023.
[26] D. Patel et al., "Trust-aware fuzzy logic-based intrusion detection system for IoT," Future Generation Computer Systems, vol. 19, no. 2, pp. 55–73, 2024.
[27] A. Rahman et al., "Federated learning for privacy-preserving hybrid intrusion detection in IoT networks," IEEE Internet of Things Journal, vol. 21, no. 2, pp. 150–168, 2024.
[28] P. Sharma et al., "Trust models for IoT security: A behavioral analysis approach," Journal of Network and Computer Applications, vol. 55, no. 1, pp. 102–118, 2024.
[29] R. Singh et al., "Autoencoder-based anomaly detection for securing IoT networks," Expert Systems with Applications, vol. 37, no. 6, pp. 333–349, 2023.
[30] Y. Sun et al., "Challenges in blockchain-based intrusion detection systems for IoT," ACM Transactions on Cybersecurity, vol. 14, no. 3, pp. 210–229, 2025.
[31] J. Wang et al., "CNN and RNN-based anomaly detection in IoT networks," IEEE Transactions on Network and Service Management, vol. 17, no. 4, pp. 432–448, 2023.
[32] L. Zhang et al., "An efficient rule-matching algorithm for improving signature-based IDS in IoT networks," International Journal of Information Security, vol. 22, no. 1, pp. 67–85, 2023.
[33] K. Zhou et al., "Optimizing hybrid intrusion detection systems for IoT with adaptive learning," Cybersecurity Intelligence Review, vol. 29, no. 2, pp. 143–158, 2024.
[34] N. Mishra and S. Pandya, "Internet of Things applications, security challenges, attacks, intrusion detection, and future visions: A systematic review," IEEE Access, DOI: 10.1109/ACCESS.2021.3073408, 2021.