Journal of Intelligent Systems and Internet of Things
Vol. 15, No. 02, PP. 183-190, 2025
DOI: https://doi.org/10.54216/JISIoT.150213

Securing IoT through Intrusion Detection Systems: An Overview

Razan Abdulhammed[1], Shaima Miqdad Mohamed Najeeb[1], Rabei Raad Ali[1,*], Mohammed Ahmed Jubair[2]

[1]Technical Engineering College for Computer and AI, Northern Technical University, 41000, Mosul, Iraq

[2]Department of Computer Technical Engineering, Al-Maarif University College, Al-Ramadi, 31001, Iraq

Emails: rabdulhammed@ntu.edu.iq; shaimamiqdad76@ntu.edu.iq; rabei@ntu.edu.iq; mohammed.sites89@gmail.com

Abstract

Internet of Things (IoT) has emerged as a new paradigm for integrating internet resources and physical objects. It provides a better standard of living in different domains, like industrial processes, home automation, and environmental monitoring. The growth of IoT depends on the need to connect more devices via the Internet. However, anywhere internet connectivity is involved, security poses as an enormous challenge. Intrusion Detection Systems (IDS) can protect IoTs by applying rules related to IoTs operation. This paper reviews some of the mechanisms of IoT-related IDS, which protect IoT devices against various attacks. The paper includes a summary of the recent developments of IDS against many security threats. A review is presented regarding various IDS designs developed in the last decade with different methods, ideas, and approaches toward a better understanding of suitable IDS platforms that provide security against the global growth of attacks and intruders. It also involves the examination of the IDS basics, types, and components of the previously proposed systems, as well as discussing the pros and disadvantages of each. We organize the taxonomy of investigated IDS approaches using the detection approaches. This work aims to provide a thorough summary of the existing IDS designs and issues to empower research and development for IDS about IoTs.

Received: September 25, 2024 Revised: November 20, 2024 Accepted: January 17, 2025

Keywords: VANETs; DTDF-TARP; UAVs; routing protocol; CLO-MFG; RDJ-EDC

1. Introduction

The core technology that shapes a smart environment is the framework integration of the sensor-actuators, allowing information to be generated, collected, and shared among different devices, applications, and platforms. The goal is to develop a Common Operating Picture (COP) that enables controlling unrestricted things of the environment [1]. The vision of the Internet of Things (IoT) is to create new services and applications by diffusing the things and objects of the environment for pervasive presence in wired and wireless connected networks based on different unique addressing techniques and schemes [2]. In contrast, various definitions have been suggested for IoT. This paper refers to IoT as the network of interconnected objects of different sizes, types, and locations. The objects include computers, smartphones, cameras, industrial systems, vehicles, toys, home appliances, medical instruments, buildings, cities, and animals. These objects communicate and share information using communication protocols to trace, reorganize, posit, control, monitor, upgrade, and administer remote objects in a safe and real-time manner. IoT, soft computing, and data mining integrations are highly advanced trends in the modern world that have become popular due to several advantages. Integrating IoT with soft computing and data, mining has become an active research area and offers several contributions in different sectors. IoT must go through a transformation to address the challenges associated with data, insecurity, and the environment. Analytics of data obtained from things gives a strong hold on intrusion detection systems for making security decisions. This whole integrated approach to IoT, data mining, soft computing, and IDS is given various independent names such as facts, components, steps, dimensions, attributes, fields, technologies, or simply, doing things.

Signature-based IDS approaches can detect the attacks if the network behaviour matches the signature of attacks stored in the IDS database. This approach is an effective and accurate detection method that alerts the network once the attack is triggered. It is easy to understand and can be easily deployed [3]. In contrast, specification-based approaches need experts to manually define the thresholds and standards of the detection approach [4]. This article

presents a survey of IDS designs developed in the last decade with different methods, ideas, and approaches. We organize the taxonomy of investigated IDS approaches based on the detection approach. The review shows that anomaly-based detection approaches are applied in 45% state of the art, whereas signature, specification, and hybrid constitute 25%, 20%, and 10%, respectively. This research goal is to contribute to the growing area of research in IoTs by exploring intrusion detection system designs, datasets, and performance evaluation metrics. Our contributions to this area of research can be summarized as follows:

- Present an investigation of various mechanisms proposed against network attacks and intrusions in the light of IDS and IoTs.
- An examination of the basics of IDS, as well as the types and proposed system components.
- Summarize popular benchmark datasets used for designing IDS for IoTs and identify the most suitable dataset for designing IDS for IoTs.
- Introduces a taxonomy of intrusion detection system evaluation metrics.
- Recommend a suitable architecture design for an IoT environment.

2. Review Methodology

This research aims to review the available work in recent years on securing IoTs via IDS. We used various resources and libraries such as IEEE, ACM, Hindawii, Elsevier, Springer, and MDPI based on different keywords. The main keywords are “intrusion detection" and "intrusion detection systems for IoT.” The selection process was based on certain criteria, such as being relevant to the IoT networking environment, being relevant to intrusion detection systems, being relevant to Anomaly, Signature, Specification Behavior, or Hybrid-based intrusion detections, being relevant to intrusion detection datasets, being relevant to performance evaluation metrics of intrusion detection systems. Based on the selection criteria, 90 articles were excluded by reviewing the titles and abstracts of the retrieved articles. To be more specific, articles that secure IoTs using integrity, cryptography, and authentication techniques were not reviewed, whereas articles that secure IoTs using IDS were reviewed entirely. This section is dedicated to a related to intrusion detection systems in IoTs. In [5], the study aims to understand the differences between IDS platforms and the cross-platform distributed approach. In [6], the authors, analysis, and comparison of state-of-the-art NIDS proposals in the IoT context, covering architecture, validation strategies, treated threats, algorithm deployments, and machine learning. In [7], the authors focused on mechanisms of IDSs, while also delving into the IoT architecture and emerging security vulnerabilities. In [8], the authors provide an overview of IDS models and cover the analysis of various machine learning and deep learning techniques. It introduced IoT systems-related technologies, protocols, architecture, and threats. In [9], the authors highlight the challenges and opportunities of implementing intrusion detection in IoT and prevention utilizing artificial intelligence and fog computing architecture. In [10], the authors classify IDSs for detection method, IDS placement, security, and validation. In [11], the authors focused on architecture types and proposed future directions in IoT-based IDS. It highlights the unsuitability of traditional security practices due to their poor coverage of the IoT domain. In [12], the study highlights the powerful capabilities of Artificial Intelligence methods such as Machine Learning and Deep Learning in meeting the IDS requirements of IoT. In [13], the authors focused on IDS, Intrusion Prevention Systems (IPS), and Intrusion Response Systems (IRS). Table 1 highlights related surveys.

Table 1: A compassion among related survey and under review survey

Ref.	Dataset	Performance Metrics	Application
[5]	×	×	×
[6]	✓	×	×
[7]	×	×	✓
[8]	×	×	×
[9]	×	×	×
[10]	×	×	×
[11]	×	×	×
[12]	×	×	×
[13]	✓	✓	×

3. The Intrusion Detection System (IDS) Model

In this subsection, we review and analyse IDS-related work divided into four approaches: anomaly-based, signature-based approach, specification-based approach, and hybrid-based approach. Each approach plays a significant role in the evolution of IDS, with an anomaly-based approach focusing on deviations from normal behaviour, a signature-based approach based on known attack patterns, a specification-based approach based on predefined rules, and a hybrid-based approach combining the strengths of the other three. One of the most significant challenges in this area is identifying the attacker once they are inside the network. However, previous work has yet to investigate the evaluation latency in determining the performance of IDS. According to this review, a utilization summary of detection approaches of the sample papers presented in this review is highlighted in Figure 1.

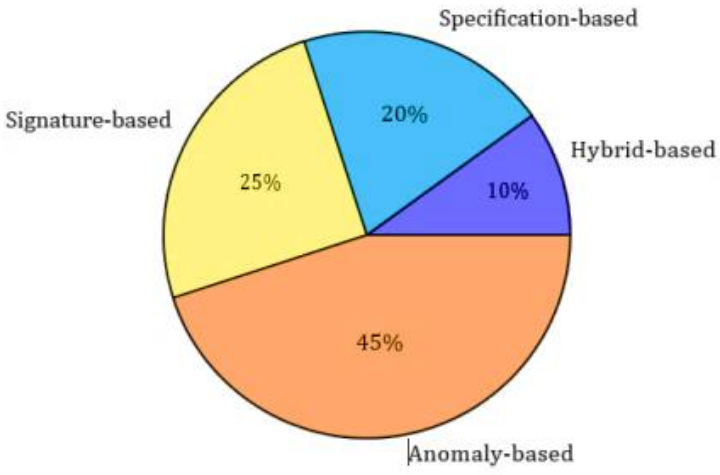

Figure 1. A summary of the detection approach of the sample of papers

IoT elements generally involve identification, sensing, communication, computation, service, and semantics. Moreover, the technological concepts that can be considered as the enabling and facilitating technologies that made IoTs possible [2] include sensor networks, microprocessors, micro-controllers, Radio Frequency Identification, Global Position System, General Radio Packet Service, and Wi-Fi. Radio Frequency Identification is used to identify objects in IoT. These ranges encompass short-range communication, short-to-medium-range communication, medium-range communication, and long-range communication. Table 2 highlights different IoT wireless connectivity technologies.

Table 2: IoT Wireless Connectivity Techniques

Communication Range	**Technology**
Contact (0-10) Meters	RFID, NFC (EMV)
Short (10-100) Meters	Bluetooth, Bluetooth LE, Zigbee, Z-Wave
Short to Medium (100-1000) Meters	WiFi
Medium (5000-10000) Meters	Zigbee-NAN (6LoWPAN), Wi-SUN (6LowPAN)
Long (10000) Meters	Cellular (2G, 3G, 4G and 5G), LE-MTC
Very Long (>10000) Meters	MQTT IoT

The data in IoTs is accomplished either at a remote server [14]. The objects in IoTs, applications, and systems are vulnerable to unauthorized access by intruders who attempt to break into the network and gain unauthorized access to confidential information. The role and position of IDS within the IoT's paradigm are shown in Figure 2.

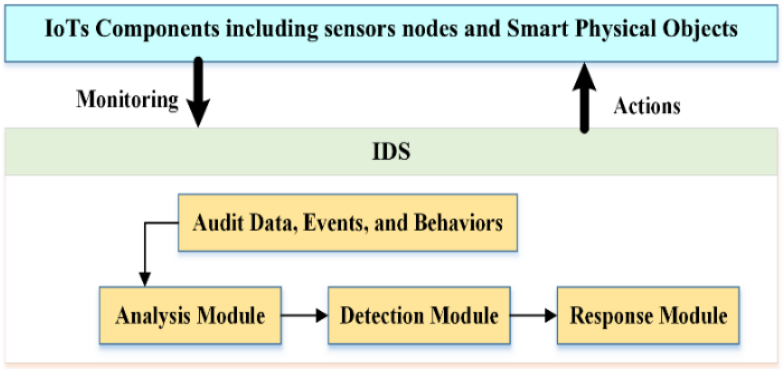

Figure 2. Intrusion Detection System Model.

A. Anomaly-based IDS

A novel model for IDS by Pajouh et al. [15] is based on a two-tier classification approach to detect malicious attacks. It was applied based on component analysis and dimension reduction techniques. The proposed model achieved high detection rates in deploying a multi-layer classifier and low false positives in deploying feature refinement and protocols of IoTs. Al Baalbaki et al. [16] presented an Anomaly Behaviour Analysis System (ABAS) for the Zigbee protocol. Their proposed system could detect Zigbee attacks with low false alarms and high detection rates and classify them based on their destination, origin, and impact. The approach was evaluated by launching DoS, pulse, delay, jamming, NWK knockdown, and flooding attacks. Arrington Alipour et al. [17] described anomaly-based IDS against service session hijacking, spoofing, and MAC address spoofing. They used the IEEE 802.11 wireless network protocol and behaviour-based techniques to detect normal behaviours triggered in the network and analyse them based on state machine monitoring. The approach has also been evaluated regarding detection rate and low false alarms. The analysis of attacks is classified based on the anomaly-behaviour analysis reference data. Airehrour et al. [18] proposed host-based IDS to detect blackhole attacks in 6LoWPAN environments using a trust-based mechanism that incorporates the node-computed trust value. The authors proposed this model based on the forwarding behaviour of neighbouring nodes in the network. The authors, however, did not estimate the overhead cost of energy consumption and the memory usage of their proposed IDS on the performance of the network and the nodes. Granjal et al. [19] designed a new anomaly-based IDS model to identify and avoid Denial of Service (DoS) attacks in environments in 6LoWPAN and CoAP communication protocols.

B. Specification-based IDS

Le et al. [20] suggested specification-based IDS to detect rank and local repair attacks in RPL network environments. However, the authors must provide simulation or numerical results to validate their proposed IDS. Wallgren et al. [21] proposed IDS designed for IPv6 was to meet the requirements of IPv6-connected devices in WSN. It was designed, implemented, and evaluated for IoT regarding routing attacks, including sinkholes, spoofed information, and selective forwarding attacks. It could detect all malicious nodes of sinkholes or selective forwarding attacks. However, it yielded a low true positive rate. This implies that there are many false alarms when detecting malicious nodes. In addition, limited energy and memory are challenging to the approach based on IPsec message security technology. The experiments were run in the Cooja Contiki network simulator, which provided realistic results. The average standard deviation showed the accuracy of the RPL protocol integral of the IoT result. A novel architecture was presented for networks considering the potential applications of IoT against internal and external intrusions. The detection of intrusion can be extended to complement the approach for improved detection in IoT. However, detecting attacks requires improvement in operating systems other than Contiki OS. The proposed security monitor can detect attacks by checking and comparing the run time behaviour and the expected behavior model. The specification language was based on event calculus algebraic data structure and monadic logic. It detects not only cyber-attacks but also all behavioural deviations and attacks, such as bugs. Therefore, it is applicable for legacy systems security. These systems are also non-adaptive to the constant changes of attacks.

C. Signature-based IDS

A proposed automated method for generating a signature-based detection approach was presented by Mondal et al. [23] by applying PCA to determine the importance of sub-strings in different instances of worms. Different experiments have been performed to demonstrate the efficiency of the developed algorithm based on signature generation and substring exaction. The basis of the detection mechanism was PCA to help determine the signature data. Experiments were performed and showed a successful detection and reduction in false positive rates. The results showed improved success in detecting polymorphic worms. However, the proposed approach was only

dedicated to polymorphic worms and cannot be effective against innovative worms. Kshirsagar al. [24] presented a signature-based technique that implemented intrusion information retrieval. The algorithm is developed to utilize ontological approaches for better information retrieval to detect and prevent attacks based on inherent reasoning ontology. The mitigation technique is based on a risk management policy that could have a check on the intrusion over the network. Cardoso et al. [25] developed a Complex Event Processing Intrusion Detection System (CEPIDS) to detect DDoS attacks. The authors used a set of Complex Event Processing Rules (CEPR) for syn flood, UDP flood, ICMP flood, and port scan attacks. The authors compared and contrasted CEPIDS with Snort and Bro IDS. CEPIDS achieved better performance compared to Bro IDS in terms of CPU and RAM utilization and lower packet loss. The system demonstrated that the CEP mechanism is adequate and efficient for the IoT environment and can become a resourceful tool for further study and extension of the framework towards new attacks and sets of CEP rules.

D. The hybrid-based IDS

Raza [26] proposed the SVELTE host-based real-time IDS to detect selective forward and sinkhole attacks in the 6LoWPAN network. SVELTE was designed based on a hybrid architecture in which the border router processed the IDS modules. At the same time, the network nodes were responsible for a lightweight task, such as sending data to the border router and notifying it about the malicious traffic they received. The significant drawbacks of SVELTE include high false positive rates, stationary node nature, consumed power, and the assumption of a small number of nodes. Sedjelmaci et al. [27] developed a hybrid-based detection method based on game theory against new attack signatures. A balance between energy consumption and accuracy detection was considered to show the results of the proposed anomaly detection approach. The hybrid proposed approach requires low energy for detection while high detection accuracy is guaranteed. In addition, low false positive rates were generated. The work was implemented in a Wireless Sensor Network (WSN). Krimmling and Peter [28] developed a framework that ran on a Raspberry Pi to evaluate a lightweight hybrid-based intrusion detection technique for an innovative city application that uses the Constrained Application Protocol) COAP (protocol. The flexible framework could be extended and updated with different application codes. However, the study did not provide any numerical result regarding false positive and false negative rates. The presented taxonomy and accompanying analysis provide a structured understanding of current methodologies, paving the way for future research to enhance security measures in IoT ecosystems.

4. Review Outcomes

The resource limits can modify the capability of IDS to some degree. Some review studies addressed the problems of energy consumption and energy constraints of IoT devices that can affect the functionality of devices. The use of low-capacity IoT devices without adequate knowledge of the potential influence may render the network vulnerable to security attacks. Understanding the resource limits available to effectively integrate these limitations into the intrusion detection system is important. However, our view emphasizes that the performance of the intrusion detection system is directly influenced by the available resource limits. According to most existing studies, IDS within IoT environments generally have positive impacts. Various studies have revealed notable outcomes following IDS analysis, including enhanced protection levels, risk count reduction, attack prevention, and attack mitigation. Critically, the enormous growth of IoT systems has resulted in a lack of field knowledge about attacks. IDS has automation features to facilitate real-time identification, analysis, and efficient defense capabilities to respond to an occurrence. The review perspective is that well-designed IDS can identify available threats efficiently. These methods can be valid for enhancing the capabilities of intrusion detection systems in the IoT, but whether these modified IDS solutions would still function as expected on a regular IoT-based system remains to be determined due to possible glitches. This involves a thorough review of existing literature, analysis of current trends, and exploration of potential future developments, leaving no stone unturned in our quest for knowledge and understanding.

A. Threats Landscape Challenges

The attacks in IoT are of many types, including internal and external attacks. In other words, insider and outsider attacks are mainly categorized into two major types. The outsider attacker is not an actual node in the network, while the insider attacker is an element of the network. The potential cyber-attacks of IoT applications are sinkhole attacks, wormhole attacks, Sybil attacks, hello flood attacks, and denial of service attacks. Sinkhole attacks initiate a malicious node to trace the network traffic and attract the adjacent nodes. It shows the routing cost as much as minimum to introduce false nodes in the network infrastructure. Wormhole attacks create a virtual tunnel between different nodes to forward nodes among the actual nodes. It can also be utilized to convince the distinct nodes to be neighbours. Selective forwarding attacks act as normal actual nodes to drop packets, such as black hole attacks. Sybil attacks have multiple identities to attack the routing protocol and detection algorithm. Flood attacks target the hello message to utilize the routing protocol broadcast, which sends and receives hello messages from the source node to add the neighbours to the table. DoS attacks can destroy connectivity and resource availability,

which prohibit legitimate users from accessing network resources and services. It affects the network resources, CPU time, and bandwidth [29].

B. IDS Designs Challenges

In IoT environments, most components have limited battery, processing power, and memory devices on the network's edge (sensors and actuators). These are connected to a gateway (which can also be application-specific with a limited resource device). Sengupta et al. [30], classify the attacks based on discussing the countermeasures against these attacks and the objects of vulnerability. The inherent mechanism in Routing Protocols for Low-power (RPL) and Lossy Ne works could mitigate the effect of sinkhole attacks. Future research should concentrate on further risk management investigations to enhance the suggested countermeasures, as IoT networks are scarcely restricted environments.

3 Performance Metrics Challenges

The performance metrics measure and evaluate the parameters that affect the performance of an IDS and the IoT network [30]. Other measures include false alarm rate, possibility of attack, reliability of attack detection, error reporting and recovery, and induced traffic latency [28]. Taxonomy of intrusion detection systems evaluation metrics. The taxonomy groups the evaluation metrics into three board types: Performance, Complexity, and Security. Complexity-based metrics are quantitative metrics for measuring complexity based on IDS design and implementations. Memory usage represents the amount of system random access memory (RAM) used by the IDS while in operation [16]. The performance-based metrics are further grouped into confusion-matrix-based, graph-based, and balanced-based.

4 Datasets Challenges

In this section, we will highlight the crucial role of benchmark datasets in the development of intrusion detection systems for IoT, a field of research that is of utmost importance in cybersecurity. Table 4 introduces standard datasets that are not just data points but tools that developers can utilize to design intrusion detection systems for IoT.

Table 3: Most common datasets for IDS implementation in IoT

Dataset	Characteristic
NSL-KDD	Suitable for IoTs
CICIDS2017	Suitable for IoTs
AWID	Suitable for IoTs
UNSW-NB15	Suitable for IoTs
IOTs-MQTT	Specific for IoTs
RPL-Nidds17	Specific for IoTs
Iot Sentinel	Specific for IoTs
BoT_IoT	Specific for IoTs
N-BaIoT	Specific for IoTs
ToN-IoT	Specific for IoTs
MedBIoT	Specific for IoTs
MQTT-IOT-IDS2020	Specific for IoTs
IoT-23	Specific for IoTs
IoTID20	Specific for IoTs

These datasets are not just for academic scrutiny, but also for practical use in assessing, designing, and evaluating IDS for IoT. The field of IoT computing is in dire need of appropriate datasets that reflect real-time environments. The urgency of this need is underscored by the fact that the data have been gathered over TICS, making the case for datasets based on real IoT computing environments. In this context, datasets incorporate protocols such as MQTT, XMPP, LoRWAN, Bluetooth, Wi-Max, Zigbee, and NFC [14-25]. Nonetheless, the dataset is collected based on datalink layer protocols and host-based audit material, which makes it suitable for host-based intrusion detection systems in the data link layer.

6. Conclusion

The IoT paradigm has established a ground of high expectations from the capacity of transformation of physical objects to other domains and applications. However, besides the benefits of developing IoT applications, some attacks are challenging the best benefits of these applications in terms of security and privacy. The current security solutions and countermeasures have obstacles and can only be employed in traditional networks. IDS is one of the very essential security tools against attackers in IoT environments. In this paper, we introduced a survey of the most recent developments of IDS research efforts and their roles in the literature concerning the security of IoT applications, systems, and networks. We observed that the research of IDS is still insufficient to adapt to the quick development of IoT environments. Further, the proposed solutions have not covered all types of attacks and are not suitable across various platforms of IoT technologies. Additionally, the detection methods for adequate security improvement are not well consolidated. Integrating advanced machine learning techniques into these systems may improve their efficacy and reliability against emerging cyber threats. IoT environments can benefit from behavior-based detection approaches because most sophisticated systems deliver a well-defined concept of cognitive processes and can exploit their consistent behaviour to build an intrusion detection system. The minimal processing burden of signature-based detection and resource-constrained features of IoT devices make signature-based detection useful in designing IDS for IoT. Once designing effective IDS for IoT environments, it is crucial to consider detection latency. This is especially important given the real-time nature of many IoT applications, such as those in smart living, nuclear and industrial sectors, healthcare, and military use, where prompt detection is vital. Even a slight delay in identifying intrusions or attacks can have severe consequences. Therefore, establishing new performance and lifecycle metrics tailored to IoT systems and applications is critical. While developers typically report traditional performance metrics such as FPR, FNR, TPR, TNR, accuracy, and detection rate, it is also essential to assess factors like detection latency and memory usage. Due to IoT's large-scale and distributed nature, a hybrid detection approach is necessary, rather than relying on an autonomous one.

References

[1] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions," *Future Generation Computer Systems*, vol. 29, pp. 1645–1660, 2013.

[2] K. K. Patel, S. M. Patel, and P. Scholar, "Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges," 2016.

[3] A. R. Khan, "Zero Trust-Based Blockchain-Based IoT Security with Consensus and Access Control Framework," *Journal of Intelligent Systems & Internet of Things*, vol. 12, no. 1, 2024.

[4] R. Jabbar et al., "Urban Traffic Monitoring and Modeling System: An IoT Solution for Enhancing Road Safety," *arXiv preprint arXiv: 2003.07672*, Mar. 2020. [Online]. Available: https://arxiv.org/abs/2003.07672.

[5] R.-Y. Ju and W. Cai, "Fracture Detection in Pediatric Wrist Trauma X-ray Images Using YOLOv8 Algorithm," *arXiv preprint arXiv: 2304.05071*, Apr. 2023. [Online]. Available: https://arxiv.org/abs/2304.05071.

[6] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki, "Network Intrusion Detection for IoT Security Based on Learning Techniques," *IEEE Communications Surveys & Tutorials*, vol. 21, pp. 2671–2701, 2019.

[7] M. F. Elrawy, A. I. Awad, and H. F. Hamed, "Intrusion Detection Systems for IoT-Based Smart Environments: A Survey," *Journal of Cloud Computing*, vol. 7, 2018.

[8] J. Asharf et al., "A Review of Intrusion Detection Systems Using Machine and Deep Learning in Internet of Things: Challenges, Solutions and Future Directions," *Electronics*, 2020.

[9] A. Boyanapalli and A. Shanthini, "A Comparative Study of Techniques, Datasets and Performances for Intrusion Detection Systems in IoT," 2020.

[10] B. B. Zarpelão, R. S. Miani, C. T. Kawakani, and S. C. Alvarenga, "A Survey of Intrusion Detection in Internet of Things," *Journal of Network and Computer Applications*, vol. 84, pp. 25–37, 2017.

[11] E. Benkhelifa, 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, pp. 3496–3509, 2018.

[12] H. Wu, H. Han, X. Wang, and S. Sun, "Research on Artificial Intelligence Enhancing Internet of Things Security: A Survey," *IEEE Access*, vol. 8, pp. 153826–153848, 2020.

[13] Kamaldeep, M. Dutta, and J. Granjal, "Towards a Secure Internet of Things: A Comprehensive Study of Second Line Defense Mechanisms," *IEEE Access*, vol. 8, pp. 127272–127312, 2020.

[14] M. S. Mahmoud and A. A. Mohamad, "A Study of Efficient Power Consumption Wireless Communication Techniques/Modules for Internet of Things (IoT) Applications," *IoT*, 2016.

[15] H. H. Pajouh, R. Javidan, R. Khayami, A. Dehghantanha, and K. Choo, "A Two-Layer Dimension Reduction and Two-Tier Classification Model for Anomaly-Based Intrusion Detection in IoT Backbone Networks," *IEEE Transactions on Emerging Topics in Computing*, vol. 7, pp. 314–323, 2019.

[16] B. A. Baalbaki, J. Pacheco, C. Tunc, S. Hariri, and Y. B. Al-Nashif, "Anomaly Behavior Analysis System for ZigBee in Smart Buildings," in *IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA)*, 2015, pp. 1–4.

[17] H. R. Alipour, Y. B. Al-Nashif, and S. Hariri, "IEEE 802.11 Anomaly-Based Behavior Analysis," in *International Conference on Computing, Networking and Communications (ICNC)*, 2013, pp. 369–373.

[18] D. Airehrour, J. Gutiérrez, and S. K. Ray, "Securing RPL Routing Protocol from Blackhole Attacks Using a Trust-Based Mechanism," in *26th International Telecommunication Networks and Applications Conference (ITNAC)*, 2016, pp. 115–120.

[19] J. Granjal, J. M. Silva, and N. Lourenço, "Intrusion Detection and Prevention in CoAP Wireless Sensor Networks Using Anomaly Detection," *Sensors (Basel, Switzerland)*, vol. 18, 2018.

[20] A. Le, J. K. Loo, K. K. Chai, and M. Aiash, "A Specification-Based IDS for Detecting Attacks on RPL-Based Network Topology," *Information*, vol. 7, p. 25, 2016.

[21] L. Wallgren, S. Raza, and T. Voigt, "Routing Attacks and Countermeasures in the RPL-Based Internet of Things," *International Journal of Distributed Sensor Networks*, 2013.

[22] B. A. Baalbaki, J. Pacheco, C. Tunc, S. Hariri, and Y. B. Al-Nashif, "Anomaly Behavior Analysis System for ZigBee in Smart Buildings," in *IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA)*, 2015, pp. 1–4.

[23] A. Mondal, S. Paul, A. Mitra, and B. Gope, "Automated Signature Generation for Polymorphic Worms Using Substrings Extraction and Principal Component Analysis," in *IEEE International Conference on Computational Intelligence and Computing Research (ICCIC)*, 2015, pp. 1–4.

[24] D. Kshirsagar and S. Kumar, "An Ontology Approach for Proactive Detection of HTTP Flood DoS Attack," *International Journal of System Assurance Engineering and Management*, vol. 14, pp. 840–847, 2021.

[25] A. M. Cardoso, R. F. Lopes, A. S. Teles, and F. B. Magalhães, "Poster Abstract: Real-Time DDoS Detection Based on Complex Event Processing for IoT," in *International Conference on Internet-of-Things Design and Implementation*, 2018.

[26] S. Raza, L. Wallgren, and T. Voigt, "SVELTE: Real-Time Intrusion Detection in the Internet of Things," *Ad Hoc Networks*, vol. 11, pp. 2661–2674, 2013.

[27] H. Sedjelmaci, S. Senouci, and T. Taleb, "An Accurate Security Game for Low-Resource IoT Devices," *IEEE Transactions on Vehicular Technology*, vol. 66, pp. 9381–9393, 2017.

[28] J. Krimmling and S. Peter, "Integration and Evaluation of Intrusion Detection for CoAP in Smart City Applications," in *IEEE Conference on Communications and Network Security*, 2014, pp. 73–78.

[29] S. T. Zargar, J. B. Joshi, and D. Tipper, "A Survey of Defense Mechanisms against Distributed Denial of Service (DDoS) Flooding Attacks," *IEEE Communications Surveys & Tutorials*, vol. 15, pp. 2046–2069, 2013.

[30] J. Sengupta, S. Ruj, and S. D. Bit, "A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT," *Journal of Network and Computer Applications*, vol. 149, 2020.

[31] A. Rghioui, A. Khannous, and M. Bouhorma, "Denial-of-Service Attacks on 6LoWPAN-RPL Networks: Threats and an Intrusion Detection System Proposition," 2014.