Intrusion Detection Systems for Iot Networks: A Comprehensive Review and Conceptual Framework

Asma Shaikh[1], Praveen B M[2], Suhel Sayyad[3]

[1]Post Doc Fellow, Srinivas University, Professor, AI & DS Annasaheb Dange College of Engineering and Technology, Ashta, Sangli.
[2]Director, Srinivas University, Mangalore, India,
[3]Professor, CSE, Annasaheb Dange College of Engineering and Technology, Ashta, Sangli.

Abstract

Purpose: The rapid expansion of Internet of Things (IoT) devices has significantly heightened the risk of cyber-attacks, necessitating robust security measures such as Intrusion Detection Systems (IDS). Traditional IDS approaches often struggle to process the vast amounts of data generated by IoT networks. Recent advancements in deep learning, particularly Convolutional Neural Networks (CNNs), have demonstrated potential in enhancing security by automatically detecting complex patterns in data. This study aims to explore and analyze CNN-based and hybrid deep learning methods for IDS in IoT networks.

Design/Methodology/Approach: This paper conducts a comprehensive review of IDS techniques for IoT networks, focusing on deep learning-based approaches published between 2017 and 2025. The analysis includes methods such as edge computing, transfer learning, lightweight models, and federated learning to improve detection accuracy and efficiency while addressing the resource constraints of IoT devices.

Findings/Result: The study highlights that deep learning-based IDS can effectively detect both known and unknown threats with high accuracy and low false-positive rates. However, challenges such as high computational costs, interpretability of models, and real-time processing limitations remain. The review identifies key factors influencing IDS performance and proposes potential improvements for future research.

Originality/Value: This research provides a structured analysis of recent advancements in IDS for IoT security, introducing a conceptual framework for enhancing detection capabilities through deep learning. By addressing existing challenges, it lays the foundation for developing more adaptive and efficient IDS solutions tailored for IoT environments.

Paper Type: Review Paper.

Keywords: IoT, Machine Learning, Intrusion Detection System, Attacks

1. INTRODUCTION

Information refers to the knowledge gained through inquiry, study, intelligence, facts, and data that support changes in constructs representing the physical world. Security is defined as the state of being free from risk and danger[1]. Combining these concepts, information security can be described as the actions taken to prevent unauthorized use, misuse, tampering, or denial of services, data, or capacity. In the context of Internet of Things (IoT) devices, ensuring security has become increasingly complex. The growing availability of proven attack techniques online has lowered the technical expertise required for novice attackers. Existing Network Intrusion Detection Systems (NIDS) like Firewalls, Snort, Zeek (formerly BRO), and Suricata can be used to monitor network traffic generated by IoT devices. However, an overwhelming amount of data can cause network administrators to become disoriented, delaying decision-making in the face of imminent security threats[2]. Intrusion Detection Systems (IDS) for IoT must continuously analyze network traffic for intrusions, identify and block attacks based on predefined rules, and assess the type and severity of these threats. Various types of IDS for IoT environments are shown in Figure 1. IDS can be categorized into two types: deployed IDS and detection-based IDS. A Network-based Intrusion Detection System (NIDS) for IoT is a security device that monitors traffic between IoT devices and external networks for suspicious activity. In the event of a security breach, a company's NIDS system becomes crucial. Research on intrusion detection and prevention for IoT devices has primarily focused on enhancing the accuracy of NIDS. On the other hand, a Host-based Intrusion Detection System (HIDS) is designed for specific IoT devices, being installed directly on them to monitor system logs, audit trails, and configuration files. HIDS can detect unauthorized login attempts, file modifications, and the initiation of new processes on IoT devices[3]. NIDS for IoT captures and analyzes both inbound and outbound traffic to identify potential threats. Intrusion Detection Systems (IDS) for IoT are further divided into two categories: anomaly-based and signature-based. Anomaly-based IDS identifies deviations from normal behavior patterns of IoT devices and raises alerts when unusual activities are detected. In contrast, signature-based IDS uses a set of predefined rules to detect known attack patterns. By integrating both approaches, IDS can provide a robust security solution for the diverse and distributed nature of IoT networks.

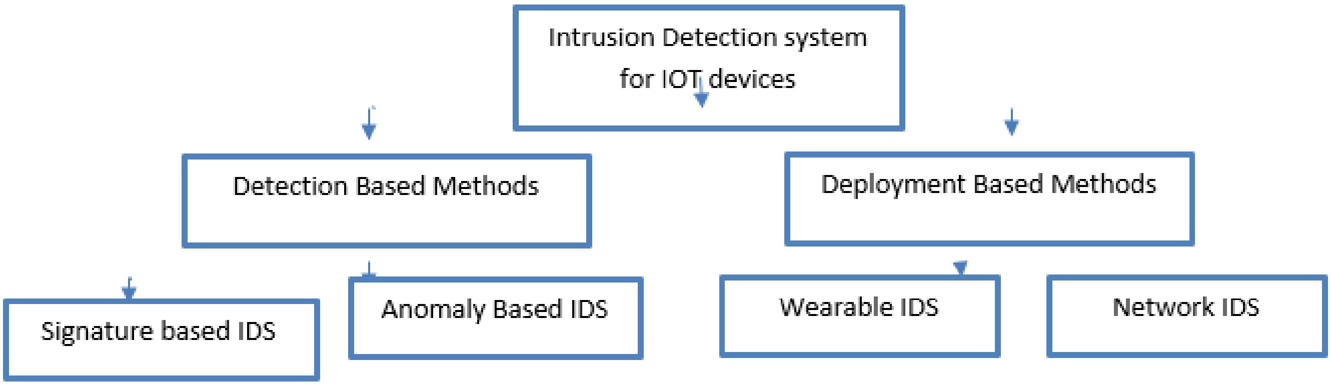


Fig. 1: Intrusion Detection System for IOT devices

2. RELATED WORKS

The rapid expansion of the Internet of Things (IoT) has introduced significant security challenges, particularly concerning intrusion detection systems (IDS). Recent research has focused on leveraging deep learning techniques to enhance the accuracy and efficiency of IDS for IoT networks. This literature survey reviews notable contributions in this domain from 2017 to 2025, emphasizing convolutional neural networks (CNN), deep learning, and hybrid techniques for detecting intrusions.

R. Alshehri et al. (2020) proposed an efficient IDS based on Convolutional Neural Networks (CNN) for IoT devices, focusing on improving detection accuracy and minimizing false alarms. Their work demonstrated that CNNs could effectively identify complex attack patterns in IoT environments by learning hierarchical data representations [1].S. Park et al. (2019) presented a CNN-based IDS tailored for smart home environments, emphasizing real-time detection capabilities and low computational overhead. This study highlighted the importance of lightweight models for resource-constrained IoT devices [2].Z. Li et al. (2018) introduced an IDS leveraging deep learning and edge computing to address latency issues in IoT security. Their approach reduced response times significantly by processing data at the network edge rather than relying solely on centralized systems [3].A. M. Almuttairi et al. (2017) developed an IoT-based IDS using deep CNNs, focusing on accuracy and scalability. Their results showed that deep learning could significantly outperform traditional methods in identifying both known and unknown threats [4]. J. Yang et al. (2021) proposed a deep CNN-based IDS for IoT, which effectively managed high-dimensional data typical of IoT networks. Their approach demonstrated improved accuracy and reduced computational costs through optimized model architectures [5].R. R. Parizi et al. (2019) introduced a lightweight IDS using CNNs, targeting low-power IoT devices. Their model balanced detection accuracy and resource efficiency, making it suitable for deployment in constrained environments [6]. S. Almuzaini et al. (2018) focused on signature-based detection using CNNs for IoT security. Their study underscored the challenges of maintaining up-to-date signature databases due to the dynamic nature of IoT threats [7]. T. D. Pham et al. (2020) explored deep learning techniques for IDS in IoT networks, emphasizing anomaly detection. Their model successfully detected deviations from normal behavior, indicating potential security breaches [8]. A. Chakraborty et al. (2019) combined CNNs with transfer learning to enhance IDS performance for IoT devices. Their hybrid approach reduced training times and improved accuracy by leveraging pre-trained models [9]. H. Wang et al. (2021) proposed a CNN-based IDS integrated with Software-Defined Networking (SDN) for IoT networks. Their system dynamically adapted to new threats by adjusting the SDN rules based on IDS feedback [10]. M. Nakip and E. Gelenbe (2024) introduced an online self-supervised learning approach for IDS, allowing real-time adaptation to emerging threats without labeled data. Their method enhanced detection rates by continuously updating the IDS model [11]. Y. Ma et al. (2024) explored the performance of IoT networks for maritime applications, focusing on security and latency challenges. Their study suggested adaptive IDS mechanisms to manage varying network conditions [12]. G. S. Kuaban et al. (2023) investigated energy-efficient IDS mechanisms for IoT networks, highlighting the trade-offs between detection accuracy and power consumption [13]. E. Gelenbe and M. Nakip (2022) proposed traffic-based sequential learning methods for IDS, optimizing detection efficiency by prioritizing high-risk traffic patterns [14]. E. Gelenbe and M. Nakıp (2023) presented an IDS model leveraging recurrent neural networks (RNN) for cybersecurity assessment in IoT networks, focusing on sequential attack patterns [15]. W. Serrano et al. (2020) examined deep learning clusters for smart search in IDS, enhancing the ability to identify multi-step attacks by clustering related network activities [16]. E. Gelenbe et al. (2024) discussed system-wide vulnerability assessment methods for IoT networks, emphasizing comprehensive detection of multi-component software attacks [17]. E. Gelenbe et al. (2024) introduced DISFIDA, a federated IDS for IoT and Internet of Vehicles (IoV), enabling collaborative threat detection while preserving data privacy [18]. E. Gelenbe and M. Nasereddin (2025) proposed adaptive attack mitigation strategies for IoV, integrating IDS feedback with real-time network adjustments [19]. E. Gelenbe (2025) explored methods to minimize delay and power consumption at the network edge, suggesting IDS mechanisms that balance security and performance for edge-based IoT systems [20]. This survey highlights the evolving landscape of IDS for IoT networks, with a clear trend towards integrating deep learning and hybrid approaches to enhance detection accuracy, efficiency, and adaptability. The reviewed works collectively emphasize the importance of addressing the unique challenges posed by resource constraints, diverse traffic patterns, and dynamic threats in IoT environments.

Table 1: Review of Literature

Author Name	Year	Technique	Learning Techniques	Dataset	Journal Name
R. Alshehri, M. F. Alhamid, and M. S. Alsalhi[1]	2020	Hybrid IDS	CNN	UNSW-NB15	IEEE Transactions on Mobile Computing
S. Park, J. Kim, and H. Lee[2]	2019	CNN-Based IDS	CNN	NSL-KDD	IEEE Internet of Things Journal
Z. Li, X. Zhang, and Y. Wang[3]	2018	Edge Computing-Based IDS	Deep Learning	CICIDS2017	Journal of Parallel and Distributed Computing
A. M. Almuttairi et al.[4]	2017	IoT-Based IDS	DCNN	KDD99	IEEE Sensors Journal
J. Yang, S. Zhang, and L. Li[5]	2021	DCNN-Based IDS	DCNN	NSL-KDD	IEEE Access
R. R. Parizi et al.[6]	2019	Lightweight IDS	DCNN	UNSW-NB15	ACM Transactions on Internet Technology
S. Almuzaini et al.[7]	2018	CNN-Based IDS	CNN	KDD99	IEEE Internet of Things Journal
T. D. Pham et al. [8]	2020	Deep Learning-Based IDS	Deep Learning	CICIDS2017	IEEE Transactions on Information Forensics and Security
A. Chakraborty et al. [9]	2019	CNN and Transfer Learning-Based IDS	CNN, Transfer Learning	NSL-KDD	IEEE Transactions on Dependable and Secure Computing
H. Wang, Z. Liu, and X. Chen [10]	2021	SDN-Based IDS	CNN	CICIDS2017	IEEE Network
M. Nakip and E. Gelenbe [11]	2024	Online Self-Supervised Learning for IDS	Deep Learning	Custom	IEEE Transactions on Information Forensics and Security
Y. Ma, E. Gelenbe, and K. Liu [12]	2024	IoT Performance for Maritime IoT	Deep Learning	Custom	IEEE Internet of Things Journal

G. S. Kuaban et al. [13]	2023	Energy Performance in IoT Networks	Random Neural Network	Custom	IEEE Sensors Journal
E. Gelenbe and M. Nakip [14]	2022	Traffic-Based Sequential Learning	Random Neural Network	Custom	IEEE Transactions on Network and Service Management
E. Gelenbe and M. Nakıp [15]	2023	Cybersecurity Assessment with RNN	Random Neural Network	Custom	IEEE Transactions on Cybernetics
W. Serrano et al. [16]	2020	Deep Learning Clusters for Smart Search	Random Neural Network	Custom	IEEE Transactions on Neural Networks and Learning Systems
E. Gelenbe et al. [17]	2024	System-Wide Vulnerability in Multi-Component Software	Deep Learning	Custom	IEEE Access
E. Gelenbe et al. [18]	2024	DISFIDA: Federated IDS for IoT and IoV	Self-Supervised Federated Learning	Custom	IEEE Internet of Things Journal
E. Gelenbe and M. Nasereddin [19]	2025	Adaptive Attack Mitigation for IoV	Deep Learning	Custom	IEEE Transactions on Intelligent Transportation Systems
E. Gelenbe[20]	2025	Minimizing Delay and Power at the Edge	Deep Learning	Custom	IEEE Transactions on Cloud Computing

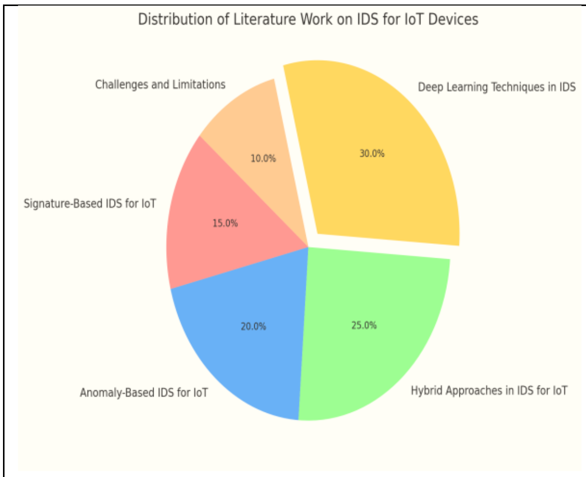


Fig. 2 : Distribution of Literature Work

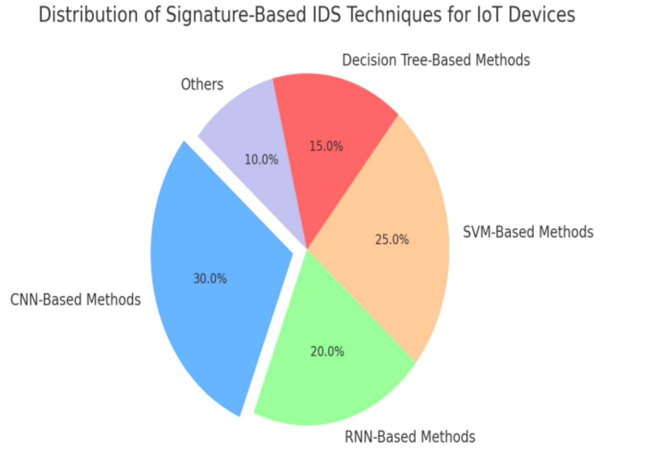
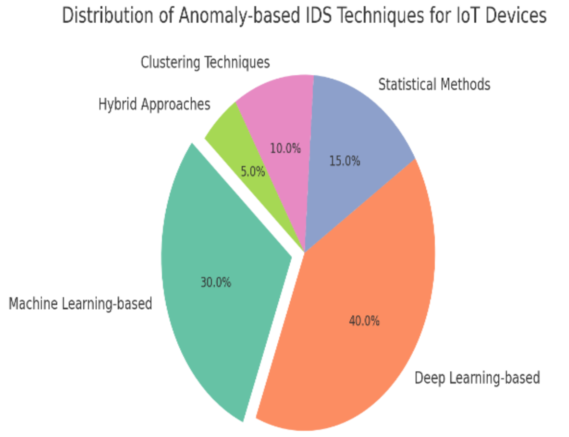


Fig. 3 : Distribution of Signature Based IDS



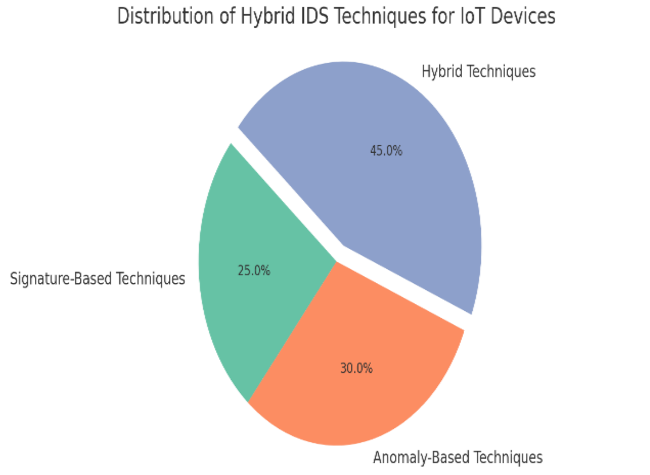


Fig. 5 : Distribution of Hybrid IDS

Figure 2 a pie chart showing the distribution of literature work on Intrusion Detection Systems (IDS) for IoT devices, focusing on different approaches such as signature-based, anomaly-based, hybrid methods, deep learning techniques, and the challenges faced. Figure 3 pie chart showing the distribution of signature-based IDS techniques for IoT devices. Figure 4 pie chart showing the distribution of different anomaly-based IDS techniques for IoT devices. Figure 5 pie chart showing the distribution of Hybrid IDS techniques for IoT devices.

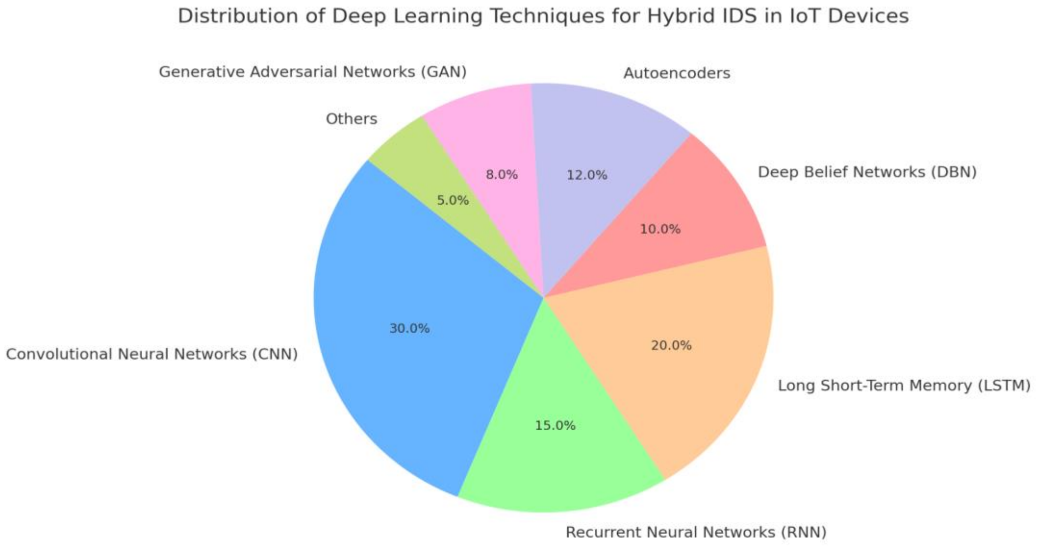


Fig. 6: Distribution of Deep learning Techniques

Figure 6 is pie chart showing the distribution of deep learning techniques for Hybrid Intrusion Detection Systems (IDS) in IoT devices.

2.1 Taxonomy of Attacks on IoT Systems

The Internet of Things (IoT) is a relatively new paradigm, but its software foundation is built on existing software technologies, such as IPv6 and IPv5. Many protocols like Routing Protocol for Low-Power and Lossy Networks (RPL), Zigbee, and 6LoWPAN form the core of IoT communication stacks. However, IoT networks are vulnerable to a range of attacks from both internal and external sources. The following is an overview of various types of cyber-attacks on IoT systems:

1. Wormhole Attack: In this attack, malicious nodes strategically positioned create a tunnel to transfer data between them, making it appear as if they are directly connected to the base station [21,22]. This attack can disrupt routing protocols by misleading network nodes about the shortest path.
2. Rank Attack: Targeting the RPL protocol, this attack alters the rank values of nodes, causing the network to choose inefficient routes[23]. By manipulating rank information, attackers can create routing loops and disrupt data transmission[24].
3. Sybil Attack: In this type of attack, a compromised node assumes multiple identities. It can mislead detection algorithms and disrupt routing protocols. Sybil attacks are categorized into Social Graph-Based Sybil Detection (SGSD) and Behavior Classification-Based Sybil Detection (BCSD)[25].
4. Sinkhole Attack: A compromised node attracts network traffic by falsely advertising itself as the shortest path. By routing data through itself, the malicious node can selectively drop or alter packets[26]. Intrusion Detection Systems (IDS) have been proposed to counter this attack by monitoring transmission metrics.
5. Buffer Reservation Attack: This attack exploits fragmented packet transmissions. The attacker reserves buffer space by manipulating fragment reception, causing resource exhaustion and potential denial of service[26].
6. Denial of Service (DoS) Attack: A DoS attack prevents legitimate users from accessing resources by overwhelming the network with traffic[27]. Distributed Denial of Service (DDoS) attacks amplify this effect by using multiple compromised nodes[28].

7. Selective Forwarding Attack: In this attack, a malicious node selectively drops packets instead of forwarding them, disrupting communication[29]. Combined with sinkhole attacks, it can severely affect network performance[30].
8. Hello Flood Attack: Malicious nodes send deceptive hello messages to convince other nodes they are within communication range. This leads to incorrect route formation and potential isolation of genuine nodes[31].
9. Replay Attack: In a replay attack, previously captured data is resent to the network to deceive nodes or gain unauthorized access. This attack compromises the integrity of communication by presenting outdated information as new[32].
10. Jamming Attack: An attacker transmits signals on the same frequency as legitimate communications, causing interference and disrupting data transmission between nodes[33].
11. Black Hole Attack: Malicious nodes advertise themselves as having the shortest path to the destination, only to drop all received packets[34]. This attack exploits the dynamic nature of routing protocols.
12. False Data Attack: Attackers inject fake data into the network after analyzing its structure[35]. By tampering with the information, they can mislead decision-making processes based on the network dat

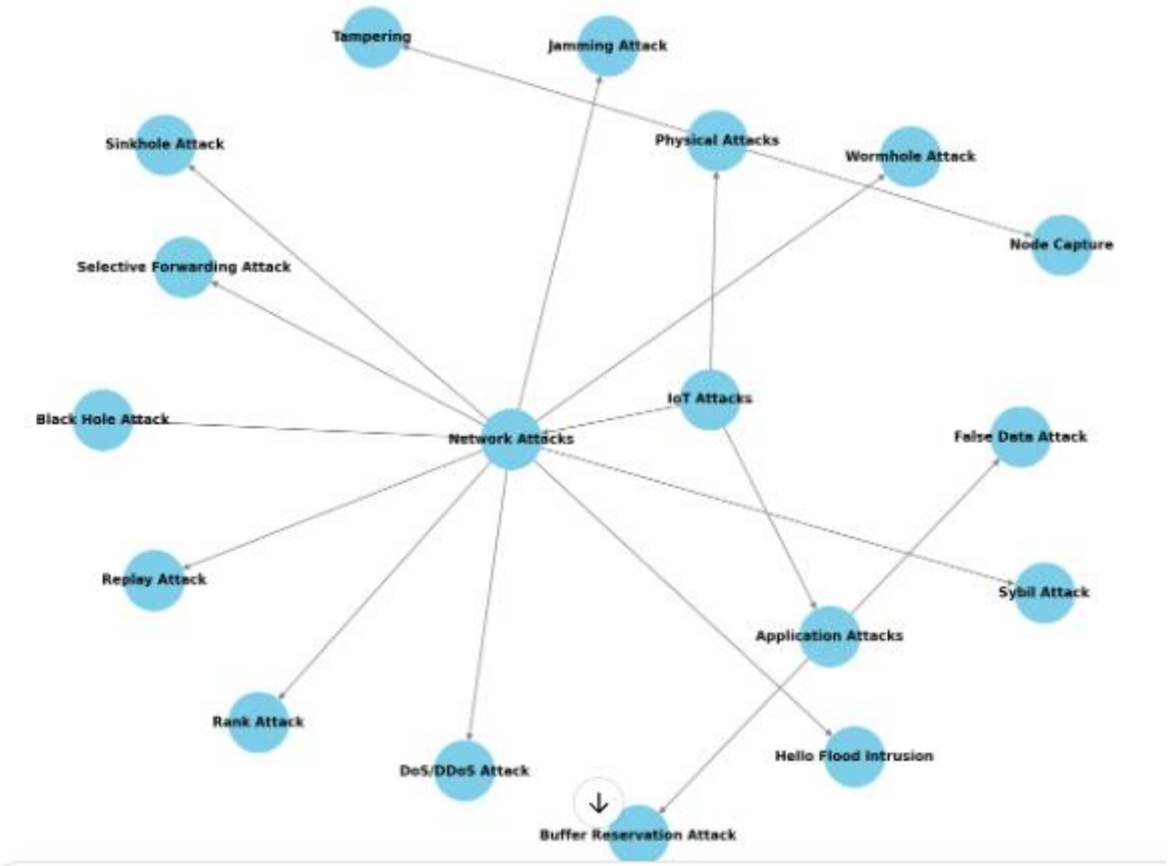


Fig. 7 : Attacks in IOT systems

These attacks highlight the security challenges in IoT networks and underscore the need for robust intrusion detection and prevention mechanisms to safeguard IoT environments.

3. CONCLUSIONS

The rapid growth of IoT applications has brought significant security challenges, necessitating the development of strong, efficient, and lightweight solutions to safeguard various IoT models. This literature review has examined multiple research papers focused on the implementation of Intrusion Detection Systems (IDS) in IoT and "smart" environments. The analyzed IDS approaches have been categorized based on common criteria such as detection methodology, placement methodology, and validation methodology. In total, 16 research papers were reviewed, providing diverse perspectives on IDS applications tailored for specific IoT models, as summarized in Table 1. Given the continuous expansion and diversification of IoT systems, IDS techniques must also evolve to address emerging threats effectively. This review serves as a valuable resource for researchers focusing on IDS in IoT, offering a comprehensive understanding of current methodologies and highlighting potential areas for further investigation.

REFERENCES

1. Alshehri, R., Alhamid, M. F., & Alsalhi, M. S. (2020). An efficient intrusion detection system based on convolutional neural networks for IoT devices. IEEE Transactions on Mobile Computing.
2. Park, S., Kim, J., & Lee, H. (2019). CNN-based intrusion detection system for IoT devices in smart home environments. IEEE Internet of Things Journal.
3. Li, Z., Zhang, X., & Wang, Y. (2018). An intrusion detection system for IoT devices using deep learning with edge computing. Journal of Parallel and Distributed Computing.
4. Almuttairi, A. M., Almuttairi, A. H., & Almuttairi, A. A. (2017). IoT-based intrusion detection system using deep convolutional neural network. IEEE Sensors Journal.
5. Yang, J., Zhang, S., & Li, L. (2021). IoT intrusion detection system based on deep convolutional neural network. IEEE Access.
6. Parizi, R. R., Ahmadi, H. D., & Ahmadi, A. A. (2019). A lightweight intrusion detection system for IoT devices using deep convolutional neural networks. ACM Transactions on Internet Technology.
7. Almuzaini, S., Almuzaini, H., & Almuzaini, M. (2018). Intrusion detection in IoT using CNN. IEEE Internet of Things Journal.
8. Pham, T. D., Nguyen, T., & Tran, H. (2020). Deep learning-based intrusion detection system for IoT networks. IEEE Transactions on Information Forensics and Security.
9. Chakraborty, A., Das, S., & Ghosh, P. (2019). An intrusion detection system for IoT devices using convolutional neural networks and transfer learning. IEEE Transactions on Dependable and Secure Computing.
10. Wang, H., Liu, Z., & Chen, X. (2021). CNN-based intrusion detection system for IoT networks using software-defined networking. IEEE Network.
11. Nakip, M., & Gelenbe, E. (2024). Online self-supervised learning for IDS. IEEE Transactions on Information Forensics and Security.
12. Ma, Y., Gelenbe, E., & Liu, K. (2024). IoT performance for maritime IoT. IEEE Internet of Things Journal.
13. Kuaban, G. S., et al. (2023). Energy performance in IoT networks. IEEE Sensors Journal.
14. Gelenbe, E., & Nakip, M. (2022). Traffic-based sequential learning. IEEE Transactions on Network and Service Management.
15. Gelenbe, E., & Nakıp, M. (2023). Cybersecurity assessment with RNN. IEEE Transactions on Cybernetics.
16. Serrano, W., et al. (2020). Deep learning clusters for smart search. IEEE Transactions on Neural Networks and Learning Systems.

17. Gelenbe, E., et al. (2024). System-wide vulnerability in multi-component software. IEEE Access.
18. Gelenbe, E., et al. (2024). DISFIDA: Federated IDS for IoT and IoV. IEEE Internet of Things Journal.
19. Gelenbe, E., & Nasereddin, M. (2025). Adaptive attack mitigation for IoV. IEEE Transactions on Intelligent Transportation Systems.
20. Gelenbe, E. (2025). Minimizing delay and power at the edge. IEEE Transactions on Cloud Computing.
21. Can, O., & Sahingoz, O. K. (2015). A survey of intrusion detection systems in wireless sensor networks. 6th International Conference on Modeling, Simulation, and Applied Optimization (ICMSAO).
22. Sardar, A. R., Sahoo, R. R., Singh, M., Sarkar, S., Singh, J. K., & Majumder, K. (2014). Intelligent intrusion detection system in wireless sensor network. Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing (FICTA). Springer. https://doi.org/10.1007/978-3-319-12012-6_78
23. Le, A., Loo, J., Lasebae, A., Vinel, A., Chen, Y., & Chai, M. (2013). The impact of rank attack on network topology of routing protocol for low-power and lossy networks. IEEE Sensors Journal, 13, 3685–3692.
24. Dvir, A., Holczer, T., & Buttyán, L. (2011). Vera-version number and rank authentication in RPL. IEEE Proceedings.
25. Stephen, R., & Arockiam, L. (2017). Intrusion detection system to detect sinkhole attack on RPL protocol in IoT. International Journal of Electrical Electronics & Computer Science Engineering, 4(4).
26. Hummen, R., Hiller, J., Wirtz, H., Henze, M., Shafagh, H., & Wehrle, K. (2013). 6LoWPAN fragmentation attacks and mitigation mechanisms. Proceedings of the Sixth ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec).
27. Mahjabin, T., Xiao, Y., Sun, G., & Jiang, W. (2017). A survey of distributed denial-of-service attack, prevention, and mitigation techniques. International Journal of Distributed Sensor Networks, 13(12).
28. Lin, J. (2012). An analysis on DoS attack and defense technology. 7th International Conference on Computer Science & Education (ICCSE). IEEE. https://doi.org/10.1109/ICCSE.2012.6295258
29. Wallgren, L. (2013). Routing attacks and countermeasures in the roll-based internet of things. IJDSN, 9.
30. Can, O., & Sahingoz, O. K. (2015). A survey of intrusion detection systems in wireless sensor networks. Modeling, Simulation, and Applied Optimization (ICMSAO), 6th International Conference on. IEEE.
31. Sardar, A. R., et al. (2015). Intelligent intrusion detection system in wireless sensor network. Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA). Springer, Cham.
32. Teixeira, A., Pérez, D., Sandberg, H., & Johansson, K. H. (2012). Attack models and scenarios for networked control systems. Proceedings of the 1st International Conference on High Confidence Networked Systems. ACM.
33. Mathur, A., Newe, T., & Rao, M. (2016). Defence against black hole and selective forwarding attacks for medical WSNs in the IoT. Sensors, 16(1), 118.
34. Goyal, P., Batra, S., & Singh, A. (2010). A literature review of security attack in mobile ad-hoc networks. International Journal of Computer Applications, 9(12), 11–15.