Seminars in Medical Writing and Education. 2024; 3:552
doi: 10.56294/mw2024552

ORIGINAL

Exploring Intrusion Detection Systems (IDS) in IoT Environments

Explorando los sistemas de detección de intrusiones (IDS) en entornos de IoT

Amit Kumar Dinkar[1] ✉, Ajay Kumar Choudhary[2]

[1]Department of Computer Science, Veer Kunwar Singh University. Ara- 802301, India.
[2]Department of Physics, G. B. College. Ramgarh.

Cite as: Dinkar AK, Choudhary AK. Exploring Intrusion Detection Systems (IDS) in IoT Environments. Seminars in Medical Writing and Education. 2024; 3:552. https://doi.org/10.56294/mw2024552

Submitted: 17-11-2023 **Revised:** 06-02-2024 **Accepted:** 24-04-2024 **Published:** 25-04-2024

Editor: PhD. Prof. Estela Morales Peralta

Corresponding author: Amit Kumar Dinkar ✉

ABSTRACT

Introduction: the Internet of Things (IoT) has revolutionized numerous sectors, such as home automation, healthcare, and industrial operations, by enabling interconnected devices to facilitate automation, real-time data analysis, and intelligent decision-making. Despite its transformative potential, the rapid proliferation of IoT has introduced critical cybersecurity challenges due to the heterogeneous and fragmented nature of IoT environments.
Objective: IoT networks consist of diverse devices with varying capabilities and protocols, making the implementation of standardized security measures complex.
Method: traditional approaches, including encryption, authentication, and access control, often fall short in addressing evolving cyber threats. Intrusion Detection Systems (IDS) tailored to IoT offer a promising solution, enabling real-time monitoring, anomaly detection, and attack prevention.
Result: however, the resource constraints of IoT devices and diverse architectures pose significant design challenges for IDS. Future advancements should focus on lightweight, adaptive IDS models leveraging machine learning, artificial intelligence, and blockchain technologies to enhance security frameworks. Collaboration among researchers, industry, and policymakers is essential to develop scalable solutions, ensuring IoT ecosystems remain secure and efficient in combating cyber threats.
Conclusions: this paper reviews IoT security fundamentals, evaluates IDS solutions, and highlights key challenges, offering directions for future research to improve IoT cybersecurity through innovative strategies.

Keywords: IoT; Intrusion Detection System; Cybercrime.

RESUMEN

Introducción: el Internet de las cosas (IoT) ha revolucionado numerosos sectores, como la automatización del hogar, la atención médica y las operaciones industriales, al permitir que dispositivos interconectados faciliten la automatización, el análisis de datos en tiempo real y la toma de decisiones inteligente. A pesar de su potencial transformador, la rápida proliferación de IoT ha introducido desafíos críticos de ciberseguridad debido a la naturaleza heterogénea y fragmentada de los entornos de IoT.
Objetivo; Las redes de IoT constan de diversos dispositivos con diferentes capacidades y protocolos, lo que hace que la implementación de medidas de seguridad estandarizadas sea compleja.
Método: los enfoques tradicionales, incluido el cifrado, la autenticación y el control de acceso, a menudo no logran abordar las amenazas cibernéticas en evolución. Los sistemas de detección de intrusiones (IDS) adaptados a IoT ofrecen una solución prometedora que permite la supervisión en tiempo real, la detección de anomalías y la prevención de ataques.

Resultado: sin embargo, las limitaciones de recursos de los dispositivos IoT y las diversas arquitecturas plantean importantes desafíos de diseño para IDS. Los avances futuros deberían centrarse en modelos IDS ligeros y adaptables que aprovechen el aprendizaje automático, la inteligencia artificial y las tecnologías blockchain para mejorar los marcos de seguridad. La colaboración entre investigadores, industria y formuladores de políticas es esencial para desarrollar soluciones escalables, garantizando que los ecosistemas de IoT sigan siendo seguros y eficientes en la lucha contra las amenazas cibernéticas.
Conclusiones: este documento revisa los fundamentos de seguridad de IoT, evalúa las soluciones IDS y destaca los desafíos clave, ofreciendo direcciones para futuras investigaciones para mejorar la ciberseguridad de IoT a través de estrategias innovadoras.

Palabras clave: LoT; Sistema de Detección de Intrusos; Cibercrimen.

INTRODUCTION

The Internet of Things (IoT) is an emerging paradigm that has revolutionized various domains, including home automation, industrial operations, healthcare, and environmental monitoring.[1] By enabling seamless connectivity among devices, IoT facilitates automation, real-time data processing, and smart decision-making.[2] However, despite its advantages, the rapid expansion of IoT has also introduced significant cybersecurity threats. The interconnected nature of IoT devices increases vulnerability to cyberattacks, making security a critical concern. One of the major challenges in securing IoT networks is their heterogeneous and fragmented nature, which complicates the development of standardized security mechanisms. Unlike traditional networks, IoT environments comprise diverse devices with varying capabilities, operating systems, and communication protocols, making it difficult to implement uniform security measures.[3]Various security solutions have been proposed to enhance IoT safety, including encryption techniques for data confidentiality, authentication mechanisms to verify device identity, access control policies within IoT networks, and trust management frameworks to protect user privacy. However, these existing approaches are often insufficient in mitigating the ever-evolving threats that target IoT infrastructures. To address these challenges, the development of more robust and adaptive security tools is essential. One promising approach is the use of Intrusion Detection Systems (IDS) specifically designed for IoT networks. IDS can monitor network traffic, detect anomalies, and prevent potential attacks by identifying malicious activities in real time.[4] While IDS solutions have been widely used in traditional networks, their direct application to IoT is limited due to the unique characteristics of IoT environments. The constrained computational resources of IoT devices, diverse network architectures, and the wide range of protocol stacks and standards create additional obstacles in designing effective IDS solutions for IoT.

The need for advanced IDS frameworks tailored to IoT is crucial to ensuring cybersecurity in interconnected environments. Future research should focus on developing lightweight, scalable, and adaptive IDS models that can efficiently operate in resource-constrained IoT devices.[5] Machine learning and artificial intelligence (AI)-based IDS approaches could play a significant role in enhancing threat detection capabilities by learning from attack patterns and adapting to new threats dynamically. Additionally, integrating blockchain technology into IoT security frameworks may help establish decentralized and tamper-resistant security models, further strengthening defense mechanisms.[6] As IoT continues to evolve, addressing cybersecurity challenges remains a priority. The future of IoT security lies in a collaborative effort among researchers, industry experts, and policymakers to establish comprehensive security frameworks. By leveraging innovative technologies such as AI, blockchain, and cloud-based security solutions, IoT ecosystems can achieve enhanced protection against cyber threats while maintaining their efficiency and functionality.

This paper is structured as follows: Section II introduces fundamental concepts related to IoT security and IDS. Section III presents a literature review analyzing previous research on IDS solutions tailored for IoT environments. Finally, Section IV concludes with key insights, discusses unresolved challenges, and suggests future research directions to improve IoT security.

Literature review

The reviewed literature highlights various approaches to Intrusion Detection Systems (IDS) in IoT environments, including deep learning, blockchain integration, federated learning, hybrid detection models, and cloud-based solutions. These methods contribute significantly to IoT security but also present unique challenges such as computational complexity, data privacy concerns, scalability issues, and real-time processing limitations. Among these approaches, machine learning-based IDS and deep learning-enhanced solutions have shown promising results in improving detection accuracy. However, they often require large datasets and high computational power, making them less suitable for constrained IoT devices. Blockchain-integrated IDS provides decentralized security, but its high latency and scalability remain barriers to practical deployment. Federated learning and

cloud-based IDS offer distributed processing advantages, though they introduce communication overhead and cloud security risks.

Table 1. Design and main results of the analyzed studies

Study	Methodology	Key Contributions	Limitations
Al-Hawawreh et al. (2020)[7]	Deep learning-based IDS for IoT	Developed an IDS using convolutional neural networks (CNNs) and long short-term memory (LSTM) for real-time attack detection.	High computational cost and limited applicability in resource-constrained IoT devices.
Sharma et al. (2021)[8]	Blockchain-integrated IDS	Proposed a decentralized IDS using blockchain for secure data sharing among IoT devices.	High latency due to blockchain overhead and scalability concerns.
Raza et al. (2019)[9]	Lightweight anomaly detection IDS	Designed an energy-efficient IDS for IoT using rule-based anomaly detection.	Limited detection accuracy for complex attacks.
Mukherjee et al. (2020)[10]	Machine learning-based IDS	Used Random Forest and Support Vector Machine (SVM) classifiers to enhance intrusion detection efficiency.	Requires large labeled datasets for training and validation.
Liu et al. (2022)[11]	Federated learning approach for IDS	Implemented a collaborative IDS where IoT nodes contribute to the detection model without centralized data storage.	Increased communication overhead and security risks associated with federated learning.
Kaur et al. (2021)[12]	Hybrid IDS combining anomaly and signature-based detection	Integrated a hybrid approach that detects both known and unknown threats efficiently.	Higher computational complexity and resource consumption.
Ahmed et al. (2020)[13]	Cloud-based IDS for IoT	Implemented an IDS that offloads computational tasks to the cloud, reducing the burden on IoT devices.	Increased dependency on internet connectivity and cloud security concerns.
Singh et al. (2019)[14]	Game theory-based IDS	Developed an IDS that uses game theory to predict and mitigate cyber threats in IoT networks.	High complexity in strategy formulation and practical implementation challenges.
Kumar et al. (2021)[15]	Deep reinforcement learning for IDS	Applied reinforcement learning to dynamically adapt IDS responses to evolving attack patterns.	Requires significant training time and lacks explainability in decision-making.
Zhang et al. (2022)[16]	Quantum computing-enhanced IDS	Explored the potential of quantum computing to enhance IDS processing speed and detection accuracy.	Still in experimental stages with high implementation costs.

Research On Intrusion Detection Systems (IDS) In IOT

The exploration of Intrusion Detection Systems (IDS) within the Internet of Things (IoT) has led to the adoption of various techniques, primarily leveraging machine learning (ML) and deep learning (DL) models. Researchers have categorized IDS methodologies based on their algorithmic approaches and areas of specialization.[17] Ensemble learning methods, such as AdaBoost and Random Forest (RF), have proven highly effective in strengthening network security by combining multiple classifiers. These approaches have demonstrated impressive accuracy when tested on datasets like WSN-DS and UNSW-NB15, which contain diverse attack scenarios. Deep learning architectures, including Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) models, have emerged as powerful tools in detecting cyber threats.[5] Hybrid models like CNN-BiLSTM and LSTM-based frameworks excel in extracting complex patterns from large-scale datasets such as N-BaIoT and BoT-IoT.[18] These models achieve exceptional detection rates by learning temporal dependencies in network traffic, enhancing the precision of anomaly detection. Traditional machine learning models, including automated ML and Naïve Bayes, remain relevant for IoT security due to their efficiency and computational simplicity. In scenarios where rapid threat detection is critical, these models provide reliable results, particularly when applied to datasets like KDDcup99. The continuous advancement of IDS methodologies ensures enhanced security frameworks, adapting to the evolving landscape of IoT-based cyber threats.[19]

METHOD

Dataset and evaluation metrics

The development of Intrusion Detection System (IDS) datasets for the Internet of Things (IoT) has played a crucial role in advancing cybersecurity research. Over the years, researchers have introduced multiple datasets to address the growing security challenges in IoT environments.[5] A timeline of dataset releases from 2015 to 2023 highlights the increasing efforts to strengthen IDS frameworks. The foundation for modern IDS research began in 2015 with the release of two significant datasets—UNSW-NB15 and KDDCUP99—both widely utilized

for evaluating network intrusion detection models. These datasets provided benchmark data for detecting anomalies and classifying attacks in conventional and IoT-driven networks. In 2016, the WSN-DS dataset was introduced, focusing on wireless sensor network security, followed by CICIDS2017 in 2017, which aimed at improving intrusion detection with realistic network traffic simulations. The evolution continued in 2018 with the N-BaIoT dataset, which specifically addressed security threats targeting IoT botnets. Interestingly, 2019 did not see the introduction of any major IDS datasets, possibly due to researchers refining existing datasets rather than developing new ones. However, 2020 marked a turning point with a surge in dataset releases, including ToN-IoT, BoT-IoT, and IoTID20. These datasets enriched the field by covering a broader range of cyber threats, from IoT-specific attacks to botnet-driven intrusions. In 2021, datasets such as SIMARGL and AS-IDS were introduced, expanding the scope of IDS research by incorporating new attack vectors and security challenges in IoT networks. The following year, 2022, saw the release of Seven CPS-specific and CIC-MalMem-2022, which provided insights into cyber-physical systems (CPS) and malware detection in memory-constrained environments. The most recent addition, UNR-IDD, was released in 2023, representing the latest efforts to enhance intrusion detection for IoT infrastructures.

Dataset

The dataset contains 1 048 576 rows and 47 columns, providing a substantial amount of data for analysis. The summary statistics reveal key insights into the numeric features, while the distribution of the target variable (label) indicates the prevalence of different attack types.[20]

Distribution of Flow Durations Across Different Attack Types

The Distribution of Flow Durations by Attack Type refers to a statistical analysis and visualization that examines how the durations of network flows vary across different types of attacks in a dataset. In a boxplot (or similar visualization), the distribution of flow durations is represented for each attack type. Analyzing the distribution of flow durations by attack type helps network security professionals understand the behavior of different attacks, identify potential threats, and develop strategies for detection and mitigation. It can also assist in tuning security systems to better respond to specific types of attacks based on their characteristics.

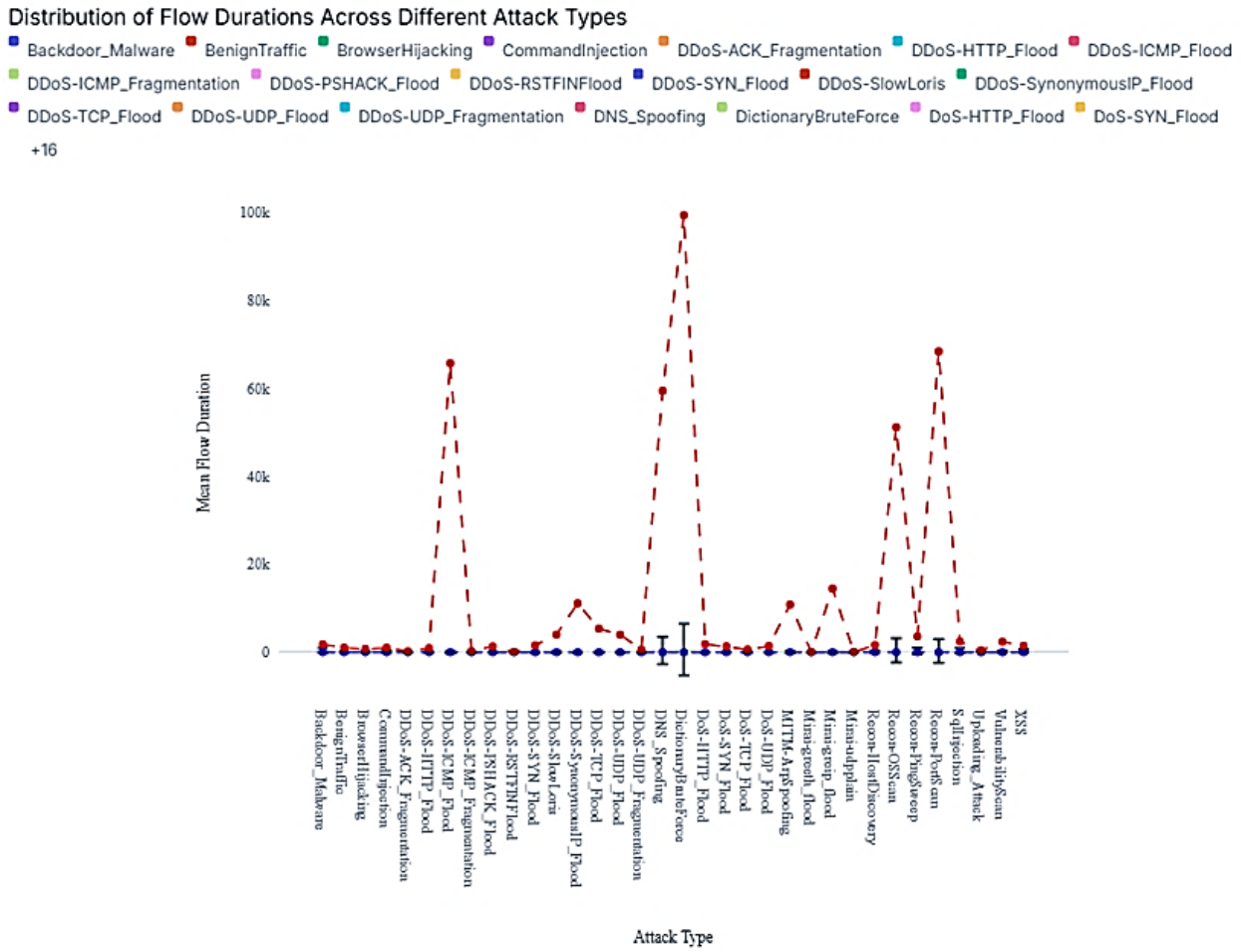

Figure 1. Distribution of Flow Durations Across Different Attack Types[20]

https://doi.org/10.56294/mw2024552

The correlation and standard deviation calculations were successfully executed, and the results are now available for review. The correlation between the number of flags set and the total size of packets for each attack type has been computed, along with the standard deviation of packet sizes for each attack type. The correlation results will help you understand how the number of flags set relates to the total size of packets for different attack types, while the standard deviation provides insight into the variability of packet sizes across these attacks as shown in figure 2 and figure 3.

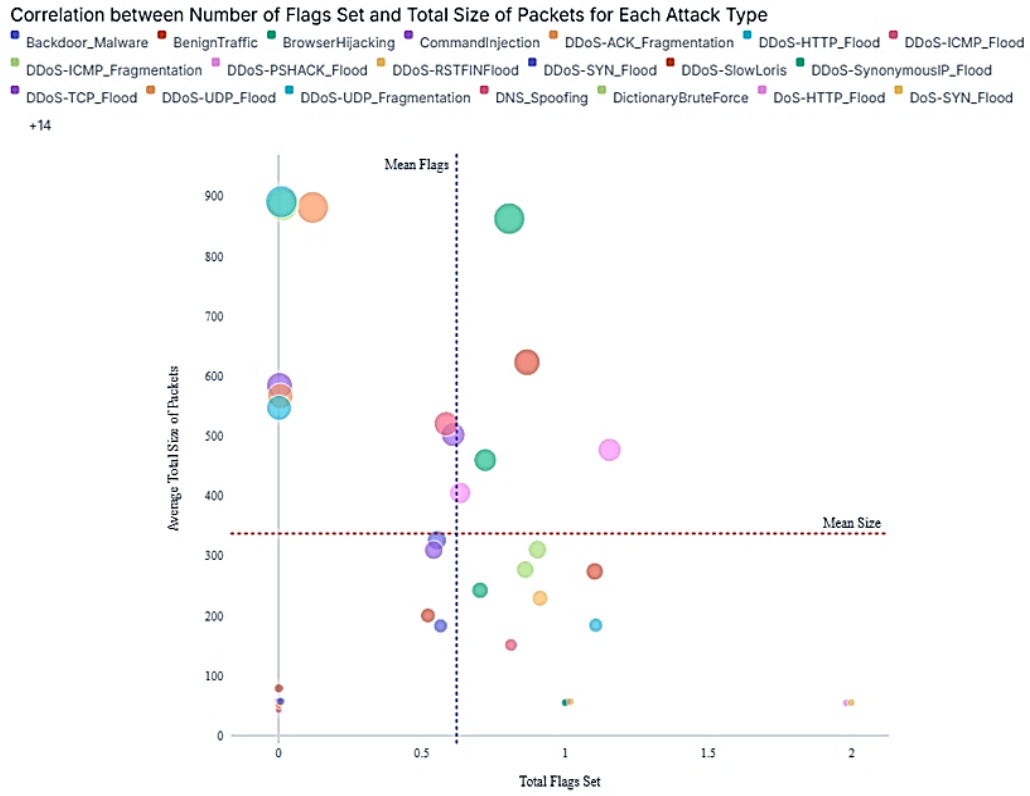

Figure 2. Correlation between the number of flags set and the total size of packets for each attack type[20]

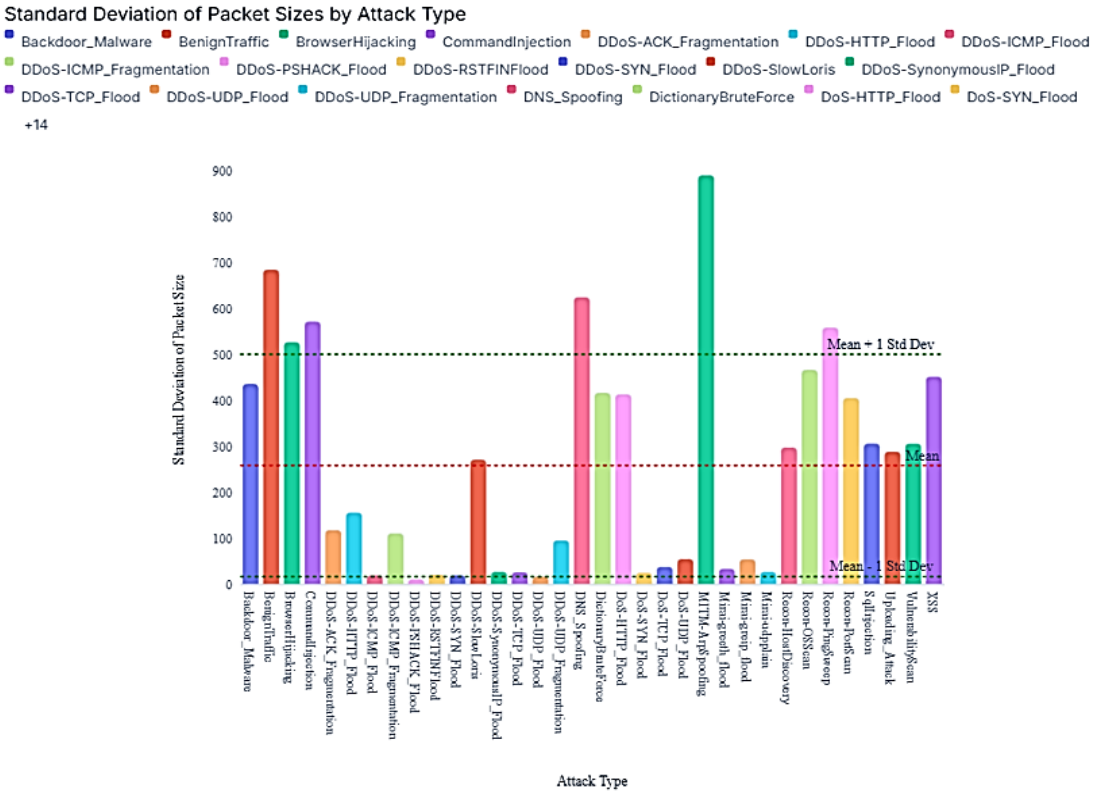

Figure 3. standard deviation of packet sizes by attacks type[20]

https://doi.org/10.56294/mw2024552

CONCLUSION

The rapid proliferation of the Internet of Things (IoT) has introduced significant security challenges, necessitating the development of advanced intrusion detection systems (IDS). Current IDS frameworks face several limitations, including a lack of IoT-specific datasets, inefficiencies in model design, and an absence of standardized evaluation metrics. Existing datasets often fail to reflect the diverse and dynamic nature of IoT environments, with issues such as class imbalances hindering the creation of robust IDS solutions. Furthermore, integrating complex machine learning models into resource-constrained IoT devices presents significant computational challenges. To address these issues, effective evaluation methodologies must simultaneously consider accuracy, computational cost, and adaptability. Although deep learning techniques hold considerable promise, their potential within IoT contexts remains underexplored. Privacy concerns and vulnerabilities to adversarial attacks further complicate the deployment of IDS, underscoring the need for innovative solutions.

One key challenge lies in feature engineering, where balancing feature selection and extraction techniques remains unresolved. A unified approach could streamline research efforts and enhance model performance. Future studies should focus on creating comprehensive IoT-specific datasets that capture the heterogeneity of devices, communication protocols, and contemporary cyber threats. These datasets must represent real-world complexities to enable the development of reliable IDS solutions. Another critical area for exploration is optimizing lightweight, energy-efficient IDS models. Such models must balance computational efficiency with detection accuracy, making them suitable for deployment on IoT devices with limited resources. The establishment of standardized benchmarks that reflect real-world IoT scenarios is equally important to ensure consistent evaluation and comparison of IDS models. Lastly, prioritizing holistic evaluation approaches that integrate multiple factors—accuracy, adaptability, and energy efficiency—will address the unique challenges of IoT environments. By resolving these challenges, researchers can pave the way for more secure, effective, and practical IDS solutions tailored to IoT ecosystems.

REFERENCES

1. Vaigandla K, Azmi N, Karne R. Investigation on intrusion detection systems (IDSs) in IoT. Int J Emerg Trends Eng Res. 2022;10(3).

2. Md Alimul Haque, Shameemul Haque KK and NKS. Digital Transformation and Challenges to Data Security and Privacy [Internet]. Anunciação PF, Pessoa CRM, Jamil GL, editors. Digital Transformation and Challenges to Data Security and Privacy. IGI Global; 2021. (Advances in Information Security, Privacy, and Ethics). Available from: http://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/978-1-7998-4201-9

3. Almrezeq N, Haque MA, Haque S, El-Aziz AAA. Device Access Control and Key Exchange (DACK) Protocol for Internet of Things. Int J Cloud Appl Comput [Internet]. 2022 Jan;12(1):1–14. Available from: https://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/IJCAC.297103

4. Hossain MA, Haque MA, Ahmad S, Abdeljaber HAM, Eljialy AEM, Alanazi A, et al. AI-enabled approach for enhancing obfuscated malware detection: a hybrid ensemble learning with combined feature selection techniques. Int J Syst Assur Eng Manag [Internet]. 2024; Available from: https://doi.org/10.1007/s13198-024-02294-y

5. Rahman MM, Shakil S Al, Mustakim MR. A survey on intrusion detection system in IoT networks. Cyber Secur Appl [Internet]. 2025;3:100082. Available from: https://www.sciencedirect.com/science/article/pii/S2772918424000481

6. Elrawy MF, Awad AI, Hamed HFA. Intrusion detection systems for IoT-based smart environments: a survey. J Cloud Comput. 2018;7(1):1–20.

7. Al-Hawawreh M, Moustafa N, Garg S, Hossain MS. Deep learning-enabled threat intelligence scheme in the internet of things networks. IEEE Trans Netw Sci Eng. 2020;8(4):2968–81.

8. Sahu AK, Sharma S, Tanveer M, Raja R. Internet of Things attack detection using hybrid Deep Learning Model. Comput Commun. 2021;176:146–54.

9. Li F, Shinde A, Shi Y, Ye J, Li XY, Song W. System statistics learning-based IoT security: Feasibility and suitability. IEEE Internet Things J. 2019;6(4):6396–403.

10. Sahu NK, Mukherjee I. Machine learning based anomaly detection for IoT network:(Anomaly detection

in IoT network). In: 2020 4th international conference on trends in electronics and informatics (ICOEI)(48184). IEEE; 2020. p. 787–94.

11. Agrawal S, Sarkar S, Aouedi O, Yenduri G, Piamrat K, Alazab M, et al. Federated learning for intrusion detection system: Concepts, challenges and future directions. Comput Commun. 2022;195:346–61.

12. Kaur S, Singh M. Hybrid intrusion detection and signature generation using deep recurrent neural networks. Neural Comput Appl. 2020;32(12):7859–77.

13. Ahmad W, Rasool A, Javed AR, Baker T, Jalil Z. Cyber security in iot-based cloud computing: A comprehensive survey. Electronics. 2021;11(1):16.

14. Gill KS, Saxena S, Sharma A. Gta-ids: game theoretic approach to enhance ids detection in cloud environment. Comput Informatics. 2022;41(3):665–88.

15. Kocher G, Kumar G. Machine learning and deep learning methods for intrusion detection systems: recent developments and challenges. Soft Comput. 2021;25(15):9731–63.

16. Zhang Y, Zhang X, Sun J, Lin H, Huang Y, Lv D, et al. Fault-tolerant quantum algorithms for quantum molecular systems: A survey. arXiv Prepr arXiv250202139. 2025;

17. Haque S, Zeba S, Alimul Haque M, Kumar K, Ali Basha MP. An IoT model for securing examinations from malpractices. Mater Today Proc. 2021 Apr;

18. Santos L, Rabadao C, Gonçalves R. Intrusion detection systems in Internet of Things: A literature review. In: 2018 13th Iberian conference on information systems and technologies (CISTI). IEEE; 2018. p. 1–7.

19. Md. Alimul Haque, Anil Kumar Sinha MUB and NKS. Comparative study on Wireless threats and their Classification. In 2017. Available from: http://bvicam.in/INDIACom/news/INDIACom 2017 Proceedings/Main/papers/2511.pdf

20. iot intrusion [Internet]. Available from: https://www.kaggle.com/datasets/subhajournal/iotintrusion

FINANCING

The authors did not receive financing for the development of this research.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest.

AUTHOR CONTRIBUTIONS

Conceptualization: Amit Kumar Dinkar, Ajay Kumar Choudhary.
Investigation: Amit Kumar Dinkar, Ajay Kumar Choudhary.
Methodology: Amit Kumar Dinkar, Ajay Kumar Choudhary.
Writing - original draft: Amit Kumar Dinkar, Ajay Kumar Choudhary.
Writing - review and editing: Amit Kumar Dinkar, Ajay Kumar Choudhary.