Global **A**dvances in **M**ultidisciplinary **A**pplications in **N**ext-Gen **A**nd **M**odern Technologies (**GAMANAM)**
Volume 1, Issue 1, January 2025, Pp: 57-60

Survey Paper

A Quick Survey to Enhance IoT Security: The Role of Intrusion Detection Systems in Addressing Cyber Threats

[1*]Jabeen Sultana

[1*]*Department of Computer Science, College of Computer and Information Sciences, Imam Mohammad Ibn Saud Islamic University, Riyadh, Kingdom of Saudi Arabia*

**Corresponding Author(s): jsmali@imamu.edu.sa*

Received:13/11/2024, Revised: 11/11/2024, Accepted:25/12/2024 Published:12/01/2025

Abstract: The rapid growth of Internet of Things (IoT) devices has transformed industries like healthcare and smart cities by improving connectivity and efficiency. However, this increased connectivity has also brought serious security risks, making IoT devices common targets for cyberattacks. Protecting these devices is essential to ensure the safety of critical systems and user privacy. Intrusion Detection Systems (IDS) play a key role in identifying and preventing malicious activities in IoT networks by using the techniques offered by Machine Learning (ML) and Deep learning (DL). This survey looks at the unique security challenges in IoT, highlights the importance of IDS in addressing these challenges, and discusses gaps in current research. It aims to provide simple and practical ideas for building better IDS solutions to secure IoT environments effectively.

Keywords: Internet of Things (IOT), Intrusion Detection Systems (IDS), Machine Learning (ML), Deep learning (DL) and cyberattacks.

1. Introduction

IoT encompasses a vast network of devices, ranging from sensors and actuators to everyday appliances, interconnected through the internet, often operating with constrained resources. The inherent diversity, heterogeneity, and scale of IoT deployments make them highly susceptible to diverse cyber threats. Traditional security measures are often inadequate to combat the sophisticated and evolving nature of attacks targeting these IoT ecosystems. The Internet of Things (IoT) has significantly transformed various industries, including healthcare, smart cities, transportation, and industrial automation, by enabling extensive connectivity and efficiency. However, this widespread interconnectivity has introduced substantial security challenges, making IoT devices prime targets for cyberattacks. The inherent resource constraints and diverse nature of these devices further exacerbate their vulnerability to intrusions. Ensuring the security of IoT ecosystems is crucial to protect sensitive data, maintain system integrity, and uphold user privacy. Intrusion Detection Systems (IDS) have emerged as a vital component in this defense strategy, designed to monitor network traffic, detect potential threats, and respond to unauthorized access or attacks. Recent research has focused on enhancing IDS for IoT environments.

While several studies have delved into intrusion detection systems, a substantial gap exists in comprehensive and specialized approaches specifically crafted for IoT environments. Existing literature primarily focuses on general intrusion detection methods or adaptations from traditional networks, lacking in-depth exploration and evaluation of techniques tailored to the intricacies of IoT. Furthermore, there's a dearth of consensus on the most effective methods, performance metrics, and evaluation frameworks specifically applicable to IoT intrusion detection. This research endeavors to bridge this gap by conducting a systematic investigation into intrusion detection mechanisms explicitly designed for IoT ecosystems. By addressing this critical gap, the research aims to contribute novel insights and methodologies essential for securing the increasingly interconnected and vulnerable IoT landscape. The challenges and opportunities associated with utilizing deep learning techniques for handling large-scale IoT data streams. It provides insights into architectures, algorithms, and emerging trends in leveraging deep learning for intrusion detection within IoT environments [1]. The research provides insights into the strengths and weaknesses of different models and datasets,

aiding in understanding the applicability of deep learning techniques for intrusion detection in IoT [2]. Focused on IoT security, this research offers a comprehensive review that includes discussions on intrusion detection. It explores the integration of machine learning, blockchain solutions, and their potential implications for enhancing security in IoT ecosystems. The research outlines open challenges and provides insights into how combining machine learning and other technologies can contribute to robust intrusion detection mechanisms in IoT [3].

This quick survey highlights the significance of intrusion detection in IoT, the prevalent challenges, and the gap in specialized research focused on this critical aspect of IoT security. The proliferation of interconnected devices within the Internet of Things (IoT) landscape has revolutionized numerous sectors, ranging from healthcare to smart cities. However, this interconnectedness has introduced unprecedented security challenges, with IoT devices becoming prime targets for cyber threats and intrusions. Ensuring the security and integrity of these devices is paramount to safeguarding critical systems and user privacy. One of the crucial mechanisms to address this concern is Intrusion Detection Systems (IDS) tailored for IoT environments. Despite these advancements, developing effective IDS for IoT remains challenging due to the resource limitations of devices, the heterogeneous and dynamic nature of IoT environments, and the necessity for real-time detection and response. This survey explores the role of IDS in securing IoT ecosystems, examines existing approaches, and identifies areas for improvement, aiming to contribute to the development of robust and scalable IDS solutions in order to overcome the complexities faced by IoT systems.

2. Literature

The Internet of Things (IoT) needs better intrusion detection systems (IDS) to deal with security risks. Many current methods can't handle new threats or the unique challenges of IoT. This survey explores the recent application of deep learning in analyzing big data streams generated by IoT devices. It covers various aspects, including data analytics, anomaly detection, and intrusion detection. Implementing machine learning algorithms tailored for IoT environments to detect intrusion patterns, anomalies, or attacks within the IoT ecosystem is the current trending topic among researchers. Focusing on intrusion detection in IoT using machine learning and deep learning warrants exploring specialized literature that delves into these domains. This survey discusses the research findings on intrusion detection in IoT using ML and DL techniques. This research conducts an in-depth comparative research of different deep learning approaches applied specifically to cybersecurity intrusion detection. It explores various datasets used for evaluating intrusion detection models and compares the performance of different deep learning architectures. The research provides insights into the strengths and weaknesses of different models and datasets, aiding in understanding the applicability of deep learning techniques for intrusion detection in IoT.

This research conducted an in-depth comparative research of different deep learning approaches applied specifically to cybersecurity intrusion detection. It explores various datasets used for evaluating intrusion detection models and compares the performance of different deep learning architectures. This conference research presents a specific IoT intrusion detection system based on deep neural networks. It discusses the design and implementation of the system, emphasizing the application of deep learning techniques for identifying intrusions within IoT networks. The research likely includes details on the architecture, dataset used, training methodologies, and performance evaluation of the proposed intrusion detection system [4]. This research explores the role of machine learning in identifying and securing IoT devices. It likely covers aspects of intrusion detection by leveraging machine learning techniques. It could discuss methods for anomaly detection, classification of normal/abnormal behavior in IoT devices, and the application of machine learning algorithms for enhancing IoT security [5]. Focused on healthcare IoT applications, this survey research examines intrusion detection systems employing machine learning techniques. It likely discusses specific use cases within healthcare IoT, highlighting the application of machine learning for detecting intrusions or anomalies. The research might cover different machine learning models applied in healthcare IoT environments for enhanced security measures [6].

This research presents a new model that combines two advanced techniques, CNN and GRU, to detect intrusions more effectively. It also uses a method called FW-SMOTE to fix problems with unbalanced data. Tests on the IoTID20 dataset showed a high accuracy of 99.60%, better than existing methods. It also worked well on another dataset, UNSW-NB15, with 99.16% accuracy. This new approach solves major problems in IoT intrusion detection and sets a new standard for protecting IoT systems [7]. This review looks at various machine learning methods for detecting intrusions in IoT systems, including supervised, unsupervised, deep learning, and hybrid models. It evaluates how well these methods work, their challenges, and how they can be used in real-world scenarios. The research also discusses current industry problems and trends, emphasizing the need for continued research to keep up with the fast-changing IoT security landscape [8].

This research gives a clear and up-to-date overview of IoT Intrusion Detection Systems (IDS), organizing and reviewing important research on the topic. It classifies different types of IoT IDS, making it easier for researchers to understand the main ideas. The research also looks at how machine learning and deep learning are used in IoT IDS, including methods for detecting intrusions, validating results, and deploying systems. It discusses the complexity of these techniques and how they are tested. Finally, the research suggests the best methods to use depending on the specific needs of the IoT IDS [9]. Industrial Internet of Things (IIoT), part of Industry 4.0, aims to improve product quality and reduce production costs by using advanced technologies like edge/fog/cloud computing, 5G/6G, and artificial intelligence. However, with many devices

connected, there's a need to protect them from cyber threats. To address this, we propose using deep learning (DL) models for anomaly-based intrusion detection. Our approach combines two powerful models: Convolutional Neural Networks (CNN) and Gated Recurrent Units (GRU). We tested the model on a new real-world industrial dataset, Edge-IIoTset, for both binary and multiclass classification. Our results showed that the CNN-GRU model outperformed others in accuracy, precision, false positive rate, and detection cost. In multiclass classification, it also reduced the detection cost by 88% compared to using GRU alone [10].

These days the attacks faced by deep web, dark web and surface web are mainly because of URL attacks. In present times, real URL's need to be differentiated with fake URL's in order to reduce the web attacks [11]. Real time data was collected from twitter database using search keywords like cyberattacks and COVID-19. Data was properly cleaned using tool kit available in python and further classification was carried out. It was identified that SVM attained maximum classification accuracy of 94% [12]. Furthermore, in one of the researches related to cyber security, it was identified that classification was carried out in dual stages. Initially, NSL-KDD data was classified using deep learning classifier namely autoencoder. Secondly, the classified data was tested for its accurateness using Isolation Forest and this was work was proposed for fog environment and it was noted that 95% accuracy was attained by IF [13]. This study used spam URL data from Kaggle to classify URLs as spam or not using machine learning models. Two methods, 10-fold cross-validation and hold-out, were tested. Random Forest performed the best with 97% accuracy using 10-fold cross-validation, followed by Support Vector Machine (SVM) with 92% accuracy and Naive Bayes with 91% accuracy. The models were evaluated based on accuracy, true positive rate, false positive rate, precision, and recall [14].

The proposed Intrusion Detection System (IDS) uses two deep learning models, CNN and LSTM, to classify IoT traffic as either safe or harmful. CNN detects patterns in the data, while LSTM tracks time-based details, making the system more accurate and efficient. The model was tested using the CICIoT2023 and CICIDS2017 datasets. It performed very well, with an accuracy of 98.42%, a low error rate of 0.0275, and a false positive rate of 9.17%. The F1-score was 98.57%. These results show that the CNN-LSTM system is highly effective in protecting IoT devices from cyber threats [15]. This IoT survey using ML and DL collectively provides a comprehensive understanding of the application of machine learning and deep learning techniques for intrusion detection in IoT environments. They offer insights into methodologies, comparative studies, challenges, and potential solutions in this domain, contributing significantly to the advancement of IoT security measures.

3. Conclusion

The overarching problem lies in developing effective and efficient intrusion detection mechanisms specifically designed for IoT environments. Conventional intrusion detection methods, largely developed for traditional networks, may not be directly applicable or optimized to address the unique challenges posed by IoT ecosystems. There exists a critical need for tailored intrusion detection approaches that consider the resource constraints, diverse communication protocols, and the dynamic nature of IoT networks. Research also shows that using techniques like FW-SMOTE can help fix problems with unbalanced data, making intrusion detection more effective. Many research works have focused on how deep learning can improve security in IoT, especially for healthcare systems, by detecting intrusions and anomalies in real time. Overall, combining different machine learning methods and adapting them to the specific needs of IoT can help strengthen security. As IoT systems grow, continued research and development of better IDS will be key to keeping these systems safe from new cyber threats. In conclusion, as IoT devices are used more in areas like healthcare and industry, protecting them from cyber threats becomes increasingly important. Intrusion detection systems (IDS) that use machine learning, especially deep learning models like CNN and GRU, can help detect unusual behavior and improve security. These models have been shown to work better than traditional methods in terms of accuracy and efficiency.

References

[1] H. Xu, et al., "Deep Learning for IoT Big Data and Streaming Analytics: A Survey," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 3415-3431, 2018.

[2] M. Choras, "Deep Learning for Cybersecurity Intrusion Detection: Approaches, Datasets, and Comparative Research," *Journal of Cybersecurity*, vol. 1, no. 1, pp. 1-19, 2020.

[3] Z. Abdelmoety, et al., "IoT Security: Review, Blockchain Solutions, and Open Challenges," *IEEE Access*, vol. 8, pp. 159171-159194, 2020.

[4] J. Huang, et al., "IoT Intrusion Detection System Using Deep Neural Network," *2019 IEEE International Conference on Consumer Electronics (ICCE)*, pp. 1-4, 2019.

[5] M. Usama, et al., "Machine Learning for IoT Device Identification and Security," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 1205-1214, 2018.

[6] T. Shanmugapriya and P. Suresh, "A Survey on Intrusion Detection Systems in IoT Based Healthcare Applications Using Machine Learning Techniques," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, no. 8, pp. 3421-3431, 2020.

[7] A. Qaddos, M. U. Yaseen, A. S. Al-Shamayleh, et al., "A novel intrusion detection framework for optimizing IoT security," *Scientific Reports*, vol. 14, no. 21789, 2024, doi: 10.1038/s41598-024-72049-z.

[8] B. R. Kikissagbe and M. Adda, "Machine Learning-Based Intrusion Detection Methods in IoT Systems: A

Comprehensive Review," *Electronics*, vol. 13, no. 18, pp. 3601, 2024, doi: 10.3390/electronics13183601.

[9] A. Khraisat and A. Alazab, "A critical review of intrusion detection systems in the Internet of Things: Techniques, deployment strategy, validation strategy, attacks, public datasets, and challenges," *Cybersecurity*, vol. 4, no. 18, 2021, doi: 10.1186/s42400-021-00077-7.

[10] R. Saadouni, A. Khacha, Y. Harbi, C. Gherbi, S. Harous, and Z. Aliouat, "Secure IIoT networks with hybrid CNN-GRU model using Edge-IIoTset," *2023 15th International Conference on Innovations in Information Technology (IIT)*, Al Ain, United Arab Emirates, pp. 150-155, 2023.

[11] J. Sultana and A. K. Jilani, "Exploring and Analysing Surface, Deep, Dark Web and Attacks," in *Security Incidents & Response Against Cyber Attacks*, A. Bhardwaj and V. Sapra, Eds. Springer, 2021.

[12] J. Sultana and A. K. Jilani, "Classifying Cyberattacks Amid COVID-19 Using Support Vector Machine," in *Security Incidents & Response Against Cyber Attacks*, A. Bhardwaj and V. Sapra, Eds. Springer, 2021.

[13] K. Sadaf and J. Sultana, "Intrusion detection based on autoencoder and isolation forest in fog computing," *IEEE Access*, vol. 8, pp. 167059-167068, 2020.

[14] A. K. Jilani and J. Sultana, "A Random Forest Based Approach to Classify Spam URLs Data," *ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems (ICETSIS)*, pp. 268-272, 2022