IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.67

Volume 5, Issue 7, March 2025

Review of Adaptive Deep Learning Approaches for Intrusion Detection in IoT Network

Pooja Khare[1] and Akash Singh[2]

Research Scholar, Babulal Tarabai Institute of Research and Technology, Sagar, India[1]

Assistant Professor, Computer science & Engineering, Babulal Tarabai Institute of Research and Technology, Sagar[2]

poojakhare1523@gmail.com and akashst133@gmail.com

Abstract: *As the Internet of Things (IoT) ecosystem continues to expand, the security of IoT networks becomes an increasingly critical concern. The vast and interconnected nature of IoT devices introduces unique challenges for intrusion detection systems (IDS) to safeguard against potential threats. Traditional intrusion detection methods often fall short in addressing the dynamic and evolving nature of attacks in IoT environments. This paper explores the efficacy of adaptive deep learning approaches for intrusion detection in IoT networks, aiming to enhance the resilience and responsiveness of security mechanisms.*

The proposed adaptive deep learning model leverages the power of neural networks to automatically learn and adapt to emerging threats. The model is designed to dynamically adjust its parameters based on the evolving characteristics of the network and the attack landscape. The adaptive nature of the deep learning approach enables it to continuously improve its detection capabilities without requiring explicit retraining, making it well-suited for the dynamic nature of IoT environments.

The study begins with an overview of the unique challenges posed by IoT networks, including the heterogeneity of devices, resource constraints, and the need for real-time threat detection. Subsequently, a comprehensive review of existing intrusion detection techniques in IoT is presented, highlighting their limitations and the motivation for adopting adaptive deep learning methodologies..

Keywords: Intrusion Detection Systems (IDS), Adaptive Deep Learning Models, IoT Network Security, Anomaly Detection Techniques, Cyber Threat Mitigation

I. INTRODUCTION

In recent years, the proliferation of Internet of Things (IoT) devices has transformed the way we interact with the digital world. IoT has enabled seamless connectivity and communication among a myriad of devices, ranging from smart home appliances and wearables to industrial sensors and autonomous vehicles. While this interconnectedness brings unprecedented convenience, it also introduces new challenges, especially in terms of security. The vulnerability of IoT networks to cyber threats necessitates robust intrusion detection mechanisms to safeguard the integrity and confidentiality of sensitive data.

Traditional intrusion detection systems (IDS) have been effective in conventional network environments, but the unique characteristics of IoT networks demand adaptive and sophisticated approaches. Deep learning, a subset of machine learning, has emerged as a powerful tool for tackling complex tasks in various domains. Its ability to automatically learn hierarchical representations of data has shown promise in enhancing the accuracy and efficiency of intrusion detection systems. This paper explores the landscape of adaptive deep learning approaches tailored for intrusion detection in IoT networks, examining their strengths, challenges, and potential impact on the evolving cybersecurity paradigm.

Deep Learning for Intrusion Detection

Deep learning techniques, particularly neural networks, have demonstrated remarkable success in various applications such as image recognition, natural language processing, and speech recognition. Their effectiveness lies in their capacity to automatically learn hierarchical features from raw data. In the context of intrusion detection, deep learning models can analyze network traffic patterns, device behavior, and system logs to identify anomalous activities indicative of potential security threats.

DOI: 10.48175/IJARSCT-24417

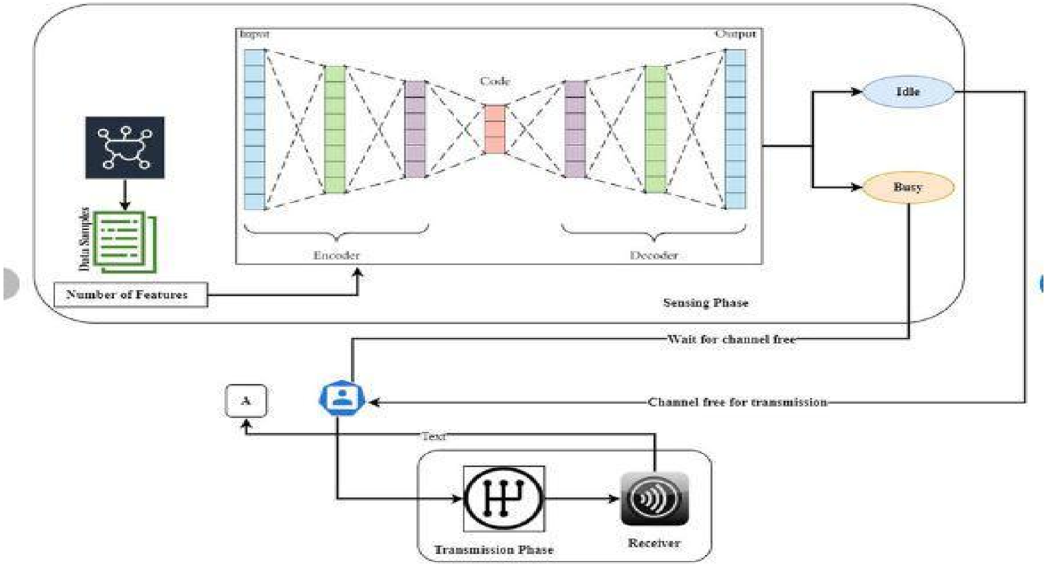

Figure 1 Three-phase of AENN IoT data transmission process.

One notable advantage of deep learning-based intrusion detection systems is their ability to adapt and learn from the evolving characteristics of IoT networks. Unlike rule-based systems that rely on predefined signatures, deep learning models can generalize patterns and adapt to novel threats without constant manual updates. This adaptability is crucial in the dynamic and diverse landscape of IoT, where new vulnerabilities and attack vectors continually emerge.

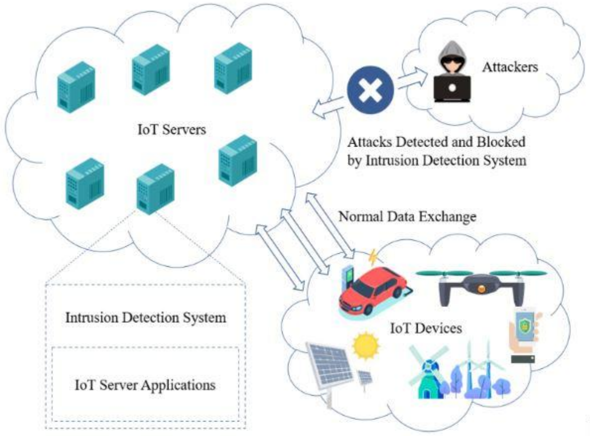
Attackers
IoT Servers
Attacks Detected and Blocked
by Intrusion Detection System
Normal Data Exchange
IoT Devices
Intrusion Detection System
IoT Server Applications

Figure 2 Sequential Model Based Intrusion Detection System for IoT Servers Using Deep Learning

II. LITERATURE SURVEY

[1] Archana V. Potnurwar, Vrushali K. Bongirwar, Samir Ajani, Nilesh Shelke, Mrunalee Dhone, Namita Parati,"Deep Learning-Based Rule-Based Feature Selection for Intrusion Detection in Industrial Internet of Things Networks", 2023.

In the field of Industrial IoT area, It produces enormous volumes of data by utilising the power of sensors. The IIoT does, however, confront considerable obstacles, particularly in the form of cyber-attacks that can jeopardise organisations and interrupt operations. Sensitive information is stolen as a result of these attacks, in addition to causing losses in money and reputation.To address these risks, numerous Network Intrusion Prevention Systems (NIDSs) have been developed to protect IIoT systems. But creating a useful and intelligent NIDS is a challenging endeavour, largely because there aren't many large data sets that can be utilised to design and test such systems.In response to these difficulties, this research proposes a novel deep learning-based intrusion detection technique for IIoT systems. To help identify relevant data derived from TCP/IP packets, a hybrid rule-based feature selection mechanism is included in the proposed system. The solution attempts to increase the precision and effectiveness of intrusion detection in IIoT environments by utilising deep learning methods.In this study, deep learning techniques are employed to offer a novel method for industrial internet of things (IIoT) system intrusion detection. The proposed paradigm combines a Deep Feed Forward Neural Network model (DFFNN) with a hybrid rule-based feature selection strategy to quickly train and assess data obtained from TCP/IP packets. The effectiveness of the technique was evaluated on two well-known network datasets, NSL-KDD and UNSW-NB15.

[2] Rajasekhar Chaganti , Wael Suliman , Vinayakumar Ravi , and Amit Dua "Deep Learning Approach for SDN-Enabled Intrusion Detection System in IoT Networks", 2023 .

Owing to the prevalence of the Internet of things (IoT) devices connected to the Internet,the number of IoT-based attacks has been growing yearly. The existing solutions may not effectively mitigate IoT attacks. In particular, the advanced network-based attack detection solutions using traditional Intrusion detection systems are challenging when the network environment supports traditional as well as IoT protocols and uses a centralized network architecture such as a software defined network (SDN). In this paper, we propose a long short-term memory (LSTM) based approach to detect network attacks using SDN supported intrusion detection system in IoT networks. We present an extensive performance evaluation of the machine learning (ML) and deep learning (DL) model in two SDNIoT-focused datasets.

[3] Saif Mohammed Ali, Amer S. Elameer, and Mustafa Musa Jaber, "IoT network security using autoencoder deep neural network and channel access algorithm," 2022 .

Internet-of-Things (IoT) creates a significant impact in spectrum sensing, information retrieval, medical analysis, traffic management, etc. These applications require continuous information to perform a specific task. At the time, various intermediate attacks such as jamming, priority violation attacks, and spectrum poisoning attacks affect communication because of the open nature of wireless communication. These attacks create security and privacy issues while making data communication. Therefore, a new method autoencoder deep neural network (AENN) is developed by considering exploratory, evasion, causative, and priority violation attack. The created method classifies the transmission outcomes used to predict the transmission state, whether it is jam data transmission or sensing data. After that, the sensing data is applied for network training that predicts the intermediate attacks. In addition to this, the channel access algorithm is used to validate the channel for every access that minimizes unauthorized access. After validating the channel according to the neural network, data have been transmitted over the network.

[4] Dr.S.Kalarani, and St Joseph's,"An Intelligent Network Intrusion Detection System using Deep Neural Network," 2022 .

Machine learning techniques are extensively used to enhance intrusion detection (IDS) systems to detect and classify cyber-attacks on the network and host levels quickly and automatically. A comprehensive evaluation of DNN and other classic machine learning classifier experiments is presented in a variety of publicly available benchmark malicious datasets. The optimum DNN network parameters and network topology are determined using the KDDCup99 and NSDL-KDD Datasets by the following hyperparameter selection method. Network Intrusion Detection Systems (NIDS) support system administrators in their organizations in exploring network security breaches.

[5] Amjad Rehman Khan,1 Muhammad Kashif,2 Rutvij H. Jhaveri , 3 Roshani Raut , 4 Tanzila Saba,1 and Saeed Ali Bahaj5, "Deep Learning for Intrusion Detection and Security of Internet of Things (IoT): Current Analysis, Challenges, and Possible Solutions", 2022 .

In the last decade, huge growth is recorded globally in computer networks and Internet of (ings (IoT) networks due to the exponential data generation, approximately zettabyte to a petabyte. Consequently, security issues have also been arisen with the network growth. However, intrusion detection in such big data is challenging. Smart homes, cities, grids, devices, objects, e-commerce, e-banking, e-government, etc., are different advanced applications of the evolving networks. Many Intrusion Detection Systems (IDS) have been developed recently due to most computer networks' exposure to security and privacy threats. Data confidentiality, integrity, and availability damage will occur in case of IDS prevention failure. Conventional techniques are not effective enough to cope the advanced attacks. Advanced deep learning techniques have been proposed for automatic intrusion detection and abnormal behavior identification of networks. (is research aims to provide an inclusive analysis of intrusion detection based on deep learning techniques followed by different intrusion detection systems.

[6] Jin Cao 1, Liwei Lin 2, Ruhui Ma 1,*, Haibing Guan 1, Mengke Tian 3,4 and Yong Wang 4,"An Efficient Deep Learning Approach To IoT Intrusion Detection", 2022 .

With the rapid development of the Internet of Things (IoT), network security challenges are becoming more and more complex, and the scale of intrusion attacks against the network is gradually increasing. Therefore, researchers have proposed Intrusion Detection Systems and constantly designed more effective systems to defend against attacks. One issue to consider is using limited computing power to process complex network data efficiently. In this paper, we take the AWID dataset as an example, propose an efficient data processing method to mitigate the interference caused by redundant data and design a lightweight deep learning-based model to analyze and predict the data category. Finally, we achieve an overall accuracy of 99.77% and an accuracy of 97.95% for attacks on the AWID dataset, with a detection rate of 99.98% for the injection attack.

[7] Alaa Mohammed Banaamah and Iftikhar Ahmad *, " Intrusion Detection in IoT Using Deep Learning " 2022

Cybersecurity has been widely used in various applications, such as intelligent industrial systems, homes, personal devices, and cars, and has led to innovative developments that continue to face challenges in solving problems related to security methods for IoT devices. Effective security methods, such as deep learning for intrusion detection, have been introduced. Recent research has focused on improving deep learning algorithms for improved security in IoT. This research explores intrusion detection methods implemented using deep learning, compares the performance of different deep learning methods, and identifies the best method for implementing intrusion detection in IoT.

[8] K. Janani and S. Ramamoorthy,"Threat analysis model to control IoT network routing attacks through deep learning approach , 2022 .

Most of the recent research has focused on the Internet of Things (IoT) and its applications. The open interface and network connectivity of the interconnected systems under the IoT network make them vulnerable to hackers. A model has been proposed to identify and classify IoT routing attacks. To generate IoT routing datasets, the Cooja simulator is used at first. The IoT routing dataset is then augmented into larger volumes using ADASYN, which is also used to solve the class imbalance problems. A deep learning hybrid model based on a Long-Short-Term Memory (LSTM) network and adaptive Mayfly Optimization Algorithm (LAMOA) was presented for the classification of IoT attacks. The adaptive MOA adjusts the weights in the various layers of the LSTM network and the Fully Connected Layer with SoftMax Classification. As part of the validation process.

[9] Stefanos Tsimenidis1 · Thomas Lagkas1 · Konstantinos Rantos1,"Deep Learning in IoT Intrusion Detection'' , 2021 .

The Internet of Things (IoT) is the new paradigm of our times, where smart devices and sensors from across the globe are interconnected in a global grid, and distributed applications and services impact every area of human activity. With its huge economic impact and its pervasive infuence over our lives, IoT is an attractive target for criminals, and cybersecurity becomes a top priority for the IoT ecosystem. Although cybersecurity has been the subject of research for decades, the large-scale IoT architecture and the emergence of novel threats render old strategies largely ineffcient. Deep learning may provide cutting edge solutions for IoT intrusion detection, with its data-driven, anomaly-based approach and ability to detect emerging, unknown attacks.

[10] Ying Zhang*, Peisong Li and Xinheng Wang, "Intrusion Detection for IoT Based on Improved Genetic Algorithm and Deep Belief Network", 2021 .

With the advent of the Internet of Things, the security of the network layer in the Internet of Things is getting more and more attention. Traditional intrusion detection technologies cannot be well adapted in the complex Internet environment of the Internet of Things. Therefore, it is extremely urgent to study the intrusion detection system corresponding to today's Internet of Things security. This paper presents an intrusion detection model based on improved Genetic Algorithm and Deep Belief Network. Facing different types of attacks, through multiple iterations of the GA, the optimal number of hidden layers and number of neurons in each layer are generated adaptively, so that the intrusion detection model based on the DBN achieves a high detection rate. Finally, the NSL-KDD dataset was used to simulate and evaluate the model algorithm.

III. PROPOSED RESEARCH METHODOLOGY

The research methodology section outlines the systematic process that will be employed to conduct the study on adaptive deep learning approaches for intrusion detection in IoT networks. The research aims to explore and evaluate the effectiveness of adaptive deep learning techniques in enhancing the security of IoT networks against various types of intrusions. This section provides a comprehensive overview of the research design, data collection methods, data analysis techniques, and the overall approach to achieving the research objectives.

Research Design:

The research design serves as the blueprint for the study, guiding the researcher in making decisions about data collection, analysis, and interpretation. For this study, a mixed-methods research design will be adopted to combine both qualitative and quantitative approaches.

a. Quantitative Approach:

Experimental Design: Conduct experiments to evaluate the performance of adaptive deep learning models in detecting intrusions.

Controlled Environment: Simulate IoT network environments with controlled variables to ensure reproducibility and reliability.

Statistical Analysis: Employ statistical tools to analyze quantitative data, such as accuracy, precision, recall, and F1 score.

b. Qualitative Approach:

Interviews and Surveys: Gather insights from cybersecurity experts, IoT network administrators, and end-users to understand qualitative aspects, such as usability and user experience of adaptive deep learning-based intrusion detection systems.

Population and Sample Selection:

Population: The population for this study includes IoT networks and devices across various domains and industries.

Sample Selection: Employ a purposive sampling technique to select representative IoT networks for experimentation. Ensure diversity in terms of network size, device types, and communication protocols.

Data Collection:

a. Quantitative Data:

Intrusion Scenarios: Simulate diverse intrusion scenarios, including DDoS attacks, malware, and unauthorized access.

IoT Network Traffic: Capture and analyze network traffic data using network simulators and real-world IoT testbeds.

Performance Metrics: Measure the performance of adaptive deep learning models using metrics like accuracy, false positive rate, and detection time.

b. Qualitative Data:

Interviews: Conduct interviews with cybersecurity experts to gather qualitative insights into the adaptability and robustness of the proposed models.

Surveys: Administer surveys to IoT network administrators and end-users to assess the perceived effectiveness and usability of the intrusion detection system.

Adaptive Deep Learning Model Implementation:

Implement state-of-the-art deep learning models for intrusion detection, considering recurrent neural networks (RNNs), long short-term memory networks (LSTMs), and attention mechanisms.

Develop adaptive mechanisms to allow models to evolve and improve over time based on new intrusion patterns and variations.

DOI: 10.48175/IJARSCT-24417

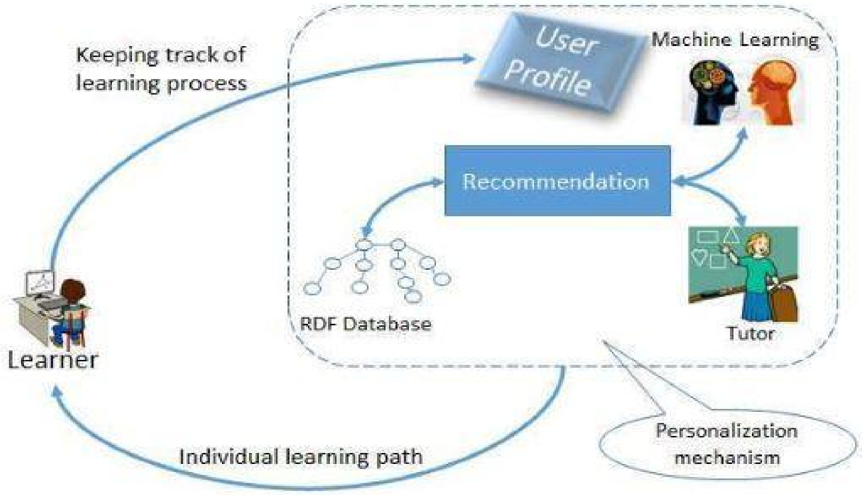

Figure 3 Adaptive E-learning System Architecture.

IV. FUTURE WORK

IoT Network Architecture:

This section delves into the intricacies of IoT network architectures, emphasizing the diverse range of devices and communication protocols involved. Understanding the unique characteristics of IoT networks is crucial for developing effective intrusion detection solutions tailored to their specific challenges.

Security Challenges in IoT Networks:

Discussing the various security challenges in IoT networks, including device heterogeneity, limited resources, and the dynamic nature of IoT environments. Addressing these challenges is essential for devising adaptive intrusion detection systems capable of handling the complexity of IoT ecosystems.

Intrusion Detection Systems (IDS) in IoT:

Explore existing intrusion detection approaches in IoT networks, including signature-based, anomaly-based, and hybrid systems. Discuss their limitations in adapting to evolving threats and highlight the necessity for more sophisticated techniques.

Adaptive Deep Learning for Intrusion Detection:

Introduce the concept of adaptive deep learning as a promising approach for intrusion detection in IoT networks. Detail the advantages of leveraging deep neural networks, such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs), in handling the intricacies of IoT data streams.

Transfer Learning for IoT Intrusion Detection:

Investigate the application of transfer learning to enhance the performance of intrusion detection models in IoT networks. Highlight how pre-trained models can be fine-tuned to specific IoT scenarios, reducing the need for extensive labeled datasets.

V. CONCLUSION

In conclusion, adaptive deep learning approaches have emerged as a promising solution for enhancing the security of IoT networks through effective intrusion detection mechanisms. The dynamic and evolving nature of IoT environments demands a robust and flexible system capable of adapting to novel threats in real-time. Deep learning models, such as recurrent neural networks (RNNs) and convolutional neural networks (CNNs), have demonstrated their efficacy in learning complex patterns and anomalies inherent in IoT data streams. The adaptability of these models to evolving attack vectors is particularly crucial in the context of the Internet of Things, where the threat landscape is continually evolving.

DOI: 10.48175/IJARSCT-24417

One of the key advantages of adaptive deep learning lies in its ability to automatically adjust its parameters and features based on the changing characteristics of IoT network traffic. This adaptability enables the system to maintain high detection accuracy even in the face of previously unseen and sophisticated attacks. The self-learning capabilities of deep learning models contribute to reducing false positives and false negatives, thus enhancing the overall reliability of intrusion detection systems in IoT environments.

Moreover, the integration of contextual information and feature extraction techniques within adaptive deep learning models further refines their detection capabilities. The context-awareness enables the system to differentiate between normal and malicious activities based on the specific context of the IoT devices and their interactions. This not only improves the accuracy of intrusion detection but also reduces the computational overhead associated with processing vast amounts of IoT data.

REFERENCES

[1] P. Ambika, “Machine learning and deep learning algorithms on the Industrial Internet of Things (IIoT),” Advances in Computers, vol. 117, no. 1, pp. 321–338, 2020.

[2] R. Ashima, A. Haleem, S. Bahl, M. Javaid, S. K. Mahla, and S. Singh, “Automation and manufacturing of smart materials in Additive Manufacturing technologies using the Internet of Things towards the adoption of Industry 4.0,” Materials Today: Proceedings, vol. 45, pp. 5081–5088, 2021.

[3] L. M. Gladence, V. M. Anu, R. Rathna, and E. Brumancia, “Recommender system for home automation using IoT and artificial intelligence,” Journal of Ambient Intelligence and Humanized Computing, pp. 1–9, 2020.

[4] T. Sherasiya, H. Upadhyay, and H. B. Patel, “A survey: intrusion detection system for internet of things,” International Journal of Computer Science and Engineering (IJCSE), vol. 5, no. 2, pp. 91–98, 2016.

[5] J. B. Awotunde, R. G. Jimoh, S. O. Folorunso, E. A. Adeniyi, K. M. Abiodun, and O. O. Banjo, “Privacy and security concerns in IoT-based healthcare systems,” Internet of Things, pp. 105–134, 2021.

[6] E. A. Adeniyi, R. O. Ogundokun, and J. B. Awotunde, “IoMT-based wearable body sensors network healthcare monitoring system,” in IoT in Healthcare and Ambient Assisted Living, pp. 103–121, Springer, vSingapore, 2021.

[7] Mohanta BK, Jena D, Ramasubbareddy S, Daneshmand M, Gandomi AH. Addressing security and privacy issues of IoT using blockchain technology. IEEE Internet Things J. 2020;8(2):881–8.

[8] Reddy YB, Latifi S. Trust and access controls in IoT to avoid malicious activity. In: Cloud Network Management. London, UK: Chapman and Hall/CRC; 2020. p. 87–103.

[9] Bhatt P, Bhatt S, Ko M. Poster: IoT SENTINEL-An ABAC approach against cyber-warfare in organizations. In: Proceedings of the 25th ACM Symposium on Access Control Models and Technologies; 2020. p. 223–5.

[10] Islam MR, Aktheruzzaman KM. An analysis of cybersecurity attacks against internet of things and security solutions. J Computer Commun 2020;8(4):11–25.