e-ISSN: 2582-5208

International Research Journal of Modernization in Engineering Technology and Science

(Peer-Reviewed, Open Access, Fully Refereed International Journal)

Volume:06/Issue:07/July-2024 Impact Factor- 7.868 www.irjmets.com

REAL TIME MALLICIOUS ATTACK IN IOT BASED INFRASTRUCTURE

Sharayu Patil*1, Prof. R.P. Chaudhari*2

*1,2Shri Sant Gadge Baba College Of Engineering & Technology Bhusawal, Dist Jalgaon, India.

DOI : https://www.doi.org/10.56726/IRJMET60138

ABSTRACT

This method sounds promising for enhancing intrusion detection in cyber-physical systems. Leveraging deep learning particularly generative adversarial networks (GANs), can indeed offer advantages in identifying cybersecurity vulnerabilities and breaches. By contrasting unsupervised and deep learning-based discriminative approaches, you're likely exploring a range of methodologies to address the limitations of traditional intrusion detection systems. GANs, in particular, are known for their ability to generate synthetic data that closely resembles real data, which could be highly beneficial in detecting novel types of intrusions. The reported performance increase of 95% to 97% in terms of accuracy, reliability, and efficiency is impressive. Achieving such gains is crucial in the realm of cybersecurity where the detection of attacks needs to be both timely and precise. Additionally, setting the dropout value to 0.2 and the epoch value to 25 seems to have contributed to achieving these results, indicating the importance of hyperparameter tuning in deep learning models.

Keywords: Cyber Security, Internet Of Things, Intrusion Detection System (IDS)Anomaly Detection, Security Attacks, Deep Learning, Network Security.

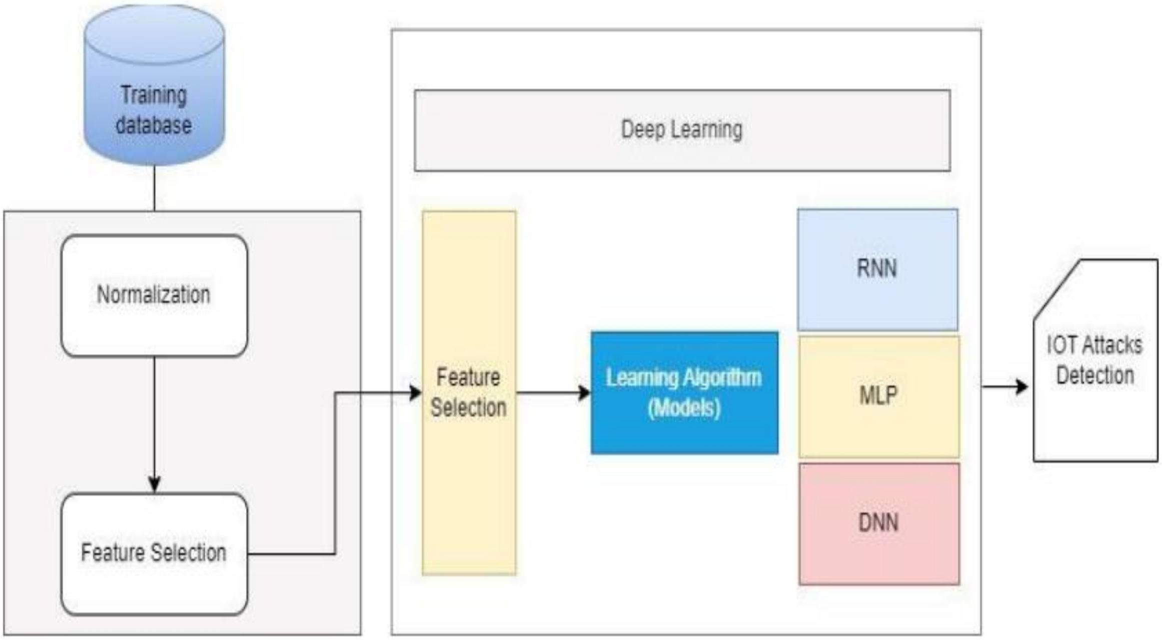
I. INTRODUCTION

Deep learning (DL) methods are used with different operators, which become beneficial for distinct mechanisms, especially the artificial neural network (ANN). It comprises three layers: input, output, and hidden [2], [3]. However, in DL, each layer is in a nonlinear fashion, which sent responses based on the data provided through input layers. Recently, DL approaches have been frequently used to discover graphic recognition, image processing, signal processing, and voice and audio recognition. Substantially, DL learning approaches The associate editor coordinating the review of this manuscript and approving it for publication was Vicente Alarcon-Aquino . are widely used in medicine for genomics and diseases [4]. The structure and functionality of the DL methods use complex data organization (such as images, text, and numbers hierarchy) and illustrate how to manage big data with forward, and back backpropagation methods focused. In addition, the other question raises how devices change the values and hyperparameters with dimensions to compute the Size of samples rendering the different layers. Successful methods make a minor difference between testing and training presentation and representation. The outdated wisdom characteristics result from a minor deviation from the family's usual quality and structural approaches to training [5]. Due to the reasons assumed and adopted DL methods in many areas, 9136 This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/ VOLUME 11, 2023 I. A. Kandhare et al.: Detection of Real-Time Malicious Intrusions and Attacks privacy and security concerns are critical. In DL methods, the key issue is data movement, where data is transferred between encrypted forms in training, testing, and interface modules. In addition, the DL prevailing in all models for the training part relies on enormous data, confidential and sensitive data for the user, primarily training data.

II. METHODOLOGY

DATA PRE-PROCESSING

Pre-processing is a crucial step in preparing electronic data for analysis, involving various manipulations and transformations of dataset values. Its primary aim is to optimize information acquisition by modifying the data detected by the observer .One common preprocessing technique is normalization, which adjusts the scale of the data to a common range. This process is particularly beneficial for algorithms related to neural networks, as reduces complexity and facilitates algorithm classification



Proposed framework for intrusion detection in the IoT environment

DEEP DISCRIMINATE MODELS (DDM)

In the designed framework, a deep neural network (DNN) serves as a central component for intrusion detection in network security applications. The DNN architecture is chosen for its ability to handle complex data and perform feature extraction and representation learning effectively.The DNN model utilized in the framework consists of multiple input and output layers, enabling it to process and analyse data from various sources. This multilayer perceptron architecture enhances the model's capacity to represent intricate relationships within the data.The DNN architecture typically comprises three main categories of layers: input layers, hidden layers, and convolution layers. These layers work together to extract meaningful features from the input data and perform anomaly detection and analysis tasks. In initial experiments using the DNN model on datasets such as NLS-KDD, promising results have been achieved, particularly in identifying zero-day attacks. The model has demonstrated superior performance compared to traditional techniques, showcasing its efficacy in enhancing network security

RECURRENT NEURAL NETWORK

RNNs (Recurrent Neural Networks) are a class of neural networks designed to handle sequential data by allowing prior outputs to be fed back into the network as inputs, while maintaining hidden states. Unlike CNNs (Convolutional Neural Networks) and DNNs (Deep Neural Networks), which only consider the current inputs' effect without taking into account past and future information, RNNs excel at capturing temporal dependencies in data.With their ability to capture temporal patterns and dependencies, RNNs have demonstrated remarkable performance in tasks such as sequence recognition and classification.

III. RESULT AND DISCUSSION

EXPERIMENT AND RESULT

With the rapid expansion of applications and network usage, security has emerged as a paramount concern for network systems. Many Internet of Things (IoT) devices rely on self-created systems, rendering them vulnerable to a variety of attacks. At the network layer, issues such as denial of service (DoS) assaults, gateway attacks, sniffers, and unauthorized access pose significant threats. Intrusion Detection Systems (IDS) have evolved alongside the advent of large-scale, high-dimensional IoT and computer networks. In this section, we assess the outcomes of the proposed framework to elucidate the efficacy of a Deep Learning-based approach in addressing security concerns for edge IoT devices within enterprise network environments. Table 3 presents the outcomes of Deep Learning discriminative methods across various attack types, highlighting the nature and characteristics of these attacks.

Generative models demonstrate varying degrees of accuracy in detecting different types of attacks. The Deep Belief Network (DBM) stands out with the highest accuracy rates across five attack types: Denial of Service (DoS) attacks including DOS_GoldEyes_Attack (94.63%) and DOS_LOIC_UDP_Attack (94.93%), as well as Botnet (95.09%), DoS Attacks-Hulk (96.02%), and DoS attacks-SlowHTTPTest (95.03%).

IV. FUTURE SCOPE

The future of IoT-based infrastructure is both promising and challenging, with a continuous expansion of interconnected devices across various industries. However, this growth is paralleled by an increasing sophistication of real-time malicious attacks. Understanding and addressing the future scope of these threats is crucial for the sustained development and security of IoT ecosystems.

Enhanced Detection and Response Systems

As IoT devices become more prevalent, the development of advanced detection and response systems will be essential. Future research should focus on leveraging artificial intelligence and machine learning to create adaptive security solutions capable of identifying and mitigating attacks in real-time. These systems can learn from patterns and behaviors to predict potential threats before they manifest, thereby providing a proactive defense mechanism.

Integration of Blockchain Technology

Blockchain technology offers promising solutions for enhancing the security and integrity of IoT networks. By decentralizing data storage and ensuring tamper-proof transactions, blockchain can prevent unauthorized access and data breaches. Future studies could explore the integration of blockchain with IoT to create more secure and transparent infrastructures, particularly in applications requiring high levels of trust and reliability.

V. CONCLUSION

The conclusion drawn from this seminar highlights the challenges and limitations encountered in previous research concerning the application of deep learning (DL) techniques in the early detection and mitigation of cyber threats. These challenges are deemed significant in the current global scenario, where cyber threats are increasingly prevalent. Despite ongoing research efforts, many unresolved issues persist, necessitating further investigation.

One key challenge lies in adapting DL methods effectively for attack detection as practical classifiers. While DL approaches offer advantages such as feature reduction, dimensionality reduction, and cost-effective evaluation through feature extraction, refining these methods into reliable classifiers remains a daunting task.

The study under discussion employs various DL techniques for cyber-attack and malware detection, emphasizing identification and discrimination. It summarizes seven approaches, encompassing DL architectures such as Recurrent Neural Networks (RNN), Convolutional Neural Networks (CNN), Deep Neural Networks (DNN), as well as generative models/methods like Restricted Boltzmann Machines (RBM), Deep Belief Networks (DBN), Deep Boltzmann Machines (DBM), and Denoising Autoencoders (DA).

VI. REFERENCES

[1] A. Ahmim, L. Maglaras, M. A. Ferrag, M. Derdour, and H. Janicke, "A novel hierarchical intrusion detection system based on decision tree and rules-based models," in Proc. 15th Int. Conf. Distrib. Comput. Sensor Syst. (DCOSS), May 2019, pp. 228–23

[2] A. Ahmim, L. Maglaras, M. A. Ferrag, M. Derdour, and H. Janicke, "A novel hierarchical intrusion detection system based on decision tree and rules-based models," in Proc. 15th Int. Conf. Distrib. Comput. Sensor Syst. (DCOSS), May 2019, pp. 228–233.

[3] Z. Dewa and L. A. Maglaras, "Data mining and intrusion detection systems," Int. J. Adv. Comput. Sci. Appl., vol. 7, no. 1, pp. 1–10, 2016

[4] B. Stewart, L. Rosa, L. A. Maglaras, T. J. Cruz, M. A. Ferrag, P. Simoes, and H. Janicke, "A novel intrusion detection mechanism for SCADA systems which automatically adapts to network topology changes," EAI Endorsed Trans. Ind. Netw. Intell. Syst., vol. 4, no. 10, p. e4, 2017

[5] Y. Imrana, Y. Xiang, L. Ali, and Z. Abdul-Rauf, "A bidirectional LSTM deep learning approach for intrusion detection," Expert Syst. Appl., vol. 185, Dec. 2021, Art. no. 115524.

[6] J. Azevedo and F. Portela, "Convolutional neural network—A practical case study," in Proc. Int. Conf. Inf. Technol. Appl. Singapore: Springer, 2022, pp. 307–318.

[7] J. Yosinski, J. Clune, Y. Bengio, and H. Lipson, "How transferable are features in deep neural networks?'' in Proc. Adv. Neural Inf. Process. Syst., vol. 27, 2014, pp. 1–9.

[8] C. Szegedy, V. Vanhoucke, S. Ioffe, J. Shlens, and Z. Wojna, "Rethinking the inception architecture for computer vision," in Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR), Jun. 2016, pp. 2818–2826.

[9] D. Hossain, G. Capi, and J. M., "Optimizing deep learning parameters using genetic algorithm for object recognition and robot grasping,'' J. Electron. Sci. Technol., vol. 16, no. 1, pp. 11–15, 2018.