International Journal of

DATA SCIENCE AND IOT MANAGEMENT SYSTEM

Peer Reviewed, Referred & Indexed Journal

ISSN: 3068-272X www.iidim.com Original Research Paper

An Efficient Framework for Real-Time Intrusion Detection in IoT Cyber Security Environments

Mrs. M.NVR Krishna Priya[1], Shaik Asma Firdose[2], Billipelli Tejaswi[3], Angalakurthi Hima Sree[4], Doppana Tejaswini[5], Bhanu Rekha Pandaraboyina[6]

[1]Assistant Professor, St. Ann's College of Engineering & Technology, Chirala, Andhra Pradesh 523157

[2-6]UG Student, St. Ann's College of Engineering & Technology, Chirala, Andhra Pradesh-523157

ABSTRACT: Computer networks are increasingly exposed to viruses, malicious activities, and other hostile attacks. Intrusion detection serves as a critical component of network security, acting as an active defence mech1`anism. However, traditional intrusion detection systems often provide lower accuracy, suffer from high false-positive rates, and fail to identify emerging intrusion patterns. To address these limitations, this study proposes a deep learning based framework for detecting cyber security vulnerabilities and breaches in cyber-physical systems. The framework contrasts unsupervised learning with discriminative deep learning approaches and incorporates a generative adversarial network to detect cyber threats within IoT-enabled industrial intelligent control (IIC) networks. The proposed method demonstrates improved reliability and effectiveness in identifying diverse attack types while maintaining the confidentiality and integrity of sensitive user and system information. State of the art deep learning classifiers including RNNs, MLPs, and DNNs integrated into the framework achieve strong true-negative and detection rates for attack categories such as Brute Force XXS, Brute Force WEB, DoS Hulk, and DOS_LOIC_HTTP across benchmark datasets like NSL-KDD, KDDCup99, and UNSW-NB15. Overall, the approach provides a robust, adaptable, and high-accuracy solution for modern network defence.

Key Words: Intrusion Detection, Deep Learning, Generative Adversarial Networks, Cyber-Physical Systems, IoT Security.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X ww.iidim.com Original Research Paper

1. 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 are widely used in medicine for genomics and diseases [4]. Deep Learning (DL) methods handle complex data structures and large datasets using forward and back propagation, but they raise concerns related to hyper parameter tuning, data privacy, and secure data movement. Since DL models rely heavily on sensitive training data, protecting confidentiality is critical. Intrusion Detection Systems (IDS), including Network-based (NIDS) and Host-based (HIDS), monitor network activity to identify malicious behavior, providing real-time alerts while ensuring minimal impact on system performance.

However, each generation selects a set of different deep learning pre-trained methods such as RNN, CNN, and DL MLP. The framework used discriminative architecture, which includes convolutional neural networks (CNN), recurrent neural networks (RNN), and deep neural networks (DNN), a set of items that are included in IDS independently. As a result, one individual item indicates a possible combination of many systems that will be used to build more profound and more relevant aspects. Deep learning algorithms are trained to evaluate the model's effectiveness by simply concatenating the in-depth features. The deep feature representations are then destroyed, and the final classification results are made with a network that was made by itself and had several dense, hidden layers.

2. LITERATURE SURVEY

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X ww.iidim.com Original Research Paper

The deep learning methods brought a big revolution in computer science with additional powerful subfields and various fields, including Natural Language Processing (NLP), machine learning, computer vision, and speech/audio processing. In visual data analytics, Convolutional Neural Networks (CNNs) have exhibited substantial gains in picture categorization, object identification, and video motion monitoring. A CNN contains a sequence of linear and nonlinear layers called a hierarchical structure, with a direct connection and shared weights. It was first proposed for simple picture recognition. LeNet-5 CNNs have two convolutional layers, each followed by a sub-sampling layer and, eventually, a convolution for class prediction. It was later widely employed in various scientific and real-world applications as hardware technology (e.g., GPUs) progressed [2].

Work in 2021 and 2022 of machine learning and deep learning for detecting intrusion and cyber security attacks. This survey has discussed the minimal work of deep learning and machine learning. The studies focused on the issues, challenges, and shortcomings of ML and DL techniques for detecting ICS anomalies and the current ICS-to-cloud infrastructure. ML methods secure ICT on the network and physical levels by managing the information through packets and controlling anomalies. The research on ML-AIDS identifies and efficiently implements the effective and efficient anomalies of networks and computers. Recently, many researchers have been dedicated to developing ML with NIDs. The IDS faced challenges in accuracy by reducing false alarm rates. For that reason, the DL with an IDS system was deployed as a potential solution to identify intrusion attacks. Beyond that, binary and multiclass experiments were performed on the CSECIC-IDS2018 and the Bot-IoT datasets.

3 SYSTEM ARCHITECTURE

The system architecture integrates IoT devices generating network traffic, followed by preprocessing and feature

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X ww.iidim.com Original Research Paper

extraction. Deep learning models including RNNs, MLPs, DNNs, and GANs are employed for classification and anomaly detection. The trained model performs intrusion detection, producing security alerts and responses to enhance overall network protection and system reliability.

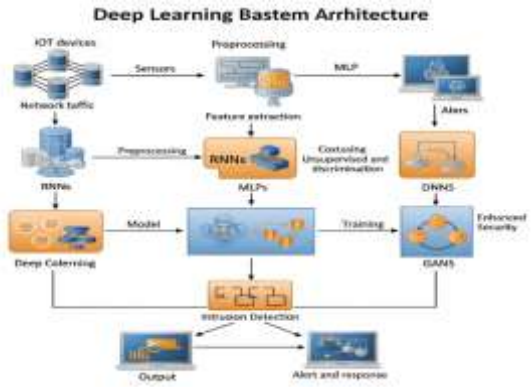

Fig 1: System Architecture

3.1 METHODOLOGY

The methodology of this research is designed to build a robust intrusion detection framework using deep learning techniques, evaluated on the UNSW-NB15 dataset. The process begins with dataset selection, where realistic normal and malicious traffic flows are collected. Each record contains protocol information, packet statistics, byte counts, and attack labels, making it suitable for both binary and multi-class classification tasks.

Next, data preprocessing is performed to improve model accuracy. Missing values are replaced with zeros, categorical features such as protocol type and service are label-encoded, and features are normalized to zero mean and unit variance. This ensures balanced contributions during training and prevents.

The baseline system employs CNN and RNN models. CNN extracts spatial patterns from traffic features, while RNN captures temporal dependencies. Although effective, these models show limitations in handling complex evolving attack scenarios. To overcome this, the proposed system introduces a Generative Adversarial Network (GAN). TheGAN consists of a generator that learns synthetic attack patterns and a discriminator that distinguishes real from generated traffic. This adversarial training improves robustness, addresses class imbalance, and enhances generalization to unseen attacks. The GAN objective function is defined as:

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.iidim.com Original Research Paper

$$\min_G \max_D V(D,G) = \mathbb{E}_{x\sim p_{data}(x)}[\log D(x)] + \mathbb{E}_{z\sim p_z(z)}[\log(1 - D(G(z)))]$$

where $D(x)$is the discriminator output for real data, $G(z)$is the generator output for synthetic data, and p_{data}, $p_z$represent the distributions of real and latent variables respectively.

Finally, performance evaluation is conducted using accuracy, precision, recall, and F1-score. Confusion matrices and comparative graphs are generated to analyze class-wise predictions. The trained GAN model is also tested on unseen traffic to validate real-time applicability, confirming its ability to detect and mitigate malicious intrusions in IoT-enabled cyber security infrastructures.

4. DESIGN AND CONSTRUCTION

The design of the proposed system is structured to provide a robust intrusion detection framework using deep learning models. The architecture begins with dataset acquisition, where the UNSW-NB15 dataset is selected due to its realistic representation of modern attack scenarios. Each record contains protocol information, packet statistics, and attack labels, making it suitable for both binary and multi-class classification tasks.

In the construction phase, the dataset undergoes preprocessing to ensure quality and consistency. Missing values are replaced with zeros, categorical features such as protocol type and service are label-encoded, and normalization is applied to balance feature contributions. The dataset is then reshaped to match the input requirements of CNN, RNN, and GAN models, and split into training and testing sets using an 80:20 ratio.

The baseline system employs CNN and RNN architectures. CNN extracts spatial correlations among traffic features, while RNN captures sequential dependencies. However, these models show limitations in handling evolving attack patterns. To address this, the proposed system incorporates a Generative Adversarial Network (GAN). The GAN consists of a generator that produces synthetic intrusion

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

patterns and a discriminator that distinguishes between real and generated traffic. This adversarial learning process enhances robustness, improves generalization, and reduces false positives. Finally, the constructed system is evaluated using accuracy, precision, recall, and F1-score. Confusion matrices and comparative performance graphs are generated to validate the effectiveness of the GAN model against CNN and RNN baselines. The deployment phase ensures real-time applicability, where the trained model predicts malicious traffic and initiates mitigation strategies, confirming its suitability for modern IoT cyber security infrastructures.

5 RESULTS AND DISCUSSION

The proposed GAN-based intrusion detection framework was implemented and compared against CNN and RNN models using the UNSW-NB15 dataset. The results highlight the effectiveness of adversarial learning in improving detection accuracy, robustness, and scalability for IoT-enabled cyber security infrastructures.

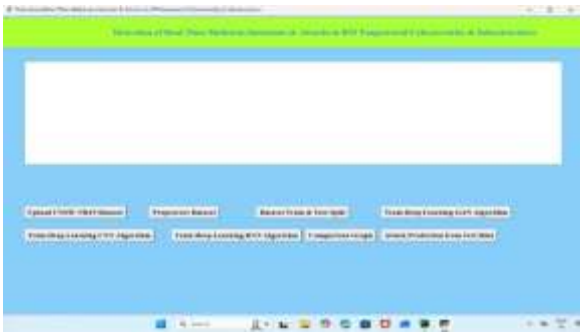

Fig 2: Model Deployment Environment

Figure 2 presents the system's workflow, beginning with dataset upload, pre-processing, and model training. This overview demonstrates the modular design of the framework, ensuring adaptability across different intrusion detection scenarios.

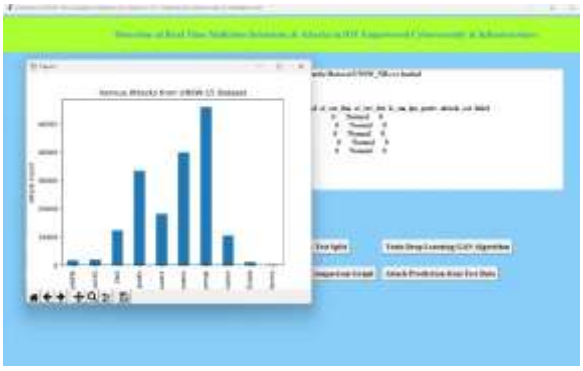

Fig 3. Preprocess Dataset

Figure 3 illustrates the pre-processing pipeline, including missing value handling, label encoding, and normalization. These steps significantly improved data quality

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.iidim.com Original Research Paper

and ensured balanced feature contributions during training.

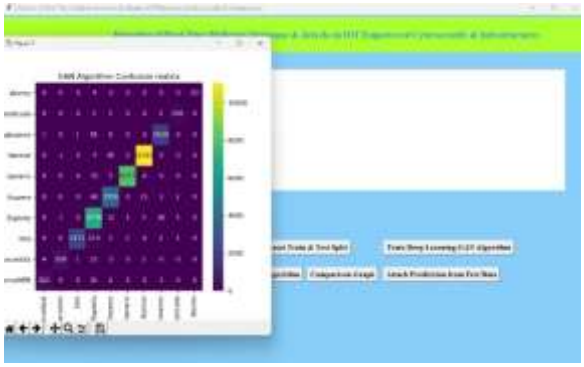

Fig 4: GAN Algorithm

Figure 4 shows the training process of the proposed GAN model. The generator and discriminator networks iteratively improved, resulting in enhanced robustness against unseen and zero-day attacks compared to CNN and RNN baselines.

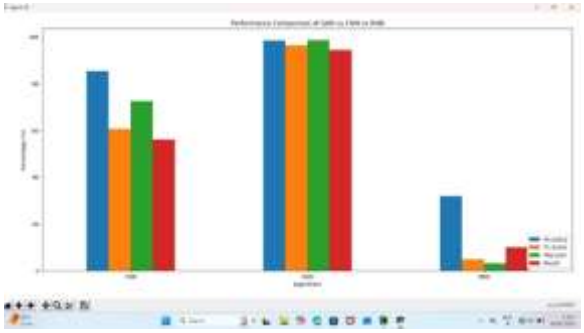

Fig 5: Comparison Graph

Figure 5 provides a comparative analysis of CNN, RNN, and GAN models. The GAN consistently achieved higher accuracy, precision, recall, and F1-scores, confirming its superiority in detecting diverse attack categories.

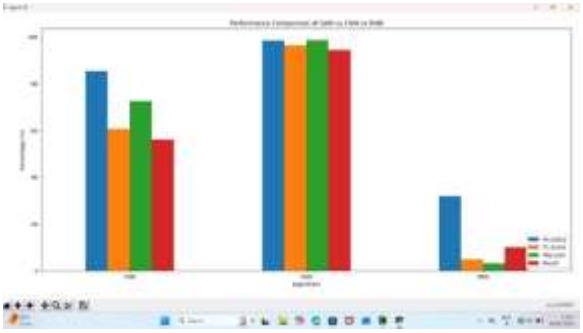

Fig 6: Attack Prediction from Test Data

Figure 6 demonstrates the model's real-time applicability. The GAN successfully classified malicious traffic with minimal false positives, validating its deployment potential in IoT cyber security infrastructures.

6. CONCLUSION

The proposed system provides an end-to-end solution for detecting real-time malicious intrusions and attacks in IoT-enabled cyber security environments. By integrating multiple deep learning algorithms, including conventional CNN and RNN models alongside a novel GAN-based approach, the system effectively

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X ww.iidim.com Original Research Paper

analyses network traffic data and classifies each request as normal or malicious. Data pre-processing, including handling missing values, encoding categorical features, and feature normalization, ensures that the models receive high-quality, consistent input. The use of one-hot encoding and train-test splitting allows accurate evaluation of model performance. Experimental results, supported by metrics such as accuracy, precision, recall, F1-score, and confusion matrices, demonstrate that the GAN-based model outperforms traditional deep learning models in detecting complex intrusion patterns and anomalous behavior. The inclusion of a user-friendly GUI enables real-time predictions and visualization of performance metrics, making the system practical for cyber security professionals and IoT infrastructure managers. Overall, the system demonstrates the feasibility and effectiveness of applying advanced deep learning techniques for proactive intrusion detection in modern networked environments.

FUTURE SCOPE

Future enhancements include adopting online learning techniques for continuous adaptation to emerging threats and integrating advanced hybrid models such as CNN, RNN, GAN, and Transformers to improve detection accuracy. Edge deployment can further optimize real-time performance and reduce network load, while incorporating explainable AI enhances transparency. Additionally, leveraging multi-modal data fusion will strengthen the system's ability to detect complex and zero-day attacks, ensuring greater scalability and robustness.

REFERENCES

[1] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," Nature, vol. 521, no. 7553, pp. 436–444, 2015.

[2] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "ImageNet classification with deep convolutional neural networks," Commun. ACM, vol. 60, no. 2, pp. 84–90, Jun. 2017.

[3] M. K. Islam, M. S. Ali, M. M. Ali, M. F. Haque, A. A. Das, M. M. Hossain,

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.iidim.com Original Research Paper

D. S. Duranta, and M. A. Rahman, "Melanoma skin lesions classification using deep convolutional neural network with transfer learning," in Proc. 1st Int. Conf. Artif. Intell. Data Analytics (CAIDA), Apr. 2021.

[4] A. Ahmim, M. Derdour, and M. A. Ferrag, "An intrusion detection system based on combining probability predictions of a tree of classifiers," Int. J. Commun. Syst., vol. 31, no. 9, p. e3547, Jun. 2018.

[5] 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.

[6] 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.

[7] 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.