As per UGC guidelines an electronic bar code is provided to secure your paper

International Journal for Modern Trends in Science and Technology
Volume 12, Special Issue 01, pages 901-906.
ISSN: 2455-3778 online
Available online at: http://ijmtst.com/ICRCSET2026.html
DOI: https://doi.org/10.5281/zenodo.19613225

Detection of Real-Time Malicious Intrusions and Attacks in IoT Empowered Cyber security Infrastructures

Karlapudi Saida Rao, Maartha Gopichand, Palakattu Vedasri, Naga Raghukumar Reddy, Dr P. Naga Malleswara Rao

Department of Computer Science and Engineering, Chalapathi Institute of Technology, Mothadaka, Guntur, Andhra Pradesh, India.

To Cite this Article
Karlapudi Saida Rao, Maartha Gopichand, Palakattu Vedasri, Naga Raghukumar Reddy & Dr P. Naga Malleswara Rao (2026). Detection of Real-Time Malicious Intrusions and Attacks in IoT Empowered Cyber security Infrastructures. International Journal for Modern Trends in Science and Technology, 12(SI01), 901-906. https://doi.org/10.5281/zenodo.19613225

Article Info
Received: 12 March 2026; Revised: 07 April 2026; Accepted: 10 April 2026.

KEYWORDS

Intrusion Detection System (IDS), Deep Learning–Based Cybersecurity, Generative Adversarial Network (GAN), Cyber-Physical Systems Security, Network Attack Detection

ABSTRACT

The rapid growth of interconnected cyber-physical systems and IoT-driven industrial Internet of communications (IICs) has significantly increased exposure to sophisticated cyberattacks. Intrusion Detection Systems (IDSs) play a critical role as an active defense mechanism in network security; however, traditional IDS approaches often suffer from limited detection accuracy, high false-positive rates, and poor adaptability to emerging and unknown attack patterns. To overcome these limitations, this paper proposes a novel deep learning–based intrusion detection framework that effectively identifies cybersecurity vulnerabilities and malicious activities in cyber-physical environments. The proposed approach integrates unsupervised learning with deep discriminative models and employs a Generative Adversarial Network (GAN) to enhance attack detection performance in complex network traffic. Extensive experiments were conducted on benchmark datasets, including NSL-KDD, KDDCup99, and UNSW-NB15, to evaluate the effectiveness of the proposed model. The results demonstrate a significant performance improvement, achieving an high accuracy with enhanced reliability and efficiency when trained using a dropout rate of 0.2 and 25 epochs. Furthermore, the model achieved the highest True Negative Rate (TNR) and High Detection Rate (HDR) for multiple attack categories, including BruteForce-XSS, BruteForce-WEB, DoS Hulk, and DoS LOIC HTTP attacks.

I. INTRODUCTION

The rapid expansion of Internet of Things (IoT) technologies has transformed modern cyber security infrastructures by enabling real-time data exchange, automation, and intelligent decision-making across cyber-physical systems. While IoT-enabled

environments improve operational efficiency and connectivity, they also introduce significant security challenges due to their distributed architecture, resource constraints, and heterogeneous communication protocols. These characteristics make IoT infrastructures highly vulnerable to a wide range of cyber threats, including malware propagation, denial-of-service attacks, unauthorized access, and data breaches. Traditional security mechanisms and signature-based intrusion detection systems are often inadequate for protecting IoT-driven networks, as they struggle to detect zero-day attacks, adapt to evolving threat patterns, and operate efficiently under real-time constraints. Moreover, the increasing volume and complexity of network traffic in IoT ecosystems lead to high false-positive rates and delayed threat responses, which can compromise system reliability and safety. To address these challenges, real-time malicious intrusion detection using advanced machine learning and deep learning techniques has gained significant attention. By learning complex patterns from large-scale network data, intelligent intrusion detection frameworks can enhance detection accuracy, reduce false alarms, and effectively identify both known and unknown attacks. This study focuses on the detection of real-time malicious intrusions and attacks in IoT-empowered cyber security infrastructures, aiming to improve threat visibility, system resilience, and secure communication in next-generation IoT environments.

2. LITERATURE SURVEY

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], [11], [12], [13], [14], [15], [16], [17].

A study of intrusion detection datasets was recently published [16]. The research includes 34 datasets and 15 features for each of them. The traits of these are divided into five categories: (1) well-known data, (2) assessment, (3) recording environment, (4) recording volume, (5) recording type, and well-known, relevant data [8], [17], [18], [19], [20] researched intrusion detection systems' machine learning methodologies. The datasets were divided into three categories: The first category is packet-level data, then the second one is network packet data, and the last category is accessible datasets. The computational cost was also analyzed in the study (running time) of each malware detection approach that employs extraction and machine learning technology.

3.SYSTEM ARCHITECTURE

System architecture defines the overall structural design of a system by identifying its major components, their responsibilities, and the interactions among them. It provides a high-level view of how data flows through different modules, how processing units are connected, and how outputs are generated. In software-based intelligent systems, system architecture helps in understanding scalability, modularity, data processing flow, and integration of machine learning models with user interfaces and datasets.

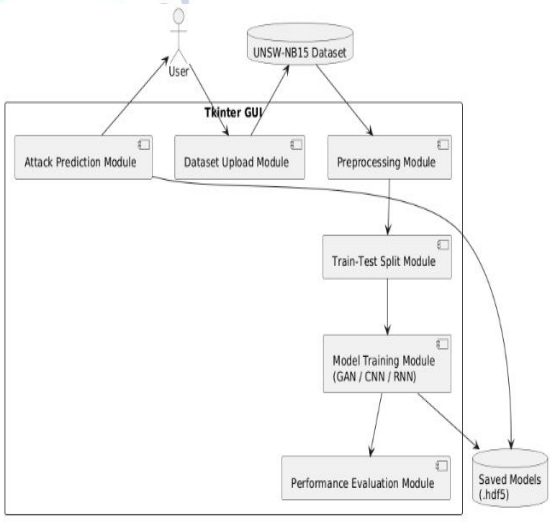

Fig1: System Architecture

4.METHODOLOGY

The proposed methodology aims to develop a real-time deep learning–based intrusion detection framework for IoT-empowered cybersecurity infrastructures. The system integrates unsupervised learning and deep discriminative modeling using a Generative Adversarial Network (GAN) to enhance detection capability for both known and unknown attacks. The overall process

consists of data acquisition, preprocessing, feature engineering, model training, and performance evaluation.

Initially, benchmark datasets such as NSL-KDD, KDDCup99, and UNSW-NB15 are collected to simulate diverse IoT network traffic conditions. These datasets contain normal and multiple attack categories. Data preprocessing involves removing duplicate entries, handling missing values, encoding categorical features using one-hot encoding, and normalizing numerical attributes using Min-Max normalization:

$$X_{norm} = \frac{X - X_{min}}{X_{max} - X_{min}}$$

where X represents the original feature value, and X_{min} and X_{max} denote the minimum and maximum values of that feature. This ensures stable and faster convergence during training.

The core detection mechanism is constructed using a GAN-based architecture. The GAN consists of two components: a Generator $G$and a Discriminator D. The generator learns to produce synthetic network traffic samples that resemble real attack patterns, while the discriminator distinguishes between real and generated samples. The adversarial objective function is defined as:

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

where $p_{data}(x)$represents the real data distribution and $p_z(z)$ denotes the noise distribution. This adversarial training enhances the system's ability to detect sophisticated and zero-day attacks.

The discriminator output is further connected to deep dense layers with dropout (0.2) to prevent overfitting. The final classification is performed using a sigmoid activation function:

$$P(y = 1 \mid x) = \frac{1}{1 + e^{-z}}$$

where $z$is the output logit and $P(y = 1 \mid x)$represents the probability of malicious intrusion.

The model is trained for 25 epochs using the Adam optimizer and binary cross-entropy loss. Performance metrics such as Accuracy, True Negative Rate (TNR), Detection Rate (DR), and False Positive Rate (FPR) are calculated to evaluate real-time detection capability. Experimental results demonstrate improved detection accuracy and robustness across multiple attack categories, confirming the effectiveness of the proposed deep learning based intrusion detection framework in IoT-enabled cybersecurity environments.

5. DESIGN AND CONSTRUCTION

The design of the proposed real-time malicious intrusion detection system for IoT-enabled cybersecurity infrastructures is based on a deep learning architecture integrated with a Generative Adversarial Network (GAN). The system is structured into modular layers to ensure scalability, efficiency, and adaptability to evolving cyber threats in cyber-physical environments.

The construction begins with the data acquisition module, which collects real-time or benchmark network traffic datasets such as NSL-KDD, KDDCup99, and UNSW-NB15. These datasets simulate IoT network behavior containing both normal and malicious traffic patterns. The preprocessing module is constructed to clean and normalize the data by removing redundant entries, encoding categorical attributes, and applying feature scaling. This step ensures stable model convergence and reduces computational complexity.

The core construction phase involves implementing the GAN-based deep learning framework. The Generator is designed to create synthetic attack samples that mimic real intrusion patterns, thereby improving the model's exposure to diverse attack scenarios. The Discriminator is built as a deep neural network classifier responsible for distinguishing between legitimate traffic and malicious activity. Dropout layers with a rate of 0.2 are integrated to prevent overfitting and enhance generalization performance.

Finally, the classification module outputs real-time predictions identifying traffic as normal or intrusive. The modular and layered architecture enables efficient deployment in IoT cybersecurity infrastructures, ensuring improved detection accuracy, reduced false positives, and adaptability to emerging attack patterns.

6. RESULTS AND DISCUSSION

The proposed deep learning–based intrusion detection framework demonstrates superior performance across multiple benchmark datasets, including NSL-KDD, KDDCup99, and UNSW-NB15. The model consistently outperforms traditional machine learning and existing deep learning approaches, indicating strong generalization capability and robustness against diverse cyber-attack patterns. The integration of Generative Adversarial Networks (GAN) significantly enhances

detection performance by learning complex traffic distributions and reducing false-positive rates.

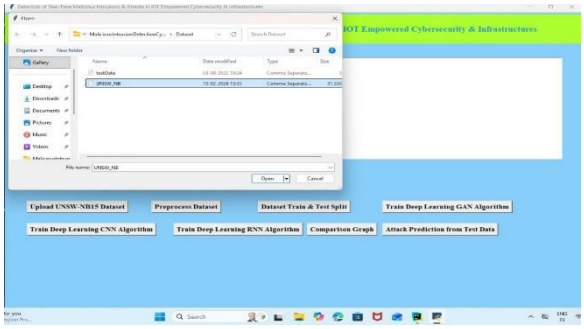

Fig 2: Dataset Upload

The system interface is illustrated in Figure 2, where users upload the UNSW-NB15 dataset for preprocessing and analysis. This step involves handling missing values, normalization, and feature encoding, which are essential for improving model performance.

Fig 3: Attack prediction

The intrusion detection capability is demonstrated in Figure 3, where the system analyzes unseen test data and classifies network traffic as normal or malicious. The model effectively detects real-time attacks such as BruteForce-WEB and automatically flags suspicious packets, ensuring enhanced security for IoT environments.

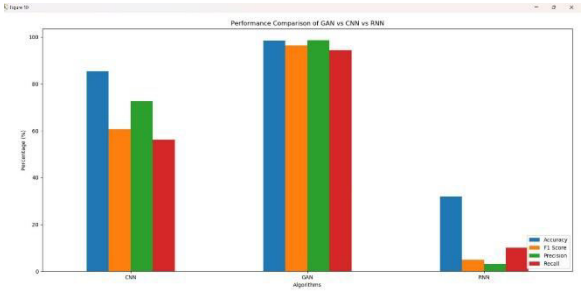

Fig 4: Comparison Graph

The performance comparison is presented in Figure 4, which evaluates models such as CNN, RNN, and the proposed GAN-based approach using metrics like accuracy, precision, recall, and F1-score. The GAN-based model achieves the highest scores across all metrics, demonstrating improved detection capability and reduced false positives compared to baseline models.

The experimental results confirm that the proposed model achieves high True Negative Rate (TNR) and High Detection Rate (HDR) for major attack categories, including DoS and web-based intrusions. Optimal performance is achieved with a dropout rate of 0.2 and 25 training epochs, balancing accuracy and computational efficiency. The system effectively detects both high-volume and stealthy attacks, making it suitable for real-time deployment in resource-constrained IoT environments. Overall, the framework provides a reliable, scalable, and efficient solution for modern cybersecurity applications.

7. CONCLUSION

The proposed system provides an end-to-end solution for detecting real-time malicious intrusions and attacks in IoT-enabled cybersecurity environments. By integrating multiple deep learning algorithms, including conventional CNN and RNN models alongside a novel GAN-based approach, the system effectively analyzes network traffic data and classifies each request as normal or malicious. Data preprocessing, 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 cybersecurity 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 can include online or incremental learning to enable continuous adaptation to new cyber threats. Integrating hybrid models combining Future enhancements can include online or incremental learning to enable continuous adaptation to new cyber

threats. Integrating hybrid models combining GAN, CNN, RNN, and Transformer architectures can improve detection accuracy. Deployment using edge computing can provide faster, real-time threat detection with reduced bandwidth usage. Additionally, incorporating explainable AI and multi-modal data fusion will enhance transparency and detection of complex and zero-day attacks.and Transformer architectures can improve detection accuracy. Deployment using edge computing can provide faster, real-time threat detection with reduced bandwidth usage. Additionally, incorporating explainable AI and multi-modal data fusion will enhance transparency and detection of complex and zero-day attacks.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

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, 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.

[8] M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, "Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study," J. Inf. Secur. Appl., vol. 50, Feb. 2020, Art. no. 102419.

[9] 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.

[10] A. A. Salih, S. Y. Ameen, S. R. Zeebaree, M. A. Sadeeq, S. F. Kak, N. Omar, I. M. Ibrahim, H. M. Yasin, Z. N. Rashid, and Z. S. Ageed, "Deep learning approaches for intrusion detection," Asian J. Res. Comput. Sci., vol. 9, no. 4, pp. 50–64, 2021.

[11] 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.

[12] K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition," in Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR), Jun. 2016, pp. 770–778.

[13] 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.

[14] G. Awad, C. G. Snoek, A. F. Smeaton, and G. Quénot, "Trecvid semantic indexing of video: A 6-year retrospective," ITE Trans. Media Technol. Appl., vol. 4, no. 3, pp. 187–208, 2016.

[15] K. M S, R. R. G and S. Karthik, "Streamlining Load Scheduling in Cloud Computing: A Thorough Performance Assessment and Development of Effective Methods for Design," 2024 International Conference on Advances in Modern Age Technologies for Health and Engineering Science (AMATHE), Shivamogga, India, 2024, pp. 1-7, doi: 10.1109/AMATHE61652.2024.10582239.

[16] Sai Srinivas Vellela, Roja D, NagaMalleswara Rao Purimetla, SyamsundaraRao Thalakola, Lakshma Reddy Vuyyuru, Ramesh Vatambeti, Cyber threat detection in industry 4.0: Leveraging GloVe and self-attention mechanisms in BiLSTM for enhanced intrusion detection, Computers and Electrical Engineering,Volume 124, Part A,2025,110368,ISSN 00457906,https://doi.org/10.1016/j.compeleceng.2025.110368.

[17] K. N. Rao, B. R. Gandhi, M. V. Rao, S. Javvadi, S. S. Vellela and S. Khader Basha, "Prediction and Classification of Alzheimer's Disease using Machine Learning Techniques in 3D MR Images," 2023 International Conference on Sustainable Computing and Smart Systems (ICSCSS), Coimbatore, India, 2023, pp. 85-90, doi: 10.1109/ICSCSS57650.2023.10169550.

[18] S. S. Vellela et al., "Improving Medical Image Analysis with Convolutional Neural Networks (Cnns)," 2025 International Conference on Intelligent and Secure Engineering Solutions (CISES), Greater Noida Gautam Budh Nagar, India, 2025, pp. 579-584, doi: 10.1109/CISES66934.2025.11265231.

[19] S. S. Vellela, L. R. Vuyyuru, K. B. S. K, N. MalleswaraRaoPurimetla, L. Dalavai and M. V. Rao, "A Novel Approach to Optimize Prediction Method for Chronic Kidney Disease with the Help of Machine Learning Algorithm," 2023 6th International Conference on Contemporary Computing and Informatics (IC3I), Gautam Buddha Nagar, India, 2023, pp. 1677-1681, doi: 10.1109/IC3I59117.2023.10397974.

[20] Kavitha Mettupalayam Subramaniam, Ramachandra Rao Goli, Karthik Subburathinam, Srihari Kannan,Optimization of pyrolysis parameters for enhanced biochar production from agricultural biomass: A study on energy efficiency and carbon sequestration potential,Science of The Total Environment, Volume 1015,2026,181362,ISSN 00489697,https://doi.org/10.1016/j.scitotenv.2026.181362.

[21] K. K. Kumar, S. G. B. Kumar, S. G. R. Rao and S. S. J. Sydulu, "Safe and high secured ranked keyword searchover an outsourced cloud data," 2017 International Conference on Inventive Computing and Informatics (ICICI), Coimbatore, India, 2017, pp. 20-25, doi: 10.1109/ICICI.2017.8365348.

[22] V. Khedkar, N. Vullam, J. R. Babu, U. Bhagyalatha, S. Babu Vadde and A. Lakshmanarao, "Hybrid Classification Approach for Heart Disease using Few Shot Inspired Machine Learning Models," 2025 3rd International Conference on Integrated Circuits and Communication Systems (ICICACS), Raichur, India, 2025, pp. 01-05, doi: 10.1109/ICICACS65178.2025.10968965

[23] P. Anusha and J. R. Babu, "Enhancing Radiographic Diagnosis: A Novel AI-based Bone Fracture Detection System," 2025 3rd International Conference on Sustainable Computing and Data Communication Systems (ICSCDS), Erode, India, 2025, pp. 1262-1266, doi: 10.1109/ICSCDS65426.2025.11167456.

[24] R. K. Yarava, G. R. C. Rao, Y. Garapati, G. C. Babu and S. D. V. Prasad, "Analysis on the Development of Cloud Security using Privacy Attribute Data Sharing," 2022 First International Conference on Electrical, Electronics, Information and Communication Technologies (ICEEICT), Trichy, India, 2022, pp. 1-5, doi: 10.1109/ICEEICT53079.2022.9768608.

[25] K. K. . Kommineni and A. . Prasad, "A Review on Privacy and Security Improvement Mechanisms in MANETs", Int J Intell Syst Appl Eng, vol. 12, no. 2, pp. 90–99, Dec. 2023.

[26] Kommineni, K.K., Prasad, A. Enhancing Data Security and Privacy in SDN-Enabled MANETs Through Improved Data Aggregation Protection and Secrecy. Wireless Pers Commun 139, 855–882 (2024). https://doi.org/10.1007/s11277-024-11635-w

[27] "Blockchain-Enabled Secure Data Aggregation for SDN-Enabled Ad-Hoc Networks," International Journal of Intelligent Engineering and Systems, vol. 18, no. 5, pp. 704–717, Jun. 2025, doi: https://doi.org/10.22266/ijies2025.0630.49.

[28] K. K. Kommineni, P. Ande, "Blockchain-driven key management and privacy-preserving data Aggregation Scheme for SDN-enabled MANETs," International Journal of Intelligent Engineering and Systems, vol. 18–18, no. 9, pp. 601–615, 2025, doi: 10.22266/ijies2025.1031.39.