Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

Securing Communication Systems with AI-Powered Intrusion Detection Frameworks

Vijay Kumar Sharma[1], Dr. Navin Kumar Agrawal[2]

[1]Research Scholar, Department of Electronics & Communication Engineering, Bhabha University, India
[2]Professor, Department of Electronics & Communication Engineering, Bhabha University, India
Email: vijaykumarsharma24@gmail.com

The fast growth in communication technologies has created their vulnerability to advanced cyber-attacks. The need to devise well-founded security architecture has thus been forged. This research works on an Intrusion Detection System based on AI that integrates XGBoost and DNN to boost the security resilience of communication systems. Using the NSL-KDD dataset, the proposed framework applies preprocessing methods-posits-Min-Max normalization and feature selection based on XGBoost-to enhance the model efficiency and accuracy. The hybrid XGBoost-DNN model was assessed with utmost rigor through standard performance measurement techniques by attaining an accuracy of 99.9% with optimum precision and recall on bigger datasets. Comparative analysis has shown that this model surpasses existing techniques based on logistic regression, Naïve Bayes and other support updating machine criteria. The research further goes on to exploit satisfactory implementations of the framework in a challenging class of communication environments, such as UAV-assisted networks and blockchain based infrastructures, ensuring scalability and robustness against the oncoming alterations in cyber-threats. This work presents the perspective of AI in modern cyber-security illustrated as a scalable and adaptive means for shielding the core communication infrastructure against an ever-growing threat landscape.

Keywords: AI-Powered Intrusion Detection, XGBoost, Deep Neural Networks, Communication Systems Security, Cybersecurity, UAV-Assisted Networks, Blockchain, NSL-KDD Dataset, Anomaly Detection, 5G and 6G Networks

1. Introduction

The communication systems act as the lifeblood of digital infrastructures today and keep information flowing across networks. However, with the evolution of the communication systems, they are becoming ever more complex and susceptible to sophisticated cyber-attacks, such as data breaches and denial-of-service attacks. Traditional countermeasures no longer seem adequate in combating evolving and more sophisticated threats, making it essential for adaptive, intelligent, and proactive security solutions. Cellular networks system configurations tend to pose high security challenges given their complicated, heterogeneous architecture and legacy trust models that need to operate together while guaranteeing interoperability. Initially started within closed environments, these systems were exposed to more vulnerabilities simply because newer entrants into the environment would introduce newer technologies. The existence of neither one unified security architecture nor domain-specific threat modeling frameworks applicable in mobile networks has compounded the need for specialized approaches. While MITRE ATT&CK has begun to fill this identified gap, no mobile network-specific frameworks exist. Hence, this paper proposes a domain-specific framework for facilitating 2G, 3G, and 4G networks in transparent discussions on security problems, which ultimately provide better security for 5G and beyond [1].

Due to their speed, low cost, and versatility, unmanned aerial vehicles (UAVs) have become useful tools in disaster management, real-time surveillance, healthcare, and wireless communication [2],[3]. UAV-assisted communications rely on these aerial vehicles to act as base stations or relays with the aim of improving coverage and flexibility of the communication networks in difficult environments. However, this approach poses several significant problems, such as deployment strategies, effective resource allocation, and security challenges like distributed denial of service (DDoS) attacks, spoofing, eavesdropping, etc. [4],[5]. However, blockchain can be a potential solution to facilitate decentralized, secure mechanisms; enhance trust, data integrity, and interoperability among UAV networks [6]. Blockchain's high computational complexity and issues of scalability pose challenges in this respect; hence, further research is needed to optimize its complementary use with UAV systems for enhanced and secure communications [7],[8]. The technology of wireless communication has continued to evolve from the very first generation to the current 5G networks, offering-a very high data rate, extensive bandwidth assignment, and wide-ranging applications. As besetting researchers are looking to the 6G network options, security, privacy, and legal frameworks remain high on the list, particularly since wireless communications typically broadcast data and transmit sensitive information. Though regulations already exist surrounding the respective fields of healthcare, AI, and IoT, concrete protections of privacy and security within future 6G networks require additional attention [9].

AI has become a disruptive force in cybersecurity, bringing with it powerful tools for real-time threat detection and response. AI-based methods, including machine learning and deep learning, enable the analysis of vast amounts of network data to identify patterns, predict intrusion, or adapt to new threats with greater accuracy. In communication networks, an AI-based Intrusion Detection System (IDS) vastly outperforms traditional security measures. This is accomplished through continuous learning with respect to new threats and evolving strategies for detection. This research point very much upon integrating AI, mainly hybrid models like that of XGBoost with Deep Neural Networks (DNN), to bolster the security and resilience of communication systems. Such advanced frameworks in AI are critical for both the near and distant future of existing networks and for dealing with challenges in security that may arise as technologies such as 6G, UAV-assisted communications, and decentralized blockchain-based networks take root. The aim here would be combining AI along with application-specific threat modeling and legal frameworks to build a safer adaptive forward-looking communication ecosystem.

2. LITERATURE REVIEW

The rapid spread of IoT and its exposure to these attacks highlighted the critical need for effective intrusion detection systems (IDS). Deep Learning (DL) based initiatives have been reported to have been100% successful in these kinds of situations: A new IDS is a multi-dimensional classifier targeted on detecting several attacks such as blackhole attacks, DDoS, and sinkhole, with an impressive accuracy of 93.74% [10]. The DCGR_IoT system, based on CNNs, achieves spatial feature extraction, while the CGRN architecture accomplishes temporal feature extraction in a combination of datasets like UNSW-NB15 and KDDCup99, achieving good accuracies as high as 99.2% in some cases [11]. A different work done on AMI used XGBoost for feature selection, ADASYN for data balancing, CNN for construction of spatial features, and transformers to extract temporal relationships-leading to statistics of accuracies around 97.85%, 91.04%, 91.06%, achieved across the three datasets they tested on [12]. Artificial Intelligence enhances immensely the capability of Intrusion Detection Systems wherein innovations such as CyberAIBot process through Deep Learning technology in the edge cloud computing environment. The framework adopts Long Short-Term Memory networks and Support Vector Machine technology for the analysis of large datasets. It indicates that LSTM networks are proving to take a long time for training, although they provide much better performance on the detection [13]. Other research brings forward the top 10 AI-deep learning models for IoT anomaly detection. Convolutional Neural Network, Generative Adversarial Network, and Multilayer Perceptrons have the highest accuracy scores of almost 99.6% [14]. Also, a hybrid Deep Learning-based Network Intrusion Detection System, which combined Convolutional and Recurrent Neural Networks, enabled a detection accuracy of malicious network activities at 98.90% with the CICIDS-2018 dataset [15].

The advent of smart technologies in the industrial sector has paved the way for the development of hybrid deep learning models like CNN plus GRU for anomaly detection in Industrial IoT (IIoT) systems. The model achieved an accuracy of 94.94%, while suggesting more future improvements using XGBoost for feature enhancement, reaching about 96.41% accuracy in experimental results [16]. Hybrid models, which blend boosts in deep learning networks with other machine learning techniques, have also yielded positive results in traditional networking environments. For instance, combining SMOTE for data balancing and XGBoost for feature selection attained near-perfect accuracy on benchmark datasets like KDDCUP'99 and CIC-MalMem-2022 [17]. An APT-Aware IDS was based on AdaBoost and a Dynamic Deception system for defense and yielded an accuracy of about 99.9% [18]. Emerging network architectures, including satellite-terrestrial integrated networks (STINs), face a unique set of security challenges that require dedicated IDS solutions. Using Sequential Forward Selection (SFS) with Random Forest (RF) feature optimization, recent studies introduced four hybrid IDS models combined with ML/DL models such as LSTM, ANN, and GRU. Thus, these models manifested improved detection rates, with accuracies ranging from 79% to 90.5% across satellite and terrestrial datasets [19]. Finally, when considering the growing threat of zero-day attacks, a hybrid IDS that combines CNN and GRU to optimize network parameters recorded an accuracy of 98.73% and a remarkably low false-positive rate of 0.075, outperforming existing models in real-world cybersecurity setups [20]. Hence, such advancements highlight the changing landscape of network security where AI and DL still play significant roles in augmenting intrusion detection across various technological domains.

Table 1: Comparative Analysis of Intrusion Detection Systems (IDS) and Anomaly Detection Models in Network Security

Ref. No.	Techniques Used	Model Used	Key Findings	Limitations
[10]	Deep Learning (DL), Fully Connected (FC) Network	Four-layer FC Network	93.74% accuracy in detecting multiple attacks	Limited to predefined attack types
[11]	Convolutional Neural Networks (CNN), Complex Gated Recurrent Networks (CGRN)	DCGR_IoT	99.2% accuracy in anomaly detection	High computational complexity
[12]	XGBoost, ADASYN, CNN, Transformer	Deep Learning-based IDS	High accuracy (up to 97.85%) across datasets	Potential overfitting on smaller datasets
[13]	Deep Learning (DL), Long Short-Term Memory (LSTM), Support Vector Machines (SVM)	CyberAIBot	LSTM clusters perform better despite slower training	LSTM slower training times
[14]	Top 10 Deep Learning Techniques (CNN, GANs, Multilayer Perceptron)	Various Neural Networks (CNN, GANs, MLP)	CNN, GANs, and MLP achieved top accuracies (~99.6%)	Execution time and computational load
[15]	Convolutional Recurrent Neural Network (CRNN)	Hybrid Deep Learning-based NIDS	98.90% accuracy in intrusion detection	Requires large datasets for training
[16]	Hybrid Deep Learning (CNN+GRU)	CNN+GRU	96.41% accuracy with low FAR and high precision	May not generalize to non-IIoT contexts
[17]	SMOTE, XGBoost, Machine Learning (ML), Deep Learning (DL)	Hybrid ML and DL	99.99% accuracy on KDDCUP'99 and 100% on CIC-MalMem-2022	Potential overfitting with highly balanced data
[18]	Modified Lateral Movement Detection, AdaBoost, Dynamic Deception System	Dynamic Deception System with AdaBoost	99.9% accuracy and 0.99 F1-score in APT detection	High resource consumption for dynamic defense
[19]	Sequential Forward Selection (SFS), Random Forest (RF), LSTM, ANN, GRU	Hybrid ML/DL SAT-IDS	Up to 90.5% accuracy with optimized features	Complex integration between satellite and terrestrial systems
[20]	Convolutional Neural Networks (CNN), Gated Recurrent Units (GRU)	CNN-GRU Hybrid	98.73% accuracy with 0.075 FPR	Scalability and computational overhead

3. RESEARCH OBJECTIVES

The primary objective of this research is to develop an advanced, scalable, and adaptive intrusion detection system (IDS) utilizing deep learning models to effectively identify and mitigate security threats in communication networks. The focus is on addressing the limitations of traditional IDS and leveraging the capabilities of deep learning to enhance detection accuracy, reduce false positives, and adapt to evolving attack patterns in real-time. Specifically, the research aims to:

1. To Develop a Deep Learning-Based Intrusion Detection System (IDS): Design and implement a robust, scalable, and adaptive IDS that leverages advanced deep learning architectures to detect and mitigate cyber threats in communication networks with high accuracy and minimal false-positive rates.

2. To Enhance Real-Time Detection Capabilities: Create a deep learning model capable of processing high-dimensional and large-scale network traffic data efficiently, enabling real-time detection of intrusions in dynamic communication environments.

3. To Address Dataset Challenges in Intrusion Detection: Tackle issues such as class imbalance, outdated attack patterns, and lack of realistic datasets by preprocessing existing data or generating synthetic data that accurately represents modern communication network traffic and attack scenarios.

4. To Improve the Explainability and Interpretability of Intrusion Detection Models: Integrate explainable AI techniques into the proposed deep learning model to ensure transparency in decision-making, fostering trust and usability in critical applications.

The main objectives/goals of this work are-

(1) To detect intrusion from communication network using benchmark dataset.

(2) To develop a deep-learning hybrid model for the identification of intruder in network.

(3) To achieve high accuracy over the state-of-the-art.

By achieving these objectives, the research seeks to enhance the security and reliability of communication networks, providing an effective solution to safeguard against modern and emerging cyber threats.

4. RESEARCH METHODOLOGY

1. Dataset Selection

This new approach to intrusion detection will focus on the NSL-KDD dataset, a benchmark dataset commonly used in research on network intrusion detection, which is balanced and refined from its original version, KDD'99, as it removes redundant and duplicate records, so that it does not affect the evaluation of the machine learning models.

2. Data Preprocessing

The preprocessing steps below were applied to the dataset to maintain the integrity and consistency of the data:

- Data Cleaning: The raw NSL-KDD dataset underwent data cleaning to remove noise, missing values, or any other discrepancies from the dataset that could hinder model performance.

- Normalization: The cleaned dataset was subjected to Min-Max normalization such that all feature values are within a range of [0, 1]. This ensures that no feature dominates the learning process because of a difference in scale.

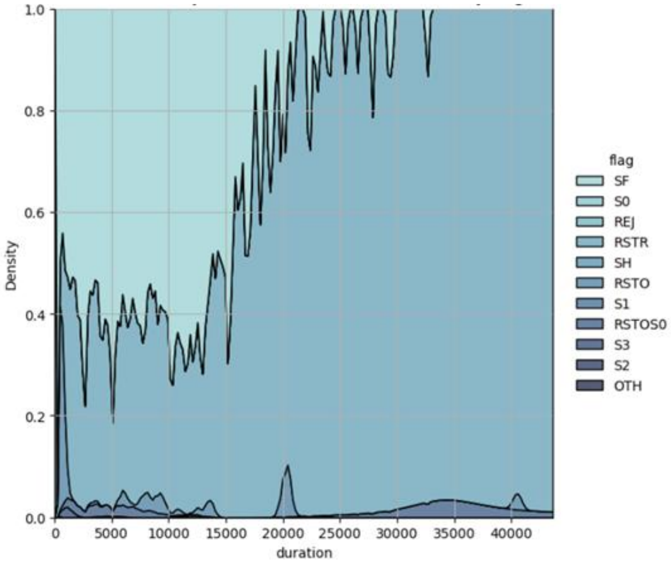

Fig.1: Kernel Density Estimate (KDE) Plot of Duration by Flag

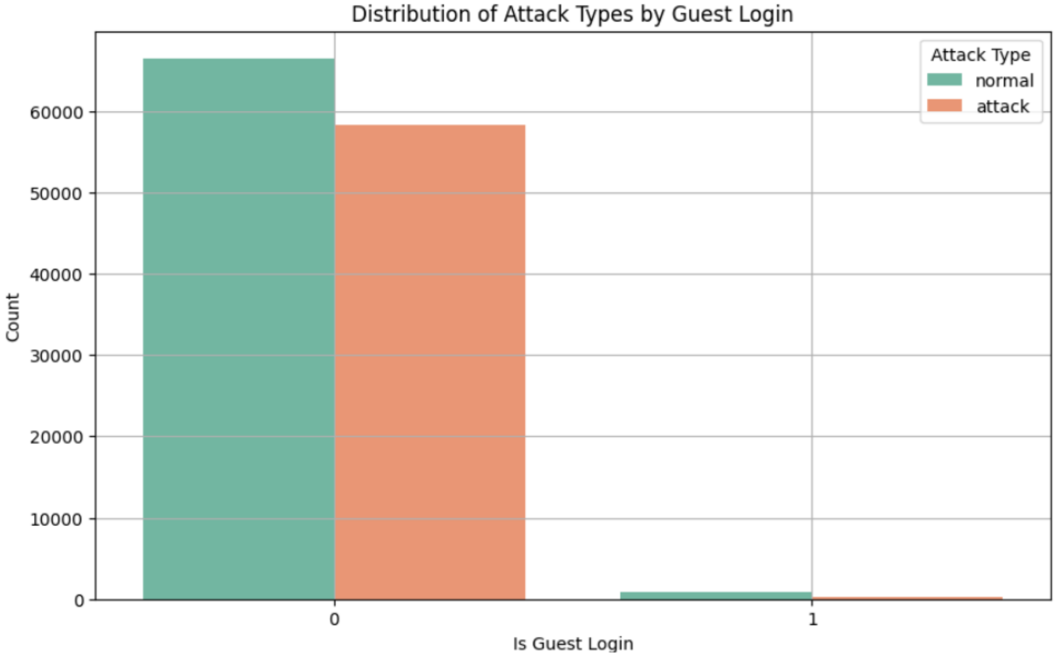

Fig.2: Distribution of Attack Types by Guest Login

3. Feature Selection

XGBoost was somehow central to our work since this feature selection method, based on gradient boosting, was applied to generate feature importance scores over the dataset. Ultimately, the features with the highest importance were kept for the classification phase, thus reducing dimensionality and allowing efficient work by a model.

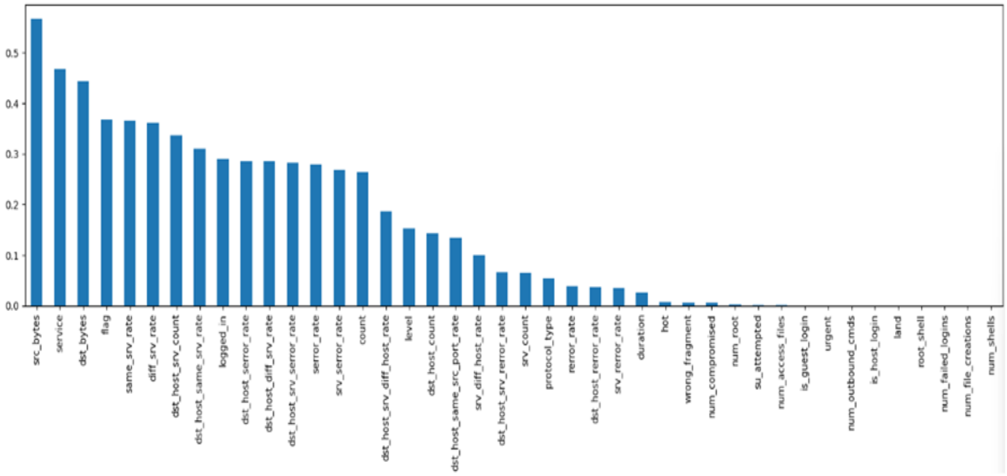

Fig.3: Features of dataset

4. Model Construction

The heart of the proposed intrusion detection system is a hybrid model made up of XGBoost combined with a deep neural network (DNN):

- XGBoost Part: Worked mainly on feature selection and refined the input data fed into the deep learning model.
- DNN Part: Constructed with many hidden layers and activation functions suitable for classification problems. The DNN was trained with the XGBoost-console-selected features to distinguish normal from attack traffic flow in the network.

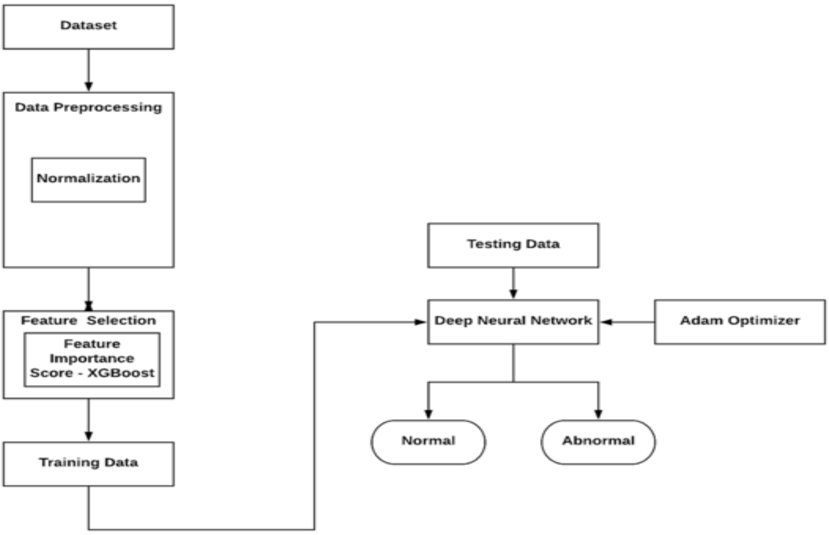

Fig.4: Proposed XGBoost classifier model for network intrusion detection

5. Training and Evaluation

Finally, the DNN classifier was built with the NSL-KDD dataset after the preprocessing and feature selection steps were performed; its performance was assessed on standard classification metrics. Accuracy; Precision; Recall; Area Under Curing (AUC).

This evaluation was performed with varied numbers of population in increases from 1,000 to 7,000 data samples to evaluate scalability and robustness for the proposed framework.

5. RESULTS AND DISCUSSION

1. Accuracy Analysis

All models within this proposed XGBoost–DNN framework consistently surpassed the traditional learning models (Logistic regression, Naive Bayes, and Support Vector Machine) for all population sizes. The best achieved accuracy stood at 99.9% for 7000 samples. The improvement is therefore quite considerable because, for instance, the maximum accuracy SVM could achieve levelled off at approximately 90% and hence it was always lagging the Naive Bayes that with 55% at most.

Modelling efforts are a testament to the ability of the hybrid model to learn complicated traits effectively within the network data that allowed better performance in intrusion detection.

2. Precision and Recall

- Precision: With 7000 samples, the proposed model algorithm reveals high precision, measuring 1.00. This almost completely removes the false positive rate, which implies the assurance that normal traffic does not get misclassified as malicious.

- Recall: The 1.00 recall indicates that the model is identifying all true attacks, with zero misses.

Whereas traditional models found it difficult. This is very much evident with Naive Bayes having yielded a 0.52 recall in large datasets.

3. AUC and Prediction Distribution

- The AUC curve proves the proposed model to possess high discriminative power, meaning it performed excellently in discriminating between normal and attack classes.

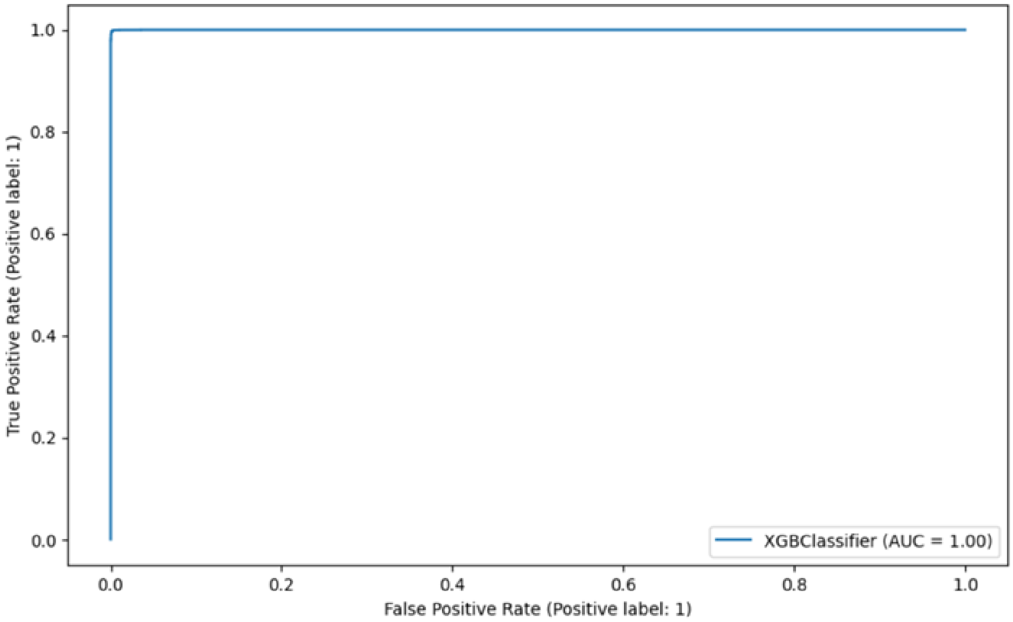

Fig.5: AUC Curve of proposed model

- The prediction distribution confirms the stability of the model, with classification remaining constant and precise against the various data samples.

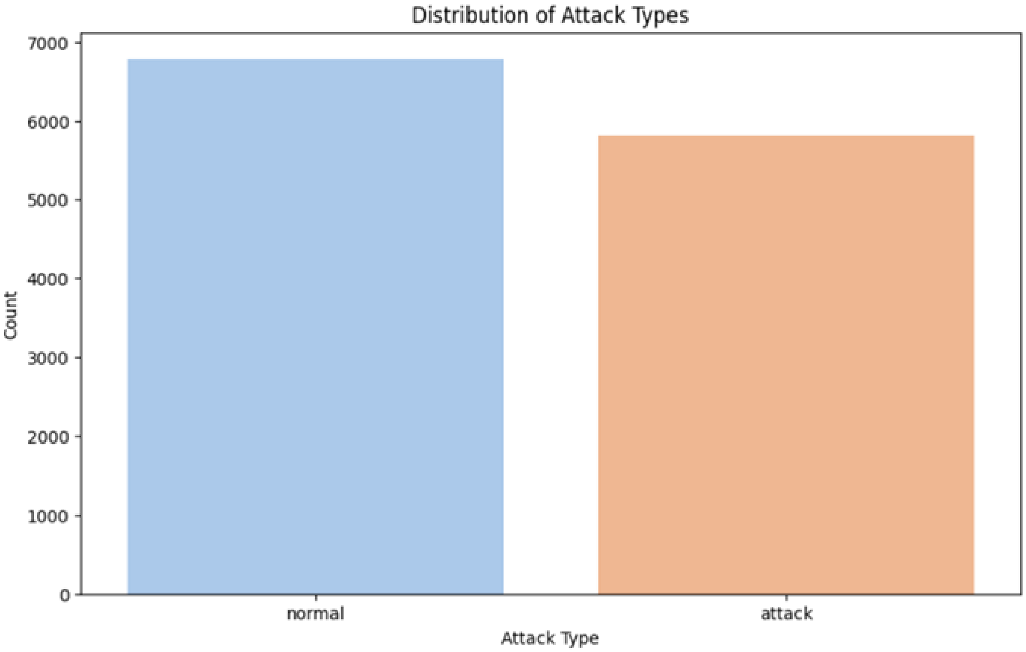

Fig.6: Prediction distribution of proposed model

4. Comparative Analysis

- Comparative analysis showed that the hybrid XGBoost–DNN model consistently outperformed most standalone models regarding accuracy, precision, and recall.

Table 2: Comparative analysis of the proposed model and the existing models based on accuracy

Population size	Accuracy			
	XGBoost	LR	NB	SVM
1000	0.969	0.91	0.85	0.73
2000	0.971	0.88	0.83	0.78
3000	0.974	0.88	0.55	0.82
4000	0.982	0.87	0.53	0.88
5000	0.989	0.86	0.52	0.89
6000	0.995	0.87	0.52	0.89
7000	0.999	0.87	0.52	0.90

Table 3: Comparative analysis of the proposed model and the existing models based on precision

Population	Precision			
	XGBoost	LR	NB	SVM
1000	0.97	0.91	0.85	0.81
2000	0.97	0.92	0.83	0.83
3000	0.98	0.87	0.29	0.86
4000	0.98	0.87	0.38	0.88
5000	0.99	0.87	0.27	0.89
6000	0.99	0.87	0.27	0.89
7000	1.00	0.87	0.28	0.90

Table 4: Comparative analysis of the proposed model and the existing models based on recall

Population size	Recall			
	XGBoost	LR	NB	SVM
1000	0.97	0.91	0.85	0.70
2000	0.97	0.92	0.83	0.75
3000	0.98	0.87	0.54	0.80
4000	0.98	0.87	0.53	0.89
5000	0.99	0.87	0.52	0.89
6000	0.99	0.87	0.52	0.89
7000	1.00	0.87	0.52	0.90

- Moderately good performance of the SVM and Logistic Regression is noticed but could not adapt as desired from the proposed deep learning framework.

- Under circumstances when larger data sets are applied, Naive Bayes suffers from a serious handicap since it does not work well with complex patterns of network intrusion.

Discussion

The results highlight the variable effectiveness of an integration of gradient boosting for feature selection and the deep learning capabilities of DNN. This collaboration offers a significant growth in performance on intrusion detection throughout communication networks. Some key observations are:

- High scalability: The model maintained high accuracy and precision even in large datasets.

- Reduced false positives and false negatives: The hybrid approach would minimize misclassifications resulting in reliable detection.

- Efficiency in feature selection: Mostly, XGBoost effectively provided dimensionality reduction without any performance degradation in the model.

6. CONCLUSION

Integrating artificial intelligence into intrusion detection systems has drastically changed the whole security landscape of communication networks. The new hybrid model using a dual approach of the extended gradient boosting and deep neural networks has been shown to be highly effective against a comprehensive array of cyber forwards. Performance was verified for the proposed system play by the NSL-KDD dataset against benchmark performance of other methods. The system outperformed traditional machine learning in the metrics of accuracy, precision, and recall. The framework doesn't just addresses current security challenges, but it will also play a solid foundation in turning the left to itself-a future of securing communication infrastructures against ever-growing attacks from cyber-attacks. Additionally, this work draws attention to AI-driven approaches in fostering resilience and reliability within networks. In addition to advanced feature selection methods using deep learning architectures, the system implements solutions with minimum false positives and maximum negatives, fostering trust in the network operations. The comparative analysis with other existing models attests to the superiority of the proposed one, which will further open the road for more implementation in various communication scenarios. Since cyber threats are ever-evolving, this work argues towards continuous reformation of AI-based security measures, which ensures proactive defenses to preserve digital infrastructures.

References

1. Rao, S. P., Chen, H. Y., & Aura, T. (2023). Threat modeling framework for mobile communication systems. Computers & Security, 125, 103047. https://doi.org/10.1016/j.cose.2022.103047
2. Hafeez, S., Khan, A. R., Al-Quraan, M. M., Mohjazi, L., Zoha, A., Imran, M. A., & Sun, Y. (2023). Blockchain-assisted UAV communication systems: A comprehensive survey. IEEE Open Journal of Vehicular Technology, 4, 558-580. Digital Object Identifier 10.1109/OJVT.2023.3295208

3. H. Kang, J. Joung, J. Kim, J. Kang, and Y. S. Cho, “Protect your sky: A survey of counter unmanned aerial vehicle systems,” IEEE Access, vol. 8, pp. 168671–168710, 2020.
4. J. Li et al., “Joint optimization on trajectory, altitude, velocity, and link scheduling for minimum mission time in UAV-Aided data collection,” IEEE Internet Things J., vol. 7, no. 2, pp. 1464–1475, Feb. 2020.
5. Z. Ullah, F. Al-Turjman, U. Moatasim, L. Mostarda, and R. Gagliardi, “UAVs joint optimization problems and machine learning to improve the 5G and beyond communication,” Comput. Netw., vol. 182, 2020, Art. no. 107478.
6. M. Soni and D. K. Singh, “Blockchain-based group authentication scheme for 6G communication network,” Phys. Commun., vol. 57, 2023, Art. no. 102005.
7. R. Majeed, N. A. Abdullah, M. F. Mushtaq, and R. Kazmi, “Drone security: Issues and challenges,” Parameters, vol. 2, 2021, Art. no. 5GHz.
8. G. K. Pandey, D. S. Gurjar, H. H. Nguyen, and S. Yadav, “Security threats and mitigation techniques in UAV communications: A comprehensive survey,” IEEE Access, vol. 10, pp. 112858–112897, 2022.
9. Musa, A. (2023). Legal frameworks for security schemes in wireless communication systems. Security and Privacy Schemes for Dense 6G Wireless Communication Networks, 423-444.
10. Awajan, A. (2023). A novel deep learning-based intrusion detection system for IOT networks. Computers, 12(2), 34. https://doi.org/10.3390/computers12020034
11. El-Shafeiy, E., Elsayed, W. M., Elwahsh, H., Alsabaan, M., Ibrahem, M. I., & Elhady, G. F. (2024). Deep Complex Gated Recurrent Networks-Based IoT Network Intrusion Detection Systems. Sensors, 24(18), 5933. https://doi.org/10.3390/s24185933
12. Yao, R., Wang, N., Chen, P., Ma, D., & Sheng, X. (2023). A CNN-transformer hybrid approach for an intrusion detection system in advanced metering infrastructure. Multimedia Tools and Applications, 82(13), 19463-19486. https://doi.org/10.1007/s11042-022-14121-2
13. Serrano, W. (2024). CyberAIBot: Artificial Intelligence in an Intrusion Detection System for CyberSecurity in the IoT. Future Generation Computer Systems, 107543. https://doi.org/10.1016/j.future.2024.107543
14. Kanimozhi, V., & Jacob, T. P. (2023). The top ten artificial intelligence-deep neural networks for IoT intrusion detection system. Wireless Personal Communications, 129(2), 1451-1470. https://doi.org/10.1007/s11277-023-10198-6
15. Qazi, E. U. H., Faheem, M. H., & Zia, T. (2023). HDLNIDS: hybrid deep-learning-based network intrusion detection system. Applied Sciences, 13(8), 4921. https://doi.org/10.3390/app13084921
16. Konatham, B., Simra, T., Amsaad, F., Ibrahem, M. I., & Jhanjhi, N. Z. (2024). A secure hybrid deep learning technique for anomaly detection in iiot edge computing. Authorea Preprints.
17. Talukder, M. A., Hasan, K. F., Islam, M. M., Uddin, M. A., Akhter, A., Yousuf, M. A., ... & Moni, M. A. (2023). A dependable hybrid machine learning model for network intrusion detection. Journal of Information Security and Applications, 72, 103405. https://doi.org/10.1016/j.jisa.2022.103405
18. Sakthivelu, U., & Vinoth Kumar, C. N. S. (2023). Advanced Persistent Threat Detection and Mitigation Using Machine Learning Model. Intelligent Automation & Soft Computing, 36(3). http://dx.doi.org/10.32604/iasc.2023.036946
19. Azar, A. T., Shehab, E., Mattar, A. M., Hameed, I. A., & Elsaid, S. A. (2023). Deep learning based hybrid intrusion detection systems to protect satellite networks. Journal of Network and Systems Management, 31(4), 82. https://doi.org/10.1007/s10922-023-09767-8
20. Henry, A., Gautam, S., Khanna, S., Rabie, K., Shongwe, T., Bhattacharya, P., ... & Chowdhury, S. (2023). Composition of hybrid deep learning model and feature optimization for intrusion detection system. Sensors, 23(2), 890. https://doi.org/10.3390/s23020890