Refining Intrusion Detection System Attack Identification with AI Technologies

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

[1]Research Scholar, Department of Electronics & Communication Engineering, Bhabha University, Bhopal

[2]Professor,Department of Electronics & Communication Engineering, Bhabha University, Bhopal

Abstract- In this work, our objective is to execute binary classification using the CIC-IDS-2017 cyber security dataset. Classify network flow samples into benign or malicious categories, in the context of an Intrusion Detection System. We achieve state of the art results 99.25% optimizing for the minimal memory usage, by efficiently utilizing feature selection with the XGBoost algorithm, feature engineering and data balancing using SMOTEalgorithm.This is represented as a scalable and adaptive means of protecting core communication infrast ructure from ever-growing threat situations. Abnormal recognition, 5G and 6G networks

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

Today, communication systems act as life eliminators for digital infrastructures and hold information about the network.However, the development of communication systems makes it more complex and susceptible to highly developed cyberattacks, such as data injuries and denial of service. Traditional measures seem no longer sufficient when fighting development and more sophisticated threats. This makes it essential for adaptive, intelligent and proactive security solutions. The configuration of the Cellular Networks System is based on complex, uneven architectures and legacy trust models that must collaborate with, while ensuring interoperability and tends to be highly security challenges. These systems were initially started in a closed environment and were initially more vulnerable. The presence of uniform security architectures and domain specific threat model frameworks that can be used in mobile networks has reinforced the need for special approaches. Miter ATT&CK has begun to fill this identified gap, but there is no mobile network specific framework. Therefore, this paper suggest domain specific frames to promote 2G, 3G, and 4G networks in a transparent discussion of security issues.Due to speed, low cost and versatility, unmanned aerial vehicles (UAVs) can be useful for disaster management, practical surveillance, healthcare, and wireless communication [2], [3]. UAV supported communications are based on these aircraft that act as base stations or relays to improve the coverage and flexibility of communication networks in challenging environments. However, this approach is B. It sets up several critical issues, including presentation strategies, effective resource allocation, security challenges such as DDOS attacks (distributed denial of service), spoofing, and listening [5]. However, blockchain becomes a possible solution to promote a decentralized, secure mechanism. Improve trust, data integrity and interoperability between UAV networks [6]. In this regard, it represents high compensation and scalability issues for computational and scalability issues. Therefore, further testing is required to optimize supplemental use in UAV systems for improved and safe communication [7] [8]. Wireless communication technology has evolved from the first generation to today's 5G networks, offering extremely high data rates, wide bandwidth allocations and a wide range of applications. Researchers question the terms of 6G network options, security, data protection and legal frameworks, so the listing conditions remain high, especially as wireless communications send data and forward sensitive information. Although regulations alreayexist in

relation to the healthcare, AI and IoT sectors, further caution is needed to be given to specific privacy and security protections in future 6G networks[9].

AI can be a disturbing force in cyber security, bringing real-time threat detection and response. AI based methods, including machine learning and deep learning, allow analyzing large amounts of network data, identify ing patterns, predicting intrusions, and more accurately adapting to new threats. In communications networks, AI based intrusion detection systems (IDS) far exceed traditional security measures. This is achieved through continued learning and further development strategies for recognition in relation to new threats. This research is extremely important for AI integration, such as hybrid models such as XGBoost (DNN)with XGBoost, primarily XGBoost, to enhance the safety and resistance of communication systems. Such advanced framework conditions in AI are extremely important for both the near and far future of existing networks, and for addressig the security challenges that may arise as technologies such as 6G, UAV-assisted communications, and distributed block chain based networks. The goal here is to combine AI and application threat modelling with legal frameworks to create a safer, adaptive, future communication ecosystem.

2. LITERATURE REVIEW

The rapid spread of IoT and exposure to these attacks indicated the important need for effective intrusion detection systems (IDS). Deep Learning (DL)-based initiatives have been reported to have been 100% successful in such circumstances. The new IDS is a multidimensional classifier that recognizes several attacks, such as black hole attacks, DDOs, and dollar clocks, with an impressive accuracy of 93.74% [10]. The CNNS-based DCGR_IOT system reaches spatial characteristic extraction, and the CGRN architecture reaches temporal characteristic extraction with combinations of data records such as UNSW-NB15 and KDDCUP99, achieving accuracy of up to 99.2% in some cases [11]. Another work on AMI extracts the temporal relationship with statistical accuracy by using Xgboost for feature selection, Adasyn for data compensation, and CNN for spatial features construction, and 97.85%, 91.04%, and 91.06%, and three data records were realized and tested [12]. Artificial intelligence improves the ability of intrusion systems where innovations such as cyber ibots are handled through deep cloud computing environments. This framework uses long-term long-term storage networks and supports vector machine technology to analyze large data records. This indicates that LSTM networks for training take a long time, but the performance of detection is much better [13]. Other findings provide the top 10 AI deep learning models for IoT anomaly detection. The accuracy values for folding networks, generically controversial networks, and multi-layer perseprons are almost 99.6% [14]. Furthermore, a hybrid deep learning-based network intrusion detection system for folding and recurrent neural networks has now enabled recognition accuracy of 98.90% of malicious network activity in the CICIDS-2018 dataset [15]. (iioot) System. This model achieved 94.94% accuracy, and made future improvements with XGBoost to improve the properties, achieving an accuracy of approximately 96.41% in experimental results [16]. The hybrid model of deep learning network boost and other machine learning technologies also achieves positive results in traditional network environments. For example, for benchmark datasets such as KDDCUP'99 and CIC-MALMEM-2022, the combination of the choice of Small and XGBoost for data compensation achieved almost perfect accuracy [17]. The pass-conscious IDS was based on a reversal aboost for defense and a dynamic deception system, resulting in around 99.9% accuracy [18]. Network architectures, including satellite ground integrated networks (STINs), face a series of security challenges that require committed identity solutions. Using sequential forward selection (SFS) with random forest (RF) functionality, in Feate-Optimization, the new study introduced four hybrid-ID models in combination with ML/DL models such as LSTM, ANN, and GRU. Therefore, these models show improved discrimination rates, with the accuracy of satellite and ground datasets between 79% and 90.5% [19]. When taking the growing threat from a hybrid ID that combines CNN and GRU to optimize network parameters, 98.73% accuracy, and zero-day attacks that optimize significantly lower false positive rates than existing models of real-world cyberset setups [20]. Thus, these advances highlight the changing landscape of network security where AI and DL still play a key role in expanding intrusion awareness in various technical areas. No.Use of the techniques used model limits on key findings

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 main goal of this research is to develop sophisticated, scalable, adaptive, adaptive trusion systems (IDs) that use deep learning models to effectively identify and identify safety threats in communication networks. The focus is on the use of traditional ID restrictions and deep learning skills to improve recognition obligations, reduce false positive outcomes, and adapt to the development of attack patterns in real time. In particular, the research aims to:

1. Deep Learning-Based Intrusion Detection System (IDS) Development: Design robust, scalable and adaptive IDs using advanced deep learning architectures to recognize and reduce cyber threats in communication networks with high accuracy and minimal false positives.
2. Improved real-time recognition capabilities: Create deep learning models that efficiently process high-dimensional and large-scale network traffic data and enable intrusion detection in dynamic communication environments.
3. To combat the challenges of data records in intrusion recognition: fighting issues such as sound balance, outdated attack patterns, lack of realistic data records, or generating synthetic data that accurately represents

traffic and scenarios for the latest steps.
4. Improved explanation and interpretation of intrusion marking models: Integration of explanatory AI technologies into proposed deep learning models to promote tariff transparency in decision-making and pro mote trust and user-friendly in critical applications. network.
(3) To achieve high accuracy through state-of-art.

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.

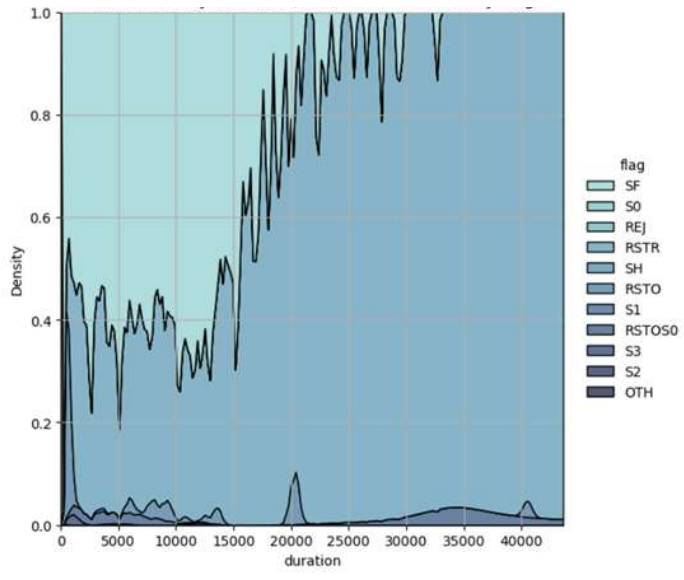

Fig.1: Kernel Density Estimate (KDE) Plot of Duration by Flag

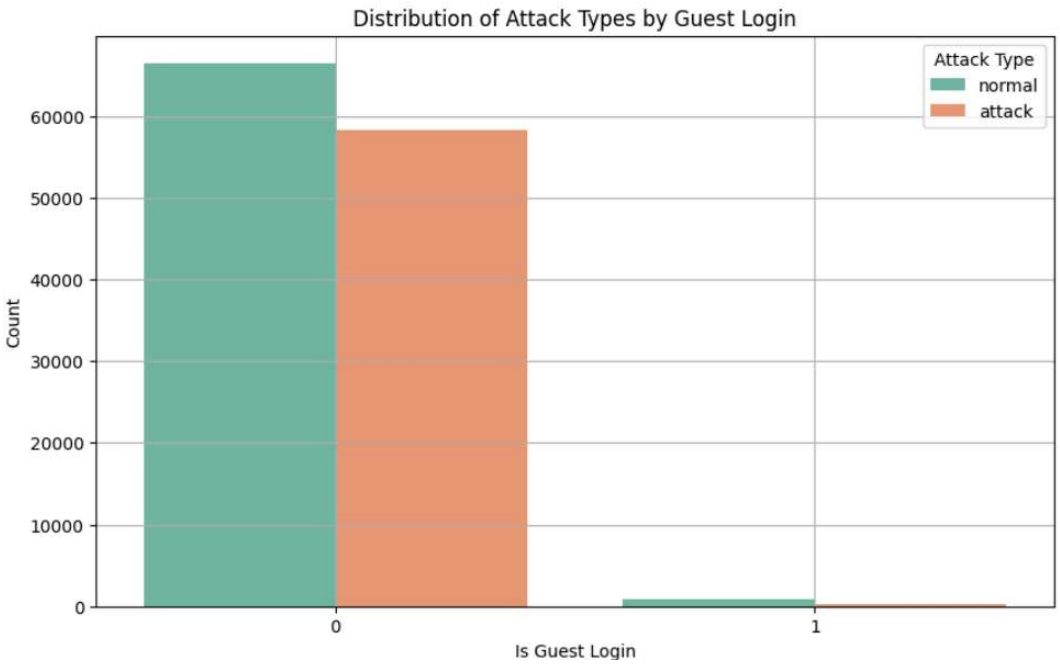

Fig.2: Distribution of Attack Types by Guest Login

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.

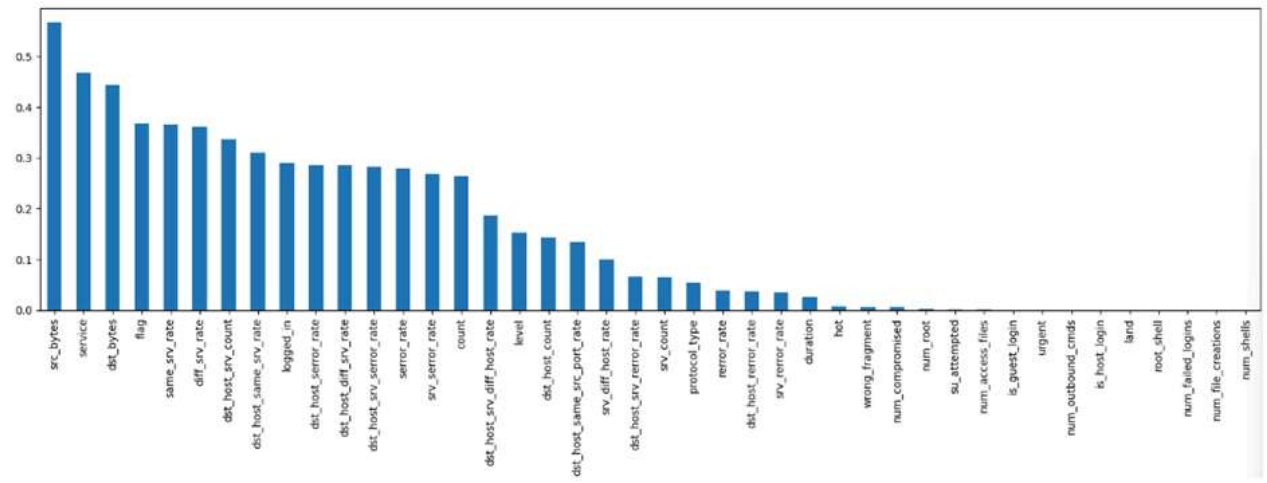

Fig.3: Features of dataset

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.

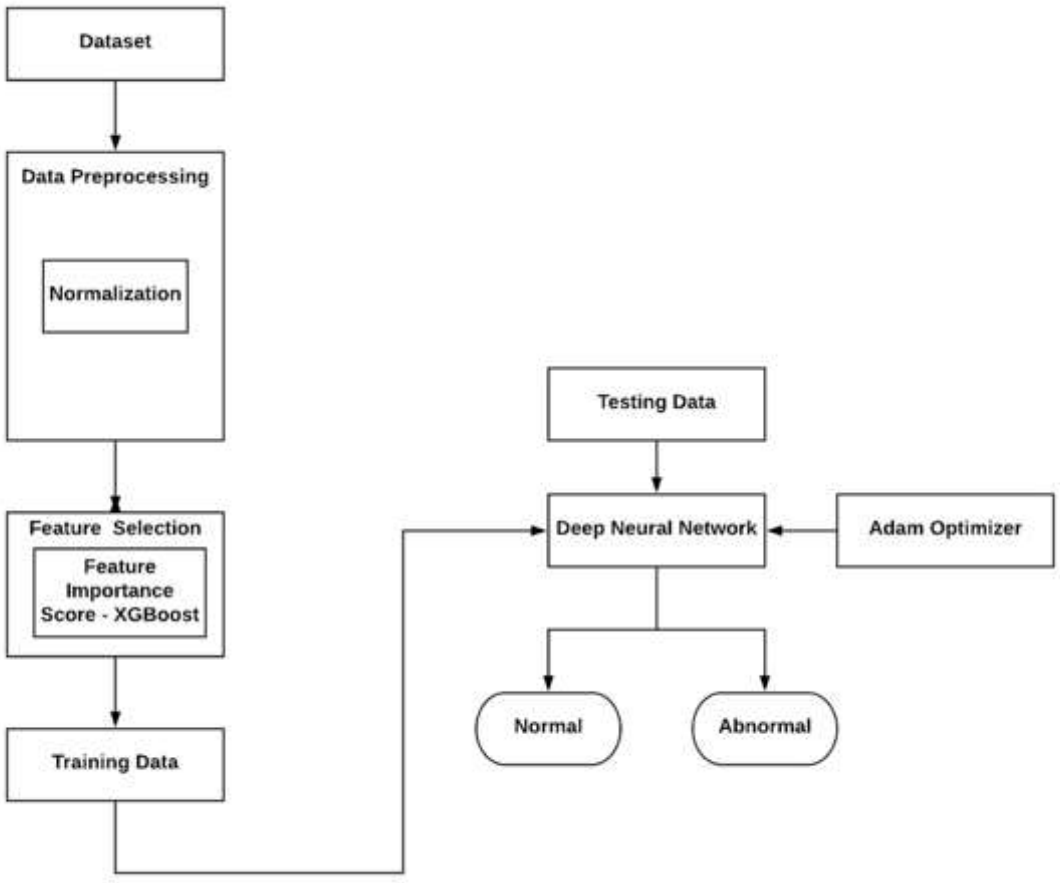

Fig.4: Proposed XGBoost classifier model for network intrusion detection

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.

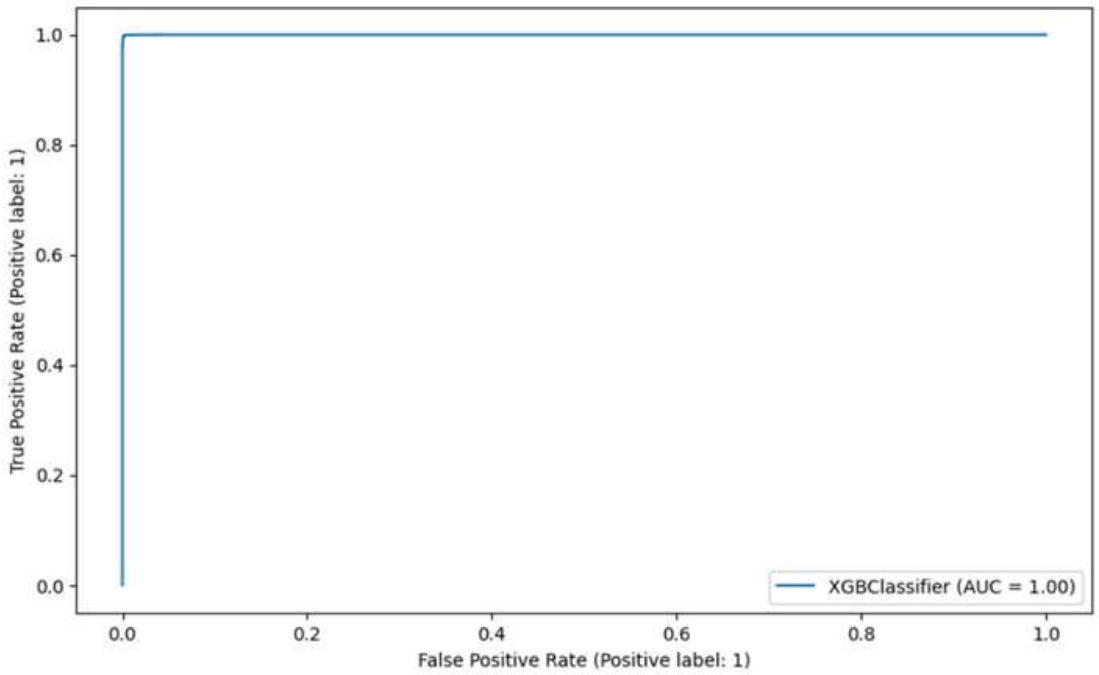

Fig.5: AUC Curve of proposed model

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

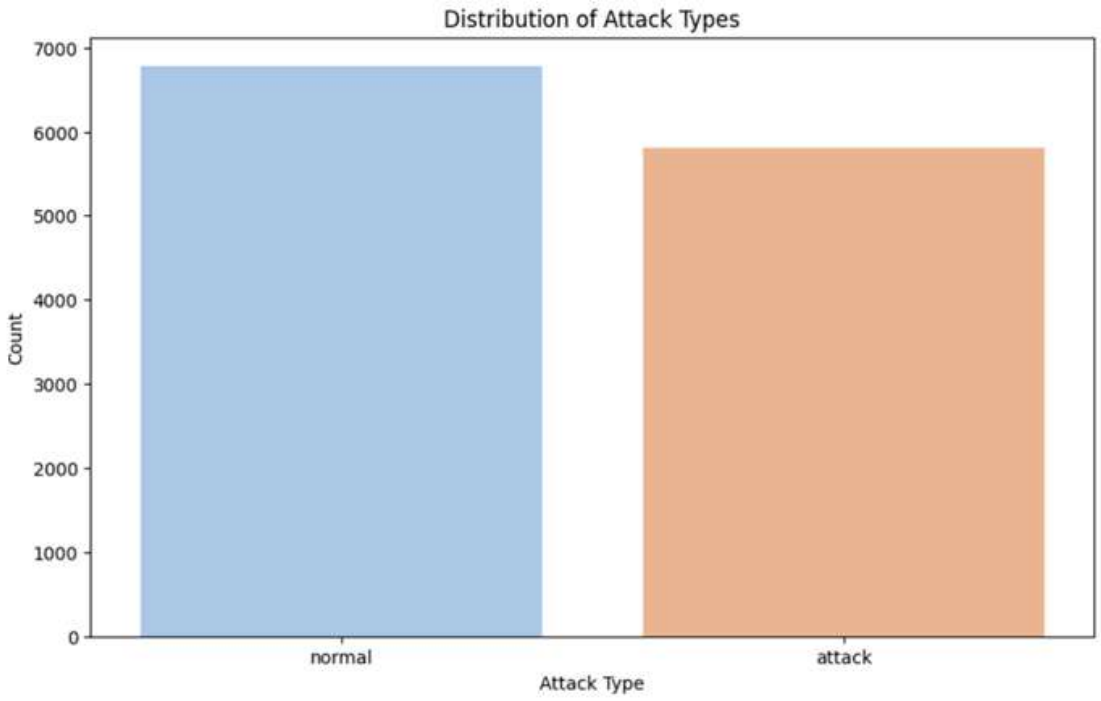

Fig.6: Prediction distribution of proposed model

4. Comparative Analysis

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

Table2: 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

Table3: 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 defences to preserve digital infrastructures.

7. 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
[21] [1]Vijay Kumar Sharma, [2]Dr. Navin Kumar Agrawal Vol.20, S16 (2024) Securing Communication Systems with AI-Powered Intrusion Detection Frameworks https://doi.org/10.62441/nano-ntp.vi.5086