International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

A Bag of Features and Blockchain-Based Efficient Cyber-Attack Detection in Healthcare Using Deep Convolutional Neural Networks

Mr. Jagdish F. Pimple[1*], Dr. Avinash Sharma[2]

Submitted: 03/02/2024 **Revised**: 11/03/2024 **Accepted**: 17/03/2024

Abstract: This paper proposed novel model for detection of cyber-attacks in healthcare, merging a convolutional neural network (CNN) with a bag of features (BoF) to address challenges associated with low accuracy and class imbalance in existing cyber-attacks detection. Feature selection is accomplished through a bag of features, mitigating problems with feature duplication. A convolutional neural network is then used to extract spatial information, and average pooling and max pooling techniques are combined after that. By integrating attention processes, features are given different weights, which lowers overhead and improves model performance.Simultaneously, a bag of features is utilized to capture long-distance dependent information, facilitating comprehensive feature learning. Finally, classification is executed through a SoftMax function. Evaluation of Testing of the suggested attacks detection model is done using the CIC-IDS2017 and NSL-KDD datasets. Investigational outcomes demonstrate classification accuracies of 86.25%, 99.69%, and 99.65%, respectively, surpassing existing CNN models by margins of 1.95%, 0.47%, and 0.12%. The model effectively addresses issues of low accuracy and class imbalance, showcasing its robustness and efficacy in attacks detection tasks.

Keywords*: - Healthcare, Blockchain, DCNN, bag of features (BoF)*

1.Introduction

The integration of technology into healthcare systems has greatly improved their scalability and capacity across various platforms[1]. This integration relies heavily on the internet, serving as the backbone for incorporating technologies such as blockchain, healthcare management systems, and security protocols to safeguard patient records. However, the stacking of multiple communication protocols has introduced vulnerabilities, particularly in the realm of cybersecurity[2]. The exponential growth of cyber traffic has exacerbated security threats, especially concerning the confidentiality and integrity of medical patients' records. Blockchain technology emerges as a promising a way to overcome these obstacles. By providing an immutable and decentralized ledger, blockchain offers an enduring capacity for healthcare systems, ensuring the trustworthiness and longevity of patient data. Recognizing the urgency of the situation, numerous authors have proposed innovative approaches to combat cyber threats in healthcare systems. Specifically, there has been a noticeable tendency in recent years towards the development of deep learning-based algorithms for the proactive detection of potential attacks. The integration of technology, particularly blockchain, has revolutionized healthcare systems, enhancing their scalability and security[3.4,5]. While challenges persist in the face of evolving cyber threats, the adoption of deep learning algorithms signifies a proactive step towards safeguarding patient data and maintaining the integrity of healthcare services. The concept of "Bag of Features" represents a novel approach to detecting and preventing cyber-attacks within healthcare systems. It stands as a state-of-the-art method for mapping features essential in processing healthcare data across networks. Healthcare systems face a myriad of challenges, particularly in managing the complexity of communication parameters. This complexity results in overhead traffic and increased system intricacy, creating vulnerabilities that cyber attackers exploit, compromising the security of healthcare systems. In response to these challenges, the Bag of Features methodology emerges as a promising solution. By effectively capturing and processing relevant features in healthcare data, it offers a structured approach to understanding and managing the complexities of healthcare system communication. Implementing the Bag of Features approach not only enhances the finding and prevention of cyber attacks but also improves the overall security posture of healthcare systems. Its ability to systematically analyse communication parameters provides valuable insights for mitigating security risks and safeguarding sensitive healthcare data. The adoption of the Bag of Features concept denotes a significant step forward in addressing the cybersecurity tasks faced by healthcare systems. By leveraging this innovative methodology, healthcare organizations can better protect

[1]*Research Scholar, Department of Computer Science & Engineering, Madhyanchal Professional University Bhopal, MP.*
Email*- pimplejagdish@gmail.com, jpimple@stvincentngp.edu.in*
[2]*Professor, Department of Computer Science & Engineering, Madhyanchal Professional University Bhopal, MP.*
Email*- avinashvtp@gmail.com*

patient information and ensure the integrity and reliability of their systems amidst growing cyber threats. Blockchain technology plays a crucial role in safeguarding the privacy of extensive healthcare reports, scalable to operate across billions of devices. Within today's landscape of information and communication technology, the healthcare sector stands as a prominent arena. Enabled by the Internet of Things , Remote patient monitoring and computerized health recordkeeping have become indispensable components of healthcare practices. However, the diverse and voluminous healthcare data from myriad sources raise concerns regarding data quality assurance, particularly given their potential utilization in various applications such as disease prediction. Ensuring data quality becomes particularly challenging during the integration of data from diverse devices. Additionally, the confidentiality of healthcare data shared over networks becomes a pressing concern, exacerbated by the risk of single-point failure inherent in centralized storage solutions. Centralized storage also exposes systems to the threat of denial-of-service attacks. Blockchain technology emerges as a viable solution to these challenges. Functioning as a distributed ledger, blockchain facilitates the synchronization of information among healthcare providers. Sensitive health information is contained in every blockchain block and is only accessible by those with permission. Blockchain's enhanced capacity, immutability, permission procedures, and decentralized storage make it appealing.The immutability of blockchain data ensures that unapproved entities cannot alter the stored information, thus providing a secure foundation for the development of disease prediction models using deep learning algorithms. By leveraging blockchain technology, the healthcare industry can address data quality, confidentiality, and security concerns, thereby fostering innovation and efficiency in healthcare delve The paper presents a hybrid algorithm for detecting cyber-attacks in healthcare systems. This algorithm leverages the Bag of Features methodology, which involves optimizing and selecting feature points from the traffic data of blockchain. By employing this approach, the algorithm aims to effectively capture and process relevant features essential for identifying potential cyber threats within healthcare networks. The Bag of Features technique involves a process of feature optimization, where relevant features are selected and extracted from the blockchain traffic data. This procedure is essential for improving the algorithm's capacity to precisely identify and categorize cyberattacks.By focusing on key feature points, the algorithm can effectively distinguish between normal network behaviour and malicious activities. The suggested algorithm blends deep convolutional neural networks (CNNs) with the Bag of Features methodology. CNNs are a subclass of deep learning models that are well-known for their performance in pattern recognition and image processing applications. CNNs are incorporated into the hybrid model to improve the algorithm's capacity to identify sophisticated cyberthreats in healthcare systems. The primary objective of the hybrid algorithm is to detect various types of cyber threats targeting healthcare networks. By leveraging both the Bag of Features approach and deep CNNs, the algorithm can analyse network traffic data in real-time, identifying suspicious patterns or anomalies indicative of potential cyber-attacks. This proactive detection capability is crucial for mitigating security risks and safeguarding sensitive healthcare data. The remaining sections of the paper are arranged as follows: Section II covers related work in the field of cyber-attack detection; Section III offers a methodology for cyber-attack detection; Section IV examines the proposed algorithm experimentally using standard datasets; Section V covers results and discussion; and Section VI concludes the paper.

2. Related Work

The rapid evolution of technology has democratized access to the Internet, with a vast majority of individuals relying on it for various professional and personal activities. From communication to business transactions, the Internet serves as a cornerstone for myriad sensitive operations. While it facilitates connectivity and interaction, the integrity and confidentiality of these engagements are under constant threat from malicious actors' intent on disrupting network security. Instances of cyber-attacks targeting networks are on the rise, necessitating a deeper understanding of these threats and the development of robust security measures. Organizations across sectors, including industries and governments, are compelled to seek effective network security solutions to safeguard their operations from the escalating risk of cyber-attacks. As no network remains impervious to such threats, the demand for resilient and adaptable network security systems continues to surge, driven by the imperative to protect both business assets and client data. [1] introduces an IoT architectural model for smart healthcare, leveraging machine learning to prescribe suitable drugs for patients. The model demonstrates high effectiveness in drug prediction, with Random Forest achieving a classification accuracy of 99.23%. [2] presents a scheme ensuring data privacy and integrity in IoMT networks using techniques like homomorphic encryption and secret sharing. It also emphasizes the role of virtual nodes on the edge to prevent unauthorized access to data by cloud servers. [3] discusses the role of blockchain technology in enhancing privacy preservation and security in healthcare systems.

It provides a comprehensive review of blockchain-based healthcare systems, highlighting challenges such as scalability and key management. [4] introduces SC-UCSSO for 5G-IoT telemedicine, emphasizing privacy, security, and performance. The scheme aims to prevent various attacks while enabling users to control data transmission estimations and timing. [5] proposes a security framework to enhance privacy and security in E-Health systems, incorporating real-time entropy testing and planning for hardware random number generator analysis in the future. [6] focuses on preserving user identities in contact-tracking apps, emphasizing privacy concerns and power constraints. The paper discusses the use of blockchain-based PKI to secure against data poisoning attacks. [7] introduces the RDT algorithm for preserving and recovering medical data, highlighting its superior computing speed and accuracy compared to other models. [8] emphasizes enhancing IoT security and privacy through unique signatures, with a focus on attribute selection and cryptography library optimization. [9] proposes a protocol to prevent re-identification of sensitive information, addressing privacy concerns in data collection and integration. [10] highlights the importance of privacy preservation in healthcare and discusses challenges associated with securing and handling private data, especially in IoT and edge healthcare solutions. [11] explores challenges in distributed data sharing and analysis in healthcare and banking, focusing on vulnerabilities to privacy attacks. [12] proposes the SUSI scheme for enhancing security and privacy in RM-PoC, showing improved communication metrics in simulation studies. [13] discusses the benefits and limitations of ML in healthcare communication, emphasizing the role of AI chatbots. [14] introduces a blockchain-enabled collaborative approach to enhance medical transactions and data preservation in e-Healthcare applications. [15] discusses blockchain-based solutions for confidentiality protection in drone communications, addressing resource constraints and regulatory guidelines. [16] emphasizes the need for privacy mechanisms in Federated Learning (FL) systems to prevent attacks and comply with GDPR regulations. [17] presents a blockchain-based algorithm, SCAWKNN, for predicting heart disease from healthcare data, outperforming traditional algorithms in accuracy. [18] discusses the convergence of AI and blockchain in sustainable IoT applications, focusing on secure smart city applications. [19] introduces a system for accurately detecting hypoglycaemia, prioritizing essential parameters to boost accuracy and patient survival. [20] explores the use of blockchain and quantum technologies in medical data handling, highlighting operational uses and gaps in understanding quantum computing aspects in healthcare.

3. Proposed Methodology

In this section, the methodology for detecting cyber-attacks is outlined, combining the bag of features methodology with deep convolutional neural networks (DCNN).The bag of features method involves selecting key features from complex traffic data scenarios, encompassing both normal and attack instances. This approach allows for the extraction and representation of essential characteristics from diverse traffic data, aiding in the identification of patterns indicative of attacks within the network. Deep convolutional neural networks (DCNN) are then employed for the detection of binary data, distinguishing between normal and attack traffic. DCNNs are renowned for their efficiency in processing binary data, making them well-suited for cyber-attack detection tasks. Additionally, DCNNs exhibit high data handling capacity, enabling them to effectively analyse large volumes of traffic data and extract meaningful patterns for accurate classification. By integrating the bag of features approach with DCNNs, the proposed methodology offers a comprehensive framework for cyber-attack detection, leveraging the strengths of both methods to improve detection systems' precision and effectiveness in intricate network environments. The processing of algorithm and model shown in figure 1. The processing of algorithm describes here.

The modeling procedure based on DCNN and the Bag of Features. This article details the algorithm's working procedure.

Xi= sample of Bag of Features

N =size of sample data

V= vector of feature data process.

O = mapped data of cluster

G=Group of patterns,

SM= Vector of DCNN

Wn= weight matric

Bf =mapping of features

D = dimension of data

R = relation of feature data

S= sample of set

$B^{\emptyset}$= adjust matrix

Ac = learning factor

The process of training sample as
$(X_i \in R^D, y_i \in R)$,i=1…….m

$sample\ of\ input\,(p)$ if $*= V$

$[s^1, \ldots . s^k] \leftarrow [rand(1,k) \times (p-w)] + 1$

$V \leftarrow n$ vector of neuron

For $i \leftarrow 1$ *to* N *do*

$O \cdot \in C^D \leftarrow S *= V$

$N_*^i \in R^D \leftarrow biase\ of\ O$

$G \in R^D \leftarrow pattern\ N$

End for

Input sample of BF $g_*^1, \ldots \ldots . g_*^m$

$F_{RBF} \in R^{D \times m} \leftarrow \emptyset([g_*^1, \ldots \ldots . g_*^m])$ *Adjust* W

$W \in R^D \leftarrow BF^{-1}$

$F \in R^d \leftarrow W^T \emptyset(G)$

For $C \leftarrow 1$ *to* A_c *do* *training of class* Cb

Adjust the weight factor of cascading process

$CC \in R^{d^{\sim}} \leftarrow$ relative feature process of SOM

Call kernel function

$$k(x_i, x_j) = \exp\left(\frac{-\|x_i - x_j\|^2}{\gamma}\right), \gamma \in R_+$$

End for

Adjustment matrix $B^{\emptyset}$ of space F mapping of same class

$$B_{ij}^{\emptyset} = \{ \begin{matrix} e^{(-\|x_i - x_j\|^{\angle})}. \\ e^{(-\|x_i - x_j\|^2)}. \end{matrix}$$

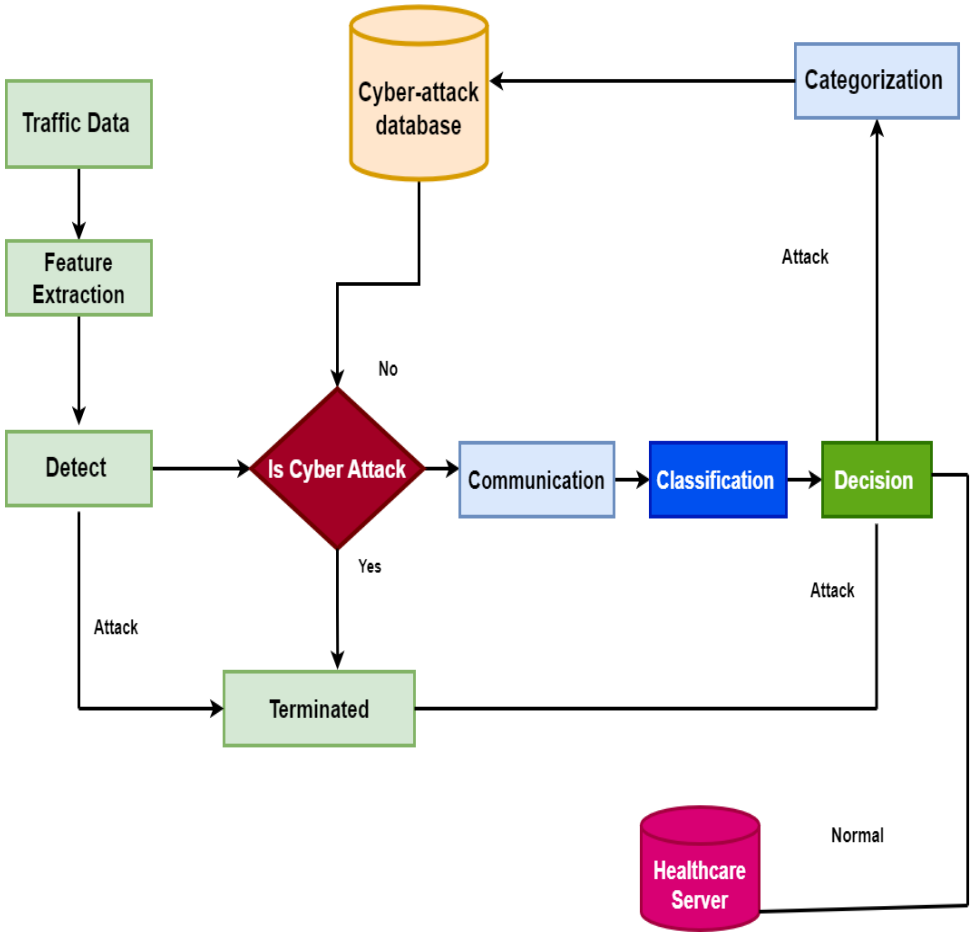

Figure.1 Projected Model of Cyber-attack detection in healthcare system

4. Experimental Result

The suggested algorithm's simulation has been tried with several feature sets. The MATLAB software version 2018R is used in the simulation process. Two intrusion detection datasets, such as the NSL-KDD 2015 and CIDDS-001 datasets, were used to validate the algorithm [7]. There are 125973 instances, 41 characteristics, and 2 classes in the former NSL-KDD dataset. Subsequently, 1018950 instances with 14 attributes and 2 classes are included in the CIDDS-001 dataset. The suggested algorithm's performance is contrasted with that of other algorithms for cyber-physical security systems, including

FDD-CNN, DIN-VI, BGF-CNN, and CML-ADI. Algorithm performance is measured in terms of F-score, sensitivity, specificity, and accuracy [18, 19, 20].

$$Accuracy = \frac{Total\ No.of\ Correctly\ Classified\ Instances}{Total\ No.of\ Instances} \times 100$$

$$pricision = \frac{TP}{TP + FN} \times 100$$

$$Recall = \frac{TN}{TN + FP} \times 100$$

$$F - score = \frac{2TP}{2TP + FN + FN}$$

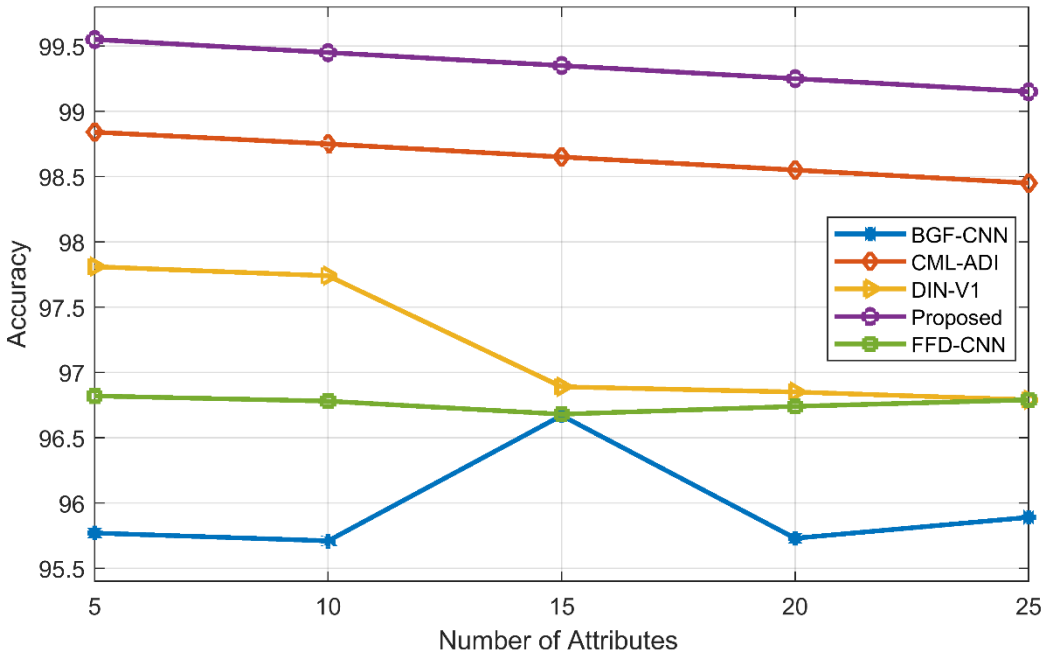

Figure: 2 Performance examination of Number of attributes of NSL-KDD 2015 dataset & Accuracy .

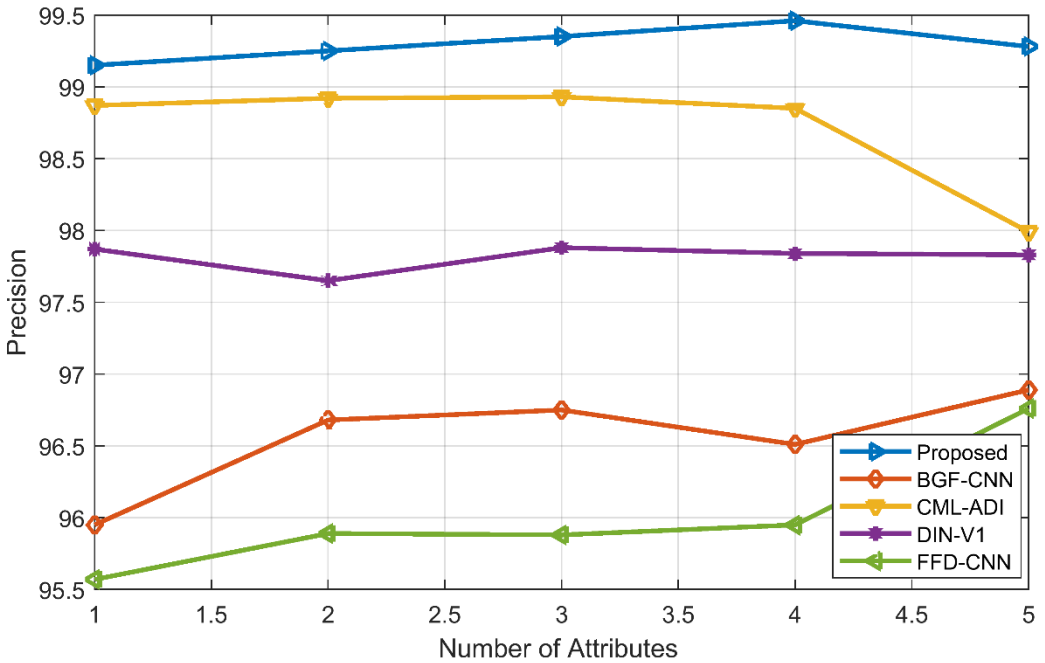

Figure: 3 Performance examination of Number of attributes of NSL-KDD 2015 dataset and precision.

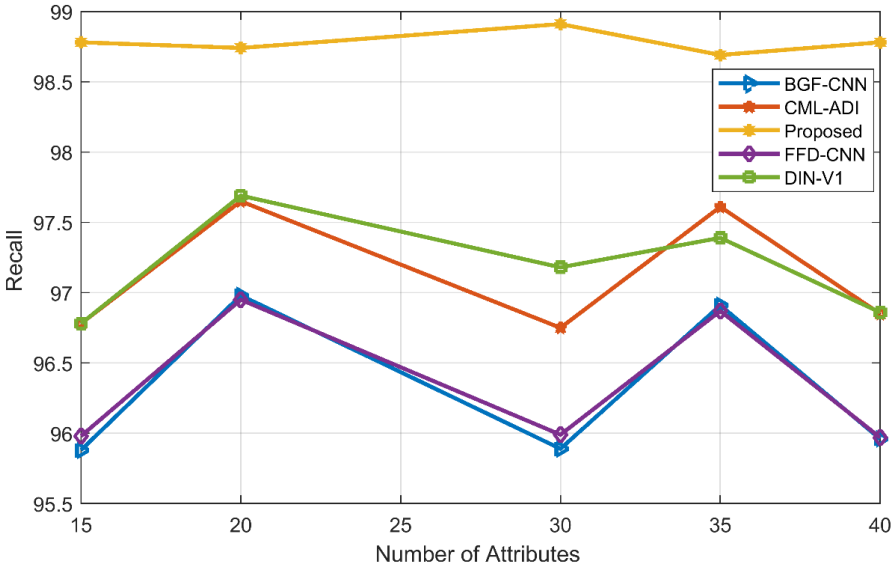

Figure: 4 Performance examination of Number of attributes of NSL-KDD 2015 dataset and Recall.

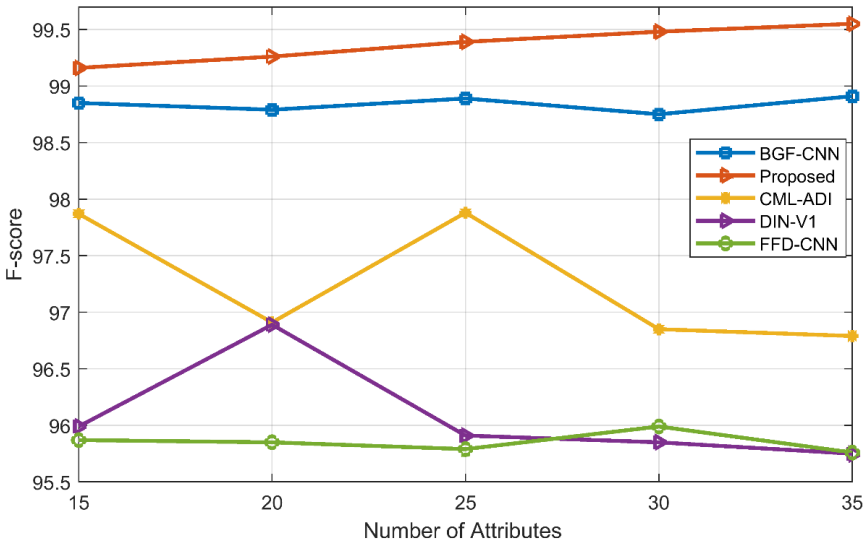

Figure: 5 Performance examination of Number of attributes NSL-KDD 2015 dataset and F-score.

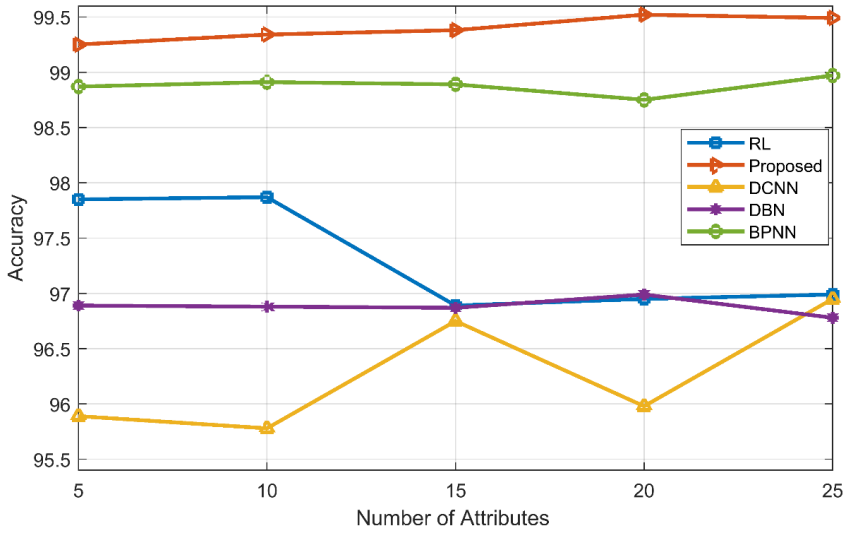

Figure: 6 Performance examination of Number of attributes of CIDDS-001 dataset and Accuracy.

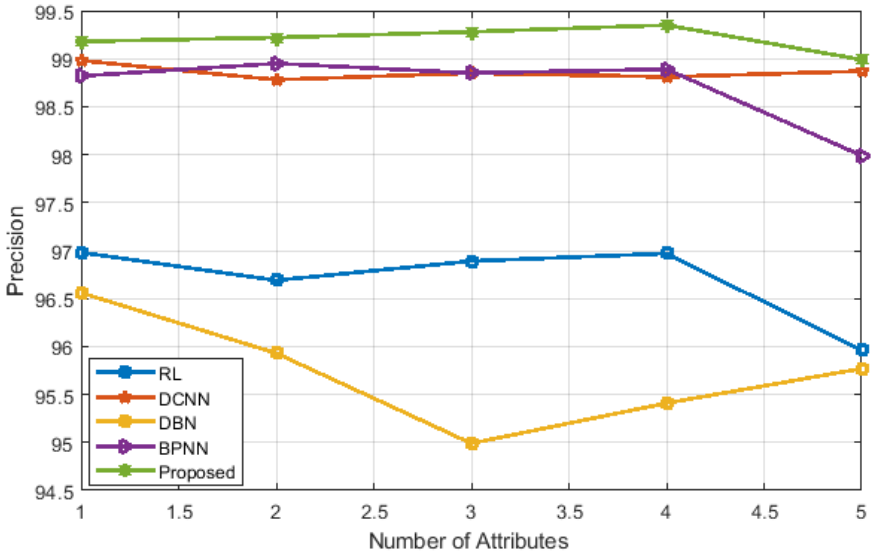

Figure: 7 Performance examination of Number of attributes of CIDDS-001 dataset and precision .

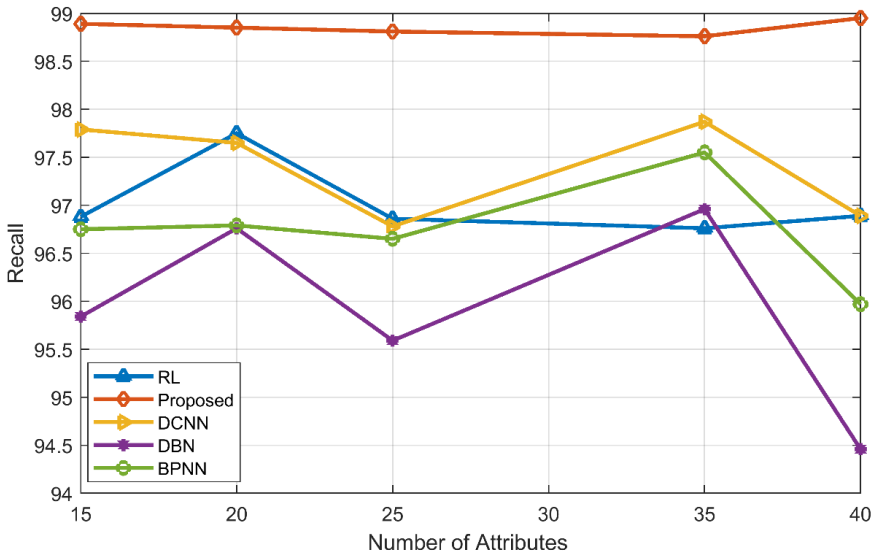

Figure: 8 Performance evaluates of Number of attributes of CIDDS-001 dataset and recall.

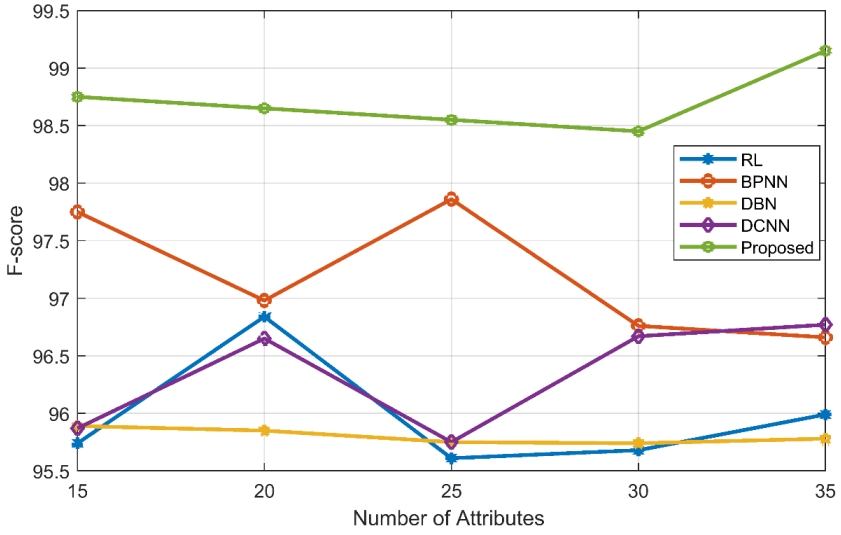

Figure: 9 Performance examination of Number of attributes of CIDDS-001 dataset F-score.

5. Results & Discussion

This section describes a comparative analysis of cyber-attack detection algorithms in healthcare systems, specifically focusing on the outcomes of the projected algorithm compared to existing ones. Figure 2, 3, 4, and 5 present the suggested algorithm's performance measures (accuracy, precision, recall, and F-score) on NSL-KDD datasets with varying numbers of features. These metrics indicate that the proposed algorithm significantly enhances cyber-attack detection compared to BFG-CNN and FDD-CNN algorithms. Additionally, the analysis extends to another dataset, CIDDS-001, where existing algorithms were employed. The performance of these algorithms is illustrated in Figure 6, 7, 8, and 9, again in terms of F-score, recall, accuracy, and precision.

Table-1. Comparative results of NSL-KDD dataset of different set of attributes for detection.

Number of Attribute	Methods	Accuracy	Precision	Recall	F-score
5	CML-ADI	98.84	98.87	96.78	97.87
	DIN-V1	97.81	97.87	96.77	95.99
	FFD-CNN	96.82	95.57	95.98	95.87
	BGF-CNN	95.77	95.95	95.88	98.85
	Proposed	99.55	99.15	98.78	99.16
10	CML-ADI	98.75	98.92	97.65	96.91
	DIN-V1	97.74	97.65	97.69	96.89
	FFD-CNN	96.78	95.89	96.95	95.85
	BGF-CNN	95.71	96.68	96.98	98.79
	Proposed	99.45	99.25	98.74	99.26
15	CML-ADI	98.65	98.93	96.75	97.88
	DIN-V1	96.89	97.88	97.18	95.91
	FFD-CNN	96.68	95.88	95.99	95.79
	BGF-CNN	96.67	96.75	95.89	98.89
	Proposed	99.35	99.36	98.91	99.39
20	CML-ADI	98.55	98.85	97.61	96.85
	DIN-V1	96.85	97.84	97.39	95.85
	FFD-CNN	96.74	95.95	96.87	95.99
	BGF-CNN	95.73	96.51	96.91	98.75
	Proposed	99.25	99.46	98.69	99.48
25	CML-ADI	98.45	97.99	96.85	96.79
	DIN-V1	96.79	97.83	96.86	95.75
	FFD-CNN	96.79	96.76	95.97	95.76
	BGF-CNN	95.89	96.98	95.96	98.91
	Proposed	99.15	99.28	98.78	99.55

Table.2 Comparative performance of CIDDS-001 dataset and number of attribute (15, 20, 25, 30, and 35).

Number of Attribute	Method	Accuracy	Precision	Recall	F-score

15	DCNN	95.89	98.98	97.79	95.87
	BPNN	98.87	98.82	96.75	97.75
	RL	97.85	96.98	96.88	95.75
	DBN	96.89	96.56	95.84	95.89
	Proposed	99.25	99.18	98.89	98.75
20	DCNN	95.78	98.78	97.65	96.65
	BPNN	98.91	98.95	9679	96.98
	RL	97.87	96.69	97.75	96.84
	DBN	96.88	95.93	96.76	95.85
	Proposed	99.34	99.22	98.85	98.65
25	DCNN	96.75	98.85	96.78	95.75
	BPNN	98.89	98.85	96.65	96.86
	RL	96.89	96.89	96.86	95.61
	DBN	96.87	94.99	95.59	95.75
	Proposed	99.38	99.28	98.81	98.55
30	DCNN	95.98	98.81	97.87	96.67
	BPNN	98.75	98.89	97.55	96.76
	RL	96.95	96.97	96.76	95.68
	DBN	96.99	95.41	96.96	95.74
	Proposed	99.52	99.35	98.76	98.45
35	DCNN	96.65	98.87	96.89	96.77
	BPNN	98.97	97.99	95.97	96.66
	RL	96.99	95.96	96.89	95.99
	DBN	96.78	95.77	94.46	95.78
	Proposed	99.49	98.99	98.95	99.15

Based on its greater accuracy, precision, recall, and F-score across various datasets and feature variations, the proposed algorithm performs better than existing ones overall in terms of identifying cyber-attacks in healthcare systems.

6. Conclusion & Future Work

An advanced deep learning-based approach for identifying and categorizing cyberattacks in Blockchain communication networks is presented in this study. The three separate subsystems that make up the system—the feature engineering subsystem, the feature learning subsystem, and the detection and classification subsystem—are carefully designed, tested, and verified. As part of this research project, each subsystem is developed independently before being integrated, confirmed, and validated. Utilizing a CNN-based architecture, the proposed system demonstrates exceptional capability in identifying and categorizing slightly modified cyberattacks inherent to Blockchain networks, as represented by the NSL-KDD dataset encompassing key attacks in Blockchain computing. Achieving a remarkable detection accuracy of 99.3% in distinguishing normal and anomalous traffic, the system also showcases a classification accuracy of 98.2% in segmenting Blockchain traffic into five distinct categories. A rigorous five-fold cross-validation procedure is used, with five separate tests for every classification model, to guarantee resilience in system validation. To provide a thorough understanding of system performance, the evaluation process also makes use of the confusion matrix parameters (TN, TP, FN, and

FP) and computes a number of performance metrics, such as false alarm rate, classification precision, recall, and F1-score of classification. In the end, the experimental results show that the suggested method outperforms several current intrusion detection systems in the same field of research, confirming its effectiveness and dominance in cyberattack identification and categorization in Blockchain communication networks.

References

[1] Aldabbas, Hamza, Dheeb Albashish, Khalaf Khatatneh, and Rashid Amin. "An architecture of IoT-aware healthcare smart system by leveraging machine learning." Int. Arab J. Inf. Technol. 19, no. 2 (2022): 160-172.

[2] Salim, Mikail Mohammed, Inyeung Kim, Umarov Doniyor, Changhoon Lee, and Jong Hyuk Park. "Homomorphic encryption based privacy-preservation for iomt." Applied Sciences 11, no. 18 (2021): 8757.

[3] Raghav, Nidhi, and Anoop Bhola. "Blockchain based privacy preservation in healthcare: a recent trends and challenges." Psychol. Educ. J 58 (2021): 5315-5324.

[4] Lin, Tzu-Wei, Chien-Lung Hsu, Tuan-Vinh Le, Chung-Fu Lu, and Bo-Yu Huang. "A smartcard-based user-controlled single sign-on for privacy preservation in 5G-IoT telemedicine systems." Sensors 21, no. 8 (2021): 2880.

[5] Kishore, Pushkar, Swadhin Kumar Barisal, Kulamala Vinod Kumar, and Durga Prasad Mohapatra. "Security Improvement and Privacy Preservation in E-Health." In ICC 2021-IEEE International Conference on Communications, pp. 1-6. IEEE, 2021.

[6] Alsahli, Mohammed Abdullah, Ahmed Alsanad, Mohammad Mehedi Hassan, and Abdu Gumaei. "Privacy preservation of user identity in contact tracing for COVID-19-like pandemics using edge computing." IEEE Access 9 (2021): 125065-125079.

[7] Sharif, Md Haris Uddin. "Privacy preservation of medical data using random decision tree." (2021).

[8] DivyaKeerthi, S., K. Ashokkumar, S. K. B. Sangeetha, S. Gayathri, and K. Kamala. "IoT-enabled infrastructure privacy preservation in big data." European Journal of Molecular & Clinical Medicine 8, no. 2 (2021): 724-731.

[9] Rodriguez-Garcia, Mercedes, Antonio Balderas, and Juan Manuel Dodero. "Privacy Preservation and Analytical Utility of E-Learning Data Mashups in the Web of Data." Applied Sciences 11, no. 18 (2021): 8506.

[10] Almusallam, Naif, Abdulatif Alabdulatif, and Fawaz Alarfaj. "Analysis of Privacy-Preserving Edge Computing and Internet of Things Models in Healthcare Domain." Computational and Mathematical Methods in Medicine 2021 (2021).

[11] Chamikara, Mahawaga Arachchige Pathum, Peter Bertok, Ibrahim Khalil, Dongxi Liu, and Seyit Camtepe. "Privacy preserving distributed machine learning with federated learning." Computer Communications 171 (2021): 112-125.

[12] Deebak, Bakkiam David, Fadi Al-Turjman, and Anand Nayyar. "Chaotic-map based authenticated security framework with privacy preservation for remote point-of-care." Multimedia Tools and Applications 80 (2021): 17103-17128.

[13] Siddique, Sarkar, and James CL Chow. "Machine learning in healthcare communication." Encyclopedia 1, no. 1 (2021): 220-239.

[14] Khan, Abdullah Ayub, Asif Ali Laghari, Muhammad Shafiq, Omar Cheikhrouhou, Wajdi Alhakami, Habib Hamam, and Zaffar Ahmed Shaikh. "Healthcare Ledger Management: A Blockchain and Machine Learning-Enabled Novel and Secure Architecture for Medical Industry." Human-Centric Computing and Information Sciences 12 (2022).

[15] Wu, Yulei, Hong-Ning Dai, Hao Wang, and Kim-Kwang Raymond Choo. "Blockchain-based privacy preservation for 5g-enabled drone communications." IEEE Network 35, no. 1 (2021): 50-56.

[16] Truonga, Nguyen, Kai Suna, Siyao Wanga, Florian Guittona, and YiKe Guoa. "Privacy Preservation in Federated Learning: Insights from the GDPR Perspective."

[17] Hasanova, Huru, Muhammad Tufail, Ui-Jun Baek, Jee-Tae Park, and Myung-Sup Kim. "A novel blockchain-enabled heart disease prediction mechanism using machine learning." Computers and Electrical Engineering 101 (2022): 108086.

[18] Ahmed, Imran, Yulan Zhang, Gwanggil Jeon, Wenmin Lin, Mohammad R. Khosravi, and Lianyong Qi. "A blockchain-and artificial intelligence-enabled smart IoT framework for sustainable city." International Journal of Intelligent Systems 37, no. 9 (2022): 6493-6507.

[19] Mahzabin, Rahnuma, Fahim Hossain Sifat, Sadia Anjum, Al-Akhir Nayan, and Muhammad Golam Kibria. "Blockchain associated machine learning and IoT based hypoglycemia detection system with auto-injection feature." arXiv preprint arXiv:2208.02222 (2022).

[20] Kaushik, Keshav, and Adarsh Kumar. "Demystifying quantum blockchain for healthcare." Security and Privacy (2022): e284.

[21] Pimple, Jagdish F., Avinash Sharma, and Jitendra Kumar Mishra. "Medisecure: A blockchain-enabled ensemble learning approach for user-controlled single sign-on and privacy preservation in medical cyber-physical systems." In International Conference on the Role of AI in Bio-Medical Translations' Research for the Health Care Industry, pp. 71-86. Cham: Springer Nature Switzerland, 2023.

[22] Pimple, Jagdish F., Avinash Sharma, and Jitendra Kumar Mishra. "Elevating Security Measures in Cyber-Physical Systems: Deep Neural Network-Based Anomaly Detection with Ethereum Blockchain for Enhanced Data Integrity." *Journal of Electrical Systems* 19, no. 2 (2023).