[1]Mr. Jagdish F. Pimple

[2]Dr. Avinash Sharma

[3]Dr.Jitendra Kumar Mishra

Elevating Security Measures in Cyber-Physical Systems: Deep Neural Network-Based Anomaly Detection with Ethereum Blockchain for Enhanced Data Integrity

Abstract: - The rapid development of physical device-based data collection in emerging technology needs smart, secure, and intelligent transmission. Cyber physical systems compete with the requirement of intelligent transmission of data. In cyber physical systems, security is a very challenging task due to the heterogeneous connections of devices in real time. This paper proposes a novel methodology for cyber-attack finding in cyber physical systems. The proposed system employed a DNN-deep neural network for the categorization of normal and attack data. The employed deep neural network design for 4 hidden layers for the detection of anomalies. For the secured transmission, we employed the blockchain process in Ethereum. The process of Ethereum generates blocks of blockchain with headers and transmits data over the cyberworld to the physical world with the alteration of data. For the authentication of the projected algorithm tested on two real-time datasets, such as NSL-KDD15 and CIDDS_001. The working of proposed algorithm is very promising in compression of existing algorithms of deep learning like RNN-recurrent neural networks, DBN, and DNN.

Keywords: Deep neural network, Intrusion detection, Blockchain, Cyber–physical system, Security

I. INTRODUCTION

Cyber-physical systems (CPS) are pillars for controlling the world's sensitive infrastructure of information technology. The CPS concept is based on three major components: cyberspace, physical space, and the kinematics of data. The installation of CPS can be compromised by hundreds or thousands of sensors and actuators. The scale of data collection is very large and creates several challenges, such as data analysis, performance, and security. The diverse nature and capacity of heterogeneous data support systems draw attention to online medical record systems. The E-medical record system enables patients and doctors to store personal medical records and treatment plans. Health-related data about patients is sent to the internet for real-time processing and analysis of a massive amount of data. In this case, the dynamic integration of the cyber and physical parts of medical cyber-physical systems (MPCS) calls for an enhanced computing foundation. The sensitivity of the personal records of patients is very high due to the multiple integrations of data sources and agents' systems. Privacy and security are important factors in the CPS system. For robust security and privacy, several authors employed the blockchain approach. The blockchain approach enhances the safety process of the cyber physical system. Blockchain technology provides secured distributed data transmission over cyberspace to the physical world. Blockchain technology has provided fresh insight into the security and assurance of medical records thanks to its decentralisation, scattered data storage, end-to-end transmission, and encryption algorithm features. By using valid security techniques, it can reconcile the logical contradiction between information sharing and security insurance. Data security is a major concern for intelligent healthcare systems, and protecting patient privacy is now essential. Despite the integration of blockchain technology into cyber physical systems, security and data analysis are major problems. For the security of data, several authors employed machine learning and deep learning algorithms. Deep learning algorithms provide capacity for data classification and detection of heterogeneous data. Deep-neural-networks (DNN) and (RNN) recurrent neural networks were employed in [10, 12] for the finding of intrusions in CPS systems. To minimize security issues in Cyber-physical systems (CPS),

[1]Research Scholar, Department of Computer Science & Engineering, Madhyanchal Professional University Bhopal, MP.

[1]Assistant Professor, Department of Information Technology, St.Vincent Pallotti College of Engineering and Technology,Nagpur

pimplejagdish@gmail.com, jpimple@stvincentngp.edu.in

[2]Professor, Department of Computer Science & Engineering, Madhyanchal Professional University Bhopal, MP.

[2]Professor, Department of Computer Science & Engineering, Oriental College of Technology, Bhopal MP.

avinashvtp@gmail.com

[3]Associate Professor Department of Electronics & Communication, Madhyanchal Professional University Bhopal, MP.

jitendra_mishra0125@yahoo.co.in

this paper offers secured intrusion detection through blockchain data broadcast and grouping in the medical system. The proposed algorithm enhances the detection capacity of intrusion before processing the patient's data. The proposed algorithm employed feature optimization of complex features of intrusion in the physical system. The process of feature optimization employed the BAT optimization method. The BAT optimization algorithm is a dynamic population-based swarm intelligence algorithm. The contribution of paper summaries as follows:

- Proposed robust intrusion detection in cyber physical system with blockchain technology.
- The suggested algorithm goes through multiple stages, including data transfer, encryption, intrusion detection, and data transmission.
- Employed the proposed algorithm for anomaly detection
- Compare existing algorithms for performance evaluation.

The remaining papers are organized as below: Section II refer to related work; Section III offers a recommended technique; Section IV is an experimental study; and Section V serves as a conclusion.

II. RELATED WORK

The realm of cyber-physical security has garnered considerable attention from researchers, particularly concerning its application in healthcare systems and integration into the overarching framework of cybersecurity protocols. Recently, various authors have proposed the methods based on ML- machine learning and DL-deep learning to fortify the security capabilities of Cyber-Physical Systems (CPS). This comprehensive review outlines the recent advancements in algorithms pertaining to cyber-physical systems.

The authors of [1] presented a deep learning-based approach designed to defend against cyberattacks. To prevent possible data breaches, they implemented the Long Short-Term Memory (LSTM) paradigm inside the standardized smart metering infrastructure. The goal of this system was to provide improved security. It was called AMLODA-B (Adversarial Machine-Learning Occupancy-Detection-Avoidance with Blockchain).

In [2], authors proposed a methodology that optimizes content caching and resource allocation, particularly beneficial in the context of Mobile Edge Computing (MEC) for Virtual Car Sharing (VCPS), improving driving experience.

Moreover, [4] addressed the crucial issue of preserving privacy and safeguarding data integrity against potential integrity attacks. This study also focused on detecting zero-day attacks with minimal false alarm rates to protect CPS data.

In [5], authors introduced a patient-centric approach aimed at securing data on reliable devices, such as end-users' smartphones, ensuring discretion over data sharing access. Based on experimental data, their proposed solution outperformed other existing models with a superior attack estimation ratio of 96.5%, accuracy ratio of 98.2%, efficiency ratio of 97.8%, latency reduction to 21.3%, and lower communication costs at 18.9%.

Subsequently, in [6], authors utilized PHR-Cypher-Text of IoMT on the Interplanetary File System (IPFS), employing blockchain technology for keyword index authentication via zero-knowledge proof.

In [7], the focus was on health experts tracing users who opt out or are impotent to engage in contact locating, proposing a solution utilizing edge servers that reduces power usage by end-users up to 97%.

Additionally, [8] proposed privacy protection solutions specifically for edge healthcare and IoT applications, emphasizing methods to incorporate privacy into medical solutions, including fog-assisted smart cities, smart automobiles, and smart grids, ensuring reliable and secure data gathering with short computational rate and compression ratio.

The authors of [10] enhanced security in medical IoT data and electronic health records (EHRs) within S-Healthcare Services by integrating data access control and data usage auditing mechanisms. This resulted in increased processing and communication efficiency.

Furthermore, [11] validated their approach using heart disease dataset, showcasing enhanced disease prediction accuracy in EHR systems. In [13], bidirectional security and enhanced timeliness of information acquisition, particularly in the context of 5G, were emphasized, safeguarding case database privacy and patient information.

Subsequent studies like [15] highlighted capabilities of an OCBS framework for secure and patient-centric integration with off-chain storage. Moreover, in [16], a fog computing model based on blockchain for IoMT was proposed, ensuring high reliability in file transfer.

Authors in [17] provided security analysis of AISCM-FH and its impact on key performance parameters, while [19] evaluated performance characteristics of proposed methods for improved security against healthcare data attacks. In [20], a prototype model integrating IoMT and blockchain technology to enhance patient-health-factor analysis was demonstrated. Additionally, [21] introduced a blockchain-enabled edge computing mechanism using consensus protocols and smart contracts to address privacy concerns and scalability issues.

In tandem with fog computing, [22] investigated blockchain's potential in mitigating privacy and security challenges, addressing drawbacks from IoMT and fog computing (FC) perspectives. [23] Compiled research on novel blockchain solutions combined with AI technologies, setting new standards for the food and medical industries.

Moreover, [24] proposed a healthcare data safety framework employing blockchain technology to notify network consumers of any unauthorized data modifications. Furthermore, [25] introduced secure, transparent techniques utilizing blockchain and machine learning models to enhance patient treatment and healthcare system integrity.In [26], deep learning methods and platforms used in AI-based blockchain systems were examined, covering supervised and unsupervised machine learning challenges. Authors in [27] presented a smart contract solution based on blockchain and machine learning, enhancing security and lowering resource consumption for real-time medical applications. [28] investigated privacy and security issues in machine-learning models, emphasizing resource utilization effectiveness.[29] highlighted various usages of blockchain in the medical industry, particularly in instantaneous data observing and analytics. Finally, [30] explored blockchain applications in COVID-19 and offered recommendations for fortifying the healthcare system through blockchain integration with big data, IoT, AI, and machine learning.

III. PROPOSED METHODOLOGY

Figure 1 depicts a proposed model of a physical system for securing the transmission of patients' data from the cyberworld to the physical world. The proposed model consists of a physical space that generates data on patients, doctors, and hospital records. The other component is the intrusion detection system; in this phase, analyse the processing of data. after the processing of data employs blockchain technology and generates different blocks and shares them in distributed manners. The distributed blocks were stored in a database server and employed a deep learning based classification method for finding of attacks & normal data. After the completion of the classification task, estimate the parameters of the algorithms. The processing of a model is described as follows:

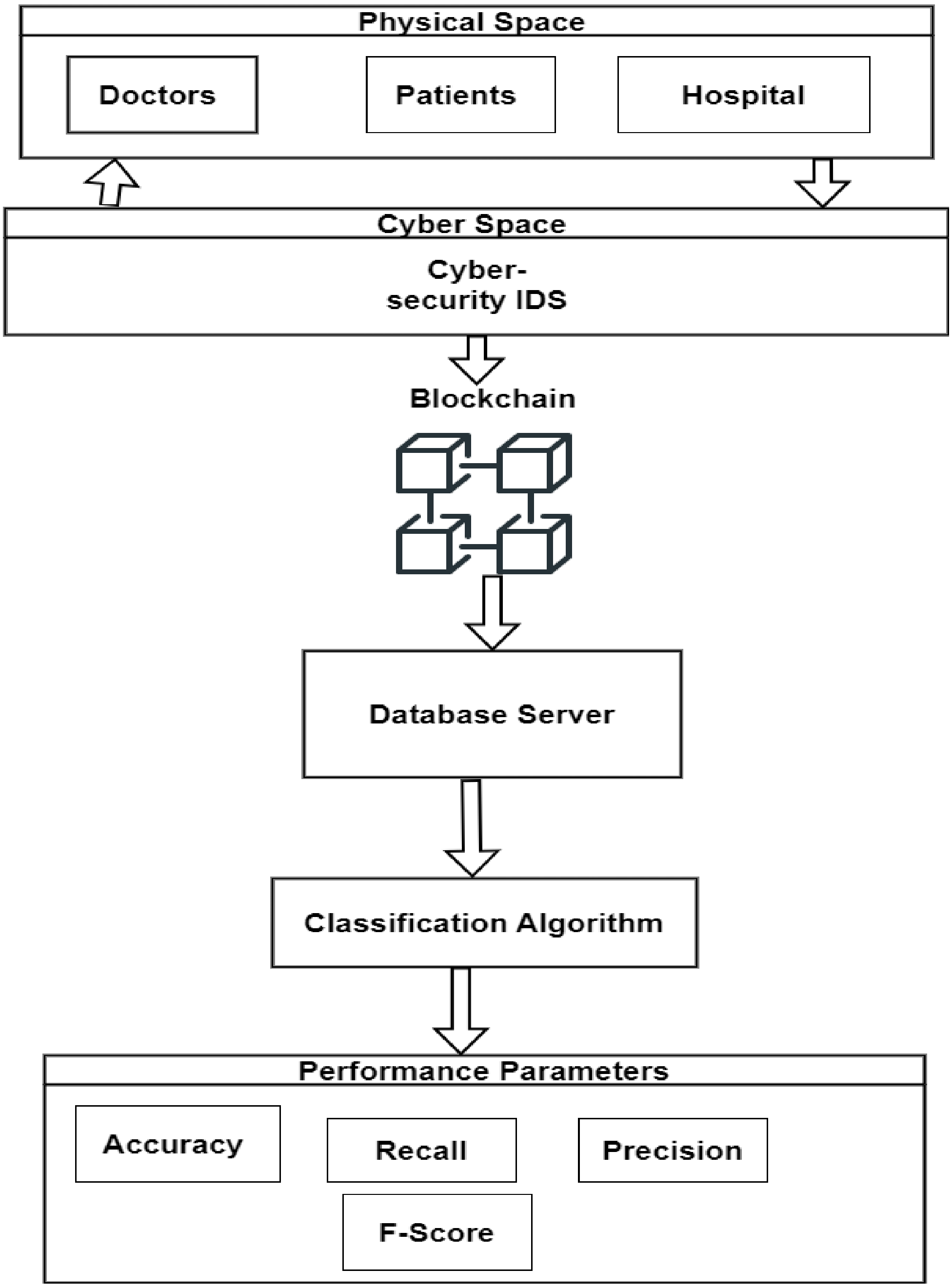

Figure 1 proposed model of cyber security in cyber physical system

Data gathering:

In this phase collect data form different sources of physical devices in cyber physical system, the intrusion detection process is employed on the gathered data to estimate existence of intrusion. To find intrusion in all data employs DNN model. For the detection of intrusion design deep neural network of hidden layer M=4. The design classification algorithm has two class one is attack class and other is normal class. For the processing of activation function RLU is employed. The non-linear relationship of algorithm describes as two variables K and Ki+1

$$Ki + 1 = \delta(wki + b) \dots\dots\dots\dots\dots\dots\dots\dots (1)$$

where and δ is the activation function ,W and b are the model parameters. K and Ki+1 are variables that come from layers. the deep neural network, a multilayer neural network argument with advanced learning. The network categorization is defined as y=f(u). The definition of the network function process is

K1= $\delta 1$(w1u+b1)

k2= $\delta 2$(w2p1+b2)

….

………

Y= δL(wLpL-1+bL)

here L is number of layers

Process of training of Deep neural network

The connection of neurons defines the method of collected data

$F_k : R^{n_x} \rightarrow R^{n_x},$ where $x_k \in R^{n_x}$

The set of data proceed in training

Hypothesis of error estimated by E

$E_j = H_j\left(x_j\right) + v_j, \quad \forall\, k \le j \le k + A$

where $H_j: R^{n_x} \rightarrow R^{n_y}$ is the relation of multilayer input.

Estimate trained pattern

$x_k = F_0 \rightarrow k(x_0) + \xi k$

3 define learning factor as

$$x'_k = arg\min_x \left\{ \|x - x_k\| B_k^{-1} + \sum_{j=k}^{k+A} \|H_j F_j(x) - y_j\| R_j^{-1} \right\}$$

Algorithm

Define $i = 0$

while $i < L$ do

process the training of DNN network

$\{x'_k \,\mathrm{I}\, k \in [M\,.i, M\,.(i+1)]\}$

$$x'_k = arg\min_x \left\{ \|x - x_k\| R_k^{-1} + \sum_{k}^{k+p} \|H_j\, M_j, (x)\| p_j^{-1} \right\}$$

Estimate the class

Attacks $= \{Fs(x'_{k-1}),\ x'_k\}$ with $k \in [i.M, (i+1).M]$

Measure i for next step

end

Processing of Blockchain

After the detection of intrusions in gathered data, the secured transmission of image data is given in database server. The Ethereum blockchain process is segmented into four distinct blocks, each securely transmitted and stored in the cloud. These blocks contain the timestamp, the hash value of the oldest block, the most recent block, and transaction information. Blockchain is an open, shared, decentralized digital ledger that has been applied to many different types of transaction storing. Due to the fact that every block consists of the cryptographic value of the preceding block, an intruder record cannot be altered. Every transaction in the blockchain model is verified by miners and cryptographically signed using a hash value. As illustrated in Fig. 2, it includes blocks of each transaction as well as a repeated measure of the entire ledger. Blockchain provides the capacity to share, distribute, safely, and trustable the data ledger in a decentralized manner. Using smart contract code, decentralized storage, a kind of blockchain, is used to store the most data related to both recent and older blocks. LitecoinDB, SiacoinDB, IPFS, BigchainDB, Swarm, and others have all applied for decentralized databases lately. The Interplanetary File System (IPFS) is a shared, p2p, scattered database that forwards and links common files [16].

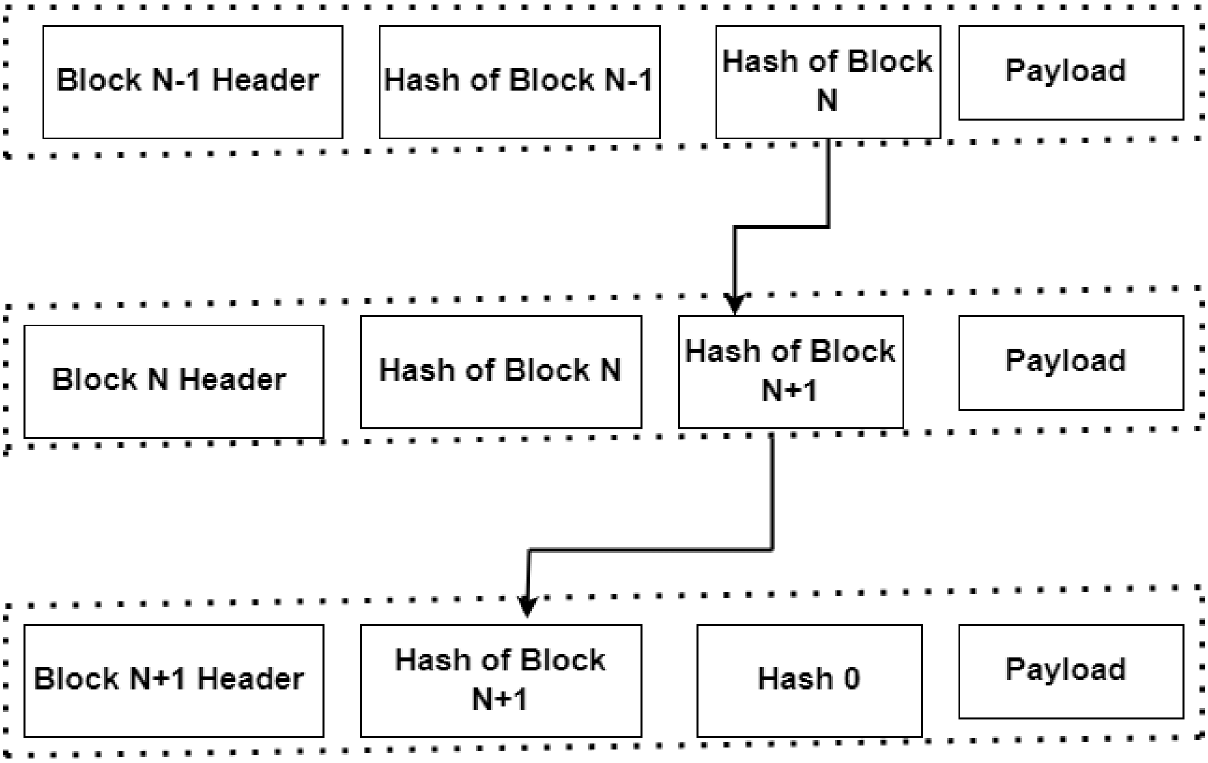

Figure 2 blocks of Blockchain

IV. EXPERIMENTAL ANALYSIS

The simulation of the planned algorithm has been tested in several scenarios. The process of simulation uses MATLAB software version 2018R. For the validation of the algorithm, it employed two intrusion detection datasets, such as the NSL-KDD 2015 and CIDDS-001 datasets [7]. The NSL-KDD dataset involves 125,973 instances with 41 characteristics and two classes, whereas the CIDDS-001 dataset encompasses 1,018,950 instances by 14 attributes and two classes. To assess the efficiency of the proposed methodology in cyber-physical security systems, it is compared against established algorithms like DBN, DNN, and RNN. The algorithms' performance is evaluated in context on metrics such as sensitivity, accuracy, specificity, and F-score as referenced in [35, 36, 37].

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

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

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

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

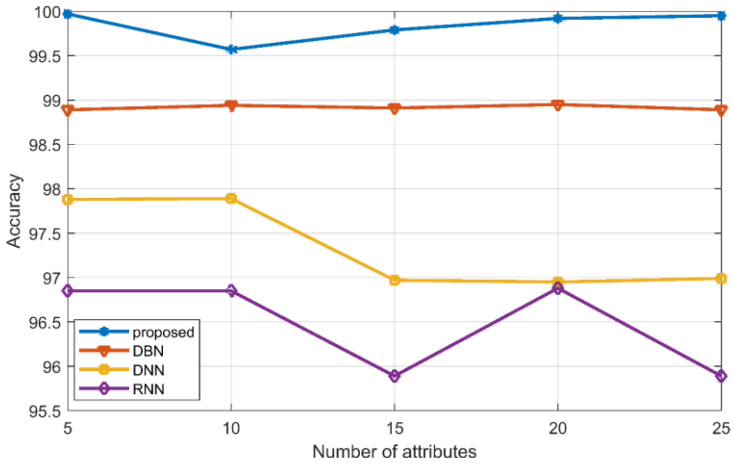

Figure: 3 performance analysis of Accuracy and Number of attributes of using method Proposed, DBN, DNN, and RNN, and NSL-KDD 2015 dataset.

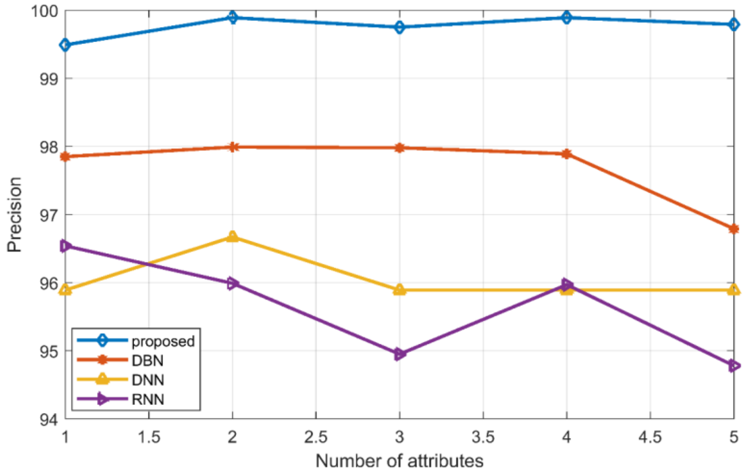

Figure: 4 performance analysis of precision and Number of attributes of using method Proposed, DBN, DNN, and RNN, and NSL-KDD 2015 dataset.

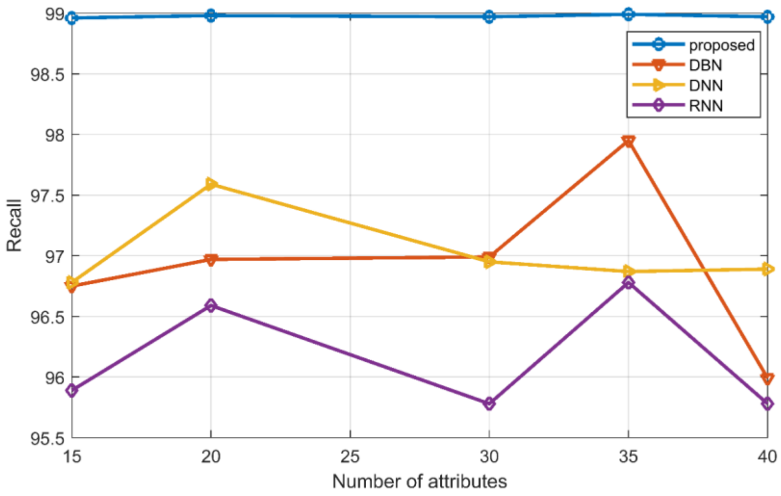

Figure: 5 performance analysis of Recall and Number of attributes of using method Proposed, DBN, DNN, and RNN, and NSL-KDD 2015 dataset.

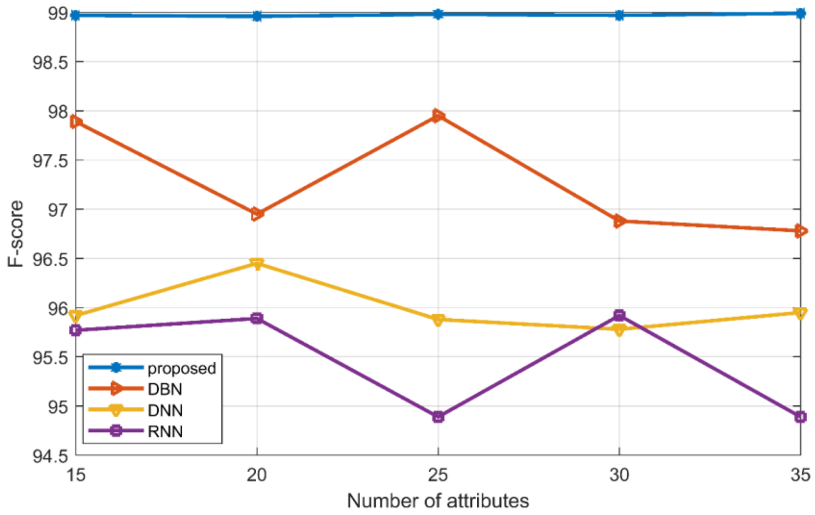

Figure: 6 performance analysis of F-score and Number of attributes of using method Proposed, DBN, DNN, and RNN, and NSL-KDD 2015 dataset.

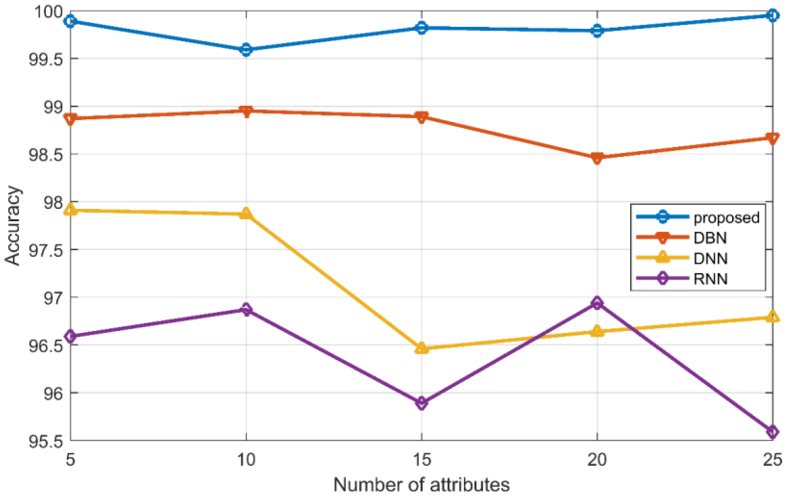

Figure: 7 performance analysis of Accuracy and Number of attributes of using method Proposed, RNN, DNN, and DBN, and CIDDS-001 dataset.

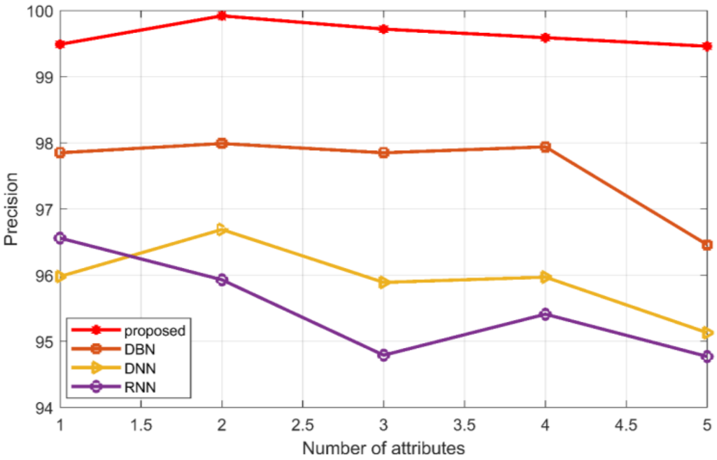

Figure: 8 performance analysis of precision and Number of attributes of using method Proposed, RNN, DNN, and DBN, and CIDDS-001 dataset.

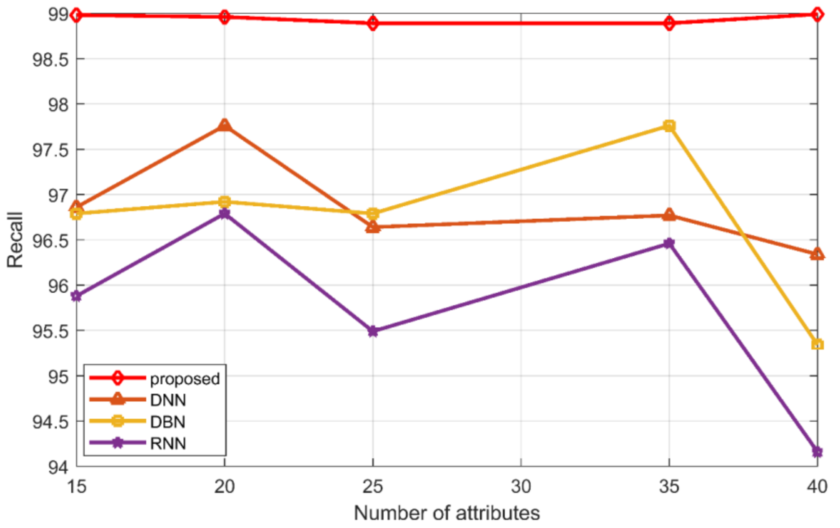

Figure: 9 performance analysis of recall and Number of attributes of using method Proposed, RNN, DNN, and DBN, and CIDDS-001 dataset.

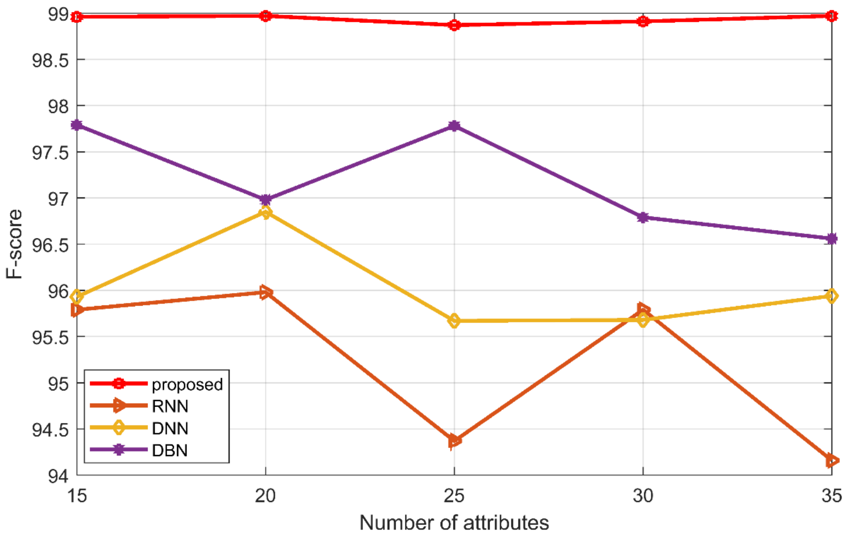

Figure: 10 performance analysis of F-score and Number of attributes of using method Proposed, RNN, DNN, and DBN, and CIDDS-001 dataset.

V. CONCLUSION & FUTURE WORK

This paper intends an innovative method for secure anomaly detection with blockchain and a deep neural network-based classification algorithm. The process of the proposed model consists of several sequences, such as data gathering, anomaly detection, and the creation of blocks. Comparing the proposed system with the current system reveals a number of security flaws. The proposed system provides good accuracy, demonstrating a favourable perception of the performance factor. Additionally, the outcomes are maintained through the use of blockchain technology, which inherits characteristics such as transparency, immutability, and crypto-hash-based connectivity. By taking into account certain parameters like F-score, recall, and precision, the planned system is also equated with the current system. Further, the proposed algorithms were tested on two reputed datasets, NSL-KDD15 and CIDDS001. The results of the suggested algorithm is matched with other deep learning algorithms like RNN, CNN, & DNN. In the future, we will employ feature optimisation algorithms using swarm intelligence.

REFERENCES

[1] Yilmaz, Ibrahim, Kavish Kapoor, Ambareen Siraj, and Mahmoud Abouyoussef. "Privacy protection of grid users data with blockchain and adversarial machine learning." In Proceedings of the 2021 ACM Workshop on Secure and Trustworthy Cyber-Physical Systems, pp. 33-38. 2021.

[2] Olowononi, Felix O., Danda B. Rawat, and Chunmei Liu. "Federated learning with differential privacy for resilient vehicular cyber physical systems." In 2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC), pp. 1-5. IEEE, 2021.

[3] Zhou, Junlong, Liying Li, Ahmadreza Vajdi, Xiumin Zhou, and Zebin Wu. "Temperature-constrained reliability optimization of industrial cyber-physical systems using machine learning and feedback control." IEEE Transactions on Automation Science and Engineering (2021).

[4] Keshk, Marwa, Benjamin Turnbull, Elena Sitnikova, Dinusha Vatsalan, and Nour Moustafa. "Privacy-preserving schemes for safeguarding heterogeneous data sources in cyber-physical systems." IEEE Access 9 (2021): 55077-55097.

[5] AlZubi, Ahmad Ali, Mohammed Al-Maitah, and Abdulaziz Alarifi. "Cyber-attack detection in healthcare using cyber-physical system and machine learning techniques." Soft Computing 25, no. 18 (2021): 12319-12332.

[6] Wang, Yong, Aiqing Zhang, Peiyun Zhang, Youyang Qu, and Shui Yu. "Security-aware and privacy-preserving personal health record sharing using consortium blockchain." IEEE Internet of Things Journal 9, no. 14 (2021): 12014-12028.

[7] 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.

[8] Potnurwar, A. V. ., Bongirwar, V. K. ., Ajani, S. ., Shelke, N. ., Dhone, M. ., & Parati, N. . (2023). Deep Learning-Based Rule-Based Feature Selection for Intrusion Detection in Industrial Internet of Things Networks. International Journal of Intelligent Systems and Applications in Engineering, 11(10s), 23–35.

[9] 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).

[10] Ullah, Ata, Muhammad Azeem, Humaira Ashraf, Abdulellah A. Alaboudi, Mamoona Humayun, and Nadeem Z. Jhanjhi. "Secure healthcare data aggregation and transmission in IoT—A survey." IEEE Access 9 (2021): 16849-16865.

[11] S. Ajani and M. Wanjari, "An Efficient Approach for Clustering Uncertain Data Mining Based on Hash Indexing and Voronoi Clustering," 2013 5th International Conference and Computational Intelligence and Communication Networks, 2013, pp. 486-490

[12] El Majdoubi, Driss, Hanan El Bakkali, and Souad Sadki. "SmartMedChain: A blockchain-based privacy-preserving smart healthcare framework." Journal of Healthcare Engineering 2021 (2021).

[13] Domadiya, Nikunj, and Udai Pratap Rao. "Improving healthcare services using source anonymous scheme with privacy preserving distributed healthcare data collection and mining." Computing 103, no. 1 (2021): 155-177.

[14] Liu, Yaru, Jia Yu, Jianxi Fan, Pandi Vijayakumar, and Victor Chang. "Achieving privacy-preserving DSSE for intelligent IoT healthcare system." IEEE Transactions on Industrial Informatics 18, no. 3 (2021): 2010-2020.

[15] Limkar, Suresh, Ashok, Wankhede Vishal, Singh, Sanjeev, Singh, Amrik, Wagh, Sharmila K. & Ajani, Samir N.(2023) A mechanism to ensure identity-based anonymity and authentication for IoT infrastructure using cryptography, Journal of Discrete Mathematical Sciences and Cryptography, 26:5, 1597–1611

[16] Sun, Yi, Jie Liu, Keping Yu, Mamoun Alazab, and Kaixiang Lin. "PMRSS: privacy-preserving medical record searching scheme for intelligent diagnosis in IoT healthcare." IEEE Transactions on Industrial Informatics 18, no. 3 (2021): 1981-1990.

[17] Wang, Ke, Chien-Ming Chen, Zhuoyu Tie, Mohammad Shojafar, Sachin Kumar, and Saru Kumari. "Forward privacy preservation in IoT-enabled healthcare systems." IEEE transactions on industrial informatics 18, no. 3 (2021): 1991-1999.

[18] Miyachi, Ken, and Tim K. Mackey. "hOCBS: A privacy-preserving blockchain framework for healthcare data leveraging an on-chain and off-chain system design." Information Processing & Management 58, no. 3 (2021): 102535.

[19] Duhayyim, Mesfer AI, Fahd N. Al-Wesabi, Radwa Marzouk, Abdalla Ibrahim Abdalla Musa, Noha Negm, Anwer Mustafa Hilal, Manar Ahmed Hamza, and Mohammed Rizwanullah. "Integration of Fog Computing for Health Record Management Using Blockchain Technology." Computers, Materials & Continua 71, no. 2 (2022).

[20] Wazid, Mohammad, Ashok Kumar Das, Sachin Shetty, Joel JPC Rodrigues, and Mohsen Guizani. "AISCM-FH: AI-Enabled Secure Communication Mechanism in Fog Computing-Based Healthcare." IEEE Transactions on Information Forensics and Security 18 (2022): 319-334.

[21] Kamruzzaman, M. M., Bingxin Yan, Md Nazirul Islam Sarker, Omar Alruwaili, Min Wu, and Ibrahim Alrashdi. "Blockchain and fog computing in IoT-driven healthcare services for smart cities." Journal of Healthcare Engineering 2022 (2022).

[22] Poongodi, J., K. Kavitha, and S. Sathish. "Healthcare Internet of Things (HIoT) data security enhancement using blockchain technology." Journal of Intelligent & Fuzzy Systems 43, no. 4 (2022): 5063-5073.

[23] Ajani, S. N. ., Khobragade, P. ., Dhone, M. ., Ganguly, B. ., Shelke, N. ., & Parati, N. . (2023). Advancements in Computing: Emerging Trends in Computational Science with Next-Generation Computing. International Journal of Intelligent Systems and Applications in Engineering, 12(7s), 546–559.

[24] Almalki, Jameel, Waleed Al Shehri, Rashid Mehmood, Khalid Alsaif, Saeed M. Alshahrani, Najlaa Jannah, and Nayyar Ahmed Khan. "Enabling blockchain with IoMT devices for healthcare." Information 13, no. 10 (2022): 448.

[25] Chu, Kuo Ming. "Understanding IoHT and Edge/Fog Computing Solutions for Smart In-Home Remote Healthcare." Fog Computing Solutions for Smart In-Home Remote Healthcare (2022).

[26] Wiling, B. (2021). Locust Genetic Image Processing Classification Model-Based Brain Tumor Classification in MRI Images for Early Diagnosis. Machine Learning Applications in Engineering Education and Management, 1(1), 19–23. Retrieved from http://yashikajournals.com/index.php/mlaeem/article/view/6

[27] Alam, Shadab, Mohammed Shuaib, Sadaf Ahmad, Dushantha Nalin K. Jayakody, Ammar Muthanna, Salil Bharany, and Ibrahim A. Elgendy. "Blockchain-based solutions supporting reliable healthcare for fog computing and internet of medical things (IoMT) integration." Sustainability 14, no. 22 (2022): 15312.

[28] Vyas, Sonali, Mohammad Shabaz, Prajjawal Pandit, L. Rama Parvathy, and Isaac Ofori. "Integration of artificial intelligence and blockchain technology in healthcare and agriculture." Journal of Food Quality 2022 (2022).

[29] Tello, Alcides Bernardo, Jiuhong Xing, Aparna Lalitkumar Patil, Lalitkumar Premchandra Patil, and Shabnam Sayyad. "Blockchain Technologies in Healthcare System for Real Time Applications Using IoT and Deep Learning Techniques." International Journal of Communication Networks and Information Security 14, no. 3 (2022): 257-268.

[30] Hassan, Mir. "A Blockchain-based intelligent machine learning system for smart health care." (2022).

[31] Kumar, Ritik, Arjunaditya, Divyangi Singh, Kathiravan Srinivasan, and Yuh-Chung Hu. "AI-powered blockchain technology for public health: A contemporary review, open challenges, and future research directions." In Healthcare, vol. 11, no. 1, p. 81. MDPI, 2022.

[32] Gaur, Rajkumar, Shiva Prakash, Sanjay Kumar, Kumar Abhishek, Mounira Msahli, and Abdul Wahid. "A Machine-Learning–Blockchain-Based Authentication Using Smart Contracts for an IoHT System." Sensors 22, no. 23 (2022): 9074.

[33] Lakhan, Abdullah, Mazin Abed Mohammed, Jan Nedoma, Radek Martinek, Prayag Tiwari, Ankit Vidyarthi, Ahmed Alkhayyat, and Weiyu Wang. "Federated-learning based privacy preservation and fraud-enabled blockchain IoMT system for healthcare." IEEE journal of biomedical and health informatics 27, no. 2 (2022): 664-672.

[34] Abbas, Alhamzah F., Naveed Akhtar Qureshi, Nohman Khan, Rabia Chandio, and Javed Ali. "The Blockchain Technologies in Healthcare: Prospects, Obstacles, and Future Recommendations; Lessons Learned from Digitalization." International Journal of Online & Biomedical Engineering 18, no. 9 (2022).

[35] Srivastava, Shilpa, Millie Pant, Sunil Kumar Jauhar, and Atulya K. Nagar. "Analyzing the Prospects of Blockchain in Healthcare Industry." Computational and Mathematical Methods in Medicine 2022 (2022).

[36] Sairise, Raju M., Limkar, Suresh, Deokate, Sarika T., Shirkande, Shrinivas T. , Mahajan, Rupali Atul & Kumar, Anil(2023) Secure group key agreement protocol with elliptic curve secret sharing for authentication in distributed environments, Journal of Discrete Mathematical Sciences and Cryptography, 26:5, 1569–1583, DOI: 10.47974/JDMSC-1825

[37] Boutebba, H., Lakhal, H., Slimani, K., & Belhadi, T. (2023). The nontrivial solutions for nonlinear fractional Schrödinger-Poisson system involving new fractional operator. Advances in the Theory of Nonlinear Analysis and Its Applications, 7(1), 121–132.

[38] Granados, C. (2023). Convergence of Neutrosophic Random Variables. Advances in the Theory of Nonlinear Analysis and Its Applications, 7(1), 178–188.

[39] Naas, A., Benbachir, M., Abdo, M. S., & Boutiara, A. (2022). Analysis of a fractional boundary value problem involving Riesz-Caputo fractional derivative. Advances in the Theory of Nonlinear Analysis and Its Applications, 6(1), 14–27.