2023 International Conference on Network, Multimedia and Information Technology (NMITCON) | 979-8-3503-0082-6/23/$31.00 ©2023 IEEE | DOI: 10.1109/NMITCON58196.2023.10275980

AI and Blockchain-based Secure Message Exchange Framework for Medical Internet of Things

1st Barkha Panchal
Department of Comp. Sci. & Engg.
Institute of Technology,
Nirma University
Ahmedabad, India
22mces07@nirmauni.ac.in

2nd Snehal Parmar
Department of Comp. Sci. & Engg.
Institute of Technology,
Nirma University
Ahmedabad, India
22mces10@nirmauni.ac.in

3rd Tejal Rathod
Department of Comp. Sci. & Engg.
Institute of Technology,
Nirma University
Ahmedabad, India
20ftphde39@nirmauni.ac.in

4th Nilesh Kumar Jadav
Department of Comp. Sci. & Engg.
Institute of Technology,
Nirma University
Ahmedabad, India
21ftphde53@nirmauni.ac.in

5th Rajesh Gupta
Department of Comp. Sci. & Engg.
Institute of Technology,
Nirma University
Ahmedabad, India
rajesh.gupta@nirmauni.ac.in

6th Sudeep Tanwar
Department of Comp. Sci. & Engg.
Institute of Technology,
Nirma University
Ahmedabad, India
sudeep.tanwar@nirmauni.ac.in

***Abstract*—With the advent of revolutionary technologies, the Internet of Things (IoT) has proved its effectiveness in the medical sector. The inclusion of sensors in IoT devices enables connectivity and facilitates the collection of valuable data for patient monitoring and effective treatment methods. Sensors are tagged with the medical equipment and foster real-time tracking of medical devices such as oxygen pumps, nebulizers, wheelchairs, etc. It collects medical data that has the patient's personal and sensitive information regarding medical history, such as heart rate, diagnosis information, drug prescription, body temperature, etc. However, the security of medical data has become a significant concern. Therefore, this paper proposes an artificial intelligence (AI) and blockchain-enabled scheme that offer cyber security to medical IoT data. Here, different machine learning (ML) classifiers, such as decision tree (DT), K-Nearest neighbor (KNN), Naive Bayes (NB), support vector machine (SVM), and gradient boosting classifier (GBC) are used to classify medical IoT data as an attack (1) and normal (0) class. Then, an IPFS-based blockchain network is used to offer security and transparency to the medical IoT data. Moreover, for evaluation, different performance metrics are considered, such as accuracy, training time, receiver operating characteristic (ROC) curve, and scalability. Among all ML classifiers, KNN achieves the highest accuracy of** 95.4%**.**

***Index Terms*—Medical applications, Healthcare, Internet of Things (IoT), Blockchain, Smart Contract, IPFS**

I. Introduction

Nowadays, various technological advancements such as smart agriculture, smart healthcare, smart home, autonomous vehicle, etc., make people's life easy. The healthcare industry is growing rapidly, driven by an aging population, consumer demand for better services at more affordable prices, and an increasing global focus on preventative health. The most significant technological advance in recent years is the Internet of Things (IoT) in the healthcare sector [1]. It is used for structured patient monitoring, empowering doctors to provide top-notch treatment. IoT-enabled healthcare applications, such as defibrillators, monitoring equipment, nebulizers, and wheelchairs, provide real-time monitoring and observation [2]. This medical equipment has the ability to significantly reduce costs and enhance patient outcomes. With these new developments, IoT in healthcare has an optimistic future. However, during the last few years, a concentrated effort has been made to design and create inexpensive sensors that can perform comparable functions [3]. These sensors produce an all-encompassing, low-cost, multi-sensor-based healthcare system that is accessible and widely installable across geographies when integrated on hardware platforms and coordinated with back-end processing systems [4].

Moreover, IoT devices are being used in the healthcare sector to enhance patient experiences [5]. Remote monitoring is made possible by IoT-connected healthcare applications, which also improve the integration and intelligence of physical settings [6]. The overall effectiveness of operations, clinical duties, and resource management improve the patient experience. However, all connected devices exchange data in real time; privacy is the main IoT problem. Private information may be at risk if the end-to-end communication is not secure [7]. Criminals may profit from other people's personal information. Accuracy issues could arise from the real-time management of such massive data sets. Using IoT security concerns like distributed denial-of-service (DDoS), ransomware, and social engineering, important information can be taken from both individuals and businesses [8]. Attackers may utilize IoT infrastructure's security weaknesses to execute complex cyberattacks.

Artificial intelligence (AI)-based cybersecurity solutions for medical IoT devices can help secure sensitive medical data

979-8-3503-0082-6/23/$31.00 ©2023 IEEE

Authorized licensed use limited to: Khulna Univ of Engineering & Technology - KUET. Downloaded on February 21,2024 at 16:14:59 UTC from IEEE Xplore. Restrictions apply.

and protect against cyber threats [9] [10]. It provides several features, such as anomaly detection, threat intelligence, compliance, encryption, and data protection [11]. By incorporating AI and machine learning (ML), these solutions can improve the speed, accuracy, and efficiency of detecting and responding to cyber threats in medical IoT environments [12] [13]. Numerous researchers have employed ML-based solutions to address the security of medical IoT data. For example, Rhbech *et al.* [14] proposed advanced encryption standard encryption techniques to provide secure data monitoring of COVID-19 data, such as facial and geo-location identification. Here, they used the MQ telemetry transport protocol for secure node utilization in corporate communication. Then, Khadidos *et al.* [15] introduced a probabilistic super learning-based random hashing approach to secure medical data on the IoT-based cloud.

Further, Sankaran *et al.* [16] proposed a secure M-trust privacy protocol for a smart healthcare monitoring scheme that delivers privacy and security of the medical data. To measure the performance of the proposed protocol, they used different performance evaluation metrics, such as end-to-end delay, packet delivery ratio, computation time, and CPU utilization. Here, the researchers used different cybersecurity and cryptographic approaches to secure medical IoT data. However, in the aforesaid work, there are several shortcomings, such as cryptographic algorithms becoming insufficient when there are a huge number of devices and a large amount of patient data. Further, it has centralized trust, which is responsible for key distribution. Hence, all these factors affect the security of sensitive medical IoT data. Therefore, inspired by the aforementioned gaps, an AI and blockchain-enabled cyber security scheme is proposed to secure medical IoT data. First of all, medical data is collected from the different sensors which are attached to the IoT devices. Then, different ML classifiers are applied, such as decision tree (DT), K-Nearest neighbor (KNN), Naive Bayes (NB), support vector machine (SVM), and gradient boosting classifier (GBC), to classify whether the data has attack or normal. After that, the blockchain technology is used that offers decentralization, trust, transparency, and privacy for medical IoT data. Further, a layered architecture is proposed that includes a sensor, AI, blockchain, governance, and communication layer. Here, the performance of the proposed scheme is measured by considering different performance evaluation metrics, such as accuracy, training time, receiver operating characteristic (ROC) curve, and scalability.

A. Research Contributions

The following are the primary contribution of the paper:

- To propose an AI and blockchain-enabled secure data exchange framework for Medical Internet of Things.
- In the proposed scheme, different ML classifiers, such as DT, KNN, NB, SVM, and GBC, which classify medical IoT data into attack (1) and normal (0) classes are used to classift the medical IoT data. Moreover, the data imbalance problem is analyzed in the proposed work, and balanced the dataset using sampling process.
- To enhance the secure data storage, an IPFS-based blockchain technology is implemented, where smart contracts ensure data validation and immutable blocks ensures secure data storage for Medical IoT.
- In this paper, various metrics, such as accuracy, training time, ROC curve, and scalability, have been considered to evaluate the performance of the proposed scheme.

B. Organization

The subsequent sections of the paper are planned as follows: In Section II, discusses the proposed layered architecture for the proposed scheme that secures the medical IoT data. Then, Section III analyzes the results of the AI-based classification and blockchain-based secure storage for medical IoT data. The gist of the paper is concluded in Section IV.

II. The Proposed Approach

The development of top-notch services that assist people with diverse healthcare needs is one of the most crucial goals. Hence, this section proposea a medical IoT architecture that enhances system functionality, effectively uses available resources, and tool optimization in the medical domain. Fig.1 represents a broad structure for medical IoT systems that shows the integrated technologies and key elements of the healthcare architecture. It consists of five layers: the sensor layer, AI layer, blockchain layer, governance layer, and communication layer. These layers are used for data collection, pre-processing, classification, and secure storage. In the following sub-section, the working of each layer is discussed in detail.

A. Sensor layer

Nowadays medical industry adapts smart technologies such as IoT, augmented reality (AR), virtual reality (VR), etc., to offer better healthcare. Hence, this layer comprises various medical sensor devices that measure blood pressure, oxygen saturation, heart rate, EEG, magnetic field, EEG, and temperature. Further, various wearable devices, such as fitness trackers, smartwatches, and VR headsets, measure the patient's daily activity, heart rate, sleep patterns, walking steps, etc. It uses IoT applications for monitoring and medication refill services. There are various medical IoT sensor devices in this layer, such as $s_1 s_2, \ldots, s_i \in S$. Moreover, different uses, such as $u_1, u_2, \ldots, u_j \in U$, use these sensors to get medical benefits as shown in Eq. 1.

$$U_j \xrightarrow{uses} S_i \tag{1}$$

The data is collected from different sensors and passed to the next AI layer, which classifies whether the attack manipulates the data or not.

Authorized licensed use limited to: Khulna Univ of Engineering & Technology - KUET. Downloaded on February 21,2024 at 16:14:59 UTC from IEEE Xplore. Restrictions apply.

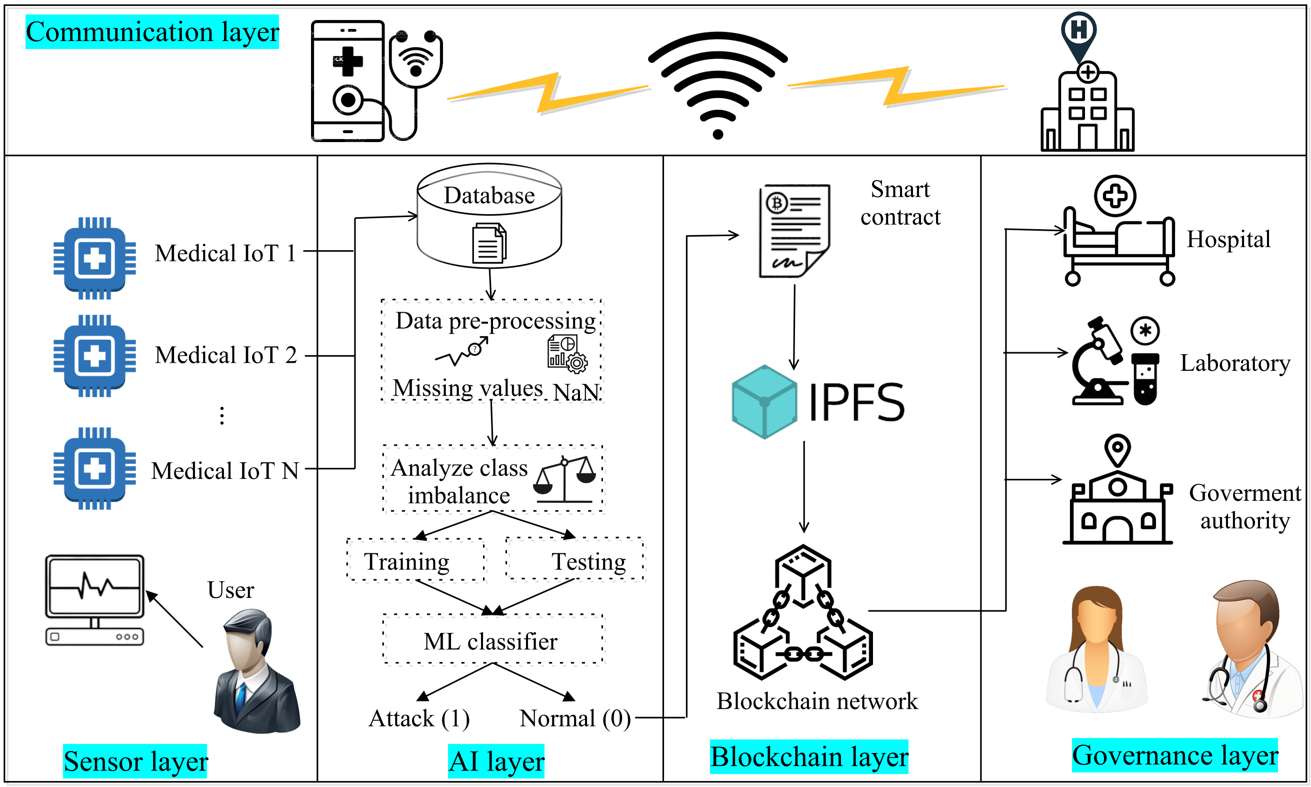


Fig. 1: Proposed architecture for Medical IoT

B. AI layer

The collected data from the sensor layer is stored in the database of comma-separated values (CSV) files. The final dataset is represented as ω, which consists of normal and IoT attack traffic for medical IoT. This data is passed into this layer, which classifies the data as an attack or normal data. Before passing the data to the ML classifier, there is a requirement to preprocess data and analyze class imbalance. The first step is data preprocessing, which includes cleaning, instance selection, normalization, one-hot coding, modification, feature extraction, and selection. This dataset uses preprocessing to identify the missing values, noisy data, NaN values, and normalization. Here, a standardization scaling is used to normalize the data, which uses mean and standard deviation. The mathematical representation of the standardization scaling is shown in Eq. 2

$$D' = \frac{D - \mu}{\sigma} \tag{2}$$

where μ indicates the mean value and σ represents standard deviation. Further, the data is very imbalanced; therefore, a synthetic minority oversampling (SMOTE) is used, which creates new and synthetic observations from the existing data and gives a balanced dataset. Then, the next step is data splitting, where the dataset is divided into training (ω_{tr}) and testing (ω_{ts}) part as mentioned in Eqs. 3 and 4. Initially, the training data is fed into the ML classifier, and then once the classifier is trained, the testing data is fed into the classifier.

$$\omega_{tr}, \omega_{ts} \xrightarrow{fed} ML_c \xrightarrow{classify} \gamma \tag{3}$$

$$\gamma = \begin{cases} 1 & Attack \\ 0 & Normal \end{cases} \tag{4}$$

where ML_c indicates ML classifier and γ is classified data. Here, different ML classifiers, such as DT, KNN, NB, SVM, and GBC, are used to bifurcate the data into attack (1) and normal (0) means non-attack part. Medical systems are vulnerable to cybersecurity risks as healthcare becomes more computerized and linked, which might compromise patient health and safety. Further, normal data consist of patient's personal and sensitive medical information, which requires strong security. Hence, the normal data is further passed to the next layer blockchain layer, which offers security and privacy of the data.

C. Blockchain layer

This layer provides security for the patient's medical data. It uses blockchain, a distributed ledger that keeps track of transactions on numerous computers. The data is passed through the smart contract, a self-executing contract with the agreement's

Authorized licensed use limited to: Khulna Univ of Engineering & Technology - KUET. Downloaded on February 21,2024 at 16:14:59 UTC from IEEE Xplore. Restrictions apply.

conditions encoded straight into code. It offers automation, trust, and transparency. Then, the data is stored in IPFS, a peer-to-peer file storage system. It provides content addressing content-addressable, versioning, and deduplication. It seeks to transform how the patient's medical data are kept, accessed, and shared over the internet. Further, large files are expensive and inefficient; therefore, the data of large files can be kept on IPFS, and their content identifiers can be stored on the blockchain.

$$\gamma_0 \xrightarrow[pass-data]{SC} IPFS \xrightarrow{stores} Blockchain_N \tag{5}$$

In Eq. 5 γ_0 represents the normal medical IoT data. SC denotes smart contract and $Blockchain_N$ is the blockchain network. In this way, the medical IoT data is stored in a secure and decentralized blockchain network. Now, the secured data is accessible to the governance authority.

D. Governance layer

Once the data into the blockchain network is secured, different authorities, such as hospitals, laboratories, research organizations, and government authorities, use the normal medical data for further analysis. The private sector, governments, and civil society acting in their respective roles define and implement shared principles, rules, regulations, decision-making processes, and programs that affect the development and use of medical IoT data.

E. Communication layer

The working aforementioned layers are comprised of the communication layer. For example, from the sensor layer, the patient's data is stored in the database. The classification of data in the AI layer. Then, the blockchain layer offers secure storage using an IPFS-based mechanism. Moreover, different governance authorities used patients' personal and sensitive information to offer better medical care and further research. All these layers communicate with each other using the fifth-generation (5G) interface. Hence, there is a need for this layer to share data from one layer to the other layer efficiently.

III. Results and Discussions

This section represents the performance analysis of the proposed approach for secure medical IoT data. A detailed discussion of the results are as follows.

A. Experimental Setup

The proposed approach works in two phases; the first phase consists of classifying the medical IoT data as attack or normal. And the second phase is the security part, where the blockchain network is implemented. Firstly, the classification is performed on Jupyter Notebook (with version v7. 0.0), a Python-integrated development environment (IDE). Here, different libraries are used, such as Pandas (2.0.3), Numpy (1.25.1), Matplotlib (3.7.2), imbalanced-learn, Sklearn, etc., for data preprocessing, data balancing, and classification. Specifically, pandas is used to data cleaning and managing the dataset, Numpy is utilized for data manipulation and numerical computations, and Matplotlib for data visualization. Once the data is classified in attack (1) and normal (0) classes, the next step is securing normal data in the blockchain network. The blockchain network is implemented on Remix IDE (web 3.0 version 1.5.2), which is an online platform that uses solidity programming to develop smart contracts. Here, smart contracts are created with functions, such as addDevice(), removeDevice(), updateDeviceIpAddress(), and getDevice for secure medical IoT data storage. For that a solidity compiler is used with version v0.8.7+commit.e28d00a7 to compile the smart contract. Further, it is deployed on a test network, i.e., Sepolia test network using a MetaMask wallet.

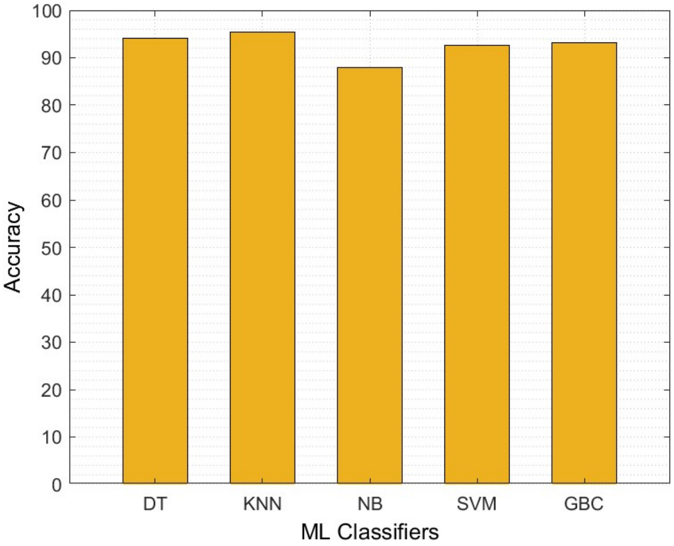


Fig. 2: Accuracy of ML classifiers.

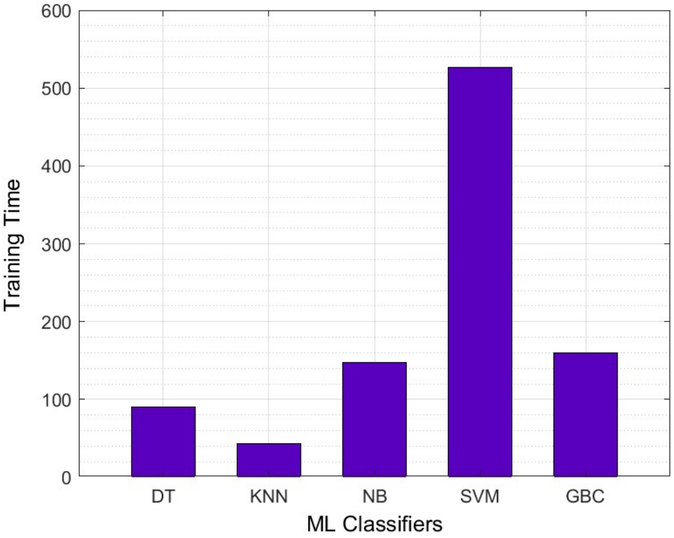


Fig. 3: Training time of ML classifiers

B. Result analysis

This section discusses the results of the proposed scheme forsecuring medical IoT data, which consists patient's personal

Authorized licensed use limited to: Khulna Univ of Engineering & Technology - KUET. Downloaded on February 21,2024 at 16:14:59 UTC from IEEE Xplore. Restrictions apply.

information. This subsection discusses AI and blockchain-based results that offer medical IoT data classification and secure storage, respectively.

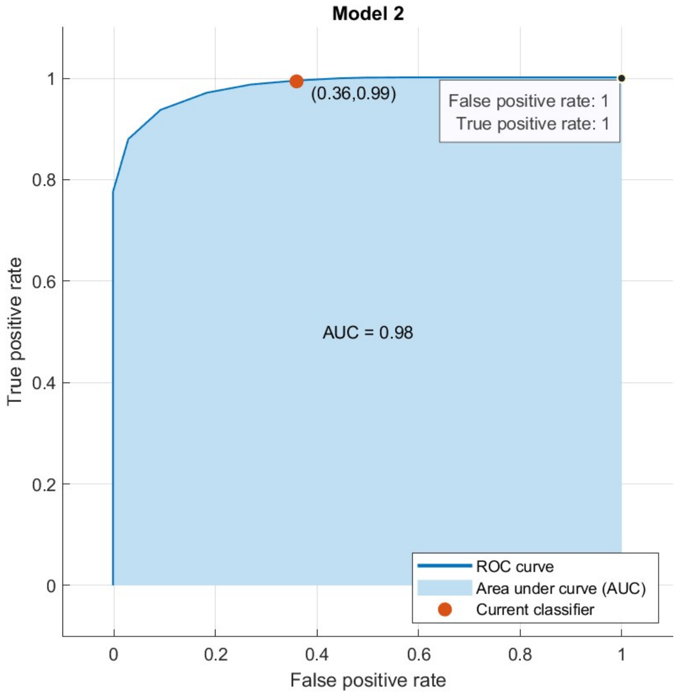


Fig. 4: ROC curve for KNN classifier

1) AI-based results: The AI layer works for the data pre-processing, splitting, balancing, and classification. Here, various performance evaluation metrics are considered for the proposed architecture, such as accuracy, precision, recall, F1-score, training time, and ROC curve. Here, Table I shows the comparative analysis of the different ML classifier's based on different performance evaluation metrics, such as accuracy, precision, recall, and F1-score. Then, Fig.2 represents the accuracy of the proposed ML classifiers, such as DT, KNN, NB, SVM, and GBC. It calculates what portion of the model's predictions were accurate. The result graphs conclude that the KNN achieves the best accuracy for medical IoT data. It achieves the highest accuracy at 95.4% and performs best compared to other ML classifiers, such as DT, NB, SVM, and GBC. This is because KNN can handle feature interactions naturally without having to define them and also offer non-linear relationships between target variables and features. Moreover, it makes predictions based on the training example's proximity. It works well when the data shows local patterns. In contrast, DT and SVM are used to generate global models; they perform worse than KNN for medical IoT data.

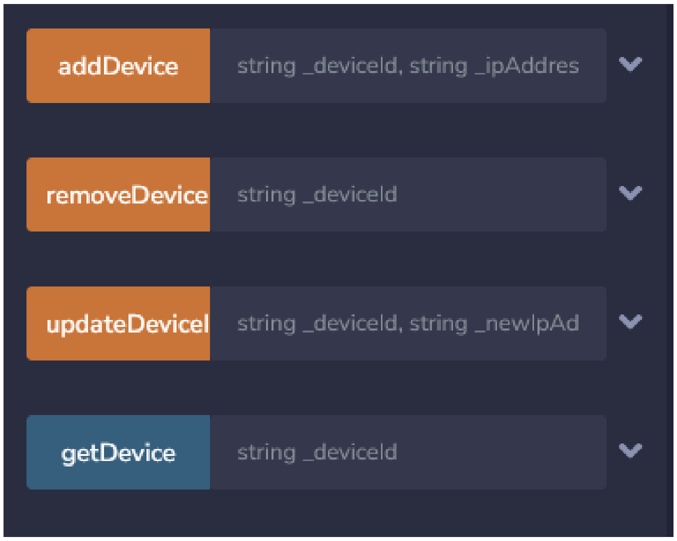
Fig.3 shows training time comparison for the different ML classifiers. From the graph, it seems that KNN takes minimum time to train the data compare to other classifiers because it stores the training data in memory. Further, it follows instance-based learning without any explicit training. In contrast, SVM takes the maximum to train the data because, for large datasets, it is computationally expensive. Then, Fig.4 represents the ROC curve of the KNN classifier. It shows the area under the curve (AUC) value, which means that the AUC value lies between 0 to 1. If the value of AUC is higher, it shows the best classifier.

TABLE I: A comparative analysis of ML classifiers performance for different metrics

Model	Accuracy	Precision	Recall	F1-score
DT	94.13	93.81	94.03	93.67
KNN	95.4	94.4	94.1	95.6
NB	87.9	86.8	88.1	87.63
SVM	92.7	90.8	91.9	92.34
GBC	93.1	92.9	92.8	95.7

C. Blockchain-based results

This section presents the performance analysis of the blockchain-based smart contract that validates the incoming data from the AI layer. Fig. 5 shows different user-defined functions of smart contract that explicitly manages the incoming data from the AI layer. For example, addDevice() allows the owner to add a new device to the network by providing the device ID, IP address, and device type. Similarly, removeDevice() enables the owner to remove a device from the network. updateDeviceIpAddress() allows the owner to update the IP address of an IoT device, and getDevice() retrieves the details of a device based on its ID. Fig. 6 shows the comparison of transaction and execution cost, which is applied when any smart contract is deployed on the test network. It refers to the amount of computational resources (gas) required to execute a transaction on the Ethereum blockchain. The Remix development environment has an in-built gas consumption feature from where the transaction and execution cost is calculated. The x-axis represents different user-defined functions of the smart contract. Fig. 7 shows the bandwidth utilization of the IPFS utilized in the blockchain


addDevice string _deviceId, string _ipAddres

removeDevice string _deviceId

updateDeviceI string _deviceId, string _newIpAd

getDevice string _deviceId

Fig. 5: Smart contract functions.

Authorized licensed use limited to: Khulna Univ of Engineering & Technology - KUET. Downloaded on February 21,2024 at 16:14:59 UTC from IEEE Xplore. Restrictions apply.

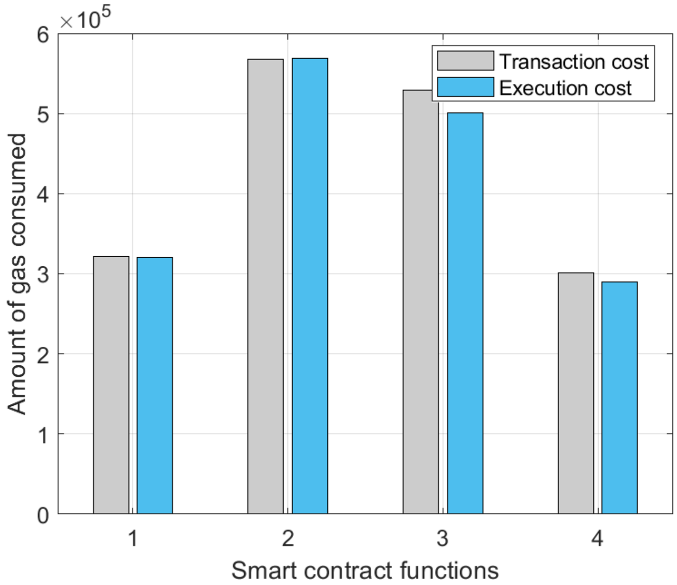


Fig. 6: Amount of gas consumed while deploying the smart contract.

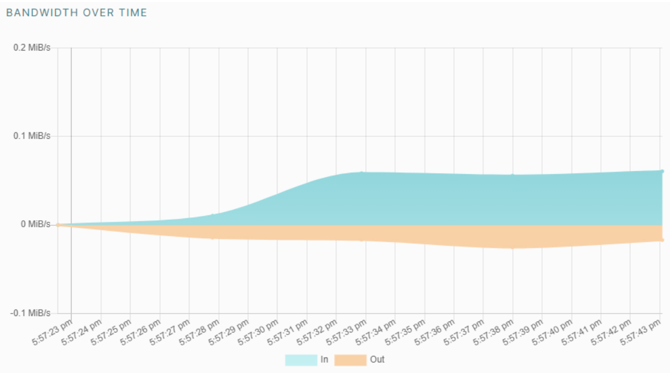


Fig. 7: Bandwidth utilization of IPFS

network. The proposed work utilized IPFS that act as on-site storage for IoMT data, where for each data block a hash is calculated. Further, the hash is forwarded to the blockchain network. Since blockchain only stores the hash of IoMT data, it improves the response time of the blockchain network. The higher the response time, the higher the number of blockchain participants can be involved.

IV. Conclusion

IoT leverages the power of connected gadgets, sensors, and data analytics in healthcare to enhance patient care and treatment. This paper proposed an AI-enabled scheme incorporating an IPFS-based blockchain network that offers security to medical IoT data. In this study, different ML classifiers, such as DT, KNN, NB, SVM, and GBC, are employed to classify healthcare data into attack and normal classes. Subsequently, we utilized an IPFS-based blockchain network that provides transparency, authentication, confidentiality, and privacy to the medical IoT data. Furthermore, various performance evaluation metrics have been considered, including accuracy, training time, ROC curve, and scalability. In this context, KNN achieves the highest accuracy, 95.4%, compared to other ML classifiers.

In future work, we will enhance the performance of the proposed framework by replacing the public blockchain with a private blockchain i.e. hyperledger fabric that creates permissioned blockchain infrastructure to confront and manage modern security vulnerabilities in the healthcare sector.

References

[1] S. Zaman, K. Alhazmi, M. A. Aseeri, M. R. Ahmed, R. T. Khan, M. S. Kaiser, and M. Mahmud, "Security Threats and Artificial Intelligence Based Countermeasures for Internet of Things Networks: A Comprehensive Survey," *IEEE Access*, vol. 9, pp. 94668–94690, 2021.

[2] S. K. Jagatheesaperumal, P. Mishra, N. Moustafa, and R. Chauhan, "A holistic survey on the use of emerging technologies to provision secure healthcare solutions," *Computers and Electrical Engineering*, vol. 99, p. 107691, 2022.

[3] N. Taimoor and S. Rehman, "Reliable and Resilient AI and IoT-Based Personalised Healthcare Services: A Survey," *IEEE Access*, vol. 10, pp. 535–563, 2022.

[4] I. Keshta, "AI-driven IoT for smart health care: Security and privacy issues," *Informatics in Medicine Unlocked*, vol. 30, p. 100903, 2022.

[5] F. Alshehri and G. Muhammad, "A Comprehensive Survey of the Internet of Things (IoT) and AI-Based Smart Healthcare," *IEEE Access*, vol. 9, pp. 3660–3678, 2021.

[6] T. A. Hailu, G. Viajiprabhu, A. S. Endris, and N. Arappali, "Artificial Intelligence based Network Security System to Predict the Possible Threats in Healthcare Data," in *2022 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS)*, pp. 1191–1197, 2022.

[7] R. Gupta, N. K. Jadav, H. Mankodiya, M. D. Alshehri, S. Tanwar, and R. Sharma, "Blockchain and Onion-Routing-Based Secure Message Exchange System for Edge-Enabled IIoT," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 2, pp. 1965–1976, 2023.

[8] M. Sills, P. Ranade, and S. Mittal, "Cybersecurity Threat Intelligence Augmentation and Embedding Improvement - A Healthcare Usecase," in *2020 IEEE International Conference on Intelligence and Security Informatics (ISI)*, pp. 1–6, 2020.

[9] J. I. Khan, J. Khan, F. Ali, F. Ullah, J. Bacha, and S. Lee, "Artificial Intelligence and Internet of Things (AI-IoT) Technologies in Response to COVID-19 Pandemic: A Systematic Review," *IEEE Access*, vol. 10, pp. 62613–62660, 2022.

[10] D. Jadav, M. S. Obaidiat, S. Tanwar, R. Gupta, and K.-F. Hsiao, "Amalgamation of Blockchain and AI to Classify Malicious Behavior of Autonomous Vehicles," in *2021 International Conference on Computer, Information and Telecommunication Systems (CITS)*, pp. 1–5, 2021.

[11] Z. Zhang, H. A. Hamadi, E. Damiani, C. Y. Yeun, and F. Taher, "Explainable Artificial Intelligence Applications in Cyber Security: State-of-the-Art in Research," *IEEE Access*, vol. 10, pp. 93104–93139, 2022.

[12] N. K. Jadav, A. R. Nair, R. Gupta, S. Tanwar, Y. Lakys, and R. Sharma, "AI-driven network softwarization scheme for efficient message exchange in IoT environment beyond 5G," *International Journal of Communication Systems*, vol. n/a, no. n/a, p. e5336.

[13] J. K. Sandhu, A. Kaur, and C. Kaushal, "A Review of Breast Cancer Detection Using the Internet of Things and Machine Learning," in *2023 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE)*, pp. 145–150, 2023.

[14] A. Rhbech, H. Lotfi, A. Bajit, A. Barodi, S. El Aidi, and A. Tamtaoui, "An Optimized And Intelligent Security-Based Message Queuing Protocol S-MQTT Applied to Medical IOT COVID-19 DATA Monitoring Platforms," in *2020 International Symposium on Advanced Electrical and Communication Technologies (ISAECT)*, pp. 1–6, 2020.

[15] A. O. Khadidos, S. Shitharth, A. O. Khadidos, K. Sangeetha, and K. H. Alyoubi, "Healthcare data security using IoT sensors based on random hashing mechanism," *Journal of Sensors*, vol. 2022, pp. 1–17, 2022.

[16] K. S. Sankaran, T.-H. Kim, and P.N.Renjith, "An Improved AI based Secure M-Trust Privacy Protocol for Medical Internet of Things in Smart Healthcare System," *IEEE Internet of Things Journal*, pp. 1–1, 2023.

Authorized licensed use limited to: Khulna Univ of Engineering & Technology - KUET. Downloaded on February 21,2024 at 16:14:59 UTC from IEEE Xplore. Restrictions apply.