IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

The Framework of Privacy-Preserving Diabetes Prediction using Blockchain

Niharika Patel
Department of Computer Science and Engineering
Odisha University of Technology and Research
Bhubaneswar, Odisha, India

Manoranajan Panda
Department of Computer Science and Engineering
Odisha University of Technology and Research
Bhubaneswar, Odisha, India

Abstract: The blockchain is now finding practical applications in industries such as healthcare because of its inherent characteristics, including a distributed ledger, decentralized storage, authentication, privacy, and immutability**.** A strong legal framework often imposes high levels of authentication, interoperability, and data sharing for blockchain applications in the healthcare sector. Blockchain has made advances into a multitude of industries, including business, government, online voting, and healthcare, to name a few. One of the most popular and significant sectors is healthcare, which consists of an electronic health record (EHR) system and a control system. Globally, the mortality rate for diabetes is increasing, making it one of the fastest growing chronic illnesses. Using the Blockchain platform, a system for monitoring diabetic disease using machine learning algorithms can be developed that will provide early diagnosis of diabetes as well as protect patient electronic health records. Our EHRs sharing infrastructure integrates symptom-based illness prediction, Blockchain, and the interplanetary file system (IPFS) with patient health data gathered via wearable sensor devices. Once the data is acquired, an ML unit is used by the EHR manager to generate the required results. With the patient's and practitioner's approval, the findings, as well as the healthcare data are stored on the Blockchain. The healthcare industry should benefit from our proposed system in terms of storing, processing, and securely exchanging patient health information.

Keywords: *Blockchain, Secure systems, Healthcare, Diabetes disease, Classification algorithms.*

1. Introduction

The blockchain foundation is a data chain that works by keeping data in distributed recording ledgers that are scattered astride all computing systems. Using a peer-to-peer or shared network, the framework combines network clients (who participate in transactions) with blockchain excavators (which participate in exchanges). The ledger is kept in a decentralized network of hubs established by all network excavators or miners using cryptographic method. A control system and electronic health records (EHRs) are at the heart of the Internet of Things (IoT) and other sophisticated technologies in healthcare. Control systems aid in the implementation of control measures, whereas electronic health records (EHRs) are crucial in making medical care more accessible, affordable, and timely. With smart healthcare systems, patients' biomedical characteristics, i.e. pulse rate, sugar level, electroencephalograms (EEG), electrocardiograms (RCG), and other critical biomedical signals, as it may be

monitored and determined [1, 2]. EHR delivers the most comprehensive and valuable information for diagnosing and detecting numerous diseases, as well as a single form of medical decision-making. Because of the fore mentioned qualities of IoT in healthcare, it is becoming increasingly popular.

Chronic diseases, like diabetes, stroke, and Alzheimer's disease, are long-term illnesses with no treatment. Diabetes is one of the most frequent and quickly growing serious illnesses, with a rising death rate, particularly among women, across the world. Having diabetes is a result of being unable to produce enough insulin by the pancreas or not having the body utilize insulin properly. Early and effective diagnosis and treatment of diabetes in its early stages may assist to reduce the disease's mortality rate and save patients' lives [3, 4]. Machine Learning (ML), Deep Learning (DL), and Cloud-Assisted technologies have all risen in popularity in recent years as intelligent approaches to diabetes diagnosis and prevention.

Scalability, security, adaptability, and availability are key issues that Machine Learning (ML) and Deep Learning (DL) face. Previously, different cloud-based healthcare data sharing technologies [5] were utilized to accomplish this goal, with operation depersonalization and data encryption offering flexibility, scalability, security, and cost data. Consumers, on the other hand, are wary of entrusting their personal information to the cloud because of its sensitivity and privacy concerns. To overcome the inadequacies of the previous methodologies, a secure and interoperable system, as well as the creation of an efficient and scalable architecture that addresses all of the aforementioned problems, is required. The blockchain is a distributed ledger that uses smart contracts to keep documents immutable [6-9].

The main motive of this research is to construct a Blockchain-enabled data sharing system for healthcare that comprises three phases:

a) Registration phase
b) Authentication phase
c) Communication with Blockchain. Phase

With the help of machine learning classifiers, we propose a model that can predict and diagnose diabetic patients' health states, including whether they are diabetics. Numerous performance assessment measures are used to evaluate the prediction models' performance and efficiency, including accuracy, sensitivity, and precision, as well as the f1-measure and the ROC curve. Physicians should be able to appropriately recognize diabetic patients and safeguard their health using the suggested technology.

2. Related Work

For stakeholders in the healthcare system, blockchain has far-reaching implications. We looked at a variety of current experiments, medical services-related applications, methodologies, and software solutions in our research.

The first company to use Ethereum Blockchain Technology was Gem Health Network (Metler et al, 2016). It allows medical professionals to access data from similar medical providers without relying on centralized storage. It helps to reduce the risk of clinical negligence caused by outdated data and to avoid medical complications caused by misinformation. Patient identity management is a restriction, presuming that any form of key management is in place to prevent data from being tampered with or abused [10].

The OmniPHR Model (Rohers et al, 2017) focused on PHR interoperability and P2P network interoperability. PHR would be stored and coordinated in a hierarchical fashion, similar to how networked information blocks are delivered. Patients may access information from anywhere, providers can separate the devices that supply data for the PHR, and clients can use a device that reads the data from the PHR. This is a limitation since the information needed to enforce the requirements would not be supplied. Another issue is that the patient must grant authorization for anybody else to view the data, and OmniPHR does not handle key management or recovery [11].

Using blockchain technology, MedRec Model (Azaria et al, 2016) is a decentralized record management system for healthcare records. This solution improves record sharing interoperability by allowing patients and providers to exchange data without depending on a weak link. It also addressed data mining incentives, which had been a major concern in the implementation of a medically designed blockchain. The framework seeks to handle identification in the same way as DNS does. The model's flaw is that it focuses solely on digital rights management rather than tackling database security. Due to concerns and the blockchain foundation's pseudo-unknown nature, information forensics can be used to discover the patient-provider link. It's also having trouble growing the system to handle high transaction volumes [12].

The PSN Network (Zhang et al, 2016) is a sensor and mobile computer network that uses wireless technology. It aims to keep the computational load on the BP screen as low as possible and avoids overloading the PSN nodes with data. It protects data from being leaked by a malicious third party. The framework's flaw is that it ignores the issue of blockchain key management that arises when a key is lost [13].

In addition to multi-tenancy support, the Virtual Resource Concept's final option was to change load distribution among edge hosts to the edge hosts (Samaniego and Deters et al., 2016). It supports the storage of healthcare data in a system while also preserving safe, scalable, and secure permanent information storage. Scalability isn't an issue in this paradigm, and there's no significant replacement capacity [14].

By utilizing nearby devices as witnesses, context-driven information logging (Siddiqui et al., 2017) enables secure data logging from wearable devices while storing fingerprints that may later be used for forensic investigations. It aids in the preservation of healthcare data and ensures data monitoring accuracy. Due to the lack of key replacement procedures and intrinsic security features such as encryption, security is neglected here [15].

Smart contracts and access control measures were the emphasis of the MeDshare Model (Xia et al, 2017). When it detects a breach in the framework, it captures information and restricts access to any hostile entity. Cloud experts and other components that hold sensitive clinical data can perform data provenance and review as well as exchange medical data with medical community organizations without compromising patient privacy. The framework's fundamental problem was that with the rise in requests, the latency increased. Another source of worry is a lack of necessary management and recovery [16].

The Clinical Trial and Precision Medicine (Shae and Tsai, 2017) platform was developed as a blockchain-based stage framework for the purposes of improving the transparency and quality of clinical preliminary data analysis. Another benefit of the blockchain is that it allows for peer-verified clinical preliminary results without allowing data owners to lose ownership of their data. As a result, this method would be able to provide medical data with more integrity and security by implementing blockchain architecture between inputs and outputs. [17].

Healthcare Data Gateway (Yue et al, 2017) is a database management framework, an access-based data query framework, and a data management function that emphasizes security affirmation, depersonalization, transmission for data requests, and data backup and recovery, it helps patients better own, control, and transfer their data. While HDG intends to enable safe data transfer, it fails to handle the issue of giving emergency access to user data. A misplaced key is also unreplaceable [18].

The algorithms used to diagnose breast cancer were investigated (Shler Farhad Khorshid & Adnan Mohsin Abdulazeez, 2021). The K-NN algorithm was used to identify breast cancer in PJAEE, 18 (4) (2021) 1944. Each method used a different categorization strategy, and the bulk of the datasets used in the investigations were unique. To summarize, K-NN implementation is rather simple. K-NN provided the most accurate forecast (99.12 %) [19].

To diagnose Cardio Vascular Disease, the proposed model (N. Komal Kumar et al, 2020) employs a variety of Machine Learning classification algorithms, including random forest, decision tree, logistic regression, SVM, and K.N.N. (CVD). According to the findings, the random forest classifier approach surpasses the other classifier algorithms in terms of accuracy [20].

A machine learning system (J.Neelaveni and Geetha Devasana, 2020) will be used to identify Alzheimer's disease using psychological data such as age, number of visits, MMSE, and education [21].

3. Proposed System Model

The purpose and system model of our proposed framework, Privacy-Preserving Diabetes Prediction Using Blockchain, are described here.

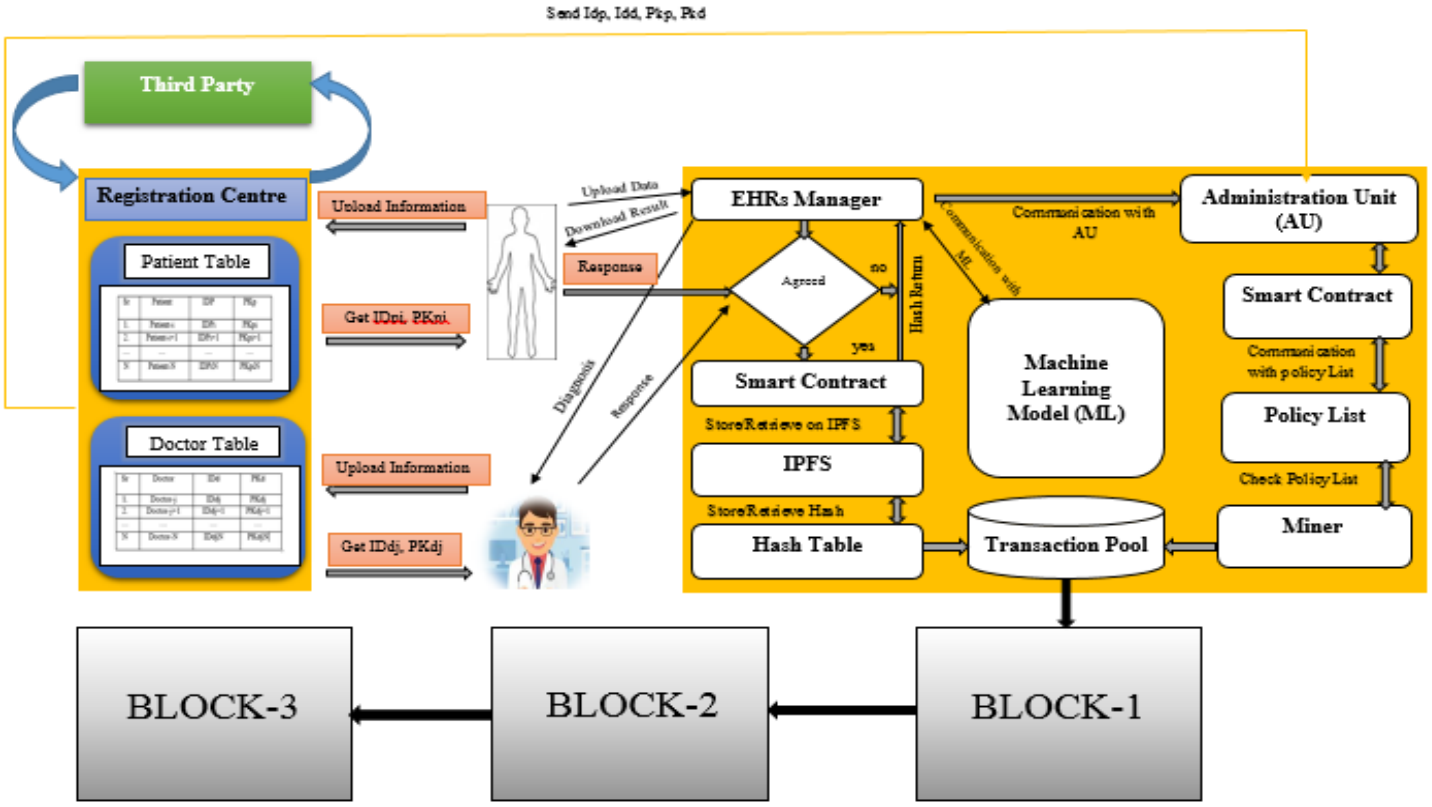

Fig-1: proposed framework of blockchain enabled diabetes prediction

3.1 Proposed system model

Figure 1 illustrates the proposed framework of Privacy-Preserving Diabetes Prediction Using Blockchain. In order to register, the patient and doctor must first send a request to the Registration Center (RC). Information about patients and doctors is collected by the Registration Center (RC), which assigns a user ID number and private key and same is forwarded to administration unit. Before communicating with the EHRs Manager, this user (patient or doctor) must have the EHRs Manager authorize his or her ID. If the authentication is successful, the user will be able to upload and download data; otherwise, a penalty will apply. As soon as the authorized user has been successfully verified, healthcare data can be uploaded/downloaded, and subsequently stored on Blockchain with the support of both the patient and the doctor. In the subsections that follow, we go into the work of the various components of our proposed framework in great depth.

3.1.1 Registration Centre (RC)

Patients and medical care providers, such as practitioner, give information to the Registration Center (RC), which is maintained in a database in a secure manner. The patient's data contains things like their name, father's name, age, place of residence, and so on, whereas the practitioner's data includes things like their name, qualification, specialism, and contact number. The RC then processes the identities of the worried patient (PID) and doctor using their respective public keys (DID). The RC provides a single id and public key to the specified patient/doctor after a successful computation. When adding/retrieving information from/to the Blockchain, the patient/ID doctor's information is also communicated to the administration unit for authentication. The Registration Center is linked to a Smart Device that captures customer information. Third party is a cloud storage server that backups all of the registration center's data.

3.1.2 Smart Device

There are many smart gadgets out there, such as cell phones, laptops, desktop computers, and sensors. Using the smart device, both patients and doctors can log into the framework. Once they have successfully logged in, the patient gives RC his or her personal information (name, father's name, age, address, etc.) and the practitioner gives RC his or hers (name, qualification, specialization, contact number, etc.). After that, the information was transferred to the Electronic Health Records (EHRs) Manager, who processed it.

3.1.3 Electronic Health Records (EHRs) Manager

Our proposed framework is incomplete without EHR managers, and they play a crucial role in its implementation. It serves as a central controller and may perform a variety of tasks. To create a transaction (patient addresses) or retrieve history from Blockchain, a patient sends a request to the EHRs Manager. The practitioners use a similar procedure. When a patient or practitioner files a request, the EHR's administration requests the requester's public key. Following the distribution of the public key, it is submitted to the administrative unit for verification. By using the public key, Blockchain is able to determine if the requester has permission to upload and retrieve data. In order to validate the public key of the requester, the administration unit uses a smart contract from the policy list. By using the EHR Manager's public key, an encrypted transaction is sent to Interplanetary File Framework (IPFS), a cloud storage server, which connects to the Blockchain network. It incorporates a Smart Contract (SC), which distributes resources, such as money, stock, and property in a transparent, conflict-free manner without the need of an intermediary.

3.1.4 Smart Contract (SC)

Smart Contracts (also called Crypto Contracts) are computer programs that administer and validate the exchange of digital assets between parties. A smart contract is similar to a standard contract in the sense that it executes the contract. These are the programs that perform exactly as their creators intended (coded, changed). A traditional contract is enforceable by law as well, but smart contracts are enforced by code. The EHRs Manager and Administration Unit are linked by the Smart Contract.

3.1.5 Administration Unit (AU)

An ID and public key of the patient and doctor are assigned to this region by the RC. All cloud transactions and activities are controlled by the Administration Unit, which grants or revokes authorized access. The administration unit checks the requester's access credentials when a new transaction is received from the EHRs manager with the user public key. An access authorization is awarded to the requester once the public key is validated in the smart contract's policy list, otherwise, a penalty is imposed, and all EHR administration activities are refused. As soon as the Administration Unit sends a message to the EHR Manager authorizing users, the EHR Manager sends IoT data from the Smart Device to the Machine Learning (ML) Unit for diagnosis, allowing the unit to diagnose the condition.

3.1.6 Machine Learning Unit

Our suggested framework's machine learning unit is a critical component. The purpose of the machine learning unit is to collect health related data from EHRs Manager, which is given by smart devices such sensors nodes. The diabetic illness datasets are used to train by machine learning unit. After the dataset has been trained, and submitted to ML unit, and it may then forecast a patient's health difficulties and whether or not he or she has diabetic condition. We employed five machine learning (ML) classification methods in this research: DT, KNN, RF, LR, and SVM. Accuracy, sensitivity, precision, recall, and ROC curves are among the performance metrics used to demonstrate classification models. As soon as patient and practitioner agree to send their records to Blockchain, the EHR Manager receives diagnosis reports from the ML unit and tranters them to the Interplanetary File System.

3.1.7 Interplanetary File System (IPFS)

A cloud storage server, IPFS, provides the EHR Manager with a hash of a document or transaction submitted. In order to maintain the hash table up to current, it additionally records the created hash. All storage nodes are assumed to be IPFS-based in this study, with the IPFS framework being developed and maintained by a consortium of healthcare providers, such as hospitals. As with getting the address from the content of the record, it employs a similar approach. A unique hash string is created for each file to identify the record. A Blockchain record's hash string may be used to find the whole document stored in IPFS.IPFS enables the delivery of large volumes of data in a cost-effective manner. When a new transaction occurs, the EHRs manager evaluates it first from the administrative unit under the policy list, according to our proposed structure. The transaction must be stored in the cloud after it has been verified. Prior to storage, an automatically generated hash is established and kept in a hash table. The next safe transaction is received by the transaction pool, which is a collection of transactions. 1) a transaction that adds to the Blockchain, and 2) a transaction that is removed from the Blockchain. This is also where the newly mined transaction is maintained and may be transmitted to a specific requester. The determined hash can then be mined or assigned to the Blockchain by exporting it from the transaction pool. The hash of the endorsed transaction is then calculated and preserved for future use in the hash database.

3.1.8 Hash Table

Before a transaction is posted to the Blockchain network, the hash table is used to keep track of its hash. When patients and practitioners agree to connect a transaction to the Blockchain under our proposed architecture, they sign a document that confirms that the transaction will be available for future use if needed. As soon as the transaction is endorsed, it is moved from the hash table to the Transaction Pool for recording on the Blockchain.

3.1.9 Transaction Pool

This pool stores all transactions that are added to/removed from the Blockchain. In the transaction pool, there are two categories of transactions: truncations that should be kept on Blockchain and recoverable transactions. Under our proposed method, the miner is in charge of encoding the transaction in a block, which is subsequently verified before being added to the Blockchain network.

3.2 ML Algorithm Classifier

As part of our proposed system, three actions are included: registration for users, authentication for users, and submission of diabetic data.

Table-1

A description of Symbols and their meanings.

Symbols	Meaning
DT	Decision Tree
SVM	Support Vector Machines
RF	Random Forest
LR	Logistic Regression
KNN	K-Nearest Neighbor

i) Decision Tree (DT)

It is built in a manner like a flowchart. A test on an attribute is shown by each internal node. Each branch represents a test result. A class prediction is indicated by each external node. It is presumed that all qualities are irrelevant if they do not appear in the tree. The collection of attributes that show as a reduced subset in the tree form. It is a very specific type of probability tree that enables you to make a decision about some kind of process.

ii) Support Vector Machine (SVM)

The Support Vector Machine (SVM) is a method used for classification and regression in Supervised Machine Learning. Although it is occasionally quite helpful for regression, classification is where it excels. In essence, SVM identifies a hyper-plane that establishes a distinction between the various types of data. In essence, it consists of methods for outlier detection, regression, and classification. A high-dimensional feature space presents the challenge of employing linear functions, so SVM and support vector regression turn the optimization problem into dual convex quadratic programs.

iii) Random Forest (RF)

Leo Bierman and Adele Cutler, the inventors of the widely used machine learning technique known as random forest, combined the output of various decision trees to get a single outcome. Its widespread use is motivated by its adaptability and usability because it can solve classification and regression issues. Supervised Machine Learning is used for Classification and Regression problems. It creates decision trees from various samples, using their average in the case of regression and majority vote for classification.

iv) Logistic Regression (LR)

In statistical analysis, it is a method to predict a binary outcome i.e. yes or no based on previous observations of a dataset. Using a logistic regression model, a dependent data variable can be predicted by considering the correlation between one or more independent variables. In order to predict the categorical dependent variable, it is used in conjunction with a predetermined set of independent factors. A categorical dependent variable's output is predicted by logistic regression.

v) K-Nearest Neighbor (KNN)

A supervised learning algorithm known as k-nearest neighbor (KNN) uses proximity as a basis for classifying or predicting data points based on their proximity. Although it can be applied to classification or regression issues, it is commonly employed as a classification algorithm. Because it relies on the idea that similar points can be discovered close to one another. KNN is a run-time-only computing model for lazy learning. K value and distance function are two hyper parameters.

4. Simulation of ML classification models

This section displays the results of several machine learning classification approaches on a diabetic illness dataset that was gathered by the author. Five machine learning algorithms were investigated: KNN, DT, RF, LR, and SVM. Before using classification methods to normalize and delete missing values, the dataset is subjected to a variety of preprocessing techniques. The performance of classification models is measured using a variety of performance assessment criteria. Python is a programming language that is used for experimentation and implementation. In the simulation part, Table-1 presents the Symbols and their meanings:

4.1 Performance evaluation of Classifier

This subsection uses the diabetic diabetes dataset to explain the experimental findings and performance of all five classification methods. The performance of all of the studied categorization models is shown in Table 2.

As shown in Table 3, KNN performs better in terms of performance evaluation metrics than all other classification models. KNN obtained 99.03 % classification accuracy, 98.43 % sensitivity, 1.0% precision, as well as 99.20 % AUC, 99.21 F1-Score, and 99.21 ROC. Diabetic testing with sensitivity indicates that a person has diabetes based on the results of that test. Conversely, specificity indicates that the person is healthy and that the diagnostic result was negative. LR performed well, with accuracy of 97.11%, sensitivity of 96.87 %, precision of 98.41 %, AUC of 99.1 %, F1 -score of 97.63, and ROC of 97.18. In comparison to the other classification algorithms, KNN came in last. Using ranges 1 to 35, we completed manytrials for the KNN classifier. Table 3 shows that KNN achieved good results at k=1. In comparison to other classification algorithms, SVM and RF fared equally well in terms of classification accuracy of 98.07 %, 96.87% sensitivity, 1.0% precision, and 98.41 f1 score, and 1.00 AUC, and ROC of 98.43. When compared to the other classification models, DT performed the worst, with an accuracy of 97.11%, 95.31% sensitivity, 1.0% precision, 97.7% AUC, 97.6 F1-Score, and a ROC of 97.65. Figure 4 Figure 5 depicts the results of all five classification models on datasets obtained by the author. In terms of all performance criteria, KNN had the greatest resulting value, while DT had the lowest.

The results of the five classification models on the obtained datasets are shown in Figures 2 and 3. The highest resulting value was 99.03 percent for KNN (K=1), whereas DT had the lowest performance across all performance criteria.

Table-2

Based on own collected dataset, performance of all 5 ML Classification algorithms was evaluated.

Classification Model	Accuracy	Sensitivity	Precision	F1-Score	ROC
Logistic Regression	97.11	96.87	98.41	97.63	97.18
Random Forest	98.07	96.87	1.0	98.41	98.43
Decision Tree	97.11	95.31	1.0	97.60	97.65
K-Nearest Neighbors	99.03	98.43	1.0	99.21	99.21
Support Vector Machine	98.07	96.87	1.0	98.41	98.43

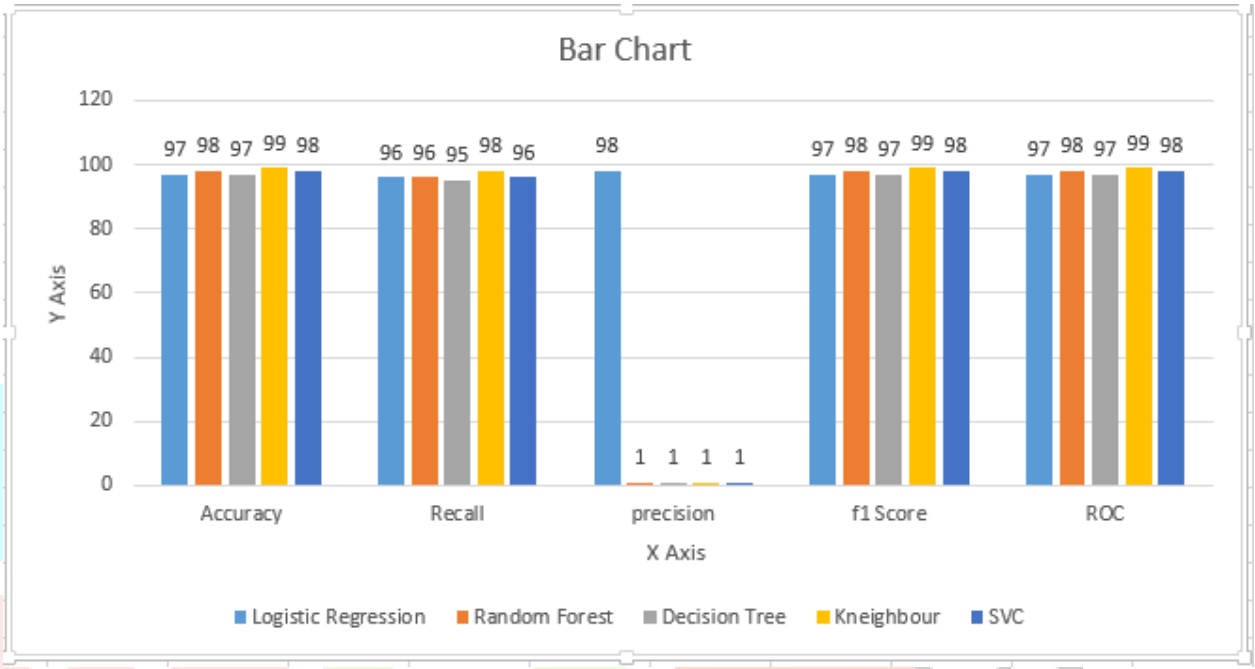

Fig-2: performance analysis of ml classifier

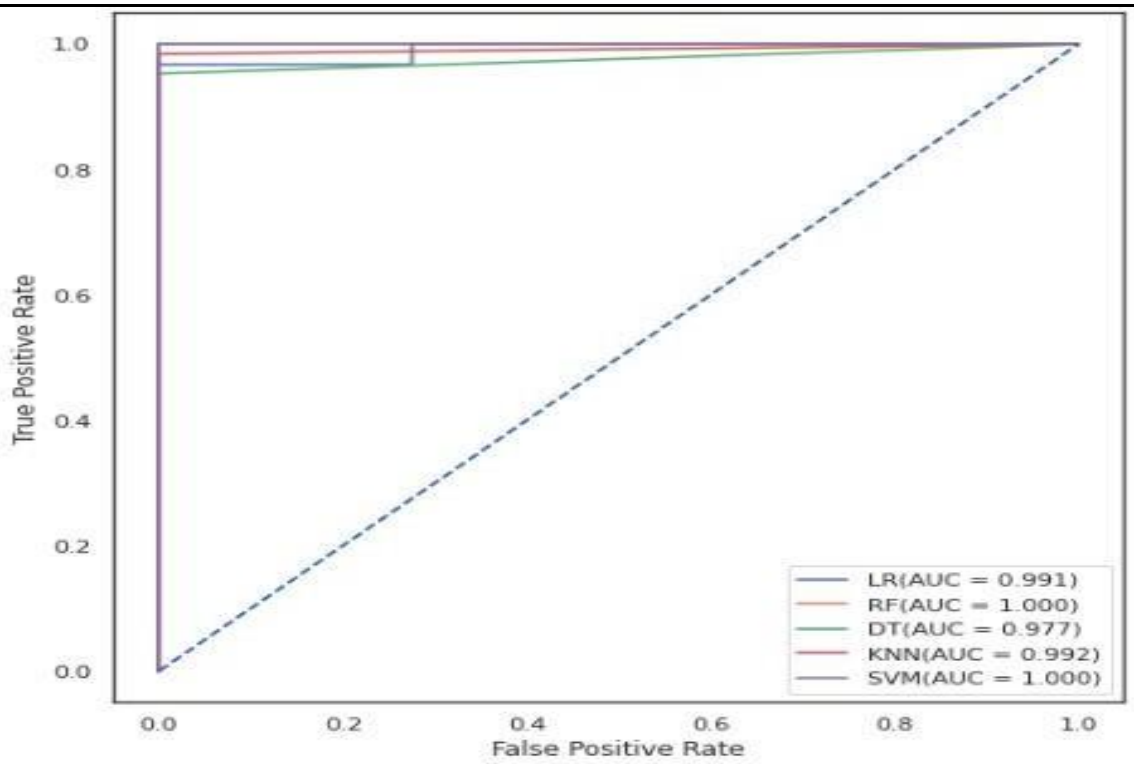

Fig-3: auc-roc curve of ml classifier

5. Conclusion and Future work

With this paper, we present a paradigm for privacy-preserving diabetes prediction that utilizes Blockchain technology, which involves three phases: registering users, establishing user authentication, and sending data to IoT devices using Blockchain technology. During the initial step of our suggested solution, the user must complete the registration procedure before communicating with a Blockchain network. Using an authentication unit from EHR Manager, the user validates his or her identity. Machine learning algorithms were demonstrated for detecting diabetes in a patient and securely sharing the information with a healthcare expert. We also double-checked that our suggested technique can fulfil the privacy, integrity, and authentication criteria. Additionally, we are planning a hypothetical smart contract arrangement for this healthcare system. According to the security analysis, our suggested system can match our projected security needs. A performance study of our proposed Blockchain network shows that it is well-organized and practical.

We wish to undertake further research into innovative Machine Learning Techniques for sickness identification in order to improve our performance. Using lightweight Blockchain technology in other industries is not limited to healthcare, such as transportation, gaming, voting, government systems and education. Furthermore, we seek to create a comprehensive Blockchain-based defense against Blockchain attacks.

References

[1] Lo'ai AT, Mehmood R, Benkhlifa E, Song H. Mobile cloud computing model and big data analysis for healthcare applications. IEEE Access 2016;4:6171–80.

[2] Xia Q, Sifah EB, Asamoah KO, Gao J, Du X, Guizani M. MeDShare: Trust-less medical data sharing among cloud serviceproviders via Blockchain. IEEE Access 2017;5:14757–67.

[3] Kadobera D, Sartorius B, Masanja H, Mathew A, Waiswa P. The effect of distance to formal health facility on childhood mortality in rural Tanzania, 2005–2007. Global Health Action 2012;5:19099.

[4] Krumkamp R, Sarpong N, Kreuels B, Ehlkes L, Loag W, Schwarz NG, Zeeb H, Adu- Sarkodie Y, May J. Health care utilization and symptom severity in Ghanaian children–a cross-sectional study. PLoS One 2013;8.

[5] Liu X, Wang Z, Jin C, Li F, Li G. A Blockchain-Based Medical Data Sharing and Protection Scheme. IEEE Access 2019;7:118943–53.

[6] Liu XLi, Ye L, Zhang H, Du X, Guizani M. BPDS: A Blockchain based privacy-preserving data sharing for electronic medical records. 2018 IEEE Global Commun Conf (GLOBECOM) 2018:1–6.

[7] Gupta R, Tanwar S, Tyagi S, Kumar N, Obaidat MS, Sadoun B. Habits: Blockchain-based telesurgery framework for healthcare 4.0. Int Conf Comput Inf Telecommun Syst (CITS) 2019:1–5.

[8] Guo H, Li W, Nejad M, Shen C-C. Access control for electronic health records with hybrid Blockchain-edge architecture. 2019 IEEE Int Conf Blockchain (Blockchain) 2019:44–51.

[9] Franke KH, Krumkamp R, Mohammed A, Sarpong N, Owusu-Dabo E, Brinkel J, Fobil JN, Marinovic AB, Asihene P, Boots M. A mobile phone based tool to identify symptoms of common childhood diseases in Ghana: development and evaluation of the integrated clinical algorithm in a cross-sectional study. BMC Med Inf Decis Making 2018;18:23.

[10] Mettler, M., 2016. Blockchain technology in healthcare: the revolution starts here. In: e-Health Networking, Applicationsand Services (Healthcom), 2016 IEEE 18th International Conference on. https://doi.org/10.1109/HealthCom.2016.7749510 IEEE.

[11] Roehrs, A., da Costa, C.A., da Rosa Righi, R., 2017. OmniPHR: a distributed architecture model to integrate personalhealth records. J. Biomed. Inf. https://doi.org/10.1016/j.jbi.2017.05.012.

[12] Azaria, A., et al., 2016. Medrec: using blockchain for medical data access and permission management. In: Open and BigData (OBD), International Conference on. https://doi.org/10.1109/OBD.2016.11. IEEE.

[13] Zhang, J., Xue, N., Huang, X., 2016. A secure system for pervasive social network-based healthcare. IEEE Access4,9239–9250.

[14] Samaniego, M., Deters, R., 2016. Hosting virtual IoT resources on edge-hosts with blockchain. In: Computer and Information Technology (CIT), 2016 IEEE International Conference on. https://doi.org/10.1109/CIT.2016.71. IEEE.

[15] Siddiqi, M., All, S.T., Sivaraman, V., 2017. Secure lightweight context-driven data logging for bodyworn sensing devices.In: Digital Forensic and Security (ISDFS), 2017 5th International Symposium on https://doi.org/10.1109/ISDFS.2017.7916500. IEEE.

[16] Xia, Q., et al., 2017. MeDShare: trust-less medical data sharing among cloud service providers via blockchain. IEEEAccess 5, 14757–14767.

[17] Shae, Z., Tsai, J.J., 2017. On the design of a blockchain platform for clinical trial and precision medicine. In: Distributed Computing Systems (ICDCS), 2017 IEEE 37th International Conference on. https://doi.org/10.1109/ICDCS.2017.61. IEEE.

[18] Yue, X., et al., 2016. Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy riskcontrol. J. Med. Syst. 40 (10), 218.

[19] Khorshid, S. F., Abdulazeez, A. M., & Sallow, A. B. (2021). A Comparative Analysis and Predicting for Breast CancerDetection Based on Data Mining Models. *Asian Journal of Research in Computer Science*, *8*(4), 45-59. https://doi.org/10.9734/ajrcos/2021/v8i430209

[20] Kumar, N. Komal, et al. "Analysis and prediction of cardio vascular disease using machine learning classifiers." *2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS)*. IEEE, 2020.

[21] J. Neelaveni and M. S. G. Devasana, "Alzheimer Disease Prediction using Machine Learning Algorithms," 2020 6thInternational Conference on Advanced Computing and Communication Systems (ICACCS), 2020, pp. 101-104, doi: 10.1109/ICACCS48705.2020.9074248.