Journal of Information Security and Applications 58 (2021) 102771

Contents lists available at ScienceDirect

Journal of Information Security and Applications

journal homepage: www.elsevier.com/locate/jisa

Blockchain-Enabled healthcare system for detection of diabetes

Mengji Chen [a], Taj Malook [b], Ateeq Ur Rehman [b,*], Yar Muhammad [b], Mohammad Dahman Alshehri [c], Aamir Akbar [b], Muhammad Bilal [d,*], Muazzam A. Khan [e]

[a] College of Mechanical and Electrical Engineering, Guangxi Science & Technology Normal University, Guangxi, China
[b] Department of Computer Science, Abdul Wali Khan University Mardan, Khyber Pakhtunkhwa, Pakistan
[c] Department of Computer Science, College of Computers and Information Technology, Taif University, P.O. Box 11099, Taif, 21944, Saudi Arabia
[d] Department of Computer Engineering, Hankuk University of Foreign Studies, Yongin-si, Gyeonggi-do, 17035, Korea
[e] Department of Computer Science, Quaid-i-Azam University Islamabad, Pakistan

ARTICLE INFO

Keywords:
Blockchain
Secure systems
Healthcare
Diabetes disease
Classification algorithms

ABSTRACT

Blockchain has penetrated numerous domains such as, industries, government agencies, online voting, and healthcare, etc. Among these domains, healthcare is one of the trending and most important one, which consists of a control system and an Electronic Health Records (EHRs). Diabetes is one of the most rapidly growing chronic diseases that increases the death ratio across the globe. This paper presents a Blockchain-enabled diabetes disease detection framework that provides an earlier detection of this disease by using various machine learning classification algorithms and maintains the EHRs of the patients in a secure manner. Our EHRs sharing framework combines symptom-based disease prediction, Blockchain, and interplanetary file system (IPFS) in which the patient's health information are collected via wearable sensor devices. This information is then sent to EHRs manager, where an ML model is executed for further processing to collect the desired results. The results along with the physiological parameters are then stored in the Blockchain with the approval of concerned patient and his/her practitioner. It is anticipated that our proposed system will help the healthcare society in order to store, process, and share the patient health information in a secure manner.

1. Introduction

The advancement in Information and Communication Technology (ICT) has brought the world into a new era, where all the necessities are just on a single click. These new technologies and control systems play a vital role in every aspect of human life such as agriculture, smart cities, industrial automation, smart home, and healthcare, etc. Among these applications, healthcare is the most important one, which is one of the basic necessities of human life. The application of advance technologies, i.e., Internet of Things (IoT) in Healthcare basically consists of a control system and electronic health records (EHRs). Control system helps in providing the control strategies, while the EHRs performs a significant role in providing easy to use, low-cost, and stronger timeliness for medical services. In smart healthcare systems, patient's biomedical parameters such as pulse rate, sugar level, Electroencephalogram (EEG), Electrocardiograph (RCG), and other indispensable biomedical signs can be checked and diagnosed by implanting tracking and sensing devices to the human body [1,2]. EHR provides the most substantial and useful data for the diagnosing and identification of various disease and also gives one kind of judgment for handling medical disputes. Because of the mentioned characteristics of IoT in healthcare, it has attracted a wide range of attention recently.

Chronic diseases such as diabetes, stroke, and Alzheimer, etc. are persistent diseases which sticks to a person for a long time and have no permanent cure. Among these diseases, diabetes is one of the most common and rapidly increasing fatal diseases which escalate the death ratio specifically in woman all over the world. Diabetes is a genuine, constant infection that happens either when the pancreas does not create enough insulin or when the body cannot adequately utilize the insulin it produces. Early and accurate diagnosis and proper treatment at the initial stages of diabetes can help in the reduction of death ratio caused by this disease and securing the lives of the patients [3,4]. Intelligent techniques such as Machine Learning (ML), Deep Learning (DL) and Cloud-Assisted approaches have recently gained popularity for the detection and prevention of diabetes in recent years.

Machine Learning (ML) and Deep Learning (DL) are facing some

* Corresponding authors.
E-mail addresses: 05064@hcnu.edu.cn (M. Chen), ateeq@awkum.edu.pk (A.U. Rehman), alshehri@tu.edu.sa (M.D. Alshehri), m.bilal@ieee.org (M. Bilal), muazzam.khattak@qau.edu.pk (M.A. Khan).

https://doi.org/10.1016/j.jisa.2021.102771

Available online 7 February 2021

deficiencies in term of scalability, security, flexibility, and availability. For this purpose, some cloud-based healthcare data sharing schemes [5] have been used earlier for providing flexibility, scalability, security, and economic details through operation depersonalization and data encryption. However, due to the patient's data sensitivity and privacy, the users hesitate to transfer their data to the cloud. In order to overcome the problems in the previous approaches there is a need for a secure and interoperable system, and to develop an efficient and scalable architecture that tackles all the issues mentioned above. Blockchain has the ability to circumvent partially or fully, the challenges of security problems faced by the patients and healthcare systems. Blockchain is a distributed ledger where the records are stored immutably with smart contracts [6-9].

Motivated by the recent revolution of Blockchain in various fields, specifically in healthcare, this study aims to develop a Blockchain-enabled data sharing system for healthcare which consists of the following phases:

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

Our proposed system works in a systematic way which will be discussed in detail in Section 3. Furthermore, various machine learning classifiers are used to predict and diagnose the health status of diabetic patients that whether the patient has diabetes disease or not. Finally, the performance and efficiency of the prediction models are comparatively analyzed with the help of various performance evaluation metrics such as accuracy, sensitivity, specificity, precision, f1-measure, Matthew correlation coefficient (MCC) and ROC curve. It is anticipated that the proposed system will assist the physician in the accurate diagnosing of diabetic patients, and the safeguarding of the patient's sensitive data.

The rest of the paper is organized as follow. In Section 2, related work is presented. In Section 3, proposed system design is discussed followed by performance evaluation in Section 4. Finally, the paper is concluded, and future research directions are provided in Section 5.

2. Review of literature

This section presents the related works that are classified into three categories, i.e., traditional smart healthcare system (TSHCS), Blockchain-based network scenarios (BBNS), and Blockchain-based smart healthcare system (BBSHS).

2.1. Traditional Smart Healthcare System (TSHCS)

Today, people are capable to access more reliable, detailed, and efficient medical information about them, while protecting their personal privacy. With the development of Internet technology and cloud computing, a lot of research has been performed to improve the efficiency and safety of smart healthcare systems (SHCS). Protecting personal health information stored at the semi-trusted cloud attribute-based encryption (ABE) servers are implemented to attain a fine-grained access control [10]. M Li et al. [11] have developed a novel fine-grained patient-centered structure using ABE technology, and flexible data access control to encrypt the data of EHRs users. Zhang et al. [12] analyzed and discovered that there is a considerable number of duplicate EHRs data in the cloud warehouse. The proposed approach is an effective solution for the reduction of duplication and storage cost in the cloud server. Hua et al. [13] proposed an online healthcare system named CINEMA, which is an efficient and a safe diagnostic platform, in which users can implement queries on cloud servers with no independent data decryption. The main drawback of their proposed system was that it requires high storage and computing power to allow millions of users to access the server at the same time and to query their requests.

These schemes include safe storage and fine-grained access control in the cloud, but there are still some problems associated with these schemes. For example, how internal prevention and malicious attacks destroys the cloud servers. Hence in this study, we present a Blockchain-enabled distributed framework rather than cloud data storage and privacy servers.

2.2. Blockchain-based Network Scenarios (BBNS)

Blockchain was originally suggested for building a Public distributed Ledger for all Bitcoin transactions [14]. After that, several research activities concentrate on key issues of the Blockchain technology itself, such as performance enhancement [15,16], double-spending intrusion resolution [19,20] and building efficient and distributed consensus mechanisms [17,18]. In the meantime, still a lot of other studies focused on the development of Blockchain-based practical applications. For instance, Yang et al. [19] proposed, a decentralized management of trusts framework that focuses on the Blockchain updating and publishing techniques, which maintain the trust details of all vehicles in a vehicular network. They have also strengthened the global consensus through a new proposed mechanism by consensus to bid for updated confidence for all RSU's. Guan et al. in [20] proposed a privacy-preserving and efficient data aggregation system based on Blockchain, in a smart grid, for optimal scheduling and for the protection of private information of a user. The users in his proposed system were divided into various groups. However, these schemes will solve their specified problems in the particular network situations, but in smart healthcare systems they cannot be implemented straight away. Thus, we proposed a Blockchain and machine learning enabled healthcare system, in order to attain the protection of privacy and security in healthcare.

2.3. Blockchain-based smart healthcare system

The Blockchain has been used in multiple studies in recent years due to its optimistic way of getting personal health information in secure manner. Certain research efforts [21-23] concentrate on demonstrating the benefits of Blockchain-based smart healthcare systems and proposing architectures; but very few studies are conducted on the implementation. Some literatures, such as [24-25], concentrate on the management of fine-grained access of user data obtained by IoT. They are not, however, moving any further consider ensuring the privacy of electronic health records (EHRs) developed by Physicians. Additionally, some proposed systems [26-29] were committed to the use of Blockchain which enabling users to monitor their monitored EHRs in conventional smart healthcare systems. Ali et al. [30] implemented the privacy of user-centric health care data preservation scheme known as MediBchain, wherein, users can encrypt and store their sensitive data on permissioned Blockchain. Only users who have the right password will access it, however, if users want to share their healthcare details, they need to share their passwords that carry out gross grain access controls, but it can easily lead to key leaks. MediBchain lacks modified passwords and key upgrade schemes. Later on, Zhang et al. [31], using Shamir's hidden exchange to authenticate fine-grained access authorization from consumers and physicians.

Healthcare data is considered extremely complex, and it needs to be secured and protected from unauthorized access by using secure resources and techniques. Thus, the process of storing, sharing, and managing medical data must be done in a safe way. Blockchain technology arises as a solution to these security challenges in the IoT networks and technology by storing data in blocks in a distributed and secured manner. Various types of research have been conducted by different researchers using both the combination of IoT and Blockchain. Blockchain improves the confidence of a single, centralized authority. However, still supports secure and "trustless" transactions frequently between communicating entities [32]. It offers decentralization, lastingness, and accord by methods for cryptography and game speculation.

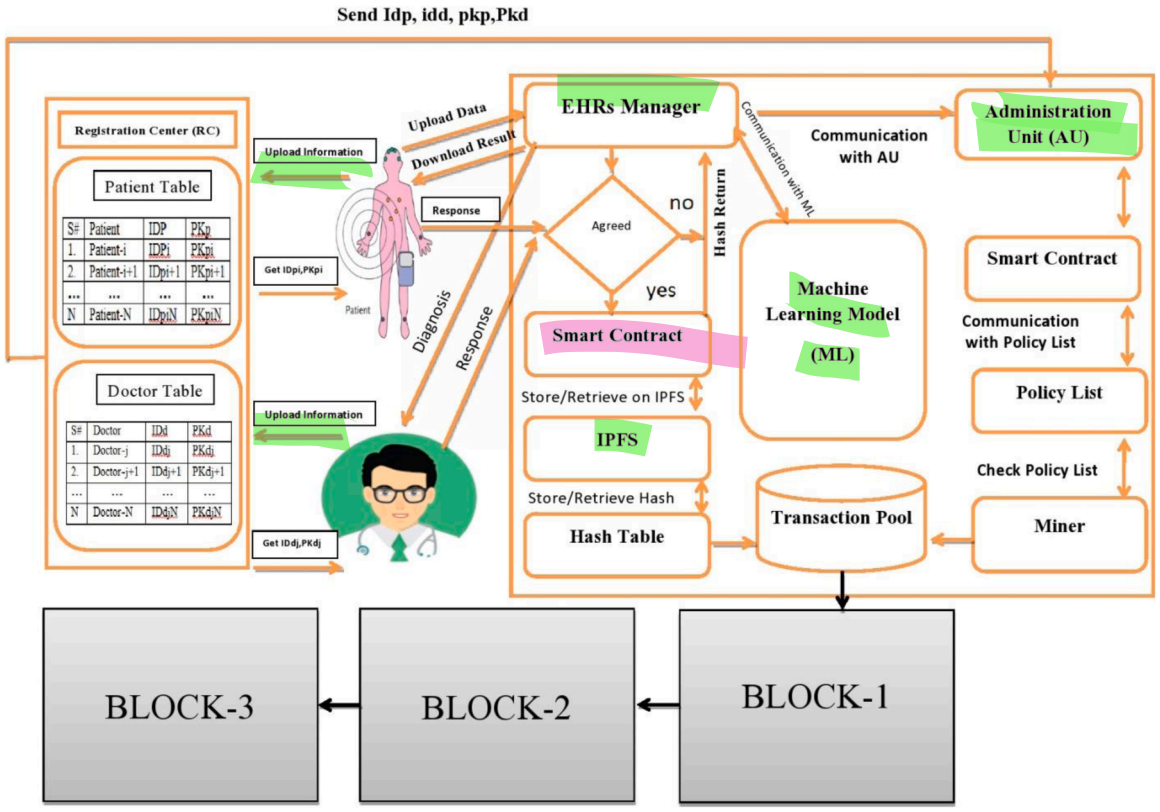

Fig. 1. Proposed System model of Blockchain Enabled Diabetes Detection

This advancement provides a solid foundation for different application zones, including cryptocurrency [33]. In [34], the author introduced a content extraction signature (CES) to restrict/ prevent patient's sensitive information from unauthorized access. In [7], the author has introduced a Blockchain-based Tele-Surgery framework for Healthcare. In [35], the author has introduced a hybrid attribute-based architecture for Blockchain and edge nodes to control access of Electronic Health Records (EHRs) data for traceability and accountability. In [36], the author proposed a tier-based end to end architecture for continuous patient monitoring. In their proposed system, patient centric agent (PCA), which is a center piece, manages a Blockchain component in order to preserve privacy, when data streaming from body sensors needs to be stored securely. In [37], the author has talked about a mechanism for secured and efficient data accessibility for the patient and doctor in a given healthcare system. Their proposed system successfully explains the appending of records to Blockchain and retrieves that from there. They failed to explain the registration of patients and doctors as well as don't explain the procedure of how a patient and a doctor will maintain authentication and how patient's data will be diagnosed through machine learning. In [38], the author has proposed a health-chain, that composed of Dchain and Uchain, wherein the user can easily add or revoke a doctor by leverage user transactions for key management. However, their proposed system does not explain how a patient or doctor would be registered with hospitals and failed to include prediction of disease by symptom. In [39], the author has designed a smartphone-based tool to identify symptoms of common childhood diseases in Ghana. They developed and evaluate an integrated clinical algorithm in a cross-sectional study, wherein they improved the diagnosis and treatment of children of the rural areas. Further, they designed a tool to support the guardians of children living in areas with limited access to healthcare. For information exchange, they used audio files, instead of text messages, and their study mainly targets guardians of the ill children.

The existing IoT-based health monitoring systems are facing the problem of security, and also there is a need for a system that detects and predict the health conditions of a person in real-time, in order to prevent him/her from more damage, and to protect his/her information from unauthorized persons, and to store it permanently in immutable ledger for future as well.

Our proposed framework uses ML algorithms to predict the health conditions i.e., diabetes disease of a patient and store the health information permanently in the Blockchain. Once the information of a patient is stored, the doctor will then be able to observe the EHRs of his patients whenever he wants in the future. This research study encourages the use of ML algorithms with highly secured Blockchain for developing an IoT and ML based intelligent prediction model. The performance of the proposed model is evaluated with the help of various performance measures. The experimental results prove the effectiveness of the proposed model.

3. Proposed system design

This section represents the system model and design goals of our proposed system named, Blockchain-enabled Healthcare System for the Detection of Diabetes disease.

3.1. Proposed system model

Fig. 1 represents the block diagram of our proposed Blockchain-enabled healthcare system for the detection of diabetes disease. The patient and doctor first register themselves by requesting to Registration Center (RC), which obtained all necessary information of the concerned and then assign private key along with ID, and the same then forwarded to the Administration Unit. When this user (patient or doctor) wants to interact with the EHRs Manager he/ she must authorized his/ her ID from EHRs Manager. If the authentication is successful, then he/ she can be able to upload/ download data (healthcare information) to/from EHRs Manager otherwise a penalty will be generated on this specific ID.

After successful authentication now the authorized user is able to upload/ download healthcare information and may be store on Blockchain after patient and doctor approval. Our proposed system consists of various components, each component, and its working is discussed in much detail in the following subsections.

3.1.1. Registration Center (RC)

The Registration Center (RC) is used to collect information from the patients and healthcare practitioners i.e., doctors, and store them in the database in a secure manner. The information collected from the patient's includes patient's name, father name, age, and address, etc. whereas, the information gathered from the practitioner's includes practitioner's name, qualification, specialization, and contact number. The RC then computes the concerned patient's identity (PID) and doctor's identity (DID) as well, with their own public keys. After successful computation, the RC then sends single identity and public key to the particular patient/practitioner. The same identity of the patient/practitioner is sent to the administration unit as well, from where they will be verified, when they want to append/retrieve data to/from the Blockchain [40]. The Registration Center is connected with Smart Device that provides information of the users.

3.1.2. Smart device

The smart device includes smartphones, laptops, desktops, and sensor nodes. Both the patients and practitioners have access to the smart devices and are using it, in order to login into the system. After logging in successfully, the patient provides his/her own information (name, father name, age, and address, etc.) while the doctor provides his/her own information (name, qualification, specialization, and contact number, etc.) to RC, in order to store their information in the database in a secure manner. Next Smart Device sent data to Electronic Health Records (EHRs) Manager for further processing.

3.1.3. Electronic Health Records (EHRs) Manager

The EHRs is an important component of our proposed system which plays a significant role in the operations of the proposed system. It works as a central controller and performs multiple operations. When a patient wants to do a transaction (patient addresses) to Blockchain or want to retrieve history from Blockchain he/she sends a request to EHRs Manger [40-43]. Similar process is done for the practitioner as well. Whenever, the patient/practitioner does a request, the EHRs manager asks for the public key of the requester. After providing the public key, it is then sent to the administration unit for verification, on the basis of public key it is then decided that whether the requester has the right to upload or retrieve data to/from Blockchain or not. The administration unit verify the public key of the requester through a smart contract from the policy list. When a patient or the practitioner is verified successfully, the EHRs Manager then sends an encrypted transaction to the Interplanetary File system (IPFS), which is a cloud storage server, for establishing connection with the Blockchain network, using the public key of EHRs Manager. EHRs Manager connects to Smart Contract (SC) which exchange money, property, stocks etc. in a transparent, conflict-free method while circumventing the facilities of a middleman.

3.1.4. Smart Contract (SC)

A Smart Contract (Crypto Contract) is a PC program that legitimately and consequently controls the exchange of digital assets between the gatherings under specific conditions. A smart contract works similarly as a conventional contract by consequently implementing the contract. These are the programs that execute precisely as they are set up (coded, modified) by their makers [37,40]. Similarly, conventional contract is enforceable by law, while smart contracts are enforceable by code. Smart Contract connects with EHRs Manager and Administration Unit.

3.1.5. Administration Unit

This component receives ID and public key of the concerned patient and practitioner, assigned by the RC. By granting or revoking, the Administration Unit manages all activities and transactions on the cloud [40]. When a new transaction is received with the user public key from the EHRs manger, the administration unit then verifies the access rights of the requester based on the public key in the policy list. Data access permission is granted to the requester when the public key is verified in the policy list of the smart contract, otherwise a penalty is issued and all the EHRs manager activities are denied and the request is discarded from the Blockchain network as well. The Administration Unit sends message of approval of users to EHRs Manager, who sends IoT data received from Smart Device to Machine Learning Unit for diagnosis.

3.1.6. Machine Learning Unit

ML unit is an important and the most significant component of our proposed system. The responsibility of ML model is to take health data from EHRs Manager provided by smart device i.e. sensor nodes. The ML model is first trained on the diabetes disease dataset. After training, the patient data is provided to the model, who then predict the health conditions of a patient that whether he/she has diabetes disease or not. Five ML classification algorithms namely, DT, KNN, RF, LR, and SVM are utilized in our study. The performance of all classification models are computed with the help of various performance metrics such as, accuracy, sensitivity, specificity, AUC, precision, recall, MCC, and ROC curve. EHRs Manager receives diagnosis from ML and sends it to Interplanetary File System is both patient and doctor agree to send this record to Blockchain.

3.1.7. Interplanetary File System (IPFS)

IPFS is a cloud storage server that automatically returns a hash of the uploaded file or transaction to the EHR Manager [37,40]. It also stores the generated hash to update the hash table. In this paper, we assume that all storing nodes are IPFS-based, where IPFS system is accomplished and preserved by the group of healthcare providers, for instance hospitals. It uses a content addressing method where the address is derived from the content of the file. Each file is hashed into a hash string and each hash string is unique to identify the file. Anyone can find the complete file stored in IPFS via the hash string of the file on Blockchain. IPFS makes it possible to distribute large volume of data with high efficiency. In our proposed system when a new transaction takes place, the EHRs manager first verifies it from the administration unit under policy list. After verification the transaction needs to be store in the cloud. Before storage an automatic generated hash is calculated and stored in a table called hash table. Next secure transaction is transmitted to a pool of transactions called transaction pool. This pool consists of two kinds of transactions 1) a transaction that would be appending to the Blockchain, 2) transactions which are retrieved from the Blockchain through mining. Similarly, the newly mined transactions are stored here which can be provided to a particular requester. The calculated hash can then be sent to the transaction pool from here, it is ready for mining or assigned to the Blockchain. Next the hash of approved transaction is calculated and stored in the hash table for future reference.

3.1.8. Hash Table

The hash table is used to store the calculated hash of all the approved transactions which would append to the Blockchain network [41]. In our proposed system when both the patient's and practitioners are agree on the appending of the transactions to the Blockchain, they send their agreement along with the signature which proves that a particular transaction will be available for the future use when needed. From hash table this approved transaction is store in the Transaction Pool from where it is ready to store on Blockchain.

3.1.9. Transaction Pool

This pool stores all the transactions that would be append/retrieve to/from the Blockchain. Transaction pool can be divided into two parts i.e., truncations that need to be stored on Blockchain and the transactions

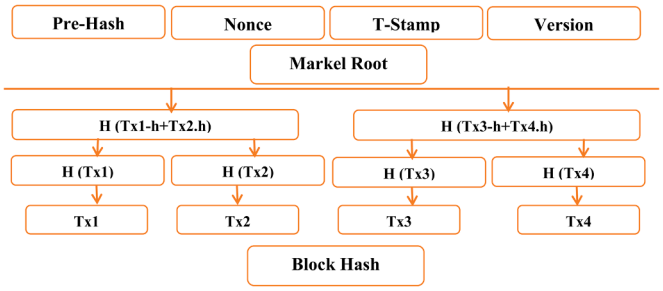

Fig. 2. Block Structure of the block in the proposed system

that need to be retrieved. Miner in our proposed system is responsible for adding the transactions in a block, which is then verified in order to add it to the Blockchain network. In our proposed system, we assumed that 1 MB block can contain maximum 5349 IoT transactions (txIoT) and assumed that each minute a block is produced. Thus, the throughput of IoT Transactions can be reached to 89 [38].

3.1.10. Block Structure

Fig. 2 illustrates the Block structure in our proposed system which consists of the following components [41]

A. *Previous Hash (Pre-Hash):* A hash is a function that alters an input of letters and numbers into a coded output of an immutable size. A hash is formed by an algorithm and is essential for Blockchain organization in cryptocurrency. In our proposed system, the hash of a block is generated by the header of the block which contains several parameters such as, hash of the previous block, nonce, version of the block, time stamp, signature of the user, and Merkel Tree which contain IoT transactions.

B. Nonce: A nonce is a contraction for "number just utilized once" which is a number added to a hashed or scrambled block in a Blockchain that, when rehashed, meets the trouble level limitations.

C. Time Stamp: The time stamp records the hour of the block's age. The time stamp makes the exchange of data on the block unchanging, which can be utilized in the form of significant information to demonstrate the exchange.

D. Markel Tree: A Merkel tree is an information structure which is used in numerous software applications. In bitcoin and other crypto currencies, Merkel trees serve to encode all the Blockchain transactions more effectively and safely.

E. Block Header: A block header is utilized to distinguish a specific block in the entire Blockchain and is hashed over and again to make confirmation of work for mining rewards. Every block contains an exclusive block header which is used for the unique identification of each block.

F. Signature (Si): The signature in our proposed system indicates the user agreement.

In our proposed system, we focus on four operations i.e., User Registration, User Authentication, Diabetes data upload and Block Acceptance. The patient and doctor Registration process can be view in Algorithm-1 and Algorithm-2 respectively.

Algorithm-1 explains the procedure of patient registration by accepting seven attributes (i.e., Name of the patient, Father Name, Age, Address, CNIC Number, gender and Medical History). After obtaining required information a Hash (hi) then calculated where it stored in the hospital Database and unique user ID and Public Key is assigned to user and the same forwarded to Administration Unit.

Algorithm 1:Patient Registration

Input: Mij, where j represents j^{th} patient and i represents 7 attributes of patient i.e
i ϵ {1, 2, 3…..7}, m^{th} password (pwdm), k^{th} password (pwk).
Output:{Return Result}

1 For each = k=1, j<= N, j++ do

(Here N represents maximum registrations at the Registration Center)

1 Pwdk← password

(Enter password)

1 Pwdm← password

(Enter password again)

1 If pwdk == pwdm then
2 Print (access granted)

After successful registration j^{th} patient provides 7 attributes i.e. i ϵ {Name,
Father Name, Age, Address, CNIC No, Sex, Medical History}

1 For each I ==1, i<= 7, i++ do
2 hj← h (Mi||T||i||t)
3 end for
4 store-infoj← hj

(store patient data in Registration Server's Database)

1 Send patient ID (IDpj) and Public Key (PKpj) to patient and Administration Unit.
2 Else
3 Print (access denied)
4 Return "registration failed"
5 End if
6 End for

Algorithm-2 explains the procedure of doctor registration by accepting seven attributes (i.e. Name of the patient, Father Name, Age, Address, CNIC Number, gender and qualification/ Specification). After obtaining required information a Hash (hj) then calculated where it stored in the hospital Database and unique user ID and Public Key is assigned to user and the same forwarded to Administration Unit.

Algorithm 2: Doctor Registration

Input: Mij, where j represents j^{th} doctor and i represents 7 attributes of doctor i.e
i ϵ {1, 2, 3…..7}, m^{th} password (pwdm), k^{th} password (pwk).
Output: {Return **Result}**

1 For each = k=1, j<= N, j++ do

(Here N represents maximum registrations at the Registration Center)

1 Pwdk← password

(Enter password)

1 Pwdm← password

(Enter password again)

1 If pwdk == pwdm then
2 Print (access granted)

After successful registration j^{th} doctor provides 7 attributes i.e. i ϵ {Name,

Father Name, Age, Address, CNIC No, Sex, qualification and specification}

1 For each I ==1, i<= 7, i++ do
2 hj← h (Mi||T||i||t)
3 end for
4 store-infoj← hj

(store doctor data in Registration Server's Database)

1 Send doctor ID (IDdj) and Public Key (PKdj) to patient and Administration Unit.
2 Else
3 Print (access denied)
4 Return "registration failed"
5 End if
6 End for

Algorithm-3 explains the procedure of user (doctor/ patient) Authentication by starting authentication session. First the Smart Device encrypts the desired user ID with the Public Key of ith EHR Manager and assigned to a variable i.e. Encrypted ith message (EncrypMi), which the then be sent to EHR Manager who Decrypt it with the help of its Private Key (SKEHRi) and obtained the ID of requester. The ID then sent to Administration Unit where it can be checked under Policy in the Policy list, if it presents there then authentication become successful otherwise a penalty will be generated on this particular ID. In our system this panel will be a warning message to the requester.

Algorithm 3:User Authenticaiton

Input:j^{th} User ID.
Output:{Result}

1 Authentication session started for j^{th} user
2 EncrypMi← Encrypt (PKEHRi, IDpj)

(smart- device encrypt User ID i.e. patient or doctor with EHRs Manager's Public Key (PKEHRi))

1 Smart-device sends EncryptMi to EHRs Manager
2 decrypEHRi← decrypt (SKEHRi, EncryptMi)

(EHRs manager decrypt the encrypted message of smart- device with its own Private Key (SKEHRi))
EHRs Manager sends user ID to Administration Unit

1 if policy-list (KPpj) == true then
2 Administration Unit verifies required ID in policy-list
3 Result← ("authentication successful")

(Administration Unit return successful if user ID found)

1 Acknowledged to j^{th} user
2 Else
3 Result← penalty (IDpj, action)

(Administration Unit returns penalty with specific action if user ID not found)

1 End if
2 **Return "Result"**

Algorithm-4 explains the procedure of IoT data uploading of user starting from for-each loop, first the IoT data of patient is encrypted with a symmetric key (Ki), which then sent by Smart Deice to EHR Manager who decrypt it and sent to Machine Learning Unit which runs different Machine Learning algorithms (see Section 5). When the successful diagnosis is obtained, the required result is sent to EHR Manager who uploads it to Inter Plenary File System (IPFS) after the agreement of both patient and doctor.

Algorithm 4:	**Iot Data Uploading**
Input:	i^{th} IoT device data, Ki symmetric key.
Output:	**{Result}**
	1. For each IoT data upload time $slot_{min}$ to IoT data upload time $slot_{max}$
	(maximum IoT upload data)
	2. EIoTi← Encrypt (Ki, IoTi)
	(smart- device sends encrypted IoT data (EIoTi) to EHRs Manager)
	3. DIoTi← decrypt (Ki, EIoTi)
	(EHRs Manager decrypt EIoTi with symmetric key (Ki))
	4. EHRs Manager sends IoTi to Machine Learning Unit
	5. Machine Learning Unit generated required i^{th} diagnosis (diagi) and send to EHRs Manager.
	6. EHRs Manager send the diagnosis (diagi) to concerned doctor and patient forget approval.
	7. If patient and doctor === agree then
	8. Send DIoTj to IPFS nodes and get hash of encrypted IoT data (HEIoTi)
	9. Generate timestamp ts1
	10. Set sj← sign (skuj, H (IDUj), ts1, htmxi, HEIoTi)
	11. Set htxi← H (IDuj, ts1, HEIoTi, sj)
	12. Set txIoTi← H (IDuj, ts1, htxi, sj)
	13. Result ← txIoTi
	14. Else
	15. Result ← data uploat failed
	16. End if
	17. Return result

Algorithm-5, of the proposed system, explains the procedure of adding new block to Blockchain, in the start the list of available miners is provided by miner under strict policy of the Policy List. Then the block header is calculated. If the target becomes true, target hash and nonce are calculated. If the selected Miner is verified and all the conditions meet then block is added to the Blockchain otherwise block is not accepted to add to the Blockchain.

Algorithm 5:	**Block Acceptance**
Input:	previous block hash, random list of i^{th} Miners (Mi).
Output:	**{Block Acceptance}**
	1. Enter M [i] from available list of miners
	(Selected Random Miner)
	2. SelectedMiner [j]← M [i]
	(Assign selected Miner to Selected Miner list)
	3. If SelectedMiner [j]== true then
	(Condition start)
	4. Build Markel Tree of the transactions
	(Build Markel Tree)
	5. BlockHeader← (Tstamp||MR||V||PBH)
	(Calculated Block Header)
	6. Calculate nonce
	(Calculate required nonce)
	7. BlockHash← (Tstamp||MR||V||PBH||nonce)
	(Calculated Hash of the current Block)
	8. If SelectedMiner [j]== verified, sig== true and BlockHash== targetHash, nonce= true and Tstamp== true then
	(Condition start)
	9. Result ← Block Accepted
	(Block Accepted if condition matched)
	10. Else
	11. Result Block not Accepted
	(Block not Accepted if condition not match)
	12. End if
	13. Return Result
	14. End if

3.2. Security analysis and performance evaluation

This section examines the protection of Blockchain-Enabled

Table 1
Notations and their descriptions

Notation	Description
Pwdi and pwdj	i^{th} and j^{th} password
Mi	i^{th} message
Hj	j^{th} Hash
PKpj	j^{th} patient public key
IDpj	j^{th} patient ID
PKdj	j^{th} doctor public key
IDdj	j^{th} doctor ID
PKEHRi	i^{th} Electronic Health Records public key
SKEHRi	j^{th} Electronic Health Records private key
IDpj	j^{th} patient ID
Ki	Symmetric key
DIoTi	Decrypted IoT ith data
EIoTi	Encrypted IoT jth data
Si	Signature
txIoTi	i^{th} IoT transaction
HEIoTi	Hash of encrypted j^{th} IoT transaction
PBH	Previous Block Hash
V	Version

Healthcare System for the Detection of Diabetes based on the design goals set out in Section 3.2 along with Performance Evaluation of the proposed system.

3.2.1. Security Analysis of the proposed scheme

The security Analysis of the Blockchain-Enabled Healthcare System for the Detection of Diabetes can be explained as follows:

3.2.2. Security preservation

In our proposed system, patient block can only have hash of encrypted IoT data (HEIoT) and opponents can only obtain Enc(ki, IoTi) from Interplanetary File System (IPFS). The IoT data is encrypted with a symmetric key which can only be accessible to opponents who possess this key. We suppose that the computational power of opponents is restricted, and both user's and practitioner's private keys such as SKui and SKdj respectively are secured. So, the opponents cannot obtain the desired IoT data and its diagnosis made by Machine Learning Model. Our scheme could therefore provide conditional security for IoT data as well as for its diagnosis.

3.2.3. Accountability

Accountability in our proposed model indicates that any third party may audit that whether the IoT data is produced by a user and the diagnosis is done by the practitioner. The users should be accountable for their IoT data. As the IoT transaction (txIoTi) of the users contain the signature of a particular user, under the supposition that the private key (SKui) of the user is secured. Therefore, no one can imitate a user to generate transactions without user's private key (SKui). When suspicious data is detected, the relevant user can be found according to the signature in the transaction. So, it is malicious user-generated data to consume the medical resources, the system is indeed indisputable.

So as to avoid medical disagreements, from the other side, the diagnoses made by ML model should be the responsibility of the EHRs manager. We assumed that the ML model make accurate detection which is then sent to the patient and his/her concerned doctor. The ML model is Handel by EHRs Manager, if it refuses to make the appropriate diagnosis in compliance with the policy list's professional rules, then EHRs Manager must be held responsible. The proposed scheme therefore has to be responsible.

3.2.4. Performance evaluation

In this portion, we are going to test the efficiency and achievability of our proposed model, which can be further divided into block design functionality and processing time of transactions time generation of our Blockchain-enabled diabetes disease detection.

In our implemented prototype, we simulate the patient and doctor nodes with a smart phone, while the experiment is built in Java programming language. Block mining is measured on a 64-bit windows 7 OS with Intel (R) Core (TM) i7-4790, 3.60 GHz processor. It is added that Blockchain is written in Python.

Table 1.

Table 2
Parameters used for Block header of our proposed system

Parameter used	Previous Hash	Time Stamp	Nonce	Merkel Root
Length in Bytes	32	4	4	32

Table 3
Parameters used for the body of Block of our proposed system

Parameter used	User ID	txIoT	Signature (Si)	Hash	Symmetric Encryption
Length in Bytes	32	132	32	32	128

Table 4
Processing time of cryptographic operations

User	Operation (milli sec)
RSA encryption	0.209
SHA-256	0.012
RSA signing	3.60
AES encryption	0.134

Table 5
Computational time complexity of Algorithm 1- Algorithm 5

Algorithms	Time Complexity
Algorithm 1	$O(n^2)$
Algorithm 2	$O(n^2)$
Algorithm 3	O(n)
Algorithm 4	O(n)
Algorithm 5	O(n)

3.4.5. Block capacity

According to [38], Previous Hash length, Index and Markle Root are all set as 32 Bytes; the length of Time Stamp and Nonce set as 4 bytes as shown in Table 2, while parameters in the body of block can be seen in Table 3, wherein the User ID, signature, and Hash are set as 32 Bytes, the length of IoT transaction (txIoT) and Symmetric Encryption set as 132 Bytes and 128 Bytes respectively.

We may assume that 1 M Bytes block can contain 5349 IoT transactions (txIoT) and each minute a block is produced, the throughput can reach to 89 IoT transactions (txIoT) a second.

3.2.6. Processing time of transactions

In this portion of our proposed system, the processing time for several major cryptographic operations such as Sha-256, AES, and RSA are measure on PC and an Android devices as given in the Table 4.

Table 6
Computational time of utilized ML Models

Classification algorithm	Computational time (sec)
DT	1.211
KNN	2.701
RF	2.002
LR	0.912
SVM (LINEAR)	0.905
SVM (RBF)	1.320

Table 7
Computational time complexity of used ML Models

Classification algorithm	Time Complexity
DT	$O(n^2)$
KNN	$O(n^2)$
RF	O(nlogn)
LR	O(n)
SVM (Kernel=LINEAR)	$O(n^2)$
SVM (Kernel=RBF)	$O(n^3)$

Table 8
Notations and their meanings

Parameter Used	Meaning
DT	Decision Tree
SVM	Support Vector Machines
RF	Random Forest
LR	Logistic Regression
PIDDD	Pima Indian Diabetes Disease Dataset

From Table 4, it is obvious that the RSA signing technique takes much time i.e. 3.60 ms as compare to the rest of approaches. RSA encryption stood second in this regard by taking the processing time of 0.209 ms. The smallest processing time was observed for SHA-256 i.e. 0.012 ms and is considered to be the most prominent one.

Table 5 demonstrates the computational time complexity of all of our proposed algorithms i.e. Algorithm 1, Algorithm 2, Algorithm 3, Algorithm 4, and Algorithm 5.

The computational time of all the utilized ML classification algorithms is represented in Table 6. From Table 6 it is observed that SVM with Kernel=Linear has the smallest processing time i.e. 0.905 seconds while the KNN classification model has the largest processing time i.e. 2.701 seconds.

Indeed, the computational time complexity of an algorithm is an important parameter in describing its significance. Table 7 illustrates the computational time complexities of all the ML models used in this study. From table 7 it is clear that the SVM with kernel=RBF has the worst case time complexity of $O(n^3)$ and is considered to be more complex while the smallest worst case time complexity was observed for the LR i.e. O (n).

4. Simulation results of ML classification models

The experimental results of various machine learning classification algorithms are represented in this section. We investigated the performance of 5 ML classification algorithms namely, KNN, DT, RF, LR, and SVM on Pima Indian Diabetes Disease Dataset (PIDDD). In order to normalize the dataset and remove the missing values, various preprocessing techniques are applied to the dataset before used by the classification algorithms. For measuring the performance of classification model's various performance evaluation metrics are used. For experimental work and implementation, python is used as a tool. Following table-8, represents parameters and their meaning used in the simulation section:

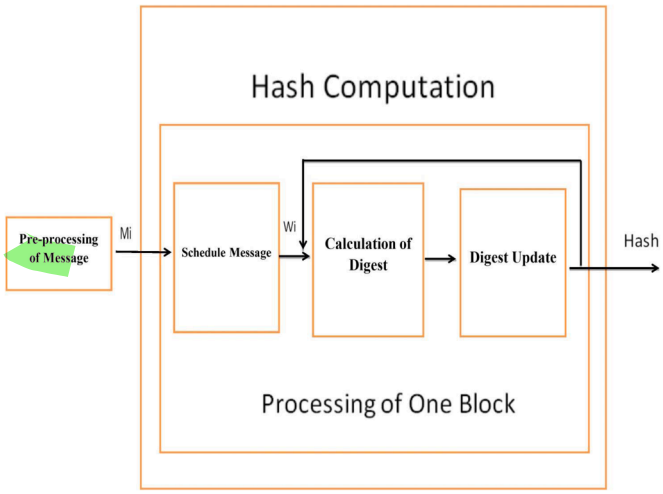

Fig. 3. Hash Operation in Blockchain

4.1. Performance of Classifiers using PIDDD

In this subsection the experimental results and the performance of all 5 utilized classification algorithms are discussed using PIDDD. The performance of all investigated classification models is demonstrated in Table 9.

Table 9, shows that SVM with kernel=rbf performed excellently in terms of all performance evaluation metrics as compared to the rest of the classification models. SVM achieved classification accuracy of 80.51%, 54.43% sensitivity, 94.07% specificity, 80.0% precision, 90.74% AUC, 0.80 F1-Score, and MCC of 0.55. Sensitivity demonstrates that the diagnostic result was positive, and the person has diabetes disease. On the other hand, specificity notifies that the diagnostic result was negative, and the person is healthy. Again, SVM with kernel='-linear' performs very well and attained classification accuracy of 79.65% and stood second in terms of all performance evaluation metrics as shown in Table 8. LR showed good performance and achieved an accuracy of 79.22%, specificity of 89.47%, 59.49% sensitivity, the precision of 78.0%, AUC of 89.04%, 0.77 F1-score, and MCC of 0.52. KNN stood last in this regard as compared to the other classification algorithms. We accomplished multiple trials for the KNN classifier by taking numerous values for 'K' (3, 5, 7, 9, 11, 13, and 15). KNN attained good results at k=9 as shown in Table 8. Multiple experiments of KNN for different values of K (3, 5, 7, 9, 11, 13, and 15) and their corresponding results are shown in Fig. 6.

Fig. 3, illustrates the performance of all utilized classifiers. SVM performed extremely well as compared to other classification algorithms in terms of classification accuracy, specificity, and sensitivity. KNN showed the lowest performance in terms of accuracy, specificity, and sensitivity, by comparing it with the rest of the classification models.

Fig. 4.

Fig. 5, shows the F1-score and MCC results of all 5 classification models on PIDDD. The highest resultant value was observed for SVM with Kernel='RBF', while KNN showed the lowest performance in terms of all performance measures.

Table 9
Performance of all 5 classification algorithms using PIDDD

Classification Model	Accuracy	Specificity	Sensitivity	Precision	AUC	F1-Score	MCC
DT	77.60	84.86	62.03	77.0	87.0	0.77	0.48
KNN (K=9)	75.01	86.21	54.43	74.0	82.23	0.74	0.40
RF	78.64	86.18	58.22	78.0	86.0	0.78	0.46
LR	79.22	89.47	59.49	78.0	89.04	0.77	0.52
SVM (LINEAR)	79.65	92.10	55.69	79.0	89.41	0.79	0.53
SVM (RBF)	80.51	94.07	54.43	80.0	90.74	0.80	0.55

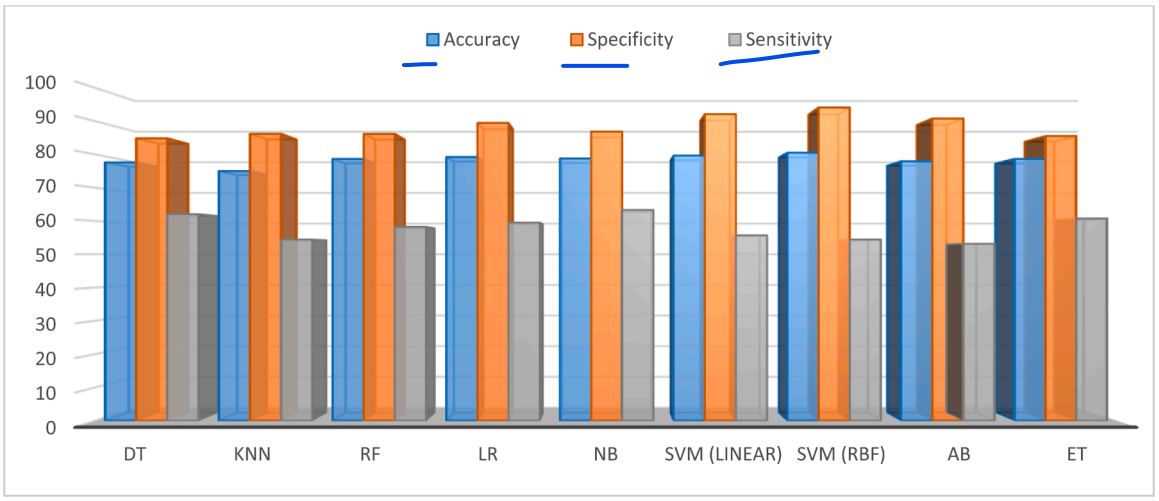

Fig. 4. Performance of all 5 utilized classification algorithms on PIDDD

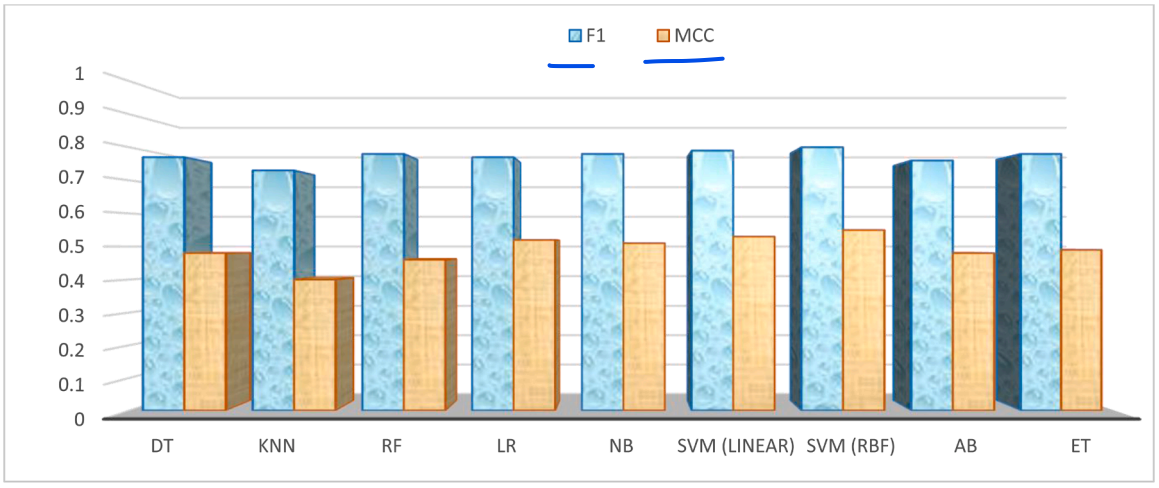

Fig. 5. F1-score and MCC of all 5 classification algorithms on PIDD

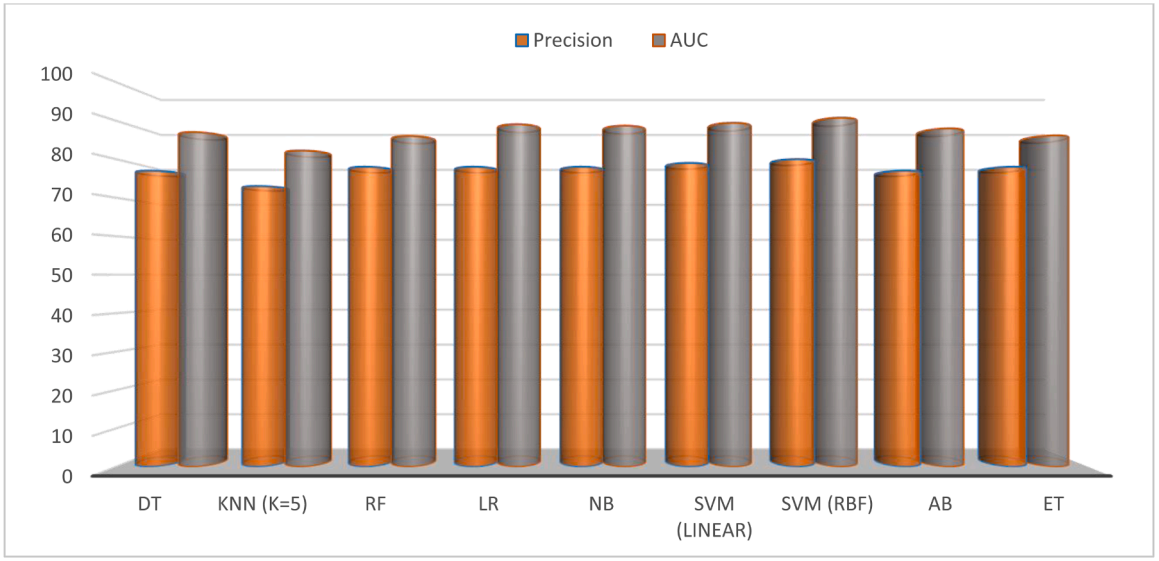

Fig. 6. Precision and AUC of all 5 classification algorithms on PIDD

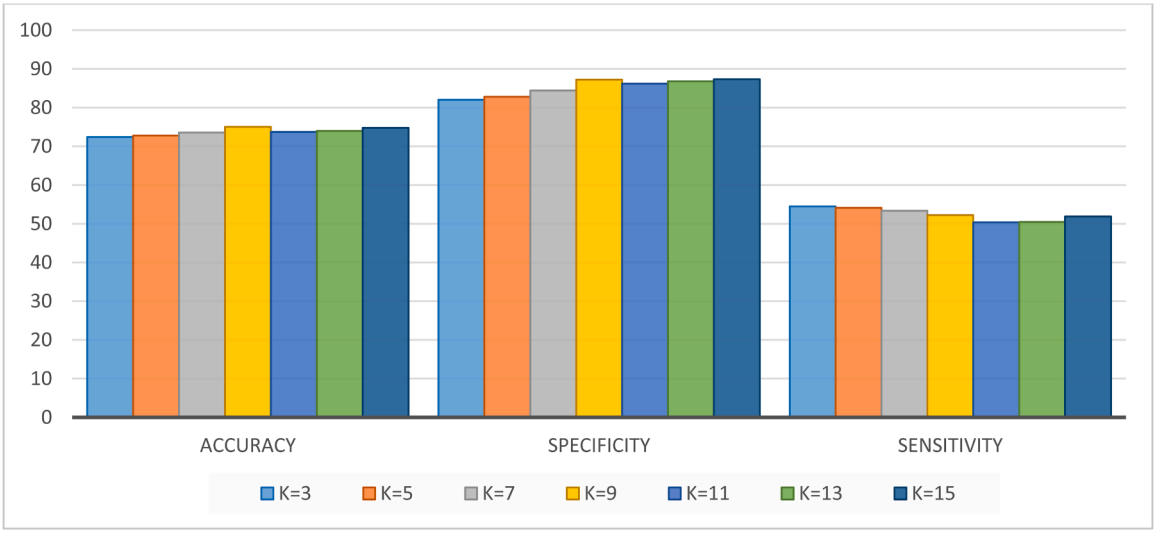

Fig. 7. Performance of KNN on multiple values of K (3, 5, 7, 9, 11, 13 and 15).

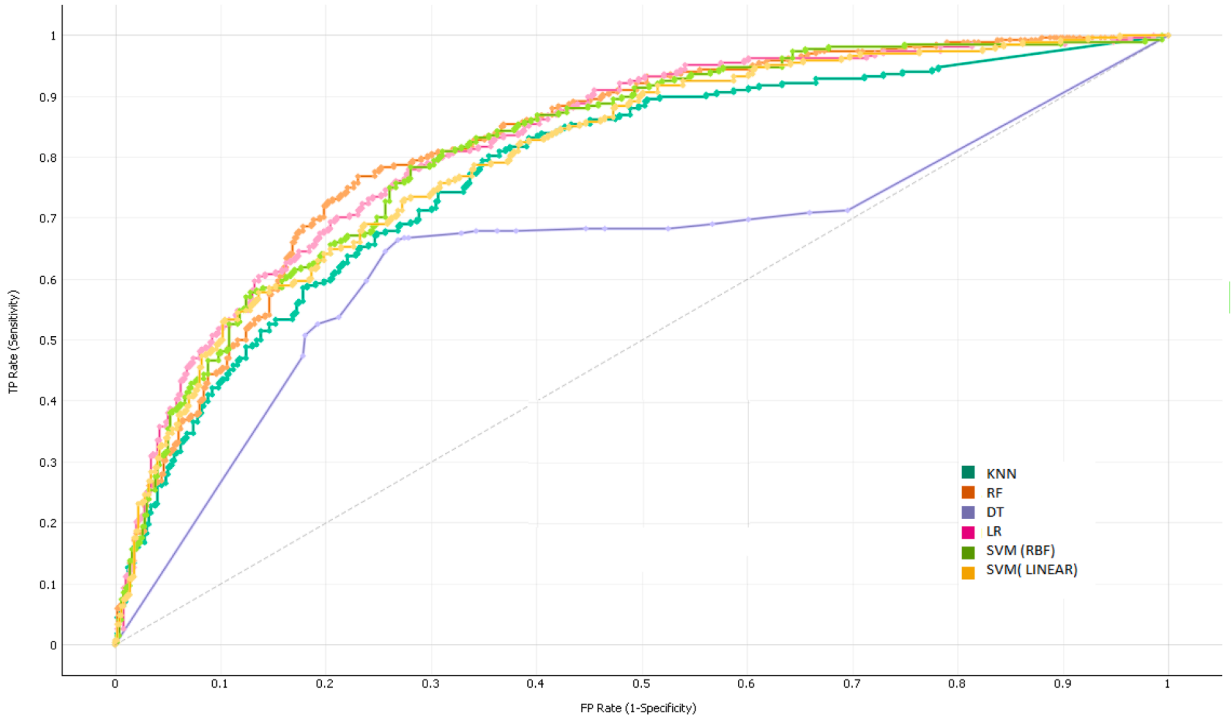

Fig. 8. ROC curves of all 5 classification algorithms.

Precision and AUC-score of all 6 investigated classification algorithms on PIDDD used in this study are shown in Fig. 5.

Fig. 7, describes the performance i.e. accuracy, specificity and sensitivity of KNN classification model for various values of K (3, 5, 7, 9, 11, 13 and 15) by performing multiple experiments.

Fig. 8, represents the ROC curve of all 5 utilized ML classification algorithms on PIDDD.

Nowadays, ML classification algorithms play a vital role in medical fields by predicting and diagnosing various diseases accurately and effectively. The identification and detection process of various diseases such as chronic diseases is considerably improved with the help of these ML models. Here in our study, we have discussed and implemented 5 popular ML classification algorithms and proposed a framework for the identification and prediction of diabetes disease. The proposed system is expected to be helpful for the physician in diagnosing diabetes disease in an effective way.

5. Conclusion

In this paper, we proposed a Blockchain-enabled diabetes detection scheme which consists of three phases i.e., registration phase, user authentication phase and IoT data upload with Blockchain phase. In our proposed system, the user first complete the process of registration during the first phase to ensure communication with a Blockchain network. The user verifies identity from Electronic Health Records (EHRs) Manager stored in an authentication unit. The machine learning techniques was introduced to detect diabetes of patient as well as to securely share the results with the healthcare practitioner. Besides, we

examined that our proposed scheme can fulfill the necessities of privacy, integrity and authentication. We have also planned the possible smart-contract agreement considering this healthcare setup. The security examination presents that our proposed system can meet our expected security necessities. Performance evaluation of our proposed system shows that our proposed Blockchain network is well-organized and achievable in practice. For future work, we plan to investigate more Machine Learning Techniques for different diseases detection to attain better performance. Using advanced procedures to obtain patient's healthcare data from sensors, plan to introduce lightweight Blockchain, plan to implement Blockchain technology in more sectors other than healthcare such as government systems etc., transport, gaming industries, online voting system, and in education. In addition, we plan to develop an advanced Blockchain based model to prevent Blockchain attacks

Author contribution

All persons who have made substantial contributions to the work reported in the manuscript (e.g., technical help, writing and editing assistance, general support). The authors are listed/numbered based on their contribution in the paper.

Declaration of Competing Interest

None of the authors in this publication has any conflict of interest.

Acknowledgement

Taif University Researchers Supporting Project number (TURSP-2020/126), Taif University, Taif, Saudi Arabia

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 service providers 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] Zhang Y, Zheng D, Deng RH. Security and privacy in smart health: efficient policy-hiding attribute basedac cess control. IEEE Internet of Things J 2018;5(3):2130–45.
[11] Zhang Y, Xu C, Li H, Yang K, Zhou J, Lin X. HealthDep: An efficient and secure reduplication scheme for cloud-assisted ehealth systems. IEEE Trans Ind Inf 2018; 14(9):4101–12.
[12] Hua J, Zhu H, Wang F, Liu X, Lu R, Li H, Zhang Y. CINEMA: Efficient and privacy-preserving online medical primary diagnosis with skyline query. IEEE Internet of Things J 2018.
[13] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.
[14] Nikitin K, Kokoris-Kogias E, Jovanovic P, Gailly N, Gasser L, Khoffi I, Cappos J, Ford B. CHAINIAC: Proactive software-update transparency via collectively signed skipchains and verified builds. In: Proceedings of the 26th USENIX Security Symposium. The Advanced Computing Systems Association; 2017. p. 1271–87.
[15] Kogias EK, Jovanovic P, Gailly N, Khoffi I, Gasser L, Ford B. Enhancing Bitcoin security and performance with strong consistency via collective signing. In: Proceedings of the 25th USENIX Security Symposium. The Advanced Computing Systems Association; 2016. p. 279–96.
[16] Karame GO, Androulaki E, Capkun S. Double spending fast payments in Bitcoin. In: Proceedings of the 2012 ACM conference on Computer and communications security. ACM; 2012. p. 906–17.
[17] Ruffing T, Kate A, Schr¨oder D. Liar, Liar, Coins on Fire!: Penalizing equivocation by loss of Bitcoins. In: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. ACM; 2015. p. 219–30.
[18] Chen J, Yao S, Yuan Q, He K, Ji S, Du R. CertChain: Public and efficient certificate audit based on Blockchain for TLS connections. In: Proceedings of the 37th IEEE International Conference on Computer Communications (INFOCOM '18). IEEE; 2018. p. 2060–8.
[19] Yang Z, Yang K, Lei L, Zheng K, Leung VC. Blockchain-based decentralized trust management in vehicular networks. IEEE Internet of Things J 2018.
[20] Kang J, Yu R, Huang X, Wu M, Maharjan S, Xie S, Zhang Y. Blockchain for secure and efficient data sharing in vehicular edge computing and networks. IEEE Internet of Things J 2018.
[21] Guan Z, Si G, Zhang X, Wu L, Guizani N, Du X, Ma Y. Privacy-preserving and efficient aggregation based on Blockchain for power grid communications in smart communities. IEEE Commun Mag 2018;56(7):82–8.
[22] Shae Z, Tsai JJ. On the design of a Blockchain platform for clinical trial and precision medicine. In: Proceedings of the 37th IEEE International Conference on Distributed Computing Systems (ICDCS). IEEE; 2017. p. 1972–80.
[23] Esposito C, De Santis A, Tortora G, Chang H, Choo K-KR. Blockchain: a panacea for healthcare cloud-based data security and privacy? IEEE Cloud Comput 2018;5(1): 31–7.
[24] Kuo T-T, Kim H-E, Ohno-Machado L. Blockchain distributed ledger technologies for biomedical and health care applications. J Am Med Inform Assoc 2017;24(6): 1211–20.
[25] Ouaddah A, Elkalam AAbou, Ait Ouahman A. FairAccess: a new Blockchain-based access controlframe work for the Internet of Things. Secur Commun Netw 2016;9 (18):5943–64.
[26] Novo O. Blockchain meets IoT: An architecture for scalable access management in IoT. IEEE Internet of Things J 2018.
[27] Al Omar A, Rahman MS, Basu A, Kiyomoto S. Medibchain: A Blockchain based privacy preserving platform for healthcare data. In: Proceedings of 2017 International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage. Springer; 2017. p. 534–43.
[28] Zhang X, Poslad S. Blockchain support for flexible queries with granular access control to electronic medical records (EMR). In: Proceedings of 2018 IEEE International Conference on Communications (ICC). IEEE; 2018. p. 1–6.
[29] Nakamoto S, Bitcoin A. A peer-to-peer electronic cash system. Bitcoin; 2008. URL, https://bitcoin.org/bitcoin.pdf.
[30] Johnston D, Yilmaz SO, Kandah J, Bentenitis N, Hashemi F, Gross R, Wilkinson S, Mason S. The general theory of decentralized applications, dapps. GitHub; June, 2014.
[31] Liu XLi, Ye L, Zhang H, Du X, Guizani M. BPDS: A Blockchain based privacy-preserving data sharing for electronic medical records. In: 2018 IEEE Global Communications Conference (GLOBECOM); 2018. p. 1–6.
[32] Gupta R, Tanwar S, Tyagi S, Kumar N, Obaidat MS, Sadoun B. Habits: Blockchain-based telesurgery framework for healthcare 4.0. In: 2019 International Conference on Computer, Information and Telecommunication Systems (CITS); 2019. p. 1–5.
[33] Yu Xu, Yang Jing, Xie Zhiqiang. Training SVMs on a bound vectors set based on Fisher projection. Front Comput Sci 2014;8(5):793–806.
[34] 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.
[35] Yu Xu, Chu Yan, Jiang Feng, Guo Ying, Gong Dunwei. SVMs classification based two-side cross domain collaborative filtering by inferring intrinsic user and item features. Knowl-Based Syst 2018;141:80–91.
[36] Uddin MA, Stranieri A, Gondal I, Balasubramanian V. Continuous Patient Monitoring With a Patient Centric Agent: A Block Architecture. IEEE Access 2018; 6:32700–26. https://doi.org/10.1109/ACCESS.2018.2846779.
[37] Ramani V, Kumar T, Bracken A, Liyanage M, Ylianttila M. Secure and efficient data accessibility in blockchain based healthcare systems. In: 2018 IEEE Global

Communications Conference (GLOBECOM); 2018. p. 206–12. https://doi.org/10.1109/GLOCOM.2018.8647221.
[38] Xu J. Healthchain: A Blockchain-Based Privacy Preserving Scheme for Large-Scale Health Data. IEEE Internet of Things J Oct. 2019;6(5):8770–81. https://doi.org/10.1109/JIOT.2019.2923525.
[39] Yu Xu, Jiang Feng, Du Junwei, Gong Dunwei. A cross-domain collaborative filtering algorithm with expanding user and item features via the latent factor space of auxiliary domains. Pattern Recognit 2019;94:96–109.
[40] Alshehri MD, Hussain FK. A fuzzy security protocol for trust management in the internet of things (Fuzzy-IoT). Computing 2019;101(7):791–818.
[41] Nguyen DC, Pathirana PN, Ding M, Seneviratne A. Blockchain for Secure EHRs Sharing of Mobile Cloud Based E-Health Systems. IEEE Access 2019;7:66792–806. https://doi.org/10.1109/ACCESS.2019.2917555.
[42] Elkhodr Mahmoud, Alsinglawi Belal, Alshehri Mohammad. A privacy risk assessment for the Internet of Things in healthcare. Applications of Intelligent Technologies in Healthcare. Cham: Springer; 2019. p. 47–54.
[43] Zheng Z, Xie S, Dai H, Chen X, Wang H. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. In: 2017 IEEE International Congress on Big Data (BigData Congress); 2017. p. 557–64. https://doi.org/10.1109/BigDataCongress.2017.85.