A Robust Blockchain Framework for Healthcare Information System

D. Dharani, K. Anitha Kumari, S. Aishwarya, G. M. Sangavi, N. Lavanya

*Abstract***:** *Nearly every organization needs solution to handle sensitive data. Though there are different systems to store and transmit electronic records, users often deal with missing or tampered information when they distribute it in a public network. When the data is distributed, the traceability and governance of it throughout the globe is impractical. The evolving world of Data Security demands healthcare industry to have an infrastructure in place to deal with patient records. Regardless of the nature of present and future security risks, Blockchain Technology will play a vital role to maintain the originality of the digital data. Blockchain stores data in a decentralized, distributed ledger for achieving immutability and transparency. The system analyses a case study which aims at maintaining Healthcare records in Blockchain ledger to facilitate secure storage of the patient's details. For efficient prediction of diabetes the Blockchain and machine learning algorithms are integrated. The various other applications of combining Blockchain technology with machine learning algorithms are Smart city applications, Forensic information storage systems, Energy data management systems, banking and finance management systems.*

*Keywords***:** *Blockchain, Healthcare records, Diabetes prediction, Machine learning.*

I. INTRODUCTION

The Blockchain is a type of immutable database. It has the ability for individuals to maintain the data and to establish trust. It is a peer to peer network where there is no involvement of central authority [5]. Blockchain holds list of blocks connected using cryptographic hash and the very first block in the Blockchain is called as Genesis block. Each block consists of Block header and list of transactions. These blocks are created by miners. Mining is a method to identify valid block which has to be accepted by all the other nodes of the network. Block header holds previous Block hash, Timestamp, Version, Merkle root hash and Nonce. Merkle tree is the data structure that is an encoded tree representation of the Blockchain transactions. Sequence of blocks forms a ledger that is distributed across several nodes of a Blockchain network. As a consequence, transaction is replicated and stored straight away in several nodes. Thus, Every Transaction of entities in a network is recorded in a distributed ledger which is transparent to every other entity in the network. And so, immutability and security of the data is ensured using Blockchain Technology [12].

D. Dharani*, Information Technology, PSG College of Technology, Coimbatore, India. E-mail: dharani0609@gmail.com

K. Anitha Kumari, Information Technology, PSG College of Technology, Coimbatore, India. E-mail: anitha.psgsoft@gmail.com

S. Aishwarya, Information Technology, PSG College of Technology, Coimbatore, India. E-mail: aishu29december@gmail.com

G. M. Sangavi, Information Technology, PSG College of Technology, Coimbatore, India. E-mail: sangavigm1999@gmail.com

N. Lavanya, Information Technology, PSG College of Technology, Coimbatore, India. E-mail: lavanyakrishnan18071998@gmail.com

Smart contracts are sequence of codes used to perform a particular task in Blockchain network and written commonly using Solidity, Go or Vyper Languages. These tiny programs are stored on every ledger of a Blockchain network and invoked when transaction or the function has to be committed. Consensus algorithm is a mechanism with which all the entities in a Blockchain network agree a common and mutual conformity about the state of the ledger that helps in building trust among the third party network entities. It ensures that whatever the copy which is available to individual entities is consistent and the updated one. There exists different consensus protocols such as, Proof of Work(PoW), Proof of Stake(PoS),Practical Byzantine Fault Tolerance(PBFT), Proof of Burn(PoB), Proof of Elapsed Time(PoET), Proof of Authority(PoA) and so on. Based on the need of an application the consensus mechanisms are chosen [11].

Primarily there are two types of Blockchain Network-Private and Public Blockchain. In a Public Blockchain, Anyone who accesses the internet can be a part of the network. The Proof of Work consensus helps to maintain the trust that there can be no fraud in the transactions. The Private Blockchain is a closed network of well authorized entities. The level of security, authorization and accessibility remains in the control of the enterprise or organization which owns it. A hybrid Blockchain is a flexible and a combination of both private and public Blockchain that enables only selected data records in a network to be allowed to move around public network. For all its intricacy, its potentiality to maintain the records in a decentralized way in a peer to peer network with greater user privacy and keen security, makes this technology suitable for various thriving Distributed Applications (DApps)[3].

II. BLOCKCHAIN IN HEALTHCARE INDUSTRY

Blockchain provides tremendous opportunities to tackle challenges that are exist in healthcare domain. For Maintaining Electronic Medical Records (EMR) the Blockchain Technology can be one of the best solutions [8]. It ensures originality of the patient records. The Blockchain ensures data integrity and privacy of patient in sharing healthcare data. The Blockchain follows the patient-centric healthcare model; the patient has the control over their healthcare data. The Blockchain provides trusting layer behind the patient-centric model [10].

The Blockchain records when used for Clinical Research, the result would be accurate and up to standard. For money transactions like insurance claim and billing also, the Blockchain technology would be a right choice. It helps to bring the patients, providers and the insurers into one network to provide long-time insights to patient's healthcare data and ease in maintaining health claims management. It helps to eliminate major issues such as

duplications in claims, manual errors and pattern identification. The Blockchain provides financial data processing through smart contract and prevent redundancies and inefficiencies in insurance claim management [13].

Drug supply chain management involves transactions of drugs from pharmaceutical companies to pharmacies. The proper monitor and tracking mechanism should be followed in the supply chain to prevent tamper and counterfeit of the drug. The mechanism is used to ensure the end users and all the stakeholders to verify the ingredients of the drug. Incorporating Blockchain in the supply chain would enhance security and transparency among different entities. It helps to track and trace the supply chain where the details be maintained in an open safe and tamper-free system available to multiple parties. The permissioned Blockchain network can be used in the supply chain for the partners to track the pharmaceutical supplies [13].

Prescription management requires proper process to delivery healthcare service. The misuse of the prescription leads to intense problem. The Blockchain based solution provides secure prescription process where all the transactions are stored in the network. The prescription issued by the doctor to a patient is stored in the Blockchain, only the designated pharmacist can provide the drugs based on verification [13].

III. INFERENCES ON SECURED AND TAILORED HEALTHCARE RECORDS

Personal health data received from mobile and wearable technology benefits health care providers and medical research. Providing ownership of data for user-centric healthcare system using decentralized and permissioned storage is one of the noticeable benefits of Blockchain technology. A mobile application is developed to collect health data from wearable devices and physical input are synchronize to the cloud for data sharing between health care providers and health insurance companies. A proof of integrity and legalization is retrievable from cloud platform and is connected to the Blockchain. Hyper ledger Fabric, a permissioned Blockchain used to grant privacy of personal health care systems from the user end to the cloud and also ensures user originality of health data [1].

Blockchain technology provides a way for interoperability challenges present in the healthcare systems and helps individuals, health care entities and healthcare providers to share electronic healthcare data in a secure way. Public Blockchain is used for access-control of healthcare records. It provides scalability, access security and data privacy. Every person in the distributed network of health care Blockchain can have a copy of everyone's record. Since health care data is dynamic and expensive, storing of all records leads to more bandwidth and network utilization. So an index is maintained that stores the details of records such as location and metadata information. With user's unique identification access of the records, the process is made easier [2].

Blockchain is a decentralized protocol that combines transparency and immutability for providing security for the transactions [7]. Smart contracts are built on Blockchain to support on- chain storage and to develop decentralized applications. Patient can access their medical records in real time without any hassle. Decentralized Application (DApps)

provides identification and authentication for patients and health providers. DApps can be developed using Ethereum, which is an open-source Blockchain platform that supports smart contracts. DApps provide services for millions of users by providing scalability, traffic handling mechanisms and provide facility for communication between health care providers [3].

Conventional health system does not provide control access to patients for modification or cancellation of their records. Providers have control over the records and maintain with their premises permanently. If a patient switches to other healthcare providers in their lifetime, the health record of the patient is available to different providers that lead to the data theft and results in lack of security ultimately patient information will be at risk [4]. If patient wants to access the record for modification, it becomes tedious and impossible. To circulate the modified record, the patient have to contact all the providers with whom they have share the record that is considered to be time consuming and tedious. Blockchain gives patients a complete, immutable logs and trouble-free admittance to their medical records across different providers and treatment sites [6].

IV. CASE STUDY- DIABETES PREDICTION USING HEALTHCARE DATA STORED IN BLOCKCHAIN

The case study analyses a straightforward approach which makes sure that the patients retain the ownership of their healthcare data and restrict access of third parties to the data [9]. To ensure security and privacy of data in an efficient manner, Blockchain technology is typically preferred and used. For implementing Blockchain, An Ethereum Blockchain platform is chosen and smart contracts are written in solidity language [15]. The details are shared between doctor and patient for the implementation of Blockchain for healthcare management, without the involvement of any third party systems. The data of the patient is placed on the Blockchain with proper permission from patient.

The goal of the system is to provide secure transfer and to predict diabetes. The blood sugar level obtained from the patient side is sent the doctor side. Only the authorized doctor can have access control over the patients disease related information. Authorization process is carried out with the help of account and deployed addresses that are generated whenever a transaction is recorded. User details are stored in the database for further processing and prediction. Machine learning algorithms like logistic regression, decision tree and random forest are used to check if a patient has diabetes or not. To choose the best algorithm, accuracy, f-measure, precision and recall are used as evaluation metrics for prediction. The system focuses on Blockchain creation, user interface creation, establishing smart contract and prediction of diabetes.

A. User Interface

The user interface is designed in such a way that the patient can have direct access to enter his/her medical information. Individual text boxes are created for entering the necessary patient details regarding diabetes prediction.

The set of text boxes which are developed for easing the user to enter the information includes the following attributes Pregnancies, Glucose, Blood Pressure, Insulin, BMI, Age. Since these attributes are considered to be the key parameters for predicting diabetes, the data has to be filled in a more accurate manner. The patient fills the form based on his/her medical record appropriately. When the user finishes uploading the details, an update button which is designed is enabled. Once the update button is enabled, a smart contract is established and the newly entered patient details will be passed to a function in solidity environment. Since the transactions that happen in smart contract are processed by the Blockchain, there is no third party involved. Hence, the data updated by the patient remains highly secured.

B. Connectivity

The functions in HTML are connected to the functions in solidity through Web3 provider. For the web connection to occur, TestRPC must be running in the background. The TestRPC will be listening on a port number and this will connect the web3 provider to an external Ethereum node. A contract is created and compiled in solidity. The obtained parameters from the user are passed to the solidity function. Solidity has functions for both retrieving and sending the value. The contract created in solidity must be deployed by selecting the requirement environment. The deployed address of the solidity file is added in the HTML program. Thus connection happens. By default, an Application Binary Interface (ABI) is created for the contract created in solidity. ABI is a JavaScript Object Notation (JSON) format of the program that must be added in HTML program. Thus the structure of the contract is understood by HTML program. In solidity, there are default accounts available. New accounts can also be added. Each account in turn has an account address. The particular account address can be assigned in html program. By this way, only the authorized doctors have the way of obtaining information from the patient. If any other person tries to retrieve the content, the address doesn't match and the access is denied.

If the connections are successful, end to end transaction happens. Any middle person couldn't able to intervene and retrieve the contents. The blocks are created by default and transaction details are maintained in the remix IDE. Now the transacted details are displayed in the user interface. These details are inserted in the diabetes dataset for prediction. The obtained value is inserted as a new tuple in the dataset. The dataset already contains many tuples of different patients pertaining to diabetes.

C. Diabetes Prediction

Three classification algorithms are applied over the diabetes dataset and their performance is measured. The algorithms used are random forest, decision tree and logistic regression. Sample portion of the data set collected for the proposed system is shown in Fig.1.

	Pregnancies	Glucose	BloodPressure	Insulin	BMI	Age	Outcome
1							
2	6	148	72	0	33.6	50	1
3	1	85	66	0	26.6	31	0
4	8	183	64	0	23.3	32	1
5	1	89	66	94	28.1	21	0
6	0	137	40	168	43.1	33	1
7	5	116	74	0	25.6	30	0
8	3	78	50	88	31	26	1
9	10	115	0	0	35.3	29	0
10	2	197	70	543	30.5	53	1
11	8	125	96	0	0	54	1
12	4	110	92	0	37.6	30	0
13	10	168	74	0	38	34	1
14	10	139	80	0	27.1	57	0
15	1	189	60	846	30.1	59	1
16	5	166	72	175	25.8	51	1

Fig. 1. Sample dataset

The pima-indians-diabetes-database dataset is considered for the research work from the website kaggle[14]. It consists of 769 rows with features as pregnancies, glucose, blood pressure, skin thickness, insulin, BMI, diabetes, age with 1 outcome.

- *Logistic regression*

Logistic regression belongs to the category of supervised machine learning classification algorithms. For predicting the probability of a categorical dependent variable, logistic regression classification algorithm can be applied. Here, the dependent variable takes either of binary values 0(failure) 1(success). It can directly predict the probabilities that are well-calibrated when compared to other classification algorithms. It belongs to predictive analysis which is mainly focused on the concept of probability. Logistic function is different from linear function as it makes use of more complex cost function known as sigmoid function. This complex cost function can limit the predicted values between the range of 0 and 1 whereas linear regression can have values out of these boundaries. This process is carried out in sigmoid function. This function helps in mapping any real valued number to value between 0 and 1.
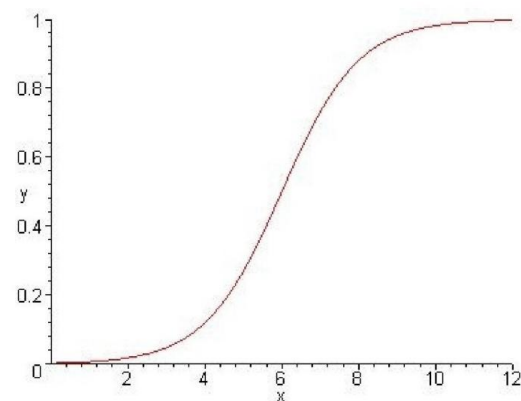

Fig. 2. Logistic regression

Logistic regression measures the relationship between the dependent variable and independent variables by estimating probabilities using the sigmoid function that generates S-curve shown in Fig. 2 that helps in returning a probability value. The types of logistic regression include binomial, multinomial and ordinal. In binomial type, two values 0 and 1 are possible for target variable. In multinomial type, three values are possible for target variable.

Whereas in the case of ordinal type the target variable can take only ordered categories. Confusion matrix is constructed to measure the overall efficiency. Accuracy determines the predicted result is correct to which extent.

- *Decision tree*

It is also a supervised machine learning classification algorithms. It is a flow chart like structure consisting of internal nodes, branches and leaf nodes where the path from root to node represents the classification rules, internal nodes represents the test on an attribute, leaf node represents the class label and branch node represents the outcome of the test. Stability and ease of interpretation is high when compared to other algorithms. It undergoes the following process of breaking down the dataset into smaller and smaller subsets and at the same time a decision tree is built. It has the capability of handling both numerical and categorical data. On a particular variable splits are carried out. Pruning is the main process that is followed to reduce the size of the tree. Overfitting is the main drawback of decision tree and it can be minimized or avoided by combining adjacent nodes that has a very low information gain. Overfitting happens when the data is trained well and the presence of noise in testing data leads to negative impact on performance model. Class label (0/1) for the diabetes dataset is predicted using decision tree algorithm. Each node in the tree acts as a test case for unique attribute, and each edge descending from the node correspond to the possible answers to the test case. This process is recursive in nature and is repeated for every sub tree rooted at the new node. The obtained result at the end contains the decision nodes with the leaf nodes as shown in Fig. 3.
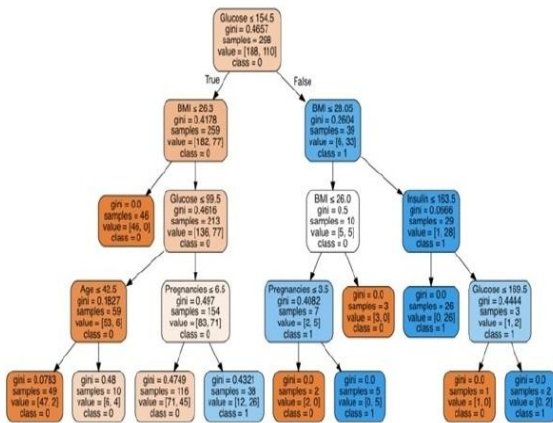

Fig. 3. Decision Tree

- *Random Forest*

Random forest is an ensemble learning method as it consists of various individual decision trees that act as an ensemble. Out of all the predictions provided by the individual decision trees the one with majority turns out to be the model's prediction as depicted in Fig. 4. The main benefit is that the trees protect each other from their individual errors. Out of all selected features there has to be some actual signals so that the model built out of it works perfectly than random guessing.
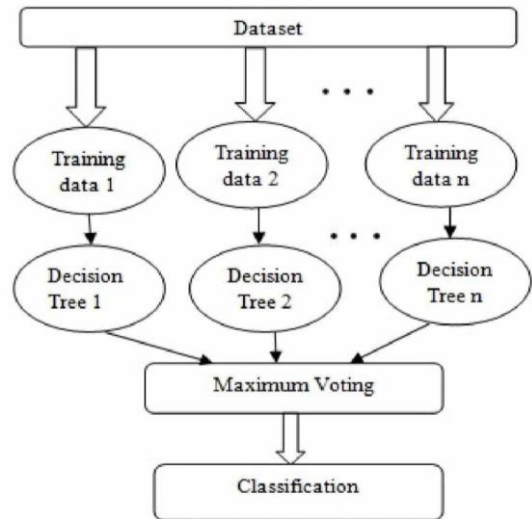

Fig. 4. Random forest

The individual trees provide suitable predictions which have low correlation amongst them. Uncorrelated outcomes help in providing better results. Each decision tree in the random forest generates a class and the class with the most votes becomes the models's final class.
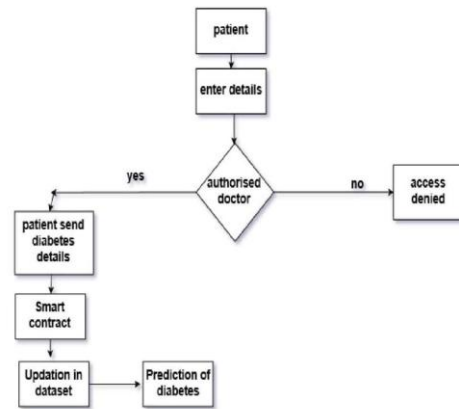

Fig. 5. Flow diagram

Fig. 5 shows the overall structure of the system. Initially, the patient enters the medical details in the webpage. For every transaction, account, address and deployed address are generated. With the help of these parameters, authorization process is carried on and for authorized doctor, transaction of these medical details happen in a secured manner with the help of smart contract. The next step is updating the user data into the dataset. Finally diabetes is predicted by applying the supervised algorithms.

V. PERFORMANCE ANALYSIS

The main goal is to predict whether the user have the chance of prone to diabetes or not. For diabetes dataset, the attributes include pregnancies, glucose, blood pressure, BMI, age and outcome. Precision, recall, f-score and Accuracy are considered as evaluation metrics.

For the dataset considered, precision, recall, f-score and accuracy are measured by applying logistic regression, decision tree and random forest algorithms.

Logistic Regression shows the substantial improvement in the metrics considered when compared to Decision tree and Random forest as shown in Fig. 6 and Table-I. The formula for obtaining evaluation metrics precision, recall, F-score and accuracy are listed below .

$$\text{Precision} = \text{True Positives} / (\text{True Positives} + \text{False Positives}) \qquad (1)$$

$$\text{Recall} = \text{TruePositives} / (\text{TruePositives} + \text{FalseNegatives}) \qquad (2)$$

$$\text{F-Measure} = (2 * \text{Precision} * \text{Recall}) / (\text{Precision} + \text{Recall}) \qquad (3)$$

$$\text{Accuracy} = \text{True Positive} + \text{True Negative} / (\text{True Positive} + \text{False Positive} + \text{False Negative} + \text{True Negative}) \qquad (4)$$

Here true positive and true negative are an outcome where the system correctly predicts the positive and negative cases respectively. False positive predicts as true where it is actually not and false negative predicts as false where it is actually true.

Table- I: Performance analysis of classification algorithms

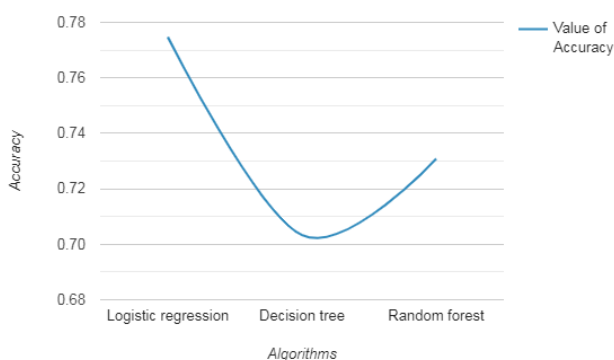| Evaluation metrics	Logistic Regression	Decision Trees	Random Forests
Precision (%)	76	70	73
Recall (%)	76	69	72
F- score (%)	76	69	73

Fig. 6. Accuracy of classification algorithms

VI. CONCLUSION

Conventional healthcare systems are cumbersome for patients to access the health records. Patients often need their health reports for updating purposes. On the other hand, the privacy and security of data is highly at risk. Thus confidential information is greatly at threat as the data can be modified in between and the contents can be tampered. To overcome this problem, a secure network is built where only the authorized doctors and patients are granted access. The proposed system provides transparency and immutability to healthcare documents that can be leveraged to maintain healthcare interoperability. For the better system performance, the machine learning algorithms like logistic regression, decision tree and random forest is incorporated. This leads to faster prediction. The analysis is also made to choose the algorithm that performs best for the diabetes prediction. Current work is used for diabetes prediction in public block chain platform. Future enhancement is to improve the performance on the system and maintain the private block chain on cloud.

REFERENCES

1. Liang X, Zhao J, Shetty S, Liu J, Li D. Integrating blockchain for data sharing and collaboration in mobile healthcare applications. In2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC) 2017 Oct 8 (pp. 1-5). IEEE.
2. Linn LA, Koo MB. Blockchain for health data and its potential use in health it and health care related research. InONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST 2016 (pp. 1-10).
3. Zhang P, Walker MA, White J, Schmidt DC, Lenz G. Metrics for assessing blockchain-based healthcare decentralized apps. In2017 IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom) 2017 Oct 12 (pp. 1-4). IEEE.
4. Ekblaw A, Azaria A, Halamka JD, Lippman A. A Case Study for Blockchain in Healthcare:"MedRec" prototype for electronic health records and medical research data. InProceedings of IEEE open & big data conference 2016 Aug 24 (Vol. 13, p. 13).
5. Al Omar A, Rahman MS, Basu A, Kiyomoto S. Medibchain: A blockchain based privacy preserving platform for healthcare data. InInternational conference on security, privacy and anonymity in computation, communication and storage 2017 Dec 12 (pp. 534-543). Springer, Cham.
6. Azaria A, Ekblaw A, Vieira T, Lippman A. Medrec: Using blockchain for medical data access and permission management. In2016 2nd International Conference on Open and Big Data (OBD) 2016 Aug 22 (pp. 25-30). IEEE.
7. Zhang P, Schmidt DC, White J, Lenz G. Blockchain technology use cases in healthcare. InAdvances in computers 2018 Jan 1 (Vol. 111, pp. 1-41). Elsevier.
8. Esposito C, De Santis A, Tortora G, Chang H, Choo KK. Blockchain: A panacea for healthcare cloud-based data security and privacy?. IEEE Cloud Computing. 2018 Mar 28;5(1):31-7.
9. Kim H, Song H, Lee S, Kim H, Song I. A simple approach to share users' own healthcare data with a mobile phone. In2016 Eighth International Conference on Ubiquitous and Future Networks (ICUFN) 2016 Jul 5 (pp. 453-455). IEEE.
10. Kish LJ, Topol EJ. Unpatients—why patients should own their medical data. Nature biotechnology. 2015 Sep 8;33(9):921.
11. Wang W, Hoang DT, Hu P, Xiong Z, Niyato D, Wang P, Wen Y, Kim DI. A survey on consensus mechanisms and mining strategy management in blockchain networks. IEEE Access. 2019 Jan 30;7:22328-70.
12. Rahman MS, Khalil I, Bouras A. Design Principles for Migrating from Traditional Systems to Blockchain Systems.

Retrieval Number: E9944069520/2020©BEIESP
DOI: 10.35940/ijeat.E9944.069520

1153

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

13. Katuwal GJ, Pandey S, Hennessey M, Lamichhane B. Applications of blockchain in healthcare: current landscape & challenges. arXiv preprint arXiv:1812.02776. 2018 Dec 6.
14. Pima Indians Diabetes Database: https://www.kaggle.com/uciml/pima-indians-diabetes-database. Date accessed: 07/10/2016.
15. Ethereum Project: https://www.ethereum.org/. Date accessed: 08/05/2020.

AUTHORS PROFILE

Dr K Anitha Kumari is working as an Associate Professor in Department of IT in PSG College of Technology, India. She is Highly Passionate and curious about Learning New stuffs in Security Protocols. As an Independent Researcher, she had an Opportunity to present her UGC sponsored paper based on Quantum Cryptography in USA and visited a few Foreign Universities. To her credit, she had filed a PATENT and published around 55 Technical Papers in refereed and Impact Factored International/National Journals/Conferences published by Elsevier, Springer, T&F, etc.,.Also, she's been an Active Reviewer for Prestigious Journals published by IEEE (IEEE Communications Surveys and Tutorials (IF: 20.230), IEEE Transactions on Industrial Informatics (IF: 5.43)), IEEE Access, Springer, Wiley, etc., and Technical Program Committee (TPC) for CECNet 2017, NGCT-2017 WICC-2018 and NCCI-2018 conferences. Her areas of interest include Cloud & IoT Security, Design and Analysis of Security Protocols, Attacks & Defense, Security in Computing, Bioinformatics, Cognitive Security, Quantum Cryptography, Web Service Security, Network Security and Analysis of Algorithms. Out of her research interest, she has contributed book chapters published by T & F, Springer and delivered ample Guest Lectures. Her security project is sanctioned and granted by AICTE for a sum of Rs.11,80,000/-. She's been the mentor for Technovator Projects (2019, 2018 & 2014) and 'MEDROIDZ', an ICICI – Trinity 2014 funded project that was selected as one among the 6 projects in India. She also mentored 5 projects exhibited in NST Fair and AICTE Vishwakrama Award Project. Academically, she has secured RANK-I and awarded Gold Medal in ME (SE) & in BE (CSE) from Anna University and from Avinashilingam University. She secured Elite+Gold Medal (Top 1%) in NPTEL – Cloud Computing course. She also won prizes in intra and inter institutional cultural events. As a Supervisor, she is currently guiding PhD scholars in her research area. Currently she's being the Programme Coordinator for PSG CARE Sponsored One Year Certification Course on Cyber Security. You may contact her at anitha.psgsoft@gmail.com / kak.it@psgtech.ac.in.

Ms D Dharani is working as an Assistant Professor in Department of IT in PSG College of Technology, India. She received her M.Tech degree in Information Technology in the year 2016 and B.Tech degree in Information Technology in the year 2014 from Anna University, India. Currently she is actively attending the PSG CARE Sponsored One Year Certification Course on Data Science. She had also attended many Workshops, FDPs and gained ample knowledge. She is proficient in handling subjects such as Data Analytics, Data structures, Theory of Computing and C Programming. She had guided various students' projects in areas like machine learning, Data analytics and IoT. She had published papers in International/National Journals/Conferences. Her research interest includes areas of Blockchain Technology, Edge Data Analytics and Machine Learning. You may contact her at dharani0609@gmail.com / ddi.it@psgtech.ac.in.

Ms S Aishwarya is a UG Scholar in the Department of Information Technology at PSG College of Technology, India. Her research area includes Blockchain for Healthcare and Machine Learning. She worked in developing the Chatbot for mini project. She did her current work in data security for healthcare.

Ms G M Sangavi is a UG Scholar in the Department of Information Technology at PSG College of Technology, India. She has good technical and analytical skills. Her research area includes Machine Learning, IoT and Data Analytics. Her areas of interests include IoT, Data Security, Cloud Computing and Application Development. She did a project with different innovative ideas and tried to implement in real time basis. She has done project works on areas such as Android Application Development, Machine Learning, Development of chatbots and Data security for healthcare.

Ms N Lavanya is a UG Scholar in the Department of Information Technology at PSG College of Technology, Coimbatore, India. She is a committed student eager to learn new technologies and stuffs. She is enhancing her strategic Planning and management qualities. She is resourceful, innovative and seeking a prospective and challenging opportunity to reveal her potential talents and improve her skills and interests. She has done project works on areas such as Machine learning, artificial intelligence, data analytics and cyber security.