JCBI
Journal of Computing & Biomedical Informatics
ISSN: 2710 - 1606
Volume 07 Issue 01
2024

Research Article
https://doi.org/10.56979/701/2024

Methodology for Ensuring Secure Disease Prediction using Machine Learning Techniques

Aleena Imran[1], Kaleem Razzaq Malik[1], Ali Haider Khan[2], Muhammad Sajid[1*], and Muhammad Arslan[3]

[1]Department of Computer Science, Air University Islamabad, Multan Campus, Multan 60000, Pakistan.
[2]Department of Software Engineering, Faculty of Computer Science, Lahore Garrison University, Lahore, 5400, Punjab, Pakistan.
[3]Department of Information Technology, Faculty of Computer Science, Lahore Garrison University, Lahore, 5400, Punjab, Pakistan.
[*]Corresponding Author: Muhammad Sajid. Email: msajid@aumc.edu.pk

Received: April 11, 2024 **Accepted:** May 19, 2024 **Published:** June 01, 2024

Abstract: In today's digital world, the e-healthcare system has increased the patient data in vast amount. Protecting this confidential patient data from unauthorized access and tampering is crucial as the data contains sensitive details regarding patient's health and any tampering on such details would result in manipulation of patient data which could lead to misdiagnosis and incorrect treatment plans. Conventional healthcare systems lack the ability to secure patient data from unauthorized access which eventually leads to data tampering and data loss. Data security and data privacy are crucial components within the healthcare sector and can be enhanced by the utilization of blockchain framework. Within the healthcare domain, disease identification and prediction is also a critical challenge. This study focuses on disease detection and prediction such as diabetes mellitus and blood pressure by implementing ML models such as Decision Tree, SVM, KNN, Naive Bayes, Random Forest and ensemble learning while maintaining the integrity of patient sensitive health data. The diagnostic results predicted by classifier and new patient data have been stored on smart contracts. Only authorized persons such as healthcare professionals can have access to patient sensitive health related data and diagnostic results predicted by the classifier. The research aims to enhance the efficiency of machine learning classifiers along with data integrity.

Keywords: Blockchain; Healthcare; Machine Learning; Prediction; Diseases; Blood Pressure; Diabetes; Classification.

1. Introduction

Blockchain technology, a distributed ledger, comprises of distinct attributes, such as immutability, decentralization, immutable data, traceability, and transparency [1], [2], [3]. The integrity and security of transactions occurring on blockchain network can be guaranteed by implementing consensus algorithms on individual nodes [4]. Trust is the essential attribute of blockchain that is attained by eliminating access of unauthorized or third parties. Moreover, the smart contract, a coded script, is the fundamental element of blockchain technology. Complex access control strategies can be enabled by the integration of mart contracts in a system, thereby guaranteeing the efficient security of data storage and adherence to access regulations [5]. Individuals do not have to rely upon dependable intermediaries and possess the capacity to independently manage their personal information [6]. The adoption of blockchain technology is increasing significantly in various sectors like government, healthcare, finance, and industry, offering the potential for a secure digital future [7]. Out of all these applications, healthcare holds the utmost significance as it is a fundamental requirement for human existence [8]. Within the healthcare sector, some

weaknesses and inefficiencies present hazards to the security of patient data, such as unlawful entry into confidential information. Potential data breaches or leaks can have severe consequences for patients.

Significant advancements in healthcare encompass disease prognosis and patient monitoring for specific ailments, utilizing diverse symptoms collected from many Internets of Things (IoT) devices. Therefore, a massive data repository is necessary to store the immense volume of data produced [9]. IoT devices have the objective of collecting health-sensitive data, analyzing the information, and sharing high-priority sensitive data [10]. IoT devices utilized in healthcare applications [11] are responsible for managing data that necessitates safeguarding measures to ensure confidentiality and privacy. The centralized nature of the underlying architecture of the Internet of Things (IoT) gives rise to significant concerns regarding the security and confidentiality of data. The traditional cryptographic method of providing security poses risks to sensitive healthcare data. Therefore, there is a need for a decentralized approach to ensuring security. In addressing the complexities related to decentralization of security and integration, the potential of blockchain technology is considerable. The utilization of blockchain technology offers significant advantages by cyphering stored data and signing each block digitally, ensuring an elevated degree of reliability. Blockchain technology is perfect for applications that are distributed in nature facilitating accurate monitoring of operations and requisite the reliability of crucial data [12].

The prediction of diseases within the healthcare sector is a major challenge. Diabetes, hypertension, stroke, Alzheimer's disease, etc. are chronic illnesses that are persistent and endured for a prolonged duration and do not possess a permanent cure. Within this category, one of the most common and swiftly increasing fatal ailments is blood pressure and diabetes mellitus [8]. The timely diagnosis and appropriate treatment at the early stages of blood pressure and diabetes mellitus can save the lives of individuals and decrease the mortality ratio caused by these diseases [13], [14]. Recently, due to the ability of smarter decision-making through the analysis of large and complex data, intelligent approaches comprising Machine Learning, Deep Learning and Cloud assisted techniques have gained much popularity for the prediction of diseases such as blood pressure and diabetes Mellitus. [8]. Predicted diagnostic outcomes may contain confidential details regarding a patient's health. The implementation of security measures to safeguard patient’s confidential data ensures the maintenance of individuals' privacy and mitigates the risk of illegal dissemination of personal health information.

Nowadays, safeguarding confidential health data is of utmost significance in the digitally connected world. The secure storage and transfer of predicted diagnostic outcomes keep data secure and immutable. Any unauthorized access or modifications could lead to changes in personal health information which could result in misdiagnoses and incorrect treatment plans. Scalability, flexibility, availability, and security are some challenges faced by machine learning (ML) and deep learning (DL) approaches [8]. It is vitally important to prioritize data security and privacy which are essential components when developing machine-learning models for medical diagnoses and treatment plans. Prior studies have implemented cloud-based healthcare data-sharing methods [15] to attain this goal, providing benefits such as adaptability, expandability, safety, and cost-efficiency through operational depersonalization and data encryption. Nevertheless, the users’ exhibit reluctance in transferring their data to the cloud due to the sensitivity and privacy concerns associated with the patient's data. To address the limitations of prior methodologies, it is imperative to establish a robust and compatible system that ensures security. Additionally, it is crucial to devise an effective and adaptable architecture that effectively addresses the aforementioned challenges. Blockchain possesses the capacity to partially or completely overcome the security concerns encountered by patients and healthcare institutions [16], [17], [18], [19].

The remaining sections of this proposed study are structured as follows. Related work is given in Section 2. The proposed methodology is covered in Section 3, and experimental results are covered in Section 4. Section 5 concludes the paper.

2. Related Work

Data security and privacy are crucial factors that necessitate careful consideration in the development of machine-learning algorithms for medical diagnostics within the healthcare domain. Potential data breaches or leaks might have significant repercussions for both patients and healthcare providers. This section examines the numerous research that has been undertaken to safeguard sensitive health-related

data. An approach for predicting cardiac disease using a machine learning-based model which is Sine Cosine Weighted K-Nearest Neighbor (SCA_WKNN) is presented in the work by Hasanova et al. [12]. Data stored on tamper-resistant blockchain network is used to train the applied model. The SCA_WKNN model outperforms WKNN and K-NN. Similarly, in another study by Shynu et al. [20] in which diabetes and heart diseases have been predicted and identified by utilizing a secure blockchain-enabled healthcare service in fog computing. The health-related information is first collected from fog nodes and is stored in blockchain. For clustering patient records, a novel rule-based clustering technique is utilized. Feature selection based adaptive neuro-fuzzy inference system (FS-ANFIS) is implemented to detect diabetes and heart diseases.

Additionally, another study proposed by Mantey et al. [22] offers a technique that protects patients' private information while enabling them to receive customized treatment alerts. In this work, 1,000 products from the Internet of Medical Things (IoMT) and a dataset of 50 patients with 13 attributes are analyzed using machine and deep learning approaches. Furthermore, Wang et al. [21] provide a blockchain-based safe medical data management system for telemedicine. The system addresses problems associated with unrestricted sharing and low data trust. The system design consists of a three-tier framework comprised of immediate patient monitoring, block storage, and smart contract negotiation for security. The system also utilizes extendable machine-learning approaches for disease identification. The suggested methodology outperforms in patient disease prediction and safety data management of telemedicine. Another study introduced by Ali et al. [23] offers a unique permission-based blockchain infrastructure intended to improve healthcare system security. This system uses hybrid deep learning approaches to provide instantaneous evaluation, secure flexible data sharing, instant medical detection, and prediction of illnesses.

Additionally, in one study where Neelakandan et al. [24] applied BDL-SMDTD algorithm to securely transfer medical images and to predict diseases accurately. The study also utilizes a blockchain approach for the storage and transfer of medical related data securely. For data encryption, moth flame optimization along with elliptic curve cryptographic technique have been applied. For segmentation, histogram approach have been utilized, SVM have been used for disease classification and for feature extraction, and Resnet-v2 along with Inception model have been implemented. Work conducted by Juneja and Marefat [25] utilizes Blockchain technology to securely store and retrieve the necessary data for the classifier. This study utilizes the MIT-BIH Arrhythmia database to detect Ventricular Ectopic Beats (VEB) and Supraventricular Ectopic Beats (SVEB). The Ethereum sandbox simulation architecture employed in a separate study by Subramanian & Sreekantan Thampy [2] ensures the security of healthcare records for diabetic patients by utilizing the interplanetary file system (IPFS). The NEM symbol blockchain is employed by a consortium for proof-of-concept. The diabetes blockchain application is operated by a smart contract, while users are safeguarded using attribute-based encryption. The consolidation of transactions and blocks enhances both the velocity and effectiveness.

The study conducted by Kumar et al. [26] examines the phenomenon of model transfer between users and companies through the utilization of federated learning methodologies. The objective is to mitigate privacy concerns and disruptions arising from the centralized flow of information. The model undergoes training and is thereafter distributed across users and volunteered organizations, wherein tokens are granted to clients as a form of recognition for their contributions. The federation process was evaluated using the COVID-19. The healthcare industry is experiencing a growing volume of electronic health records (EHRs), posing challenges in maintaining data security and optimizing diagnostic procedures. In their recent publication, Sammeta and Parthiban [27] introduce a novel model called Hyper ledger blockchain-enabled secure medical data management with deep learning-based diagnosis (HBESDM-DLD). This model encompasses several components such as encryption, optimal key generation, and diagnosis. The proposed approach facilitates user control over access, enables hospital authorities to do data read and write operations, and notifies emergency contacts. The system employs a multi-channel hyper ledger blockchain to store and exchange data, together with a diagnostic model based on variational auto encoders for detecting diseases.

Table 1. Related Studies

Ref.	Title	Methodology	Limitation
Kumar et al. (2023)	Securing health care data through blockchain enabled collaborative machine learning	The paper examines the phenomenon of model transfer between users and companies through the utilization of federated learning methodologies. The objective is to mitigate privacy concerns and disruptions arising from the centralized flow of information. The model undergoes training and is thereafter distributed across users and volunteered organizations, wherein tokens are granted to clients as a form of recognition for their contributions. The federation process was evaluated using the COVID-19.	Blockchain technology is employed to enable the sharing of machine learning models between relevant parties.
Ali et al. (2023)	Blockchain-Powered Healthcare Systems: Enhancing Scalability and Security with Hybrid Deep Learning	The cluster head receives the IoT data that have been gathered from the sensors then the blockchain-based data transaction happens. The next stage is outsourcing the encryption of data to the cloud via homomorphic encryption. The next stage in their suggested architecture is feature extraction. Additionally, the suggested architecture makes use of Support Vector Machines (SVM) to categorize individuals and data according to their traits and interactions with the system. Finally, a validation model is used to verify and validate the result.	After encryption, information is transferred to the cloud for further processing.
Hasanova et al. (2022)	A novel blockchain-enabled heart disease prediction mechanism using machine learning.	The paper presents a novel approach for predicting cardiac disease using ML-based SCA_WKNN (Sine Cosine Weighted K-Nearest Neighbour) model. tamper-resistant blockchain data is utilized to train the model.	
Wang et al. (2022)	Blockchain-based Secure Medical Data Management and Disease Prediction.	In this paper, medical records are stored on blockchain which is then used by classifier for disease prediction.	
Subramanian et al.	Implementation of Blockchain	Healthcare data of patients with diabetes are secured using the	

(2021)	Consortium to Prioritize Diabetes Patients' Healthcare in Pandemic Situations	Ethereum sandbox simulation framework.	Patient Dataset is stored on blockchain.
Shynu et al. (2021)	Blockchain-Based Secure Healthcare Application for Diabetic-Cardio Disease Prediction in Fog Computing	The patient's health data is first gathered from fog nodes and saved on a blockchain. The patient health records are then aggregated using the innovative rule-based clustering technique. Finally, a feature selection-based adaptive neuro-fuzzy inference system (FS-ANFIS) is used to forecast the onset of cardiovascular and diabetes illnesses.	
Juneja et al. (2018)	Leveraging Blockchain for Retraining Deep Learning Architecture in Patient-Specific Arrhythmia Classification	Blockchain is utilized to safely access and store the data that the classifier needs. The MIT-BIH Arrhythmia dataset is utilized in this work, and the findings indicate improved accuracy for both supraventricular and ventricular ectopic beats (SVEB) and ventricular ectopic beats (VEB).	

All of the aforementioned studies as shown in table 1, utilize blockchain technology to store datasets for disease prediction by classifiers, employing blockchain technology to enable the sharing of machine learning models between relevant parties and utilizing blockchain technology to facilitate the data exchanges which is then sent to the cloud for additional processing after being encrypted. However, none of the above-mentioned studies are storing predicted diagnostic results on blockchain, which also contain sensitive information about patients' health. Additionally, no studies have been conducted to store new patient data on blockchain for the purpose of predicting the presence of specific diseases. In order to ensure data security and integrity, it is imperative to develop a system that can securely store both projected diagnostic results and new patient data on a blockchain platform.

3. Materials and Methods

This section explains the proposed system methodology in which blockchain technology has been integrated with machine learning models for disease prediction such as diabetes mellitus and blood pressure while ensuring data integrity and data security in the healthcare sector. The predicted outcomes and newly acquired patient data will be securely stored within a blockchain network, as depicted in Figure 1.

3.1. Data Acquisition

Machine learning has been employed to forecast diseases using two datasets, Diabetes and Blood Pressure. The dataset on diabetes comprises a total of 768 records, each including 8 numeric parameters. The dataset on blood pressure has 2000 records, each containing 10 numeric variables. Either of the datasets was acquired via kaggle.

3.2. Data Preprocessing

Multiple pre-processing techniques have been implemented on both datasets which will be elaborated upon individually.

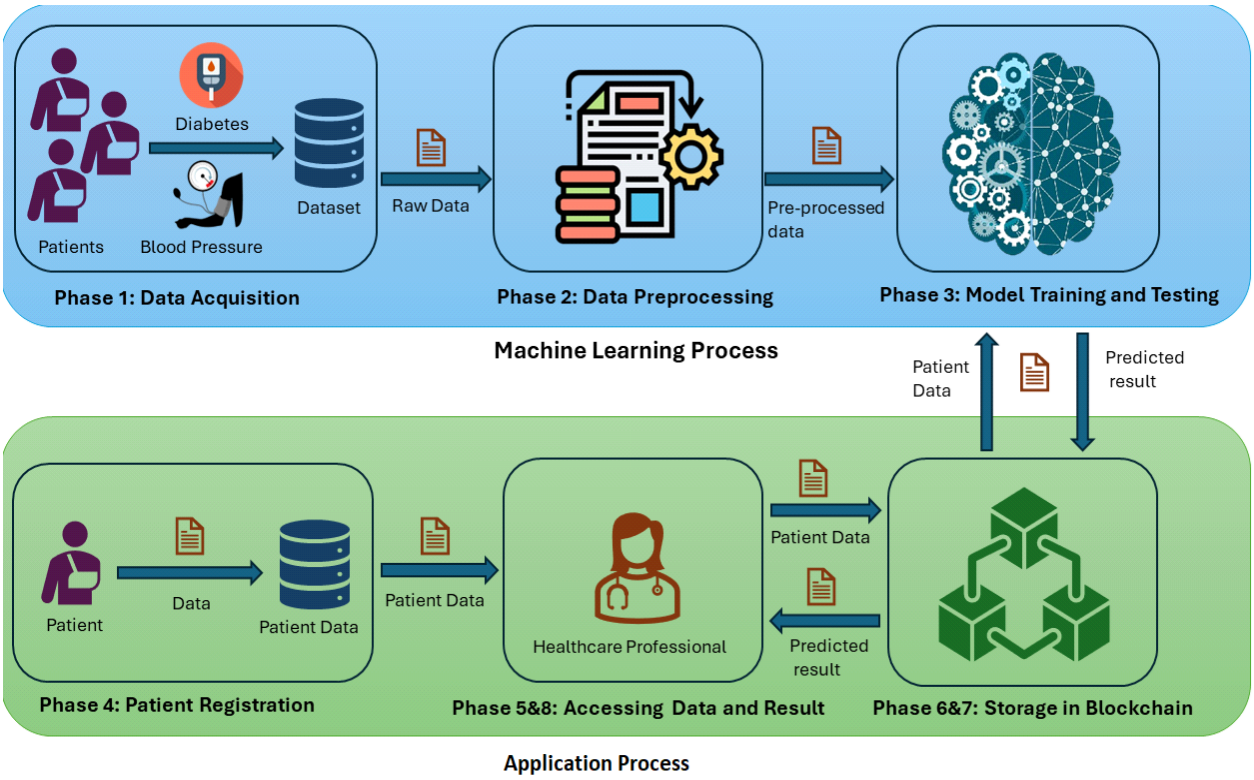

Figure 1. Proposed System Model

The proposed system model contains the following phases which are explained in detail below:

3.2.1. Diabetes Mellitus Dataset

The dataset was carefully examined to identify any missing values, duplicates, and outliers to maintain the integrity of the data. The dataset does not contain any missing values, duplicates, and outliers. The dataset was imbalanced in which 268 instances were classified as positive (class 1) and 500 records were classified as negative (class 0) for diabetes. Synthetic Minority Oversampling Technique have been applied to overcome this issue. SMOTE produces synthetic samples by considering minority class and balances the class distribution efficiently. The size of the dataset was also increased by applying SMOTE and then given to classifier for blood pressure prediction and identification.

3.2.2. Blood Pressure Dataset

The initial step involved in the preprocessing phase of the blood pressure dataset is to address any missing values, duplicates and outliers. Missing values were identified in the dataset and resolved by applying the straightforward technique in which missing values were replaced with average values of their corresponding attributes. The approach effectively addressed the problem of missing values in the dataset while maintaining the integrity of the data. Furthermore, the dataset was augmented by producing new synthetic samples with the help of the SMOTE technique to ensure the equitable representation of both positive and negative samples. The pre-processed dataset given to ML models provide a robust platform for accurate blood pressure detection.

3.3. Machine Learning Phase

In this phase, both the datasets (diabetes mellitus and blood pressure) were split into training and testing sets having a split ratio of 70-30. 70% of the data were being utilized for the training purpose of the machine learning models and 30% of the data was reserved for the model performance evaluation. Various Machine learning models were trained during the training phase for the disease prediction. Random Forest, Naïve Bayes, ANN, KNN, SVM and decision tree were employed during the training phase for blood pressure detection. Likewise, for diabetes mellitus detection, KNN, Random Forest, Decision Tree, ANN, Naïve Bayes, XGBoost, and ensemble learning approaches were utilized. Performance evaluation metrics such as accuracy, precision, recall, and F1- score were assessed to evaluate the performance of machine learning approaches.

3.4. Patient Registration

Patients will register by providing their personal and medical information upon arrival at the hospital. This will facilitate hospital systems in the creation of a massive amount of electronic health records which will later be used for the diagnosis of diseases such as diabetes mellitus and blood pressure. The patient registration phase will assist healthcare professionals in accessing patient information for decision-making on a particular disease.

3.5. Accessing Patient Data

During this phase, healthcare professionals will access patient data from the hospital's database. The patient data consisting of patient private, and health related information is then stored on smart contracts which are implemented on Ethereum blockchain for the security and integrity of patient data. From blockchain, the patient private and health related data is transferred to ML classifier for disease identification and prediction for the diagnosis of blood pressure and diabetes mellitus. In order to protect data form unauthorized access, access control mechanisms have been implemented in smart contracts which will allow only healthcare practitioners to access patient data.

3.6. Accessing Diagnostic Results

During this phase, the diagnostic outcomes predicted by ML classifiers are accessed and stored on smart contracts by the utilization of web3.py for the integrity and confidentiality of patient data as the outcomes contains sensitive information and any tampering may result in misdiagnosis and incorrect treatment plan. Smart contracts contains access control strategies allowing only healthcare practitioners to gain access on patient data. After gaining access on diagnostic outcomes, healthcare professionals will diagnose and provide proper treatments to patients**.**

4. Results and Discussion

Experimental evaluation has been done in this section in which ML model results of both disease datasets such as diabetes mellitus and blood pressure have been evaluated by using performance evaluation metrics such as accuracy, precision, recall, and F1-score. The blockchain technology integrated along with ML approach have also been evaluated. Section 4.1 evaluates ML model performance and blockchain integration have been evaluated in section 4.2.

4.1. Machine Learning Model Evaluation

Diabetes Mellitus and Blood pressure dataset's model performances have been evaluated separately.

4.1.1. Diabetes Mellitus

Various machine-learning models have been utilized on the diabetes dataset. The models evaluated included Random Forest, Decision Tree, SVM, KNN, Naïve Bayes, ANN (MLP), Xgboost, and Ensemble model. The experimental results are summarized in Table 2 and Figure 2.

Table 2. Model Accuracies for Diabetes Dataset

Model	Accuracy	Precision	Recall	F1-measure
Random forest	0.96	0.96	0.96	0.96
Decision Tree	0.90	0.90	0.90	0.90
SVM	0.76	0.76	0.76	0.76
KNN	0.96	0.96	0.96	0.96
Naïve Bayes	0.75	0.75	0.75	0.75
ANN (MLP)	0.76	0.77	0.76	0.76
Xgboost	0.95	0.96	0.95	0.95
Ensemble model	0.968	0.97	0.97	0.97

The Ensemble model demonstrated the highest accuracy of 0.968 in the diabetes dataset, closely followed by the Random Forest model with an accuracy of 0.96. The results suggest that the Ensemble model outperforms the individual models in accurately forecasting diabetes outcomes.

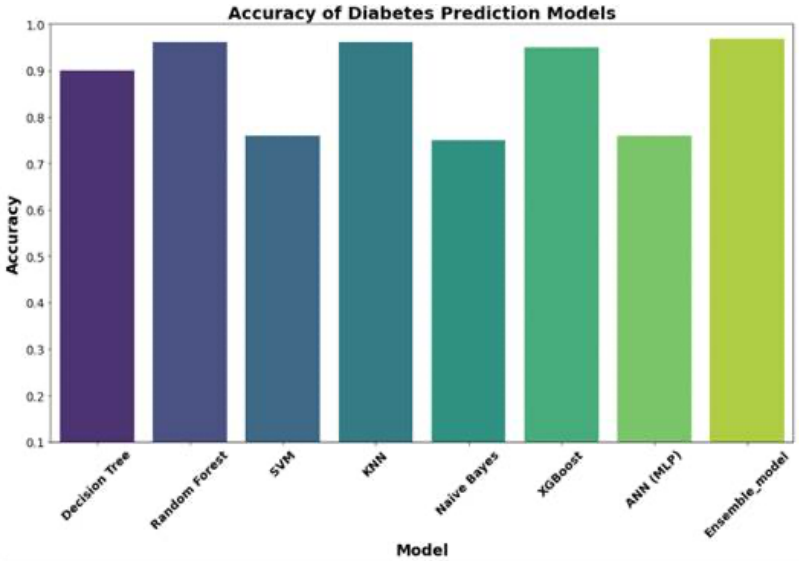

Figure 2. Model Accuracies for Diabetes Dataset

4.1.2. Blood Pressure Dataset

Similarly, different machine-learning models have been applied to the blood pressure dataset. The models included are Random Forest, Decision Tree, SVM, KNN, Naïve Bayes, and ANN (MLP). Table 3 and Figure 3 summarizes the experimental results as shown below:

Table 3. Model Accuracies for Blood Pressure Dataset

Model	Accuracy	Precision	Recall	F1-measure
Random forest	0.86	0.86	0.86	0.86
Decision Tree	0.79	0.79	0.79	0.79
SVM	0.53	0.53	0.53	0.52
KNN	0.72	0.72	0.72	0.72
Naïve Bayes	0.68	0.71	0.68	0.67
ANN (MLP)	0.52	0.52	0.52	0.52

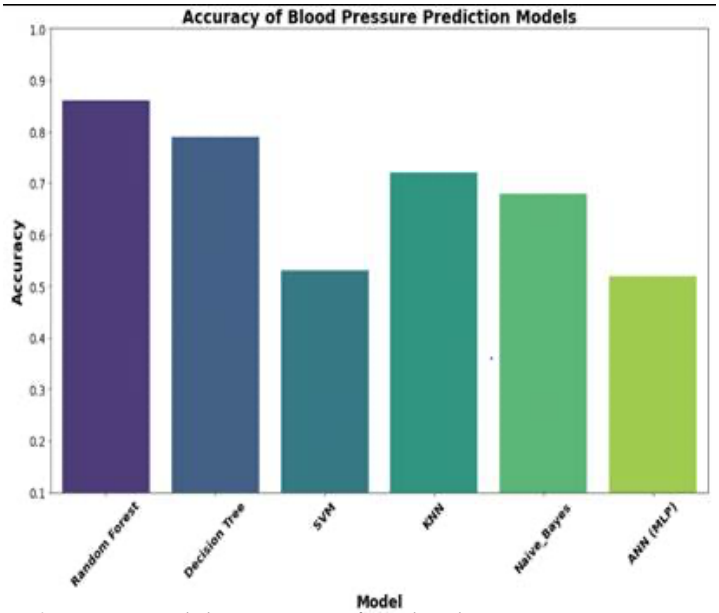

Figure 3. Model Accuracies for Blood Pressure Dataset

From figure 3 and table 3, it has been shown that Random Forest classifier outperforms well in predicting blood pressure disease with an accuracy of 0.98.

4.2. Blockchain Integration

Blockchain technology was incorporated into the study framework to ensure safe data storage and retrieval, in addition to model training and testing. Remix was utilized to create and deploy smart

contracts, which enabled the storage of predicted diagnostic outcomes on the blockchain network. The integration of blockchain was evaluated using a local Ethereum blockchain framework named Ganache. The predicted diagnostic results were successfully and securely stored on the blockchain network. Web3.py was implemented successfully in Jupiter Notebook to interact with smart contracts deployed on Remix to securely store and access predicted diagnostic results.

5. Conclusion and Future work

This paper introduces a methodology for ensuring a secure disease prediction such as Diabetes Mellitus and Blood Pressure detection using machine learning techniques. Various machine-learning algorithms such as Random Forest, Decision Tree, KNN, Naïve Bayes, ANN and ensemble learning have been employed on diabetes and blood pressure datasets and evaluated using performance evaluation metrics such as accuracy, precision, recall and F1-score. The ensemble learning outperforms well for Diabetes Mellitus prediction and Random Forest shows the highest accuracy for Blood Pressure Detection. Furthermore, Blockchain technology has been integrated for secure storage and transmission of predicted diagnostic outcomes and newly acquired patient data which ensures data integrity, immutability, and transparency. Data privacy and security concerns have been addressed in this research by leveraging blockchain technology, especially in the healthcare domain. The proposed integration of blockchain technology has shown remarkable results in enhancing the privacy and security of patient data.

References

1. B. S. Egala, A. K. Pradhan, V. Badarla, and S. P. Mohanty, "Fortified-Chain: A Blockchain-Based Framework for Security and Privacy-Assured Internet of Medical Things with Effective Access Control," IEEE Internet Things J, vol. 8, no. 14, pp. 11717–11731, Jul. 2021, doi: 10.1109/JIOT.2021.3058946.
2. G. Subramanian and A. Sreekantan Thampy, "Implementation of Blockchain Consortium to Prioritize Diabetes Patients' Healthcare in Pandemic Situations," IEEE Access, vol. 9, pp. 162459–162475, 2021, doi: 10.1109/ACCESS.2021.3132302.
3. P. P. Ray, Di. Dash, K. Salah, and N. Kumar, "Blockchain for IoT-Based Healthcare: Background, Consensus, Platforms, and Use Cases," IEEE Syst J, vol. 15, no. 1, pp. 85–94, Mar. 2021, doi: 10.1109/JSYST.2020.2963840.
4. T. T. Kuo, H. E. Kim, and L. Ohno-Machado, "Blockchain distributed ledger technologies for biomedical and health care applications," J Am Med Inform Assoc, vol. 24, no. 6, pp. 1211–1220, Nov. 2017, doi: 10.1093/JAMIA/OCX068.
5. S. Parthasarathy, A. Harikrishnan, G. Narayanan, J. J. Lohith, and K. Singh, "Secure Distributed Medical Record Storage using Blockchain and Emergency Sharing Using Multi-Party Computation," 2021 11th IFIP International Conference on New Technologies, Mobility and Security, NTMS 2021, Apr. 2021, doi: 10.1109/NTMS49979.2021.9432643.
6. J. Xu et al., "Healthchain: A Blockchain-Based Privacy Preserving Scheme for Large-Scale Health Data," IEEE Internet Things J, vol. 6, no. 5, pp. 8770–8781, Oct. 2019, doi: 10.1109/JIOT.2019.2923525.
7. X. Zhang and S. Poslad, "Blockchain Support for Flexible Queries with Granular Access Control to Electronic Medical Records (EMR)," IEEE International Conference on Communications, vol. 2018-May, Jul. 2018, doi: 10.1109/ICC.2018.8422883.
8. M. Chen et al., "Blockchain-Enabled healthcare system for detection of diabetes," Journal of Information Security and Applications, vol. 58, p. 102771, May 2021, doi: 10.1016/J.JISA.2021.102771.
9. R. Arul, R. Alroobaea, U. Tariq, A. H. Almulihi, F. S. Alharithi, and U. Shoaib, "IoT-enabled healthcare systems using block chain-dependent adaptable services," Pers Ubiquitous Comput, vol. 28, no. 1, pp. 43–57, Feb. 2024, doi: 10.1007/S00779-021-01584-7.
10. F. Alkurdi, I. Elgendi, K. S. Munasinghe, D. Sharma, and A. Jamalipour, "Blockchain in IoT Security: A Survey," 2018 28th International Telecommunication Networks and Applications Conference, ITNAC 2018, Jul. 2018, doi: 10.1109/ATNAC.2018.8615409.
11. R. Cao, Z. Tang, C. Liu, and B. Veeravalli, "A Scalable Multicloud Storage Architecture for Cloud-Supported Medical Internet of Things," IEEE Internet Things J, vol. 7, no. 3, pp. 1641–1654, Mar. 2020, doi: 10.1109/JIOT.2019.2946296.
12. H. Hasanova, M. Tufail, U. J. Baek, J. T. Park, and M. S. Kim, "A novel blockchain-enabled heart disease prediction mechanism using machine learning," Computers and Electrical Engineering, vol. 101, p. 108086, Jul. 2022, doi: 10.1016/J.COMPELECENG.2022.108086.
13. R. Krumkamp et al., "Health care utilization and symptom severity in Ghanaian children--a cross-sectional study," PLoS One, vol. 8, no. 11, Nov. 2013, doi: 10.1371/JOURNAL.PONE.0080598.
14. D. Kadobera, B. Sartorius, H. Masanja, A. Mathew, and P. Waiswa, "The effect of distance to formal health facility on childhood mortality in rural Tanzania, 2005–2007," Glob Health Action, vol. 5, pp. 1–9, 2012, doi: 10.3402/GHA.V5I0.19099.
15. X. Liu, Z. Wang, C. Jin, F. Li, and G. Li, "A Blockchain-Based Medical Data Sharing and Protection Scheme," IEEE Access, vol. 7, pp. 118943–118953, 2019, doi: 10.1109/ACCESS.2019.2937685.
16. K. H. Franke et al., "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 Inform Decis Mak, vol. 18, no. 1, pp. 1–10, Mar. 2018, doi: 10.1186/S12911-018-0600-3/TABLES/4.
17. H. Guo, W. Li, M. Nejad, and C. C. Shen, "Access control for electronic health records with hybrid blockchain-edge architecture," Proceedings - 2019 2nd IEEE International Conference on Blockchain, Blockchain 2019, pp. 44–51, Jul. 2019, doi: 10.1109/BLOCKCHAIN.2019.00015.
18. R. Gupta, S. Tanwar, S. Tyagi, N. Kumar, M. S. Obaidat, and B. Sadoun, "HaBiTs: Blockchain-based telesurgery framework for healthcare 4.0," CITS 2019 - Proceeding of the 2019 International Conference on Computer, Information and Telecommunication Systems, Aug. 2019, doi: 10.1109/CITS.2019.8862127.
19. J. Liu, X. Li, L. Ye, H. Zhang, X. Du, and M. Guizani, "BPDS: A Blockchain Based Privacy-Preserving Data Sharing for Electronic Medical Records," Proceedings - IEEE Global Communications Conference, GLOBECOM, 2018, doi: 10.1109/GLOCOM.2018.8647713.
20. P. G. Shynu, V. G. Menon, R. L. Kumar, S. Kadry, and Y. Nam, "Blockchain-Based Secure Healthcare Application for Diabetic-Cardio Disease Prediction in Fog Computing," IEEE Access, vol. 9, pp. 45706–45720, 2021, doi: 10.1109/ACCESS.2021.3065440.
21. X. Wang, Y. Lu, Y. Wang, and W. B. Chen, "Diabetic retinopathy stage classification using convolutional neural networks," Proceedings - 2018 IEEE 19th International Conference on Information Reuse and Integration for Data Science, IRI 2018, pp. 465–471, Aug. 2018, doi: 10.1109/IRI.2018.00074.
22. E. A. Mantey, C. Zhou, J. H. Anajemba, I. M. Okpalaoguchi, and O. D. M. Chiadika, "Blockchain-Secured Recommender System for Special Need Patients Using Deep Learning," Front Public Health, vol. 9, p. 737269, Sep. 2021, doi: 10.3389/FPUBH.2021.737269/BIBTEX.
23. A. Ali et al., "Blockchain-Powered Healthcare Systems: Enhancing Scalability and Security with Hybrid Deep Learning," Sensors 2023, Vol. 23, Page 7740, vol. 23, no. 18, p. 7740, Sep. 2023, doi: 10.3390/S23187740.

24. S. Neelakandan, J. Rene Beulah, L. Prathiba, G. L. N. Murthy, E. Fantin Irudaya Raj, and N. Arulkumar, "Blockchain with deep learning-enabled secure healthcare data transmission and diagnostic model," https://doi.org/10.1142/S1793962322410069, vol. 13, no. 4, Jan. 2022, doi: 10.1142/S1793962322410069.
25. A. Juneja and M. Marefat, "Leveraging blockchain for retraining deep learning architecture in patient-specific arrhythmia classification," 2018 IEEE EMBS International Conference on Biomedical and Health Informatics, BHI 2018, vol. 2018-January, pp. 393–397, Apr. 2018, doi: 10.1109/BHI.2018.8333451.
26. C. U. Om Kumar, S. Gajendran, V. Balaji, A. Nhaveen, and S. Sai Balakrishnan, "Securing health care data through blockchain enabled collaborative machine learning," Soft comput, vol. 27, no. 14, pp. 9941–9954, Jul. 2023, doi: 10.1007/S00500-023-08330-6.
27. N. Sammeta and L. Parthiban, "Hyperledger blockchain enabled secure medical record management with deep learning-based diagnosis model," Complex and Intelligent Systems, vol. 8, no. 1, pp. 625–640, Feb. 2022, doi: 10.1007/S40747-021-00549-W/FIGURES/10.