electronics

MDPI

Article

Diabetic Retinopathy Detection: A Blockchain and African Vulture Optimization Algorithm-Based Deep Learning Framework

Posham Uppamma and Sweta Bhattacharya *

School of Information Technology and Engineering, Vellore Institute of Technology, Vellore 632014, Tamil Nadu, India
* Correspondence: sweta.b@vit.ac.in

Abstract: Blockchain technology has gained immense momentum in the present era of information and digitalization and is likely to gain extreme popularity among the next generation, with diversified applications that spread far beyond cryptocurrencies and bitcoin. The application of blockchain technology is prominently observed in various spheres of social life, such as government administration, industries, healthcare, finance, and various other domains. In healthcare, the role of blockchain technology can be visualized in data-sharing, allowing users to choose specific data and control data access based on user type, which are extremely important for the maintenance of Electronic Health Records (EHRs). Machine learning and blockchain are two distinct technical fields: machine learning deals with data analysis and prediction, whereas blockchain emphasizes maintaining data security. The amalgamation of these two concepts can achieve prediction results from authentic datasets without compromising integrity. Such predictions have the additional advantage of enhanced trust in comparison to the application of machine learning algorithms alone. In this paper, we focused on data pertinent to diabetic retinopathy disease and its prediction. Diabetic retinopathy is a chronic disease caused by diabetes and leads to complete blindness. The disease requires early diagnosis to reduce the chances of vision loss. The dataset used is a publicly available dataset collected from the IEEE data port. The data were pre-processed using the median filtering technique and lesion segmentation was performed on the image data. These data were further subjected to the Taylor African Vulture Optimization (AVO) algorithm for hyper-parameter tuning, and then the most significant features were fed into the SqueezeNet classifier, which predicted the occurrence of diabetic retinopathy (DR) disease. The final output was saved in the blockchain architecture, which was accessed by the EHR manager, ensuring authorized access to the prediction results and related patient information. The results of the classifier were compared with those of earlier research, which demonstrated that the proposed model is superior to other models when measured by the following metrics: accuracy (94.2%), sensitivity (94.8%), and specificity (93.4%).

Keywords: blockchain; diabetic retinopathy; TaylorAVO; CNN; EHR

Citation: Uppamma, P.; Bhattacharya, S. Diabetic Retinopathy Detection: A Blockchain and African Vulture Optimization Algorithm-Based Deep Learning Framework. *Electronics* **2023**, *12*, 742. https://doi.org/10.3390/electronics12030742

Academic Editor: Antoni Morell

Received: 14 November 2022
Revised: 20 December 2022
Accepted: 26 December 2022
Published: 1 February 2023

1. Introduction

Recent developments have shown that the blockchain is advantageous for researchers, since it can safely store personal healthcare information [1]. Healthcare data are quite complex, and must be kept secure from unauthorized access. Blockchain technology provides a safe environment for storing, sharing, and managing information in IoT networks and technology. It also encourages the safest and most "trustless" transformation among the communicating entities and is a decentralized framework where every block is linked together [2]. EHRs are digitalized versions of patients' health information, which are usually documented as health charts in a paper-based system. EHRs provide real-time patient-centric records that ensure the instant availability of patient information to authorized healthcare professionals. EHRs include patients' medical and treatment histories, diagnoses, treatment plans, allergies, immunizations, radiological images, test results, and various health-related information that enables healthcare providers to make decisions

about patient care. Several organizations in the health industry can collaborate with individual EHRs using blockchain [3]. A group of parties offers authentication and costly data steps for all the contributing participants [4]. Blockchain technology is used in various applications to improve trust and information privacy, allowing participants to share and transfer data with a degree of trust and integrity [5]. The convenient health record storage system is rendered by the EHR manager and improves the electronic access to patients' manual medical records. This method is utilized to allow patients to reduce, produce, maintain, and spread the EHR to colleagues, family, and healthcare providers [6].

Blockchain technology has the potential to improve clinical trial information management in a variety of ways, including eliminating bottlenecks granting planning permissions, and streamlining communication between the numerous players involved in the supply chain. For computerized disease surveillance and overall health monitoring, data collection and analysis, which may include gathering large amounts of personal or non-sensitive information, may be needed. Blockchain can revolutionize the storage and sharing of a patient's electronic health records. It can provide a more secure, transparent, and traceable foundation for the exchange of health information. Multiple data management systems may be interconnected using this technique. A blockchain-based electronic health record could make it possible for systems in numerous countries to work together [7]. These patients can transfer their EHRs from one firm to another by sharing their EHRs in various situations throughout their lifetime. The models built from the massive e-healthcare records determine performance and reliability [8,9]. Diabetes is a disease that poses a threat to many lifestyles and leads to widespread damage to human organs, namely the kidney, eyes, lungs, and heart [10,11]. Diabetic retinopathy is a severe eye disease and one such side effect of diabetes. The World Health Organization (WHO) estimates that approximately 285 million people worldwide have impaired vision, of which 39 million are blind and 246 million suffer from low vision caused by DR. As the name implies, the retina is specifically targeted by DR because the high blood glucose levels can damage the retinal vessels [12,13]. Ophthalmologists classify DR into two categories, namely, proliferative diabetic retinopathy (PDR) and non-proliferative diabetic retinopathy (NPDR). NPDR is further divided into mild, moderate, and severe stages [14]. It is possible to reduce blindness from DR when it is diagnosed early and treated effectively. Moreover, a medical practitioner can diagnose this disease either manually or automatically with the help of a few rudimentary detection devices. Various medical imaging evaluation models have been considered to effectively aid in DR diagnosis and prognosis to reduce the burden on eye practitioners [15–17]. Deep learning methods are one such tool, chosen to study the functions of DR grading. Deep conventional neural network (DCNN)-based methods were selected to enhance the DR detection performance [18–20]. CNN was used to extract visual characteristics to train the network. Patients' reports are analyzed to detect complications using these features. This paper presents a novel blockchain-based optimal neural network framework to detect DR disease. This framework supports medical professionals in the earlier provision of treatment to diabetic retinopathy patients, ensuring the secure storage and exchange of healthcare records in the EHRs.

The present generation of healthcare systems requires patient records and relevant information to be accessed at any place, which could accelerate decision-making and care by healthcare providers. The traditional EHR systems fail to meet the requirements of secured data availability and distribution, facing the challenges of unauthorized access and data tampering [21]. The proposed method focuses on two objectives: Firstly, the implementation of an optimized deep learning algorithm that enables the accurate detection of DR. Further, the patient and severity, which are pertinent to the DR parameters and the resultant diagnostic results post-implementation of the DL algorithm, must be stored securely and be accessible to authorized stakeholders. Thus, the proposed framework encompasses the use of the TaylorAVO algorithm in association with SqueezeNet architecture for optimal parameter selection and further classification of the same. DR detection results, as well as selected parameters regarding patients, are stored in blockchain,

ensuring data privacy and security. This paper contributes to improvements in the accuracy of diabetic retinopathy detection using the hybrid model TaylorAVO-SqueezeNet and the patient EHRs information, which are placed in the blockchain network. This hybrid deep learning model extracts optimal image features using the TaylorAVO algorithm and trains them using SqueezeNet. Registration, key generation, and authentication are all stages of the proposed method. The registration procedure begins with the doctor and patient entering their information. Following the registration phase, the private key is assigned and forwarded to the administrative unit. During the authentication process, data are uploaded and downloaded, along with the patient and the doctor, using the private key. Finally, the data are secured using the blockchain.

The major contributions of this paper are as follows:

- An exhaustive review of the various applications of blockchain and machine learning implementations in EHR, highlighting the associated limitations.
- The implementation of the TaylorAVO algorithm, which helps to generate optimal features from the DR patient data, which are further trained using the SqueezeNet to ensure effective disease diagnosis.
- The implementation of blockchain technology to store EHRs and ensure that authorized healthcare providers and patients can access the relevant information.

1.1. Motivation

Electronic health records (EHRs) allow healthcare providers to instantly track and monitor patients' medical records to enable accelerated decision-making. The traditional methods of health record management require expensive equipment for monitoring patients' vital symptoms, in addition to maintenance of their medical history, leading to the misutilization of resources, with the associated challenges of reduced efficiency, security, and reliability. There is a high possibility of such confidential records being tampered with and manipulated, leading to compromises in patient care. Additionally, the unavailability of data at any instance for critical decision-making leads to the possibility of patient care and support being delayed. This acts as the motivation to develop a framework that enables accurate decision-making, ensuring secure data transmission and availability. The present study, therefore, proposes a deep-learning-based framework, which includes the use of optimization techniques to help with the detection of DR with enhanced accuracy. This framework incorporates the use of blockchain technology, which ensures that DR-related patient data, detection results, and related treatment plans are secured and can only be accessed by authorized stakeholders.

1.2. Paper Organization

The structure of the paper is organized as follows: Section 2 discusses the related studies in the form of a literature review, emphasizing prominent and relevant studies performed on DR data; Section 3 provides a detailed description of the proposed framework; Section 4 elucidates the experimental analysis report; Section 5 provides the consolidated conclusion and highlights the scope of future research.

2. Literature Review

Blockchain is an emerging technology, used in various disciplines, including healthcare data management. This healthcare data include remote patient observations, maintaining EHR data, supply chain management for medicines, healthcare data analytics, and research in the biomedical field, where maintaining security and data integrity is an essential concern [22,23]. The smart healthcare environment increasingly manages medical records electronically, as compared to traditional practices. The EHR system reduces the burden of data redundancy issues, security problems, and effective data management. The eHealth service provider system could preserve the authentication details of patients and other service assistants without being dependent on cloud-based services [24]. The authors in [25,26] proposed a blockchain framework for an EHR-sharing system to provide secure

and high-quality healthcare data-sharing among all stakeholders. This framework includes a decentralized third-party system to enhance the consistency of the data and monitor the various healthcare activities over the network using a health information system. Regarding security concerns, the authors in [27] considered a blockchain-based secure data management system using the Internet of Medical Things (IoMT), which includes data transmission between cloud servers, personal server systems, and medical devices. This is more interactive and it is more secure for patients and providers to share healthcare information using these IoMT devices. Bitcoin is becoming increasingly popular as a digital payment method [28]. The proposed model focused on healthcare data, such as medical treatments and post and pre-surgery details, which could be linked to digital payments through the blockchain. All healthcare professionals within the system could access this application. The authors in [29], presented a framework that offered the early detection of diabetes using prevalent machine learning algorithms in association with the maintenance of patients' EHRs. The patient health records, which were collected using wearable sensor devices and further distributed through EHR systems, were dependent on the interplanetary file system (IPFS) that originated in the blockchain. The information was presented to the EHRs manager, and the data were fed into various ML models, wherein data processing was performed, which generated predictive outcomes. The system fulfilled the need for privacy, integrity, and authentication but failed to prevent blockchain attacks.

The authors in [30] proposed a blockchain safety framework (BSF) for the successful and secure storage and maintenance of EHRs. This presented a safe and secure technique for gathering medical statistics for doctors, patients, and insurance agents. The proposed framework concentrated on the safety of doctors, patients, and events, wherein the structure supported confidentiality and safety aspects relevant to the healthcare sector. The proposed methodology and the simulation results enabled effective and secure access to EHR records within the shortest possible time. However, this method failed to yield similar positive results in other domains. Traditional methods that focused on DR detection mechanisms depicted the limitations of diabetic retinopathy detection, especially in the use of healthcare data. The authors [31] proposed a healthcare framework for the detection of diabetic disease based on deep machine learning, in addition to the data fusion technique. The deep ensemble learning method helped to increase the knowledge of fusion-based data to eliminate the unnecessary burden on the model and further improve its performance. In [32], a hybrid model was proposed for diagnosing DR from retinal lesion images based on the medical imaging process and deep learning techniques. DR detection depends on an image enhancement mechanism and acts as an open issue when using fundus images with an impact on the model performance.

The authors in [33] performed pre-processing and dimensionality reductions using PCA. The firefly algorithm was used for feature extraction; then, a deep learning model was used on the DR dataset, which is publicly available and taken from the UCI repository. Although the model generated enhanced accuracy, it failed to perform well in the case of larger datasets or datasets in other domains. The authors in [34] proposed a unique approach to microaneurysms and hemorrhage detection on fundus images. The methodology included pre-processing, blood vessel segmentation and removal, fovea localization, and elimination and function extraction, which helped in DR detection disorders resulting from microaneurysms and hemorrhages. These methods failed to extract appropriate features for lesion detection. The authors in [35] proposed a semi-supervised auto-encoder graph community (SAGN) model, used for DR diagnosis, which helped to eliminate insignificant constraints. The SAGN method contained three primary modules namely neighbor correlation mining, auto-encoder feature learning, and graph representation. This achieved an enhanced performance considering the limited labeled retinal images. In [36], the authors proposed a novel deep convolutional neural network, considering multi-view retinal images for the automatic prognosis of DR. The experimental results revealed four image feature extraction perspectives using sharedNet in the case of automated DR detection. The model ensured enhanced feature extraction by improving the network capability.

It also required the addition of attention mechanisms in lesion annotations to improve the effectiveness of the proposed model. The traditional methods improved the security of health records using various blockchain-based healthcare frameworks, in association with deep learning methods, to detect the patient's condition, as presented in Table 1.

Table 1. Various blockchain-based healthcare frameworks in association with deep learning applications.

Reference	Methodology	Key Contributions	Limitations
[29]	Blockchain-based diabetes detection framework	• Focused on EHRs data to provide security and disease detection using a machine learning algorithm	• The blockchain framework was not tested on other domains • Prediction accuracy was biased
[30]	BSF-EHR	• Development of blockchain security framework to efficiently store and secure EHRs information	• Framework failed to generate positive results in other domains
[31]	The smart healthcare recommendation system for multi-view disease prediction (SHRS-M3DP)	• Development of an SHRS-M3DP methodology concentrating on disease detection using the data fusion technique	• The advanced disease prediction algorithm was not used
[32]	Medical image-enhancing techniques and the CNN model	• Histogram equalization method was employed to improve image quality • CNN model implemented for disease classification	• Alternative medical databases were not considered for various diagnosis-related operations
[33]	Hybrid deep learning model (PCA-firefly algorithm)	• A hybrid deep learning model was developed, concentrating on dimensionality reduction • Firefly algorithm implemented for DR detection	• The framework did not apply to larger datasets in various domains
[34]	DR detection for Gaussian interval type-2 fuzzy membership (GIT2FMFS)	• GIT2FMFS method proposed to identify DR stages of microaneurysms and hemorrhages using the GIT2FMFS technique on retinal images	• The performance of the model required further enhancement
[35]	Semi-Supervised Auto Encoder Graph Network (SAGN)	• Development of SAGN framework to grade fundus images from specific correlation features	• Limited data labeling accuracy could be improved
[36]	MVDRNet	• Development of multi-view diabetic retinopathy detection mechanism using the shared net and attention-fusion net generates feature maps on fundus images	• Diversified DR retinal disorder and related data were not considered

3. Proposed Methodology

3.1. Blockchain-Based Healthcare Framework

The proposed blockchain-based healthcare framework concentrates on handling the requests of doctors and patients, allowing them to register themselves through the registration hub. The information from patients and healthcare professionals was gathered at the registration center unit. The smart device was combined with the registration center to provide information to the user. The registration center can gather all the required information, generate a private key with an ID, and deliver this to the administrative unit.

The EHR manager should provide an authorized ID to each doctor and patient. The EHR Manager, the User, the Admin Unit, and the Interplanetary File System are the four entities that make up the authentication procedure. The penalty is displayed for the specific ID if the authentication is unsuccessful. After successful authentication, the doctor and patient are certified. The blockchain-based healthcare framework architecture is shown in Figure 1.

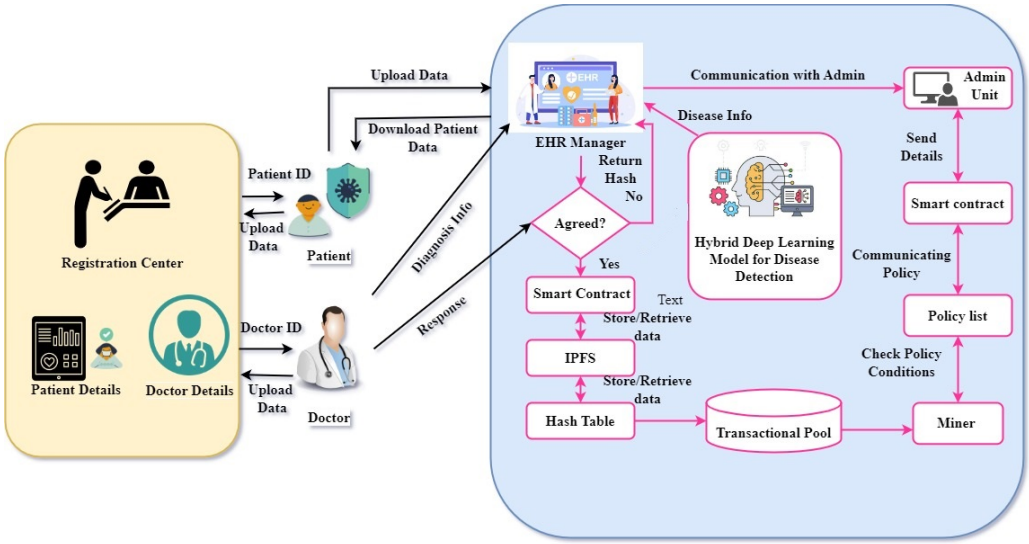


Figure 1. The proposed model of blockchain-based healthcare framework.

3.1.1. Registartion Center (RC)

Patient information, such as the father's name, age, and address, is collected and sent to the doctors with the help of the registration center. The smart device is combined with the registration center to provide the information to the user. The administration unit is in charge of the verification. After successful validation, the EHRs Manager can submit the encoded transactional information to the Interplanetary File system (IPFS).

3.1.2. Smart Devices

The smart device consists of desktops, laptops, smart mobiles, and sensor nodes. A smart device should be accessible to the patients for login purposes. The information is subjected to the smart devices' EHRs manager for further processing. The administration unit provides information to allow the EHR manager to accept users. It also delivers IoT data collected from the smart device to the deep learning unit for further diagnosis.

3.1.3. Electronic Health Records (EHRs)

The EHR is a key component of the proposed system. This serves as a centralized authority that hosts several activities, ensuring optimum performance. The users are requested to complete the transaction and related requests are sent to the EHR manager. The administrative unit has the public key as a part of the smart contract, which is used to verify transactions.

3.1.4. Smart Contracts

The smart contract is connected to the EHRs manager and administration unit. This is a program that transfers digital assets among gatherings under specific conditions. The programmers created these smart contracts to meet their unique requirements.

3.1.5. Deep Learning Unit

Deep learning plays a vital role in our proposed system. The publicly available IDIRD-diabetic retinopathy image dataset was used to train the deep learning model for the diagnosis of DR-affected patients. The proposed TaylorAVO-SqueezeNet architecture is

used for disease classification to detect normal and abnormal cases. The EHR manager receives the diagnosis information and sends it to the IPFS. Finally, the patient records are stored in the blockchain, ensuring data security.

The entities involved in this methodology are the user, EHR manager, admin unit, and IPFS. As part of the initialization process, a random number is generated and sent to the IPFS. Next, the registration process begins, involving three phases of registration, between the admin unit and the IPFS, the EHR's manager and the admin unit, and the user and the admin unit. Post-registration, when the user requests any transaction, this is performed through appropriate authentication, eliminating the chances of unauthorized access. The mechanism of authentication involves three phases: interactions between the admin unit and IPFS, the EHR manager and admin unit, and the user and EHR manager. Finally, the DR is detected at the EHR manager unit.

Step 1: Initialization phase

This is the first step in the authentication process, in which the IPFS initialization is completed using a random number and hash function. Here, the random number is in the range [0, 2].

Step 2: User registration phase

The user registration phase consists of three steps: the registration between the admin unit and IPFS, the EHR manager and admin unit, the admin unit, and the user. The registration process is explained in Algorithm 1. The details of each phase are mentioned below.

- Registration between admin unit and IPFS: The admin unit username and password are generated in the admin unit, which is denoted as Ad_{id}, Ad_{pwd}. The Ad_{id}, Ad_{pwd} is sent to the IPFS; then, the IPFS generates the verification message V_1, a random number (b) and hashing (h). The verification message V_1 in the admin unit is sent to IPFS and stored as V_1^*, along with the random number (d). Finally, the admin unit is registered with IPFS.
- Registration between the EHR manager and admin unit: An user ID and password are generated in the EHR manager, which is provided as E_{id} and E_{pwd} to the administrative unit. The admin unit generates the verification message V_2. In this instance, the random number 'a' and the hashed E_{id} are concatenated, and the result is added to the random number 'c'.
- Registration between admin unit and user: The user ID and password are generated and sent to the administrative unit in the form of U_{id} and $U_{pwd}s$, which are further sent to IPFS. The verification message V_3 is generated by combining the hash code 'h' and the random number 'c'. The results are stored in the EHR management. The random number generated by hashing enables the user to be registered with the EHRs manager.

Algorithm 1 Registration Between Admin, EHR manager, and User

procedure ADMIN UNIT TO IPFS
Admin registered with(Ad_{id}, Ad_{pwd})
(Ad_{id}, Ad_{pwd}) $\rightarrow$ IPFS
IPFS: h(V_1, rand 'd') $\rightarrow$ Admin
if Admin verify V_1 **then**,
IPFS $\leftarrow$ V_1^*, rand d: Admin
Admin is registered in IPFS
else
Terminated
end if
end procedure
procedure EHR MANAGER TO ADMIN UNIT
EHR Manager(E_{id} and E_{pwd})
EHR: (E_{id}, E_{pwd}) $\rightarrow$ Admin Unit
Admin: (E_{id}, E_{pwd}) $\rightarrow$ IPFS
EHR Manager $\leftarrow$ h(V_2): Admin
if EHR verify V_2^* **then**,
Admin $\leftarrow$ (V_2^* and rand 'c'): EHR
EHR is registered with the Admin
else
Terminated
end if
end procedure
procedure ADMIN UNIT TO USER
User(U_{id} and U_{pwd})
EHR Manager and IPFS $\leftarrow$ (U_{id} and U_{pwd})
if EHR verify (U_{id} and U_{pwd}) **then**,
User $\leftarrow$ (V_3, h): EHR
EHR Manager $\leftarrow$ (V_3^*,h and rand 'c'): User
User verified with (EHR Manager and IPFS)
else
Terminated
end if
if User $\leftarrow$ EHR: S_k **then**,
User verified and Upload data
Data stored in Blockchain(R)
else
Terminated
end if
end if
end procedure

Step3: Authentication Phase

The authentication process encompasses the interaction between the admin unit and IPFS, the EHR manager and admin unit, and the user and EHRs manager, as specified in Algorithm 2.

- Authentication between admin unit and IPFS: The authentication message A_1 is generated in the admin unit. The admin ID and password are represented as Ad_{id}, Ad_{pwd}. The hashing (h) is combined with the admin ID and the password is integrated with the time stamp T. Then, the authentication message is sent to the IPFS, and the IPFS checks the time stamp's validity. The process continues until the yes criteria are fulfilled; otherwise, it is terminated.
- Authentication between EHR manager and admin unit: The authentication process between the EHR manager and the administrative unit is maintained in this phase.

The authentication message A_2, hashed (h) secret key S_k, and the hashed E_{id} is concatenated with the time stamp T. Then, the admin unit verifies the time stamp(T) validity. The session continues until the yes criteria are fulfilled; otherwise, it is terminated. The EHR manager stores the authentication message A_2, hashed secret key S_k^* and hashed E_{id}.

- Authentication between the user and EHR manager: The authentication message A_3 is generated by the EHR manager for the user, which includes the stored hashed secret keyS_k, and security parameter 'y'. Then, the user sends the authentication message to the EHR manager for verification. After verification, the authentication message A_3 is created, which includes the stored hashed secret key S_k^* and User ID combined with the security parameter y. If the user is verified, then the OTP is sent to the manager by the user. The OTP is generated with a user ID with the hash function, formed by the hash function combined with the random number b. The EHR manager generates OTP, which is sent to the user and stored as OTP*. If the OTP is verified, then the user is authenticated.

Algorithm 2 Authentication Between Admin, EHR manager, and User

procedure ADMIN UNIT TO IPFS
  IPFS ← A_1(h(Ad_{id}, Ad_{pwd}), T): Admin
  if IPFS verify T **then**,
    A_1 Authenticated
  else
    Terminated
  end if
end procedure
procedure EHR MANAGER TO ADMIN UNIT
  Admin ← A_2(h(E_{id}+ S_k^*): EHR
  if Admin verify (A_2, T) **then**,
    E_{id} Authenticated
  else
    Terminated
  end if
end procedure
procedure USER TO EHR MANAGER
  EHR ← A_3(h(U_{id}+ S_k^*),y): User
  if User verify (A_3) **then**,
    EHR ← OTP: User
  else
    if OTP verify **then**,
      U_{id} Authenticated
    else
      User Terminated
    end if
  end if
end procedure

3.2. TaylorAVO-SqueezeNet for DR Detection at EHR Manager Unit

The proposed method of DR detection at the EHR unit follows three steps: pre-processing, lesion segmentation, and classification. The filtering technique used image pre-processing methodology, wherein medical images are fed into the pre-processing module. The process of lesion segmentation is carried out using RP-Net [37]. The proposed TaylorAVO algorithm is an integration of the Taylor series and African Vultures Optimization (AVO) algorithm [38], which is used to train the model. The disease classification was performed using a deep learning classifier named SqueezeNet [39]. The final classification results are registered on the blockchain for future usage, ensuring that only authorized

users can access the same. The architecture of TaylorAVO-SqueezeNet for DR detection is shown in Figure 2.

Consider that input images collected from the dataset are denoted as images, which can be expressed as

$$N = \{X_1, X_2 \ldots\ldots, X_m, \ldots\ldots X_z\} \quad (1)$$

wherein the total number of images, X_m, represents the m^{th} image. The input image X_m is pre-processed for the removal of noise.

3.2.1. Pre-Processing of the Image Using a Median Filter

Image pre-processing is crucial to enhancing the quality of the images, with the associated advantages of simple processing steps. The median filter approach is used in this work to minimize the noise from input images. This is called a non-linear filtering method and preserves the smooth edges of pixel information. The original pixel values are transmitted to the median of the grayscale pixel values, and these implementations are specifically used in digital image processing, along with the lesion segmentation process.

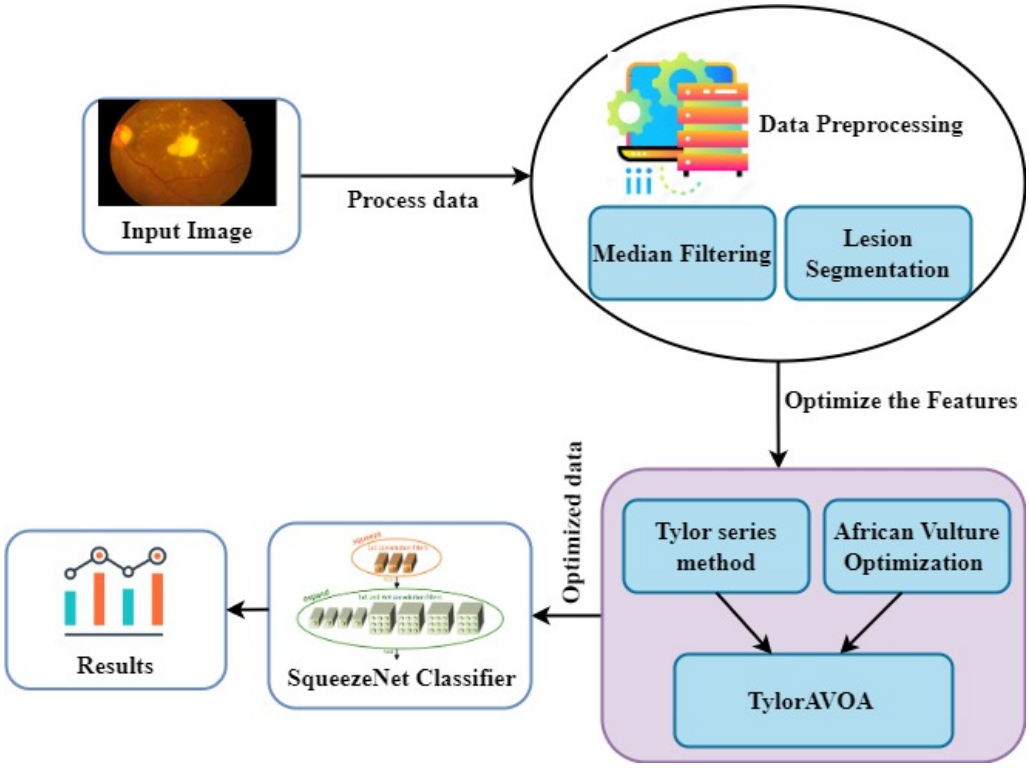


Figure 2. The proposed TaylorAVO-SqueezeNet architecture for DR Detection.

3.2.2. TaylorAVO (African Vulture Optimization) Algorithm

The TaylorAVOA is the integration of the AVO algorithm and the Taylor series. The AVO algorithm simulates the foraging behavior and movement process of African vultures. The advantage of the Taylor series lies in its simple computation process, with a short execution time. As part of the algorithm, the numerous vultures are divided into two groups based on the unique, cruel aspect of the vulture's behavior. This algorithm calculates the fitness function (f) for the entire population and finds the best position for the vulture. It is a metaheuristic algorithm, which uses an optimized rational search expression to find the best optimal search strategy compared to other nature-inspired algorithms. The TaylorAVO algorithm has a superior execution speed and a lower computational cost, providing the best optimal features. The formulation of the Taylor African vulture's algorithm works based on four assumptions [38] and pseudo-code for the algorithm, as shown in Algorithm 3.

Algorithm 3 The pseudo-code for the Taylor African Vulture algorithm

procedure
Initialization of the server model
while (termination condition is not reached) **do**
Calculate the objective function with Equation (2)
Update $K_{BestVulture_1}$ be the position of 1^{st} optimal vulture
Update $K_{BestVulture_2}$ be the position of 2^{st} optimal vulture
Taylor expression for error rate computation with Equation (5)
for (all vulture(K_h) **do**
select A(H)
Update H based on Equation (6)
if (f $\geq$ 1) **then**
if ($K_1 \geq rand_{a_1}$) **then**
Update the vulture's position with Equation (3)
else
Update the vulture's position
end if
end if
if (|f| < 1) **then**
if (|f| $\geq$ 0.5) **then**
if ($K_2 \geq rand_{a_2}$) **then**
Update the vulture's position by Equation (4)
else
Update the vulture's position by Equation (6)
end if
if ($K_2 \geq rand_{a_3}$) **then**
Update the vultures position based on Equation (3)
else
Update the vultures position based on Equation (4)
end if
end if
return $K_{BestVulture_1}$
end if
end procedure

- In the initial stage, the vultures move to find food and choose the best position for each group. The probability of finding the best solution is based on search parameter values lying between 0 and 1.

$$Q_i = \frac{f_i}{\sum_{r=1}^{n} f_i} \tag{2}$$

- For collecting the food, the vultures travel very long distances when they are highly active and energetic. If they lack sufficient strength, they fail to travel long distances. Thus, in such circumstances, the vultures become more violent when acquiring food. This behavior is expressed as follows:

$$U = (2 \times \text{ rand }_{a1} + 1) \times b \times \left[1 - \frac{\text{iter }_h}{\text{maxiter}}\right] + f \tag{3}$$

$$f = z \times \left(\sin^q\left(\frac{\theta}{2} \times \frac{\text{iter }_h}{\text{maxiter}}\right) + \cos\left(\frac{\theta}{2} \times \frac{\text{iter }_h}{\text{maxiter}}\right) - 1\right) \tag{4}$$

where U denotes gratified vulture, $iter_h$ defines the total number of the current iteration, q represents the constraint of the static number set, and the value of q is 2.5; r and 1 and z represent the random value, and maxiter defines the whole iterations. When b drops to 0, this reflects that the vulture is starving. When b crosses 0, this shows that the vulture becomes replete, and is denoted as U. When U is greater than one, the

vultures consider the food in various positions, and the AVO algorithm outperforms the exploration phase. When U is smaller than one, the AVO algorithm begins with the exploitation step. Before starting the exploration phase, the Taylor series expression is utilized to reduce the error rate while performing the number of iterations by vultures. Moreover, this helps to calculate the error rate to obtain the optimized values in each phase.

$$\sum_{x=0}^{\infty} \frac{f^{(x)}(m)}{x!}(z-m)^x \tag{5}$$

Here, $f^{(x)}$ is the differentiation function and m specifies approximation for nth derivative.

- In the exploration phase, vultures follow random paths to search for their food. This is represented by the parameter Q1, whose value should lie between 0 and 1 for any strategy. In this phase, $rand_{a1}$ is generated and is limited to 0 and 1. If the $rand_{a1}$ is greater than or equal to Q1, the expression (5) is utilized. When $rand_{a1}$ is smaller than or equal to Q1, the expression (7) is used. These approaches are used to enhance the search strategies of the vultures with these random coefficient values.

$$Q(i+1) = BV(i) - H(i) \times f \tag{6}$$

$$H(i) = |Y \times BV(i) - Q(i)| \tag{7}$$

$$Q(i+1) = BV(i) - f + \text{ rand }_{a2} \times ((ub - lb) \times \text{rand}_{a3} + lb) \tag{8}$$

- The exploitation phase was divided into two phases based on the movement of vultures. The first phase of exploitation is divided into rotating flight and siege flight phases. If the 'f' value is greater than or equal to 0.5, the vulture is repleted. In this scenario, there is a conflict when obtaining food for weak vultures from other, predominant ones.

$$Q(i+1) = G(i) \times (f + rand_{\text{a4}}) - S(t) \tag{9}$$

$$S(t) = R(i) - P(i) \tag{10}$$

The vulture moves in a circular motion, and the best two vultures' positions are given as follows:

$$C1 = R(i) \times \left(\frac{\text{rand }_{a5} \times Q(i)}{2\pi} \right) \times \cos(Q(i)) \tag{11}$$

$$C2 = R(i) \times \left(\frac{\text{rand }_{a6} \times Q(i)}{2\pi} \right) \times \sin(Q(i)) \tag{12}$$

- In the exploitation second phase, if the 'f' value is smaller than 0.5, then all the vultures have combined to search for food, and the two vultures' best positions are identified. In other situations, the vultures become more arrogant in searching for food when they become weak.

$$P_1 = BV_1(i) - \frac{BV_1(i) \times Q(i)}{BV_1(i) - Q(i)^2} \times f \tag{13}$$

$$P_2 = BV_2(i) - \frac{BV_2(i) \times Q(i)}{BV_2(i) - Q(i)^2} \times f \tag{14}$$

3.2.3. SqeezeNet Structure

SqueezeNet is a convolutional neural network model that consists of 18 layers [39]. The model intends to reduce the parameters while performing down-sampling. The architecture allows for the loading of a pre-trained version of the network, considering more than a million images from the ImageNet database. A smaller neural network with fewer features is the ultimate objective, because it can be accessed more quickly through the internet and make more effective use of the computer memory cost. The architecture enables

the ML models to be deployed in embedded systems, which include resource-constrained applications. The purpose of developing compressed networks is to reduce the communication across servers during the process of distributed training. The smaller number of CNNs requires a reduced bandwidth when exporting newer models from the cloud to the remote systems, ensuring optimized memory utilization. The architecture includes multiple layers with activation energy, which can be implemented in two ways: without the heavy compression method and with the combined compression method, thus achieving the highest level of accuracy. Many compression techniques are commonly used, including single-value decomposition, deep compression, quantization, and network pruning.

Fire Module: The "squeeze" convolution layer with only 1*1 filters comprises the fire module. This information is transmitted to the expand layer, which comprises 1*1 and 3*3 convolution filters. The module uses three tunable dimensions—s_{1*1}, e_{1*1}, and e_{3*3}. Here, s_{1*1} represents the number of filters in the squeeze layer, e_{3*3} represents the number of 3*3 filters in the expand layer, and e_{1*1} represents the number of 1*1 filters in the expand layer.

While conducting extensive research into the potential design space for CNN architectures, we came across several new CNNs, one of which is called SqueezeNet. This squeezeNet architecture is more sophisticated and allows for numerous applications to be developed in a limited environment. The primary advantage of using SqueezeNet lies in the use of fewer parameters than the traditional AlexNet architecture while yielding the same level of accuracy. The SqueezeNet model thus classifies whether a patient is affected by DR, utilizing minimal computational resources. Once the classification process is completed, the results are stored in the blockchain, which can only be downloaded by the authorized individual. The following Table 2 lists the symbols that are frequently used in algorithm implementations.

Table 2. Symbols Description.

Symbols	Description
a,b,c,d	Random numbers
h	Hash function
Ad_{id}	Admin username
Ad_{pwd}	Admin password
E_{id}	EHR manager username
E_{pwd}	EHR manager password
U_{id}	User ID
U_{pwd}	User password
S_k	Secret key
V_1	Verification message 1
V_2	Verification message 2
V_3	Verification message 3
R	Medical data
T	Timestamp
y	Security parameter

4. Results and Discussion

The implementation of the proposed model was performed using PYTHON. The hardware resources included Windows 10 OS, an Intel processor, and 8 GB RAM. The suggested model was assessed using the measures of accuracy, specificity, and sensitivity. The proposed TaylorAVO-SqueezeNet framework was compared to the existing models and prominent studies—'' Blockchain security framework for electronic health records of patients (BSF-EHR) [30], convolutional neural network (CNN) [31], Granular interval type-2 membership functions (GIT2FMFS) [34], and Semantic adaptive graph network (SAGN) [36]"—showing its superior performance. A brief explanation of the evaluation measures is provided in the following paragraph:

Accuracy: This is defined as the measure representing the proportion of true-positive results in the total observations. It is computed as

$$ACC = \frac{A_p + A_n}{A_p + A_n + B_p + B_n} \tag{15}$$

Sensitivity: Specificity is defined as the identification of the measure of actual positives.

$$Sensitivity = \frac{A_p}{A_p + A_n} \tag{16}$$

Specificity: Specificity is defined as the identification of the measure of actual negatives.

$$Specificity = \frac{A_n}{A_n + B_p} \tag{17}$$

Here, A_p, A_n, B_p, and B_n represent the rate of true positive cases, false positive cases, false negative cases, and true negative cases, respectively.

4.1. Dataset Description

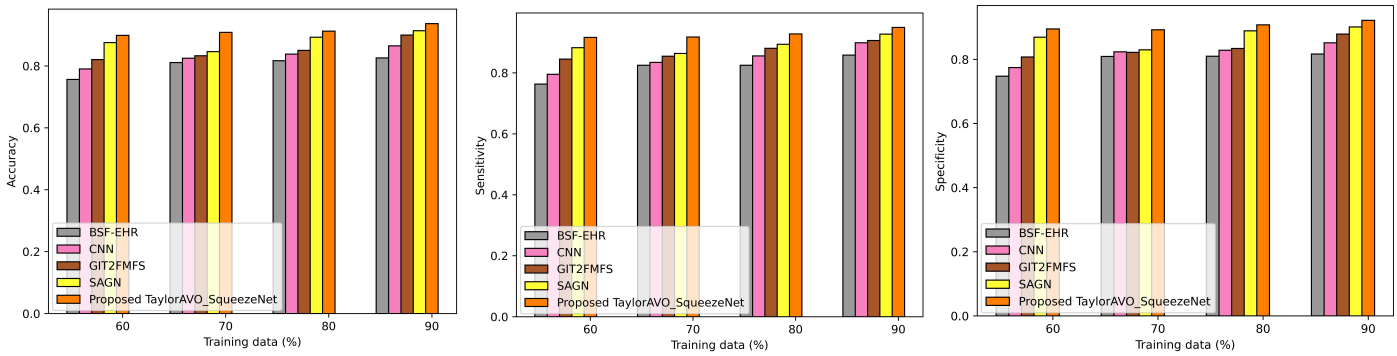
The IndianDRImage Dataset (IDRID) [40] is used to evaluate the experimental outcomes of DR detection in the proposed framework. A major concern regarding publicly available healthcare datasets is that their scarcity compels the research community to work with the few such datasets that are easily available. Thus, based on such a dataset, the types of applications lag in variability. Additionally, the models developed based on such datasets may not be suitable for generalized widescale applications. Hence, extensive characterization of the data is essential for researchers and model developers for quality evaluations of such datasets. The data can be characterized by a thorough breakdown of the features in the dataset. Considering this, the IDRID dataset is critically studied in the present study. The IDRID consists of 516 retinal fundus images, which are divided into three categories: segmentation, clinical grading, and localization of the images. There are 81 authentic color fundus images in the segmentation process and 516 authentic color fundus images in the localization and disease-grading process. The quality of the images in the dataset is enhanced using the median filtering technique, as described later in Section 3.2.1, as part of the pre-processing [41].

4.2. Experimental Analysis

As shown in Figures 3–6, the performance of the proposed TaylorAVO-SqueezeNet is examined based on accuracy, sensitivity, and specificity metrics by varying the training data, k-fold validation, and block size.

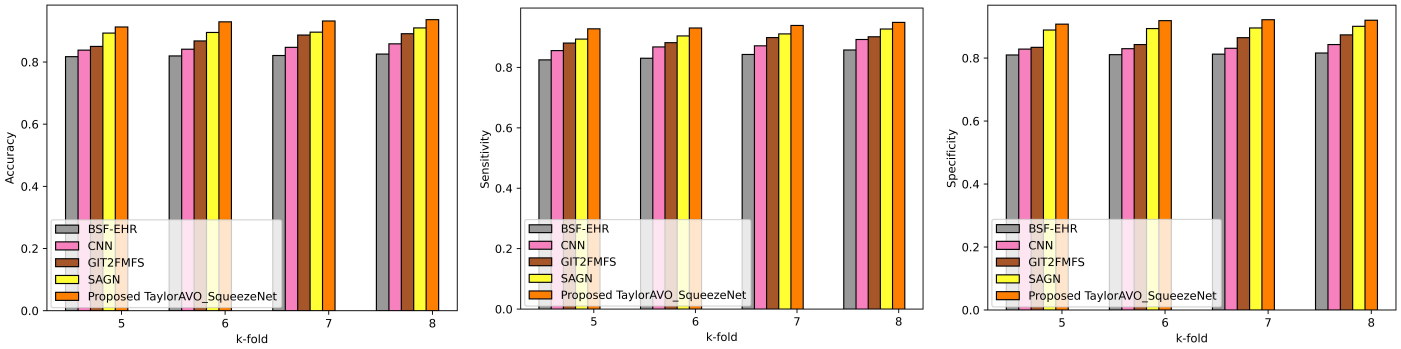
Figure 3 represents the performance of the proposed TaylorAVO-SqueezeNet based on its accuracy, sensitivity, and specificity. Here, the percentage of training data varied in association with the provision of varied block sizes. The proposed model yields enhanced results in comparison to the traditional models (BSF-EHR, CNN, GIT2FMFS, SAGN), considering the variabilities in training data and block size.

Figure 4 represents the performance of the proposed TaylorAVO-SqueezeNet model, considering accuracy, sensitivity, and specificity metrics, based on the k-fold validation. The results demonstrate that the proposed model achieves superior performance compared to conventional models (BSF-EHR, CNN, GIT2FMFS, SAGN) when varying the k-fold data validation.



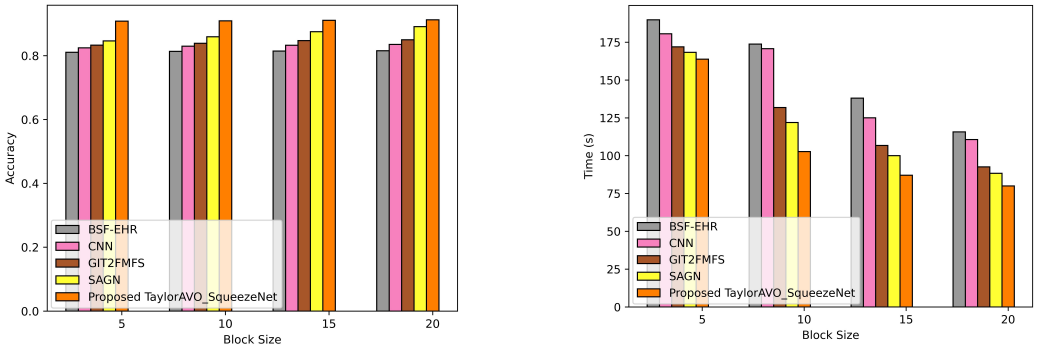
(**a**) Accuracy. (**b**) Sensitivity. (**c**) Specificity.

Figure 3. Evaluation of accuracy, sensitivity, and specificity using TaylorAVO-SqueezeNet with other traditional models according to varying training data.



(**a**) Accuracy. (**b**) Sensitivity. (**c**) Specificity.

Figure 4. Evaluation of accuracy, sensitivity, and specificity using TaylorAVO-SqueezeNet with other traditional models according to varying k-fold validation.

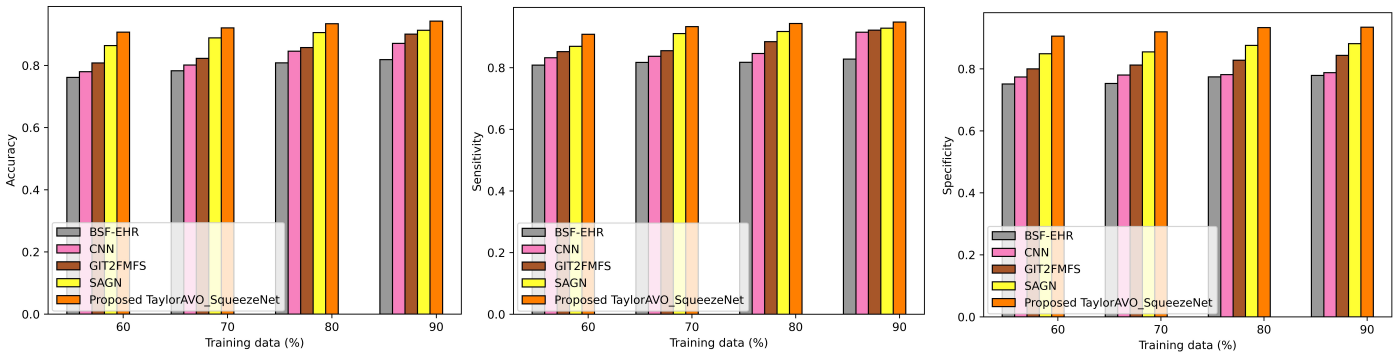


(**a**) Accuracy. (**b**) Computational Time.

Figure 5. Evaluation of accuracy and computation time using TaylorAVO-SqueezeNet with other traditional models according to varying block size and time.

In Figure 5, Figure 5a represents the performance of the proposed TaylorAVO-SqueezeNet model, wherein enhanced accuracy is observed with a blocksize increase and the trend is significant when compared with traditional models. In the same way, Figure 5b illustrates the decrease in computing time as the size of the blockchain increases, thus validating the efficiency of the proposed approach compared to conventional models. (BSF-EHR, CNN, GIT2FMFS, SAGN).

Figure 6 represents a comparison of the performance of the proposed TaylorAVO-SqueezeNet in cases of limited and large block sizes, as well as varying training data and K-fold. The graphs reveal that the performance of the model is enhanced with the increase in block size.



(**a**) Accuracy. (**b**) Sensitivity. (**c**) Specificity.

Figure 6. Evaluation of accuracy, sensitivity, and specificity using TaylorAVO-SqueezeNet with other traditional models, varying block size and time.

4.3. Performance Analysis

The proposed TaylorAVO-SqueezeNet model performance is evaluated based on the minimum and maximum data sizes as well as variations in training data, block size and k-fold data. In the case of training data variability, the model is evaluated for the metrics of accuracy, sensitivity, and specificity, wherein it is revealed that the proposed model has superior outcomes compared to the conventional models (BSF-EHR, CNN, GIT2FMFS, SAGN). Similarly, a similar outcome is observed in the case of varying k-fold, wherein the proposed model outperforms the conventional models in the aforementioned metrics. Further, the block size is also varied, and the model is evaluated considering accuracy and computation time. In this case, the outcomes validate the proposed model's superiority. The consolidated outcomes for varying parameters are represented in Table 3.

Table 3. The analysis of performance metrics for several measures.

	Performance Metrics	**BSF-EHR**	**CNN**	**GIT2FMFS**	**SAGN**	**Proposed TaylorAVO-SqueezeNet**
Limited block size						
By varying training data	Accuracy	0.8259	0.8647	0.8998	0.9136	0.9368
	Sensitivity	0.8583	0.8988	0.9062	0.9272	0.9493
	Specificity	0.8167	0.8517	0.8788	0.9012	0.9218
By varying k-fold	Accuracy	0.8253	0.8583	0.8910	0.9094	0.9363
	Sensitivity	0.8576	0.8923	0.9016	0.9271	0.9492
	Specificity	0.8160	0.8428	0.8736	0.9007	0.9202
By varying block size	Accuracy	0.8154	0.8352	0.8500	0.8912	0.9125
	Time(sec.)	115.71	110.69	92.59	88.387	79.969
Larger block size						
By varying Training data	Accuracy	0.8187	0.8709	0.9007	0.9131	**0.9426**
	Sensitivity	0.8278	0.9150	0.9218	0.9282	**0.9481**
	Specificity	0.7788	0.7878	0.8434	0.8813	**0.9345**
By varying k-fold	Accuracy	0.8164	0.8604	0.8966	0.9110	0.9415
	Sensitivity	0.8258	0.9029	0.9206	0.9253	0.9469
	Specificity	0.7781	0.7871	0.8410	0.8805	0.9341

5. Conclusion and Future Directions

In this paper, we used a novel TaylorAVO-SqueezeNet framework, which enables the accurate detection of DR using optimized deep learning techniques without compromising the privacy of EHRs, ensuring optimized security with the use of blockchain. The functioning of the model is initiated with the registration and authentication of the patient data using blockchain. As part of this process, once registration is completed, the admin unit receives the private key, which enables user authentication. Only authorized and valid users are allowed to upload or download information, which is further analyzed by the deep learning model for the detection of disease. The data pre-processing and lesion segmentation techniques used to improve the quality of the input images are part of the deep learning model. In addition to this, feature extraction is performed using the TaylorAVO algorithm to obtain the most significant features. The SqueezeNet classification technique is further implemented to classify the patient's dataset based on normal and abnormal conditions. The results of the classification are finally saved in the blockchain, where only authorized users can see them. The proposed model was tested and compared to the conventional models (BSF-EHR, CNN, GIT2FMFS, SAGN) with a training and testing data ratio of 70:30. The results reveal enhanced accuracy (0.9426), sensitivity (0.9481), and specificity (0.9345). The model yields optimal performance, utilizing lesser computational time and complexity, but there are associated challenges pertinent to an increase in computational complexity. The major issue of blockchain implementation is scalability, especially when dealing with healthcare records. Each computer that confirms the transactions and maintains the records in the blockchain ensures secured data storage from the genesis block to the latest or recent block. The security of the framework is enhanced but faces the associated challenges of network efficiency when the blockchain grows. This issue is likely to be more prominent in the case of EHR, as the record size tends to progressively grow with the increase in the number of patient records. Additionally, although blockchain implementations eliminate the costs associated with third-party transactions, there are additional costs for integrating this technology into legacy systems, especially in healthcare. These potential challenges in the existing framework will be emphasized as part of future work.

Author Contributions: Conceptualization, P.U.; Formal analysis, P.U.; Data curation, P.U., and S.B.; Methodology, P.U.; Resources, S.B.; Software, P.U.; Supervision, S.B.; Validation, S.B.; Visualization, S.B.; Writing—original draft preparation, P.U., and S.B. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the School of Information Technology and Engineering, Vellore Institute of Technology, Vellore 632014, Tamil Nadu, India.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: In this work, the diabetic retinopathy image dataset is taken from the IEEE data port https://ieee-dataport.org/open-access/indian-diabetic-retinopathy-image-dataset-idrid, accessed on 13 August 2022.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

DR	Diabetic Retinopathy
EHR	Electronic Health Record
IPFS	Interplanetary File System
BSF	Blockchain Safety Framework
SHRS-M3DP	Smart Healthcare Recommendation system for Multi-View Disease Prediction
GIT2FMFS	DR detection for Gaussian Interval Type2 Fuzzy Membership
SAGN	Semi-Supervised Auto-Encoder Graph Network

MVDRNet	Multi-View Diabetic Retinopathy Detection Mechanism
CNN	Convolutional Neural Network
DCNN	Deep Convolutional Neural Network
AVO	African Vulture Optimization Algorithm

References

1. Ramzan, S.; Aqdus, A.; Ravi, V.; Koundal, D.; Amin, R.; Al Ghamdi, M.A. Healthcare applications using blockchain technology: Motivations and challenges. *IEEE Trans. Eng. Manag.* **2022**, *early access*. [CrossRef]
2. Chattu, V.K.; Nanda, A.; Chattu, S.K.; Kadri, S.M.; Knight, A.W. The emerging role of blockchain technology applications in routine disease surveillance systems to strengthen global health security. *Big Data Cogn. Comput.* **2019**, *3*, 25. [CrossRef]
3. Zheng, X.; Mukkamala, R.R.; Vatrapu, R.; Ordieres-Mere, J. Blockchain-based personal health data sharing system using cloud storage. In Proceedings of the 2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom), Ostrava, Czech Republic, 17–20 September 2018; pp. 1–6.
4. Siyal, A.A.; Junejo, A.Z.; Zawish, M.; Ahmed, K.; Khalil, A.; Soursou, G. Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives. *Cryptography* **2019**, *3*, 3. [CrossRef]
5. Shynu, P.; Menon, V.G.; Kumar, R.L.; Kadry, S.; Nam, Y. Blockchain-based secure healthcare application for diabetic-cardio disease prediction in fog computing. *IEEE Access* **2021**, *9*, 45706–45720. [CrossRef]
6. Hakak, S.; Khan, W.Z.; Gilkar, G.A.; Assiri, B.; Alazab, M.; Bhattacharya, S.; Reddy, G.T. Recent advances in blockchain technology: A survey on applications and challenges. *Int. J. Ad Hoc Ubiquitous Comput.* **2021**, *38*, 82–100. [CrossRef]
7. Mantey, E.A.; Zhou, C.; Srividhya, S.; Jain, S.K.; Sundaravadivazhagan, B. Integrated Blockchain-Deep Learning Approach for Analyzing the Electronic Health Records Recommender System. *Front. Public Health* **2022**, *10*, 905265. [CrossRef]
8. Hasanova, H.; Tufail, M.; Baek, U.J.; Park, J.T.; Kim, M.S. A novel blockchain-enabled heart disease prediction mechanism using machine learning. *Comput. Electr. Eng.* **2022**, *101*, 108086. [CrossRef]
9. Wang, M.; Zhang, H.; Wu, H.; Li, G.; Gai, K. Blockchain-based Secure Medical Data Management and Disease Prediction. In Proceedings of the Fourth ACM International Symposium on Blockchain and Secure Critical Infrastructure, Nagasaki, Japan, 30 May 30–3 June 2022; pp. 71–82.
10. Artzi, N.S.; Shilo, S.; Hadar, E.; Rossman, H.; Barbash-Hazan, S.; Ben-Haroush, A.; Balicer, R.D.; Feldman, B.; Wiznitzer, A.; Segal, E. Prediction of gestational diabetes based on nationwide electronic health records. *Nat. Med.* **2020**, *26*, 71–76. [CrossRef]
11. Mahiba, C.; Jayachandran, A. Severity analysis of diabetic retinopathy in retinal images using hybrid structure descriptor and modified CNNs. *Measurement* **2019**, *135*, 762–767. [CrossRef]
12. Ramsingh, J.; Bhuvaneswari, V. An efficient map reduce-based hybrid NBC-TFIDF algorithm to mine the public sentiment on diabetes mellitus–a big data approach. *J. King Saud Univ.-Comput. Inf. Sci.* **2021**, *33*, 1018–1029. [CrossRef]
13. Sahlsten, J.; Jaskari, J.; Kivinen, J.; Turunen, L.; Jaanio, E.; Hietala, K.; Kaski, K. Deep learning fundus image analysis for diabetic retinopathy and macular edema grading. *Sci. Rep.* **2019**, *9*, 10750. [CrossRef]
14. Mahmoud, M.H.; Alamery, S.; Fouad, H.; Altinawi, A.; Youssef, A.E. An automatic detection system of diabetic retinopathy using a hybrid inductive machine learning algorithm. *Pers. Ubiquitous Comput.* **2021**, 1–15. [CrossRef]
15. Sahoo, R.; Sekhar, C. Detection of diabetic retinopathy from retinal fundus image using wavelet based image segmentation. *Int. J. Comput. Appl.* **2019**, *182*, 46–50. [CrossRef]
16. Abràmoff, M.D.; Reinhardt, J.M.; Russell, S.R.; Folk, J.C.; Mahajan, V.B.; Niemeijer, M.; Quellec, G. Automated early detection of diabetic retinopathy. *Ophthalmology* **2010**, *117*, 1147–1154. [CrossRef]
17. Atwany, M.Z.; Sahyoun, A.H.; Yaqub, M. Deep learning techniques for diabetic retinopathy classification: A survey. *IEEE Access* **2022**, *10*, 28642–28655. [CrossRef]
18. Gadekallu, T.R.; Khare, N.; Bhattacharya, S.; Singh, S.; Maddikunta, P.K.R.; Srivastava, G. Deep neural networks to predict diabetic retinopathy. *J. Ambient. Intell. Humaniz. Comput.* **2020**, 1–14. [CrossRef]
19. Charanya, R.; Saravanaguru, R.; Aramudhan, M. SeFra: A Secure Framework to Manage eHealth Records Using Blockchain Technology. *Int. J. E-Health Med Commun. (IJEHMC)* **2020**, *11*, 1–16. [CrossRef]
20. Fusco, A.; Dicuonzo, G.; Dell'Atti, V.; Tatullo, M. Blockchain in healthcare: Insights on COVID-19. *Int. J. Environ. Res. Public Health* **2020**, *17*, 7167. [CrossRef]
21. Sivaparthipan, C.; Muthu, B.A.; Fathima, G.; Kumar, P.M.; Alazab, M.; Díaz, V.G. Blockchain Assisted Disease Identification of COVID-19 Patients with the Help of IDA-DNN Classifier. *Wirel. Pers. Commun.* **2022**, *126*, 2597–2620. [CrossRef]
22. Agbo, C.C.; Mahmoud, Q.H.; Eklund, J.M. Blockchain technology in healthcare: A systematic review. *Healthcare* **2019**, *7*, 56. [CrossRef]
23. Han, Y.; Zhang, Y.; Vermund, S.H. Blockchain Technology for Electronic Health Records. *Int. J. Environ. Res. Public Health* **2022**, *19*, 15577. [CrossRef] [PubMed]
24. Javed, I.T.; Alharbi, F.; Bellaj, B.; Margaria, T.; Crespi, N.; Qureshi, K.N. Health-ID: A blockchain-based decentralized identity management for remote healthcare. *Healthcare* **2021**, *9*, 712. [CrossRef] [PubMed]
25. Jabbar, R.; Krichen, M.; Fetais, N.; Barkaoui, K. Adopting formal verification and model-based testing techniques for validating a blockchain-based healthcare records sharing system. In Proceedings of the 22nd International Conference on Enterprise Information Systems, Online, 5–7 May 2020; pp. 261–268.

26. Lodha, G.; Pillai, M.; Solanki, A.; Sahasrabudhe, S.; Jarali, A. Healthcare System Using Blockchain. In Proceedings of the 2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 6–8 May 2021; pp. 274–281.
27. Abbas, A.; Alroobaea, R.; Krichen, M.; Rubaiee, S.; Vimal, S.; Almansour, F.M. Blockchain-assisted secured data management framework for health information analysis based on Internet of Medical Things. *Pers. Ubiquitous Comput.* **2021**, 1–14. [CrossRef]
28. Le Nguyen, T. Blockchain in healthcare: A new technology benefit for both patients and doctors. In Proceedings of the 2018 Portland International Conference on Management of Engineering and Technology (PICMET), Honolulu, HI, USA, 7–11 August 2018; pp. 1–6.
29. Chen, M.; Malook, T.; Rehman, A.U.; Muhammad, Y.; Alshehri, M.D.; Akbar, A.; Bilal, M.; Khan, M.A. Blockchain-Enabled healthcare system for detection of diabetes. *J. Inf. Secur. Appl.* **2021**, *58*, 102771. [CrossRef]
30. Abunadi, I.; Kumar, R.L. BSF-EHR: Blockchain security framework for electronic health records of patients. *Sensors* **2021**, *21*, 2865. [CrossRef]
31. Ihnaini, B.; Khan, M.; Khan, T.A.; Abbas, S.; Daoud, M.S.; Ahmad, M.; Khan, M.A. A smart healthcare recommendation system for multidisciplinary diabetes patients with data fusion based on deep ensemble learning. *Comput. Intell. Neurosci.* **2021**, *2021*, 4243700. [CrossRef]
32. Hemanth, D.J.; Deperlioglu, O.; Kose, U. An enhanced diabetic retinopathy detection and classification approach using deep convolutional neural network. *Neural Comput. Appl.* **2020**, *32*, 707–721. [CrossRef]
33. Gadekallu, T.R.; Khare, N.; Bhattacharya, S.; Singh, S.; Maddikunta, P.K.R.; Ra, I.H.; Alazab, M. Early detection of diabetic retinopathy using PCA-firefly based deep learning model. *Electronics* **2020**, *9*, 274. [CrossRef]
34. Gharaibeh, N.Y. Detection of diabetic retinopathy using partial swarm optimization (PSO) and Gaussian interval type-2 fuzzy membership functions (GIT2FMFS). *Mater. Today Proc.* **2020**. [CrossRef]
35. Li, Y.; Song, Z.; Kang, S.; Jung, S.; Kang, W. Semi-supervised auto-encoder graph network for diabetic retinopathy grading. *IEEE Access* **2021**, *9*, 140759–140767. [CrossRef]
36. Luo, X.; Pu, Z.; Xu, Y.; Wong, W.K.; Su, J.; Dou, X.; Ye, B.; Hu, J.; Mou, L. MVDRNet: Multi-view diabetic retinopathy detection by combining DCNNs and attention mechanisms. *Pattern Recognit.* **2021**, *120*, 108104. [CrossRef]
37. Tang, H.; Liu, X.; Sun, S.; Yan, X.; Xie, X. Recurrent mask refinement for few-shot medical image segmentation. In Proceedings of the IEEE/CVF International Conference on Computer Vision, Montreal, QC, Canada, 11–17 October 2021; pp. 3918–3928.
38. Abdollahzadeh, B.; Gharehchopogh, F.S.; Mirjalili, S. African vultures optimization algorithm: A new nature-inspired metaheuristic algorithm for global optimization problems. *Comput. Ind. Eng.* **2021**, *158*, 107408. [CrossRef]
39. Iandola, F.N.; Han, S.; Moskewicz, M.W.; Ashraf, K.; Dally, W.J.; Keutzer, K. SqueezeNet: AlexNet-level accuracy with 50x fewer parameters and <0.5 MB model size. *arXiv* **2016**, arXiv:1602.07360.
40. Porwal, P.; Pachade, S.; Kamble, R.; Kokare, M.; Deshmukh, G.; Sahasrabuddhe, V.; Meriaudeau, F. Indian diabetic retinopathy image dataset (idrid). *Data* **2018**, *3*, 25. [CrossRef]
41. Mincu, D.; Roy, S. Developing robust benchmarks for driving forward AI innovation in healthcare. *Nat. Mach. Intell.* **2022**, *4*, 916–921. [CrossRef]