Egyptian Informatics Journal 23 (2022) 69–75

Contents lists available at ScienceDirect

Egyptian Informatics Journal

journal homepage: www.sciencedirect.com

Full length article

Private blockchain-based encryption framework using computational intelligence approach

Taher M. Ghazal [a,b,*], Mohammad Kamrul Hasan [a], Siti Norul Huda Sheikh Abdullah [a], Khairul Azmi Abu Bakar [a], Hussam Al Hamadi [c]

[a] Center for Cyber Security, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia (UKM), Bangi, Selangor 43600, Malaysia
[b] School of Information Technology, Skyline University College, University City Sharjah, Sharjah 1797, United Arab Emirates
[c] Center for Cyber-Physical Systems Khalifa University, United Arab Emirates

ARTICLE INFO

Article history:
Received 5 February 2022
Revised 16 June 2022
Accepted 22 June 2022
Available online 5 August 2022

Keywords:
Private blockchain
Computational Intelligence
Machine Learning

ABSTRACT

Electronic Health monitoring system has performed an essential role in managing healthcare monitoring. E-health can provide effective and valuable facilities for the patients to monitor. Though, there are protection disputes in the current E-Health system. The current e-health system, on the other hand, has security issues. Malevolent doctors may work together with cloud Storage Service Providers (CSPs) to interfere with patients' electronic health records (EHRs) or promptly leak EHR matter to other enemies for income. (EHRs). The malevolent doctors may conspire with the Patient Healthcare Monitoring Service Provider (PHMSP) to manipulate with the patients'. For profit, EHRs or directly divulge the EHR content of EHRs to other opponents. Block-chain has recently appeared as one of the most powerful methods in the protection and secrecy fields. It is assumed to be the promised security approach that will eventually replace the security challenges in existing e-health monitoring systems. Encryption in blockchain refers to technical methods that make accessing encrypted data difficult for unauthorized resources. This research proposed a blockchain-based encryption framework to provide security-based solutions using a computational intelligence methodology. The proposed approach provides better results in terms of 0.93 in the training phase and 0.91 in the validation accuracy.

1. Introduction

Data has been at the heart of all technological advancements. It has prompted many organizations and businesses to build technologies that enable interconnection between different services. Patients and other users can log in to medical facilities and retrieve health data via the internet using a healthcare information system. Secure communication is necessary to protect patient privacy and ensure public network security.

Information access, like health care, has become a part of our daily lives due to rapid technological advancement. Data sharing has become a hot topic in personal health care. The security of data transmission is becoming increasingly important. The blockchain method has also enticed more attention to secure communication mechanisms in recent years. Blockchain is one of the primary technologies that has aided this movement [1]. Blockchain is a decentralized database that is hard to manipulate, construct, or trace. It is described as a connected chain of blocks. All transaction data is stored on the blockchain, and nearly no one can change it once it has been registered. This immutability is derived from blockchain technology and the method as a whole rather than from a single operation. The blockchain method is easier to use and more stable than other protection systems.

The blockchain employs cryptographic procedures, asymmetric-key processes, and hash roles. Hash roles provide each

* Corresponding author at: Center for Cyber Security, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia (UKM), Bangi, Selangor 43600, Malaysia.
E-mail addresses: Taher.ghazal@skylineuniversity.ac.ae (T.M. Ghazal), mkhasan@ukm.edu.my (M.K. Hasan), Snhsabdullah@ukm.edu.my (Siti Norul Huda Sheikh Abdullah), khairul.azmi@ukm.edu.my (K.A.A. Bakar), Hussam.alhamadi@ku.ac.ae (H. Al Hamadi).

Peer review under responsibility of Faculty of Computers and Information, Cairo University.

Production and hosting by Elsevier

https://doi.org/10.1016/j.eij.2022.06.007
1110-8665/

participant with a unified picture of the blockchain. In blockchains, the SHA-256 hashing process is often employed as the hash role. Encryption methods are used for security characteristics, including privacy and data access monitor. Obtaining access control, on the other hand, is a substantial difficulty. In 2007, Bethencourt was the first to utilize the CP-ABE method. The ciphertext is related to an open structure in the CP-ABE method, and the user's private keys are produced from attributes. [2].

Computational intelligence techniques have been employed in various IoT security solutions, including malware detection, cyber threat detection, suspicious activity monitoring, intrusion detection, and cyberattack detection. The IoT may use CI approaches to improve its cybersecurity capabilities and secure IoT apps and consumers. A safe and computationally smart solution is needed to protect compassionate and secret healthcare data and deliver private communication between the User, Database Service provider, and Owner. [3].

There is no simple solution for bringing the decentralization notion of blockchain technology and security approaches together. There is still a great deal of work in this setting. Several researchers have looked into blockchain-based protection schemes in recent years, even though most have not proposed a structure or idea for such systems. As a result, research into blockchain-based encryption framework models with security mechanisms is meaningful and valuable. This research paper presents a private Blockchain-based encryption framework model for security purposes.

The SVM algorithm conducts categorization by creating a multidimensional hyperplane that maximizes the margin between two data clusters to best differentiate between two classes. This approach generates great discriminative power by transforming the input space into a multidimensional spa using unique nonlinear functions known as kernels.

2. Literature review

ML methods for healthcare include algorithms with self-learning neural networks that examine outdoor data on a patient's ailment, X-rays, CT scans, various tests, and screenings to improve treatment quality. The Support Vector Machine (SVM) method is a supervised ML technique that has proved efficient in handling classification issues in various biomedical domains, including bioinformatics [4,5].

Several the researchers have previously worked on a Blockchain-based encryption framework model, some of which are included in this section. The authors in this research use Blockchain to secure user data, demonstrating how to leverage blockchain method in Intrusion Detection Systems (IDSs). We employ blockchain technology in cloud storage design to provide a safe consumer environment. A blockchain network distributes sources, including connections, rather than focusing on one data centre or server.[6].

The authors suggest a blockchain-based data-sharing strategy that uses smart contracts and ABE to accomplish user revocation. The proposed architecture uses attribute level revocation to control privileges during data sharing. It uses a trusted agency for strategic management and encodes or decrypts data, putting the security of user info at risk. Users will be unable to access their information if the key management centre fails, and the complete structure will be altered.[7].

The authors recommend a new ABE method using blockchain expertise to contract out decoding safely. A smart contract is used in the proposed architecture to confirm the alternative entity's payout for a successful outsourced decryption operation. It also employs the sampling method to permit miners to verify the decryption result's accuracy. On the other hand, the proposed strategy leverages the ABE mechanism to ensure only the safe outsourcing decoding process, not the cancellation method.[8].

In this research, the authors must consider many architectural difficulties in implementing blockchain for IoT and maintaining security in industrial applications. Block-chain technologies have a lot of promise for tackling security, privacy, and trust issues in multi-stakeholder applications despite the difficulties. [9].

Weng et al. presented Deep Chain as a dispersed agenda by building blockchain-based motivation processes to meet three targets during cooperation training: secrecy, auditability, and equality. Using blockchain smart contracts and cryptography primitives, Deep Chain is suggested to protect local ramps' confidentiality and assure the training mrthod' auditability. [10].

In this research, The CI, according to Alansari et al., is critical in interpreting big data in bioinformatics, such as DNS sequence analysis, big medical data, and so on. In sophisticated and computationally expensive data processing, CI-based approaches can be applied. [11].

The authors investigated how to develop the privacy of the blockchain for secrecy safety in IoT devices. They saw Zero-Information verification as a Blockchain privacy improvement solution to eliminate security concerns like personal information invasion via block inquiry. The use case being investigated is the intelligent meter control pricing for safe charging in a single-layer Block-chain-based safe architecture. [12].

Computational intelligence paradigms are emerging because of the simultaneous placement of boosted networked interaction infrastructure, High-Performance Data Analytics (HPDA) methods, and High-Power Computing (HPC) abilities at the fog/edge, which can provide customized facilities for on-request industrial claims, such as anomaly finding, fault prediction, and enhanced digital hyper-connectivity, according to the authors of this study. [13,14]. Computational intelligence techniques used in different application to make it intelligent [15,16,17,18,19,20,21,22]. Table 1. shows the research gap between the proposed model and the literature review.

3. Proposed methodology

With the beginning of the Internet of Medical Things (IoMT) technologies, many smart gadgets have been built and combined into the healthcare monitoring system in daily life. However, security and privacy are significant challenges while communicating patient healthcare data. The growing number of gadgets and users, recent planning, and the interaction protocols (main system) cannot respond adequately to system requests such as verification, permission, and access administration. A private blockchain technology-based encryption framework is proposed in this research work to overcome the multiple phases of security, authentication, and authorization challenges. The proposed research framework shown in Fig. 1 provides an efficient e-health monitoring system while securing the patient's electronic health records.

Fig. 1 shows that the proposed system is divided into three steps: Private blockchain, Training phase, and Validation phase. Firstly, the patient data is sensed by the IoMT infrastructure and forwarded to the blockchain technology, which is used for resource authorization and access control of the proposed framework. All authorized resources within the medical care information system, such as healthcare experts, patients, and healthcare workers, must obtain patients' health records. The IoMT infrastructure detects patient health data from different medical companies such as hospitals and specialists. All users, including patients, healthcare professionals, employees, and medical staff, must request patients'

Table 1
Research Gap with Literature.

Authors	Blockchain	Preprocessing Layer	Machine Learning Technique	Accuracy	Miss-Rate
Chakraborty, S., et al., [22]	No	No	Artificial Neural Network	0.8944	0.1056
Redkar, S., et al., [23]	No	No	Support Vector Machine	0.7659	0.2341
Gu, D., et al.,[24]	No	No	CNN	0.8215	0.1785
Kroll, J. P., et al., [25]	No	No	NB	0.81	0.19
Yoo, T.K., et al., [26]	No	Yes	XGB	0.78	0.22

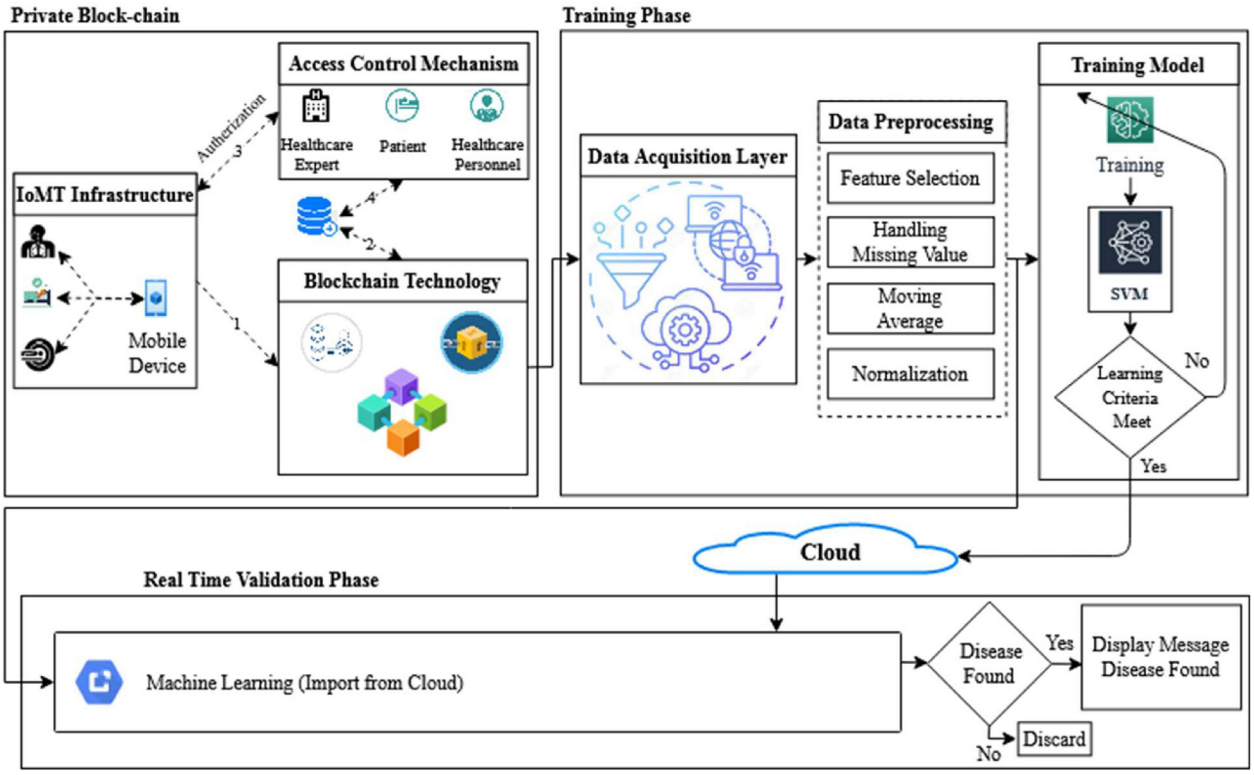

Fig. 1. Proposed framework for secure communication.

health records within the medical information system. Patients' healthcare data is saved in the healthcare service provider's database, which takes advantage of the private blockchain's non-tampering feature, as shown in Fig. 2.

Fig. 2 reveals that the user first found the Private Block-chain Connected Gateway (PBCG) smart contract discourse and formerly entered the subgroup devices list. The user must agree to any device's privacy policies before using it. This agreement is stored in the blockchain to use the PBCG when the user requests access to devise information.

Smart Contracts. This section of the authentication protocol explains a smart contract and its liabilities. Smart contracts are in place to manage the PBCG (logical communication) and all interactions between devices and the PBCG (information and privacy policies). As presented in Fig. 3 shows, the interaction between the gadgets and the PBCG is documented in the blockchain and is accomplished over it. We can think of the blockchain as a third-party trusted advisor (TTP). Therefore, the protocol's parties cannot be manipulated or violated. Table 2 presents a full overview of the dataset features.

The data obtained from the private blockchain layer is deposited to the training phase in raw form in the data acquisition layer. The raw data is sent to the preprocessing layer to mitigate the noisy data using feature selection, handling missing values, moving averages, and normalization. The preprocessed data is then forwarded to the training model via the SVM algorithm.

As we know, during SVM the line equation is.

$$\text{ɤ} = \text{ʜ}\text{ɥ} + \varsigma [19] \tag{3}$$

In Eq. (3), 'ʜ' represents the line slope and 'ς' the intersect. ɥ represent the dataset features mentioned in Table 2. Hence,

$$\text{ʜ}\text{ɥ} - \text{ɤ} + \varsigma = 0 [19]$$

Let $\bar{\text{ŧ}} = (\text{ɥ}, \text{ɤ})^{\text{T}}$ and $\bar{\text{ŧ}} = (\text{ʜ}, -1)$. Then, the equation becomes.

$$\overrightarrow{\text{ŧ}}.\bar{\text{ŧ}} + \varsigma = 0 [19] \tag{4}$$

This equation comes from two-dimensional vectors. However, Equation (4), defined as the hyperplane, performs for any number of dimensions. The direction of a vector $\bar{\text{ŧ}} = (\text{ɥ}, \text{ɤ})^{\text{T}}$ is $\bar{\text{ŧ}}$ and is distinct as.

$$\text{ŧ} = \frac{\text{ɥ}}{||\text{ŧ}||} + \frac{\text{ɤ}}{||\text{ŧ}||} [19] \tag{5}$$

where

$$||\text{ŧ}|| = \sqrt{\text{ɥ}_{+}^{2}\ \text{ɤ}_{+}^{2}\ \cdots\cdots\cdots\ \text{ŧ}_{\varsigma}^{2}} [19]$$

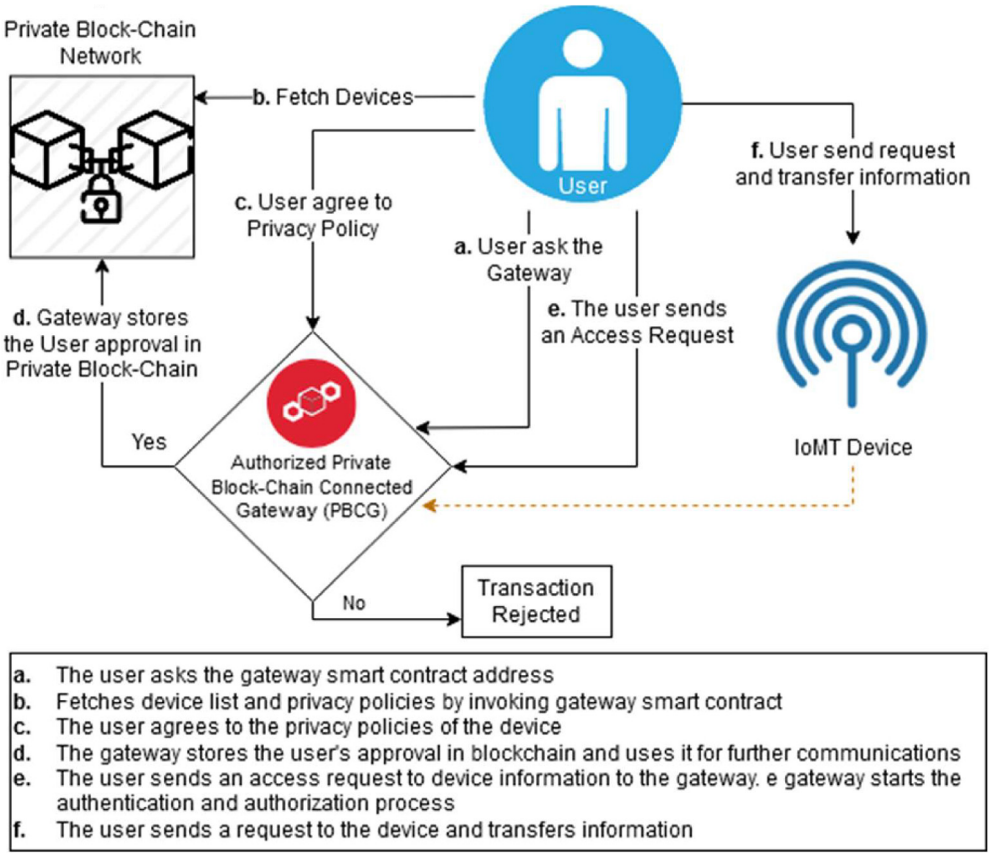

Fig. 2. Private blockchain-based authentication.

As we know that.

$$\cos(\theta) = \frac{\mathfrak{u}}{||\mathfrak{t}||} \text{ and } \cos(\mu) = \frac{\mathfrak{x}}{||\mathfrak{t}||}$$

Equation (5) can also be written as.

$$\mathfrak{y} = (\cos(\theta),\ \cos(\mu))$$

$$\overrightarrow{\mathfrak{y}}.\overrightarrow{\mathfrak{t}} = ||\mathfrak{y}||\ ||\mathfrak{t}||\cos(\theta)$$

$$\theta = \upsilon - \mu$$

$$\cos(\theta) = \cos(\upsilon - \mu) = \cos(\upsilon)\cos(\mu) + \sin(\upsilon)\sin(\mu)$$

$$= \frac{\vartheta}{||\mathfrak{y}||}\frac{\mathfrak{u}}{||\mathfrak{t}||} + \frac{\alpha}{||\mathfrak{y}||}\frac{\mathfrak{x}}{||\mathfrak{t}||} = \frac{\vartheta\mathfrak{u} + \alpha\mathfrak{x}}{||\mathfrak{y}||||\mathfrak{t}||}$$

$$\mathfrak{y}.\mathfrak{t} = ||\mathfrak{y}||||\mathfrak{t}||\left[\frac{\vartheta\mathfrak{u} + \alpha\mathfrak{x}}{||\mathfrak{y}||||\mathfrak{t}||}\right]$$

$$\overrightarrow{\mathfrak{y}}.\overrightarrow{\mathfrak{t}} = \sum_{i=1}^{\zeta} \mathfrak{y}_i\mathfrak{t}_i \tag{6}$$

The dot product can be compared using Equation (11) for ζ dimensional vectors:

Let.

$$\mathrm{B} = \mathrm{M}(\mathfrak{y}.\mathfrak{t} + \varsigma)$$

If sign (B) > 0, then this is appropriately classified; and if the sign (B) < 0, then it is imperfectly classified.

Calculate f on a training dataset by dataset Π:

$$\mathrm{B}_i = \mathrm{M}_i(\mathfrak{y}.\mathfrak{t} + \varsigma)$$

$\mathfrak{p}$ is the functional margin of the dataset.

$$\mathfrak{p} = \min_{i=1\cdots\mathfrak{v}} \mathrm{B}_i$$

The goal is to discover an optimal hyperplane, which means finding the optimal hyperplane values of $\mathfrak{y}$ and B. When comparing hyperplanes, one through the largest $\mathfrak{p}$ will be chosen. $\mathfrak{p}$ is the geometric margin of the dataset.

Lagrangian function:

$$\check{\mathrm{A}}(\mathfrak{y}, \varsigma, \mu) = \frac{1}{2}\mathfrak{y}.\mathfrak{y} - \sum_{i=1}^{\mathfrak{v}} \mu_i\left[\mathrm{M} : (\mathfrak{y}.\mathfrak{t} + \varsigma) - 1\right]$$

$$\nabla_{\mathfrak{y}}\check{\mathrm{A}}(\mathfrak{y}, \varsigma, \mu) = \mathfrak{y} - \sum_{i=1}^{\mathfrak{v}} \mu_i \mathrm{M}_i \mathfrak{t}_i = 0 \tag{7}$$

$$\nabla_{\varsigma}\check{\mathrm{A}}(\mathfrak{y}, \varsigma, \mu) = -\sum_{i=1}^{\mathfrak{v}} \mu_i \mathrm{M}_i = 0 \tag{8}$$

From Equations (7) and (8), we get.

$$\mathfrak{y} = \sum_{i=1}^{\mathfrak{v}} \mu_i \mathrm{M}_i \mathfrak{t}_i \text{ and } \sum_{i=1}^{\mathfrak{v}} \mu_i \mathrm{M}_i = 0 \tag{9}$$

while substituting the Lagrangian function $\check{\mathrm{A}}$:

$$\mathfrak{y}(\mu, \varsigma) = \sum_{i=1}^{\mathfrak{v}} \mu_i - \frac{1}{2}\sum_{i=1}^{\mathfrak{v}}\sum_{j=1}^{\mathfrak{v}} \mu_i\mu_j \mathrm{M}_i\mathrm{M}_j\mathfrak{t}_i\mathfrak{t}_j$$

Thus,

$$\max_{\mu} \sum_{i=1}^{\mathfrak{v}} \mu_i - \frac{1}{2}\sum_{i=1}^{\mathfrak{v}}\sum_{j=1}^{\mathfrak{v}} \mu_i\mu_j \mathrm{M}_i\mathrm{M}_j\mathfrak{t}_i\mathfrak{t}_j \tag{10}$$

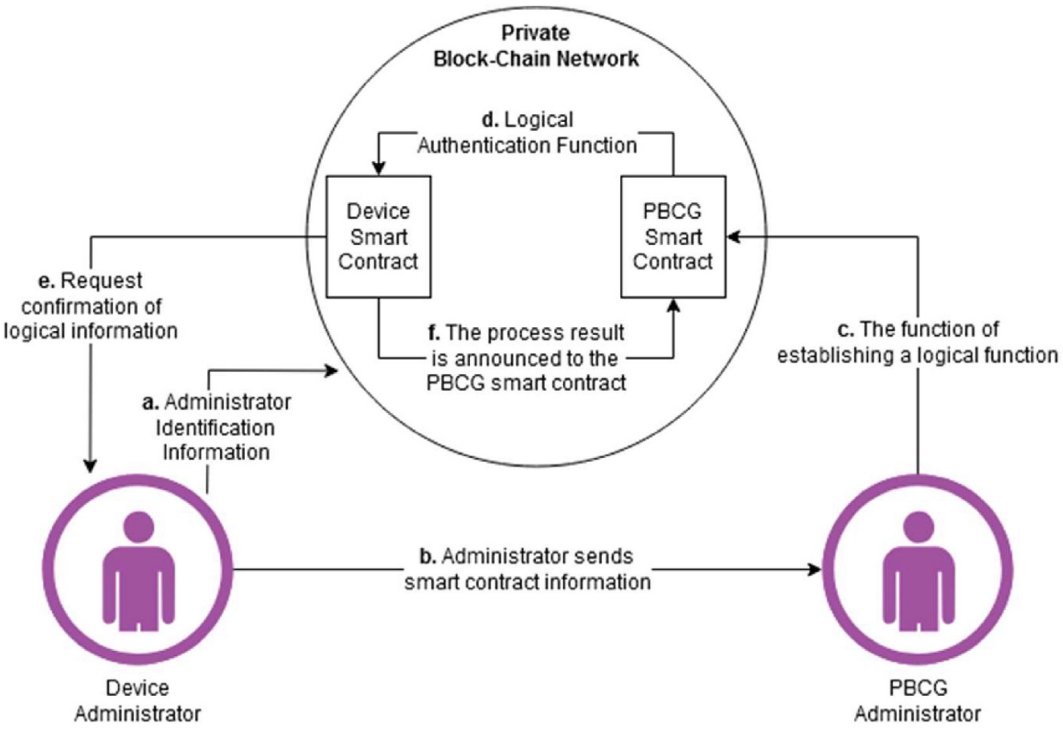

Fig. 3. Device attachment communications in the blockchain-based authentication protocol.

Table 2
Dataset Feature [28].

Sr. No.	Features	Datatype
1	age	Integer
2	sex	Character
3	bmi	Nominal
4	children	Nominal
5	smoker	Integer
6	region	Integer
7	charges	Integer
8	health	Integer

subject to $\mu_i \geq 0$, $i = 1 \cdots .\mathfrak{G}$, $\sum_{i=1}^{\mathfrak{G}} \mu_i M_i = 0$. [19].

Due to inequalities in the constraints, the Lagrangian multiplier technique is extended to Karush-Kuhn-Tucker (KKT) situations. KKT's complimentary status states that.

$$\mu_i \left[M_i(\mathfrak{y}_i.\mathfrak{t}^* + \varsigma) - 1\right] = 0 \tag{11}$$

$\mathfrak{t}^*$ denotes the optimal point.

μ is the positive value in addition to μ because the additional aspects are ≈ 0.

Thus,

$$M_i((\mathfrak{y}_i.\mathfrak{t}^* + \varsigma) - 1) = 0 \tag{12}$$

The points near the hyperplane are called support vectors. Equation (12) states that.

$$\mathfrak{y} - \sum_{i=1}^{\mathfrak{G}} \mu_i M_i \mathfrak{t}_i = 0$$

$$\mathfrak{y} = \sum_{i=1}^{\mathfrak{G}} \mu_i M_i \mathfrak{t}_i \tag{13}$$

To compute the value of ς we get.

$$M_i((\mathfrak{y}_i.\mathfrak{t}^* + \varsigma) - 1) = 0 \tag{14}$$

In Eq. (14), multiply both sides by M to get.

$$M_i^2((\mathfrak{y}_i.\mathfrak{t}^* + \varsigma) - M_i) = 0$$

where $M_i^2 = 1$

$$((\mathfrak{y}_i.\mathfrak{t}^* + \varsigma) - M_i) = 0$$

$$\varsigma = M_i - \mathfrak{y}_i.\mathfrak{t}^* \tag{15}$$

Then

$$\varsigma = \frac{1}{я} \sum_{i=1}^{я} (M_i - \mathfrak{y}.\mathfrak{t}) \tag{16}$$

$я$ is the number of support vectors. On one occasion, the hyperplane will create perceptions. The hypothesis function is.

$$c(tf_i) = \begin{bmatrix} 1\ if\ tf.t + \zeta > 0 \\ 0\ if\ tf.t + \zeta \leqslant 0 \end{bmatrix} \quad (17)$$

The hyperplane is classified as health issue (positive), and the point below is classified as no health issue (negative). Therefore, the primary purpose of the SVM algorithm is to perceive a hyperplane that can disperse the data precisely, in addition to the best need to be found, which is often called a hyperplane.

The trained patterns are then checked to see if the learning criteria are met. If it is Yes, the trained output is stored on the cloud, and if not, it is updated, and so on. The trained patterns are then imported from the cloud for prediction purposes in the validation phase. It is rechecked that if the disease is found, a message will be displayed that the disease is found, and the method will be abandoned in case of no.

4. Simulation results

This research introduces an intelligent system to predict disease better and more efficiently empowered with a computational intelligence approach. SVM techniques are being applied to the total number of instances 302 to predict real-time disease. The proposed method is applied to a dataset collected from the Kaggle data repository [28]. Moreover, the dataset is categorized into training comprises of 70% (212 samples) and 30% (90 samples) for the mentioned training and validation purposes. Different parameters used for performance calculation with other metrics are drawn by the formulas given as follows:

$$Sensitivity = \frac{\sum True\ Positive}{\sum Condition\ Positive} \quad (18)$$

$$Specificity = \frac{\sum True\ \ Negative}{\sum Condition\ \ Negative} \quad (19)$$

Table 3
Training of the proposed model during the prediction of disease (SVM).

Proposed Model Training			
Input	All no. of samples (212)	Outcome (output)	
	Expected output	Forecast Positive Actual Positive (TP)	Forecast Negative Erroneous Positive (FP)
	131 Positive	119	12
		Erroneous Negative	Actual Negative
	81 Negative	3	78

Table 4
Validation of the proposed model during the prediction of diseases (SVM).

Proposed Model Validation			
Input	All no. of samples (90)	Outcome (output)	
	Estimated output	Forecast Positive Actual Positive	Forecast Negative Erroneous Positive
	46 Positive	43	3
		Erroneous Negative	Actual Negative
	44 Negative	5	39

$$Accuracy = \frac{\sum True\ \ Positive + \sum True\ \ Positive}{\sum Total\ \ Population} \quad (20)$$

$$Miss - Rate = \frac{\sum False\ \ Negative}{\sum Condition\ \ Positive} \quad (21)$$

$$Fallout = \frac{\sum False\ \ Positive}{\sum Condition\ \ Negative} \quad (22)$$

$$LikelihoodPositiveRatio = \frac{\sum True\ \ Positive\ \ Ratio}{\sum False\ \ Positive\ \ Ratio} \quad (23)$$

$$LikelihoodNegativeRatio = \frac{\sum True\ \ Positive\ \ Ratio}{\sum False\ \ Positive\ \ Ratio} \quad (24)$$

$$PositivePredictiveValue = \frac{\sum True\ \ \ Positive}{\sum Predicted\ \ Condition\ \ Positive} \quad (25)$$

$$NegativePredictiveValue = \frac{\sum True\ \ Negative}{\sum Predicted\ \ Condition\ \ Negative} \quad (26)$$

It is shown in Table 3 that the proposed system prediction of disease through the training period. During training, a sum of 2112 samples is used, which are divided into 131,81 positive and negative samples, respectively. 119 true positives are successfully forecast, and no disease is detected, but 12 records are wrongly predicted as negatives, indicating disease. Similarly, 81 samples are obtained, with negative showing disease and positive showing no disease, with 78 samples correctly identified as negative showing disease and 3 samples inaccurately forecast as positive, indicating no disease despite the disease.

It is shown in Table 4 the proposed system prediction of disease through the training period. During training, a sum of 90 samples is used, which are divided into 46,44 positive and negative samples, respectively. 43 true positives are successfully forecast, and no disease is detected, but 3 logs are incorrectly predicted as negatives, indicating disease. Similarly, 44 samples are obtained, with negative showing disease and positive showing no disease, with 39 samples correctly identified as negative showing disease and 5 samples inaccurately forecast as positive, indicating no disease despite the disease.

It is shown in Table 5 (SVM) that during training, the performance of the proposed system in terms of accuracy sensitivity, specificity, miss rate, and precision gives 0.93, 0.97, 0.86, 0.07, and 0.91, respectively. And during validation, the proposed model provides 0.91, 0.93, 0.89, 0.09, and 0.90 in states of correctness, compassion, specificity, loss rate, and accuracy, respectively. In addition, the proposed system during training gives 0.133, 7.29, 0.081, and 0.96, and during validation, 0.113, 8.23, 0.101, and 0.93 in words of drop out positive probability ratio, probability negative ratio, and negative forecast value, respectively.

Table 6 shows the performance of the proposed frame using the ML Technique with previous approaches [22–27]. The proposed model performance in terms of "accuracy and miss rate" during the training and validation phase. During training, the proposed model gives 0.93 and 0.07 detection accuracy and miss rate, respectively. And during validation, the proposed model gives 0.91 and 0.09 detection accuracy and miss rate, respectively. The

Table 5
Performance evaluation of proposed disease detection system in training and validation using different statistical measures (SVM).

SVM	Accuracy	Sensitivity TPR	Specificity TNR	Miss-Rate (%) FNR	Fall-out FPR	LR+	LR-	PPV (Precision)	NPV
Training	0.93	0.97	0.86	0.07	0.133	7.29	0.081	0.91	0.96
Validation	0.91	0.93	0.89	0.09	0.113	8.23	0.101	0.90	0.93

Table 6
Comparison of the proposed model with Literature.

Authors	Blockchain	Preprocessing Layer	Machine Learning Technique	Accuracy	Miss-Rate
Chakraborty, S., et al., [22]	No	No	Artificial Neural Network	0.8944	0.1056
Redkar, S., et al., [23]	No	No	Support Vector Machine	0.7659	0.2341
Gu, D., et al.,[24]	No	No	CNN	0.8215	0.1785
Kroll, J. P., et al., [25]	No	No	NB	0.81	0.19
Yoo, T.K., et al., [26]	No	Yes	XGB	0.78	0.22
Proposed Model	Yes	Yes	SVM	0.91	0.09

proposed model shows that the presented approach gives better results than the previously published approaches.

5. Conclusion

In this suggested study work, a private blockchain-based encryption framework using a computational intelligence approach is presented for the sake of encryption. The computational intelligence approach is beneficial in obtaining similar attributes in the gathered data and identifying process. The test findings on a basic encryption framework reveal that private blockchain-based with computational intelligence scales efficiently as datasets develop. The findings also demonstrate that using much training data leads to better results. The detection accuracy of the resulting security system is 0.93 in the training phase and 0.91 in the validation phase, which is higher than earlier printed systems.

References

[1] Ali A, Almaiah MA, Hajjej F, Pasha MF, Fang OH, Khan R, et al. An Industrial IoT-Based Blockchain-Enabled Secure Searchable Encryption Approach for Healthcare Systems Using Neural Network. Sensors 2022;22(2):572.

[2] Sharma P, Jindal R, Borah MD. Blockchain-based cloud storage system with CP-ABE-based access control and revocation process. The Journal of Supercomputing 2022:1–29.

[3] Majhi M, Pal AK, Pradhan J, Islam SK, Khan MK. Computational intelligence based secure three-party CBIR scheme for medical data for cloud-assisted healthcare applications. Multimedia Tools and Applications 2021:1–33.

[4] Ng KLS, Mishra SK. De novo SVM classification of precursor microRNAs from genomic pseudo hairpins using global and intrinsic folding measures. Bioinformatics 2007;23(11):1321–30.

[5] Rice SB, Nenadic G, Stapley BJ. Mining protein function from text using term-based support vector machines. BMC Bioinf 2005;6(1):1–11.

[6] Khan MA, Abbas S, Rehman A, Saeed Y, Zeb A, Uddin MI, et al. A machine learning approach for blockchain-based smart home networks security. IEEE Network 2020;35(3):223–9.

[7] Nærland K, Müller-Bloch C, Beck R, Palmund S. December. Blockchain to Rule the Waves-Nascent Design Principles for Reducing Risk and Uncertainty in Decentralized Environments. In ICIS, 2017.

[8] Baza M, Nabil M, Lasla N, Fidan K, Mahmoud M, Abdallah M. In: April. Blockchain-based firmware update scheme tailored for autonomous vehicles. IEEE; 2019. p. 1–7.

[9] Ruggeri A, Celesti A, Fazio M, Villari M. An Innovative Blockchain-Based Orchestrator for Osmotic Computing. Journal of Grid Computing 2022;20(1):1–17.

[10] Rahmadika, S., Firdaus, M., Jang, S. and Rhee, K.H., 2021. Blockchain-enabled 5g edge networks and beyond: an intelligent cross-silo federated learning approach. Security and Communication Networks, 2021.

[11] Zhao S, Li S, Qi L, Da XuL. Computational intelligence enabled cybersecurity for the internet of things. IEEE Transactions on Emerging Topics in Computational Intelligence 2020;4(5):666–74.

[12] Badr S, Gomaa I, Abd-Elrahman E. Multi-tier blockchain framework for IoT-EHRs systems. Procedia Comput Sci 2018;141:159–66.

[13] Zeb S, Mahmood A, Hassan SA, Piran MJ, Gidlund M, Guizani M. Industrial digital twins at the nexus of nextG wireless networks and computational intelligence: A survey. Journal of Network and Computer Applications 2022:103309.

[14] Cortes C, Vapnik V. Support-vector networks Machine learning 1995;20(3):273–97.

[15] Bukhari, M.M., Ghazal, T.M., Abbas, S., Khan, M.A., Farooq, U., Wahbah, H., Ahmad, M. and Adnan, K.M., 2022. An Intelligent Proposed Model for Task Offloading in Fog-Cloud Collaboration Using Logistics Regression. Computational Intelligence and Neuroscience, 2022.

[16] Asif, M., Abbas, S., Khan, M. A., Ftima, A., Khan, M. A., & Lee, S. W. (2021). MapReduce Based Intelligent Model for Intrusion Detection Using Machine Learning Technique. Journal of King Saud University-Computer and Information Sciences.

[17] Abbas, S., Alhwaiti, Y., Fatima, A., Khan, M.A., Khan, M.A., Ghazal, T.M., Kanwal, A., Ahmad, M. and Elmitwally, N.S., 2022. Convolutional neural network based intelligent handwritten document recognition.

[18] Daoud, M.S., Aftab, S., Ahmad, M., Khan, M.A., Iqbal, A., Abbas, S., Iqbal, M. and Ihnaini, B., 2022. Machine Learning Empowered Software Defect Prediction System.

[19] Saleem M, Abbas S, Ghazal TM, Khan MA, Sahawneh N, Ahmad M. Smart cities: Fusion-based intelligent traffic congestion control system for vehicular networks using machine learning techniques. Egyptian Informatics Journal 2022.

[20] Saleem M, Khan MA, Abbas S, Asif M, Hassan M, Malik JA. In: July. Intelligent FSO link for communication in natural disasters empowered with fuzzy inference system. IEEE; 2019. p. 1–6.

[21] Batool T, Abbas S, Alhwaiti Y, Saleem M, Ahmad M, Asif M, et al. Intelligent Model Of Ecosystem For Smart Cities Using Artificial Neural Networks. INTELLIGENT AUTOMATION AND SOFT COMPUTING 2021;30(2):513–25.

[22] Chakraborty, S., Aich, S. and Kim, H.C, "3D textural, morphological and statistical analysis of voxel of interests in 3T MRI scans for the detection of Parkinson's disease using artificial neural networks" In Healthcare, vol. 8, no. 1, pp. 34, 2020. Multidisciplinary Digital Publishing Institute.

[23] Redkar S, Mondal S, Joseph A, Hareesha KS. A machine learning approach for drug-target interaction prediction using wrapper feature selection and class balancing. Mol Inf 2020;39(5):1900062.

[24] Gu D, Li Y, Jiang F, Wen Z, Liu S, Shi W, et al. VINet: A Visually Interpretable Image Diagnosis Network. IEEE Trans Multimed 2020;22:1720–9.

[25] Kroll, J.P.; Eickhoff, S.B.; Hoffstaedter, F.; Patil, K.R. Evolving complex yet interpretable representations: Application to Alzheimer's diagnosis and prognosis. In Proceedings of the 2020 IEEE Congress on Evolutionary Computation (CEC), Glasgow, UK, 19–24 July 2020.

[26] Yoo TK, Ryu IH, Choi H, Kim JK, Lee IS, Kim JS, et al. Explainable machine learning approach as a tool to understand factors used to select the refractive surgery technique on the expert level. Transl Vis Sci Technol 2020;9:1–14.

[27] Aslam N. Explainable Artificial Intelligence Approach for the Early Prediction of Ventilator Support and Mortality in COVID-19 Patients. Computation 2022;10(3):36.

[28] https://www.kaggle.com/