healthcare

MDPI

Article

Enhancing Privacy and Data Security across Healthcare Applications Using Blockchain and Distributed Ledger Concepts

Haibing Liu [1,2,*], Rubén González Crespo [3] and Oscar Sanjuán Martínez [3,*]

1 Evergrande School of Management, Wuhan University of Science and Technology, Wuhan 430000, China
2 School of Economics and Management, Lanzhou Jiaotong University, Lanzhou 730070, China
3 Computer Science Department, School of Engineering and Technology, Universidad Internacional de la Rioja (UNIR), 26006 Logroño, Spain; ruben.gonzalez@unir.net
* Correspondence: liuhb13@lzu.edu.cn (H.L.); oscar.sanjuan@ieee.org (O.S.M.)

Received: 21 May 2020; Accepted: 22 July 2020; Published: 29 July 2020

Abstract: Nowadays, blockchain is developing as a secure and trustworthy platform for secure information sharing in areas of application like banking, supply chain management, food industry, energy, the Internet, and medical services. Besides, the blockchain can be described in a decentralized manner as an immutable ledger for recording data entries. Furthermore, this new technology has been developed to interrupt a variety of data-driven fields, including the health sector. However, blockchain refers to the distributed ledger technology, which constitutes an innovation in the information recording and sharing without a trusted third party. In this paper, blockchain and Distributed Ledger-based Improved Biomedical Security system (BDL-IBS) has been proposed to enhance the privacy and data security across healthcare applications. Further, our goal is to make it possible for patients to use the data to support their care and to provide strong consent systems for sharing data among different organizations and applications, since this includes managing and accessing a high amount of medical information, and this technology can maintain data to ensure reliability. Finally, results show that new blockchain-based digital platforms allow for fast, easy, and seamless interactions between data suppliers to enhance privacy and data security, including for patients themselves.

Keywords: data security; privacy; healthcare applications; blockchain technology; distributed ledger technology

1. Introduction

Recent trends in technology are exploited for diverse real-world applications to provide definite solutions for end users. Assimilating technological aspects in user-related application provides diverse advantages, from the quality of service (QoS) to security [1]. The healthcare platform is visualized using electronic health records (EHRs) in its digital and technical format, providing unrestricted access to the end users. Diagnosis centers and healthcare infrastructures provide different access and data sharing processes for their users through EHRs [2–4]. EHR is an organized set of patient-/user-related information that is digitally shared through a secure platform for ubiquitous access [5]. User applications and graphical user interfaces designed for EHR access provide access to the healthcare data through simple authorization and authentication procedures. Since sensitive information, end-to-end security, and privacy are the prime concerns in sharing EHR's between users [6], this is vital as the technology requires additional infrastructures such as cloud, Internet of things, mobile devices, etc. for sharing EHR's [7].

Blockchain is another technology that is commonly used in different applications for providing distributed access to resources and unalterable information [8]. The blockchain paradigm is used for administering security in different communicating and processing systems. Healthcare application does not require trusted third-parties for administering security [9]. The electronic ledger is distributed across different communicating and processing systems to improve the swiftness in security administration and privacy preservation [10]. Besides, blockchain eases EHR sharing between end-user applications and healthcare infrastructures without interrupting the communication process [11,12]. Such facilities are provided through line-of-trust and authentication with interoperability using the distributed electronic ledger technology. Modern healthcare applications concentrate on the privacy of the users and security of the information shared to prevent anonymous and unauthorized access to illegitimate users [13,14].

Trust, authentication, and privacy are the major requirements in sharing EHRs between different users. Administering the blockchain paradigm as a decentralized ledger for monitoring shared information is becoming a familiar practice in recent years [15,16]. Blockchain-assisted authentication and trust-based security are assimilated with the medical systems for improving the quality of information sharing and preventing unauthorized interruptions [17,18]. Knowing the significance of the data, biomedical systems rely on robust authentication and trust schemes for confronting diverse attacks, data leakage, tampering, and loss. EHR access control, defining security levels, verifying users, and sharing sessions are collaboratively performed using the security systems [15,17,19]. Modified and sophisticated access control, encryption/decryption schemes, and auditing features are required to handle different attacks and illegitimacy in storing and sharing EHRs. In trust-based schemes, user-centric factors are assessed to differentiate the users to provide access controls, whereas authentication schemes focus on providing data/EHR security through hashing and encryption/decryption process [20,21].

However, blockchain refers to the distributed ledger technology, which constitutes an innovation in the information recording and sharing without a trusted third party. In this paper, Blockchain and Distributed Ledger based Improved Biomedical Security system (BDL-IBS) has been proposed to enhance the privacy and data security across healthcare applications.

2. Related Works

Tang et al. [22] proposed privacy-preserving healthcare in the trusted network to enhance the trustiness among the patient and caregivers. The Sybil attack is used to find the fake patient and terminate it from the network. The proposed method is used to make the authenticated person access the healthcare center.

Computer-aid design is implemented for security, and privacy of the trusted systems is introduced by Salnitri et al. [23]. It also gives the specification of experts to use the system from various characteristics. They are also using the higher goal for the business, and external threats are maintained for the trustworthiness in the network.

S-Alex convolution neural network and dynamic game theory (SCNN-DGT) designed by Kong et al. [24] are used in the IoT-cloud computing environment for health data management. The initial step is obtaining the information of the healthcare and classifying them in Alex's net convolutional network. This method is designed to evaluate security in the healthcare system. It validates the index screening to verify the user.

Data integrity is used for sharing the records of healthcare in a verifiable way and is introduced by Wang et al. [25]. The author developed a blockchain for privacy usage through symmetric encryption and attribute-based encryption. It attains the fine-grained access control.

Zhao et al. [26], developed key management for healthcare blockchain. The efficient key management method is used as a privacy and security mechanism in the healthcare system. It is observed by embedding the sensor to analyze the blockchain. The proposed method is used to enhance the effectiveness and high security.

Guo et al. [27] modeled a multi-authority for the Tele-medical system to improve the efficient blockchain based on the ABE scheme. In this paper, both the dynamic authentication and authorization are used for MoD service under telemedicine. ABE is mainly used to manage the system in real-time scenarios for private healthcare data. This is done in a cloud-based environment.

A blockchain is proposed for the medical records to access and permits the MedChain process, which is addressed by Daraghmi et al. [28]. Medchain is used for interoperating, secure, and effective access for patients' privacy. The security is time-based access that gives the degree of health providers.

A blockchain is used for the Electronic Health Record system (EHRs) and is proposed by Guo et al. [29]. The authors implemented a secure attribute based on signature with multi authorities. The patients send the text according to the health as the attribute evidence to the healthcare center. The trust is given to the authorities to access the message, and both use the public and private keys to avoid the escrow problem.

The medical service framework is designed to store the secure records of the patient by using the blockchain method and is introduced by Chen et al. [30]. The storage is done on the cloud for large data access. The records are shared by its aspect based on its service related to the authorized user.

Tian et al. [31], observed medical data management with private access. The blockchain is used to protect the data in two aspects such as storing the data in the local database, encrypting the data, and sharing the key to the patient for further viewing. The shared key for security and integrity is established using sibling intractable function families (SIFF) aided by blockchain. The proposed method uses integrity, availability, and privacy of medical data for better efficiency.

Wang et al. [32] presented an e-healthcare system by using Wireless Body Area Networks WBAN. The blockchain is used to generate security and resolve the low power healthcare system. The WBAN is placed in the patient's body and transmits the data by using the blockchain process.

A blockchain -based healthcare system using formal methods is developed by Brunese et al. [33]. This paper aims to exchange information from the patients to the hospital network by using magnetic resonance images. The data are transmitted by the formal equivalent for validation. They are modeled by radiomic features for automata.

Uddin et al. [34] proposed blockchain leveraged decentralized eHealth architecture (BDeHA). This architecture consists of three layers, including a sensing layer for obtaining the data through the sensor. The second is NEAR processing for sensing the IoT devices and the third one is FAR processing, which is comprised of cloud computing servers.

Griggs et al. [35] observed a healthcare blockchain using smart contracts for patient monitoring. The smart contracts are used for secure analysis management for communication with the sensor. They are also used to monitor the patients and professionals to give notification regarding the health.

Brodersen et al. [36], globally and across several industries, present an innovation model that will allow business to business-and-consumer transactions to be faster, more efficient, and highly secure. Many healthcare participants hope the same distributive database technologies allowing this new model can lead to similar outcomes within the industry and recognize that confusion, like many other major innovations.

3. Blockchain and Distributed Ledger Based Improved Bio-Medical Security System

The proposed BDL-IBS is designed to improve the trust- and privacy-related specifications of the electronic shareable health records. The system focused on maximizing the sharing rate of the secured records along with less adversary impact. In this system, blockchain technology is exploited by the medical server that tracks the trust privacy factors between the users and records. In Figure 1, an illustration of a biomedical security system with blockchain technology is presented.

The components of the bio-medical system include storage and a medical server. The storage contains the health records of the end-users in a digital format. The medical server is responsible for processing user requests and responding to them with appropriate records. A common sharing platform such as cloud and associated infrastructures are responsible for sharing EHRs. The blockchain

and distributed ledger are used in both the medical server and end-user applications. In the blockchain associated with the medical server, the trust and privacy factors are analyzed, whereas the privacy factors are alone assessed in the end-user blockchain. The trust factors include successful access and response to request ration, and privacy relies on convergence and complexity. The trust process is analyzed and explained in detail in the following subsections.

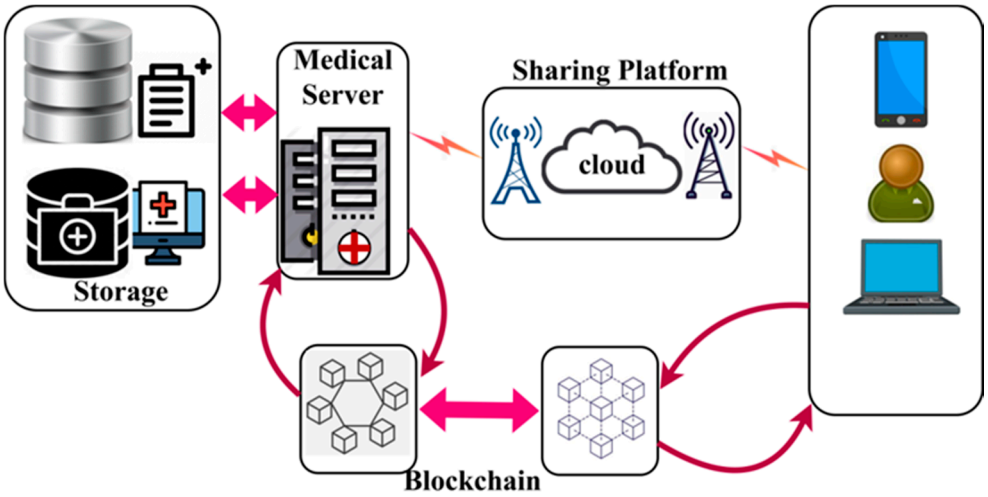


Figure 1. Biomedical Security System with blockchain.

Adversary Model: In this bio-medical security system, malicious access due to man-in-middle and data tempering adversary models are considered. In a man-in-middle attack, the adversary overlaps the end user to gain access to the HER. This results in sharing health information to an adversary and thus degrading the design of a secure biomedical system. In the case of a data tempering attack, the adversary breaches HER from any node communicating with the biomedical system. It either modifies the actual data/tracks the communication through the HER information. Figure 2a,b portrays the representation of the man-in-middle and data tampering attacks over the EHR.

For thwarting the above attack, the trust model and concentric authentication are introduced using the blockchain paradigm. As referred to earlier, the blockchain process is differentiated in both the medical server and end-user functions.

Apart from the regular two-layer network, the man-in-middle attack can be overcome by the server-client based blockchain technology as shown in Figure 2c. Since it is a server–client network, it is well suited for the medical user and end-user functions. To reduce the man-in-middle issue, a pure application-oriented implementation is followed in the objective of the proposed idea. A proper set of protocols should be determined in the server domain, and the appropriate application receives the data from the client side.

The process of trust-based validation is performed using linear decision-making, and authentication is augmented through classification-based learning.

Trust model based on Linear Decision Making: In the trust model, the factors are successful access and end-user application to fetch HER. Through conventional communication standards, the end-user application generates a query for accessing HER. The initial authorization for the end-user is provided using login ID/name and password information. This information is validated by the medical server to ensure the reputation of the user. The medical server is associated with the blockchain with the following entries, as in Table 1.

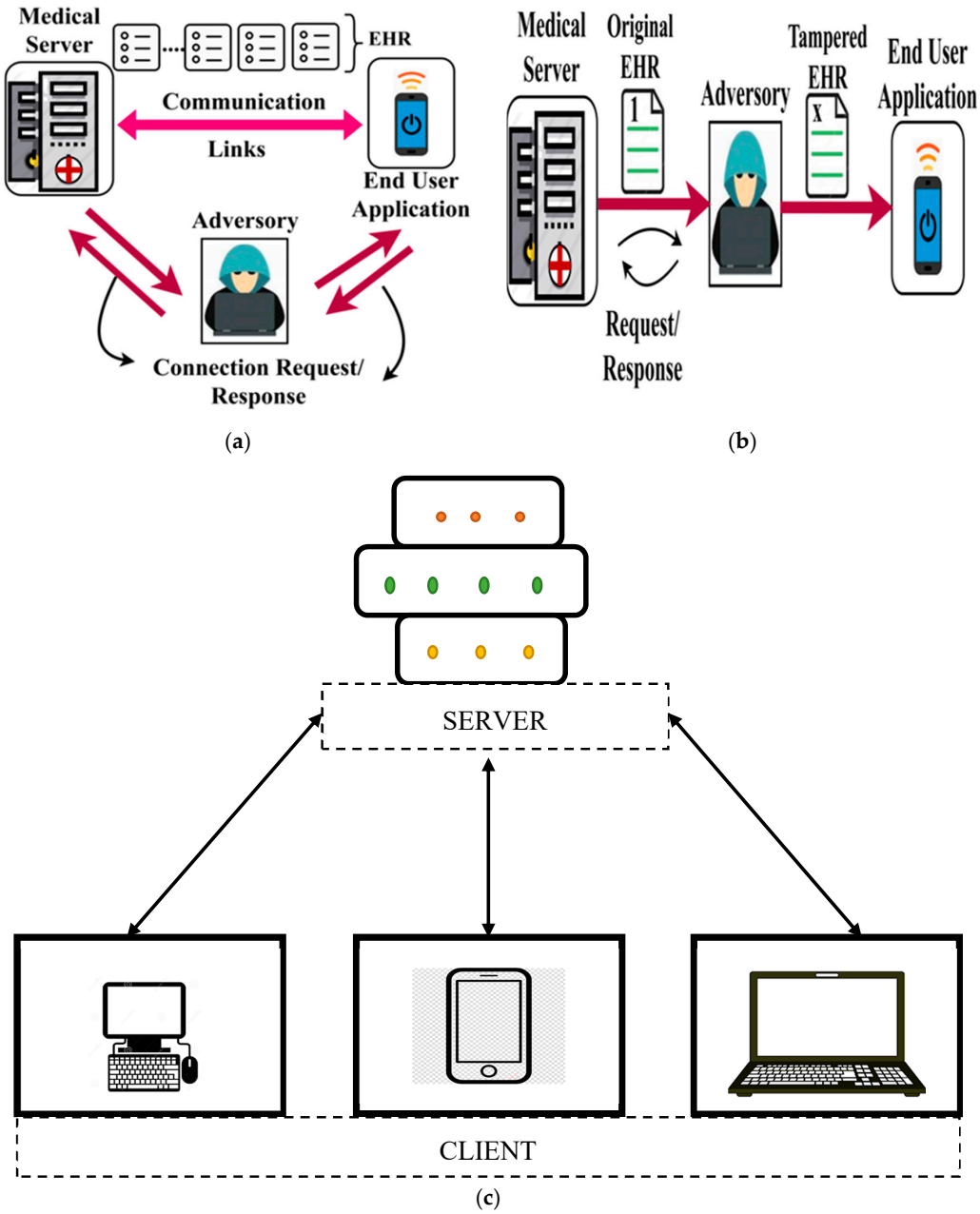


Figure 2. (**a**) Man-in-middle attack. (**b**) Data tampering attack. (**c**) Server-client based blockchain technology.

Table 1. Blockchain Entries.

Field	Description
Name/Id	User Name/Login Credential
Q	Query Request
R	Response
c	Count of EHR shared
t_s	Sharing Time
t_v	Validity Time
τ	Trust Factor

For each Q generated and received in the medical server, the state of R (i.e., sharing EHR), the factors c, t_s, t_v, and τ are updated. This information remains unchanged in the blockchain paradigm. It is to be noted that τ is valid for t_v, within which the sharing of EHR is completed. For any

case of $t_v < t_s$, the $\tau \rightarrow 0$ and the user is marked as illegitimate. For validating the above conditions, τ is computed as a linear combination of $(R,\ Q)$ and successful access probability (ρ_a). In a given t_v, the τ is computed as

$$\left.\begin{array}{c} \tau(t_v) = \frac{R(t_s)}{Q} + \rho_a \\ where, \\ \rho_a = \left(\frac{c}{Q}\right) + \left(1 - \frac{R}{Q}\right)R \end{array}\right\} \quad (1)$$

The factor $\frac{R}{Q}$ is the ratio of response to the query request received by the medical server. The linearity in identifying the trust for a period of t_v relies on $\frac{R}{Q}$ and ρ_a, where both the factors are proportional to each other. The above linear relationship between ρ_a and $\frac{R}{Q}$ is t_s is recurrently analyzed using the $\frac{t_s}{c}$ instance, i.e., the τ in all c instances is verified from its previous shared count that is given as

$$\left.\begin{array}{c} \overline{\tau} = \frac{1}{\tilde{c}}\left[\frac{R_1}{Q_1}\left(\frac{t_s}{1}\right) - \rho_a\left(\frac{t_s}{2}\right) + \frac{R_2}{Q_2}\left(\frac{t_s}{2}\right) - \rho_{a_2}\left(\frac{t_s}{2}\right) + \cdots + \frac{R_c}{Q_c}\left(\frac{t_s}{c}\right) - \rho_{a_c}\left(\frac{t_s}{c}\right)\right] \\ = \frac{1}{\tilde{c}}\left[\sum_{i=1}^{c}\frac{R_i}{Q_i}\left(\frac{t_s}{i}\right) - \rho_a\left(\frac{t_s}{i}\right)\right] = \frac{t_s}{c}\left[\sum_{i=1}^{c}\frac{1}{i}\left(\frac{R_i}{Q_i} - \rho_a\right)\right] \end{array}\right\} \quad (2)$$

From the above sequence, the varying $\frac{R}{Q}$ or ρ_a in t_s is estimated for all the c shared to the end-user. In this sequence, the varying point p initiating the change in proportionality between ρ_a and $\frac{R}{Q}$ is identified. Such identification helps to reduce the computations and security mechanisms (authentication) to prevent losses in sharing EHR. This point from the sequence t_s is computed using Equation (3) as

$$p = \sum_{i=1}^{c}\frac{[1 - \tau(t_v)_i]}{[\overline{\tau}_i - \tau(t_v)_i]} \quad (3)$$

This validating point helps to hold the verification process and trust update in the blockchain, where the actual c is updated until $p \in \overline{\tau}$ sequence. The decision for pursuing/halting EHR sharing is determined using the conditions formulated in Table 2.

Table 2. Decision conditions.

Condition	Description	Solution
$\sum_{i=1}^{c}\left(\frac{R}{Q} - \rho_a\right)_i < \sum_{i=1}^{c}\left(\frac{R}{Q} - \rho_a\right)_{i-1}$	Current trust is less than the previous trust in any of the instance of the sequence	Pause sharing until the next update is received
$p < c$	The actual share count is high that the identified point	Continue sharing until $p = c$ is reached.
$p \geq c$	The identified point is greater than the shared EHRs.	Halt EHR sharing
$\overline{\tau} = \tau(t_v)$	Sequence trust is the same as the instance trust value computed	Not feasible until $c = 1$
$\overline{\tau} < \tau(t_v)$	Sequence trust is high that the instance trust value	Halt EHR sharing

The last three conditions in Table 2 represent the unfeasible conditions as $\overline{\tau} < \tau(t_v)$ results in a negative p that is not possible in case $c > 1$. Similarly, the sequence and instant trust are the same in case of sharing only 1 record, after which $p = \infty$. This provides continuous chances for EHR sharing, whereas, in practical EHR based biomedical systems, the condition does not hold. For $p \geq c$ condition, the point is detected after all the counts are shared. Therefore, the previous state of name/ID for which it is τ with the new t_s or t_v period. The blockchain is updated for the above and hence for further sharing of EHRs. The case of the first two conditions is different, where $p < c$ follows $\overline{\tau}$ and $\tau(t_v)$ as in Equations (3) and (2), respectively. The different case of condition 1 is to be differentiated from the

other conditions as a trial to the user is given if the current trust is less than the previous sequence of trust. This impacts either ρ_a or $\frac{R}{Q}$ and hence Equation (1) is modified as

$$\tau(t_v) = \begin{cases} \left[1 - \frac{R(t_s)}{Q}\right] + \rho_a\left(\frac{t_s}{c} \times t_v\right), \; if \; \frac{R}{Q} \; isnotaconstant \\ \frac{R(t_s)}{Q} + \frac{Q-R}{Q}\rho_a, \; if \; \rho_a \; isnotaconstant \end{cases} \tag{4}$$

If both the $\frac{R}{Q}$ and ρ_a factors are not constant, then the sharing process is halted. Based on the different instances for $\frac{R}{Q}$ (or) ρ_a, the decision is made such that the sharing is not halted, whereas it is paused until the next update if τ is observed. In this pausing instance, the sharing session of the end-user application is expired. Therefore, the user has to login again to re-initiate the EHR sharing session. The time of validity based on different instances of $\tau(t_v)$ is determined using Equations (5) and (6), respectively.

$$\left.\begin{array}{c} t_{s_1} = t_v - \left(\frac{Q_1 - R_1}{Q_1}\right)t_s = t_v(ast_s = 0 \; for \; the \; first \; instance), \; \forall \left(1 - \frac{R}{Q}\right) < \rho_a \\ t_{s_2} = t_v - \left(\frac{Q_2 - R_2}{Q_2}\right)\frac{t_{s1}}{2} \\ \vdots \\ t_{s_c} = t_v - \left(\frac{Q_c - R_c}{Q_c}\right)\frac{t_{sc}}{c} \end{array}\right\} \tag{5}$$

$$\left.\begin{array}{c} t_{s_1} = t_v - \left(1 - \frac{R_1}{Q_1}\right)\rho_a t_{s_o} = t_v \; , \; \forall \left(\frac{Q-R}{Q}\right)\rho_a < \frac{R}{Q} \\ t_{s_2} = t_v - \left(1 - \frac{R_2}{Q_2}\right)\rho_a t_{s_1} \\ \vdots \\ t_{s_c} = t_v - \left(1 - \frac{R_c}{Q_c}\right)\rho_a t_{s_c} \end{array}\right\} \tag{6}$$

For the above Equation of computing t_v for fluctuating $\tau(t_v)$, tn Figure 3a,b, respectively.

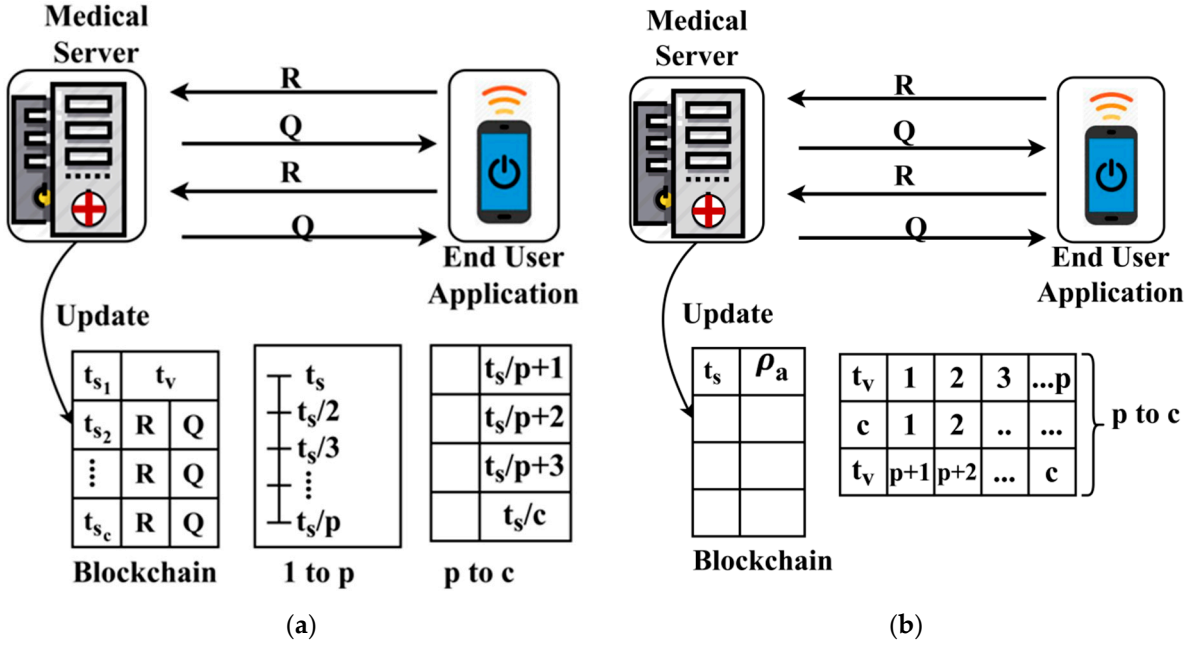


Figure 3. (**a**) Sequential update (1 to p), (**b**) concurrent update (p to c).

The process of trust-based update in the blockchain is performed using t_s using $\frac{R}{Q}$ and ρ_a factors independently. The process is consecutive if t_s and t_v is updated based on $\frac{R}{Q}$ and concurrent if the update is based on ρ_a. The process of differentiation relies on the p that is identified for both the conditions

where $\left(\frac{R}{Q}-\rho_a\right)_i < \left(\frac{R}{Q}-\rho_a\right)_{i-1}\ \forall\ i \in c$. Finally, the user with max$\{\tau\}$ or max$\{\{\overline{\tau}\}(t_s)\}$ is identified in all the instances for providing better authentication. The linear representation in Equation (2) is either fluctuate between t_s based on $\frac{R}{A}$ and ρ_a independently. The fluctuation is based on the varying t_s and t_v instances as differentiated by p. This trust-based decision-making helps to improve the ratio of successful sharing under controlled response time. In Table 3, the observed records that are classified under different conditions of Table 1 is presented for the different sharing times.

Table 3. Records Classified under Table 1 Condition.

Sharing Time (s)	Condition 1	Condition 2	Conditions 3/5	Condition 4
10	374	7152	36	0
20	718	8089	44	0
30	433	8452	17	0
40	847	7843	82	0
50	622	8741	139	0
60	249	9527	86	0
70	506	8719	152	7
80	521	9013	127	0
90	362	9486	92	0

There is only one ending transmission in the sharing time of 70, where condition 4 is satisfied by sharing count of c. The records classified under conditions 3/5 are not sent to the end user, and hence their sessions are logged out.

4. Classification-Based Concentric Authentication

In the classification-based concentric authentication, EHR is shared. In a concentric authentication, the common classification on point p serves as the decision-making for generating authentic records. The classification-based learning allocates two types of non-sequential session keys for authenticating the sharing session. This classification is based on the fluctuating $\tau(t_v)$ as in Equation (4). The impact of either of the fluctuation varies the administration of session keys to prevent the data tampering attacks. Initially, the session is set up between the medical server, and the end-user application follows a linear mapping map: RX $R_c \rightarrow \mathbb{R}_U$. Here, R_c is the group of response until a count c, and $\mathbb{R}_U$ is the random function of the end-user (U). The group consists of a random generator $r \in R_c$ along with a differential prime number p_n. For the different $\tau(t_v)$, the variable $r \in R_c$ relies on computing hashes H_{MS} and H_U for the medical server and end-user, respectively. The general format of an initial authentication is denoted as $\{R_c, R_U, p_n, r,\ H_{MS}, H_U, c\}$. The shared record count is obtained from the blockchain, where the trust of user access coupled with the records is stored. The distributed access to blockchain stored information is assessed in both end-user and medical server levels. For this authentication process, the classification occurrences of $\left(1-\frac{R}{Q}\right)$ and ρ_a in t_s is performed. As stated previously, the sequential and concurrent update of the medical server blockchain process requires different session keys and authentication procedures. Therefore, the occurrence of p for condition 1 from Table 2 is the determining factor. Let ρ_p and ρ_s represent the fluctuating and sequential probabilities in a given time t_s; then,

$$\left.\begin{array}{c} \textit{such that} \\ \end{array}\begin{array}{c} \rho(s|p) = \frac{\rho(p|s)\rho_s}{\rho_p} \\ \rho(p|s) = \prod_{i=1}^{c} \rho(p_i|s) \end{array}\right\} \tag{7}$$

As $\rho(s|p) = \frac{\prod_{i=1}^{c} \rho(p_i|s).\rho_s}{\rho_p} = \frac{\prod_{i=1}^{c} \rho(p_i|s)\rho_s}{(1-\rho_s)}$, the above classification of probability, s over p is computed for all ρ_s instead of ρ_p to linearize the solutions as in Equation (1). Based on the relationship between $\frac{R}{Q}$ and ρ_a, the classification of $\rho(p|s)$ is performed as

$$\left.\begin{array}{c} \rho(s|p_1,\ p_2,\ldots p_c) = \frac{\rho_s\ \rho(p_1,p_2,\ldots p_c|s)}{\rho(p_1,p_2,\ldots p_c)} \\ (or)\ \ \rho(s_1,s_2,\ldots s_c|p) = \frac{\rho(p|s_1,s_2,\ldots s_c)\rho_p}{\rho_p} = \rho(p|s_1,s_2,\ldots,s_c) \end{array}\right\} \quad (8)$$

where $\rho(p|s_1,s_2,\ldots s_c) = \frac{\rho_p \prod_{i=1}^{c} \rho(p|s_i)}{\rho(p_1,p_2,\ldots p_c)}$. For condition 1, the classification rule is framed as in Equation (9) for identifying p over s as in Equation (8)

$$\left.\rho(p|s_1,s_2,\ldots s_c) \simeq \rho_p \prod_{i=1}^{c} \rho(p_i|s)\right\} \quad (9)$$

where $s = argmax\, \rho_p \prod_{i=1}^{c} \rho(p_i|s)$. Here in Equation (9), the probability of ρ_p is computed based on the likelihood of $\overset{c}{p}'s$ instances and its normalization as

$$\mathcal{N}(p) = \frac{c \times \rho_p + s}{\rho_p + (c \times s)} \quad (10)$$

The above likelihood normalization of p helps to classify $p \in \left(1 - \frac{R}{Q}\right) < \rho_a$ condition or $p \in \rho_a < \frac{R}{Q}$ condition. This helps to decide between sequential and concurrent authentication procedure through the same concentric point from the fluctuating sequence of t_s. The normalization identifies precise p in the series of $\rho(p|s)$ such that $\rho(s|p)$ follows sequential authentication, whereas the previous occurrence relies on random concurrent security measures. Here, the priority of authentication is initiated from the first occurrence of ρ_p of ρ_s as determined by $\mathcal{N}(p)$. For all the first occurrences of ρ_p and ρ_s, the sequence follows $\rho(p|s_1,s_2,\ldots s_c)$ or $\prod_{i=1}^{c} \rho(p|s_i)$, and $\frac{\prod_{i=1}^{c} \rho(p|s_i)\rho_s}{(1-\rho_s)}$ (as in Equation (6)). Using this sequence and concurrency, the authentication is presented as follows. In two cases, the occurrence of the sequence and concurrency observed is discussed below.

Case 1: The sequence initiates with ρ_s

Analysis 1: The hash sequence for both H_{MS} and H_U is formulated as

$$\left.\begin{array}{c} H_{MS}(p) = r^i|pn| + r^{i-1}|pn| + \ldots + r^{i-c}|pn|p^{c-1},\ \forall\ i \in c \\ and \\ H_U(c) = r^{i-c}|pn| + r^{i-c+1}|pn| + \ldots + r^i|pn|\rho(p|s_i),\ \forall\ i \in p \end{array}\right\} \quad (11)$$

This hash is composed of $[R_c,\ H_U(p),\ c]$ and $[R_U,\ H_u(c),\ c]\ \forall\ \{R_c,\ R_U, pn,\ r,\ c\}$ and is subject to verification using the user ID and session key as follows,

$$\left.\begin{array}{c} K_{s_{ij}} = H_{MS}\left[H_{U_j}(Id)\right]|pn| + r^{i-j}\ ,\ \forall\ i \in c\ and\ j \in p \\ and \\ K_v = \prod_{i=1}^{c} g^i|pn| - (i-p) \end{array}\right\} \quad (12)$$

where K_s and K_v are the secret and verification keys generated for the hashes, and therefore in the sharing process, $K_s[H_{MS}(p),\ R, c]$ is contributed to the end-user. At the receiver end, the K_v is used for verification. If the process of sharing the records is sequential, then $i \in c$ is sequential until p or the likelihood $\mathcal{N}(p)$ occurs. This is followed for all $[H_{MS}(p), R]$ until the $c = p$ is reached, and then the coherency of $H_U(c) = H_U(p)$ until $\rho(s|p)$ is observed. The verification of the process is also sequential by mapping $R \times R_{1\ to\ p} \rightarrow R_U$ where R_U is observed from the range of hashes from 1 to $\rho(s|p_1,p_2,\ldots\ p_c)$. The first sharing verification is performed as

$$\left.\begin{array}{c}[H_{MS}(1\|B), r] = [H_{MS}(1\|B),\ K_s] \\ [H_{MS}(2\|B), r] = [H_{MS}(2\|B),\ K_s] \\ \vdots \\ [H_{MS}(p\|B), r] = [H_{MS}(p\|B),\ K_s]\end{array}\right\} \tag{13}$$

where, B denotes the blockchain record for the grouped storage of $[R, c]$ after the hashing process. In the verification at the user end, the relevance is first validated, followed by the verification process as in Equations (14) and (15) respectively.

$$H_{MS}(p\|B),\ r] = \begin{cases} [H_u\left(p\middle\|B\right)^{pn},\ r] \\ (or) \\ [H_u(p\middle\|B),\ r^{c-p} \\ (or) \\ [H_u(p\|B),\ c\rho(s_i|P)],\ i\ \in c) \end{cases} \tag{14}$$

$$\left[\frac{\prod_{i=1}^{c}\rho(p_i\middle|s)\rho_s}{(1-\rho_s)},\ H_{MS}(P\|B),\ K_s\right] = \left[\prod_{i=1}^{c} B_i.H_U(Id)_i K_{v_i},\ r\right] \tag{15}$$

In the above, the range of c is valid until p, i.e., the $\mathcal{N}(p)$ is the halting factor for sequential authentication. In the verification process, sequence as mapped in $R \times R_C \rightarrow R_U$ is the balancing factors where the sending and receiving sequence until $\rho(p\middle|s)$ is obtained. In this case, the converging interval of the proposed method is extended until the c, i.e., the restricted time from 1 to p is extended from p to c in a concentric manner. The next sequence for p to c authentication is discussed in Case 2.

Case 2: The sharing sequence experiences ρ_p.

Analysis 2: This case is unique as both sequential and concurrent authentication is performed with interfering with other processes. It is to be noted that the convergence time from the sequential process is experienced to $\rho(p\middle|s_1,\ s_2, \ldots s_c)$ from the ρ_p. This helps to identify more $\rho(s\middle|p)$, and thus the concentricity of the authentication process is expanded, reducing the chances of convergence. In this authentication process, both H_{MS} and H_U are used for performing secure sharing between the medical server and the end user. The blockchain is updated with p and $\mathcal{N}(p)$ along with the previous sequence for the appropriate user ID. Therefore, the session is initiated by verifying the following

$$\left.\begin{array}{c}[H_{MS}(p\|B),\ (c-p)] = [H_{MS}(p\|B),\ K_s,\ p],\ \forall\ p\ to\ c\ in\ the\ medical\ server \\ and \\ [H_U(c-p\|B),\ c] = [H_U(c-p)\middle\|B,\ K_v, c],\ \forall\ preceived\ by\ the\ end\ user\ application\end{array}\right\} \tag{16}$$

There are two verification steps followed for authenticating the sharing due to the fluctuating instances in t_s. The first authentication follows Equation (14), whereas the range from p to c follows

$$\left.\begin{array}{c}[H_{MS}(p\|B),\ c-p] = \begin{cases} [H_{MS}\left(p\middle\|B\right)^{c-p},\ c] \\ (or) \\ H_{MS}(c-p)\middle\|B,\ \rho(p\middle|s_i),\ i \in c \end{cases} \\ and \\ [H_U\Big(c-p\|B),\ \rho_p\Big] = \prod_{i=1}^{c} B_{c-i}H_U(Id)_i K_v.(v-p)_i\end{array}\right\} \tag{17}$$

The above process of authentication in sharing and receiving B is performed in both the medical server and the end user. Finally, the received B is verified using 1 to p sequence as in Equation (15), whereas the t to c received B is verified as follows.

$$[H_{MS}(\rho\|B),\ (c-p),\ K_s] = [H_u(c-p\|B),\ H_U(Id\ ),\ K_v,\ c-p)]\forall\ i\ \in p\ to\ c \tag{18}$$

This verification is processed for all the fluctuating shared R through the classification process. This prevents unnecessary convergence and overload complexity in handling medical records at different time instances. In Table 4, the ρ_s and ρ_p for the varying p in different sharing time along with the complexity is tabulated.

Table 4. ρ_s and ρ_p and Complexity.

p	ρ_s	ρ_p	t_s(s)	Complexity	c
1	0.59	0.38	14.72	0.12	380
2	0.74	0.23	37.49	0.069	887
3	0.64	0.33	46.44	0.052	1028
4	0.43	0.52	78.37	0.083	1849
5	0.74	0.24	78.19	0.064	2053
6	0.69	0.29	88.43	0.087	3188
7	0.82	0.15	79.77	0.042	2207
8	0.54	0.43	69.29	0.103	1352
9	0.59	0.38	76.13	0.096	1511
10	0.73	0.26	84.22	0.067	2733

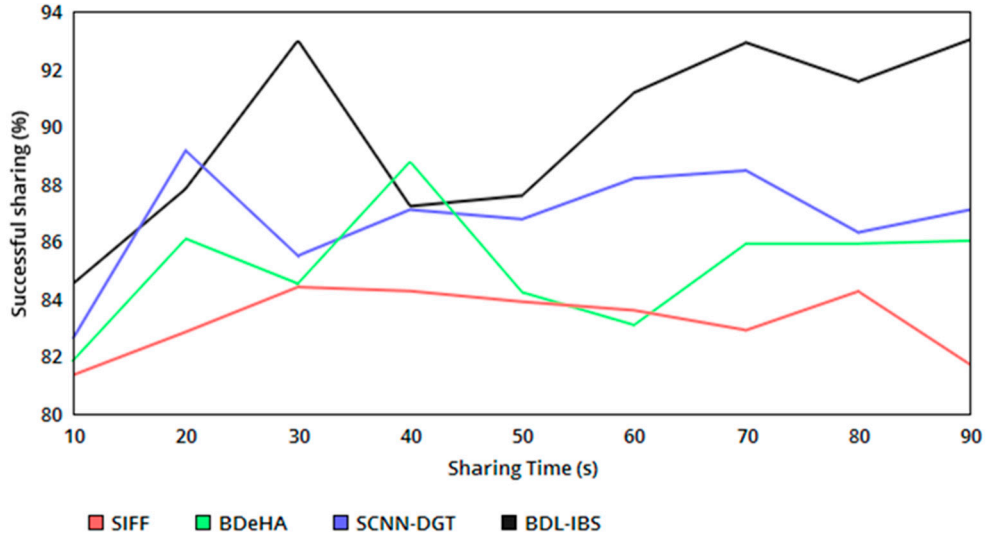
In Table 4, the complexity is computed as the number of additional hashes generated due to ρ_p to the actual existing hashes. The complexity is measured in terms of count of additional steps required for verification and authentication as observed in the keying process. If the impact of attacks is high, then the ρ_p factor increases to prevent unnecessary data tampering or modification. Hence, in this case, the number of c fluctuates as the classification is grouped under both the sharing instances.

5. Performance Analysis

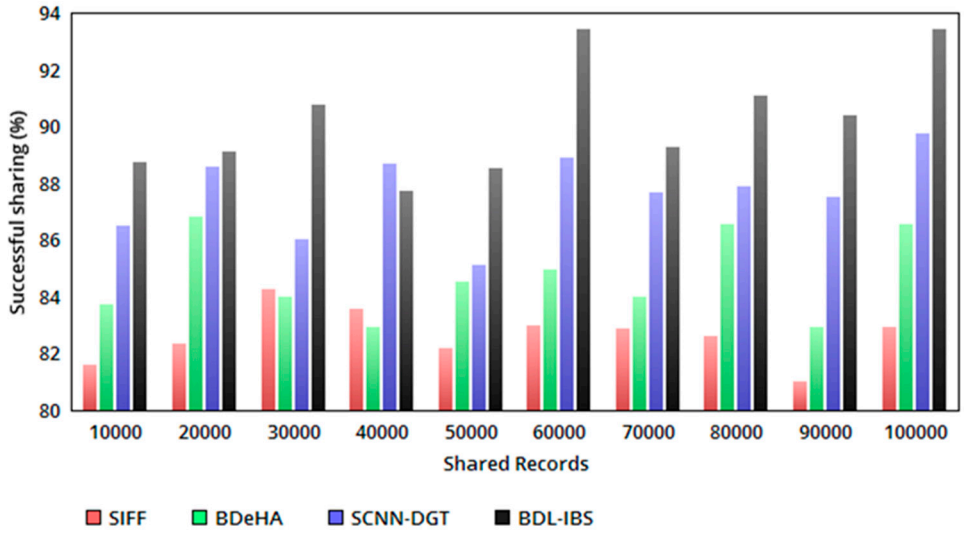
The performance of the proposed BDL–IBS is assessed using simulations using an opportunistic network environment. In this environment, a maximum of 100,000 EHRs (unique and repeated) are shared for 110 users in different time instances. A user is capable of generating four Qs at the same time, for which the sharing interval is 90 s (max). The medical server of storage 4 × 1 TB is used for storing LHRs, and two blockchain servers with restricted read/write access are configured in this simulation environment. The medical server is capable of dispatching 20 records of size 70 mb in 1 s time. The maximum wait time for a record is 60 s, and the hash process follows hyperelliptic curve cryptography of a maximum size of 160 bits. Similarly, K_v and K_s is fit as 48-bits and 36-bit, respectively. Using this simulation environment, the existing 31FF [23], BDe HA [26], and SCNN–DGT [16] methods are considered for comparative analysis. For this comparative analysis, the metrics sharing ratio, response time, computation time, and convergence time are analyzed.

5.1. Successful Sharing Ratio

The proposed security system relies on record—user-access-based trust and differential authentication to improve the successful sharing of EHRs. The trust-based relationship between ρ_a and R/Q is validated for the possible conditions in Table 2, generating $\tau(t_v)$ and $\overline{\tau}$ at different instances. In the sharing instances, pursuing/pausing sharing is determining based on $\rho_a > \frac{R}{Q}$ or $\rho_a < \frac{R}{Q}$ conditions. This condition-based decision-making determines t_s for $(p+1)$ to c instances and or t_s for $\left(\frac{p+1}{2}\right.$ to $\left.c\right)$ instances in either sequential/concurrent manner. The concentric sharing process follows t_{s_c} for any instance of $\tau(t_v)$; if the $\tau(t_v)$ is maximum, then the sharing is performed either in a sequential or concurrent manner. In this process, the blockchain updates the trust for the linear ρ_a and $\frac{R}{Q}$ relation, which remains unchanged. Therefore, sharing for varying time and EHRs follows conditional satisfaction as in Table 2, achieving a high successful sharing ratio (refer to Figure 4a, b).



(**a**)



(**b**)

Figure 4. (**a**) Successful sharing ratio versus sharing time. (**b**) Successful sharing ratio versus shared records.

5.2. Response Time

The sharing time $t_s < t_v$ is ensured in all the instances of EHR processing for the received Q. If $t_v < t_s$ is observed, then the response time increases. For analyzing the instances of sharing c, the variable $\overline{\tau}$ and $\tau(t_v)$ is differentiated. In this case, t_{s_c} for $\rho_a > \frac{R}{Q}$ is estimated as $t_v - \left(\frac{Q_c - R_c}{Q_c}\right)\frac{t_{sc}}{c}$ and $t_v - \left(1 - \frac{R_c}{Q_c}\right)\rho_a t_{s_c}$ independently. If the condition $t_s < t_v$ is achieved, then the varying point p is identified to differentiate the sharing of EHRs. Therefore, the joint sharing is not facilitated for trust varying or condition 1 (Table 2), dissatisfying users. Hence, a small wait time in a response is experienced; this disintegrates the conditions of $t_s < t_v$, where concurrent sharing and authentication is performed without additional wait time. Therefore, for the conditions 1 and 2, the response time for a Q from the end user is less compared to the other methods (refer to Figure 5).

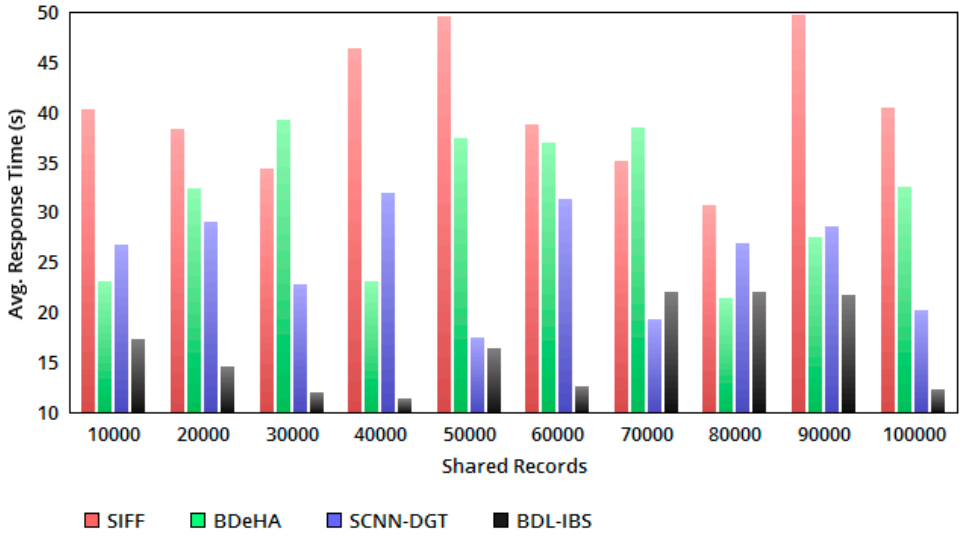


Figure 5. Avg. response time versus shared records.

5.3. Computation Time

Figure 6 presents the computation time of the proposed system as a comparative analysis with the existing methods. The authentication computing process requires either of the instances based on p, from which HMB and Hu are commonly adapted for the varying impact of untrusted users (classified under conditions 3 and 5 from Table 2). This helps to process the same number of c with the different authentication process and thereby reduces the complexity and required computations in the sequential sharing. Instead, the concurrent dissemination process of the records requires a change in first-level authentication as Equations (12) and (17) to satisfy $\mathcal{N}(p)$, confining t_s within t_v. Therefore, the required computation increases by 1, and hence some additional time for verifying the second authentication is required. The verifying process is common in both the instances, demanding less/same time of computation. Hence, the overall computation time is differentiated by ρ_p, and $\rho(p|s)$ and $\rho(s|p)$ is less in the proposed security system.

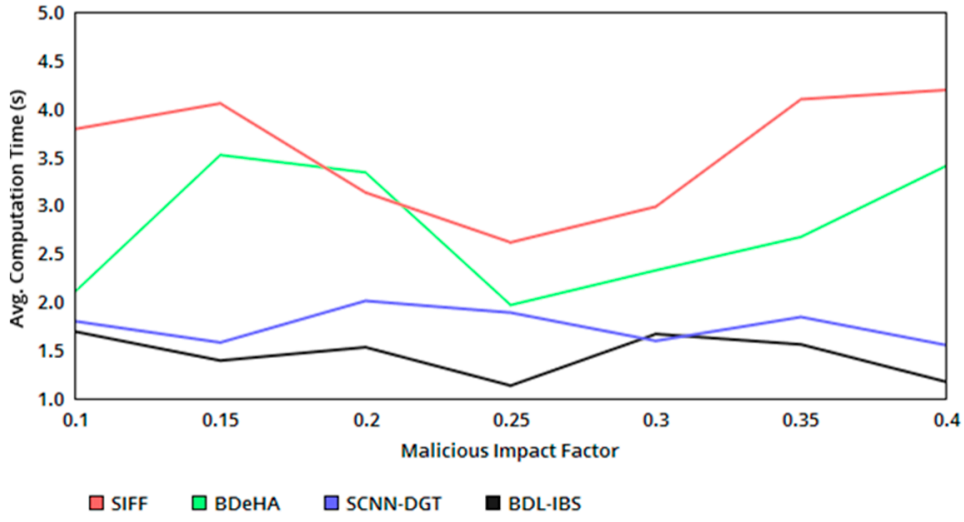


Figure 6. Avg. computation time versus malicious impact factor.

5.4. Convergence Time

The proposed security system achieves less convergence time in the authentication process. The convergence is identified using the classification of p based on the occurrence of the ρ_p and ρ_s. Following the classification process, $\mathcal{N}(p)$ for $\rho(p|s_i)$, $i \in c$ or $\rho(p_i|s)$, the converging time is identified in forehand, restricting in breaches in sharing and shared data tampering. Therefore, the identification based on p and $\mathcal{N}(p)$ helps to divide the authentication for $\rho_a > \frac{R}{Q}$ and $\rho_a < \frac{R}{Q}$ instances. The verification and authentication observed for the above conditions are different, without generating different point and probabilities. Here, detection of p segregates the authentication process for sequential and concurrent instances as 1 to p and p to c without requiring a new hash or verification procedure. As the number of convergence increases, the concurrency is increased without requiring additional computation steps. Therefore, the probabilistic classification of $\prod_{i=1}^{c} \rho(p_i|s)$ and $\prod_{i=1}^{c} \rho(p|s_i)$ for $\mathcal{N}(p)$ achieves less convergence in the proposed security system (refer to Figure 7). In Table 5, the comparative analysis results are tabulated.

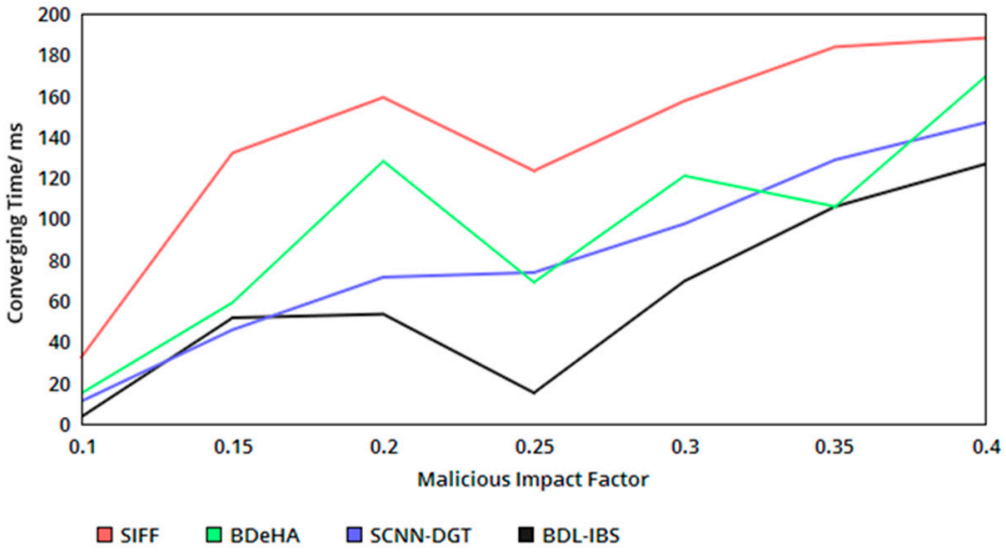


Figure 7. Converging time versus malicious impact factor.

Table 5. Comparative Analysis.

Metrics	SIFF	BDeHA	SCNN-DGT	BDL-IBS
Successful sharing (%)	82.92	86.55	89.76	93.44
Avg. Response Time (s)	40.46	32.56	20.12	12.21
Avg. Computation Time (s)	4.192	3.407	1.552	1.172
Converging Time/ms	188.09	169.43	146.89	126.7

From Table 5, it is seen that the proposed security system is capable of achieving better performance by reducing the response time and increasing the ratio of successful sharing through trust-based validations. In the authentication process, the computation and converging time are found to be less since the instances of sharing are segregated based on p.

As in Table 5 and in Figure 8, the proposed security system achieves a very high performance for analyzing various attacks. The better performance is achieved by consuming low response time, less computation time and reduced converging time. As opposite, it achieves a high successful sharing rate.

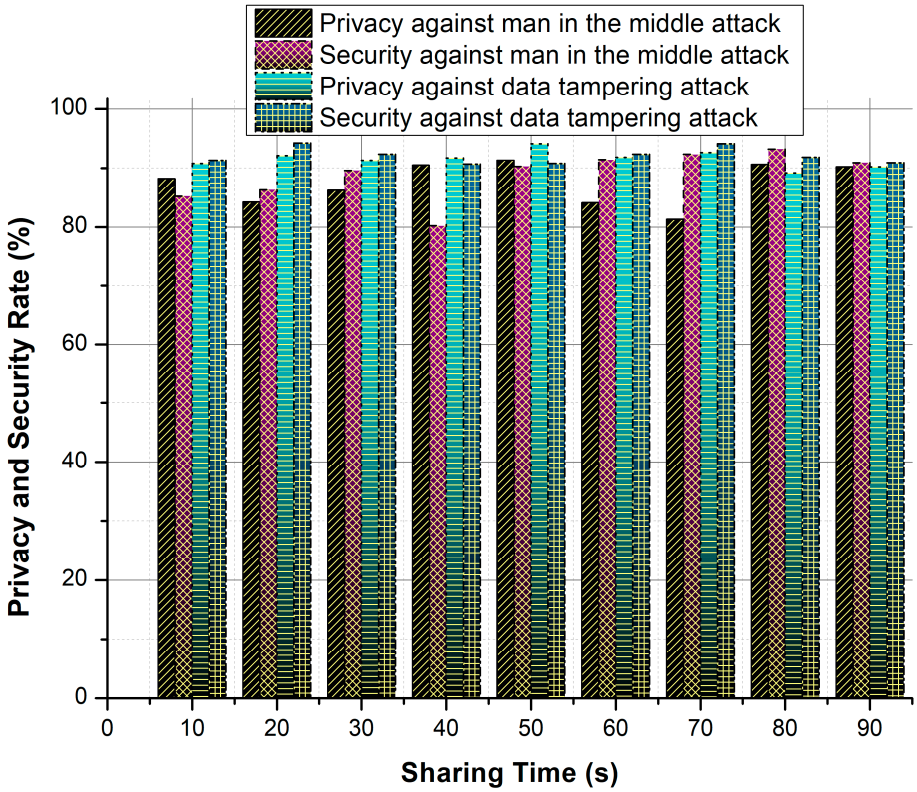


Figure 8. Privacy and security ratio against attacks.

6. Conclusions

This paper introduced a blockchain and distributed ledger-based improved biomedical security system for improving the privacy and security of EHRs. This security system relies on the blockchain paradigm for providing trust validation through linear decision-making. The authentication of EHRs is preceded using classification-based learning for identifying sequential and concurrent sharing. The process is focused on both user-level and sharing-level security and privacy of the biomedical systems. The classification of sharing instances helps to reduce the complex and overloaded computations in the authentication process with less computation time. The blockchain technology coupled with this process helps to share trust-related information and differentiate the sharing based on classification instances. The experimental analysis of the proposed security system shows that it is capable of increasing the sharing ratio by 8.077% and 7.03% for sharing time and records, respectively. It also achieves 20.11% less response time compared to the other methods. In the case of authentication, the proposed system confines computation and convergence time by 10.26% and 12.31%.

Author Contributions: Formal analysis, H.L.; funding acquisition, H.L.; methodology, R.G.C.; project administration, O.S.M.; resources, R.G.C.; software, H.L.; supervision, O.S.M.; validation, O.S.M.; visualization, R.G.C. All authors have read and agreed to the published version of the manuscript.

Funding: Thanks to the Lanzhou Jiaotong University Tianyou Young Talent Promotion Program (2019) for supporting this work.

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

References

1. Piras, E.M.; Cabitza, F.; Lewkowicz, M.; Bannon, L. Personal health records and patient-oriented infrastructures: Building technology, shaping (new) patients and healthcare practitioners. *Comput. Support. Cooper. Work CSCW* **2019**, *28*, 1001–1009. [CrossRef]
2. Tsai, M.F.; Hung, S.Y.; Yu, W.J.; Chen, C.C.; Yen, D.C. Understanding physicians adoption of electronic medical records: Healthcare technology self-efficacy, service level and risk perspectives. *Comput. Stand. Interfaces* **2019**, *66*, 103342. [CrossRef]
3. Muthu, B.A.; Sivaparthipan, C.B.; Manogaran, G.; Sundarasekar, R.; Kadry, S.; Shanthini, A.; Dasel, A. IOT based wearable sensor for diseases prediction and symptom analysis in healthcare sector. *Peer Peer Netw. Appl.* **2020**, 1–12. [CrossRef]
4. Baskar, S.; Shakeel, P.M.; Kumar, R.; Burhanuddin, M.A.; Sampath, R. A dynamic and interoperable communication framework for controlling the operations of wearable sensors in smart healthcare applications. *Comput. Commun.* **2020**, *149*, 17–26. [CrossRef]
5. Gu, D.; Li, T.; Wang, X.; Yang, X.; Yu, Z. Visualizing the intellectual structure and evolution of electronic health and telemedicine research. *Int. J. Med. Inform.* **2019**, *130*, 103947. [CrossRef]
6. Manogaran, G.; Lopez, D. A survey of big data architectures and machine learning algorithms in healthcare. *Int. J. Biomed. Eng. Technol.* **2017**, *25*, 182–211. [CrossRef]
7. Enaizan, O.; Zaidan, A.A.; Alwi, N.H.M.; Zaidan, B.B.; Alsalem, M.A.; Albahri, O.S.; Albahri, A.S. Electronic medical record systems: Decision support examination framework for individual, security and privacy concerns using multi-perspective analysis. *Health Technol.* **2018**, *10*, 795–822. [CrossRef]
8. Uddin, M.A.; Stranieri, A.; Gondal, I.; Balasubramanian, V. Continuous patient monitoring with a patient centric agent: A block architecture. *IEEE Access* **2018**, *6*, 32700–32726. [CrossRef]
9. Zhang, P.; Schmidt, D.C.; White, J.; Lenz, G. Block chain technology offers potential in healthcare. *Pharmac. Econ. Outcomes News* **2018**, *809*, 1–41.
10. Radanović, I.; Likić, R. Opportunities for use of block chain technology in medicine. *Appl. Health Econ. Health Policy* **2018**, *16*, 583–590. [CrossRef]
11. Firdaus, A.; Anuar, N.B.; Razak, M.F.A.; Hashem, I.A.T.; Bachok, S.; Sangaiah, A.K. Root exploit detection and features optimization: Mobile device and block chain based medical data management. *J. Med. Syst.* **2018**, *42*, 112. [CrossRef] [PubMed]
12. Manogaran, G.; Varatharajan, R.; Lopez, D.; Kumar, P.M.; Sundarasekar, R.; Thota, C. A new architecture of internet of things and big data ecosystem for secured smart healthcare monitoring and alerting. *Futur. Gener. Comput. Syst.* **2017**, *80*, 1–10. [CrossRef]
13. Tanwar, S.; Parekh, K.; Evans, R. Block chain—Based electronic healthcare record system for healthcare 4.0 applications. *J. Inf. Secur. Appl.* **2020**, *50*, 102407.
14. Pujitha, A.K.; Sivaswamy, J. Solution to overcome the sparsity issue of annotated data in medical domain. *CAAI Trans. Intell. Technol.* **2018**, *3*, 153–160. [CrossRef]
15. Sun, Y.; Lo, F.P.W.; Lo, B. Security and privacy for the internet of medical things enabled healthcare systems: A survey. *IEEE Access* **2019**, *7*, 183339–183355. [CrossRef]
16. Thakur, S.; Singh, A.K.; Ghrera, S.P.; Elhoseny, M. Multi-layer security of medical data through watermarking and chaotic encryption for tele-health applications. *Multimed. Tools Appl.* **2019**, *78*, 3457–3470. [CrossRef]
17. Raisaro, J.L.; Troncoso-Pastoriza, J.R.; Misbach, M.; Sousa, J.S.; Pradervand, S.; Missiaglia, E.; Michielin, O.; Ford, B.; Hubaux, J.P. MedCo: Enabling secure and privacy-Preserving exploration of distributed clinical and genomic data. *IEEE/ACM Trans. Comput. Biol. Bioinform.* **2019**, *16*, 1328–1341. [CrossRef]
18. Wazid, M.; Das, A.K.; Kumar, N.; Conti, M.; Vasilakos, A.V. A novel authentication and key agreement scheme for implantable medical devices deployment. *IEEE J. Biomed. Health Inform.* **2017**, *22*, 1299–1309. [CrossRef]
19. Shakeel, P.M.; Baskar, S.; Dhulipala, V.R.S.; Mishra, S.; Jaber, M.M. Maintaining security and privacy in health care system using learning based deep-Q-networks. *J. Med. Syst.* **2018**, *42*, 186. [CrossRef]
20. Amin, R.; Islam, S.H.; Gope, P.; Choo, K.K.R.; Tapas, N. Anonymity preserving and lightweight multimedical server authentication protocol for telecare medical information system. *IEEE J. Biomed. Health Inform.* **2019**, *23*, 1749–1759. [CrossRef]

21. Fatima, A.; Colomo-Palacios, R. Security aspects in healthcare information systems: A systematic mapping. *Proc. Comput. Sci.* **2018**, *138*, 12–19. [CrossRef]
22. Tang, W.; Ren, J.; Zhang, Y. Enabling trusted and privacy-preserving healthcare services in social media health networks. *IEEE Trans. Multimed.* **2019**, *21*, 579–590. [CrossRef]
23. Salnitri, M.; Angelopoulos, K.; Pavlidis, M.; Diamantopoulou, V.; Mouratidis, H.; Giorgini, P. Modelling the interplay of security, privacy and trust in sociotechnical systems: A computer-aided design approach. *Softw. Syst. Model.* **2019**, *19*, 467–491. [CrossRef]
24. Kong, F.; Zhou, Y.; Xia, B.; Pan, L.; Zhu, L. A security reputation model for IoT health data using S-AlexNet and dynamic game theory in cloud computing Environment. *IEEE Access* **2019**, *7*, 161822–161830. [CrossRef]
25. Wang, S.; Zhang, D.; Zhang, Y. Block chain-based personal health records sharing scheme with data ontegrity verifiable. *IEEE Access* **2019**, *7*, 102887–102901. [CrossRef]
26. Zhao, H.; Bai, P.; Peng, Y.; Xu, R. Efficient key management scheme for health block chain. *CAAI Trans. Intell. Technol.* **2018**, *3*, 114–118. [CrossRef]
27. Guo, R.; Shi, H.; Zheng, D.; Jing, C.; Zhuang, C.; Wang, Z. Flexible and efficient block chain-based ABE scheme with multi-authority for medical on demand in telemedicine system. *IEEE Access* **2019**, *7*, 88012–88025. [CrossRef]
28. Daraghmi, E.Y.; Daraghmi, Y.A.; Yuan, S.M. MedChain: A design of block chain-based system for medical records access and permissions management. *IEEE Access* **2019**, *7*, 164595–164613. [CrossRef]
29. Guo, R.; Shi, H.; Zhao, Q.; Zheng, D. Secure attribute-based signature scheme with multiple authorities for block chain in electronic health records systems. *IEEE Access* **2018**, *6*, 11676–11686. [CrossRef]
30. Chen, Y.; Ding, S.; Xu, Z.; Zheng, H.; Yang, S. Block chain-based medical records secure storage and medical service framework. *J. Med. Syst.* **2018**, *43*, 5. [CrossRef]
31. Tian, H.; He, J.; Ding, Y. Medical data management on blockchain with privacy. *J. Med. Syst.* **2019**, *43*, 26. [CrossRef] [PubMed]
32. Wang, J.; Han, K.; Alexandridis, A.; Chen, Z.; Zilic, Z.; Pang, Y.; Jeon, G.; Piccialli, F. A block chain-based eHealthcare system interoperating with WBANs. *Future Gener. Comput. Syst.* **2019**, *110*, 675–685. [CrossRef]
33. Brunese, L.; Mercaldo, F.; Reginelli, A.; Santone, A. A block chain based proposal for protecting healthcare systems through formal methods. *Proc. Comput. Sci.* **2019**, *159*, 1787–1794. [CrossRef]
34. Uddin, M.A.; Stranieri, A.; Gondal, I.; Balasubramanian, V. Blockchain leveraged decentralized IoTeHealth framework. *Internet Things* **2020**, *9*, 100159. [CrossRef]
35. Griggs, K.N.; Ossipova, O.; Kohlios, C.P.; Baccarini, A.N.; Howson, E.A.; Hayajneh, T. Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. *J. Med. Syst.* **2018**, *42*, 130. [CrossRef] [PubMed]
36. Brodersen, C.; Kalis, B.; Leong, C.; Mitchell, E.; Pupo, E.; Truscott, A.; Accenture, L. Blockchain: Securing a New Health Interoperability Experience. Available online: http://www.truevaluemetrics.org/DBpdfs/Technology/Blockchain/2-49-accenture_onc_blockchain_challenge_response_august8_final.pdf (accessed on 27 July 2020).