Design and implementation of hybrid consensus mechanism for IoT based healthcare system security

Punam Prabha¹ · Kakali Chatterjee¹

Received: 3 September 2021 / Accepted: 10 January 2022 / Published online: 9 February 2022

© The Author(s), under exclusive licence to Bharati Vidyapeeth's Institute of Computer Applications and Management 2022

Abstract Nowadays, blockchain is emerging as a worthwhile technology for managing sensitive data in electronic healthcare system. It plays an important role in healthcare, medical research and insurance sectors. The consensus algorithms used in blockchain technology for the selection of a new block, provide high-level of security to IoT devices. However, the reliability problem still exists. In the present paper, a blockchain based hybrid consensus mechanism (HCM) is implemented in electronic healthcare system (EHS) to overcome trustworthiness issues. The aim of the proposed HCM is to maintain reputation module on the basis of the block activities. In this context, EHS is designed in four layers namely: system layer, inter-network layer, blockchain layer, and cloud layer. Moreover, HCM consists of five algorithms for creation, validation, fork handling (if any), Merkle tree construction and reward/punishment module respectively. Dev C++ software platform is used for the simulation of the above mentioned HCM algorithms excluding Merkle tree construction which is simulated using conditional contrast high itemset tree. It is observed that all the blocks use same methodology to be the part of a new blockchain network. Moreover, the CPU and memory consumption in the implementation of HCM is always below two percent and about fifty percent respectively as shown in the latency graph. The basic security goal (confidentiality, integrity and availability) is guaranteed with the help of the height of the Merkle tree as

well. The performances of the proposed HCM and Proof of X-repute (PoXR) blockchain consensus algorithms are compared with respect to various parameters such as final difficulty, reward and punishment provisions etc. HCM shows superior performance as the final earned reputation is calculated for each block along with the reward and punishment modules during the deployment of blockchain network. In addition, a simple concept of Merkle-tree is opted for providing reward and punishment rather than a set of complex mathematical equations as used in PoXR consensus algorithm.

Keywords Blockchain · Consensus · Electronic healthcare system (EHS) · Punishment · Reputation · Reward

1 Introduction

Nowadays, smart healthcare system is growing exponentially to provide hassle-free and fast processing of medical facilities at reduced time and cost [1]. These services include remote patient health monitoring, routine health checkup, emergency healthcare and treatment etc. [2]. Wireless body area network (WBAN) sensor-based healthcare application is used for emergency and cost effective remote real-time health monitoring in case of critical illness, vital or communicative diseases [3]. In this process, sensor data is accumulated in WBAN device, processed and saved as patient health information (PHI). PHI is transmitted through network coordinator (IoT gateway) to the cloud server. To secure the sensitive clinical PHI against security threats like data leaking, unauthorized modification and destruction [4], IoT and blockchain based schemes are employed in [5]. In IoT and blockchain based schemes distributed public ledger (DPL)

✉ Punam Prabha
punamp.phd18.cs@nitp.ac.in

Kakali Chatterjee
kakali@nitp.ac.in

¹ Department of Computer Science and Engineering, National Institute of Technology Patna, Bihar, India

is used to maintain the same ledger on each block. In blockchain with reputable modules, selection of right block which maintain honesty until the deployment of the system based on abundant resource is very big task. Hence, a consensus algorithm is used in the system. At each round of consensus, an honest block is selected to update DPL [6].

Two notable problems exist in the contemporary blockchain consensus algorithm. The first and foremost issue arises due to the negligence of the behavior of the consensus blocks in the reput system. In such system, neither the malicious behavior of a node is identified for punishment points nor is the good behavior recognized for reward points [6]. Secondly, the present consensus algorithms use some high threshold for participation in blockchain network as an honest node. For example, Proof of Work (PoW) selects high power computing nodes to generate blocks easily as compared to low computing power nodes. This causes difficulty for simple honest node to participate in the consensus.

On the basis of these two problems, the proposed research work implements a reputation based blockchain framework to maintain PHI in the distributed environment. The main research contributions of the present paper are as follows:

- EHS implements reput-based hybrid consensus mechanism (HCM) to enhance credibility of blocks.
- Implementation results show that the proposed HCM for EHS provides reward/punishment modules for a block efficiently.
- Implementation results show that the proposed HCM algorithm consumes lesser resources than Proof of X-repute (PoXR) [6].
- Security analysis proves that the proposed framework provides confidentiality, availability and integrity of PHI.

Section 2 presents background of the research work. The proposed HCM based EHS is described in Sect. 3. In Sect. 4, a list of interested clients is hypothesized for experimental evaluation. Moreover, the performance of PoXR is compared with proposed HCM algorithm. Finally, the research findings are concluded in Sect. 5.

2 Background

In this section, the fundamental working principle of blockchain technology in smart healthcare system is discussed in-detail.

2.1 Blockchain requisite

In centralized technology, single point failure may affect the whole network which in turn, facilitates the potential hackers. The aforementioned issues are conquered in distribution based decentralized technology which is utilized in Blockchain network. Blockchain consists of a chain of blocks interlinked using Merkle tree cryptographic hash. DPL is used to store the records of all transactions saved on the database of each block.

2.1.1 Consensus mechanism

Blockchain technology uses cryptographic technique to provide non-tampering characteristics. In blockchain, different consensus algorithms are used to ensure the consistency of DPL data among nodes. A consensus protocol is referred as a method of selection of blocks in the blockchain among different interested clients (or miners). A miner is selected on the basis of the agreement or the common decision taken by the connected nodes. Several

Table 1 Assessment of different consensus algorithms

S.N	Name	References	Advantage	Disadvantage
1	PoW	[7]	Nodes having high computation power will be selected as miner	It suffers from 51% attack
2	PoS	[8]	Nodes having lots of money will be selected as miner	Miners have to gather 10% coins of blockchain network
3	DPoS	[9]	Nodes having huge number of votes by delegates will be selected as miner	Probability of getting selected as miner will be more if delegates are convinced for voting in their favor by providing currencies, gadgets etc
4	PBFT	[10]	Block created by different clients will be attached or not in the blockchain network is instantly finalized	It suffers from Sybil attack
5	PoB	[11]	Nodes burn more coins from existing coin so that the chances of being a miner in the later cycles is more	Miner has to suffer from loss of position if the value of the exchanged digital currency falls down suddenly
6	PoXR	[6]	Reward or punishment module is implemented on the basis of behavior observed during deployment of blockchain network	Huge number of parameters are required to implement reward or punishment module

Table 2 Literature survey on IoT, Blockchain and EHS

S.N	Reference	Year	Topic	Advantage	Disadvantage
1	Guo et al. [18]	2014	EHS	Preserves patient identity while providing e-healthcare or m-healthcare services	Security supervision by an EHS is not discussed to hide identity of patient among group of people
2	Jesus et al. [13]	2018	IoT	Provides security and privacy in IoT. Prevention of selfish miner (Stalker Attack)	Security of personnel identity is not considered
3	Dai et al. [16]	2019	IoT and Blockchain	A survey of blockchain and IoT applied for industries	Not suitable for 5G based applications
4	Shahnaz et al. [23]	2019	EHS	Solves data security, integrity and key management problems	Reward module is not used for appreciation
5	Ismail et al. [12]	2019	Blockchain	Temporal evolution of the different blockchain architectures and consensus protocol	Security of the data and the privacy of the user's identity are issues of high relevance
6	Prabha et al. [22]	2019	Frequent Pattern Mining	Useful for construction of tree based on transaction record	Tree is constructed for finding high utility based frequent pattern by satisfying condition of Growth and Ratio values
7	Makhdoom et al. [14]	2020	Blockchain	System of reward in the form of a digital token. Users share their data with stakeholders	Punishment mechanism is not discussed in case of misbehavior
8	Tanwar et al. [24]	2020	Blockchain	Automated data collection and verification processes, which are immutable, tamper resistant and secure	Chances of cyber-crime
9	Zheng et al. [19]	2020	Blockchain	Blockchain based transaction system with organization level provide stronger anonymity by using group-signature	Uses old method of consensus algorithm
10	Wang et al. [6]	2020	Blockchain	On the basis of reputation, trust is managed in PoXR consensus protocol. Satisfactory behavior is encouraged and bad behavior is punished to provide credibility of block in the blockchain network	Suffers from anonymization problems
11	Mayuranathan et al. [21]	2020	Blockchain	Provides security on personal information and customer daily activities stored on cloud during data transmission in entire world	Provides security against Denial of Service (DoS) and Distributed Denial of Service (DDoS) attack only
12	Prabha et al. [20]	2020	EHS, Blockchain	Health Insurance Policy is provided for security in EHS with the help of insurance company	Reward or punishment module is not discussed for appreciation or discourage based on activity
13	Cha et al. [15]	2021	Blockchain	Due to faster transaction speed, data is easily accessed from storage devices	Maintaining high security in distributed framework is a challenging task
14	Singh et al. [17]	2021	EHS	Valuable patient information is secured by introducing Privacy-Preserving Searchable Encryption technique	Same PHI is not maintained by every member of EHS
15	Aman et al. [25]	2021	EHS	Internet of Medical Things is deployed to decrease the clinical cases arise from COVID-19 pandemic	Higher degree of safety and security for medical data is still questionable

consensus algorithms in blockchain technology such as: Proof of Work (PoW) [7], Proof of Stake (PoS) [8], Delegated Proof of Stake (DPoS) [9], Practical Byzantine Fault Tolerance (PBFT) [10], Proof of Burn (PoB) [11] and PoXR [6] are reported in the literature and discussed briefly in Table 1. However, the credibility of the blockchain consensus algorithm is one of the major issues in case of semi-trusted or untrusted nodes. In this context, a distributed, decentralized reputé system based on HCM is proposed in the present paper which establishes

trustworthiness towards the improvement of the security and reliability of the system.

2.2 Related work

Blockchain network consists of participating elements, consensus protocol and cloud architecture [12]. Consensus mechanism used for the creation and validation of block in blockchain network causes security threat if the miner is selfish. A selfish node prevents an honest node to publish

Fig. 1 Basic architecture of the proposed blockchain based EHS

its blocks on the main blockchain network [13]. These types of threats could be removed by implementing PrivySharing [14]. PrivySharing is an inventive blockchain based secure and privacy-preserving data sharing mechanism. In this technique, the critical user data is kept confidential, securely processed and shared to the stakeholder on demand [14]. Blockchain based cloud architecture is also incorporated for secure sharing of information in smart city [15]. Integration of blockchain and IoT provides data privacy during the access of sensitive business-related information as well [16]. However, the existing consensus mechanism solves trusted co-operation challenges with limited credibility using reputation-based consensus mechanism easily and safely [6].

In [17], electronic healthcare system (EHS) is discussed which is based on edge computing using privacy-

preserving searchable encryption technique for handling patient records. In this technique, a certificate is issued by a trusted authority to the healthcare service provider. As a consequence, the privacy in EHS is maintained at higher accuracy and lower cost during universal accessibility [18]. Moreover, a sub-certificate is also provided to the patients by the authorized healthcare service provider [19]. In [20], blockchain technology without breaching CIA rules is employed to enhance security of healthcare related information of different healthcare stakeholders. In order to provide security on information stored on cloud server, emerging blockchain security-based algorithms are applied in [21]. The changes in information stored on cloud server could be tracked with the help of height of the Conditional Contrast High Itemset Tree (CCHIT) prepared from the transactions existing at different locations [22].

Table 3 The notations used in the proposed model

Notation	Meaning
df_d	Defined difficulty
r	Initial reputation value of patients
f_d	Final difficulty for creation of block
t_1	Time spends by patient during online accessing of E-healthcare system
t_2	Time spends by patient during offline visiting of E-healthcare system
α	Counting of online accessing of E-healthcare system by patient
β	Counting of offline visiting of E-healthcare system by patient
r_{ps}	Reputation earned from software or CPU
r_{ph}	Reputation earned by hardware or user
C_n	List of patient client
sb_{cn}	Selected list of patient client
c_l	Choice list
n_0	List of blocks
A, B, C, D, E	Name of client or patient
I, II, III, IV	Name of block
T_1, T_2, T_3, T_4	List for blockchain
r_n	Root node of Merkle tree
r_c	Child node of Merkle tree
T	Transaction list
l_1, l_2, l	Name of transaction
i_b	Confidential detail of block
e_b	Record stored on cloud server
h	Height of Merkle tree
f_r	Final earned reputation

Hence, blockchain provides a scalable, secure and integral solution for EHS [23]. Moreover, the complexity of EHS can be reduced by incorporating health record management, insurance company and blockchain technology [24]. A comparative survey based on IoT, blockchain and EHS (refer Table 2). Nowadays, the Internet of Medical Things is very prevalent for securing medical information to curb the pandemic circumstances due to COVID-19 and help to decrease its mortality rates [25].

3 Proposed blockchain based framework for electronic healthcare system (EHS)

The main objective of the proposed blockchain based framework is to provide security solution in EHS. It consists of two modules viz. selection of block and reward or punishment scheme. The basic architecture of the proposed blockchain based EHS is categorized in four layers namely, system layer, inter-network layer, blockchain layer and cloud layer respectively (sequenced in lower to upper order, see Fig. 1). The lowest layer is mainly occupied by healthcare community where doctor, nurse, lab-assistants etc. are involved. The second layer is inter-network layer

where network devices such as IoT gateway, base stations are used for communication. The third layer is intermediate between cloud layer and inter-network layer where cloud service provider forms the blockchain layer. This layer is connected with cloud where data are stored. Blockchain layer is responsible for creation, validation and selection of block for blockchain network. In addition, reward/punishment scheme is implemented on system layer by healthcare stakeholder. The identified notations used in proposed framework are mentioned (see Table 3). The proposed framework is discussed in subsequent subsections in detail.

3.1 Working principle of blockchain based EHS

The proposed EHS uses blockchain-empowered cloud architecture as depicted in Fig. 1. In the system layer of proposed EHS, medical facilities for registered patients are provided by healthcare community. In case of unavailability of expert and resources for a particular disease, the registered patients get facilities by sister healthcare community. In this layer, various IoT devices generate huge amount of patient data in real time. All these data are forwarded to inter-network layer via inter-network nodes.

Table 4 Creation of block

Algorithm 1: Final difficulty calculation
Input: $C_n, t_1, t_2, r, \alpha, \beta$
Output: f_d
1. print total number of interested patients, C_n
2. print name of the patients
3. print current reputation, r of patients with client name
4. print number of times registration form filled by patients via online (α) and offline (β) modes
5. print time taken by patients via online (t_1) and offline (t_2) to complete registration
6. for 1 to 4
7. $r_{ps} = r\alpha^{t_1}$
8. $r_{ph} = r\beta^{t_2}$
9. $f_d = r_{ps} + r_{ph}$
10. print final difficulty, f_d
11. end for

Table 5 Validation of block

Algorithm 2: Validation of block
Input: df_d, f_d, C_n
Output: sb_{cn}
1. enter value of f_d generated by client one by one
2. for 1 to 4
3. if ($C_n f_d \geq df_d$)
4. print block is successfully created
5. else
6. block is rejected
7. end for
8. print created block with client name sb_{cn}

Inter-network layer creates separate files for all interested individual patient securely and forward it to the blockchain layer. In blockchain layer, blocks are connected to each other and maintain DPL for each block. The proposed HCM is implemented in this layer. HCM contains five algorithms which are discussed in Tables 4, 5, 6, 7 and 8 respectively. The files of the interested patients are stored individually on separate systems using Algorithm 1. In later stages, these systems could be treated as blocks for blockchain network if validated successfully using Algorithm 2. After proper validation, Algorithm 3 is executed for managing fork so that only one block could be added in the blockchain network. The internal transaction record of the new block is stored on DPL. Algorithm 4 is used for finding the height of Merkle tree which is constructed using transaction records. Based on the height of the Merkle tree, reward or punishment scheme is applied for the new block on implementation of Algorithm 5. The external transaction record of the block is stored on cloud storage server which is accessible at upper layer of EHS.

The methodological flow diagram and the sequence diagram of the proposed framework are shown in Figs. 2 and 3 respectively. In this system, the files of new patients (A, B, C, D, E) are sent to blockchain layer and cloud layer via inter-network layer. In the inter-network layer, these files are arranged in queue and wait for their turn for block creation in the blockchain layer. In the blockchain layer, blockchain network exists which inter-connects different systems namely I, II, III, IV . Each system behaves as a block of the blockchain which uses DPL for storing the file of individual patient records. The secure new block is created by the healthcare service provider to capture the activity of the patient. However, this block is eligible to be a part of the blockchain network if its information is successfully validated by all members of EHS. On updating the new block in blockchain network, the later transactions are recorded in the cloud server. Consequently, the working activity of the new block is observed on the basis of the height of Merkle tree which is constructed by accessing transaction details. At the end, final reputations earned by

Table 6 Fork handling mechanism

Algorithm 3: Fork handling mechanism
Input: $sb_{cn} = (D, E)$, $n_0 = (I, II, III, IV)$ df_d , f_d , r
Output: $c_l = (l_1, l_2, l)$
1. for $i = 1$ to sb_{cn}
2. if $(f_d[i] \geq df_d$ or $E.f_d[i] \geq df_d)$
3. print fork is created.
4. else
5. print fork is not created.
6. end for
7. for $i = 1$ to sb_{cn}
8. if $(f_d[i] > f_d[i+1])$
9. return current list $c_l = l_1$ as I, II, III, IV, D
10. else if $(f_d[i] < f_d[i+1])$
11. return current list $c_l = l_2$ as I, II, III, IV, E
12. else
13. return select block having highest r
14. end for

Table 7 Merkle tree creation

Algorithm 4: Merkle tree construction
Input: $c_l = (l_1, l_2, l)$, n_0 , $count$, max , i_b , $name$, r_c , r_n , e_b
Output: M_T
1. create root, r_n of tree
2. for each transaction c_l of n_0
3. for all block $[n_0, (i_b, e_b)]$
4. if $r_n.name = n_0$ then
5. create new child, r_c of r_n
6. set $r_c.name = n_0$, $r_c.count = 0$, $r_c.max = 0$
7. $r_n.count = r_n.count + 1$
8. if $r_n.max < (i_b, e_b)$ then $r_c.max = (i_b, e_b)$
9. select r_c as root node
9. end for
10. end for

the blocks along with reward or punishment values are attached in the files of the patients.

3.2 Selection of block

The selection of a new block for the blockchain network is executed in three phases viz. creation of block (refer Table 4: Algorithm 1), validation of block (refer Table 5:

Table 8 Reward/punishment calculation

Algorithm 5: Reward/punishment calculation
Input: $n_0, f_d, t_1, t_2, r_{ps}, r_{ph}, sb_{cn}, h, i_b, e_b$
Output: r_a, r_p, f_r
1. for 1 to 4
2. if $(i_b, h == e_p, h)$
3. $r_a = 1$;
4. $r_b = 0$;
5. else
6. $r_a = 0$;
7. $r_p = 1$;
8. end for
9. calculate f_r from equation (1)
9. print $sb_{cn}.f_r, sb_{cn}.r_p$ and $sb_{cn}.r_a$

Algorithm 2) and fork handling (refer Table 6: Algorithm 3) respectively.

Phase I: In this phase, interested patients (such as A, B, C, D, E) are arranged in queue so that final difficulty for each patient could be calculated by healthcare performers. The step-by-step process of block creation is discussed below as.

- Step 1: Interested patients are gathered at a common place followed by positioning them in a queue for the assessment of final difficulty level individually.
- Step 2: Individual system files containing the records of previous registration details via online and offline modes and initial reputation (r) are created for each patient.
- Step 3: The reputation of patient is calculated on the basis of the effort taken for completing the registration process via online (r_{ps}) and offline (r_{ph}) modes. In online (r_{ps})/offline (r_{ph}) modes, the process depends on three factors viz. total number of times registration form filled via online (α)/offline (β) modes, time spend to fill the registration form via online (t_1)/offline (t_2) modes and initial reputation (r).
- Step 4: The summation of r_{ps} and r_{ph} provides final difficulty for creation of block for the blockchain network.

Phase II: The created block is added to the blockchain network after proper validation by the members of the system layer as shown in Fig. 2. On successful validation, the new block becomes a part of EHS to access the

Fig. 2 Flow diagram of proposed EHS

Fig. 3 Sequential flow of proposed framework

a C:\Users\punam\Documents\Paper 1\creation.exe

```

enter no. of times reg-form filled via online and offline mode
4
7
enter no. of times reg-form filled via online and offline mode
5
9
enter time taken by patients via online and offline mode
0.25
1.00
enter time taken by patients via online and offline mode
0.50
1.00
enter time taken by patients via online and offline mode
0.75
1.00
enter time taken by patients via online and offline mode
1.00
4.00
enter time taken by patients via online and offline mode
1.25
5.00
Final difficulty2
Final difficulty20.8284
Final difficulty381.839
Final difficulty9620
Final difficulty295282
-----
Process exited after 82.31 seconds with return value 0
Press any key to continue . . .

```

b C:\Users\punam\Documents\Paper 1\validation.exe

```

enter defined final difficulty for interested clients
5000
enter total number of interested client
5
enter final difficulty calculated by 1 interested client
2.00
block of patient is discarded.
Total number of block created0
enter final difficulty calculated by 2 interested client
20.8284
block of patient is discarded.
Total number of block created0
enter final difficulty calculated by 3 interested client
381.84
block of patient is discarded.
Total number of block created0
enter final difficulty calculated by 4 interested client
9620.00
block of patient is created successfully
Total number of block created1
enter final difficulty calculated by 5 interested client
295282.38
block of patient is created successfully
Total number of block created2
-----
Process exited after 75.02 seconds with return value 0
Press any key to continue . . .

```

c C:\Users\punam\Documents\Paper 1\forkhandling.exe

```

enter total number of block for blockchain
2
enter final difficulty of      1      client
9620
enter final difficulty of      2      client
295282.38
fork occurred
Selected Patient 2
fork occurred
Selected Patient 2
-----
Process exited after 51.85 seconds with return value 0
Press any key to continue . . .

```

d C:\Users\punam\Documents\Paper 1\reward.exe

```

enter total number of block available in blockchain network
5
enter height of merkle-tree constructed from Internal transactions
5
enter height of merkle-tree constructed from External transactions
5
REWARD1
PUNISHMENT0
enter height of merkle-tree constructed from Internal transactions
4
enter height of merkle-tree constructed from External transactions
6
REWARD0
PUNISHMENT1
enter final reputation of block available in blockchain network
5
enter their initial reputation
5
enter time taken by that patient via online and offline mode
1.25
5
enter total no. of time reg done by patient via online and offline mode
5
9
enter reputation earned via online and offline mode by that patient
37.38
295245
FINAL REPUTATION1.47628e+006
-----
Process exited after 90.07 seconds with return value 0
Press any key to continue . . .

```

Fig. 4 Snapshot of proposed HCM for reputation maintenance based on **a** Algorithm 1, **b** Algorithm 2, **c** Algorithm 3 and **d** Algorithm 5 respectively

resources of EHS securely. The step-by-step process of block validation is discussed below as.

- Step 1: The defined final difficulty (df_d) and all transaction records are stored on cloud layer as shown in Fig. 1. These parameters are securely accessed by healthcare professionals.
- Step 2: The final difficulty (f_d) of each interested patient is compared with df_d .
- Step 3: If f_d of a patient exceeds to df_d then patient is selected as block of the blockchain network. Otherwise, it is rejected.
- Step 4: The name of the selected patient along with its essential details are stored on cloud layer for further actions.

Phase III: In this phase, if more than one block is selected for single place at once then the raised condition of fork is handled as follows.

- Step 1: If final difficulty (f_d) of any two selected patients (suppose, D and E) are either same or greater than df_d then fork is generated, otherwise fork is not generated.
- Step 2: f_d of patient (D) with f_d of patient (E) is compared.
- Step 3: If f_d of D is greater than f_d of E then D is selected. The chance of selection of E is only if f_d of D is smaller than f_d of E .
- Step 4: If f_d of D is equal to f_d of E then the block with the highest earned reputation is selected.

3.3 Reward/punishment scheme

Reward/ punishment scheme is used to protect the system from different kinds of attacks performed by new block. Sometimes, malicious activity may perform by the new block and try to misuse or destroy the resources of EHS.

Phase 1: In this phase, transaction record of every block of modified blockchain network is securely accessed by healthcare stockholder from block and cloud server for Merkle tree construction similar to CCHIT. It is constructed based on internal and external transaction details of block which is stored on cloud server after the construction of modified blockchain network. After that, the height of the Merkle tree of new block is compared with the height of remaining blocks to observe the activity performed by that block (refer Table 7: Algorithm 4).

- Step 1: First of all, transaction performed by every block of the modified blockchain network is collected for Merkle tree construction.
- Step 2: Root node (r_n) of Merkle tree initializes *count* and *max* variable as 0, 0 respectively. As soon as, transaction performed by block is appeared, its child node (r_c) is created at the next level of r_n .

Table 9 Hypothesis for initial reputation of patients

S.N	Patient	Hypothesis	Initial reputation, r
1	A	suffering from cold, fever, TB etc	1
2	B	suffering from those diseases whose experts are available in sister hospital	2
3	C	suffering from those diseases whose experts are available	3
4	D	physically disabled (PD)	4
5	E	highly recommended by healthcare stakeholder	5

Table 10 Record accessed from blocks and cloud server

S.N	Block	Confidential transactions (i_b)	General transactions (e_b)
1	I	$t_1 : 2.00; t_2 : 5.50; r : 2.00; \alpha : 6; \beta : 3$	$r_{ps} : 2.16; r_{ph} : 2525.33; f_d : 2741.33; r_a : 1; r_b : 0$
2	II	$t_1 : 3.00; t_2 : 4.00; r : 7; \alpha : 7; \beta : 4$	$r_{ps} : 374.12; r_{ph} : 2236.07; f_d : 2610.19; r_a : 1; r_b : 0$
3	III	$t_1 : 3.50; t_2 : 3.50; r : 8; \alpha : 3; \beta : 5$	$r_{ps} : 374.12; r_{ph} : 2236.07; f_d : 2610.19; r_a : 1; r_b : 0$
4	IV	$t_1 : 4.50; t_2 : 6.00; r : 9; \alpha : 4; \beta : 2$	$r_{ps} : 4608; r_{ph} : 576; f_d : 5184.00; r_a : 1; r_b : 0$
5	E	$t_1 : 1.50; t_2 : 5.00; r : 5; \alpha : 5; \beta : 9$	$r_{ps} : 37.38; r_{ph} : 295245; f_d : 295282; r_a : 1; r_b : 0$

- Step 3: The occurrence of ($I, 5$) means that r_n adds I as a child node and ensure increment *count* by 1 and $r_{c.max=5}$ due to finding out *max* value as, $\max(5, 0) = 5$.
- Step 4: r_c is assigned as root node for upcoming transaction subsequence.
- Step 5: Step 1 to step 3 is iterated until occurrence of transaction is finished.

Phase II: In this phase, security analysis of the proposed EHS is observed during entire treatment process after modification of blockchain network. The sequential step-wise flow of reward/punishment method is as follows (refer Table 8: Algorithm 5).

- Step 1: The height of Merkle tree is prepared from internal and external transactions of every block.
- Step 2: The height of Merkle tree as calculated from internal transaction (i_b) to that of the external transaction (e_b) for each block is compared.
- Step 3: If height of Merkle tree for internal transaction ($E.i_b$) of a selected block (E), is equal to the height of Merkle tree for external transaction ($E.e_b$) then its r_a is incremented by 1 and its r_p is decreased by 1.
- Step 4: If height of $E.i_b$ is either greater than or lesser than the height of $E.e_b$ then its r_p is incremented by 1 and its r_a is decreased by 1.
- Step 5: The current reputation r , along with r_a and r_p is stored on cloud server for further treatment if required in future.

- Step 6: The final earned reputation (f_r) is calculated using (1). Finally, f_r with r_a and r_p are listed in patient's file.

The final earned reputation, f_r of each block is calculated using (1) as

$$f_r = \sum_{n=1}^5 (i_{b[n-1]} e_{b[n-1]}) - i_{b[n]} e_{b[n]} = t_1 r_{ps} + t_2 r_{ph} + r f_d + \alpha r_a - \beta r_p \quad (1)$$

Moreover, blockchain technology has an important advantage of stored data auditability at ease.

4 Experimental Evaluation

In this section, the architecture of blockchain for the proposed EHS is investigated. Moreover, the mechanism of earning reputation by a block is elaborated in detail. The analysis is based on the emergency requirement of EHS by a patient if and only if a single vacant seat is available. Finally, the security perspective of the proposed framework is illustrated.

4.1 Hypotheses and evaluation

Hypothetical environment is created to observe initial reputation of interested patients for successful implementation of the proposed framework such as: patient A: suffering from cold, fever, TB etc. having initial reputation 1,

Fig. 5 Resource consumed by proposed HCM during implementation of **a** Algorithm 1, **b** Algorithm 2, **c** Algorithm 3 and **d** Algorithm 5 respectively

patient *B*: suffering from some disease whose experts are not available in current healthcare community but can be called from sister supportive healthcare community in case of emergency having reputation 2, patient *C*: suffering

Fig. 6 Comparison chart among reputation value earned via online, offline mode and final difficulty

from some disease whose experts are easily available in current healthcare community having reputation 3, patient *D*: physically disabled having reputation 4, and patient *E*: highly recommended by healthcare stakeholder having reputation 5. The value of final difficulty for the creation of block for blockchain network requires initial reputation which is mentioned in Table 9.

The difficulty for creation of block is defined at the beginning of EHS and stored on the cloud server. The defined final difficulty (df_d) is assumed as 5000. As represented in Table 9, the final difficulty (f_d) is calculated for each block using Algorithm 1 (refer Table 4) and validated using Algorithm 2 (refer Table 5). Consequently, *D* and *E* are selected as the blocks of the blockchain network. Among these two choices *E* is selected using Algorithm 3 (refer Table 6). The blockchain network is updated with the new block, *E*. Hence, the information stored on the cloud server is upgraded as well.

The assumed record of all transactions performed by every block is given in Table 10. Next, Merkle tree is constructed for storing confidential and general transactions using Algorithm 4 (refer Table 7). The Merkle tree created by the blocks (*I*, *II*, *III*, *IV*) for internal and external transactions are shown in Figs. 7, and 8 respectively. If block *E* is used for providing malicious activity, then one of the secret keys, suppose t_1 is guessed by healthcare stakeholder by using DPL (refer Fig. 9). Moreover, t_1 is stored on cloud server. Hence, the Merkle tree for block (*E*) implements punishment scheme due to variation of height using Algorithm 5 (refer Table 8).

4.2 Performance evaluation

The proposed HCM Algorithm 1, 2, 3 and 5 are developed to provide security in EHS. The concept of Merkle tree construction [22] is represented as Algorithm 4. These algorithms are implemented in C++ language and executed in Dev C++ software to investigate the performance and latency of the proposed HCM. The execution is performed in HP laptop that uses Microsoft Window 10 Home Single Language operating system having

Table 11 Final difficulty along with reward and punishment for creation and validation of block in PoXR scheme

S.N	Client	t_1 (hours)	r	α	β	r_u	t_2 (hours)	f_d	r_a	r_p
1	A	0.25	1.00	1	1	1.00	1	1	1.0367	1
2	B	0.50	2.00	2	3	1.414	2	0.242	2.025	1.454
3	C	0.75	3.00	3	5	1.316	3	-5.42	3.015	1.908
4	D	1.00	4.00	4	7	1	4	-17	4.0067	2.362
5	E	1.25	5.00	5	9	0.6687	5	-33.98	5	2.816

Table 12 Comparison between PoXR and proposed HCM protocol

S.N	Parameter	PoXR	Proposed HCM protocol
1	Final difficulty (f_d)	Exponentially decreasing pattern	Exponentially increasing pattern
2	Merkle-tree construction	Not used	Constructed using CCHIT [24]
3	Height of transaction	Increases with the increment in reputation	Depends on Merkle-tree height
4	Reward and punishment module	Calculated using complex equations which require more parameters. Hence, more sensitive against parameter variations	Simply measured by comparing the height of Merkle-tree which is constructed using internal and external transaction parameters
5	Reward and punishment rate	Assigned in continuous manner	Assigned in discrete manner. Here, $r_a = 0$; $r_p = 0$ is used for neutral behavior and $r_a = 1$; $r_p = 0$ is assigned for reward, however, $r_a = 0$; $r_p = 1$ is assigned for punishment modules
6	Final earned reputation	Reward and punishment credit based final earned reputation is not calculated	Final reputation is calculated for each block along with reward and punishment module

Fig. 7 Merkle tree for secret transaction having height = 5 **a** Block I, **b** Block II, **c** Block III, **d** Block IV

Intel(R) Core (TM) i5-8265U CPU @ 1.60 GHz, 1800 MHz 4 Core(s), 8 Logical Processor(s). The snapshot of output produced is shown in Fig. 5. The resource consumed by the system during execution of code is shown in

Fig. 6. The latency graph (see Fig. 5) shows that it consumes less CPU time (up to 2%) and memory (up to 51%) respectively.

Table 13 Final difficulty for creation and validation of block

S.N	Client	t_1 (hours)	t_2 (hours)	α	β	r_{ps}	r_{ph}	f_d	$f_d \geq df_d$
1	A	0.25	1.00	1	1	1.00	1	2.00	False
2	B	0.50	2.00	2	3	2.83	6	20.8284	False
3	C	0.75	3.00	3	5	6.84	375	381.84	False
4	D	1.00	4.00	4	7	16.00	9604	9620.00	True
5	E	1.25	5.00	5	9	37.38	295,245	295,282.38	True

Fig. 8 Merkle tree for general transaction where height = 5 **a** Block I, **b** Block II, **c** Block III, **d** Block IV

In Fig. 6, a comparison of the final difficulty of all blocks (*I, II, III, IV* and *E*) is done based on reputation earned via online, r_{ps} and offline, r_{ph} mode. The bar diagram shows that the final difficulty of all blocks are same even if their reputation earned via online and offline mode is different. It is because same procedure has been followed by all blocks to be the part of blockchain network. The final difficulty in complete registration process via online and offline modes for the creation of a new block is graphically analyzed as well. Thereafter, the blockchain network is successfully deployed.

4.3 Performance comparison with PoXR algorithm

The formal expressions of PoXR for final difficulty calculation are given as (2) and (3)

$$r_u = \frac{5}{\alpha^{t_1}}, \quad (2)$$

$$f_d = t_2 - t_2\beta \sum_{r=1}^5 \left(\frac{r_u - r}{r} \right). \quad (3)$$

In PoXR, the probability of obtaining the next honest block increases with an increase in reputation. Hence, the tendency of each block to gain higher reputation makes the

process iterative. Moreover, block preserves its identity to avoid the punishment for malicious activity. The reward and punishment are calculated using (4) and (5) respectively as

$$r_a = r_a + \alpha \sum_{r=1}^5 \left(\frac{1 - count}{t_{cmp}} \right) (r_{max} - r_a), \quad (4)$$

$$r_p = r_p - \theta e^{\delta t} \sum_{r=1}^5 (r_p - r_{min}). \quad (5)$$

Both techniques are evaluated using same parameters for impartial comparisons (refer Table 11). However, PoXR involves some more parameters for the calculation of f_d , r_a and r_p modules which are given as $\psi = 0.01$, $\delta = 0.2$, $\theta = 0.01$, $t_{cmp} = 3$, $t_{dec} = 20$, $r_{max} = 5$, $r_{min} = 1$ [6]. The key findings on comparison between PoXR and the proposed HCM are enlisted in Table 12. From Tables 10, 11 and 12, it is observed that the proposed HCM is opposite in nature to that of PoXR in respect of the calculation of final difficulty and reward and punishment rates. Moreover, a simple Merkle tree is constructed for granting reward and punishment in HCM scheme against the complex PoXR scheme.

Fig. 9 Merkle tree used for punishment scheme done by new block having height 4 and 6 respectively. **a** Secret transaction, **b** general transaction

4.4 Security analysis

In this section, the working principle of the proposed blockchain network in EHS environment is investigated. It provides secret sharing of data from cloud server including award and punishment phenomenon. It is designed to satisfy CIA triad rules [26] discussed as below:

Confidentiality: Medical history of healthcare workers is stored in cloud server by applying hash functions-based encryption technique. Hash functions have pre-image resistance property. Therefore, it is computationally hard to achieve original transaction (i_b) from encrypted transaction (e_b). Hence, encrypted data could not be easily guessed by unknown user. Moreover, healthcare workers use their own secret keys, (such as t_1 , t_2 , α etc.) to maintain privacy of data. Merkle tree is constructed by each block of blockchain network on the basis of confidential transaction record (see Fig. 7).

Availability: In the proposed framework, general health related information is distributed among all blocks by using DPL, and cloud server. Therefore, the data loss in any block will be securely restored with the help of DPL. The structure of Merkle tree for general transaction record as mentioned in Table 13 is elaborated in Fig. 8.

Integrity In the proposed framework, reward/punishment-based reputation scheme is applied to restrict bad activity performed by any block. If bad activity is performed, the secret key is shifted from confidential to general transaction. Hence, the height of Merkle tree created by malicious block is not matched with the height of Merkle tree created by another block. As a consequence, malicious activity performed by new block is captured by the healthcare stake holders for punishment scheme (see Fig. 9).

The average height of Merkle tree is measured for application of reward or punishment phenomenon. The height of Merkle tree decreased or increased with the removal or addition of some details respectively on any of the transactions. Consequently, punishment is given to that block as shown in Fig. 9.

5 Conclusion

The security of confidential medical information is an important concern in EHS. To overcome these sensitive issues, several solutions are discussed in the literature. However, most of these solutions are not able to solve the

predefined research questions as pointed out in Sect. 2 of the paper. In this context, the present research work is dedicated to develop an EHS framework using HCM based blockchain technology. In this system, all interested patients have to go through different phases of block creation and validation, fork handling, and Merkle tree formation for storing transaction records. The malicious activity of the block is continuously judged by comparing height of the Merkle tree as constructed via secret and general transactions. Secret transactions are stored individually on DPL of each block; however, the general transactions are stored on cloud server. The reward/ punishment scheme is applied to maintain good environment in the proposed EHS. At the final stage of deployment, each block calculates their final difficulty. In addition, final earned reputation, reward and punishment values are added in the file of the selected patient. Moreover, patients have to maintain their reputation for entire life-cycle. The blocks of the blockchain network are compared graphically. The results show that range of final difficulty of all blocks is same instead of varying reputation earned from online and offline modes of registration process. The latency graph shows that the CPU and memory consumed during implementation of HCM (Algorithm 1, Table 4), (Algorithm 2, Table 5), (Algorithm 3, Table 6), and (Algorithm 5, Table 8) are below two percent and about fifty percent respectively. Moreover, the basic security goal (confidentiality, integrity and availability) is achieved in the developed framework during hypothetical implementation of HCM (Algorithm 4, Table 7). In addition, the proposed scheme is evaluated with respect to PoXR scheme. It is observed that the proposed HCM is simple in implementation of reward and punishment modules than that of PoXR.

Acknowledgements I confirm that this work is original and has not been published elsewhere nor it is currently under consideration for publication elsewhere.

Funding Not applicable.

Availability of data and material Not applicable.

Code availability Not applicable.

Declarations

Conflict of interest I confirm that I have no conflict of Interest

References

- Griggs K, Ossipova O, Kohlios C, Baccarini A, Howson E, Hayajneh T (2018) Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. *J Med Syst* 42(7):1–7
- Hathaliya J, Sharma P, Tanwar S, Gupta R (2019) Blockchain-based remote patient monitoring in healthcare 4.0. In: *IEEE 9th International Conference on Advanced Computing (IACC)*, Tiruchirappalli, India
- Sun J, Fang Y, Zhu X (2010) Privacy and emergency response in e-healthcare leveraging wireless body sensor networks. *IEEE Wirel Commun* 17(1):66–73
- Hossain M, Paul A, Islam M, Atiquzzaman M (2018) Survey of the protection mechanisms to the SSL-based session Hijacking attacks. *Netw Protocols Algorithms* 10(1):83–108
- Zheng X, Sun S, Mukkamala R, Vatrappu R, OrdieresMere J (2019) Accelerating health data sharing: a solution based on the internet of things and distributed ledger technologies. *J Med Internet Res* 21(6):13583
- Wang E, Sun R, Chen C, Liang Z, Kumari S, Khan M (2020) Proof of X-repute blockchain consensus protocol for IoT systems. *Comput Secur* 95:101871
- Liu D, Camp L (2006) Proof of work can work. In: *5th annual workshop on the economics of information security*, England, UK, 2006
- King S, Nadal S (2012) Ppcoin: peer-to-peer crypto-currency with proof-of-stake. Self-published paper 19(1)
- Yang F, Zhou W, Wu Q, Long R, Xiong N, Zhou M (2019) Delegated proof of stake with downgrade: A secure and efficient blockchain consensus algorithm with downgrade mechanism. *IEEE Access* 7:118541–118555
- Castro M, Liskov B (1999) Practical byzantine fault tolerance. In: *Third Symposium on Operating Systems Design and Implementation*, New Orleans, USA, 1999
- Karantias K, Kiayias A, Zindros D (2020) “Proof-of-Burn”, in financial cryptography and data security. Springer, Cham, pp 523–540
- Ismail L, Materwala H, Zeadally S (2019) Lightweight blockchain for healthcare. *IEEE Access* 7:149935–149951
- Jesus E, Chicarino V, Albuquerque C, Rocha A (2018) A survey of how to use blockchain to secure internet of things and the stalker attack. *Secur Commun Netw* 2018:1–27
- Makhdoom I, Zhou I, Lipman M, Ni W (2020) PrivySharing: a blockchain-based framework for privacy-preserving and secure data sharing in smart cities. *Comput Secur* 88:101653
- Cha J, Singh S, Kim T, Park J (2021) Blockchain-empowered cloud architecture based on secret sharing for smart city. *J Inf Secur Appl* 57:102686
- Dai H, Zheng Z, Zhang Y (2019) Blockchain for internet of things: a survey. *IEEE Internet of Things* 6(5):8076–8094
- Singh A, Chatterjee K (2021) Securing smart healthcare system with edge computing. *Comput Secur* 108:102353
- Guo L, Zhang C, Sun J, Fang Y (2013) A privacy-preserving attribute-based authentication system for mobile health networks. *IEEE Trans Mob Comput* 13(9):1927–1941
- Zheng H, Wu Q, Xie J, Guan Z, Qin B, Gu Z (2020) An organization-friendly blockchain system. *Comput Secur* 88:101598
- Prabha P, Chatterjee K (2020) Securing telecare medical information system with blockchain technology. In: *2020 2nd International Conference on Advances in Computing, Communication Control and Networking (ICACCCN)*, Greater Noida, India, 2020
- Mayuranathan M, Murugan M, Dhanakoti V (2021) Enhanced security in cloud applications using emerging blockchain security algorithm. *J Ambient Intell Humaniz Comput* 12:6933–6945
- Prabha P, Mazumdar A (2019) Conditional contrast high itemset mining for two dataset in two time slot. In: *2nd International Conference on Power Energy, Environment and Intelligent Control (PEEIC)*, Greater Noida, India, 2019.
- Shahnaz A, Qamar U, Khalid A (2019) Using blockchain for electronic health records. *IEEE Access* 7:147782–147795

24. Tanwar S, Parekh K, Evans R (2020) Blockchain-based electronic healthcare record system for healthcare 4.0 applications. *J Inf Secur Appl* 50:102407
25. Aman A, Hassan W, Sameen S, Attarbashi Z, Alizadeh M, Latiff L (2021) IoMT amid COVID-19 pandemic: application, architecture, technology, and security. *J Netw Comput Appl* 174:102886
26. Singh A, Chatterjee K (2019) Security and privacy issues of electronic healthcare system: a survey. *J Inf Optim Sci* 40(8):1709–1729