Check for updates

Received: 23 August 2021 | Revised: 28 October 2021 | Accepted: 23 November 2021

DOI: 10.1002/ett.4421

RESEARCH ARTICLE

WILEY

Blockchain-enabled secure communication mechanism for IoT-driven personal health records

Mohammad Wazid[1] | **Ashok Kumar Das**[2] | **Youngho Park**[3]

[1]Department of Computer Science and Engineering, Graphic Era Deemed to be University, Dehradun, India

[2]Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad, India

[3]School of Electronic and Electrical Engineering, Kyungpook National University, Daegu, Korea

Correspondence
Ashok Kumar Das, Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad 500032, India.
Email: iitkgp.akdas@gmail.com

Funding information
BK21 FOUR Project, Grant/Award Number: 4199990113966; National Research Foundation of Korea (NRF), Grant/Award Number: 2020R1I1A3058605

Abstract

The information system of healthcare operates through various frameworks, like wireless body area network, telecare medical information system, and mobile or electronic healthcare. All these systems need to maintain the personal health records (PHRs) for various users (ie, patients, doctors, and nurses). In such systems, we need to process and store the health related sensitive data (ie, PHRs). In this article, we aim to provide a robust security mechanism to secure exchange and storage of healthcare data, especially PHRs. We present a generic architecture of blockchain-enabled secure communication mechanism for Internet of Things-driven personal health records (BIPHRS). We then discuss various threats and security attacks of healthcare system along with different available security mechanisms. The conducted security analysis and detailed comparative study of the state of art blockchain enabled security schemes for PHR systems show that the proposed BIPHRS provides a better security and more functionality features as compared to other similar existing approaches.

1 | INTRODUCTION

A personal health record (PHR) is a health record where health related information of patients is maintained by the patient. PHR is different than the widely used electronic health record, which is operated by institutions, like, hospitals, testing laboratories, which contains data entered by their staff for example, billing information required for medical insurance claims. The motive of PHR is to provide the correct summary of the patients medical records, which can be access through the Internet via smartphone applications. PHR includes patient's data, like, physiological data, laboratory tests results, which is collected through different means.[1] Internet of Medical Things (IoMT) is the collection of smart healthcare devices (ie, implantable devices, wearable devices) which have communication capabilities and send the health related data of patients to the nearby personal server. Then personal server sends the healthcare data to the cloud servers for further storage and processing. This arrangement is useful for the collection and storing of PHRs. However, such kind of data transmission is vulnerable to different types of information security related attacks, which will be elaborated further. Therefore, we need some security solutions to secure the PHRs. Under such situations, the blockchain based solutions can be very helpful. Blockchain maintains information in a specific way through which it is very difficult to update the stored information. It is a digital ledger of transactions, which is distributed in nature, and it is also available to all authorized participants of the network. In the blockchain, every block contains certain transactions, in case of

Mohammad Wazid, Ashok Kumar Das, and Youngho Park contributed equally to this study.

 © 2021 John Wiley & Sons, Ltd.

happening of a new transaction a new record of that transaction is added to the blockchain via a block. Then, such an added information is visible to the ledger of all participants.[2,3] The decentralized database managed by multiple parties is called as distributed ledger technology (DLT). Blockchain uses DLT for storing the transactions, which are recorded with the "immutable cryptographic operations." For instance, information (healthcare records) can be added in the form of certain encrypted transactions (ie, encryption with the public key of the owner).[4,5]

Various properties of blockchain are briefed as follows:[6]

- *Immutability*: The data in terms of the blocks are stored into the blockchain. Immutability means something that cannot be modified, updated or altered. It is considered as one of the top blockchain features which assures that the technology must remain as it is—a permanent, unchangeable network. This property of the blockchain is achieved through the use of cryptographic hash function.
- *Decentralized*: The blockchain does not possess any governing authority or a single organization looking after the framework. Instead of that, a group of nodes has the responsibility to maintain the network in order to make it decentralized. Such a network is known as peer-to-peer (P2P) network, where it partitions the entire workload among participants, who are all equally privileged, known as *peers*. This is also treated as another key feature of blockchain technology.
- *Enhanced security*: Every information (data) put into the blockchain is hashed cryptographically. Therefore, the information on the network hides the true nature of the data. In addition, for sensitive healthcare related data, the information in forms of transactions is also put encrypted way.
- *Distributed ledgers*: The ledger on the blockchain network is preserved by all other nodes on the system. As a result, such a distributed computational power across the nodes helps to assure a better output.
- *Time-stamped*: All blocks in the blockchain contain block generation timestamps, which is further helpful to overcome the data freshness related issues.

Blockchain can be divided into certain categories on the basis of its deployment and features. The details of different types of blockchains are given below:[2,3,7]

- *Public blockchain*: In a public type of blockchain, the access to the blockchain is given to anyone, who wishes to take participation in the process. Bitcoin, Ethereum, and litecoin are examples of the cryptocurrency networks on the basis of public blockchain.[3]
- *Private blockchain*: In a private type of blockchain, the blockchain and its associated systems are considered as private, and they are controlled only by the authorized people from a specific organization. It is not like that anybody come and join the network of a blockchain, rather the users who get invitation can only join. For example, the blockchain of a personal health records system can be considered as a private blockchain.[3]
- *Consortium blockchain*: This blockchain in maintained by a few organizations. In a consortium type of blockchain, the processes are set up and controlled by the initially assigned users. For example, a consortium blockchain could be the blockchain of a smart transportation system.[3]

The following are the key differences of the different blockchain architectures:[2,3]

- A private blockchain is assumed to be more centralized as an authorized group from the specific organizations controls it. However, it provides more privacy as compared to the public blockchain.
- A public blockchain is considered as an open-ended and decentralized blockchain. In this type of blockchain, anybody can join the network at any time.
- In a public blockchain, the information (inside the blocks) is visible to everybody. Moreover, anybody can take participation in the ongoing consensus process. But, it is less efficient because it requires some extra time for the addition of new blocks into the blockchain.
- From efficiency point of view, the time needed for each transaction in a public blockchain is less environmental friendly as it needs a larger amount of computation power than a private blockchain.

The following are the main contributions of this article:

21613915, 2022, 4, Downloaded from https://onlinelibrary.wiley.com/doi/10.1002/ett.4421 by University Of Waterloo Dana Porter Library, Wiley Online Library on [20/07/2023]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

- We provide the details of various threats and attacks of healthcare system along with different available security mechanisms.
- We propose an architecture of blockchain-enabled secure communication mechanism for Internet of Things (IoT)-driven personal health records (BIPHRS).
- We provide an attack model to address the potential attacks of BIPHRS.
- We provide the details of blockchain enabled security schemes applicable for personal health records system.
- We also conduct a comparative study of proposed BIPHRS and other related existing schemes. In which the various security and functionality features, communication costs, and computation cost are compared and analyzed.
- Finally, a practical demonstration of the proposed BIPHRS is provided to observe its effect on the different performance parameters.

The remaining part of this article is structured as follows. The applications of blockchain enabled IoT driven personal health records system (BIPHRS) are discussed in Section 2. The security and privacy requirements of BIPHRS are highlighted in Section 3. This section also contains the details of security threats and attacks of BIPHRS. The architecture of BIPHRS is then discussed in Section 4 along with an applicable attack model. Security analysis of the proposed BIPHRS is given in Section 5. The discussion on "blockchain enabled security schemes for personal health records system" is given in Section 6. A comparative study on blockchain enabled security schemes for personal health records system is then given in Section 7. In addition, a practical implementation of the proposed BIPHRS is given in Section 8. Finally, the article is concluded in Section 9.

2 | APPLICATIONS OF BLOCKCHAIN ENABLED IOT DRIVEN PERSONAL HEALTH RECORDS SYSTEM

BIPHRS can be used for various applications. Some of them are discussed below.[8-11]

- *Management of healthcare operations*: It is very difficult for the doctor to do the inspection of multiple patients at the same time. Even that becomes very difficult in case of couturiers of very high population, that is, China, India. BIPHRS is also facilitates the quick response to the patients from concerned medical staff, that is, available doctor can provide the response. Means activities can be managed as per the needs. Therefore, BIPHRS provides support for the overall management of hospital operations.[12]
- *Detection and prevention of diseases*: BIPHRS provides support for the early detection of various kinds of illness, that is, cancer, heart attack, diabetes, asthma attack, cancer, and many more. The deployed smart healthcare devices (eg, implantable medical devices or wearable devices) continuously monitor the health of the patients and send alerts in case of any health emergency. For instance, smart healthcare devices monitor the heart rate and blood pressure of the patient and in case of any heart failure situation sends alerts to the concerned healthcare staff. Thus BIPHRS is helpful for the detection and prevention of various kind of diseases.[9,13]
- *Drug supply chain management*: Illegal medicine counterfeiting can be performed on the drugs packages in their transit from production house to the patient's delivery. The secure drug supply chain management can be conducted through blockchain based mechanism of BIPHRS. As per the above mentioned mechanism the "smart tags" can be kept over the drugs bags, which are further helpful in the proper distribution and monitoring of the drugs. That provides protection against the "anti-counterfeiting of the medicines".[14] In other circumstances "radio frequency identification (RFID)" tags can be used for the protection of drug bags against medicine counterfeiting. A blockchain can be implemented for the entire process, that is, from the factory to the consumer. If malicious actors attempt to duplicate/counterfeit a bag, such an incident can be detected by the help of deployed "blockchain based anti-counterfeiting technique." In such scenario, patient gets the original medicine which further help them to cure their medical problems quickly.
- *Facility of urgent care*: BIPHRS also provides the facility of urgent care. Most of the users and patients of the BIPHRS are connected to each other over the Internet. Therefore, tracking of health conditions of the patients is very easy. If doctors are not available in some particular time on a specific place, then the help of other available doctors can be taken. Furthermore, if healthcare equipments and medicine are not available in some place then that can also be

21613915, 2022, 4, Downloaded from https://onlinelibrary.wiley.com/doi/10.1002/ett.4421 by University Of Waterloo Dana Porter Library, Wiley Online Library on [20/07/2023]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

arranged quickly as BIPHRS also maintains the records of all these things. Hence urgent care can be provided to a patient in case of any emergency.[4,15]

- *Portal of healthcare data*: Portal of healthcare data is an essential component of BIPHRS. This platform provides patients access to their health records, which can be accessed through any device, that is, smartphone, tablets, desktop. It includes all the information stored in the PHR, like, illness of the patient, ongoing treatment, doctor for consultation, vaccination, etc. Other additional features may be like the scheduling of appointments, viewing of bills, health insurance records, and online payments of bills. In some cases, portals provide the facility to the patients to have a conversation with the healthcare experts. So no need to wait for the long hours to schedule the appointments, a patient can now simply log in, check their doctor's availability and can consult. Moreover, patients can book medicines and lab tests online through the portal.[4,12]

3 | SECURITY AND PRIVACY IN BIPHRS

BIPHRS has great impact on the lives of the people due to its applicability in various kinds of application as discussed earlier. However, it also suffers from various types of security and privacy related issues. The details of security requirements and security threats and attacks of BIPHRS are given below.[4]

3.1 | Security requirements in BIPHRS

The following are security requirements of BIPHRS.

- *Secrecy of health records*: BIPHRS stores the sensitive healthcare data of the patients. Therefore, it becomes essential to provide secrecy to the personal health records of the patients. Health records can be in any form, like, who has which illness, which treatment is going, applied medical insurance policies, etc. Various data encryption techniques (ie, symmetric key/public key) can be used to make this data secret. These encryption techniques provide the secrecy to the stored data as well the data, which is in transit.[12,16]
- *Integrity of health records*: BIPHRS's should be protected against any kind of unauthorized updating. To maintain the integrity, the PHR, we should utilize the hash algorithms, that is, SHA256. Under such mechanism a hash value is computed at the sender's end and then this will be appended with the original message. Again another hash value is calculated at the receiver's end, which will be matched with the received hash value. If both hash values are equal, then it is considered that the received message is the original one. Otherwise message was modified in the channel. It is also desirable that all sensitive credentials, like passwords should be stored in the form of hash values in the database of the servers and when a user tries to login into the system then another hash value should be computed, which should be matched with the stored hash value of the password. If that matches then user should be treated as the genuine one and allowed to log into the system.[15]
- *Availability of the system and its resources*: All resources of BIPHRS like, data resources, servers, processing units should be available to the legitimate users 24×7 hours basis and there should not be any denial of service. Meanwhile, we have to also protect the infrastructure of BIPHRS against the denial service attacks/distributed denial of service (DoS/DDoS) attacks. Because under the influence of these attacks, the system and its associated resources are not available to the legitimate user. These attacks are launched through various flooding methods, that is, SYN flood, UDP flood, HTTP flood, and many more. Therefore, it is very important to deploy some intrusion detection and prevention mechanism, which can prevent such attacks and also make available the required resources to the legitimate users.[5]
- *Authenticity of the system's entities*: It is another important feature, which should be deployed in BIPHRS. By the authentication mechanism, various entities of the BIPHRS can authenticate among each other. Further the entities can establish shared secret session keys for their secure communication.[17] Therefore, under the deployment of such mechanism, the unauthorized third party (ie, attackers, hackers) will be able to interfere into the ongoing communication. 2-factor, 3-factor user authentication schemes are famous these days and widely deployed for the purpose of authentication and key establishment.
- *Authorization and access control on the system's resources*: Authorization and access control is the process of putting restrictions on the unauthorized access to the resources of the system. Under the deployment of such kind of

21613915, 2022, 4, Downloaded from https://onlinelibrary.wiley.com/doi/10.1002/ett.4421 by University Of Waterloo Dana Porter Library, Wiley Online Library on [20/07/2023]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

mechanisms, the system stops the unauthorized user/device to get access to the valuable resources. Schemes like, certificate based access control and certificate less access control are widely used to achieve the authorization and access control.[14]

- *Non-repudiation*: Non-repudiation is related to any kind of denying. Suppose a communicating party has sent a message in the past and later on that party has denied that he/she has not sent that message. Therefore, we need some mechanism to stop this non-repudiation among the communicating parties of the system. Non-repudiation can be from both sides, that is, sender's side or receiver's side. Techniques like digital signature generation and verification (ie, digital signature standard, elliptic curve digital signature algorithm) are useful for the non-repudiation process.
- *Forward and backward secrecy*: Forward secrecy property assures that a user or a device, which leaves the network will not be able access the information, which will be exchanged in the future. Contradictory to that secrecy property assures that a user or a device, which has just joined the network does not have any access to the information, which was exchanged in the past. Access control and encryption mechanisms are helpful for the maintain the forward and backward secrecy properties.
- *Freshness of healthcare data*: Fresh data is always helpful to make correct decisions at the correct time, especially, in case of healthcare domain. Therefore, there should be some assurance that concerned authority should get the fresh data. For such purpose timestamp values can be applied to the transmitted messages.

3.2 | Security threats and attacks in BIPHRS

BIPHRS may suffer from various types of passive and active attacks. Some potential attacks of BIPHRS are discussed below.[12]

- *Replaying of information attack*: In this malicious act, adversary $\mathcal{A}$ tries to replay the old messages. Means a network entity receives the old messages, which was exchanged in the past not the new one. For the protection purpose, freshly generated timestamp values can be used in the exchanged messages. These timestamp values are also verified at the receiver's end. If verification happens successfully then message will be accepted by the receiver. Otherwise that message will be discarded.
- *Man-in-the-middle (MiTM) attack*: In this malicious act, $\mathcal{A}$ tries to update the exchanged messages and after the updating sends that message to an entity of the network. For the protection purpose, it is necessary to use randomly generated nonce values in the exchanged messages along with the secret keys and secret numbers, which are not known to $\mathcal{A}$. Therefore, under such deployment $\mathcal{A}$ cannot modify the exchanged messages successfully.
- *Impersonation attack*: In this malicious act, $\mathcal{A}$ tries to create the messages on behalf of a legitimate device/user of the network. $\mathcal{A}$ then sends the fake created message to the recipient to involve him in his/her communication. That party assumes that he/she communicates with the original party but in actual he/she communicates with $\mathcal{A}$. For the protection purpose, it is necessary to use randomly generated nonce values in the exchanged messages along with the secret keys and secret numbers, which are not known to $\mathcal{A}$. Therefore, under such deployment $\mathcal{A}$ cannot create the original messages on behalf of a legitimate entity of the network.
- *Privileged insider attack*: In privileged insider attack, the privileged insider user of the trusted registration authority (server) who has some malicious intention and also has the knowledge of some registration information of the network entities tries to deduce the secret credentials, which belong to the legitimate network entities. After executing these malicious tasks privileged insider user further tries for other associated attacks, like MiTM, impersonation and unauthorized session key computation. For the protection purpose, it is recommended to delete all registration information from the database of the trusted registration authority and do not store any secret credentials/keys in its memory.[18]
- *Unauthorized session key computation attack*: In this malicious act, $\mathcal{A}$ tries to perform the unauthorized session key computation on the deployed security protocol. For the protection purpose, it is recommended that session key should be computed using the short term secrets (ie, timestamp values, random nonce values) and long term secrets (ie, secret keys and identities). Under the deployment of such security mechanisms, $\mathcal{A}$ is not able to launch the unauthorized session key computation attack as he/she does not have the knowledge of short term secrets and long term secrets.[19]
- *Malware injection and spreading attack*: Different types of malware attacks like keylogger, spyware, virus, worms, trojan horse, ransomware, etc., can be launched in the BIPHRS, which make the system and its resources totally down and

21613915, 2022, 4, Downloaded from https://onlinelibrary.wiley.com/doi/10.1002/ett.4421 by University Of Waterloo Dana Porter Library, Wiley Online Library on [20/07/2023]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

under the influence of these attacks system will not be able to provide the services to the legitimate users of the system. Even some of them also disclosed the sensitive PHR to the unauthorized third parties. Most of the time, malware attacks are launched through a bot (Internet attacker system) or through the botnet (network of attacker system). A sophisticated botnet can bring down an infrastructure within few seconds. For the protection purpose, it is recommended to use firewalls along with some advanced intrusion detection and prevention systems.[5,20,21]

- *Malicious injection and scripting attacks*: Attacks like, SQL injection and cross site scripting, cross site request forgery are also possible in BIPHRS. Under the influence of these attacks, the sensitive information, like, passwords, card number used for the payments, health records, etc., can be leaked to the unauthorized parties. $\mathcal{A}$ may also have potential to modify some of the health records. For the protection purpose, it is recommended to use firewalls along with some advanced intrusion detection and prevention systems.
- *DoS/DDoS attacks*: In the presence of denial of service attack (DoS) or distributed denial of service (DDoS) attack, the resources of BIPHRS are not available to the legitimate users of the system. These attacks can be performed through malicious tasks like, SYN flood, HTTP flood, UDP flood, TCP flood, etc. For the protection purpose, it is recommended to use firewalls along with some advanced intrusion detection and prevention systems.
- *Physical device capture attack*: In this malicious act, $\mathcal{A}$ first steals the deployed smart healthcare devices of BIPHRS and then use them to extract sensitive information (ie, secret keys, credentials) from their memory by making the use of advanced power analysis attack. Therefore, it is recommended to not store the secret values directly in the memory of the devices. Further we should use different credentials, identities and secret values for different devices. In that situation, if a device compromises physically, then that compromising will result in the leakage of only its data not the data of the other devices. Therefore, the other part of the network is still safe and secure.
- *Stolen verifier attack*: In the stolen verifier attack, $\mathcal{A}$ tries to utilize the information, which maintained in the form of dictionary. This information belongs to the various entities of the system. Then that information is further helpful to launch other associated attacks, that is, MiTM, impersonation, illegal session key computation, etc., on BIPHRS. For the protection purpose, we should not directly store any secret information in the database of the servers (ie, healthcare server). In that case, secret information is not available to $\mathcal{A}$ to launch the related attacks.
- *Consensus attacks*: In BIPHRS, various consensus attacks (ie, 51% attack, long-range attack, the balance attack, Sybil attack) can be launched by $\mathcal{A}$ to break its security. Under the influence of these attacks, $\mathcal{A}$ tries to create/introduce a fake blockchain in the system or attempts to modify a fraction of the blocks of the blockchain. Some of the possible solutions are "deployment of large number of nodes" and "high network hashing power."

4 | SYSTEM MODELS USED IN BIPHRS

In this section, we provide the details of the proposed generic architecture on a BIPHRS. Apart from this, an attack model of BIPHRS is also presented.[4]

4.1 | Proposed generic architecture of BIPHRS

The architecture of BIPHRS is given in Figure 1. In this architecture, assume that there is a patient, who is implanted with some smart healthcare devices, like cardiac pacemaker, etc. Smart healthcare devices monitor the health of the patients and then send the health related data to the nearby personal server(s) in a secure way. The type of data (historical diagnostic data and physiological data), sensors (electrocardiogram (ECG or EKG), electroencephalogram (EEG), electromyography (EMG), galvanic skin response (GSR), photoplethysmography (PPG) etc.), and solutions (physiotherapy, brain stimulations, medicine etc.) of the healthcare domain have been considered.[22] Devices, like personal digital assistant (PDA), can be deployed as a personal server. The personal server then creates the partial blocks from the received healthcare data and then sends them to the associated cloud server via the attached access point. Each partial block contains the personal health records of the patients in the form of certain number of encrypted transactions. All transactions are encrypted with the public key of the personal server. The cloud server then creates a full block from the received partial block and it will be then forwarded to the peer-to-peer cloud server (P2PCS) network for its verification and addition into the blockchain. In the P2PCS network, a leader will be elected from the existing cloud servers. After that, the elected leader will call a consensus process for the verification and addition of the block in the blockchain. In case, if leader gets

21613915, 2022, 4, Downloaded from https://onlinelibrary.wiley.com/doi/10.1002/ett.4421 by University Of Waterloo Dana Porter Library, Wiley Online Library on [20/07/2023]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

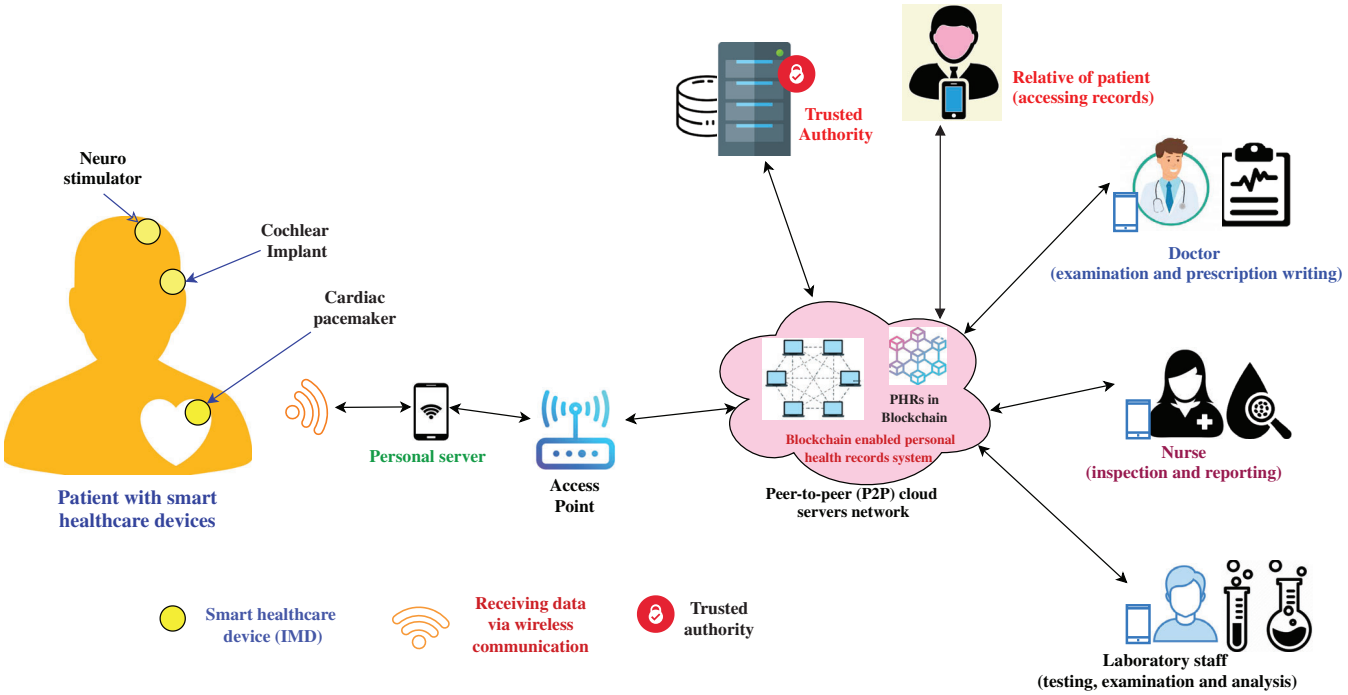

FIGURE 1 Architecture of proposed BIPHRS

the required number of commits from the follower nodes (other cloud servers), then the block will be added into the blockchain. Blockchain is maintained in the form of distributed ledger, which is shared among all miner nodes. When a new block is added into the blockchain, it will be reflected to other miner nodes of the system. The healthcare data is sensitive in nature and it should not be disclosed or modified in any case. Therefore, the blockchain technology is very helpful to achieve the information-security goals. There is a trusted registration authority, which is responsible for the registration of all devices and users of the system. At the same time, there are some users (ie, doctors, nursing staff, laboratory staff), who are interested in accessing the healthcare data of the patients. This data is useful for them in various tasks (ie, writing of prescriptions, medical treatment and procedure, laboratory test analysis and reports). The legitimate and authorized system users can access the data of BIPHRS in a secure way after executing the steps of essential user authentication protocols as specified in References 5, 23, and 24.

The overall flow activities of BIPHRS are described as follows.

- *Registration process*: Registration of devices and users is executed by the trusted registration authority. It uses secret keys, secret numbers and pseudo-identities in the generation of credentials. After that, the credentials will be stored in the memory of the different devices of the system.[4]
- *Authentication and key establishment*: Execution of authentication and key establishment phase happens among the smart healthcare devices (implantable medical devices (IMDs), wearable devices, etc.) and the personal servers, among the personal servers and the cloud servers, and also among the cloud servers and the users. It applies freshly generated timestamps, random secret nonces, and long-term secrets in computation of various transmitted messages as in Reference 4. After the successful completion of mutual authentication between two communicating parties, say χ_i and χ_j, they establish a session key, say SK_{χ_i,χ_j} for their secure communication. Various operations, like concatenation operation ($||$), bitwise *XOR* operation ($\oplus$) and cryptographic one-way hash function ($h(\cdot)$) are used in computation of different exchanged messages. The algorithmic presentation of this phase is given in Algorithm 1. After the completion of all the steps in the algorithm, both parties χ_i and χ_j establish compute the session key $SK_{\chi_i,\chi_j} = SK_{\chi_j,\chi_i}$ and start their secure communication through the session key.
- *Secure data exchange*: Secure data healthcare data transmission takes places among the communicating parties through the computed and established session keys, that is, SK_{χ_i,χ_j}.
- *Blockchain implementation*: It consists of the following steps:
  - *Step-1*: Creation of personal health records (PHRs) at the personal servers is done. Next, all PHRs will be converted into transactions. After that all the transactions will be encrypted using the public key of the personal server.[4]

21613915, 2022, 4, Downloaded from https://onlinelibrary.wiley.com/doi/10.1002/ett.4421 by University Of Waterloo Dana Porter Library, Wiley Online Library on [20/07/2023]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

Algorithm 1. Authentication and session key establishment procedure between parties χ_i and χ_j

Output: Establishment of session key between parties χ_i and χ_j

for entity χ_i and entity χ_j **do**
  χ_i generates a new timestamp τ_{χ_i} and random nonce ρ_{χ_i}
  χ_i calculates authentication request message μ_1 through τ_{χ_i} and ρ_{χ_i}
  χ_i sends the message μ_1 to χ_j via public channel
  At the arrival of μ_1, χ_j performs the verification of received timestamp τ_{χ_i}through condition $\tau_{\chi_i} - \tau^*_{\chi_i} \leq \Delta T$, where $\tau_{\chi_i}$is the actual receiving time of μ_1, $\tau^*_{\chi_i}$ is the time when μ_1 is received and ΔT is the maximum transmission delay
  if verification of τ_{χ_i} is successful **then**
    χ_j calculates random nonce ρ_{χ_i} from received message μ_1
    From calculated and received parameters, χ_j computes μ'_1
    χ_j proceeds to check the originality of μ_1 via the condition: $\mu'_1 = \mu_1$
    if $\mu'_1 = \mu_1$ **then**
      μ_1 is valid and χ_i is authenticated by χ_j
      χ_j generates a new timestamp τ_{χ_j} and random nonce ρ_{χ_j}
      χ_j calculates session key SK_{χ_j,χ_i} by making the use of τ_{χ_i}, τ_{χ_j},ρ_{χ_i}, ρ_{χ_j} and other secrets
      χ_j calculates authentication response message as μ_2 by making the use of SK_{χ_j,χ_i},τ_{χ_i}, τ_{χ_j}, ρ_{χ_i}, and ρ_{χ_j}
      χ_j sends μ_2 to χ_i
    else
      χ_j discontinues the procedure
    end if
  else
    χ_j discontinues the procedure
  end if
  At the arrival of μ_2, χ_i does the verification of received timestamp τ_{χ_j}
  if verification of τ_{χ_j} is successful **then**
    χ_i calculates ρ_{χ_j} from received μ_2
    χ_i calculates session key SK_{χ_i,χ_j}
    χ_i calculates μ'_2 through SK_{χ_i,χ_j}
    χ_i does the verification through the condition: $\mu'_2 = \mu_2$
    if $\mu'_2 = \mu_2$ **then**
      μ_2 is valid and the calculated SK_{χ_i,χ_j} is correct
      χ_j is authenticated by χ_i
      Both χ_i and χ_j establish session key $SK_{\chi_i,\chi_j} = SK_{\chi_j,\chi_i}$
      χ_i and χ_j start their secure communication using the established sessionkey $SK_{\chi_i,\chi_j} = SK_{\chi_j,\chi_i}$
    else
      χ_i discontinues the procedure
    end if
  else
    χ_i discontinues the procedure
  end if
end for

- *Step-2*: Personal servers create partial blocks from the encrypted transactions. Each partial block contains fields, like owner of the block, public key of the block and encrypted transactions. The partial blocks are then sent to the associated cloud server in a secure way through the established session key.[4]
- *Step-3*: Cloud server creates a full block from a received partial block by adding required fields, like the block's ID (number), timestamp value, Merkle tree root, hash of current block, hash of previous block, and digital signature of the block.[4] A typical structure of a block used in the proposed system is given in Figure 2.
- *Step-4*: In the considered P2PCS network, a cloud server will be selected as the leader, for instance, a cloud sever, say CS_L among all active cloud servers in P2PCS network. CS_L will call the consensus procedure for the addition

21613915, 2022, 4, Downloaded from https://onlinelibrary.wiley.com/doi/10.1002/ett.4421 by University Of Waterloo Dana Porter Library, Wiley Online Library on [20/07/2023]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

Block Header	
Block Version	$BVer$
Previous Block Hash	$PBHash$
Merkle Tree Root	MR
Timestamp	TR
Owner of Block	OB
Public Key of Owner	Pub_{CS_j}
Block Payload (Encrypted Transactions)	
Encrypted Transaction #1	$E_{Pub_{CS_j}}(Tx_1)$
Encrypted Transaction #2	$E_{Pub_{CS_j}}(Tx_2)$
⋮	⋮
Encrypted Transaction #n_t	$E_{Pub_{CS_j}}(Tx_{n_t})$
Current Block Hash	$CBHash$
Signature on Block using ECDSA	$BSign$

FIGURE 2 Structure of a block in the proposed BIPHRS

and verification of this particular block. For this purpose, we use the leader selection algorithm, which is given in Reference 25. We again use "ripple protocol consensus algorithm (RPCA)"[26] for the "block verification and its addition into the blockchain" by the help of voting mechanism. When all miner nodes (cloud servers) commit on the addition of this new block then that block will be added into the blockchain. Blockchain is maintained in the form of a distributed ledger, which is accessible to miner nodes.[4] The proposed BIPHRS can maintain various data, like historical diagnostic data and physiological data in the form of encrypted transactions in the various blocks of the implemented blockchain.[22]

- *Secure data delivery to authorized users*: Users (ie, doctors), who are interested in accessing the data of BIPHRS, can get the authorized data after the execution of required steps of authentication mechanism.[4]

The different processes of proposed BIPHRS are also explained in Figure 3.

4.2 | Attack model of BIPHRS

In this section, we discuss about various threats and attacks related to the proposed BIPHRS. For designing the blockchain enabled IoT driven personal health records system, the guidelines of famous Dolev-Yao (DY) model can be used. As per the DY model, the communicating devices and users communicate over an insecure public channel (ie, via the Internet).[5] Therefore, the messages that the entities exchange among them can be eavesdropped, modified, delayed or deleted by an active or a passive adversary residing in the network.[27] Some of the deployed smart healthcare devices can also be physically captured by an adversary $\mathcal{A}$ so that $\mathcal{A}$ may try to obtain secrets information from their memory using the sophisticated power analysis attack.[28] Further, another important threat model, known as the "Canetti-Krawczyk adversary (CK-adversary) model"[29] can also be followed for the designing of blockchain enabled personal health records system. As per the guidelines of CK-adversary model, the attacker $\mathcal{A}$ has all capabilities as like the DY model, along with that he/she can compromise the session sates and session keys, which are established between the communicating entities for their secure communication.

The trusted authority (*TA*) is considered as a full trusted authority of the network as it does the registration of various devices and users of the network. The personal servers and cloud severs, which are involved in the task of blockchain implementation are considered as the semi-trusted entities in the network. It is also assumed that the personal servers are kept inside the physical locking system in order to protect against physical device compromised attack by an adversary.[4]

5 | SECURITY ANALYSIS OF PROPOSED BIPHRS

In this section, we provide the security analysis of our proposed framework (BIPHRS). We show that BIPHRS is able to protect the following types of potential attacks against a passive or an active adversary.

21613915, 2022, 4, Downloaded from https://onlinelibrary.wiley.com/doi/10.1002/ett.4421 by University Of Waterloo Dana Porter Library, Wiley Online Library on [20/07/2023]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

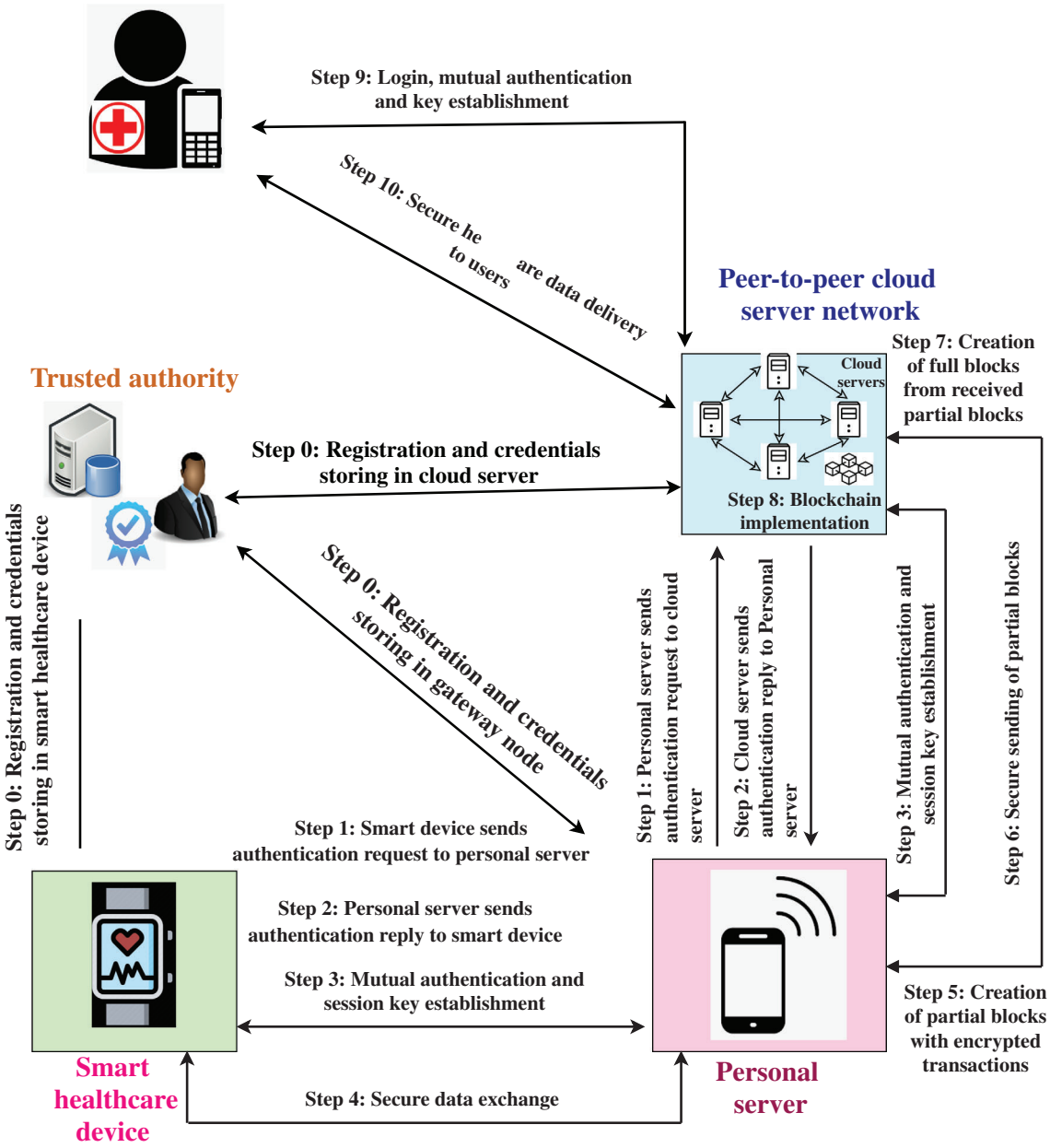

FIGURE 3 Execution of different processes of the proposed BIPHRS

5.1 | Replay attack

In the proposed BIPHRS, the freshly generated timestamps and random nonces are applied in the construction of the exchanged messages. The timestamp values are verified at the receiver's side when the messages are received. If the verification passes successfully, the messages are considered as fresh one. Otherwise, the messages are treated as the replayed messages. With the deployment of such timestamp mechanism, BIPHRS is able to prevent the replay attack.

5.2 | Man-in-the-middle and impersonation attacks

In BIPHRS, the freshly generated random secret values and secret keys are used in various transmitted messages. The secrets keys are only known to the legitimate parties. Thus, only the legitimate parties can produce the original messages as they only know the secret values. Therefore, an adversary $\mathcal{A}$ will not be able to compute the messages on behalf of

21613915, 2022, 4, Downloaded from https://onlinelibrary.wiley.com/doi/10.1002/ett.4421 by University Of Waterloo Dana Porter Library, Wiley Online Library on [20/07/2023]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

the genuine parties. In addition, $\mathcal{A}$ cannot update the content of the exchanged messages in the absence of secret values. Hence, BIPHRS can prevent both MiTM and impersonation attacks.

Remark 1. To resist both the replay and MiTM attacks, we can adopt the following strategy.[30] A communicating entity χ_i needs to store the calculated random nonce ρ_{χ_j} along with the identity of χ_j in its database. Similarly, other communicating entity $\chi_i = j$ needs to store the calculated random nonce ρ_{χ_j} along with the identity of χ_i in its database. Whenever χ_j receives a message from χ_i for subsequent sessions, it checks the database for an occurrence of ρ_{χ_i} against the identity of χ_i. If there is a match, it is assured that the sent message is an old one. In a similar way, once χ_i receives a message from χ_j for subsequent sessions, it checks the database for an occurrence of ρ_{χ_j} against the identity of χ_j. If there is a match, it is also assured that the sent message is a replayed one. As a result, if we use the combination of both current timestamps and random nonces, the replay and MiTM attacks can be prevented efficiently.

5.3 | Ephemeral Secret Leakage attack

The proposed BIPHRS considers that the construction of the session keys should rely on both the "short-term secrets (such as random nonces)" and "long-term secrets (such as secret keys and identities)." For each session, a new session key needs to be established among the communicating parties. An adversary $\mathcal{A}$ will not be able to calculate the established session key in the absence of "long term secrets" if only the short term secrets are available to the adversary $\mathcal{A}$ through a session hijacking attack. This means that BIPHRS is able to prevent the unwanted session key computation attack under the present de facto CK-adversary model.[29] As a result, Ephemeral Secret Leakage (ESL) attack is resisted in the proposed BIPHRS.

5.4 | Privileged insider attack

In BIPHRS, none of the secret credentials is not available to the privileged-insider users of the trusted authority as there is a deployed technique to delete the secret registration credentials from the memory of the trusted authority once the registration process is complete. An insider user with the malicious intention of the trusted authority cannot then launch other associated attacks, like impersonation attack, secret credential guessing attack, and unauthorized session key enumeration attack on the proposed BIPHRS. Thus, BIPHRS is also secured against a privileged-insider attack.

5.5 | Physical smart healthcare device capture attack

In BIPHRS, there is no provision to store any secret information in the plaintext format in the memory of the smart healthcare devices. Now, if an adversary $\mathcal{A}$ can physically acquire some smart healthcare devices, he/she can extract the "secret credentials" from its memory with the execution of sophisticated power analysis attacks.[28] Under such a situation, $\mathcal{A}$ cannot mount a malicious activity because the credentials stored in other non-compromised devices are completely distinct. As a result, physical compromise of some healthcare devices does not have any effect on the secure communication happen between non-compromised devices and other communicating entities in the network. This suggests that BIPHRS is secured against physical smart healthcare device capture attack.

5.6 | Stolen verifier attack

In BIPHRS, all sensitive credentials need to be stored in a secure region of database of the cloud servers. Additionally, it is assumed that the personal servers are deployed under physical locking system in order to prevent their physical stealing as it was the case in Reference 31. Thus, the secret values are not available to an adversary $\mathcal{A}$ to launch further attacks, like "impersonation, MITM, session key computation" attacks. This means that the proposed BIPHRS is secured against the stolen verifier attack.

21613915, 2022, 4, Downloaded from https://onlinelibrary.wiley.com/doi/10.1002/ett.4421 by University Of Waterloo Dana Porter Library, Wiley Online Library on [20/07/2023]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

5.7 | 51% attack and selfish mining

A blockchain-based system is vulnerable to other kinds of attacks, like "51% attack" and "selfish mining." These attacks may occur when an adversary $\mathcal{A}$ has a high "hashing power".[32] Specially, 51% attack demands that the adversary $\mathcal{A}$ requires to possess more than "half of the hashing power." Although, the 51% attack is typically mounted in opposition to "cryptocurrencies," where $\mathcal{A}$ executes some malicious task, like "double-spending," such type of attack is also theoretically possible in other consensus mechanism, such as proof-of-stake (PoS). On the other side, a selfish mining is considered as another "well-known vulnerability used by the miners to steal the block rewards." Thus, the consensus algorithms "proof-of-work (PoW)" or "proof-of-stake (PoS)" is vulnerable to 51% attack, which is not recommended to be used in the proposed BIPHRS. Hence, the proposed BIPHRS may use the "practical byzantine fault tolerance (PBFT)" consensus algorithm[33] in order to prevent 51% and selfish mining attacks.

6 | REVIEW OF BLOCKCHAIN ENABLED SECURITY SOLUTIONS FOR PERSONAL HEALTH RECORDS SYSTEM

Authentication, key management, and access control are treated as two primary security services that are applied in various applications.[34-37]

In this section, we discuss various security schemes, which are applicable for blockchain enabled personal health records system (BIPHRS). After that, we provide the comparison of their security and functionality features. The comparative study is useful to identify which scheme provides a better security and provides extra functionality features.

6.1 | Review of Liu et al's scheme

Liu et al[1] proposed a hierarchical comparison based encryption (HCBE) scheme for cloud-based personal health record systems. Some of the features of Liu et al's scheme[1] are given below:

- The HCBE scheme was proposed, which was built on an attribute hierarchy and it utilized positive negative depth first (PNDF) coding for the improvement of encryption performance of comparison based encryption (CBE) scheme.
- Next, they implemented a dynamic policy updating (DPU) scheme to delegate updation of policy operations at the cloud.
- They also analyzed the performance and the security of their schemes, and also conducted experiments for the validation the efficiency and effectiveness of the proposed schemes.

6.2 | Review of Garg et al's scheme

Garg et al[4] came up with a "blockchain enabled authenticated key management scheme" for the IoMT deployment also applicable for PHRs. Brief summary of Garg et al's scheme[4] is given below:

- They have considered private blockchain for the designing of their scheme.
- The fast "one-way cryptographic hash function" and "bitwise XOR operations" were utilized in the designing.
- Their scheme had phases, like "pre-deployment phase, key management phase, user registration phase, authentication and key agreement phase, password and biometric update phase, dynamic device addition phase and blockchain construction and addition phase."
- They have also provided the formal security verification of their scheme via AVISPA (Automated Validation of Internet Security Protocols and Applications) tool to prove its resilience against replay and MiTM attacks. Apart from that informal security analysis was provided to prove its security against the various potential attacks.
- During the performance comparisons, it had been observed that their scheme provided high security along with extra functionality features. It also required low communication and computational costs as compared to the other existing techniques.

21613915, 2022, 4, Downloaded from https://onlinelibrary.wiley.com/doi/10.1002/ett.4421 by University Of Waterloo Dana Porter Library, Wiley Online Library on [20/07/2023]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

- They have was also provided the implementation to estimate its impact on the performance parameters, that is, on transactions per second, and computation time.

6.3 | Review of Saha et al's scheme

Saha et al[38] proposed a "blockchain based access control protocol for IoT-enabled healthcare," which can be utilized for PHRs. Brief summary of Saha et al scheme[38] is given below:

- A method for the access control through the inclusion of private blockchain was proposed.
- Their scheme was useful for the trusted group of hospitals for the maintaining and secure exchange of PHRs.
- "ECC-based signature mechanism" was used in their scheme. The security of their scheme depended on solving the "elliptic curve discrete logarithm problem (ECDLP)" and "collision-resistant one-way hash function."
- Their scheme had phases, like "registration/enrollment phase, login and access control phase and blockchain formation phase."
- Their scheme was secured against active attacks like, "replay attack," "MiTM," "impersonation attacks" and "Ephemeral Secret Leakage (ESL) attack."

6.4 | Review of Xiang et al's scheme

Later on Xiang et al[39] proposed another "permissioned blockchain enabled identity management and user authentication scheme" applicable in healthcare for the maintaining of PHRs. Typical characteristics of Xiang et al's scheme[39] are given below:

- A "permissioned blockchain enabled identity management and user authentication scheme" for the maintaining of PHRs was provided.
- It had important phases, like "installation phase, enrolment phase, login phase, authentication and key agreement phase, password update phase." However, some of the essential phases like, "dynamic device addition, key revocation" were not there in their scheme.
- A comprehensive security analysis was also provided to prove its security against the different potential attacks.

6.5 | Review of Xu et al's scheme

Xu et al[40] proposed a "blockchain enabled smart healthcare system (healthchain) for large-scale health data privacy." Their proposed scheme is also applicable for PHRs. Typical characteristics of Xu et al's scheme[40] are given below:

- They proposed a "blockchain enabled smart healthcare system (healthchain)" for the secure storage and exchange of PHRs.
- In their scheme, the users had facility to upload health related data and could read doctors' diagnoses.
- The given model separated the transactions for the publication of the data from all available transactions, which was performed to achieve the access control. PHRs can be encrypted and stored in "interplanetary file system (IPFS)."
- The proposed scheme did the reduction in the communication and computation costs and preserved the privacy.
- There was also the key revocation facility through which the keys of different parties, that is, doctor might be revoked.

6.6 | Review of Aujla and Jindal's scheme

Furthermore, Aujla and Jindal[41] proposed a blockchain enabled scheme for the security of healthcare data (ie, PHRs). Some of the important features of Aujla and Jindal's scheme[41] are given below:

21613915, 2022, 4, Downloaded from https://onlinelibrary.wiley.com/doi/10.1002/ett.4421 by University Of Waterloo Dana Porter Library, Wiley Online Library on [20/07/2023]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

- A method for the secure exchange of health data to the cloud servers via edge devices was proposed.
- The mechanism of blockchain was used for the data security and also to preserve the privacy of healthcare data (ie, PHRs).
- A "tensor train decomposition model" was given for the storage of health data over the cloud servers for the prevention of duplication of data.
- Their scheme contained phases like, "registration, block creation along with validation, data generation, and block updates."

6.7 | Review of Islam and Shin's scheme[42]

Islam and Shin[42] proposed a "blockchain enabled scheme for the security of healthcare data. Some of the important features of Islam and Shin's scheme[42] are given below:

- A blockchain based system model for the secure healthcare data collection and exchange via unmanned aerial vehicles (UAVs) was presented.
- A "2-phase authentication mechanism" was presented in their scheme. A threat model to cover the various threats and attacks of such kind of communication environment was also provided.
- The security analysis was also conducted to prove its security against various possible attacks.
- It contained important phases like, "device registration phase, body sensor hive synchronization phase, data acquisition phase and data storage phase."
- A "consortium blockchain" was implemented via Ethereum platform. The network performance parameters for example, throughput, latency, and block size were calculated and analyzed.

7 | COMPARATIVE ANALYSIS

A comparative study on blockchain enabled security schemes for personal health records system has been conducted in this section.

7.1 | Comparative study on security and functionality attributes

In this section, we compared the performance of our proposed generalized framework (BIPHRS), and the schemes of Liu et al,[1] Garg et al,[4] Saha et al,[38] Xiang et al,[39] Xu et al,[40] Aujla and Jindal,[41] and Islam and Shin.[42] The details of comparative study are given in Table 1. During the comparative study, we consider the following important security and functionality features (*SFF*):

- SFF_1: "mutual authentication/access control"
- SFF_2: "anonymity property"
- SFF_3: "untraceability property"
- SFF_4: "session-key agreement"
- SFF_5: "ESL attack under CK adversary model"
- SFF_6: "data confidentiality"
- SFF_7: "data integrity"
- SFF_8: "strong replay attack"
- SFF_9: "man-in-the-middle attack"
- SFF_{10}: "dynamic controller node (personal server) addition phase"
- SFF_{11}: "dynamic smart healthcare device addition"

21613915, 2022, 4, Downloaded from https://onlinelibrary.wiley.com/doi/10.1002/ett.4421 by University Of Waterloo Dana Porter Library, Wiley Online Library on [20/07/2023]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

TABLE 1 Comparison of security and functionality features

Feature	Liu et al[1]	Garg et al[4]	Saha et al[38]	Xiang et al[39]	Xu et al[40]	Aujla and Jindal[41]	Islam and Shin[42]	Proposed BIPHRS
SFF_1	✓	✓	✓	✓	✓	✓	✓	✓
SFF_2	✓	✓	✓	✓	✓	✓	✓	✓
SFF_3	✓	✓	✓	✓	✓	✓	✓	✓
SFF_4	×	✓	✓	✓	×	✓	×	✓
SFF_5	×	✓	✓	×	×	×	×	✓
SFF_6	✓	✓	✓	✓	✓	✓	✓	✓
SFF_7	✓	✓	✓	✓	✓	✓	✓	✓
SFF_8	✓	✓	✓	✓	✓	✓	✓	✓
SFF_9	✓	✓	✓	✓	✓	✓	✓	✓
SFF_{10}	×	✓	×	×	×	×	×	✓
SFF_{11}	×	✓	×	×	×	×	×	✓
SFF_{12}	NA	✓	NA	✓	NA	NA	NA	✓
SFF_{13}	✓	✓	✓	✓	✓	✓	✓	✓
SFF_{14}	×	✓	×	✓	✓	✓	✓	✓
SFF_{15}	×	✓	✓	✓	✓	✓	✓	✓
SFF_{16}	✓	×	×	×	×	×	×	✓

Note: ×, a scheme is insecure against a particular attack or it does not support a specific feature; ✓, a scheme is secured against a particular attack or it supports a specific feature; NA, not applicable in a scheme.

- SFF_{12}: "stolen mobile device attack"
- SFF_{13}: "impersonation attacks"
- SFF_{14}: "practical implementation for blockchain"
- SFF_{15}: "blockchain-enabled security"
- SFF_{16}: "suitable for PHR communication environment"

From Table 1, it is clear that the schemes proposed by Liu et al,[1] Xiang et al,[39] Xu et al,[40] Aujla and Jindal,[41] and Islam and Shin[42] do not provide some required security and functionality features, like "session-key agreement," "ESL attack under the CK-adversary model," "availability of password update phase," "availability of biometric update phase," "availability of dynamic controller node (personal server) addition phase," and "availability of dynamic smart healthcare device addition." However, the proposed BIPHRS and Garg et al's scheme[4] achieve most of the required "security and functionality features." Moreover, the scheme of Garg et al[4] is for general-purpose IoMT uses. Nevertheless, BIPHRS sounds suitable for a secure exchange and storage of PHRs in the blockchain enabled personal health records system. The feature SFF_{15} allows the proposed BIPHRS to be more secure due to the inherent blockchain properties, like immutability and decentralization.

7.2 | Comparative study on communication costs

In this section, we compare the performance of our generalized framework with the existing Garg et al's scheme,[4] Saha et al's scheme,[38] and Xiang et al's scheme.[39] In order to do so, it is assumed that an identity is 160 bits, a random nonce is 160 bits, a timestamp is 32 bits, a hash output using SHA-256 hash algorithm is 256 bits, and an "elliptic curve point of the form: $P = (P_x, P_y)$" is $(160 + 160) = 320$ bits, assuming that "an 160-bit elliptic curve cryptography (ECC) provides the equivalent security level as that for an 1024-bit RSA public key cryptosystem".[43] A comparative analysis among the proposed generalized BIPHRS and other schemes is provided in Table 2. It is worth to note that the proposed BIPHRS needs less communication cost as compared to other schemes.

21613915, 2022, 4, Downloaded from https://onlinelibrary.wiley.com/doi/10.1002/ett.4421 by University Of Waterloo Dana Porter Library, Wiley Online Library on [20/07/2023]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

TABLE 2 Comparative study on communication costs among various schemes

Scheme	No. of messages	Total cost (in bits)
Proposed BIPHRS	2	1088
Garg et al[4]	3	1376
Saha et al[38]	2	1472
Xiang et al[39]	3	2272

TABLE 3 Approximate time needed for different cryptographic primitives[44]

Notation	Description (time to compute)	Rough computation time (in seconds)
T_h	One-way cryptographic hash function	0.00032
T_{ecm}	Elliptic curve point (scalar) multiplication	0.0171
T_{eca}	Elliptic curve point addition	0.0044
T_{fe}	Fuzzy extractor function for biometric verification	0.0171

TABLE 4 Comparative study on computational costs among various schemes

Scheme	Computation cost	Rough time needed (in milliseconds)
Proposed BIPHRS	$8T_h$	2.56
Garg et al[4]	$19T_h + T_{fe}$	21.18
Saha et al[38]	$T_{fe} + 3T_{ecm} + T_{eca} + 16T_h$	77.92
Xiang et al[39]	$5T_h + 3T_{ecm}$	52.90

7.3 | Comparative study on computational costs

In this section, we also compare the performance of our generalized framework with the existing Garg et al's scheme,[4] Saha et al's scheme,[38] and Xiang et al's scheme.[39] Table 3 shows the list of various notations used for cryptographic primitives and their approximate time (in seconds) needed, which are based on the results mentioned in Reference 44. The time required for a fuzzy extractor function for biometric verification, T_{fe} is taken approximately as that for an ECC point (scalar) multiplication, T_{ecm}.

Based on the reported results in Table 3, we have calculated the total computational costs in milliseconds required for the proposed generalized framework and the existing Garg et al's scheme,[4] Saha et al's scheme,[38] and Xiang et al's scheme.[39] The results are then displayed in Table 4. It is worth to note that the proposed BIPHRS needs less computation cost as compared to other schemes.

8 | PRACTICAL IMPLEMENTATION

In this section, we provide the details of practical implementation of the proposed BIPHRS. The details of different parameters utilized in the simulation of BIPHRS are given in Table 5. During the simulation study, we have considered three different cases: Case-1, Case-2, and Case-3. The platform "Windows 10 64-bit OS with Intel (R) core i5-8250U, 1.60 to 1.80 GHz processor" was selected to perform the experiments. We deployed "eclipse IDE 2019-12 with Java language" programming environment for the programming part. During the experiments, we have taken 40 (in Case-1), 80 (in Case-2), and 120 (in Case-3) smart healthcare devices. Again, we have considered 4 (in Case-1), 8 (in Case-2), and 12 (in Case-3) personal servers. The total number of mined blocks are 5 (for Case-1), 10 (for Case-2), and 15 (for Case-3). Additionally, we have used the sample data of various sensors, like ECG sensor and "Infrared IR Temperature Sensor".[22] A personal server creates encrypted transactions from the received health related data. In each block, 100 encrypted transactions

21613915, 2022, 4, Downloaded from https://onlinelibrary.wiley.com/doi/10.1002/ett.4421 by University Of Waterloo Dana Porter Library, Wiley Online Library on [20/07/2023]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

TABLE 5 Parameters used in simulation

Parameter	Value
Platform used	Windows 10 64-bit OS
Processor	Intel (R) core (TM), i5-8250U, 1.60 to 1.80 GHz
Size of random-access memory (RAM)	8 GB
Programming environment deployed	Eclipse IDE 2019-12 with Java
Taken cases	Case-1, Case-2, Case-3
Number of smart healthcare devices	40 (for Case-1), 80 (for Case-2), 120 (for Case-3)
Number of personal servers	4 (for Case-1), 8 (for Case-2), 12 (for Case-3)
Considered cloud servers (miner nodes)	4 for all cases

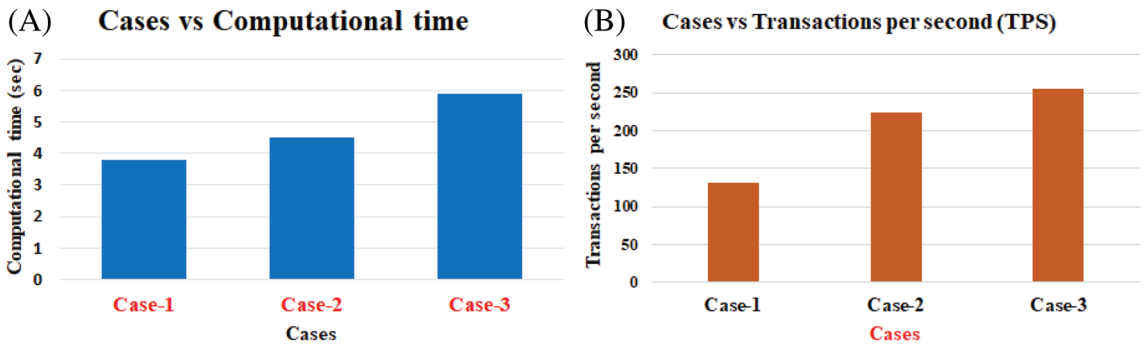

FIGURE 4 (A) Effect on computational time (seconds) and (B) effect on transactions per second (TPS)

are considered. Furthermore, four miner nodes (cloud servers) were taken for all cases. A "voting mechanism" was used in the "blockchain mining process." The selected miner node can add a block in the blockchain, if it is agreed by other authorized miner nodes in the system.

In the following, we discuss the following results in the simulation study.

8.1 | Effect on computational time

It is desirable to monitor the effect of increasing number of smart healthcare devices and personal servers on the performance of the proposed framework. It is estimated as the computation time (in seconds) for all considered cases. The computation time for Case-1, Case-2, and Case-3 are 3.79, 4.49, and 5.89 seconds, respectively. The obtained results are depicted in Figure 4. It is essential to say that "computation cost" increases with the increasing number of smart healthcare devices and personal servers (eg, from Case-1 to Case-2 and Case-2 to Case-3). This happens because an increasing number of smart healthcare devices and personal servers causes "creation and addition" of more number of blocks in the blockchain.

8.2 | Effect on transactions per second

The effect on "transactions per second (TPS)" as per the considered cases is also computed. The obtained values of TPS for Case-1, Case-2, and Case-3 are 132, 223, and 255, respectively. The obtained results are depicted in Figure 4. It is essential to say that the TPS increases as the blockchain enlarges with more number of number of smart healthcare devices and personal servers (for instance, from Case-1 to Case-2 and Case-2 to Case-3). This also occurs because an increasing number of smart healthcare devices and personal servers leads to the "creation and addition" of more number of blocks in the blockchain.

21613915, 2022, 4, Downloaded from https://onlinelibrary.wiley.com/doi/10.1002/ett.4421 by University Of Waterloo Dana Porter Library, Wiley Online Library on [20/07/2023]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

9 | CONCLUSION AND FUTURE WORKS

Blockchain technology is very helpful for secure exchange and storage of PHRs. The healthcare system is operated through various frameworks (eg, wireless body area network and telecare medical information system) that require to maintain PHRs. Therefore, there is a need to process and store PHRs in a secure way. We proposed a generalized BIPHRS. The security analysis of the proposed BIPHRS proves its security against various possible attacks. A comparative study among the state of art blockchain enabled security schemes for PHRs system and the proposed BIPHRS reveals that BIPHRS requires less communication and computation costs and provides a better security and extra functionality features as compared to the other similar schemes. The practical demonstration of BIPHRS using blockchain simulation provides its effect on different performance parameters.

Some open problems and challenges related to the proposed BIPHRS are worth to be addressed in the coming future. In the proposed BIPHRS, there is a requirement of execution of various authentication mechanisms, which are required for the mutual authentication and key establishment among the various entities. Most of the time, authentication techniques are presented with a full proof security. However, some of them are not fully secured and may be vulnerable to different potential attacks. Hence, the security protocols should be designed in such a way that they should be robust against potential attacks. The proposed BIPHRS makes use of combination of various technologies related to information security, IoT and blockchain. This also operates through various types of cryptographic algorithms (ie, IoT communication algorithms, encryption/decryption, digital signature, and consensus algorithms). Under these circumstances, we may have issues related to interoperability of tools, technologies and devices. In addition, exploring the lattice-based cryptosystem for healthcare applications[45] in the proposed BIPHRS will be another interesting future research work.

ACKNOWLEDGMENTS

The authors would like to thank the anonymous reviewers and the associate editor for their valuable suggestions, which helped us to improve the presentation and technical quality of this article. This research was supported in part by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education under Grant 2020R1I1A3058605, and in part by the BK21 FOUR Project funded by the Ministry of Education, Korea under Grant 4199990113966.

CONFLICT OF INTEREST

The authors declare no potential conflict of interest.

NOMENCLATURE

$\mathcal{A}$	an adversary
TA	trusted authority
Communicating party	smart healthcare device, personal server, cloud server or user
χ_i	ith communicating party
χ_j	jth communicating party
CS_l	lth cloud server
G	a base point on a non-singular elliptic curve cryptography (ECC)
$k.G$	$G + G + \cdots + G$ (k times), elliptic curve point (scalar) multiplication
Pri_x	ECC-based private key of party x
Pub_x	ECC-based public key of party x, where $Pub_x = Pri_x.G$
τ_{χ_i} and τ_{χ_j}	timestamp values of χ_i and χ_j, respectively
ρ_{χ_i} and ρ_{χ_j}	random nonce values of χ_i and χ_j, respectively
$h(\cdot)$	cryptographic one-way hash function
SK_{χ_i,χ_j}	session key between χ_i and χ_j
$\|\|$	concatenation operation
$\oplus$	bitwise *XOR* operation

DATA AVAILABILITY STATEMENT

Data sharing is not applicable to this article as no datasets were generated or analyzed during the current study.

21613915, 2022, 4, Downloaded from https://onlinelibrary.wiley.com/doi/10.1002/ett.4421 by University Of Waterloo Dana Porter Library, Wiley Online Library on [20/07/2023]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

REFERENCES

1. Liu X, Liu Q, Peng T, Wu J. Dynamic access policy in cloud-based personal health record (PHR) systems. *Inf Sci*. 2017;379:62-81.
2. payeum, Blockchain. Accessed June 2021. https://payeum.com/payeum-crypto-payments-blockchain.html/
3. Lastovetska A. Blockchain architecture basics: components, structure, benefits & creation. Accessed June 2021. https://mlsdev.com/blog/156-how-to-build-your-own-blockchain-architecture/
4. Garg N, Wazid M, Das AK, Singh DP, Rodrigues JJPC, Park Y. BAKMP-IoMT: design of blockchain enabled authenticated key management protocol for internet of medical things deployment. *IEEE Access*. 2020;8:95956-95977. doi:10.1109/ACCESS.2020.2995917
5. Wazid M, Das AK, Rodrigues JJPC, Shetty S, Park Y. IoMT malware detection approaches: analysis and research challenges. *IEEE Access*. 2019;7:182459-182476.
6. Iredale G. List of top blockchain features; 2002. Accessed October 2021. https://101blockchains.com/introduction-to-blockchain-features/
7. Hussain AA, Al-Turjman F. Artificial intelligence and blockchain: a review. *Transa Emerg Telecommun Technol*. 2021;32(9):e4268. doi:10.1002/ett.4268
8. Asif-Ur-Rahman M, Afsana F, Mahmud M, et al. Toward a heterogeneous mist, fog, and cloud-based framework for the internet of healthcare things. *IEEE Internet Things J*. 2019;6(3):4049-4062.
9. Chowdhury R. IoT in Healthcare: 20 examples that'll make you feel better. Accessed March 2020. https://www.ubuntupit.com/iot-in-healthcare-20-examples-thatll-make-you-feel-better/
10. Habibzadeh H, Dinesh K, Rajabi Shishvan O, Boggio-Dandry A, Sharma G, Soyata T. A survey of healthcare Internet of Things (HIoT): a clinical perspective. *IEEE Internet Things J*. 2020;7(1):53-71.
11. Nasrullah P. Internet of things in healthcare: applications, benefits, and challenges. Accessed March 2020. https://www.peerbits.com/blog/internet-of-things-healthcare-applications-benefits-and-challenges.html
12. Wazid M, Bera B, Mitra A, Das AK, Ali R. Private blockchain-envisioned security framework for AI-enabled IoT-based drone-aided healthcare services. DroneCom '20: Proceedings of the 2nd ACM MobiCom Workshop on Drone Assisted Wireless Communications for 5G and Beyond; September 25, 2020:37-42; ACM, London, UK.
13. Wazid M, Zeadally S, Das AK, Odelu V. Analysis of security protocols for mobile healthcare. *J Med Syst*. 2016;40(11):1-10.
14. Wazid M, Das AK, Khan MK, Al-Ghaiheb AA, Kumar N, Vasilakos AV. Secure authentication scheme for medicine anti-counterfeiting system in IoT environment. *IEEE Internet Things J*. 2017;4(5):1634-1646.
15. Wazid M, Das AK, Kumar N, Conti M, Vasilakos AV. A novel authentication and key agreement scheme for implantable medical devices deployment. *IEEE J Biomed Health Inform*. 2018;22(4):1299-1309.
16. Yang X, Li X, Li T, Wang X, Wang C, Li B. Efficient and anonymous multi-message and multi-receiver electronic health records sharing scheme without secure channel based on blockchain. *Trans Emerg Telecommun Technol*. 2021;e4371. doi:10.1002/ett.4371
17. Li C, Shih D, Wang C, Chen C, Lee C. A blockchain based data aggregation and group authentication scheme for electronic medical system. *IEEE Access*. 2020;8:173904-173917.
18. Kumari S, Chaudhary P, Chen C, Khan MK. Questioning key compromise attack on Ostad-Sharif et al.s authentication and session key generation scheme for healthcare applications. *IEEE Access*. 2019;7:39717-39720.
19. Li C, Lee C, Weng C, Chen S. A secure dynamic identity and chaotic maps based user authentication and key agreement scheme for e-healthcare systems. *J Med Syst*. 2016;40(11):233:1-233:10.
20. What is spyware? and how to remove it; 2020. Accessed March 2020. https://us.norton.com/internetsecurity-how-to-catch-spyware-before-it-snags-you.html.
21. Fruhlinger J. Ransomware explained: how it works and how to remove it; 2018. Accessed March 2020. https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html.
22. Park SJ, Hong S, Kim D, Seo Y, Hussain I. Knowledge based health monitoring during driving. In: Stephanidis C, ed. *HCI International 2018 – Posters' Extended Abstracts*. Las Vegas, Nevada: Springer International Publishing; 2018:387-392.
23. Shi S, He D, Li L, Kumar N, Khan MK, Choo KR. Applications of blockchain in ensuring the security and privacy of electronic health record systems: a survey. *Comput Secur (Elsevier)*. 2020;97:101966.
24. Shamshad S, Minahil MK, Kumari S, Chen CM. A secure blockchain-based e-health records storage and sharing scheme. *J Inf Secur Appl*. 2020;55:102590.
25. Zhang H, Wang J, Ding Y. Blockchain-based decentralized and secure keyless signature scheme for smart grid. *Energy*. 2019;180:955-967.
26. Wang X, Zeng P, Patterson N, Jiang F, Doss R. An improved authentication scheme for internet of vehicles based on blockchain technology. *IEEE Access*. 2019;7:45061-45072.
27. Dolev D, Yao AC. On the security of public key protocols. *IEEE Trans Inf Theory*. 1983;29(2):198-208.
28. Messerges TS, Dabbish EA, Sloan RH. Examining smart-card security under the threat of power analysis attacks. *IEEE Trans Comput*. 2002;51(5):541-552.
29. Canetti R, Krawczyk H. Analysis of key-exchange protocols and their use for building secure channels. Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques – Advances in Cryptology (EUROCRYPT'01) Innsbruck (Tyrol); 2001:453-474; Springer, Austria.
30. Das AK. Analysis and improvement on an efficient biometric-based remote user authentication scheme using smart cards. *IET Inf Secur*. 2011;5(3):145-151.
31. Wazid M, Das AK, Odelu V, Kumar N, Susilo W. Secure remote user authenticated key establishment protocol for smart home environment. *IEEE Trans Depend Secure Comput*. 2020;17(2):391-406.
32. Sayeed S, Marco-Gisbert H. Assessing blockchain consensus and security mechanisms against the 51% attack. *Appl Sci*. 2019;9(9):1788.

21613915, 2022, 4, Downloaded from https://onlinelibrary.wiley.com/doi/10.1002/ett.4421 by University Of Waterloo Dana Porter Library, Wiley Online Library on [20/07/2023]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

33. Castro M, Liskov B. Practical byzantine fault tolerance and proactive recovery. *ACM Trans Comput Syst*. 2002;20(4):398-461.
34. Odelu V, Das AK, Goswami A. SEAP: secure and efficient authentication protocol for NFC applications using pseudonyms. *IEEE Trans Consum Electron*. 2016;62(1):30-38.
35. Mishra D, Das AK, Mukhopadhyay S. A secure and efficient ECC-based user anonymity-preserving session initiation authentication protocol using smart card. *Peer-to-Peer Netw Appl*. 2016;9(1):171-192.
36. Das AK. A random key establishment scheme for multi-phase deployment in large-scale distributed sensor networks. *Int J Inf Secur*. 2012;11(3):189-211.
37. Zhang Y, He D, Obaidat MS, Vijayakumar P, Hsiao KF. Efficient identity-based distributed decryption scheme for electronic personal health record sharing system. *IEEE J Select Areas Commun*. 2021;39(2):384-395.
38. Saha S, Sutrala AK, Das AK, Kumar N, Rodrigues JJPC. On the design of blockchain-based access control protocol for iot-enabled healthcare applications. Proceedings of the ICC 2020 - 2020 IEEE International Conference on Communications (ICC); 2020:1-6; Dublin, Ireland.
39. Xiang X, Wang M, Fan W. A permissioned blockchain-based identity management and user authentication scheme for E-health systems. *IEEE Access*. 2020;8:171771-171783.
40. Xu J, Xue K, Li S, et al. Healthchain: a blockchain-based privacy preserving scheme for large-scale health data. *IEEE Internet Things J*. 2019;6(5):8770-8781.
41. Aujla GS, Jindal A. A decoupled blockchain approach for edge-envisioned iot-based healthcare monitoring. *IEEE J Select Areas Commun*. 2021;39(2):491-499.
42. Islam A, Shin SY. A blockchain-based secure healthcare scheme with the assistance of unmanned aerial vehicle in Internet of Things. *Comput Electr Eng*. 2020;84:106627.
43. Jansma N, Arrendondo B. Performance comparison of elliptic curve and RSA digital signatures. Accessed May 2021. http://nicj.net/files/performance_comparison_of_elliptic_curve_and_rsa_digital_signatures.pdf
44. He D, Kumar N, Lee J, Sherratt RS. Enhanced three-factor security protocol for consumer USB mass storage devices. *IEEE Trans Consum Electron*. 2014;60(1):30-37.
45. Chaudhary R, Jindal A, Aujla GS, Kumar N, Das AK, Saxena N. LSCSH: lattice-based secure cryptosystem for smart healthcare in smart cities environment. *IEEE Commun Mag*. 2018;56(4):24-32.

How to cite this article: Wazid M, Das AK, Park Y. Blockchain-enabled secure communication mechanism for IoT-driven personal health records. *Trans Emerging Tel Tech*. 2022;33(4):e4421. doi: 10.1002/ett.4421

21613915, 2022, 4, Downloaded from https://onlinelibrary.wiley.com/doi/10.1002/ett.4421 by University Of Waterloo Dana Porter Library, Wiley Online Library on [20/07/2023]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License