Int. j. inf. tecnol. (January 2024) 16(1):417–424
https://doi.org/10.1007/s41870-023-01588-x

ORIGINAL RESEARCH

Attack resistant blockchain-based healthcare record system using modified RSA Algorithm

Arushi Srivastava[1] · **Juhi Gupta**[1]

Received: 30 June 2023 / Accepted: 29 September 2023 / Published online: 6 November 2023

Abstract Electronic Health Records (EHRs) are steadily becoming the central information system for the healthcare industry. EHRs are not completely secure and highly vulnerable to the malicious attacks. Blockchain provides an encouraging solution to this problem and with cryptographic algorithms, there is end-to-end encryption and digital signature on the complete architecture of the transactions involved in every healthcare organization. The proposed model provides an immutable and unforgeable transaction record to patients and healthcare institutions to transmit secured data across the cloud server layer. A private and safe environment is created to store physiological data using distributed ledger system using the proposed modified logarithmic-based Rivest-Shamir-Adleman (RSA) algorithm. The performance of the considered system based on defence efficiency and time to decrypt the ciphertext is evaluated. A significant improvement in the parameters is observed to increase by 38.8% as compared to traditional EHR models using RSA algorithm. In addition, the modified RSA algorithm is tested to provide high security levels, thereby making it more robust against two factorization attacks- ciphertext attack and Fermat's factorization attack with an increased security level.

Keywords Blockchain · Cryptography · Encryption · RSA Algorithm · Attacks

✉ Juhi Gupta
singla.juhi@gmail.com

[1] Jaypee Institute of Information Technology, Noida, Uttar Pradesh, India

1 Introduction

Electronic Health Records (EHRs) deliver a suitable health record and medical data storage service that promotes previous patient medical archives on paper to be accessible on the cloud, thereby allowing patients to possess secured control of producing, managing, and sharing Electronic Health Records (EHRs) with family, friends, healthcare providers and other treatment facilities [1]. EHR data management, also called Information Island, poses adverse security challenges. To ensure a secure model with reduced transaction time, a profitable and latest solution is Blockchain. It is a decentralized entity-to-entity system in a distributed architecture that assigns its resources to the swarm of nodes, functioning collectively to make decisions on behalf of the authentic network.

The distribution of physiological data can be enhanced through secured and accessible Blockchain [2, 3]. It permits devices across the web to send data to a private network and generate immutable EHRs on a secure platform.

Over the past years, blockchain systems have been providing an optimal solution to industries in transaction ledgers. However, the traditional model using computational bilinear Diffie-Hellman (CBDH) does not secure the health record system from attacks by malicious eavesdroppers or third-party attackers. Blockchain technology has the characteristics of immutability and decentralization which provide a secure public platform by refraining from tampering of patients' physiological data at any particular time.

The usage of cryptography with Blockchain builds the trust of the data as each transaction is recorded, placed into a data block in the transaction ledger and added to a secure immutable chain that cannot be changed and hence provides cost-effective solutions than other ledgers used in public platform [4, 5]. In the healthcare industry, personal EHRs

secure the patients' physiological data in addition to creating parameters such as public and private key that can be registered by the unique digital signatures by the membership service provider (MSP) component of the block chain architecture [6].

In this section, the advanced research contributions related to Blockchain in healthcare and medical industry has been presented. With the advent of Block chain technology, numerous healthcare applications have been implemented in literature for the authenticity and data security [7]. Maji et. al. [8] proposed a model of multi-authority attribute signature scheme that consisted of the cloud storage-based system. The attributes are shared through a centralized issuing authority.

Zheng et. al. [9] discussed the traditional model of EHRs using blockchain that calculated the digital signatures and stored transactions in a digital ledger. A collusion resistance network is presented but shows the trade-off between the time and cost of calculating attributes. Takashima et. al [10] has proposed an agreement-based blockchain healthcare framework to provide enhancement for accessing data amongst healthcare providers using access control policy.

The EHRs are usually stored in repositories of healthcare facilities that are not accessible by the patients [11]. The ABE scheme ensures that the patients are allowed to manage and access their data from attributing authorities without getting the keys issued from healthcare providers each time. Further, the distribution of EHRs in the hospital management system for end-to-end data encryption is the major challenge. However, with the Rivest-Shamir-Adleman (RSA) algorithm, the problem of securing data through encryption gets reduced. A multiple authority ABE scheme by D. Cao [12] implemented a monotone predicate access tree structure, where to resolve the forgery challenge, a data-signing blockchain-based framework is proposed for the storage of patient's information on cloud servers.

Moreover, medical records are susceptible to attacks due to deciphering of the private key of the user's record. In our proposed model, we have used a combination of SHA-256 and a novel logarithmic based RSA algorithm to increase the efficiency of the system against attacks. The proposed model is tested for its robustness against two attacks, namely, ciphertext attack and factorization attack on the RSA algorithm and thereafter by analyzing its efficiency.

However, our proposed blockchain-based model is capable of being implemented on EHR and can store the physiological data of the patient. Further, it reflects all previous records stored in a blockchain encrypted using SHA-256 and the transactions are signed using RSA algorithm to provide security and protection against malicious eavesdroppers and cryptographic attacks. By utilizing only verified users for access to the blockchain, the scheme has strong scalability in the storage of the block, so the dependability of the system gets enhanced. To the best of the authors' knowledge, none of the research presented has been able to establish a fully private end-to-end encrypted system.

1.1 Motivation and contribution

Based on the aforementioned works, it can be interpreted that despite of many block chain-based health care schemes in literature, none of these addressed the integrated challenges, namely, data confidentiality, patient's accessibility, and efficiency against cryptographic attacks. In this paper, we propose a secure and efficient way to store the patient's physical and biological data using a multi-authority attribute-based protocol. The attributes are encrypted using SHA-256 algorithm combined with logarithmic based RSA algorithm for digital signatures providing an efficient asymmetric encryption method. This algorithm generates a unique hash of the input data fields like patient id, previous transaction hash, illness records, and gender using SHA-256 algorithm.

Thereafter, the hashed data fields are signed with the issuing authority's private key using the RSA algorithm for its verification against tempering or authenticity. The distribution and management of patients' physiological data is done only if the public key is verified by the issuing authorities if it is consented to transfer the diagnosis to the other hospitals or healthcare providers.

Our proposed model provides a secured and encrypted decentralized database management system with the combination of SHA-256 and modified logarithmic based RSA algorithm. This allows the patients to share the records in a secure and decentralized manner. In this paper, both the algorithms are implemented to ensure perfect privacy and resistance to collusion attacks that reduces forgery and immutability in the transaction ledgers as compared to the traditional models in literature. We have used the RSA algorithm on a decentralized issuing authority mechanism called Multi-authority Attribute Based Encryption (MA-ABE) wherein, any polynomial number of autonomous authorities can monitor characteristics and dispense secret keys. The main motivation behind this research work is to reduce the time complexity and robustness against third-party attacks in comparison to the models proposed by Rui Guo [9] and D. Cao [12]. To this end, the application and performance evaluation of the presented work has more potential to address the aforesaid challenges. The main contribution of this paper includes:

- Introducing a technique to encrypt the end-to-end patients' data as an improvement to the traditional ABE scheme proposed by Rui Guo [9] by introducing a combination of modified logarithmic based RSA and SHA 256 encryption in EHRs. The security level and efficiency are

improved to withstand hypothetical attacks-Ciphertext-only attack and Fermat's factorization attack.

- The primary challenge for multiple authorities is defending the network of devices against an attack [3]. To address this challenge, we have modified the RSA algorithm to strengthen it against attacks by replacing the modulus with its logarithmic value in order to increase the difficulty of factorizing it into the prime numbers from which it is derived.
- Another challenge is the one-time process in distributing medical records for the verification of each user. To provide the solution to this problem, our model verifies all the block signatures each time a new patient or device tries to obtain the data stored on the blockchain.

The rest of this paper is structured as follows. Section 2 discusses the proposed modified RSA algorithm with its implementation in EHR using the system architecture of the proposed model. Furthermore, Sect. 3 demonstrates implementation of the EHR model followed by the numerical simulations based on the modified algorithm on the considered model in Sect. 4 and Sect. 5 concludes the presented work and Table 3 Appendix in Sect. 6 followed by the references in Sect. 7.

2 System architecture of the proposed model

In this section, a detailed framework of the proposed model is discussed. Multi-authority attribute-based encryption scheme is used in the proposed model to securely distribute the patients' medical data in a public platform. However, there are still a few challenges whilst protecting the data from malicious attackers. Hence, to solve this problem, we implement the modified RSA signature model using Blockchain technology, which provides the characteristics of unforgeability, secure, accurate and time-efficient model of storage and maintenance.

The proposed EHR model in Fig. 1, consists of a cloud server that stores the patients' records and is responsible for sharing and distributing the records to other users. There are N authorities representing different organizations like hospitals, treatment centres, and research labs, etc. which are responsible for accepting, enrolling, and exchanging the patients' vital information.

Patients may distribute and sign their own records present in the EHRs and define the predicate while the data authenticator is allowed to access the RSA signature and confirm the accuracy. Further, the digital signatures are

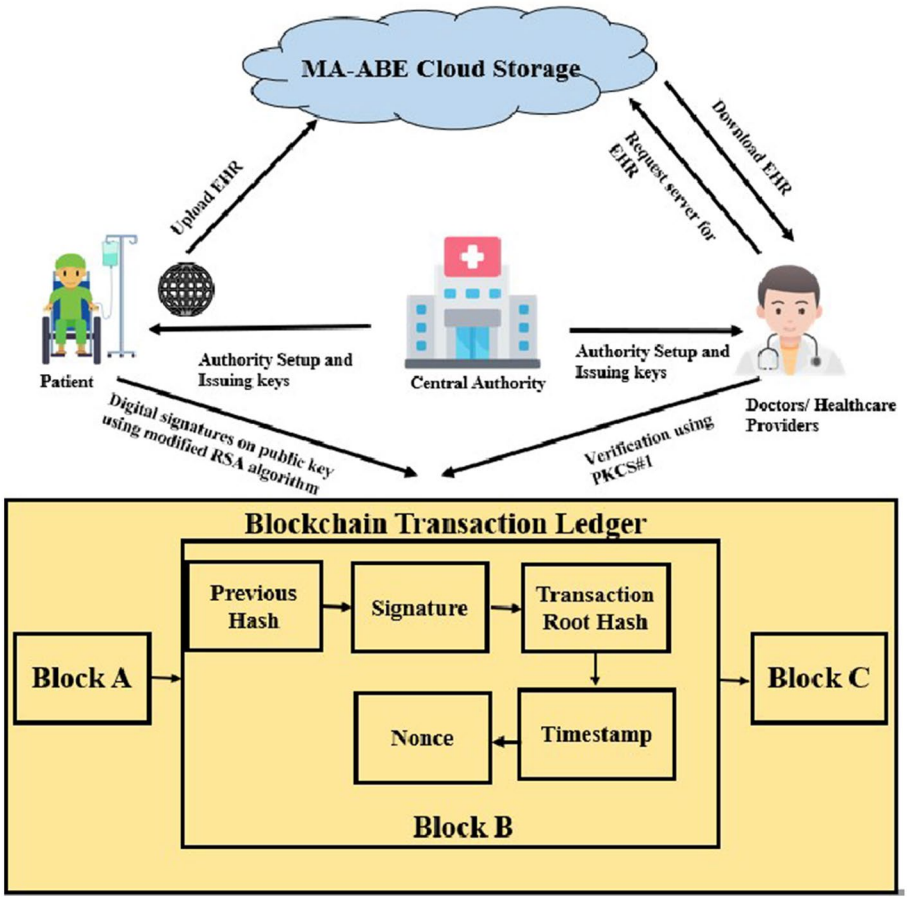

Fig. 1 System architecture of the proposed scheme

done on the keys issued to the patients in addition to the healthcare providers that can access the patients' records.

Once the trust is determined and the patient's data is stored using blockchain, the block is fingerprinted with the root hash, time stamp, and the previous hash value. MA-ABE strengthens the standard ciphertext-policy and attribute-based encryption policy, assuming no reliable central authority and thereby any organisation can become an authority.

Hence, there is no requirement of any universal synchronization other than the conception of an initial set of public reference parameters and the GID for all users that are submitted to the authority and hence, issues the keys to the users for security.

2.1 The proposed algorithm can be described in three steps

The data fields are created as a standard form of semantic data modelling for each patient. This can ensure lesser probability of attacks as all the records in the blockchain appears similar and hence, it becomes difficult to distinguish between the records at a glance.

Once the single block is created for each patient, every subsequent prescription can be filed as a separate block thereby, creating a separate and complete blockchain for every patient.

The final step involves the encapsulation of all the data stored with digital signatures using the modified RSA algorithm is defined in Sect. 4. Note that the encapsulated data has already been hashed in Step 2 by the SHA 256 algorithm.

Step 3: All the transactions are then instanced in the final class to create the transactions and perform signature verification.

The abovementioned three steps are the backbone of our proposed model and provide the highest level of security under attacks from a forger or attacker. Our model also supports security of the APIs, smartcards, and hardware implementations through Public Key Cryptographic Standards (PKCS#1).

The PKCS#1 is a platform-independent API that helps in creating or manipulating cryptographic tokens that are generated during the digital signatures. They are extremely useful for issuing user certificates for verification and authentication of the users or any hardware devices. Here, the PKCS#1 is used with the RSA algorithm to issue certificates and access the authority's signing key.

3 Implementation of proposed model

Even though blockchain combined with an EHR scheme is secure and accurate in data transmission yet, there exists some challenges in preventing attacks and mishandling of data. Hence, to provide a solution to this problem, we implemented the modified logarithmic-based RSA algorithm.

3.1 Modified RSA algorithm in EHRs

RSA is a factoring-based asymmetric cryptographic algorithm that takes in two large prime numbers 'p' and 'q' and computes the modulus (n) to generate a public key and a private key. The RSA public keys consist of the product of two prime numbers p and q and the consequent number e in the form (n, e) as presented in Appendix (Table 3). This algorithm is considered to be one of the most secure cryptographic algorithms for data transmission but consumes large memory. It takes massive RAM storage to forage the factor base of the algorithm. It efficiently prevents the data from any attacks as it takes years for a real time attack on an RSA key of length 1024-bit length. An attack on RSA would mean decrypting the authorized message by first factorizing the modulus into the two huge prime numbers and then finding the reverse of e, wherein the effort lies.

A modified version of RSA algorithm is proposed and implemented for strengthening the ciphertext and prevention of attacks, where modulus *n* is replaced with its logarithmic value to increase the difficulty of regenerating the two large prime numbers from the key. This decryption by an attacker becomes more arduous and time consuming when the logarithmic based RSA algorithms is implemented as discussed in Algorithm 1.

The public key (K_a, s) is generated based on a random value K_a in the range $\sqrt{n} < K_a < \varphi(n)$ and *s* as calculated

Algorithm 1: Modified RSA

Generate two random prime numbers: *x* and *y*.

Calculate $n = x*y$ (The key length is determined in bits).

Calculate Euler Totient Function:

$$\phi(n) = (x-1)*(y-1) \quad \text{-(1)}$$

Calculate key K_a $\sqrt{n} < K_a < \phi(n)$ and

$$GCD(K_a, \phi(n)) = 1 \quad \text{-(2)}$$

Compute $s = log(n)$ to replace *n* -(3)

Calculate key K_b such that:

$$K_a * K_b \bmod (s) = 1 \quad \text{-(4)}$$

Note: GCD- Greatest common divisor

Algorithm 2: Message encryption and decryption

Message encryption: The patient can encipher the plain text message *M*1 using the public key (K_a, s) in Algorithm 1 as follows:

$$M1^{K_a} \bmod s$$

Message decryption: The receiver can decrypt the ciphertext message M2 using the private key (K_b, s) in Algorithm 2 and *M*1 as:

$$M2 = \sqrt{M1^{K_b} \bmod s}$$

in Algorithm 1 (Eq. 3) and the private key consisting of key K_b and s is calculated in Algorithm 1 (Eq. 4) as (K_b, s). Thereafter, the keys generated in Algorithm 2 are used for enciphering and deciphering operations.

3.2 Multi-authority attribute based encryption (MA-ABE)

It provides a detailed framework of the multi authority attribute-based encryption presenting the decentralization of issuing authority as a different number of independent authorities can issue keys to the users and healthcare providers [9] (See Fig. 2). The attributes of the access tree structure are stated as $\langle t, no(t), k(t), parent(t), attribute(t), index(t)\rangle$. A node in the access tree structure is represented by t, where each node is a threshold gate (AND, OR, XOR, NAND etc.), while leaves are denoted by attributes. Further,

$no(t)$: It signifies the number of children nodes in node t in T.

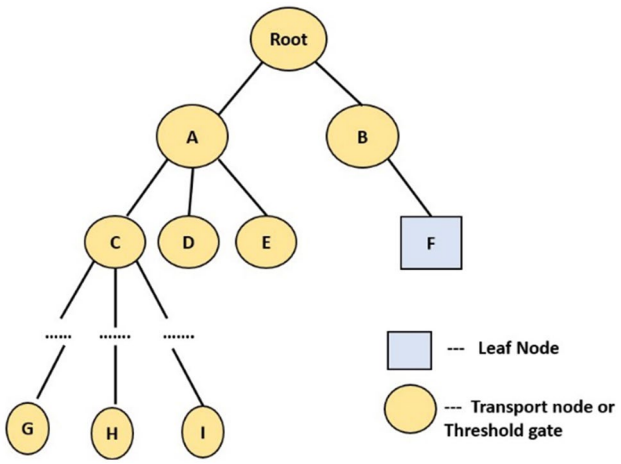

Fig. 2 Access tree structure to represent the patient's attributes [1]

Algorithm 3: Patient registration on blockchain

Input: Patient ID, Name, Gender, Disease, b_k (authentication parameter), GID, nonce, miner key, public key, private key, blockchain block *B*1.

Output: Patient registered in Blockchain

F_Name ← *Patient Name*

idN ← *Patient ID*

Request Patient ID for Registration

if *SHA256.new (public key) match* **then**

print *("Success")*

end if

else

print *("Error in matching public key");*

end else

B1 ← *SHA256(idN | | F_Name| | Disease| | GID) -(5)*

BLOCK ← create block *(B1| | nonce| | miner key| |public key| | b_k)) -(6)*

Store BLOCK in ledger

* Note: | | denotes the concatenation symbol.

$k(t)$: It denotes the threshold value of t, and $0 < k(t) \leq num(t)$. Further, $k(t) = 1$ and $k(t) = no(t)$ indicate OR and AND gates, respectively.
$parent(t)$: This is the parent of t in the access tree structure T.
$attribute(t)$: is a characteristic value on the leaf node t in T.
$index(t)$: This denotes the number associated with t; the value is from 1 to $no(t)$, which is assigned to (t) for a ominated key [1].

3.3 Patient registration on blockchain

Each patient's data can be registered on the cloud and accessed through individual blockchain. The following algorithm is used to register a patient on the blockchain by introducing the Patient ID, Name, gender, disease, GID and authentication parameters like nonce, timestamp, b_k and public key as generated in Sect. 3 using the modified RSA algorithm. The constructor sets data fields according to the arguments provided such a previous hash, miner key, and

Algorithm 4: Adding transactions to the blockchain

Input: prev_hash, miner key, nonce, timestamp, public key.

Output: Valid blockchain created

Initialize blocks= []

Calculate blockchain hash (bhash) using hex digest.

For each block:

if *blocks[prev_hash]! =blocks [bhash]:*

print ("*Block authentication failure*")

end if

else

Blockchain ← *Block (prev_hash| | miner key| | nonce| |timestamp)*

index on the block along with the transactions recorded earlier (not in case of a genesis block).

3.4 Adding transactions to the blockchain

The newly registered data is added to the existing blockchain ledger as demonstrated in Algorithm 3 Eqs. 5 and 6 using the miner key generated with each transaction and the previous hash is encrypted using modified SHA-256 algorithm.

Once the blocks are created, they are encapsulated to form a blockchain for each patient. This process in elaborated in Algorithm 4 given below:

The proposed model has been intensively tested based on the algorithms 1–4 given above on several cryptographic attacks and the performance analysis is presented in terms of defence efficiency and decryption time by the attacker as presented in Sect. 4.

Table 2 Comparison of attack efficiencies of proposed RSA attack to original RSA for both factorization attacks

Attack name	Defence efficiency (%)	Original RSA attack time (s)	Modified RSA attack time (s)
Ciphertext-only attack	22.367%	342,250	418,777.2
Fermat Factorization attack	12.72%	247,809	279,331

4 Numerical simulations

This section demonstrates the efficiency of the modified RSA algorithm with a double layer of encryption, i.e., using SHA-256 and RSA algorithm with *s* as the modulus. It is observed that when two prime numbers 'p' and 'q' are taken as input, the time for an attacker to decrypt the message increases significantly. This is indicative of the high level of strength of the encryption by the proposed algorithm and the increased security that it provides as compared to the standard algorithm as shown in Table 1.

Implementing the modified logarithmic based RSA algorithm on signed EHRs significantly improves the level of security in the permission-based network as can be concluded from the data given in Tables 1 and 2.

The time to decipher the keys in case of an attack has increased in the proposed algorithm as compared to the standard RSA algorithm. This is because the proposed modified RSA algorithm provides an exceptional level of security to our system and increases the difficulty to decipher the keys generated.

4.1 Significant increase in time for decryption

In case is any malicious attack occurs on the considered system, it would take a minimum of 7711.667 min (462,700 s) for an attacker to decrypt the double layer of encryption of the proposed model, resulting in an improvement of 38.8% as compared to the baseline EHR models using traditional RSA implemented in [9]. Hence, any tampering or forgery can be detected by the authentic nodes in the network and terminate the session established to transfer the data.

Table 1 Comparison of decryption time by an attacker using standard RSA and modified RSA algorithm

p (prime number)	q (prime number)	Message (M)	Time taken by the attacker to decrypt in (s) using standard RSA algorithm [9]	Time taken by the attacker to decrypt in (s) using modified RSA algorithm
155	76	97	333,261	462,700
339	68	114	399,729	500,001
775	9557	156	485,122	589,910
992	12,552	195	573,804	645,777

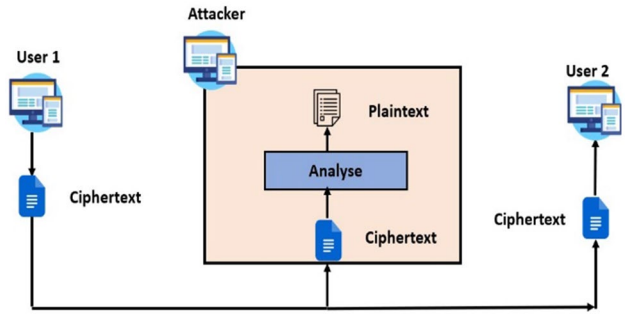

Fig. 3 Representation of a ciphertext-only attack with two users communicating and an attacker through the plaintext

4.2 Robustness against factorization attacks

Our proposed model consists of a MA-ABE scheme in blockchain combined with a modified RSA algorithm that secures the medical data of the patients from several adversaries and forgery. To test the robustness of our model, we have performed the following factorization attacks on it to determine the level of security that is provided by our model when a third-party attacker tries to forge or retrieve the data from the EHR of the patients.

4.2.1 Ciphertext-only attack on modified RSA algorithm

The ciphertext-only attack assumes that the attacker or forger can attain only passive capability to eavesdrop on the encrypted communication. The attacker thus only knows ciphertexts CT_i, where i = 1,2,3…n but not the corresponding plain texts, PT_i, i = 1,2,3…n. The attacker can depend on certain severance assumptions about the plaintexts, for example, the encryption its format. This scenario is the weakest in terms of abilities of the attacker, and thus it is the most practical in real life scenarios in the healthcare industry. Our proposed model contains a modified RSA algorithm in combination with the SHA 256 encryption and a logarithmic value of modulus (n) to combat such an attack on the EHR model. The security level, i.e., the strength of the ciphertext of the RSA algorithm is calculated in terms of the number of nodes and time taken for the actual attack to decipher the complete bit length of the private key.

In the given Fig. 3, the attacker has limited capability of deciphering the ciphertext, i.e., they can only see the enciphered data that is transmitted from user 1 to user 2. These types of attacks generally reduce the rate of successful attacks.

Algorithm 5: Fermat factorization

Input: prime numbers: *x, y*
Output: number of guesses *(g)*
Compute $n = x * y$
From Algorithm 1: $s = \log n$
Let $a := \sqrt{s}$ and $b := \sqrt{a^2 - s}$
while *b* is not an integer do:
$a = a+1$;
$b := \sqrt{a^2 - s}$
end while
Compute $g=a-b$
Output *g*

4.2.2 Attack on modified RSA algorithm using Fermat's factorization algorithm

Fermat's factorization algorithm allows efficient calculation of the prime factors of a composite numeral that is the product of two close primes. The RSA encryption and signature algorithm accounts for the factorization of huge numbers, which is an arduous task. The RSA public key contains a composite number (modulus) that is the multiplication of these primes. However, in the modified RSA algorithm the composite number in the public key is replaced by its logarithmic value to reduce the transparency and increase the strength of the public and private keys. If RSA keys are generated with primes with values that are relatively closer to each other, then RSA can be cracked with Fermat's factorization algorithm. However, on testing the proposed algorithm in real-time scenario, it has been interpreted that the factorization of the key into its prime numbers is extremely difficult and takes a significant amount of time to decipher in case an attacker attempts to decrypt the sensitive data. In the proposed model, the modified modulus has a high level of strength with an increased difficulty in determining the modulus as it is distributed in a logarithmic format as compared to the standard RSA algorithm where the modulus was distributed in the public and private keys explicitly. Hence, this attack was unsuccessful to a large extent. The Fermat factorization algorithm can be described as follows:

In comparison to previous RSA algorithms, the logarithmic RSA algorithm has been experimentally evaluated to show an increased defence capability by approximately 22.4% and 12.7% by Ciphertext-only attack and Fermat factorization attack, respectively as compared to original RSA based models implemented in [8, 12] and blockchain-based models in [16 and 17].

5 Conclusion and future work

Aiming at protecting the privacy of patients' records stored in a blockchain, our proposed model exhibits a step forward in safe and secure transmission of medical data in EHRs. The modified RSA algorithm is capable of defending the EHR model and improves the defense efficiency of the model by approximately 38.8% against the various cryptographic attacks as compared to models presented in [9] and 11.

Although there has been significant improvement in the efficiency of our model, yet, there can be advancements in the future to ensure resistance to attacks. The implementation of various trust models in MA-ABE scheme can improve the security and immutability of the records. To improve the security and maintain the unforgeability of the blockchain, the policy decision points that verify the attributes need to be implemented such that the attacker can be tracked and removed from the network before the data is tampered. Improving the policy engine, the peer-to-peer network would be helpful in limiting the access of the blockchain records and hence prevent real time attacks. Another aspect to improve the security of the proposed model is to include Proof of Elapsed Time (PoET) in the blockchain that can record the timestamp in case an attacker enters the blockchain to ensure that the verifier can identify any malicious nodes in the blockchain.

Declarations

Conflict of interest The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Appendix (Table 3)

Table 3 RSA encryption algorithm

RSA encryption
Input: required modulus bit length, n
Output: RSA encryption key, decryption key
Generate two random prime numbers: p and q
Compute RSA modulus: n = p*q
$K_{enc} = \varphi(n)-1$
$K_{dec} = K_{enc} - 1;$
$K_{enc} * K_{dec} \bmod \varphi(n)-1$

Here, K_{enc} is the encryption key and K_{dec} is the decryption key

References

1. Singh AP, Pradhan NR (2021) A novel patient centric architectural framework for blockchain enabled healthcare applications. IEEE Trans Ind Inf. 17:5779–5789
2. Misra U, Gupta R, Gupta J (2023) InterPlanetary file system based blockchain for internet of medical things. Int J Inf Technol. https://doi.org/10.1007/s41870-023-01207-9
3. Gowda NC, Malakreddy B (2023) BPCPR-FC: blockchain-based privacy preservation with confidentiality using proxy reencryption and ring signature in fog computing environments". Int J Inf Technol 15:3343–3357. https://doi.org/10.1007/s41870-023-01373-w
4. Li X, Ibrahim MH, Kumari S, Kumar R (2018) 'Secure and efficient anonymous authentication scheme for three-tier mobile healthcare systems with wearable sensors.' Telecommun Syst 67(2):323–348
5. Zhang X, Zhao J (2019) Conditional identity privacy- preserving public auditing for cloud- based WBANs against malicious auditors. IEEE Trans Cloud Comput. 1:110–121
6. Mistry C (2021) MedBlock: an AI-enabled and Blockchain-driven medical healthcare system for COVID-19. ICC 2021 IEEE Int Conf Commun. https://doi.org/10.1109/ICC42927.2021.9500397
7. Rajput AR, Li Q (2019) EACMS: emergency access control management system for personal health record based on blockchain. IEEE Access. 7:84304–84317
8. Maji HK, Prabhakaran M, Rosulek M (2008) Attribute-based signatures: achieving attribute-privacy and collusion-resistance. IACR Cryptology 2008:328
9. Guo R, Zheng D (2018) Secure attribute- based signature scheme with multiple authorities for blockchain in electronic health record systems. IEEE Trans Cloud Comput 6:11676–11876
10. Okamoto T, Takashima K (2011) Efficient attribute-based signatures for non-monotone predicates in the standard model. Public key cryptography—PKC 2011. Springer, New York, pp 35–52
11. Das P, Singh M, Roy DG. A secure softwarized blockchain-based federated health alliance for next generation IoT networks. Globecom Workshops IEEE. 2021. pp. 1–6.
12. Cao D, Zhao B, Wang X, Su J, Ji G. Multi-authority attribute-based signature. In Proc. 3rd IEEE INCoS, Japan. 2011. pp. 668–672