НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
май–июнь 2024 Том 24 № 3 http://ntv.ifmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
May–June 2024 Vol. 24 No 3 http://ntv.ifmo.ru/en/
ISSN 2226-1494 (print) ISSN 2500-0373 (online)

doi: 10.17586/2226-1494-2024-24-3-456-463

Enhancing healthcare data security in cloud environments with dual authentication and optimal key-tuned encryption

Hema Ambiha Aravindakshan[1]✉, Pragaladan Rengasamy[2]

[1,2] Sri Vasavi College, Erode, 636316, India

[1] hemaambiha@gmail.com✉, https://orcid.org/0009-0000-7495-5107
[2] pragaladanr@gmail.com, https://orcid.org/0009-0007-9407-3591

Abstract

The primary idea of this paper is the implementation of the Optimal Key-Tuned Rivest Shamir Adelman technique, a dual authentication approach for effective data sharing in the cloud within hospital data management. The system begins with user registration with the Trusted Center where user details are provided. An authentication scheme utilizing the Caesar cipher and the Secure Hashing Algorithm 512 ensures integrity. The encryption process employs the Optimal Key-Tuned Rivest Shamir Adelman scheme for secure file transmission. To enhance key creation procedures in the Rivest Shamir Adelman model, the Improved Butterfly Optimization Algorithm technique is utilized to maximize throughput. Finally, dual authentication is conducted on the receiver side for file access and downloads from the cloud server. This additional layer of authentication fortifies the system resilience against unauthorized access, ensuring that only legitimate users can interact with the healthcare data stored in the cloud. The results indicate that the system outperforms other state-of-the-art systems enabling secure sharing and downloading of health data in cloud environments.

Keywords

healthcare security, dual authentication, secure data transmission, encryption, decryption, trusted center

For citation: Aravindakshan H.A., Rengasamy P. Enhancing healthcare data security in cloud environments with dual authentication and optimal key-tuned encryption. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2024, vol. 24, no. 3, pp. 456–463. doi: 10.17586/2226-1494-2024-24-3-456-463

УДК 004.056.5

Повышение безопасности медицинских данных в облачных средах с помощью двойной аутентификации и оптимального шифрования с настройкой ключей

Хема Амбиха Аравиндакшан[1]✉, Прагаладан Ренгасами[2]

[1,2] Колледж Шри Васави, Ироду, 638316, Индия

[1] hemaambiha@gmail.com✉, https://orcid.org/0009-0000-7495-5107
[2] pragaladanr@gmail.com, https://orcid.org/0009-0007-9407-3591

Аннотация

Представлены результаты реализации метода двойной аутентификации Ривеста Шамира Адельмана с оптимальной ключевой настройкой для эффективного обмена данными в облаке в рамках управления медицинскими данными. Работа системы начинается с регистрации пользователя в доверенном центре и заполнения его данных. Схема аутентификации, использующая шифр Цезаря и алгоритм защищенного хеширования 512, обеспечивает целостность системы. В процессе шифрования применяется метод Ривеста Шамира Адельмана (RSA) с оптимальной настройкой ключей для безопасной передачи файлов. Для улучшения процедур создания ключей задействован метод улучшенного алгоритма оптимизации «бабочка», позволяющий максимизировать пропускную способность. В результате пользователь выполняет двойную аутентификацию для доступа к файлам и их загрузки с облачного сервера. Этот дополнительный уровень аутентификации повышает устойчивость системы к несанкционированному доступу, гарантируя, что только законные пользователи могут

взаимодействовать с медицинскими данными, хранящимися в облаке. Полученные результаты показали, что предложенная система превосходит другие современные системы, обеспечивая безопасный обмен и загрузку данных в облачные среды о состоянии здоровья пациентов.

Ключевые слова
безопасность здравоохранения, двойная аутентификация, безопасная передача данных, шифрование, дешифрование, доверенный центр

Ссылка для цитирования: Аравиндакшан Х.А., Ренгасами П. Повышение безопасности медицинских данных в облачных средах с помощью двойной аутентификации и оптимального шифрования с настройкой ключей // Научно-технический вестник информационных технологий, механики и оптики. 2024. Т. 24, № 3. С. 456–463 (на англ. яз.). doi: 10.17586/2226-1494-2024-24-3-456-463

Introduction

Due to the importance of healthcare in everyone's life, it is now crucial to diagnose patients and preserve them for future use to protect healthcare data like medications and past health records. This medical information was initially converted from paper records into electronic format. This approach provided various opportunities for tampering and data loss. By providing tasks that other forms of records cannot provide, Electronic Health Records (EHRs) are one such option to help healthcare facilities of all levels and sizes improve patient care [1, 2]. EHRs are producing enormous amounts of data owing to the development of digital information [3] and handling these high volumes of data requires an effective processing system [4]. So, cloud networking is growing in significance in this process [5]. Conventional EHR systems pose several privacy and security challenges despite their use and dependability. Medical data cannot be shared with scientific organizations due to patient privacy concerns, which hinders medical advancement [6]. Researchers commonly define a cybersecurity attack on healthcare information as information that has been misplaced, lost, stolen, compromised, or transmitted to unofficial recipients without their consent. According to reports, the medical records of 150 million patients were compromised between 2009 and 2014, and 94 % of healthcare organizations have reported experiencing at least one incident [7]. So, it is required to consider the privacy and security of the medical data when evaluating a decentralized and trust-based strategy [8, 9].

The best defences against hackers for EHR data are authentication and encryption [10]. The authentication process is employed to protect the identity of the data. The server can identify legitimate or registered users and reject unauthorized, unregistered, or fake users. The technique of transforming regular information into unreadable text is known as encryption. Both asymmetric and symmetric encryption techniques are available. Although symmetric encryption is computationally faster, it offers less protection to the system and makes data corruption by hackers easier. Asymmetric encryption employs two public and private keys making it challenging for hackers to break the code. This motivates us to propose an asymmetric encryption scheme called Rivest Shamir Adelman (RSA), and the key is optimally chosen using Improved Butterfly Optimization Algorithm (IBOA) and dual authentication to provide an additional level of security. The main objectives of the proposed work are outlined as follows:

— The current study applies dual authentication methods such as Caesar cipher and SHA512 to achieve effective authentication that protects the data from unauthorized users and permits only legitimate users to access cloud services.
— A novel Optimal Key-Tuned RSA (OKTRSA) is proposed to ensure the privacy and confidentiality of patient data in the cloud in which the IBOA algorithm is used to generate the keys for enhanced secure medical data transmission optimally.

Related works

Mehedi Masud et al. [11] presented a lightweight access control scheme for a cloud-assisted e-healthcare system. The system authorizes the users by generating the hash value for their credentials, such as patient ID, doctor ID, and nonce value. Once approved, their data was securely stored in the cloud to provide secure access to the user's data. The scheme attained better outcomes than the existing models for secure cloud storage of e-health data. Mohan Naik Ramachandra et al. [12] introduced a Triple Data Encryption Standard (TDES) to secure cloud data storage. The system attained a lesser encryption and decryption time of 360 ms and 475 ms, which was better than the existing schemes. Hong Zhong et al. [13] suggested an attribute-based access control scheme for edge-enabled innovative healthcare. The authorization of the users was done based on trusted authority which generated the public and master keys for data encryption. In contrast, the private key was generated using the key generation model that was used to perform decryption. The system achieved lower computational time than the existing models. Sherif Abdelfattah et al. [14] presented a secure data storage scheme for medical data in the cloud. Initially, the secret keys were generated using the key distribution centre and distributed to the patients and doctors. Then, the patient's medical records were encrypted and transferred to the cloud. Finally, the doctor decrypted the encrypted data and performed further processes. K. Ambika and M. Balasingh Moses [15] proffered an Advanced Flexi Twister Secret Block Encryption Standard (AFT-SBES) algorithm for secure cloud data storage. The patient's data was partitioned into several data blocks, and the encryption and decryption procedures were done over the portioned blocks. The system achieved a computational cost of 820 KB for 500 users in cloud simulation, which was better than previous models.

The works mentioned above provide satisfactory outcomes but have some areas for improvement. Some studies use symmetric encryption algorithms (TDES, AFT-SBES, etc.) to encrypt the patient data for secure storage which uses the same key for encrypting and decrypting the message. The possibility of attacking the data in an unsecured channel is high. Asymmetric encryption is more secure than symmetric encryption. Herein also, we adopt an optimal version of RSA in which the critical generation process is done optimally using the IBOA. In addition, some surveys are manually registered to a trusted authority. However, this manual registration provides less security to the system, and threat actors can break into your accounts more efficiently. Herein, the proposed system develops dual authentication methods such as Caesar cipher and the SHA512 algorithm to provide high-level security.

Proposed methodology

The proposed methodology addresses the critical need for a robust framework in the transmission of electronic healthcare data within cloud environments emphasizing confidentiality, integrity, and accessibility. In response to the call for specificity and depth, we present an enriched version that provides a more detailed and nuanced approach aligning with the intricacies of EHRs and the cloud environment. EHRs, in their digital manifestation, play a pivotal role in consolidating patient data, medical histories, and treatment plans. However, the transition from traditional paper records to electronic formats brought forth new challenges, especially concerning data security and privacy. This paper recognizes the nuanced nature of EHRs emphasizing the sensitivity and diversity of medical information they encapsulate. Issues, such as patient privacy, secure data access, and the seamless interoperability of EHR systems, underscore the significance of robust security measures.

Cloud Environment in Healthcare

The adoption of cloud computing in healthcare has introduced unprecedented opportunities for efficient data storage, processing, and accessibility. Nevertheless, the unique demands of healthcare data, characterized by its sensitive nature, necessitate a bespoke approach to security within cloud environments. Understanding the intricacies of cloud infrastructure, resource allocation, and data transmission protocols becomes imperative to mitigate risks associated with unauthorized access and data breaches. This paper converges on the synergy between EHRs and cloud environments acknowledging the necessity of a security framework tailored to their specific demands. The proposed methodology aligns with the intricacies of healthcare data offering a dual authentication approach, encryption techniques, and optimization algorithms to fortify the system against potential threats. By doing so, it not only addresses the pressing challenges in EHR and cloud security but also strives to set a benchmark for a more comprehensive and specific approach in safeguarding healthcare information.

Fig. 1 shows the workflow of the proposed methodology. Initially, the user must register with the Trusted Center (TC) by providing their details. Then, TC generates the cipher values for the user ID and password using Caesar cipher, and TC generates the hash values using SHA512 by combining the user's name, user ID, and timestamp. Then, these cipher and hash values are stored in the Cloud Server (CS) for authentication. After that, the user is directed to the login page by providing their login details. Herein, the TC verifies the login credentials against registered credentials. If the verification is successful, the TC grants the users to upload the file in the cloud; otherwise, it rejects the user request. After successful validation, the user can upload a file encrypted by OKTRSA in which IBOA optimally chooses the public key. Finally, on the receiver side, authentication is performed for data downloading, which enhances the system security. The proposed methodology aims to ensure the secure transmission of healthcare data in a cloud environment addressing the critical issues of authentication and encryption. Below is a detailed algorithmic representation of the key steps involved in our proposed approach. The advent of EHRs revolutionized healthcare data management providing opportunities for improved patient

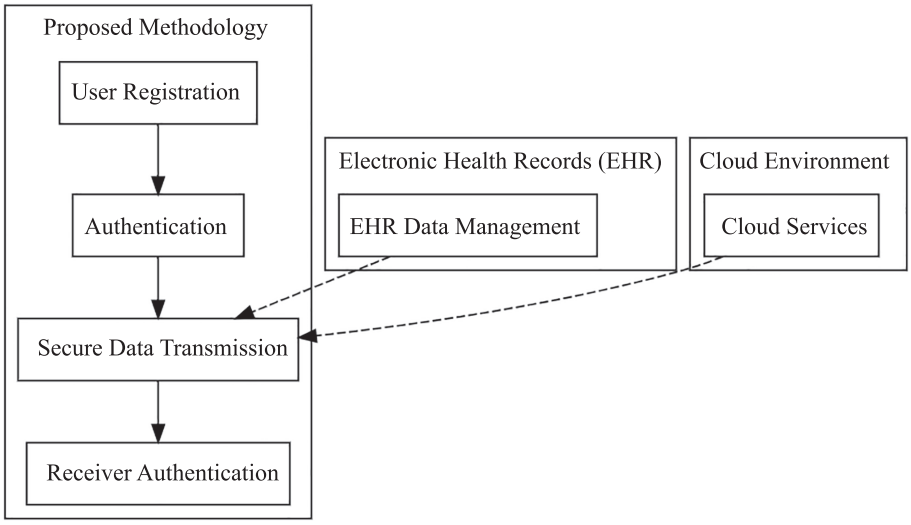

Fig. 1. Workflow of the proposed methodology

care. However, the transition from paper to electronic records also introduced security challenges necessitating robust defenses against cyber threats. Authentication and encryption stand as paramount defenses to safeguard EHR data against unauthorized access and tampering. This proposed methodology focuses on dual authentication using the Caesar cipher and SHA512 algorithm, coupled with the OKTRSA encryption technique. The IBOA optimizes the RSA key generation process, ensuring an enhanced level of security for healthcare data transmission in cloud environments. The proposed algorithm forms the cornerstone of our contribution, employing a combination of the OKTRSA encryption technique and the IBOA for key generation.

Algorithm: Secure Healthcare Data Transmission in Cloud Environment

1. User Registration

Input: User details (Name, User ID, Gender, Password, Date of Birth, Timestamp, Address, Medical History)

Output: Ciphered and Hashed Information stored in CS

1.1. GenerateCipher(User ID, Password)

Shift = Random value

CipheredText = CaesarCipher(User ID, Password, Shift)

1.2. GenerateHash(User's Name, User ID, Timestamp)

HashValue = SHA512(User's Name + User ID + Timestamp)

1.3. StoreCipherAndHashInCS(CipheredText, HashValue)

1.4. VerificationAtLogin(User ID, Password)

ProvidedCipher = CaesarCipher(User ID, Password, Shift)

Compare ProvidedCipher with StoredCipher

If Match, user is authenticated

2. Secure Data Transmission

Input: Patient's Sensitive Data

Output: Encrypted Data stored in CS

2.1. OKTRSAEncryption(Patient Data)

Public Key = IBOAForRSAKeyGeneration()

EncryptedData = RSAEncrypt(Patient Data, Public Key)

2.2. StoreEncryptedDataInCS(EncryptedData)

3. Authentication at Receiver Side

Input: Read/Download Request from User

Output: Decrypted Data for Early Diagnosis

3.1. First Level Authentication(User ID, Password)

Send Read Request along with User ID and Password to TC

Verify with StoredCipher in CS

Permit if authenticated for reading files

3.2. Second Level Authentication(User's Name, User ID, Timestamp)

If Read and Download Request,

Send Request along with User's Name, User ID, and Timestamp to TC

Calculate HashValue using SHA512(User's Name + User ID + Timestamp)

Check with StoredHashValue in CS

If Matched, user is authenticated for download

3.3. DecryptData(EncryptedData)

Use RSA Private Key to decrypt the data for early diagnosis

Set up Phase

To begin, the User must register with the Cloud Service Provider (CSP) to prove their authority. In this registration phase, the User providing details is ciphered and hashed using a combination of Caesar cipher and SHA512 algorithm because the security of patient details can be more awake the authenticity of the data. Herein, the patients initially register demographic information like User's name, user ID, gender, password, date of birth, current timestamp, address, and medical history to TC. After registration, TC generates a cipher and hash value for the information provided by the User using Caesar cipher and SHA512 to store in the database. These are explained as follows:

First, the TC generates cipher value for the user provided details by Caesar cipher by combining the user ID (D_{PI}) and password (D_{PW}). One of the well-known methods is the Caesar cipher, a kind of substitution cipher that transforms each letter in the plaintext to a new letter with a certain number of positions down the alphabet. It can be mathematically expressed as follows:

$$\overleftrightarrow{T}_l = ((D_{PI}||D_{PW}) + a)\text{mod}26.$$

Here, a refers to the shift and $\overleftrightarrow{T}_l$ denotes the cipher text for the corresponding user providing details (i.e., user ID and password). These ciphertexts are maintained by the CS for authentication purpose.

Next, the TC also generates the hash value by combining the user's name (D_N), user ID (D_{PI}), and timestamp (S_T) by using SHA512 algorithm to provide additional level of security. The SHA512 hash function produces message digests with 512-bit sizes and 1024-bit block lengths. Any message can be submitted using the SHA512 algorithm, and it will produce a hash result with a set length of 512 bits. The SHA512 hash code is displayed as follows:

$$\overleftrightarrow{H}_c = \hat{h}_f(D_N||D_{PI}||S_T).$$

Where, $\overleftrightarrow{H}_c$ indicates the hash code that is generated and $\hat{h}_f$ refers to the hash function. These generated hash values also stored in CS for authentication purpose. At the login time, the patients must provide the user ID and password for authentication when they log into the system. Then, the TC takes the cipher value using Caesar cipher and compared it to the stored ciphered value. If it matches, then the user starts to upload the files to cloud.

Secure Data Transmission

Once the user has verified, they can start uploading files to CSP. The patient's sensitive data must be encrypted before being transferred to the cloud to maintain security. A lightweight encryption scheme must be implemented because the acquired data is sparsely and frequently shared. Here, we use OKTRSA to encrypt the patients' medical data to provide higher cloud data security. The most used

public key cryptosystem is RSA, and its crucial component is the production of private and public keys. The RSA encrypts the medical data with a sender's public key and decrypts the encrypted data at the receiver end using a receiver's private key.

The public key is chosen randomly from the two huge prime integers in this key generation procedure, and the private key is computed using the public key. The key generation procedure is slowed down because the randomly chosen public key requires more time to execute. Additionally, it compromises system security while encrypting and decrypting data. Therefore, the IBOA is used to tune the RSA algorithms key generation process optimally. As a result, OKTRSA is the name given to the best public key generation procedure integrated with the traditional RSA. Key generation, encryption, and decryption are the three primary phases.

The encryption and decryption processes are done using the public and private keys. Only the private key is employed to quickly decrypt messages that have been encrypted with the public key. RSA algorithm first selects two distinct large random prime numbers $\tilde{x}$ and $\tilde{y}$. After that, it computes $\overleftrightarrow{E} = \tilde{x} \times \tilde{y}$, where, $\overleftrightarrow{E}$ is employed as the private and public key modulus. Next, compute the Euler totient function η* of $\overleftrightarrow{E}$ using the following:

$$\eta^*(\overleftrightarrow{E}) = (\tilde{x} - 1) \times (\tilde{y} - 1).$$

Random Key Generation

Then randomly chose the public key in the range of 1 to $\eta^*(\overleftrightarrow{E})$, but these randomly chosen key increases the computational time and, if they are not chosen optimally, they generate infinity values. Hence, IBOA is utilized in the current study to choose the public key optimally. Butterfly Optimization Algorithm (BOA) is a novel nature-inspired method that primarily relies on the foraging approach of butterflies which use their sense of smell to locate a source of nectar or a mating partner. Although, it resolves the challenging optimization problem and suffers from early convergence and inadequate use of the close to ideal solutions. The Wedding Dance Coefficient (WDC) is used to update the butterfly location and improve the capability of global search to address these shortcomings. IBOA is the name given to these position updates in traditional BOA centered on the WDC. Initially, the IBOA creates an initial population randomly using a uniform distribution. Next, compute the fitness of the individual by using the following formulas.

$$Fitness = \text{Max}(Throughput)$$

$$Throughput = \frac{\overline{RS}}{\tau}.$$

Where, $\overline{RS}$ refers to the resource that is created when completing the task and τ refers to the time it takes to transmit data from the sender to the receiver. Next, it moves to the iteration phase, where the candidates from the population use two phases called global phase and local phase. It is mathematically expressed as follows:

$$\mathbf{Z}_b^{t+1} = \mathbf{W}_C + \mathbf{Z}_b^t + (r_n^2 \times S^* - \mathbf{Z}_b^t) \times \mathbf{R}_b,$$

$$\mathbf{Z}_b^{t+1} = \mathbf{Z}_b^t + (r_n^2 \times \mathbf{Z}_u^t - \mathbf{Z}_v^t) \times \mathbf{R}_b,$$

where, $\mathbf{Z}_b^t$ indicates the solution for vector $\mathbf{Z}_b$ for b-th butterfly in iteration number t, S^* denotes the best position in the searching space, r^2 refers the random number in [0, 1], $\mathbf{Z}_u^t$ and $\mathbf{Z}_v^t$ represents u-th and v-th butterflies chosen randomly from the solution space, $\mathbf{R}_b$ indicates the fragrance of the butterflies, and $\mathbf{W}_C$ refers to the WDC. This coefficient enhances the global search ability of the algorithm by linearly decreased with the number of iterations. It is computed as follows:

$$\mathbf{W}_C = \mathbf{WD}_o \times J_e^t,\ 0 < J_e < 1,$$

where, J_e signifies the WDC at iteration t. The iteration process continues until the stopping criteria match. Upon completion of the iteration phase, the algorithm output generates the best solution (i.e., optimal public key ($\tilde{P}_U$)) found with its best fitness. Next, in the key generation process, the private key is computed by these optimal public keys obtained from IBOA.

$$\tilde{P}_R = (\tilde{P}_U)^{-1} \text{mod} \eta^*(\overleftrightarrow{E}).$$

Where, $\tilde{P}_R$ indicates the private key and $\tilde{P}_U$ refers to the optimal public key.

Encryption

Next, the encryption takes place after generating keys for encryption and decryption. It transforms the information into a code that is only known to a select few, hence concealing the information actual meaning. To encrypt the patient data ($\overleftrightarrow{I}_{PD}$) using a public key ($\tilde{P}_U$) that has been generated at key generation process to generate the cipher. It is defined as follows:

$$\overleftrightarrow{C}_T = (\overleftrightarrow{I}_{PD})\tilde{P}_U \text{mod} \overleftrightarrow{E}.$$

In this equation, $\overleftrightarrow{I}_{PD}$ indicates the input patient data to be transmitted to the cloud and $\overleftrightarrow{C}_T$ denotes the ciphertext for the corresponding input. These encrypted ciphertexts are securely stored in the CS for further processing.

Decryption

Decryption is converting data that has been encrypted back into its original form. In most cases, decryption is simply the reverse procedure of encryption. It decodes the encrypted information so that only a user with the appropriate authorization decrypts the data. The decryption process is mathematically expressed as follows:

$$\overleftrightarrow{I}_{PD} = (\overleftrightarrow{C}_T)\tilde{P}_R \text{mod} \overleftrightarrow{E}. \quad (1)$$

Authentication

When the user wants to download their encrypted healthcare data from the CS, authentication first occurs on the receiver side. On this receiver side, two levels of authentication are done to enhance the system security.

Level 1. Initially, if the user wants to read the files from the hospital CS, the level 1 of authentication is performed.

At this level, the user sends a read request along with the ID and password to TC. TC verifies it with the stored cipher value in the cloud to check whether it is an authenticated user. The TC permits the users to read the files from the CS if they are authorized.

Level 2. After successful completion of the level 1 of authentication, if the user wants both read and downloads the file from the CS, the user sends a read and download request along with their user's name, user ID, and timestamp to TC. Next, the TC takes hash values for the user providing details and is checked with the stored hash values. If matched, the user can read and download the files from the CS. Finally, the receiver decrypts the downloaded file using equation (1) for early diagnosis.

Results and discussion

Here, the efficiency of the proposed dual authentication and optimal encryption scheme for secure cloud storage is analyzed by comparing their outcomes with the existing methods regarding some evaluation indicators. The suggested task uses Python on a computer with a 6 GB GPU, 16 GB of RAM, an i7 Core processor, and a Windows 10 operating system. The dataset descriptions and the proposed work performance evaluation are shown in the following sections.

Dataset Descriptions

The proposed system uses the New York State Department of Health dataset to test and verify the effectiveness of the proposed work[1]. Researchers, public health professionals, media members, and community-based organizations can benefit significantly from these data sets. This dataset contains 34 columns and about 10 thousand data records. The data is split into 80:20 ratios for training and testing, respectively. The input data varied between 1000–10,000 records.

Performance Analysis

This section shows the outcomes of the proposed OKTRSA and the existing methods like RSA, Digital Signature Algorithm (DSA), Advanced Encryption Standard (AES), and Blowfish algorithm. The evaluation is carried out by some indicators such as Encryption Time (EXT), Decryption Time (DCT), Key Breaking Time (KBT), and reliability metrics.

The evaluation procedure was conducted with a detailed examination of the implementation of alternative solutions, ensuring transparency and a comprehensive understanding of the comparative analysis. Each cryptographic method (RSA, DSA, AES, Blowfish) was intricately integrated into the proposed framework, with explicit details on their roles in encryption, decryption, and key generation.

For instance, in RSA, the encryption process was governed by the formula:

$$C = P^e \bmod N,$$

where patient data P was encrypted using the public key e to generate ciphertext C. DSA contribution in digital signature generation was explained concerning authentication during file retrieval. AES and Blowfish played pivotal roles in secure data transmission, defining the encryption and decryption steps for enhanced security.

In the computation of performance metrics, KBT took center stage. Calculation is using the formula:

$$KBT = \frac{Resources\ Produced}{Time}.$$

KBT provided insights into cryptographic strength, considering key size and complexity. Reliability metrics, assessing system integrity, confidentiality, and accessibility, underwent detailed calculations based on established criteria:

$$Reliability = \frac{Resources\ Created}{Time}.$$

The training process of the algorithm involved meticulous steps, including the selection of a representative training dataset, iteration processes, and any fine-tuning procedures. During training, the algorithm adapted to the dataset, optimizing parameters for improved performance.

Table demonstrates the outcomes of the proposed and existing frameworks regarding EXT and DCT by varying the number of data records from 1000 to 10,000. EXT refers to the time the encryption model utilizes to create a ciphertext from plain text. It is computed as the difference between the encryption ending and starting times. DCT is computed as the difference between the decryption ending and starting times. The existing RSA, DSA, AES, and Blowfish take 81.77 s, 102.48 s, 119.79 s, and 129.48 s time to encrypt the records and 56.25 s, 78.86 s, 96.15 s, and 106.17 s time to decrypt the records, which are higher than the OKTRSA, because it takes 57.48 s and 33.85 s time to encrypt and decrypt the records, respectively, for the identical 1000 records. Likewise, the proposed one achieves superior outcomes for the remaining number of records (2500–10,000) than the existing methods. Hence, it is concluded that the proposed system is faster and more efficient than other methods. Fig. 2 shows the outcomes of the techniques concerning the KBT and reliability for 1000–10,000 records.

Fig. 2 shows that the proposed OKTRSA has enhanced security in medical image transmission regarding KBT and reliability.

— KBT Analysis (Fig. 2, *a*): The proposed OKTRSA exhibits improved security, with an average KBT of 87.33 ms for 10,000 records. This is 1.83 %, 3.81 %, 20.19 %, and 36.98 % less than RSA, DSA, AES, and Blowfish, respectively.
— Reliability Analysis (Fig. 2, *b*): The proposed OKTRSA achieves higher reliability (98.76 %) compared to existing methods (RSA: 95.98 %, DSA: 92.92 %, AES: 90.88 %, Blowfish: 86.04 %) for 1000–10,000 records.

When considering the KBT for a maximum of 10,000 records, the proposed OKTRSA takes an average of 87.33 ms, which is 1.83 %, 3.81 %, 20.19 %, and 36.98 % lesser than RSA, DSA, AES, and Blowfish. Thus, the

[1] New York City Department of Health and Mental Hygiene. Data sets and tables. Available at: https://npin.cdc.gov/organization/new-york-city-department-health-and-mental-hygiene-2 (accessed: 22.03.2024).

Table. EXT and DCT analysis, s

Metrics	No of Records	Proposed OKTRSA	RSA	DSA	AES	Blowfish
EXT	1000	57.48	81.77	102.48	119.79	129.48
	2500	55.61	79.49	101.77	117.84	127.51
	5000	58.52	82.64	103.47	120.77	130.51
	7500	60.57	84.82	105.81	122.54	133.57
	10,000	67.77	91.59	112.57	129.92	138.54
DCT	1000	33.85	56.25	78.86	96.15	106.17
	2500	31.97	53.86	80.92	97.95	104.86
	5000	35.02	57.25	83.32	107.99	115.98
	7500	36.86	58.86	96.17	117.88	123.89
	10,000	43.92	69.22	108.86	129.33	144.02

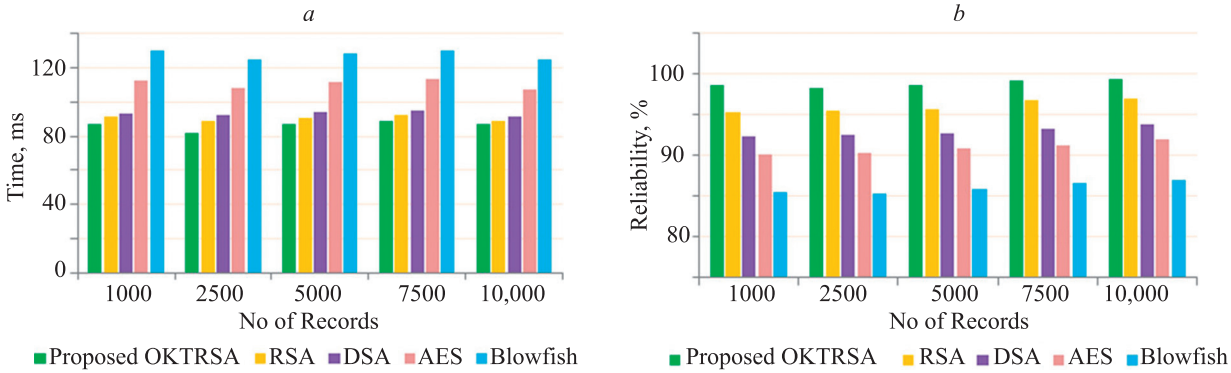

Fig. 2. Analysis based on KBT (*a*) and reliability (*b*)

overall KBT time of the proposed method is lesser than the existing methods. Next, reliability is essential to check the system efficiency and security level. Reliability is concerned with the integrity, confidentiality, and accessibility of systems. Herein, the existing RSA, DSA, AES, and Blowfish algorithms averagely have reliability of 95.98 %, 92.92 %, 90.88 %, and 86.04 % for the 1000–10,000 records, which is lesser than the OKTRSA because OKTRSA has average reliability 98.76 % for the same number of forms. So, from the overall evaluations, it could be found that the proposed one achieves superior performance than the existing methods. The reason is that the proposed one utilizes IBOA to generate the RSA key optimally, decreasing the EXT and DCT. And dual authentication by combining Caesar cipher and SHA512 is introduced to provide high-level reliability to the system.

Conclusion

This paper proposes dual authentication and secures encrypted electronic healthcare data transmission in the cloud. The proposed system mainly consists of authentication and secure data transmission. The experimental results were carried out using the New York State Department of Health dataset. The outcomes of the proposed Optimal Key-Tuned Rivest Shamir Adelman technique are investigated against the existing Rivest Shamir Adelman, Digital Signature Algorithm, Advanced Encryption Standard, and Blowfish algorithms in terms of Encryption time, Decryption time, Key breaking time, and Reliability metrics. The input is varied from 1000 to 10,000 records. In these experiments, the proposed system takes minimum average encryption, decryption, and Key breaking time of 57.48 s, 33.85 s, and 87.33 ms. Also, the proposed system archives a maximum reliability of 98.63 % for 5000 records. Thus, the findings reported the considerably better performance of the Optimal Key-Tuned Rivest Shamir Adelman technique over the existing methods. Therefore, the proposed technique can be utilized as an effective tool for enhancing security in the cloud. In future, the security performance can be improved by the design of the blockchain method.

References

1. Pai M.M.M., Ganiga R., Pai R.M., Sinha R.K. Standard electronic health record (EHR) framework for Indian healthcare system. *Health Services and Outcomes Research Methodology*, 2021, vol. 21, no. 3, pp. 339–362. https://doi.org/10.1007/s10742-020-00238-0
2. Zhao J., Zeng P., Choo K.K.R. An efficient access control scheme with outsourcing and attribute revocation for fog-enabled E-health. *IEEE Access*, 2021, vol. 9, pp. 13789–13799. https://doi.org/10.1109/access.2021.3052247
3. Chauhan R., Kaur H., Chang V. An optimized integrated framework of big data analytics managing security and privacy in healthcare data. *Wireless Personal Communications*, 2021, vol. 117, no. 1, pp. 87–108. https://doi.org/10.1007/s11277-020-07040-8
4. Maathavan K.S.K., Venkatraman S. A secure encrypted classified electronic healthcare data for public cloud environment. *Intelligent Automation & Soft Computing*, 2022, vol. 32, no. 2, pp. 765–779. https://doi.org/10.32604/iasc.2022.022276
5. Rani M., Guleria K., Panda S.N. Blockchain technology novel prospective for cloud security. *Proc. of the 2022 10th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, 2022, pp. 1–6. https://doi.org/10.1109/ICRITO56286.2022.9964666
6. Xi P., Zhang X., Wang L., Liu W., Peng S. A review of blockchain-based secure sharing of healthcare data. *Applied Sciences*, 2022, vol. 12, no. 15, pp. 7912. https://doi.org/10.3390/app12157912
7. Wu Y., Zhang L., Berretti S., Wan S. Medical image encryption by content-aware DNA computing for secure healthcare. *IEEE Transactions on Industrial Informatics*, 2023, vol. 19, no. 2, pp. 2089–2098. https://doi.org/10.1109/tii.2022.3194590
8. Mani V., Manickam P., Alotaibi Y., Alghamdi S., Khalaf O.I. Hyperledger healthchain: patient-centric IPFS-based storage of health records. *Electronics*, 2021, vol. 10, no. 23, pp. 3003. https://doi.org/10.3390/electronics10233003
9. Sivan R., Zukarnain Z.A. Security and privacy in cloud-based e-health system. *Symmetry*, 2021, vol. 13, no. 5, pp. 742. https://doi.org/10.3390/sym13050742
10. *Recent Advances in Blockchain Technology: Real-World Applications* / ed. by S.K. Panda, V. Mishra, S.P. Dash, A.K. Pani. Springer, 2023. XXIX, 317 p. https://doi.org/10.1007/978-3-031-22835-3
11. Masud M., Gaba G.S., Choudhary K., Alroobaea R., Hossain M.S. A robust and lightweight secure access scheme for cloud based E-healthcare services. *Peer-to-peer Networking and Applications*, 2021, vol. 14, no. 5, pp. 3043–3057. https://doi.org/10.1007/s12083-021-01162-x
12. Ramachandra M.N., Srinivasa Rao M., Lai W.C., Parameshachari B.D., Ananda Babu J., Hemalatha K.L. An efficient and secure big data storage in cloud environment by using triple data encryption standard. *Big Data and Cognitive Computing*, 2022, vol. 6, no. 4, pp. 101. https://doi.org/10.3390/bdcc6040101
13. Zhong H., Zhou Y., Zhang Q., Xu Y., Cui J. An efficient and outsourcing-supported attribute-based access control scheme for edge-enabled smart healthcare. *Future Generation Computer Systems*, 2021, vol. 115, pp. 486–496. https://doi.org/10.1016/j.future.2020.09.021
14. Abdelfattah S., Baza M., Badr M.M., Mahmoud M.M., Srivastava G., Alsolami F., Ali A.M. Efficient search over encrypted medical data with known-plaintext/background models and unlinkability. *IEEE Access*, 2021, vol. 9, pp. 151129–151141. https://doi.org/10.1109/access.2021.3126200
15. Ambika K., Moses M.B. TAR-AFT: A Framework to secure shared cloud data with group management. Intelligent. *Automation & Soft Computing*, 2022, vol. 31, no. 3, pp. 1809–1823. https://doi.org/10.32604/iasc.2022.018580

Литература

1. Pai M.M.M., Ganiga R., Pai R.M., Sinha R.K. Standard electronic health record (EHR) framework for Indian healthcare system // Health Services and Outcomes Research Methodology. 2021. V. 21. N 3. P. 339–362. https://doi.org/10.1007/s10742-020-00238-0
2. Zhao J., Zeng P., Choo K.K.R. An efficient access control scheme with outsourcing and attribute revocation for fog-enabled E-health // IEEE Access. 2021. V. 9. P. 13789–13799. https://doi.org/10.1109/access.2021.3052247
3. Chauhan R., Kaur H., Chang V. An optimized integrated framework of big data analytics managing security and privacy in healthcare data // Wireless Personal Communications. 2021. V. 117. N 1. P. 87–108. https://doi.org/10.1007/s11277-020-07040-8
4. Maathavan K.S.K., Venkatraman S. A secure encrypted classified electronic healthcare data for public cloud environment // Intelligent Automation & Soft Computing. 2022. V. 32. N 2. P. 765–779. https://doi.org/10.32604/iasc.2022.022276
5. Rani M., Guleria K., Panda S.N. Blockchain technology novel prospective for cloud security // Proc. of the 2022 10th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO). 2022. P. 1–6. https://doi.org/10.1109/ICRITO56286.2022.9964666
6. Xi P., Zhang X., Wang L., Liu W., Peng S. A review of blockchain-based secure sharing of healthcare data // Applied Sciences. 2022. V. 12. N 15. P. 7912. https://doi.org/10.3390/app12157912
7. Wu Y., Zhang L., Berretti S., Wan S. Medical image encryption by content-aware DNA computing for secure healthcare // IEEE Transactions on Industrial Informatics. 2023. V. 19. N 2. P. 2089–2098. https://doi.org/10.1109/tii.2022.3194590
8. Mani V., Manickam P., Alotaibi Y., Alghamdi S., Khalaf O.I. Hyperledger healthchain: patient-centric IPFS-based storage of health records // Electronics. 2021. V. 10. N 23. P. 3003. https://doi.org/10.3390/electronics10233003
9. Sivan R., Zukarnain Z.A. Security and privacy in cloud-based e-health system // Symmetry. 2021. V. 13. N 5. P. 742. https://doi.org/10.3390/sym13050742
10. Recent Advances in Blockchain Technology: Real-World Applications / ed. by S.K. Panda, V. Mishra, S.P. Dash, A.K. Pani. Springer, 2023. XXIX, 317 p. https://doi.org/10.1007/978-3-031-22835-3
11. Masud M., Gaba G.S., Choudhary K., Alroobaea R., Hossain M.S. A robust and lightweight secure access scheme for cloud based E-healthcare services // Peer-to-peer Networking and Applications. 2021. V. 14. N 5. P. 3043–3057. https://doi.org/10.1007/s12083-021-01162-x
12. Ramachandra M.N., Srinivasa Rao M., Lai W.C., Parameshachari B.D., Ananda Babu J., Hemalatha K.L. An efficient and secure big data storage in cloud environment by using triple data encryption standard // Big Data and Cognitive Computing. 2022. V. 6. N 4. P. 101. https://doi.org/10.3390/bdcc6040101
13. Zhong H., Zhou Y., Zhang Q., Xu Y., Cui J. An efficient and outsourcing-supported attribute-based access control scheme for edge-enabled smart healthcare // Future Generation Computer Systems. 2021. V. 115. P. 486–496. https://doi.org/10.1016/j.future.2020.09.021
14. Abdelfattah S., Baza M., Badr M.M., Mahmoud M.M., Srivastava G., Alsolami F., Ali A.M. Efficient search over encrypted medical data with known-plaintext/background models and unlinkability // IEEE Access. 2021. V. 9. P. 151129–151141. https://doi.org/10.1109/access.2021.3126200
15. Ambika K., Moses M.B. TAR-AFT: A Framework to secure shared cloud data with group management // Intelligent Automation & Soft Computing. 2022. V. 31. N 3. P. 1809–1823. https://doi.org/10.32604/iasc.2022.018580

Authors

Hema Ambiha Aravindakshan — PhD, Researcher, Sri Vasavi College, Erode, 636316, India, https://orcid.org/0009-0000-7495-5107, hemaambiha@gmail.com

Pragaladan Rengasamy — PhD, Associate Professor, Head, Sri Vasavi College, Erode, 636316, India, SC 57193059430, https://orcid.org/0009-0007-9407-3591, pragaladanr@gmail.com

Авторы

Аравиндакшан Хема Амбиха — PhD, исследователь, Колледж Шри Васави, Ироду, 638316, Индия, https://orcid.org/0009-0000-7495-5107, hemaambiha@gmail.com

Ренгасами Прагаладан — PhD, доцент, руководитель, Колледж Шри Васави, Ироду, 638316, Индия, SC 57193059430, https://orcid.org/0009-0007-9407-3591, pragaladanr@gmail.com

Received 07.12.2023
Approved after reviewing 25.03.2024
Accepted 16.05.2024

Статья поступила в редакцию 07.12.2023
Одобрена после рецензирования 25.03.2024
Принята к печати 16.05.2024