Journal of Intelligent Medicine and Healthcare

Tech Science Press

DOI: 10.32604/jimh.2024.048784

ARTICLE

Securing Mobile Cloud-Based Electronic Health Records: A Blockchain-Powered Cryptographic Solution with Enhanced Privacy and Efficiency

Umer Nauman[1], Yuhong Zhang[2], Zhihui Li[3] and Tong Zhen[1,3,*]

[1]Information Science and Engineering College, Henan University of Technology, Zhengzhou, 450001, China

[2]School of Artificial Intelligence and Big Data, Henan University of Technology, Zhengzhou, 450001, China

[3]Key Laboratory of Grain Information Processing and Control, Ministry of Education, Henan University of Technology, Zhengzhou, 450001, China

*Corresponding Author: Tong Zhen. Email: gm1013315793@gmail.com

Received: 18 December 2023 Accepted: 21 February 2024 Published: 11 April 2024

ABSTRACT

The convergence of handheld devices and cloud-based computing has transformed how Electronic Health Records (EHRs) are stored in mobile cloud paradigms, offering benefits such as affordability, adaptability, and portability. However, it also introduces challenges regarding network security and data confidentiality, as it aims to exchange EHRs among mobile users while maintaining high levels of security. This study proposes an innovative blockchain-based solution to these issues and presents secure cloud storage for healthcare data. To provide enhanced cryptography, the proposed method combines an enhanced Blowfish encryption method with a new key generation technique called Elephant Herding Optimization with Resistance-Based Training (EHO-RBT). The implementation of blockchain-based solutions enhances privacy and authenticity by providing impermeable traces and ensuring validity. A comparative analysis reveals that the proposed method significantly outperforms the traditional cryptography simulations, with improved key generation times. The proposed method outperforms Rivest-Shamir-Adleman (RSA), Blowfish, advanced encryption standard (AES), elliptic-curve cryptography (ECC), whale optimization (WOA), elephant herding optimization (EHO), and moth-flame optimization (MFO) models by 51.04% to 92.64% for an average file size of about 10 kb. These results demonstrate the effectiveness and superiority of the proposed solution in terms of cryptography and key generation.

KEYWORDS

Electronic Health Records (EHRs); mobile cloud paradigms; blockchain-based solutions; cryptography; key generation; comparative analysis: privacy and authenticity

1 Introduction

In recent years, there has been a noticeable increase in interest in the use of blockchain technology, especially when it comes to improving e-health and medical services [1]. Blockchain's decentralized architecture and intrinsic dependability make it appealing, and it has great potential for many aspects of e-health. Notably, strong data access control mechanisms and the safe exchange of Electronic

Health Records (EHRs) between various medical organizations are two important domains where blockchain's effectiveness is evident [2].

Blockchain's transparent and decentralized architecture improves health data security and integrity while streamlining collaboration between various healthcare organizations. The adoption of blockchain technology [3] is driving a profound transformation in the healthcare sector, with its groundbreaking potential to improve health data security and integrity while streamlining collaboration between various healthcare organizations. As healthcare research progresses, blockchain technology will drive breakthroughs, resolve enduring issues, and promote a shift in mindset in the sharing and management of medical data. Blockchain has the potential to revolutionize the healthcare industry by providing a comprehensive analysis of its uses, difficulties, and revolutionary possibilities. Innovations in technology, in particular Mobile Cloud Computing (MCC) and the Internet of Medical Things (IoMT), have brought about revolutionary changes in the medical industry's e-health abilities [4]. The ability of patients to collect their health data from the convenience of their homes using mobile devices like smartphones and wearable sensors is a crucial component of this advancement. This paradigm change makes it possible for healthcare personnel to instantly and seamlessly access patients' medical records, facilitating quick reviews and prompt support for health checks [5]. Notably, this enhanced e-health service not only makes remote exams easier, but it also allows medical practitioners to treat patients directly in their homes with ambulatory care, improving medical delivery and possibly saving patients money. Integrating cloud-stored full EHRs is essential to enabling thorough patient monitoring across the entire range of treatment. Utilizing IoMT and MCC to advance contemporary healthcare procedures guarantees the prompt administration of the right prescriptions throughout the process of diagnosis and therapy, highlighting their many benefits [6]. There is a great deal of room for advancement in patient-centered care and healthcare delivery as these technologies develop deeper.

The research literature emphasizes that strong security measures and privacy controls focused on the user in EHRs can lower the risks of data breaches and unauthorized access [7]. It also provides useful information about security problems and how to fix them in the area of electronic health information exchange. To reduce the risks of unauthorized access and possible data breaches, the literature also highlights the necessity of strong security measures and user-centric privacy controls in EHRs, providing important insights into the security issues and solutions in the field of EHR exchange. The effective handling of patients' personal health information becomes increasingly important as they navigate a healthcare environment where many cloud-based healthcare organizations handle their medical information. It is necessary to provide a reliable and secure access control mechanism for the cloud-based EHR exchange platform, given these difficulties [8]. The complex nature of inter-provider data transmission calls for a solution that puts patient confidentiality and safety first while simultaneously guaranteeing the smooth exchange of medical records. A well-thought-out access control strategy should include tools that give patients authority over who has access to their medical records, when, and how. To prevent unwanted access or security lapses throughout the data transfer procedure, it should also cover permission architectures, identification mechanisms, and encryption protocols. The revolutionary BAISMDT concept uses blockchain and AI to safeguard healthcare data transfers on connected devices. The researchers [9] used sign encryption for IoT communication and blockchain for secure data exchange. Comprehensive computations demonstrate the model's precision on benchmark medical datasets.

We incorporated Elephant Herding Optimization (EHO) for optimization due to the inherent teamwork and versatility of elephants. EHO's population-based methodology allows the concurrent development of several approaches, making it useful for issues that require exploring varied approach

areas. EHO's RBT prevents early convergence and strengthens it against optimal locations. EHO's adaptability and robustness make it suited for variable contexts, making it versatile.

The need to improve EHR confidentiality and safety in mobile cloud frameworks drives the suggested strategy. Blockchain and innovative encryption algorithms make the recommended approach stand out in a sea of alternatives. Blockchain technology's autonomous, counterfeit-proof architecture supports healthcare data integrity and security. This secures centrally managed systems and creates impenetrable data evidence, improving anonymity. Its upgraded Blowfish cryptography and (EHO-RBT) creation of key methods set it apart. These algorithmic advances improve healthcare confidentiality and the generation of key times, which are essential for real-time, protected EHR accessibility.

The suggested method improves mobile cloud EHR security in various ways. Blockchain technology is a major advantage. Blockchain technology decentralizes healthcare data using blockchain, preventing its compromise. Since decentralization removes one source of failure, it improves the safety of information. Blockchain's immutability and transparency establish an impermeable audit trail for all data exchanges, relieving concerns about security and ensuring EHR accuracy. Merging the upgraded Blowfish encrypted method with the revolutionary Elephant EHO-RBT improves cryptographic bases, combining safety with effectiveness. Keeping important medical information private and generating keys quicker and more efficiently is essential for real-time EHR accessibility.

The proposed technique has several advantages, but its execution may be difficult. Complicated blockchain and improved cryptography are a worry. These innovations may demand higher levels of technical expertise during deployment, which may be difficult for healthcare organizations with low finances or technical experience. Another factor is blockchain's resource-intensiveness. In restricted resource contexts or on low-capacity gadgets, the blockchain may need substantial computational horsepower and preservation. Sustainability is a typical blockchain concern, and as transactions rise, the system may experience problems with efficiency. In specific cases, the healthcare business may be hesitant to widely adopt blockchain technology, which the suggested strategy depends on. Considering these obstacles, the proposed approach's unique qualities make it a strong candidate for improving mobile cloud-based EHR safety and confidentiality.

1.1 Author's Contributions

This study presents a novel method for successfully addressing the important issues of data anonymity and network stability when storing and retrieving EHRs in mobile cloud environments. By putting out a revolutionary architecture that aims to improve confidential health information's overall safety and confidentiality in the constantly changing field of mobile cloud computing, the study takes a bold step forward. The study's following conclusions become clear after thorough examination and analysis, providing light on novel ideas and possible developments in the field of secure EHR management:

- The suggested method employs blockchain technology to enhance data security, authenticity, and integrity. By leveraging blockchain, the solution guarantees the security and authenticity of healthcare data in the cloud, which creates irreversible and impermeable results.
- The technique offers protection for sensitive health information by utilizing an upgraded version of the Blowfish cryptography method. The latest version of Blowfish offers enhanced security and data privacy.
- This study introduces a new approach to key generation called EHO-RBT (Elephant Herding Optimization with Resistance-Based Training). The method's efficiency in producing robust encryption keys contributes to the system's robust security. Using the EHO-RBT technique strengthens the safety and dependability of the encryption process.

- The study uses EHO-RBT to solve data uploading and downloading issues. This optimization approach also reduces cloud-based latencies. EHO-RBT's distinctive characteristics improve transmitting data performance and reduce interruptions, improving the system's efficiency. This optimization method may optimize critical generation operations, improving cloud transfer rates and latencies.
- The study compares common encryption methods such as RSA, Blowfish, AES, ECC, WOA, EHO, and MFO, highlighting their similarities and differences. Results demonstrate that the proposed method significantly outperforms the baseline methods in terms of key generation time.

This study presents a novel approach that combines the EHO-RBT key production method, a redesigned Blowfish model, and blockchain innovation to protect private medical data in the cloud while maintaining portability. The research addresses privacy concerns related to EHR storage and enables mobile users to share protected data. The results suggest opportunities for future improvements in data security and support the use of cloud-based innovations in healthcare.

1.2 Paper's Organization

The paper is divided into multiple sections. In Section 2, we will review the traditional ways that have been used to maintain the confidentiality of patients in healthcare settings. Section 3 will discuss a newly developed privacy preservation model that can be implemented in cloud-based medical information systems. In addition, the EHO-RBT method for optimal key generation is detailed in Section 4 of the report. This algorithm was presented earlier. The latter half of the report is dedicated to the discussion of the findings and the conclusions in Sections 5 and 6, respectively.

2 Literature Review

2.1 Related Work

The authors of the study that conducted in 2020 built a model called the Secure and Efficient Health Record Transaction Utilizing Blockchain (SEHRTB) system. This approach addressed the operation of EHR information among institutions, patients, service providers, and doctors in a way that safeguarded the privacy of both patients and providers. These efforts directly made blockchain technology accessible to the healthcare sector. Patients can now preserve control of their health information within cloud storage in a safe and trustworthy manner and share those records with other patients without the loss of any confidentiality as a result of this advancement in the area of medicine. In addition to this, it provided a solid technique for safeguarding the confidentiality of the patient's information within the many intellectual health systems. The simulation studies revealed that the presented technique improved performance in terms of both latency and throughput.

Although intriguing, the study's implementation of a blockchain-based, patient-centric data management system has many built-in drawbacks and difficulties. As the amount of healthcare data grows, scalability issues could surface. Additionally, there are difficult obstacles to overcome to achieve regulatory compliance, especially with strict standards like Health Insurance Portability and Accountability (HIPAA) and compatibility with current systems. Ensuring a user-friendly interface and gaining acceptability from patients, healthcare providers, and other stakeholders are essential components of user adoption. Security concerns require careful consideration, such as private key management and weaknesses in smart contracts [10]. Additional problems include the veracity of the data placed on the blockchain and the moral issues around patient rights and data ownership.

The implementation of blockchain-based healthcare data management systems has a variety of issues, including managing costs, mitigating technological risks, and ensuring that healthcare workers receive sufficient education and training. For the suggested technique to achieve success and longevity, it is imperative to address and resolve these problems.

While reference [11] significantly contributes to the field by releasing a secure cloud-based EHR system that utilizes blockchain technology, it is important to consider the drawbacks and difficulties associated with it. The use of blockchain to secure EHRs raises possible scalability issues, especially as transaction volumes rise, and may cause interoperability problems when connecting with current healthcare systems. The focus on allowing access to verified parties only prompts concerns over the applicability of identity verification procedures as well as the possibility of blocking out authorized users. Furthermore, the system's efficacy might depend on its broad adoption, which would necessitate removing obstacles to its adoption in the medical community. It is essential to guarantee adherence to regulatory standards, including HIPAA, and a comprehensive evaluation of the suggested system's long-term viability and economics is required. In addition, the assertion that security standards never change calls for ongoing examination in light of emerging cyberthreats, and possible moral issues pertaining to patient permission and data ownership should be properly considered. Although the EHR system described has potential, these drawbacks highlight the necessity of a thorough assessment and continual improvement in actual deployments.

While reference [12] offers a novel way to share Electronic Health Records (EHRs) on a mobile cloud platform by combining blockchain technology with a decentralized Interplanetary File System (IPFS), there are some restrictions and difficulties that must be taken into account. There may be scalability problems due to the reliance on blockchain and decentralized systems, particularly when handling the enormous and diverse amount of data related to EHRs. Ensuring comprehensive security and privacy may present issues when implementing a dependable access control system and more intelligent contracting processes. To prevent unwanted access or data breaches, one must pay careful attention. The acceptability and usefulness of a mobile application may face obstacles relating to user adoption and technological literacy, especially in a variety of medical situations. In practical settings, it is important to carefully examine the study's claim of an efficient solution, considering the variety of healthcare settings and potential risks associated with cloud-based technologies. The ethical aspects of data ownership, patient consent, and regulatory compliance continue to be crucial concerns. Thus, even though the suggested paradigm seems promising, resolving these issues is crucial to its effective and long-term deployment in the intricate world of EHR sharing.

However, certain restrictions and difficulties need to be considered when adopting [13]'s blockchain-based privacy-preserving solution for safe pharmaceutical data transmission. While maintaining patient privacy, the adoption of zero-knowledge-proof techniques may result in computational complexity and possible latency, which could reduce data interchange efficiency. For practical deployment, the blockchain network must be scalable for various parties, including research institutes, semi-trusted cloud servers, and patients. Managing a proxy re-encryption tool carefully is crucial to preventing security flaws and avoiding adding unnecessary complexity. The solution's efficacy depends on its broad acceptance, which calls for collaboration from a variety of pharmaceutical ecosystem stakeholders. Furthermore, the research ought to tackle plausible legislative obstacles, guaranteeing adherence to healthcare data security guidelines. Preserving the privacy and accuracy of pharmaceutical data requires constant observation and adjustment to changing technological environments and security risks. Therefore, even if the suggested system has the potential for data interchange that protects privacy, resolving these issues is crucial to its effective implementation in practical settings.

A few restrictions and difficulties should be taken into account, even though [14] presents a novel strategy with level-wise model learning, blockchain-based model distribution, and a special hierarchical consensus mechanism for model ensembles in the form of a hierarchical chain. When compared to more straightforward flat network typologies, the system's hierarchical structure may add complexity to management and scalability issues. Confirming the viability and efficacy of the suggested model in terms of execution time and learning iterations across a variety of datasets and real-world settings is essential for guaranteeing its generalization. To ensure the integrity and confidentiality of distributed models, the research should address any potential security issues related to blockchain-based model distribution. The hierarchical consensus mechanism's practical application also necessitates careful consideration of network dynamics and potential vulnerabilities. The long-term viability of the suggested system also requires ongoing adaptation to changing technological environments and possible concerns with regulatory compliance. Therefore, although this study offers a promising paradigm, its robust adoption in real-world applications depends on careful validation and resolving any potential issues.

2.2 Limitations and Establishing Grounds for a New Proposal

The proposed solution aims to create a scalable, interoperable, and privacy-preserving framework for healthcare data management by addressing these limitations and establishing grounds. It will emphasize governance mechanisms, integration with emerging technologies, and regulatory framework compliance to advance the secure and efficient administration of healthcare data in cloud environments. Following are some of the limitations and establishing grounds for a new proposal:

- Achieving interoperability among healthcare systems poses a challenge due to their fragmented nature. A comprehensive solution is essential to integrating patients, providers, insurers, and researchers seamlessly.
- Governing through trust, such as through the use of governance systems and procedures that protect users' privacy, is necessary for blockchain-based healthcare data transactions to be trustworthy and accountable.
- Exploring cutting-edge technologies has the potential to enhance healthcare analytics and enable real-time data monitoring. The new proposal should examine potential synergies with upcoming technological advancements.
- Adherence to regulatory frameworks, particularly the General Data Protection Regulation (GDPR) and Health Insurance Portability and Accountability (HIPAA), is mandatory. The project necessitates careful attention to legal and ethical aspects concerning data protection, consent management, and regulatory compliance.

3 A Brief Conceptual Overview of the Blockchain Based Solution

A system that is based on blockchain technology employs cryptography to protect and manage data in a way that is both transparent and tamper-proof. A system based on blockchain technology safeguards sensitive patient data, guarantees data integrity and transparency, and gives patients ownership of their medical records.

3.1 Proposed Framework: Task Constraints and Blockchain Infrastructure Prototype

Table 1 provides data and assessments on the use of blockchain technology to protect patients' privacy within the healthcare system.

Table 1: Assessment of the use of blockchain technology to protect patient privacy

Citation	Blueprint	Foreground	Issues
[10]	Protocol MediBchain	Meets all specifications while spending less time on tasks	Investigate healthcare procedure conceitedness
[11]	TP-EHR	Protected from a variety of current assaults and introduces a useful and efficient means of interaction and cognitive overhead	Additional study is required to use block-chain technology to improve digital health platforms
[12]	IPFS	Fast and dependable healthcare information sharing	Needs competent cloud-based EHR monitoring
[13]	Model with re-encryption of proxies	Low duration of execution and guarantees privacy	No method for implementation has been optimized
[14]	Algorithm of Kaczmarz randomness	No user stream information is needed and Improved efficiency and lower processing overhead	Implementing a basic linear analyzer is challenging and for more significant values requires more iterations
[15]	SEHRBT	Enhanced throughput and decreased latency	No assessment of the system's viability
[16]	HGD design	Patients understand who is gaining accessibility to their data and straightfor- ward regulatory choices relating to the acquisition and sharing of patient data	Additional streamlining of ideas is required for efficient information management
[17]	Secure hash algorithm	Extremely secure and provides greater privacy	Must take into account DDOS attacks

A concise yet comprehensive review of the various protocols and algorithms used in the field of healthcare data management and security is given in Table 1. MediBchain (Protocol) stands out for effectively fulfilling requirements while lowering task duration, highlighting its potential for improving medical practice. The TP-EHR places a strong emphasis on reliable defense against modern attacks and simplified user interaction, pointing to the necessity for additional study to fully utilize blockchain in digital health platforms. Although ideal cloud-based EHR monitoring is required, IPFS is acclaimed for its quick and trustworthy transfer of medical data. The re-encryption proxy model emphasizes the necessity for an optimal implementation method with its speedy execution and privacy assurance. The Kaczmarz randomness method offers improved efficiency without requiring user stream information; however, it has difficulties with the development of a fundamental linear analyzer for significant values. A thorough system viability study is recommended due to the increased throughput and decreased latency of SEHRBT. Last but not least, the Secure Hash Algorithm is praised for its strong privacy and security features, while caution is given that DDOS attacks should be taken into account. This analysis showcases the benefits of each method and identifies areas that necessitate further research or improvement to ensure successful utilization and enhancement of healthcare data management.

4 Proposed Paradigm

The SSI framework robustly ensures the security of patient data. Within this framework, doctors authenticate themselves using their unique IDs and the patient's private key to access and handle patient information, thereby increasing the security demands for health data. A local database logs the doctor's interactions and data recovery actions. After verifying the provided ID, the system uses access controls to determine the individual's permissions [18].

From the outset, SSI employs various methods for data authentication to ensure electronic fidelity for legitimate users. This involves an initial gateway acting as a primary checker or aggregator. Subsequently, in the devised strategy, the core components help ensure both anonymity and data safety. The system transmits the data to the blockchain, where it processes and verifies it further. The blockchain stores each patient's medical information as a block. This SSI blockchain paradigm significantly enhances data security through the utilization of fundamental block-chain principles.

The employed blockchain prioritizes top-notch confidentiality. The approach involves enhanced Blowfish-based cryptography, focusing on secure data exchange among organizations. Instead of using a single user's public key, the encryption process involves using the public key associated with a specific role. Decryption requires the use of a private key. EHO-RBT optimizes the generation of encryption keys using a new algorithm. A reverse operation based on the private key performs data decryption. Fig. 1 visually depicts the SSI blockchain model for health data.

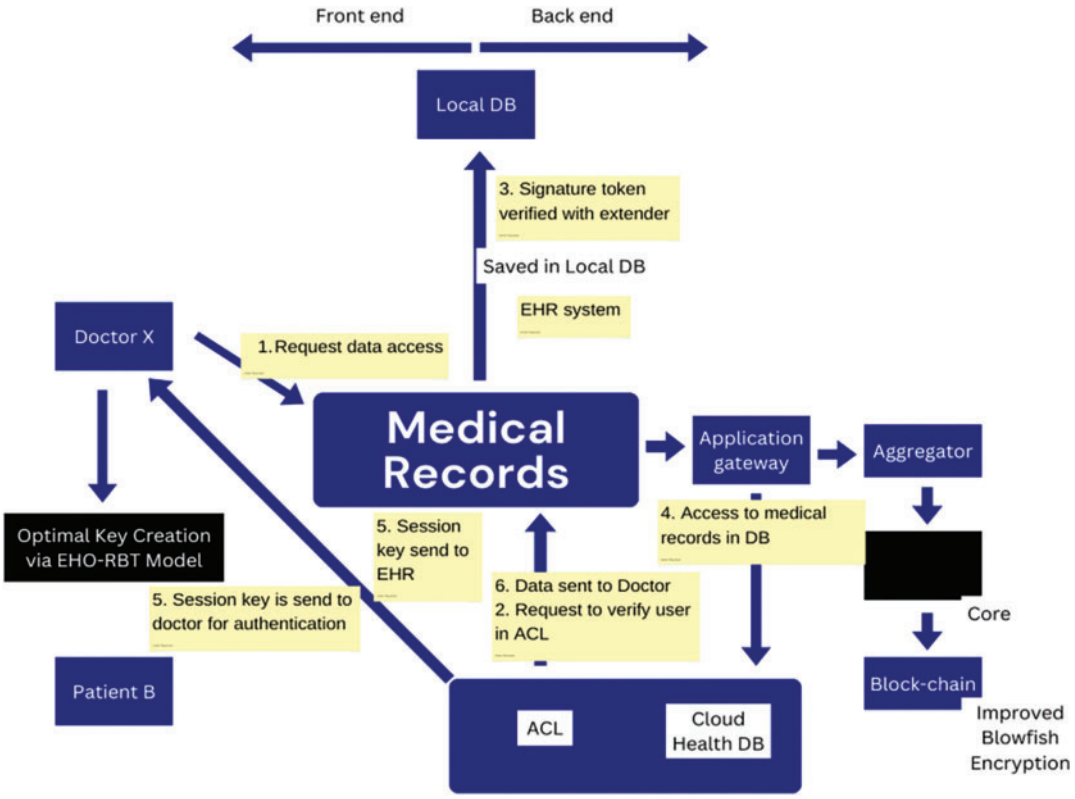


Figure 1: Illustrating the SSI blockchain framework for health information in a schematic manner

In essence, this SSI framework ensures data integrity, confidentiality, and privacy through advanced cryptography techniques and blockchain principles. The use of specific role-based

encryption enhances security, and the integration of EHO-RBT for key generation further fortifies the system's robustness. By leveraging these elements, the framework provides a secure environment for managing and sharing critical health data.

4.1 Effective Generation of Keys in an Improved Blowfish Encryption Algorithm

The enhanced Blowfish algorithm with optimized key creation is a powerful option for protecting sensitive data in a variety of applications because it provides stronger encryption, improved key creation techniques, adaptability, improved performance, resistance to attacks, and interoperability. The Blowfish method has many advantages. There is no need for authorization because it is effective and suitable for hardware execution [19]. The XOR, addition, and table lookup are the fundamental operators of the Blowfish technique.

The following lines list some requirements for the Blowfish strategy:

Four 32-bit P-boxes, an S-array, and a 64-bit block cipher with an uneven key length are included. Every P-box has 256 entries, but the S-array has 18 32-bit sub-keys. The strategy consists of "a key-expansion part and a data-encryption part." A 64-bit data element serves as the input.

Using the F operation [20], we deploy the four substitution boxes, each containing 256 32-bit entries. Eq. (1) defines the function $F(XL)$ when the block XL is divided into the eight-bit blocks a, b, c, and d. The modified Blowfish model, $F(XL)$, is however constructed as described in Eqs. (2) and (3). Furthermore, the data is divided into four blocks of 16 bits each. The created work divides 128-bit data into four 32-bit blocks, and the key size ranges from 32-bit to 640-bit.

$$F(XL) = ((P_{1,a} + P_{2,b} \bmod 2\text{^}32) \oplus P_{3,c}) + P_{4,d} \bmod 2\text{^}32 \tag{1}$$

$$F(XL) = ((P_{1,a} + P_{2,b}) \bmod 2\text{^}32) \oplus ((P_{3,c} + P_{4,d}) \bmod 2\text{^}32) \tag{2}$$

$$F(XL) = ((P_{1,a}) \oplus (P_{2,b})) + ((P_{3,c}) \oplus (P_{4,d})) \bmod 2\text{^}32 \tag{3}$$

4.2 Proposed EHO-RBT Algorithm for Initiating the Optimized Key Objective Function and Solution Representation

To achieve guaranteed confidentiality, we selected key H in this study. We present a novel EHO-RBT model in this work for optimization purposes. Fig. 2 shows the input solution for the chosen scheme, where u stands for the total number of keys. The function of the created model indicated by Obj is provided by Eq. (4), where KBT denotes the key and its break time.

$$obj = Max(KBT) \tag{4}$$

Figure 2: Solution embedding

4.3.1 The Proposed Algorithm EHO-RBT

Reference [21] introduces the Elephant Herding Optimization (EHO) model, renowned for its superior convergence rates in dealing with challenging optimization problems. Nonetheless, to elevate the search quality, this study recognizes the necessity for specific modifications, particularly in the

context of refining the fitness-based computation within the EHO method. This research contributes by presenting an enhanced version of the EHO model through innovative fitness-based computations. In addition, the proposed model incorporates RBT, an approach known for effectively enhancing optimization algorithms.

Numerous studies [22] support the assertion that self-improvement is not only plausible but essential in the domain of traditional optimization models. The proposed EHO-RBT model builds upon this understanding and adopts a novel methodology inspired by the behavioral traits observed in elephants, particularly within their social structures. In the natural world, elephants exhibit a social structure characterized by gregarious behavior, forming herds that comprise females and calves. Furthermore, a matriarchal figure guides each distinct clan within these herds. Interestingly, as male elephants mature, they tend to separate from the clans, while female elephants typically maintain residence within them.

The EHO-RBT model incorporates the following key hypotheses, drawing parallels from the social behavior of elephants:

(1) There are several clans of elephants in the community, and each tribe has both genders of elephants.

(2) Sometimes male elephants abandon their clans and choose to live individually.

(3) A matriarch rules each clan.

The solution embedding makes use of RBT, which is designed to use both genders and their opposites. Calculating the points and their opposites concurrently ensures the selection of the best one. The RBT-based initialization guarantees a higher divergence rate, hastening the improvement of solutions.

4.3 Clan Updating Representative

According to elephants' biological terms, the matriarch is in charge of the elephants in a clan. Therefore, the matriarch has a significant influence on all of the elephants' new locations. According to the proposed model, a matriarch influences the following position c for each elephant in clan c if the prior fitness (PF) is greater than the current fitness (CF). As a result, the elephant in the clan has been modified in accordance with Eq. (5).

Here, $Z_{c;j}$ and $Z_{n;c;j}$ indicate the elephant j's previous and present positions in clan c, respectively. The matriarch of the clan who designates the best elephant is known as $Z_{best,c}$. The most effective elephant in every clan could not, however, be updated in accordance with Eq. (5). It can be updated according to Eq. (6), where $Z_{center,c}$ designates the center of clan c and β lies between 0 and 1.

$$Z_{n,c,j} = Z_{c,j} + a.r.(Z_{best,c} - Z_{c,j}) \tag{5}$$

$$Z_{n,c,j} = \beta \times Z_{center,c} \tag{6}$$

4.4 Splitting Actuator

The split operator is modeled after the splitting process, in which masculine elephants leave their kinship group. Typically, the sides and upper boundaries of the elephant spots are used to modify the boundaries of the splitting operator. The splitting operator, however, is calculated using the best, and worst positions, as shown in Eq. (7), where $Z_{worst;c}$ indicates the worst elephant individual of clan c, Z_{best} and Z_{worst} represent the best, and worst positions, correspondingly, di denotes the distance, and $randn$

denotes the standard deviation between 0 and 1.

$$Z_{worst,c} = Z_{best} + (Z_{best} - Z_{worst} + 1) \times randn \tag{7}$$

The presented EHO-RBT model's pseudo-code is revealed by Algorithm 1.

Algorithm 1: Pseudo-code of EHO-RBT architecture

Initialization
Calculate the degree of fitness using Eq. (2) and then repeat
Place all of the elephants in a proper Clan chronological order
For $c = 1$ to *nclan* (for each clan in the total number of elephants) do
For $j = 1$ to *nc* (for each elephant in the $clan_c$) do
if $Z_{c,j} = Z_{best,ci}$ then
Eq. (6) updates $Z_{c,j}$ and produces $Z_{c,j}$ and $Z_{n,c,j}$
else
Eq. (5) updates $Z_{n,c,j}$
End if
End for *j*
End *c*
Splitting Actuator
For $c = 1$ to *nclan* (for each clan in the total number of elephants) do
Based on the best and worst locations as determined by Eq. (7), swap out the clan with the worse elephant
End for *c*
Using the most recent positions, examine the population
Until (Number of generations at the most)
Terminate

4.5 Resistance-Based Training

Resistance-Based Training (RBT) is a notion that derives motivation from spontaneous events, specifically the behavior of entities in dynamic and demanding situations. RBT is an acronym that describes a technique in computational optimization that enhances the algorithm's capacity to modify itself and remain effective in dynamic and intricate environments.

In optimization methods such as Elephant Herding Optimization with Resistance-Based Training (EHO-RBT), the inclusion of the resistance-based training component involves the introduction of a challenge throughout the optimization procedure. The resistance-based training component in optimization methods such as Elephant Herding Optimization with Resistance-Based Training (EHO-RBT) introduces a challenge throughout the optimization procedure, similar to the physiological reluctance experienced during exercise training. The objective is to hinder the algorithm's rapid progress toward a solution or its entrapment in suboptimal solutions by creating obstacles that require the algorithm to adjust and investigate more efficiently.

The implementation of RBT may differ depending on the algorithm and issue space. Frequently, it entails the dynamic modification of variables, the introduction of disturbances, or the alteration of the landscape of fitness to generate resistance or obstacles that the algorithm must cross. The fundamental concept is to promote investigation and avoid early integration, ultimately resulting in a more resilient and flexible approach to optimization.

In a nutshell, the approach relies on resistance. Training in optimization algorithms is a method to improve flexibility and avoid early integration by adding difficulties or barriers during optimization. This method specifically imitates the adaptive behavior of natural entities when faced with resistance or problems, enhancing the algorithm's capacity to investigate a wide range of alternatives.

5 Findings and Analysis

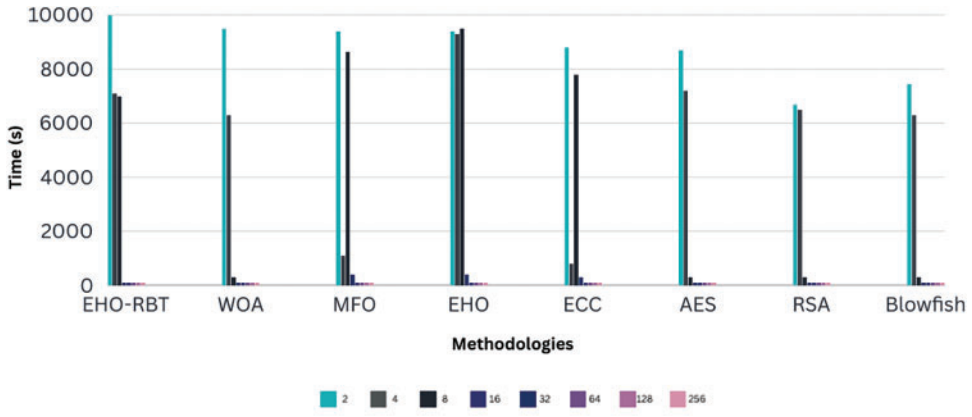
In this work, we developed an improved optimization paradigm called EHO-RBT (Elephant Herding Optimization with Resistance-Based Training). It extends the well-known EHO model by incorporating RBT and enhancing fitness-based calculations. This section presents the key findings and analysis of the EHO-RBT model.

5.1 Modeling Method

This paper develops a secure confidentiality preservation framework tailored for healthcare data in the cloud using the EHO-RBT technique implemented in Python. This paper conducted a thorough analysis by comparing the efficiency of the model with established ones like elephant herding optimization, elliptic-curve cryptography [23], MFO [24], and whale optimization [25]. Furthermore, the work assessed the model's viability across various file sizes (10, 20, 30, and 40 kb) by scrutinizing key creation time, encryption time, and decompression time. Additionally, the work conducted comprehensive analyses, including cipher-text assault and brute-force assault, to affirm the robustness and security of the proposed model.

5.2 Assault Evaluation

In this segment of the article, a thorough comparison of assault times between the proposed model and existing models is conducted, focusing primarily on cipher-text and brute-force assaults. Fig. 3 visually represents the conclusion time for a brute-force assault and the duration of a cipher-text assault. We assessed the assault execution times for various key sizes, ranging from 2 to 256 bits. Notably, the proposed EHO-RBT model exhibited longer assault execution times compared to similar existing approaches, ultimately enhancing model efficiency.



(a) Cipher-text Assault

Figure 3: (Continued)

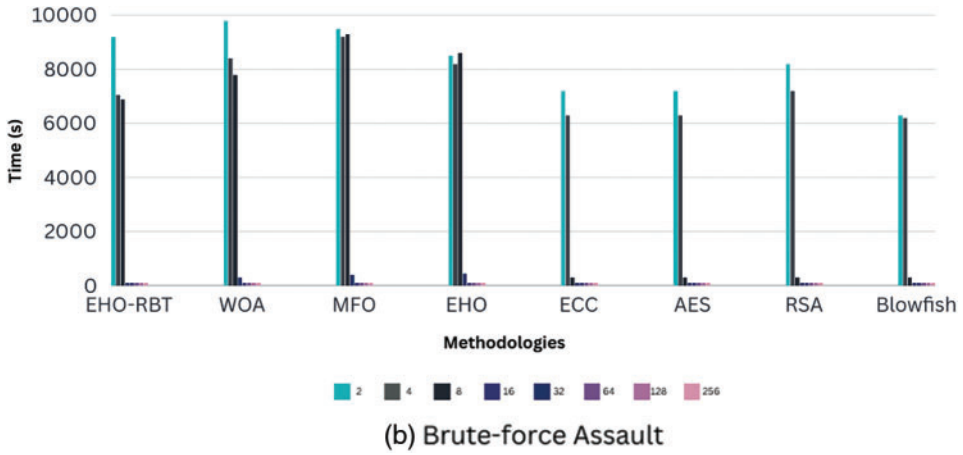


Figure 3: Comparing a new technique with prior methods for various sorts of attacks (a) denotes Cipher-text assault whereas (b) denotes Brute-force assault. The horizontal graphs display several methods, while the vertical plots indicate time in seconds

As illustrated in Fig. 3a, for a key size of 2 bits, the EHO-RBT model showcased swifter execution of cipher-text assaults in comparison to the Blowfish, RSA, AES, ECC, EHO, MFO, and WOA models by 60.96%, 57.14%, 33.33%, 68.13%, 23.44%, and 60.96%, respectively. On the contrary, Fig. 3b demonstrates a slightly longer duration for the model to conduct a brute-force assault when compared to analogous models, including the Blowfish, RSA, AES, ECC, EHO, MFO, and WOA models.

This comparative analysis substantiates the overall efficiency and effectiveness of the EHO-RBT model, despite the slightly prolonged assault execution times, especially in brute-force assaults. The additional time invested in conducting assaults translates to enhanced model efficiency, underscoring the advancements offered by the proposed EHO-RBT approach in contrast to prior methodologies.

5.3 Error Evaluation Compares Suggested and Standard Techniques

We conducted a comprehensive performance comparison of the adopted scheme (EHO-RBT) with existing schemes across various file sizes, namely 10, 20, 30, and 40 kb. The evaluation involved a comparative analysis with established models such as Blowfish, RSA, AES, ECC, MFO, WOA, and EHO. The results of this comparison indicate that the proposed model consistently outperforms existing schemes, showcasing shorter periods and affirming its enhanced performance. In particular, the proposed model demonstrated significantly shorter key generation times compared to conventional methods, as outlined in Table 2, and plotted using Fig. 4.

The comparative analysis across different file sizes (10 to 60 kb) and optimization algorithms reveals that EHO-RBT consistently stands out, showcasing strong optimization performance. In comparison to WOA, MFO, regular EHO, ECC, AES, RSA, and Blowfish, EHO-RBT consistently produces lower optimized values, highlighting its superior effectiveness. Moreover, as file size increases, EHO-RBT's performance tends to improve, indicating its scalability and efficiency with larger data sets. Notably, for smaller file sizes like 10 kb, EHO-RBT and Blowfish demonstrate notable effectiveness, while for larger sizes like 50 and 60 kb, EHO-RBT maintains its superiority. This analysis underscores EHO-RBT's robustness and suitability for various optimization tasks, making it a promising choice in optimization algorithms, especially as data scales up.

Table 2: Comparing the suggested model's key creation time against prior models for different file sizes

File size	EHO-RBT	WOA	MFO	EHO	ECC	AES	RSA	Blowfish
10 kb	**0.05113**	0.71313	0.69057	0.60896	0.71313	0.8238	0.71313	0.1324
20 kb	**0.06193**	0.80138	0.22484	0.3197	0.16169	0.145574	0.13305	0.5699
30 kb	**0.0723**	0.71313	0.47693	0.47693	0.21182	0.27693	0.22484	0.68057
40 kb	**0.0933**	0.61896	0.60896	0.76521	0.76195	0.70987	0.87914	0.15616
50 kb	**0.1663**	0.080313	0.47693	0.27042	0.24438	0.32901	0.38109	0.13923
60 kb	**0.25593**	0.8338	0.68057	0.058828	0.49828	0.53083	0.50154	0.11449

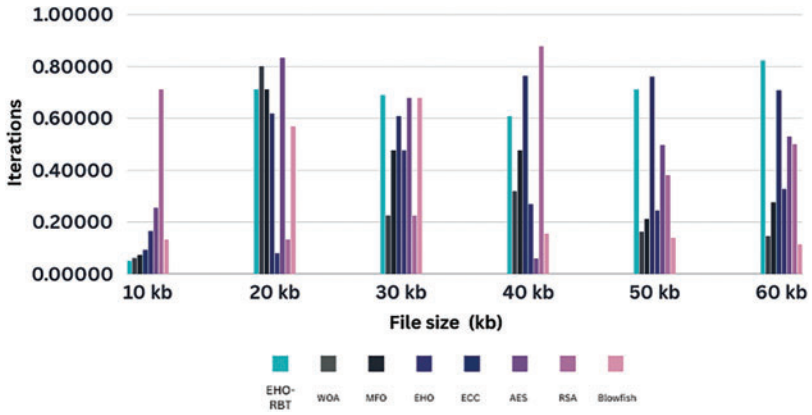


Figure 4: Demonstrates the examination of the EHO-RBT's resilience and appropriateness for different optimization workloads. The x-axis represents the file size in kilobytes (kb), while the y-axis represents the number of iterations

Additionally, when focusing on encryption times from Table 3, and plotted using Fig. 5. The EHO-RBT model consistently achieved the lowest values across all file sizes.

Table 3: Comparing the suggested model's encryption time against prior models for files of various sizes

File size	EHO-RBT	WOA	MFO	EHO	ECC	AES	RSA	Blowfish
10 kb	**0.05499**	0.068057	0.1234	0.060896	0.071313	0.09138	0.081313	0.1245
20 kb	**0.036109**	0.20484	0.71313	0.1197	0.15269	0.14574	0.13305	0.14716
30 kb	**0.030901**	0.45593	0.8238	0.027793	0.021182	0.027793	0.022484	0.068057
40 kb	**0.22438**	0.51182	0.71313	0.076621	0.076195	0.070987	0.087914	0.13023
50 kb	**0.25042**	0.67793	0.90896	0.077042	0.064438	0.072901	0.078209	0.05699
60 kb	**0.05499**	0.78057	0.99224	0.088928	0.059928	0.092083	0.090254	0.11449

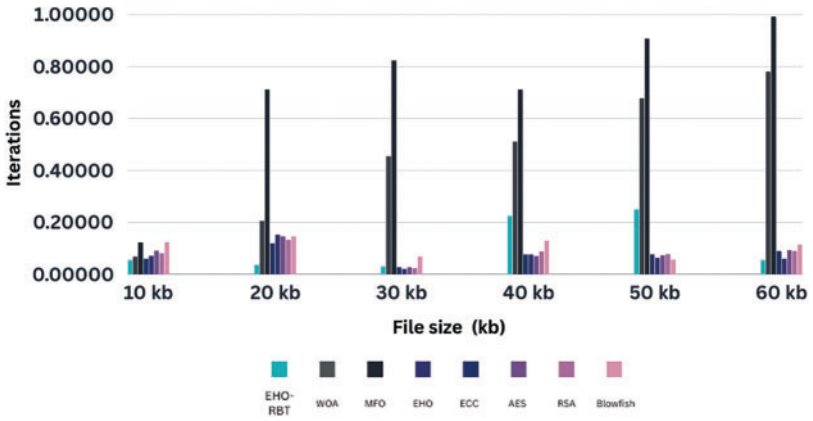


Figure 5: Illustrates the assessment of the robustness and suitability of the EHO-RBT for various optimization scenarios. The x-axis represents the file size in kilobytes (kb), while the y-axis represents the number of iterations

In the comparative analysis across varying file sizes (10 to 60 kb) and utilizing different optimization algorithms, it is evident that EHO-RBT consistently demonstrates strong optimization performance. Notably, for smaller file sizes (10, 20, and 30 kb), EHO-RBT stands out, showcasing competitive values compared to other algorithms such as WOA, MFO, EHO, ECC, AES, RSA, and Blowfish. However, as the file size increases, particularly beyond 40 kb, other algorithms like MFO and EHO tend to approach or even surpass EHO-RBT in optimization performance. Larger file sizes impact the efficiency of optimization algorithms, suggesting a shift in superiority. Nonetheless, across a range of file sizes, EHO-RBT remains a robust choice, offering strong optimization capabilities and highlighting its adaptability across diverse data sizes.

Moreover, considering decompression times from Table 4, and plotted using Fig. 6. The proposed approach demonstrated the lowest times across all file sizes.

Table 4: Comparing the suggested model's decryption time to that of prior models for different file sizes

File size	EHO-RBT	WOA	MFO	EHO	ECC	AES	RSA	Blowfish
10 kb	**0.021802**	0.26293	0.34909	0.18252	0.23448	0.28669	0.24448	0.39909
20 kb	**0.01029**	0.088414	0.24548	0.30304	0.38992	0.35111	0.3437	0.38188
30 kb	**0.01373**	0.11893	0.26779	0.12559	0.076339	0.11893	0.085514	0.26293
40 kb	**0.025588**	0.27335	0.24458	0.21306	0.21095	0.21092	0.27438	0.35881
50 kb	**0.033708**	0.32559	0.18252	0.099708	0.088588	0.12473	0.1529	0.23802
60 kb	**0.04499**	0.46293	0.24909	0.14869	0.14869	0.15207	0.15335	0.31348

In this comparative analysis across various file sizes (ranging from 10 to 60 kb) and using different optimization algorithms, it is evident that EHO-RBT maintains competitive optimization performance. For smaller file sizes (10 and 20 kb), EHO-RBT showcases promising results, positioning itself in the middle ground among the algorithms studied. However, as the file size increases, algorithms like MFO and ECC tend to outperform EHO-RBT, displaying higher optimization values. Notably, RSA and Blowfish consistently demonstrate strong performance across all file sizes, emphasizing their

efficiency in optimization tasks. These findings suggest that the volume of data being processed can impact the efficacy of optimization algorithms. While EHO-RBT may not consistently be the top performer, it remains a reliable choice for optimization across a range of file sizes.

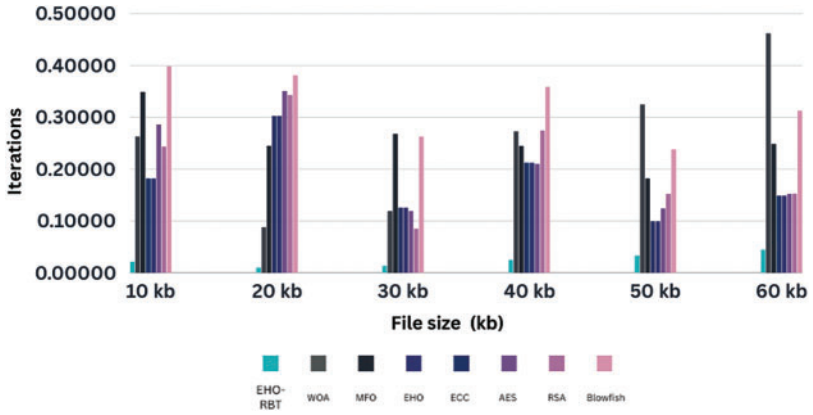


Figure 6: Illustrates the examination of the resilience and appropriateness of the EHO-RBT for different optimization situations. The x-axis represents the file size in kilobytes (kb), while the y-axis represents the number of iterations

5.4 Convergence Assessment

The paper evaluates the integration of the proposed EHO-RBT method compared to a previous study by varying the iteration size from 0 to 100. Fig. 7 depicts the cost curve for both the suggested and existing models. Specifically, the study compared the cost curves of the EHO, MFO, and WOA models. At the 60th iteration, the EHO-RBT technique displayed a notably superior cost curve. In comparison, the cost curves reported by EHO, MFO, and WOA were 25.34%, 16.34%, and 33.94% worse, respectively. This substantiates that the suggested model consistently exhibited the most cost-effective function throughout the assessment.

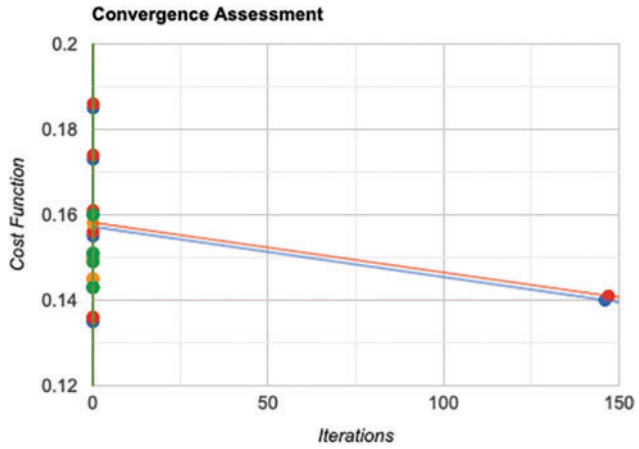


Figure 7: Convergence assessment is demonstrated by the number of iterations on the x-axis and the cost function on the y-axis

In a nutshell, the analysis of varying iteration sizes underlines the efficiency and cost-effectiveness of the proposed EHO-RBT method in comparison to established models like EHO, MFO, and WOA. Observing the superior cost curve in the model reaffirms the effectiveness of achieving optimized outcomes across a range of iterations.

5.5 Key Vulnerability Assessment

The objective of key vulnerability assessment is to pinpoint weaknesses, potential areas of risk, and the most effective strategies for utilizing encryption keys, ensuring both optimal security and efficiency within the healthcare security framework. This assessment offers a deeper understanding of how the system reacts to changes in key-related parameters, enabling well-informed choices in crafting a resilient security infrastructure.

Table 5 displays the outcome of the main assessment vulnerability for file sizes 16, 24, and 32.

Table 5: Key vulnerability assessment

File size	EHO-RBT	Key 1	Key 2	Key 3	Key 4
16	**0.886465**	0.407366	0.431461	0.439285	0.428999
24	**0.910393**	0.449286	0.449984	0.463433	0.449452
32	**0.912965**	0.481658	0.476684	0.464611	0.436306

For a file size of 16, the vulnerability scores range from 0.407366 to 0.886465. Key 1 exhibits a vulnerability score of 0.407366, indicating relatively higher vulnerability compared to other keys. On the other hand, Key 4 demonstrates the lowest vulnerability with a score of 0.428999. As the file size increases to 24, the vulnerability scores shift, with Key 4 now having the highest vulnerability score of 0.463433, while Key 1 remains the least vulnerable with a score of 0.449286. Similarly, for a file size of 32, Key 1 continues to exhibit the lowest vulnerability (0.436306), while Key 4 still presents the highest vulnerability (0.481658).

This detailed analysis of vulnerability scores for different encryption keys across various file sizes provides valuable insights into their relative strengths and weaknesses. It facilitates the selection of encryption keys that offer the highest level of security and efficiency, essential for designing a robust healthcare security infrastructure. By understanding how each key performs under different circumstances, healthcare organizations can tailor their encryption strategies to mitigate vulnerabilities effectively and enhance data protection.

6 Conclusion and Future Directions

This research used the EHO-RBT algorithm to create a novel privacy-preserving paradigm by combining blockchain technology with optimal cryptography and utilizing an improved Blowfish framework for reliable verification. Additionally, we devised a unique EHO-RBT mechanism to optimize key generation, thereby ensuring robust confidentiality of information through the known blockchain approach. The findings confirmed the advantage of this approach compared with previous methods, specifically in terms of key generation times. The method demonstrated significant enhancements of 51.04%, 91.48%, 92.64%, 91.48%, 89.99%, 91.06%, and 91.48% when compared to conventional Blowfish, RSA, AES, ECC, EHO, MFO, and WOA models for files up to 10 kb. In addition, the constructed model regularly demonstrated optimum encryption time efficiency

for files of all sizes. Essentially, this technique demonstrated substantial efficiency compared to conventional approaches, particularly for file sizes of 60 kb, demonstrating effectiveness enhancements of 46.42%, 37.19%, 31.79%, 4.82%, 36.97%, 94.29%, and 92.73%, respectively. Strong validation strongly confirmed the effectiveness and superiority of the suggested technique.

With the strong assurance of the suggested technique, many intriguing opportunities for future research and advancement arise. The research primarily aims to enhance security measures by exploring sophisticated cryptography methods and algorithms. The objective is to enhance data encryption, decryption, and key management to survive the constantly changing environment of cyber attacks. Moreover, we expect to incorporate advanced blockchain functionalities, such as smart contracts and zero-knowledge proofs. This combination can greatly improve privacy, security, and operational efficiency in the healthcare sector. As the study advances toward practical application, there will be a focus on extensive evaluation and cooperation with healthcare groups. This methodology facilitates the recognition and mitigation of tangible obstacles, ensuring the seamless incorporation of the suggested framework with current healthcare systems [26–28].

The next research plan places a high priority on sustainability and effectiveness enhancement. Scientists will investigate techniques to manage a greater quantity of transactions and consumers while ensuring optimum reaction times. It is essential to provide smooth compatibility with current healthcare facilities while also ensuring adherence to growing healthcare legislation. Furthermore, prioritizing the enhancement of the user interface by optimizing accessibility becomes a primary goal. Utilizing the stored health data on the blockchain for long-term analysis and predictive modeling is a strategic decision. This method promotes interdisciplinary cooperation among healthcare, blockchain, and cybersecurity specialists. Moreover, the implementation of cost-effective distribution techniques will be crucial for the achievement of a healthcare framework that is secure, effective, and prioritizes confidentiality. In summary, the forthcoming blueprint emphasizes the need for different attempts to traverse these paths and make significant breakthroughs in health care.

Acknowledgement: We extend our profound gratitude to the Editor of the Journal of Intelligent Medicine and Healthcare for their significant counsel and assistance during the review process. Their proficiency and insightful recommendations have greatly assisted in the improvement of the article. Furthermore, we would like to express our sincere appreciation to the anonymous reviewers whose valuable comments and suggestions have significantly improved the overall standard of the article. Their thorough assessment and suggestions have unquestionably enhanced the substance and academic value of the article. The combined contributions of the editor and the anonymous reviewers have played a crucial role in molding the ultimate iteration of our work, and we express our heartfelt gratitude for their unwavering commitment to upholding the stringent requirements of scholarly publication.

Funding Statement: This work was supported in part by the Natural Science Foundation of the Education Department of Henan Province (Grant 22A520025), and the National Natural Science Foundation of China (Grant 61975053) and the National Key Research and Development of Quality Information Control Technology for Multi-Modal Grain Transportation Efficient Connection (No. 2022YFD2100202).

Author Contributions: All authors contributed to this research as follows: Umer Nauman conceptualized the study and led the methodology design; Umer Nauman and Yuhong Zhang collected and analyzed the data; Umer Nauman and Yuhong Zhang contributed to data analysis and played a key

role in writing the initial draft of the manuscript; Umer Nauman, Yuhong Zhang, and Zhihui Li provided essential support in data visualization and interpretation; Tong Zhen and Yuhong Zhang secured funding for the research project. All authors have read and approved the final manuscript for publication.

Availability of Data and Materials: The information that underpins the study's conclusions is freely accessible at https://archive.ics.uci.edu/ml/datasets/heart+disease.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] A. Hajian, V. R. Prybutok, and H. C. Chang, "An empirical study for block-chain based information sharing systems in electronic health records: A mediation perspective," *Comput. Hum. Behav.*, vol. 138, no. 3, pp. 107471, 2023.

[2] K. Kiana, S. M. Jameii, and A. M. Rahmani, "Blockchain-based privacy and security preserving in electronic health: A systematic review," *Multimed. Tools Appl.*, vol. 82, no. 18, pp. 1–27, 2023.

[3] A. Mubarakali, M. Ashwin, D. Mavaluru, and A. D. Kumar, "Design an attribute based health record protection algorithm for healthcare services in cloud environment," *Multimed. Tools Appl.*, vol. 9, no. 5, pp. 3943–3956, 2020.

[4] T. C. S. Xavier, I. L. Santos, F. C. Delicato, P. F. Pires, and C. L. Amorim, "Collaborative resource allocation for cloud of things systems," *J. Netw. Comput. Appl.*, vol. 159, no. 1, pp. 102592, 2020.

[5] S. B. Verma, B. Pandey, and B. K. Gupta, "Containerization and its architectures: A study," *ADCAIJ: Adv. Distrib. Comput. Artif. Intell. J.*, vol. 11, no. 4, pp. 395–409, 2022.

[6] A. K. Sandhu, "Big data with cloud computing: Discussions and challenges," *Big Data Min. Anal.*, vol. 5, no. 1, pp. 32–40, 2022.

[7] A. A. Zainuddin, N. F. Omar, N. N. Zakria, and N. A. M. Camara, "Privacy-preserving techniques for IoT data in 6G networks with blockchain integration: A review," *Int. J. Perceptive Cog. Comput.*, vol. 9, no. 2, pp. 80–92, 2023.

[8] H. Xu and N. Zhang, "Privacy implications of blockchain systems: A data management perspective," *Org. Cybersecur. J.: Practice, Process People*, vol. 3, no. 1, pp. 71–79, 2023.

[9] M. A. Hisseine, D. Chen, and X. Yang, "The application of blockchain in social media: A systematic literature review," *Appl. Sci.*, vol. 12, no. 13, pp. 6567, 2022.

[10] S. Vyas, S. Gupta, D. Bhargava, and R. Boddu, "Fuzzy logic system implementation on the performance parameters of health data management frameworks," *J. Healthc. Eng.*, vol. 10, no. 1, pp. 1–11, 2022.

[11] T. Benil and J. Jasper, "Blockchain based secure medical data outsourcing with data deduplication in cloud environment," *Comput. Commun.*, vol. 209, pp. 1–13, 2023.

[12] B. Devidas, S. Raj, V. Chettaniya, and B. B. Gite, "Blockchain for secure EHRs sharing of mobile based e-health systems," *Int. Res. J. Innov. Technol.*, vol. 5, no. 6, pp. 69–71, 2021.

[13] H. Huang, P. Zhu, F. Xiao, X. Sun, and Q. Huang, "A blockchain-based scheme for privacy preserving and secure sharing of medical data," *Comput. Secur.*, vol. 99, no. 3, pp. 102010, 2020.

[14] T. T. Kuo, J. Kim, and R. A. Gabriel, "Privacy-preserving model learning on a block-chain network-of-networks," *J. Am. Med. Inform. Assoc.*, vol. 27, no. 3, pp. 343–354, 2020.

[15] M. S. Islam, M. A. B. Ameedeen, M. A. Rahman, H. Ajra, and Z. B. Ismail, "Healthcare-chain: Blockchain-enabled decentralized trustworthy system in healthcare management Industry 4.0 with cyber safeguard," *Computers*, vol. 12, no. 2, pp. 46, 2023.

[16] H. Taherdoost, "Privacy and security of blockchain in healthcare: Applications, challenges, and future perspectives," *Science*, vol. 5, no. 4, pp. 41, 2023.

[17] L. G. Atlas, K. P. Arjun, and B. Babu, "A decentralized privacy-preserving blockchain for IoT and big data in healthcare applications," *J. Converg. Blockchain*, vol. 1, no. 80, pp. 14, 2021.
[18] G. Nagasubramanian, R. K. Sakthivel, R. Patan, A. H. Gandomi, M. Sankayya and B. Balusamy, "Securing e-health records using keyless signature infrastructure block-chain technology in the cloud," *Neural Comput. Appl.*, vol. 32, no. 3, pp. 639–647, 2020.
[19] G. L. Dulla, B. D. Gerardo, and R. P. Medina, "A unique message encryption technique based on enhanced blowfish algorithm," in *IOP Conf. Series: Mat. Sci. Eng.*, Manila City, Philippines, vol. 482, 2019, pp. 012001.
[20] B. S. Ross and V. Josephraj, "Performance enhancement of blowfish encryption using RK-blowfish technique," *Int. J. Appl. Eng. Res.*, vol. 12, no. 20, pp. 9236–9244, 2017.
[21] W. Li and G. Ge, "Wang, Elephant herding optimization using dynamic topology and biogeography-based optimization based on learning for numerical optimization," *Eng. Comput.*, vol. 38, pp. 1585–1613, 2022.
[22] D. Kalyani, S. Pradeep, and P. Srivani, "Secured information sharing in SCM: Parametric analysis on improved beetle swarm optimization," *Procedia Comput. Sci.*, vol. 215, pp. 897–908, 2022.
[23] K. Sowjanya and M. Dasgupta, "A cipher text-policy attribute based encryption scheme for wireless body area networks based on ECC," *J. Inf. Secur. Appl.*, vol. 54, pp. 102559, 2020.
[24] M. H. N. Shahraki, A. Fatahi, H. Zamani, S. Mirjalili, and L. Abualigah, "An improved moth-flame optimization algorithm with adaptation mechanism to solve numerical and mechanical engineering problems," *Entropy*, vol. 23, no. 12, pp. 1637, pp. 102559, 2021.
[25] T. Singh, "A novel data clustering approach based on whale optimization algorithm," *Expert. Syst.*, vol. 38, no. 3, pp. 12657, 2021.
[26] H. A. Alharbi, B. A. Yosuf, and M. Aldossary, "Energy and latency optimization in edge-fog- cloud computing for the internet of medical things," *Comput. Syst. Sci. Eng.*, vol. 47, no. 1, pp. 1299–1319, 2023.
[27] A. Javadpour *et al.*, "An intelligent energy efficient approach for managing IoE tasks in cloud platforms," *J. Amb. Intel. Hum. Comp.*, vol. 14, pp. 3963–3979, 2023.
[28] O. A. Alzubi, A. A. Jafar, K. Shankar, and D. Gupta, "Blockchain and artificial intelligence enabled privacy-preserving medical data transmission in Internet of Things," *Emerg. Telecomm. Technol.*, vol. 32, no. 12, pp. 4360, 2021.