Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2024.046265

ARTICLE

Fortifying Healthcare Data Security in the Cloud: A Comprehensive Examination of the EPM-KEA Encryption Protocol

Umi Salma Basha[1], Shashi Kant Gupta[2], Wedad Alawad[3], SeongKi Kim[4,*] and Salil Bharany[5,*]

[1]Computer Science and Information Technology, Jazan University, Jazan, Saudi Arabia

[2]CSE, Eudoxia Research University, New Castle, USA

[3]Department of Information Technology, College of Computer Science, Qassim University, Buraydah, Saudi Arabia

[4]National Center of Excellence in Software, Sangmyung University, Seoul, Korea

[5]Department of Computer Science and Engineering, Lovely Professional University, Phagwara, Punjab, India

*Corresponding Authors: SeongKi Kim. Email: skkim9226@gmail.com; Salil Bharany. Email: salil.bharany@gmail.com

Received: 25 September 2023 Accepted: 11 February 2024 Published: 15 May 2024

ABSTRACT

A new era of data access and management has begun with the use of cloud computing in the healthcare industry. Despite the efficiency and scalability that the cloud provides, the security of private patient data is still a major concern. Encryption, network security, and adherence to data protection laws are key to ensuring the confidentiality and integrity of healthcare data in the cloud. The computational overhead of encryption technologies could lead to delays in data access and processing rates. To address these challenges, we introduced the Enhanced Parallel Multi-Key Encryption Algorithm (EPM-KEA), aiming to bolster healthcare data security and facilitate the secure storage of critical patient records in the cloud. The data was gathered from two categories Authorization for Hospital Admission (AIH) and Authorization for High Complexity Operations. We use Z-score normalization for preprocessing. The primary goal of implementing encryption techniques is to secure and store massive amounts of data on the cloud. It is feasible that cloud storage alternatives for protecting healthcare data will become more widely available if security issues can be successfully fixed. As a result of our analysis using specific parameters including Execution time (42%), Encryption time (45%), Decryption time (40%), Security level (97%), and Energy consumption (53%), the system demonstrated favorable performance when compared to the traditional method. This suggests that by addressing these security concerns, there is the potential for broader accessibility to cloud storage solutions for safeguarding healthcare data.

KEYWORDS

Cloud computing; healthcare data; security enhanced parallel multi-key encryption algorithm (EPM-KEA)

1 Introduction

The management, storage, and accessibility of health information has undergone a revolutionary change in today's networked world as a result of the confluence of medical care and technologies. The cloud computing and healthcare sector, which is known for its extremely sensitive and private patient records, has seen a significant upheaval [1]. The benefits of cloud computing include its scalability, accessibility, and convenience, as well as its reduced processing expenses. Healthcare is using this emerging model to streamline activities, improve patient care, and increase overall effectiveness as

cloud computing quickly grows its influence across many sectors [2]. A major milestone has been reached with the smooth transition from traditional systems to digital ones, including Electronic Health Records (EHRs), Electronic Medical Records (EMRs), Personal Health Records (PHRs), and Electronic Health Data (EHD) [3]. These digital archives contain a wealth of vital patient information, including health history, statistics, prescription pasts, immunization position, and more. Particularly cloud-based services are proven to be essential for managing medical records. They provide a safe and expandable platform for storing data, enabling access from anywhere and facilitating the entry, retrieval, and management of crucial health information for authorized healthcare workers, clients, and caregivers [4]. However, the electronic frontier comes with its own set of particular difficulties. Given the importance of patient data, security, and privacy are top priorities in the healthcare industry. Security risks loom large as data moves to the cloud. A detailed investigation of wireless network security is required since attacks on healthcare information are an unfortunate reality. Despite the evident advantages of cloud-based computing, remote storage's susceptibility to data breaches continues to be a major worry. A few instances of the hidden dangers are ransom threats, distributed denial-of-service (DDoS) attacks, and malware attacks [5].

To protect healthcare data on the cloud, stronger security protocols and cutting-edge encryption technologies are becoming more common [6]. Data security is a top goal, along with enhancing the efficiency, economy, and long-term viability of information processing. The investigation reveals the crucial role played by these cutting-edge technologies as we delve into the world of cloud-based healthcare data security, paving the way for a strong and secure healthcare ecosystem in the digital era. Adopting cutting-edge technologies for cloud security paves the way for future developments while also addressing current flaws. The use of artificial intelligence (AI) and machine learning (ML) in security measures has gained popularity as a proactive response to changing cybersecurity threats. By enabling healthcare systems to identify and stop potential security breaches in real time, these cutting-edge technologies provide proactive protection against new threats. Healthcare firms may strengthen their defenses, proactively discover weaknesses, and quickly respond to any security-related incidents by utilizing powered Artificial intelligence (AI) security solutions [7]. Sensitive patient data must be protected using an integrated approach in the ever-changing cloud healthcare data security ecosystem. The demand for robust security systems is increasing as cyber-attacks and data breaches become more complex. The dedication to data privacy and integrity is demonstrated by the use of strict protocols and encryption techniques, such as the Enhanced Parallel Multi-Key Encryption Algorithm (EPM-KEA). Healthcare providers can reduce the risks of illegal access and data exploitation by adding strong encryption measures, assuring the security and validity of medical information stored in the cloud [8].

The scientific community has paid close attention to the developing field of cloud computing, mainly because of its potential to reduce computing costs and improve operational effectiveness. The spread of cloud services in this context has become more noticeable and offers a range of advantages to different industries. However, the healthcare industry poses special difficulties, notably concerning the security of private patient information. As the healthcare sector increasingly uses digital solutions for data storage and administration, it is more important than ever to protect the security and privacy of patient records. Despite the many benefits of cloud-based systems, a key barrier that may prevent the timely processing and access of vital patient data is the computational cost associated with the use of cryptographic algorithms [9]. The use of strong encryption algorithms has become a crucial tactic to reduce the dangers related to the security of data. The objective is to strengthen the security of medical information preserved in the cloud by adding sophisticated encryption techniques, hence lowering the likelihood of illegal access and possible breaches. However given the ongoing risk of assaults on sophisticated systems, such as cloud computing facilities, a complete strategy must be developed

to tackle any possible vulnerability, especially those relating to wireless network security [10]. The creation of the Enhanced Parallel Multi-Key Encryption Algorithm (EPM-KEA) is an important advance in the effort to strengthen cloud data privacy in healthcare settings as a consequence of these difficulties. By increasing data security and availability, this ground-breaking method aims to raise the overall dependability and integrity of healthcare data kept in cloud environments. The construction of a more accessible and safe healthcare data ecosystem that ensures the privacy and safety of medical information in a cloud environment remains the primary objective of this investigation as it progresses.

This study identified a technique to improve cloud data privacy as the Enhanced Parallel Multi-Key Encryption Algorithm (EPM-KEA). This research used cryptographic algorithms to collect AIH data for efficient healthcare data security and privacy on the cloud. In this study, Z-score normalization is used as part of the preprocessing method to ensure the confidentiality and integrity of cloud-stored healthcare records. This research proposes an Enhanced Parallel Multi-Key Encryption Algorithm (EPM-KEA) to protect data in the cloud. Resolving security issues could make cloud storage an accessible option for safeguarding healthcare data. This outlook points to the potential benefits of addressing security concerns. By presenting observable proof of its effectiveness, this enhances the practical implementation of the proposed solution. The goal of the Enhanced Parallel Multi-Key Encryption Algorithm (EPM-KEA) is to improve the security of healthcare data and make it easier to store important patient information securely on cloud servers.

The remaining article is structured as follows: Part 2 presents the related works. The suggested EPM-KEA form is examined in Part 2. Results and analysis are presented in Part 3. The conclusion and probable developments are covered in Part 4.

2 Related Works

Studies using cloud computing and distributed ledgers to facilitate data sharing are discussed below. The authors of this study [11] propose a blockchain-based system for exchanging electronic health records that is both secure and respects patients' right to privacy. Once granted permission from the data owner, a requesting party may use a keyword search on the data provider's end to "find the relevant EHRs on the EHR consortium blockchain and then retrieve the re-encrypted cipher text from a cloud server." The technique achieves its data security goals, maintaining privacy and access control primarily via searchable encryption and conditional proxy re-encryption. This research [12] examines the risks to data protection solutions, privacy, and mitigation strategies specific to edge cloud computing. First, they briefly introduce edge computing, discussing its origins, definition, architecture, and numerous critical use cases. Then, the solutions based on cryptography developed to address data privacy and security concerns are outlined. This work [13] employs differential privacy to deal with the problem of learning detriment caused by noise injection into the user's data. It proposed a public cloud auditing method for smart cities that is both lightweight and privacy-preserving and does not depend on bilinear pairings. To guarantee the security and confidentiality of storage in the cloud and processing. A study [14] offered a novel anti-spoof multispectral biometric cloud-based identification technique. The answer was provided by using a multispectral palm print as a typical biometric feature between the two primary stages of the method, which are the offline registration process and the online verification procedure. It was the first to encrypt multispectral palm print characteristics and utilize them for protecting user privacy in the cloud. This study [15] introduces PPO-MACS, an outsourced multi-authority access control mechanism that is both effective and privacy-friendly. All user characteristics are changed to be anonymous and authenticable to achieve privacy maintenance. In addition, we propose verified outsourced decryption to reduce the computational burden on the end user. Protecting user anonymity when providing keys is a primary concern, thus the authors

develop a novel ABE system in this study [16]. The authors suggest a new system in which neither the attribute auditing center (AAC) nor the key generating center (KGC) can discover the user's attributes or secret key. This would greatly benefit many situations involving personal privacy, including the industrial big data scenario. They present a lightweight, private, and bilinear-pair-free public cloud auditing approach for smart cities [17]. To begin, the suggested approach does not need users to link devices and instead has a third-party auditor provide authentication metadata set on their behalf. Data privacy is safeguarded against both external auditors and cloud service providers. This new technique also lends itself to batch auditing in a multi-user setting. All public keys, revocation lists, etc., are maintained on a blockchain in this approach [18], utilizing the blockchain to conduct consistent identity authentication. The system management server generates the system settings and distributes the private keys to the COVID-19 healthcare providers and end users. The CEMRs are stored in the cloud, and the CSP creates the mediate decryption variables through policy correspondence [19], proposes an equation for decrypting cloud data, and provides a formula to perform the first and second encryption in a CRT-based lockable storage approach. Users can access the secure cloud data stored in cloud-based databases on a cloud server by including a new formula during the group key generation procedure. A study [20] proposed a method for privacy-protected data sharing for cloud-enhanced IoT that can be easily adapted to different situations. IoT users may now send encrypted messages to one another using identity-based encryption using the FPDS scheme. Finally, the IoT user may produce a delegation credential by specifying a granular access policy and then transmit that credential to the cloud to have all the encrypted data that comply with the access policy transformed into new ciphertexts understandable by the recipient. Security against attacks such as eavesdropping, masquerade, replay, and man-in-the-middle is ensured in the proposed [21] protocol. According to the results of the performance investigation, the ERFC cloud-based encryption method has lower communication and computation complexity than the currently used protocols. In this study [22], the authors focus on fixing three major flaws in the RCoM system. The article [23] introduced a model based on Genetic Algorithm (GA) to address data quality and privacy difficulties. A cryptographic method is used with GA to generate the keys for encryption and decryption to protect the privacy and quality of cloud data. Analysis of experimental findings demonstrates that the suggested approach protects user data privacy and integrity from unauthorized parties. This article [24] provides a safe and practical blueprint for detecting the confidentiality of data stored in cloud computing environments. Paper [25] evaluated encryption methods to protect or cloud-store enormous data. This project aims to improve cloud security by combining homographic and blowfish encryption. The results are based on the file's encryption, decryption times, and a mix of the homographic and blowfish algorithms. This work will be helpful in the future to improve cloud computing security. Paper [26] suggested a scenario in which the shape of individual presynaptic densities and the effectiveness of neurotransmitter release are regulated by ELP3-dependent acetylating of Bruch pilot at synapses. They resulted in improved neurotransmitter release and enhanced vesicle tethering. Paper [27] analyzed several current research on the Data Encryption Standard (DES) and Advanced Encryption Standard (AES) encryption Methodologies. AES is quicker than DES regarding encryption time, but DES is faster than AES on small files. Our testing of both methods with files of varying sizes indicates that neither is significantly superior to the other regarding decryption. The findings show that AES is an excellent effectiveness, speed, and usability encryption algorithm. Paper [28] proposed a safe and private electronic health records exchange platform based on the blockchain. More than that, they prove the security of the suggested protocol through a comprehensive security analysis, proving that our scheme provides the desired level of protection. Paper [29] proposed a Blockchain-based IoT-DT system that is safe and energy-efficient. This study could be further extended by concentrating on ordinary key creation models in the cryptography phase, data analytics models, and regular data mining techniques to handle significant data volumes. Paper [30] proposed a cloud-based system for enhancing data security. In the

future, complicated data operations will be possible due to recent technical advancements in static data, including data addition, update, and deletion.

The study [31] provided a thorough examination of blockchain's potential medical uses, focusing mainly on the in vitro fertilization (IVF) industry. The study [32] introduced the Internet of Things (IoT) concept, described its architecture, and revealed the risks and vulnerabilities of using IoT in medical settings. They also proposed a method for shielding sensitive health information in an IoT environment. The article [33] presented a potential blockchain-based healthcare delivery architecture. They proposed utilizing Ethereum smart contracts to decentralize healthcare administration and create a secure telemedicine infrastructure for patient data. Based on the existing data storage architecture, they created a multi-server search method in the research [34] provided to collaboratively carry out diagnostic institution location, medical data search, and even cross-domain data search. The study [35] provided a BPVSE, a unique, dynamic, and verifiable SE approach for cloud-assisted EHR. Some advantages of BPVSE over the current system are listed below. To begin, BPVSE utilizes blockchain and a hash-proof chain to publicly verify cloud-provided search results without needing a trusted third party. Study [36] provided new error-detection techniques that were effectively integrated into the NTT accelerator design and can identify all momentary and persistent problems. They identify the errors in such structures after recalculating and deciphering the parameters using two methodologies, namely negate and exchanging. Their techniques demonstrate good error containment for the stuck-at-failure scenario with simulations. Additionally, they put the schemes into practice using field-programmed gate arrays (FPGA) and made sure that both efficiency and execution metrics were reached with a tolerable amount of overhead. A study [37] addressed the problem at the Rochester Institute of Technology, they offered an efficient integration plan for research and education. Furthermore, through case studies involving side-channel analysis attacks, they described the outcomes of greater than a year-long application of the suggested technique at a graduate level.

Study [38] implemented in effect HW design for the Gaussian sampler and the ModFalcon authentication method. Both the SABER and Falcon variations of these techniques have been implemented on a former Xilinx field-programmable gate array (FPGA) family, and their efficiency and error coverage were evaluated. The proposed schemes have relatively low costs, and high detection of faults rates, and were therefore suitable for high efficiency and small-footprint HW executions of restricted possibilities. The deployment of assaults for 2022 winners of the NIST cryptography after the quantum competition was the focus of the study [39], which focuses on future-focused, developing safety concerns in the period after quantum. As a result, the ideas, knowledge, and debates can be used as a first measure in the direction of examining new requirements for programs spanning from the deeply entrenched technologies to the metaverse and Web 3.0. Rapid developments in quantum technology have created enormous prospects for scientific and technical advancement, but they also pose a serious threat to current security measures because it is thought that sophisticated quantum computers can defeat all established public-key cryptography techniques. Study [40] investigated two broad terms depending on artificial intelligence and the k-anonymity theory of privacy in the background, describing states of rising unpredictability by changing the quantity of entropy of a certain collection of attributes. Three more options were also looked at selecting the feature with the fewest different values, selecting the characteristic with the least entropy, and selecting the feature with the most entropy.

3 Proposed Methodology

To increase cloud data security, this study offers an Enhanced Parallel Multi-Key Encryption Algorithm (EPM-KEA) that uses encryption. Z-score normalization is used for preprocessing. The

EPM-KEA is a security method that increases data privacy retained in cloud computing environments. It is also known as EPM-KEA. Encryption is what is needed to have this done successfully. Fig. 1 demonstrates the flow of the optimized F-function with two S-boxes, one input switch out of two S-boxes, and the outputs may be merged or swapped. The result is XOR-ed with a master encryption key sub-key.

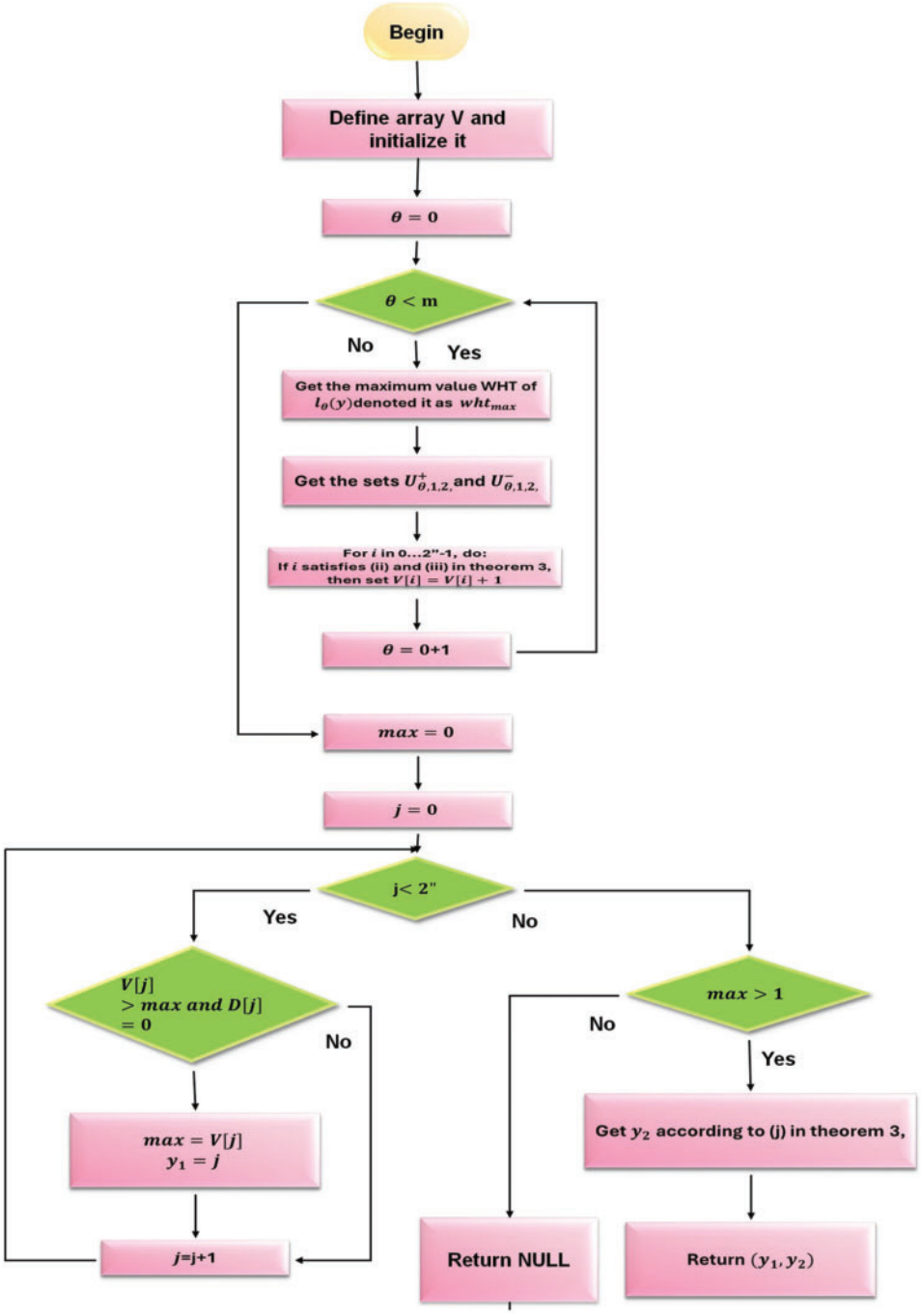

Figure 1: Optimized F-function with two S-boxes

This technique must be repeated for safe encryption numerous times, with each iteration affecting the next. The key-dependent dispersion of the XOR with sub-keys and the non-linearity and confusion of the S-boxes make the technique cryptanalysis-proof. From input transformation via S-box lookup tables through mixing and critical scheduling, the encryption method precisely monitors every step. Adopting encryption techniques primarily aims to protect or cloud-store large amounts of data. Fig. 2 illustrates the suggested methods of this study.

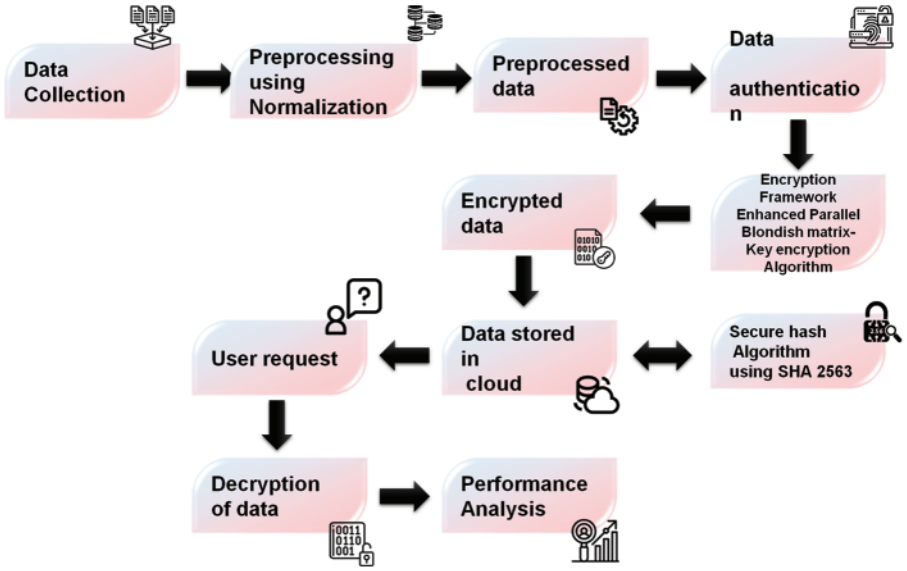

Figure 2: Suggested techniques of this study

3.1 Dataset Collection

The databases 'Authorization for Hospital Admission (AIH)' and Authorization for High Complexity Operations provide the two categories of healthcare information that constitute the source dataset used in this study: Hospitalization and high-complexity procedures. When a healthcare facility creates a request for hospitalization, a record is made in the AIH database. Its purpose is to verify the admission data, and the diagnosis is typically communicated. Therefore, although a general sense of the cost is known, hospitalization is not instantly priced. On the other hand, providers input information into the APAC database to register authorized high-complexity processes for billing. "While AIH records are stored in a unified file structure", events reported in the APAC database are categorized into six categories and stored in the appropriate database files. These categories comprise bariatric surgery, chemotherapy, medication, nephrology, radiotherapy, and miscellaneous outpatient. Public healthcare providers electronically transmit AIH and APAC files to DATASUS [41].

3.2 Preprocessing Using Z-Score Normalization

Pre-processing is the fundamental stage of data preparation, which includes organizing, sterilizing, and changing raw data to improve its quality and fit for machine learning or analysis. Z-score normalization, also known as zero-mean normalization, is achieved by taking the mean and standard deviation for each feature in the training set and dividing them by the number of components in the training data set. The mean and standard deviation for each attribute is calculated. There is a generic formula that specifies the transformation that must be made:

$$ZZ = \frac{dd - \mu\mu}{\sigma\sigma} \tag{1}$$

where d denotes the original value, or average, and the standard deviation is $\mu\mu$ and $\sigma\sigma$, respectively. Before any training can occur, the data set is utilized\using the Z-score technique. Keeping each feature's standard deviation and mean after exercise is crucial since these values may be used as weights in the system's design. We obtain pre-processed data as a result of preprocessing.

3.3 Data Authentication

The process of confirming the integrity and source of data to ensure reliability and accuracy is known as data authentication. It requires checking that the data has not been changed. Cloud authentication, which is supplied by cloud-based services, enables approved users to securely access data stored in the cloud across networks in healthcare data. The public cloud provides round-the-clock protection for the data that pertains to health coverage. In equipment failures, a power outage, or a data breach, healthcare practitioners can retrieve data straightforwardly and expediently, causing the most minor disturbance to patient care.

3.3.1 Encryption Framework Using the Enhanced Parallel Multi-Key Encryption Algorithm

The preprocessed data is now encrypted using the Enhanced Parallel Multi-Key Encryption algorithm. To protect medical data, encryption employs a combination of mathematical algorithms and a password or "key" that may be used to decode the data. The EPM-KEA algorithm is used to encrypt data, hence rendering the original data unreadable. For example, this procedure may transform a standard text into an encrypted message. The 448-bit key length of fine-tuned chaotic blowfish makes it a 64-bit block. The network has 16 Feistel nodes. The encryption key length determines algorithm security. EPM-KEA has the P-array and two 32-bit S-boxes. Each process has three parts. They are "box construction," "encryption," and "decryption."

3.3.2 Description of Epm-Kea Algorithm

- ***Sub-Key Generation (P-Array):*** The P-array has been utilized with a fixed string and Fig. 3 displays the blowfish encryption.

There are a total of 18 32-bit sub-key values in this set. Divide the critical series into 18 groups of 32 bits per each. First, the first 32-bit key (LL1) is XORed with the first P-array (OO1)value, then the second 32-bit key (LL2)with the third (LL3) value, and so on for up to 18 rounds. There are eighteen 32-bit key values for each of the eighteen 32-bit P-array values; therefore, they are XORed together. EPM-KEA is used to encrypt all zero-length strings. There are a total of 18 rounds in this procedure. A P-array is used to hold the sub-key values after that depicted in Fig. 3.

- **S-Box Preparation**

The four S-boxes need to have a connection made between them. There are 256 entries in each S-box. These values for the S-box have been encrypted with blowfish. After that, the values of the first and second S-boxes are merged, and the values of the third and fourth S-boxes are joined together. Two new S-box values are generated from the original four S-box values.

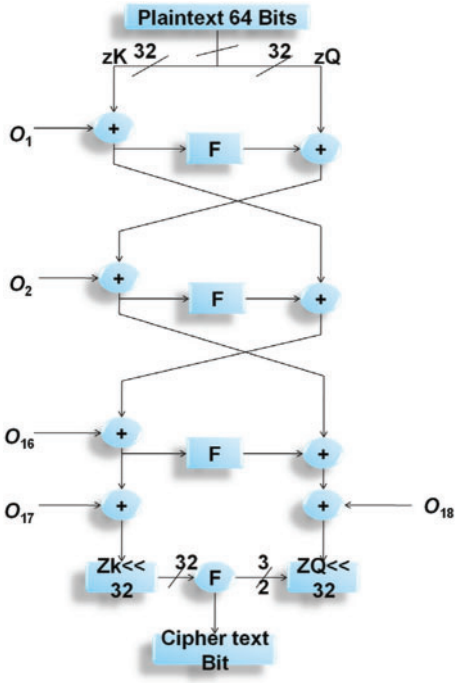

Figure 3: Blowfish encryption

- **Data Encryption**

The F-function is utilized, and there are 16 rounds of data encryption. Every match assists with a key-dependent variation and a key and data-dependent replacement of the previous round's results. At the end of each game, the right half will affect the left half, while the subkeys will affect the primary keys. Fig. 4 showcases the Blowfish algorithm. The structure being referred to here is identical to the design of EPM-KEA.

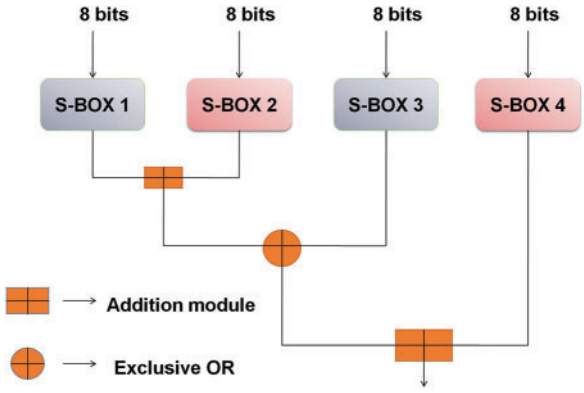

Figure 4: F-function

The significance of the irreversible function F in generating the optimal avalanche effect for a Feistel network cannot be emphasized enough. The F-function, which comprises four S-boxes, takes a 32-bit input divided into four 8-bit inputs. These four eight-bit values are combined using the addition

modulo technique before being subjected to the XOR operation. Fig. 4 provides a visual representation of the F-function.

- **Modified F-Function**

The only new addition in this release is the inclusion of S-boxes in the F-function.

The Feistel structure of the Blowfish algorithm remains unchanged, but the design of the F-function has been altered. In the Blowfish algorithm, the F-function consists of four S-boxes, whereas the EPM-KEA utilizes only two S-boxes. Fig. 5 provides a visual representation of the modified F-function.

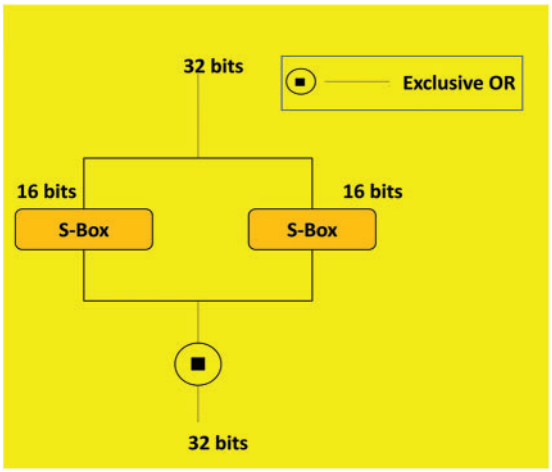

Figure 5: F-function of EPM-KEA

The following sequential steps depict how the EPM-KEA works:

- A fixed string was used to initialize the P-array and four S-boxes in the correct sequence.
- Prepare the subkeys by encrypting the key and P-array.
- Use the F-function with four S-boxes to encrypt the S-box values.
- Make two 32-bit halves of the 64-bit input data (left and right). $YYLL$ and $YYYY$ designate the left and right halves, respectively. This is done by XO Ring the 32-bit left half of the $ZZZZ$ with the sub key 001. The $ZZZZ$ is entered into the F-function.
- A pair of S-boxes composes the F-function. Splitting data into two 16-bit halves, each half is sent to one of the S boxes in the F-function.

1. The 1st and 2nd 16-bit S-boxes are now included.

2. XO Ring the 32-bit resulting bit.

3. The following is the optimized F-function: Two 16-bit halves of $UUUU$ are created: a and b, respectively.

$$FF\,(UUZZ) = FF\,(dd, cccc) = (TT1 \text{♁} TT2).\,HHHHHHHH" \text{♁} "iiiiXXOOYY$$

- F(YL) is YR with XO Red.
- When you swap values between the ZK and R values, the right half ($ZZUU$) is replaced by the left half, and the right half replaces the other half.

- The *ZZUU* and *ZZZZ* are XO Red with 0017 and 0018 after the seventeenth round, but the right and left halves are not switched.
- Finally, exclusive OR is used to combine ZZZZ and ZZUU.

Pseudo code: Optimized F-function with two S-boxes

YYLL Should be split into two 16-bit quarters, cc and dd.

$$\mathrm{FF(ZZUU)} = (\mathrm{TT0}, \mathrm{cc} \wedge \mathrm{TT1}, \mathrm{cc}) \tag{2}$$

1) Pseudo code of encryption

Split the 64-bit input data into two 32-bit parts: ZZZZ and ZZUU.
ffffHH ii = 0 ttff 16
ZZZZ IsXORed with ZZUU
Find *FF*(*YYLL*)
FF (ZZZZ) iiii XXOOYYHHdd wwiitth LLUU
Swap ZZZZ aaaadd ZZUU
SSwwaaSS ZZZZ aaaadd ZZUU
ZZUU iiii XXOOYY wwiitth OO[16]
ZZZZ iiii XXOOYYHHdd wwiitth OO[17]
FFiiaaaaFFFFFF, ccffcccciiaaHH ZZZZ aaaadd ZZUU

2) Pseudo code of decryption

Split the 64-bit input data into two 32-bit halves: *ZZZZaaaaddZZUU*
ffffHH jj = 17 ttff 1
AAZZ iiii XXOOYYHHdd wwiitth OO[ii]
FFiiaadd FF (ZZZZ)
FF (ZZZZ) iiii XXOOYYHHdd wwiitth ZZUU
SSwwaaSS ZZZZ aaaadd ZZUU
SSwwaaSS ZZZZ aaaadd ZZQ
ZZUU IISS XXOOYYHHdd wwiitth OO[1]
ZZUU iiii XXOOYYHHdd wwiitth OO[0]
CCffcccciiaaHH ZZZZ aaaadd ZZUU

3) Data stored in the cloud

To leverage users' idle hard drive space worldwide, data is stored in a distributed network, commonly referred to as the cloud. However, for those seeking an alternative to traditional cloud storage, a decentralized infrastructure can offer potential solutions to some of the challenges associated with centralized storage. This approach securely transfers the encrypted data to the cloud for storage.

4 Result and Discussion

This work presents an Enhanced Parallel Multi-Key Encryption Algorithm (EPM-KEA) that utilizes encryption to enhance cloud data security. The primary objective of adopting encryption methods is to secure and store large quantities of data on the cloud. Once security concerns are addressed, future cloud storage solutions for safeguarding healthcare data will likely be available. To compare our proposed methods with existing approaches such as Blockchain [42], IoT [43], Lamport Merkle Digital Signature (LMDS) [44], and secure Lightweight Authentication Scheme (SLAS) [45], an analysis is conducted. The parameters employed in this research include "encryption time, decryption time, execution time, security level, and energy consumption".

4.1 Encryption Time

The amount of time it takes a cryptography algorithm to transform a plain text into a cipher text is known as the encryption time of that algorithm. Table 1 and Fig. 6 represent the encryption time.

Table 1: Findings of existing and proposed methodologies for encryption time

Methods	Encryption time (s)
Blockchain [42]	55
IoT [43]	74
LMDS [44]	59
SLAS [45]	45
EPM-KEA	[Proposed]

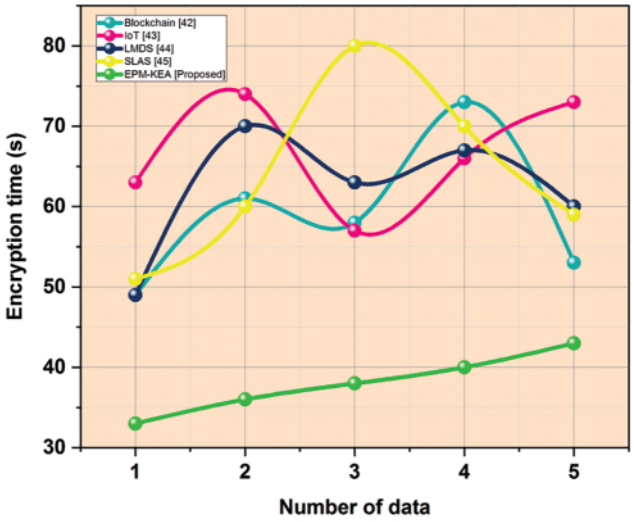

Figure 6: Encryption time

The total amount of encrypted plaintext (in bytes) divided by the encryption duration is how any encryption process' time is calculated (in ms). It shows how long the encryption technique took to build a CT from plain text. It is the difference between the beginning and finishing timings of the encryption, and also is written as

$$AA_{(aadd)} = HH'_{aa(dd)} - ff'_{gg(dd)} \tag{3}$$

where $HH'_{aa(dd)} - ff'_{gg(dd)}$ indicates the beginning and finish of the encryption process. Blockchain achieves 55 s, IoT achieves 74 s, LMDS achieves 59 s, SLAS achieves 45 s, and the proposed method EPM-KEA with 45 s.

4.2 Decryption Time

The process of decryption involves the restoration of plaintext from the received cipher text. Decryption is the term used to describe the process of returning encrypted data to its original state. Reverse encryption is a widely used practice. Since decryption necessitates a secret key or password, it

decodes encrypted content, allowing only authorized users to access it. The timing of the decryption is shown in Table 2 and Fig. 7.

Table 2: Values of decryption time

Methods	Decryption time (s)
Blockchain [42]	75
IoT [43]	58
LMDS [44]	55
SLAS [45]	60
EPM-KEA [Proposed]	**40**

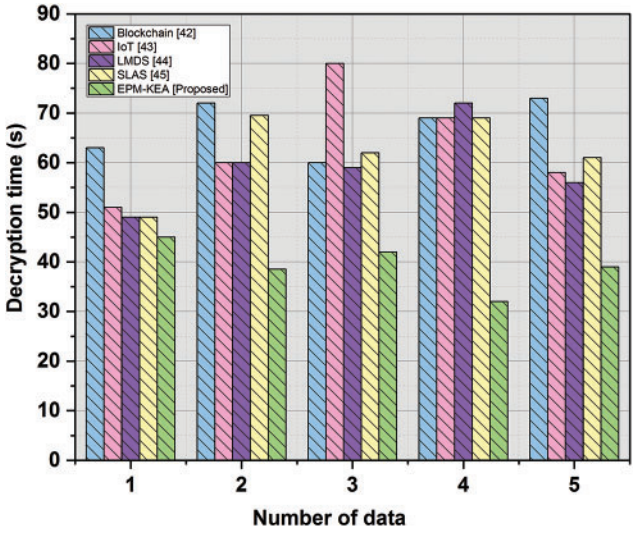

Figure 7: Decryption time

The decryption time refers to the duration required for the decryption method to produce plain text equivalent to the cipher text. It is simply the difference between the starting and ending timings of the decryption process and is expressed as such.

$$TT_{(ttdd)} = HH"_{aa(dd)} - "_{gg(dd)} \tag{4}$$

where $HH"_{aa(dd)} - "_{gg(dd)}$ denotes decryption starting time and decryption ending time. The decryption time for blockchain was estimated at 75 s. IoT was assessed using a 58-s decryption time. A 55-s decryption time for LMDS was used for evaluation. SLAS was evaluated using a 68-s decryption time.

The decryption time of 40 s was used to assess the proposed technique EPM-KEA. Comparing the suggested EPM-KEA technology to current methods like blockchain, IoT, LMDS, and SLAS, it took less time to decrypt data.

4.3 Execution Time

The duration the system carries out a task, encompassing the time spent on runtime or system functions on behalf of the study, is known as the execution time or CPU time. The implementation

determines the specific method employed to measure execution time. When calculating the full completion time of a task, the duration of runtime or network activities performed by the program is considered. The approach used to estimate the implementation determines the execution time. Table 3 and Fig. 8 illustrate the period of execution.

Table 3: Evaluation of execution time

Methods	Execution time (s)
Blockchain [42]	96
IoT [43]	89
LMDS [44]	83
SLAS [45]	73
EPM-KEA [Proposed]	**42**

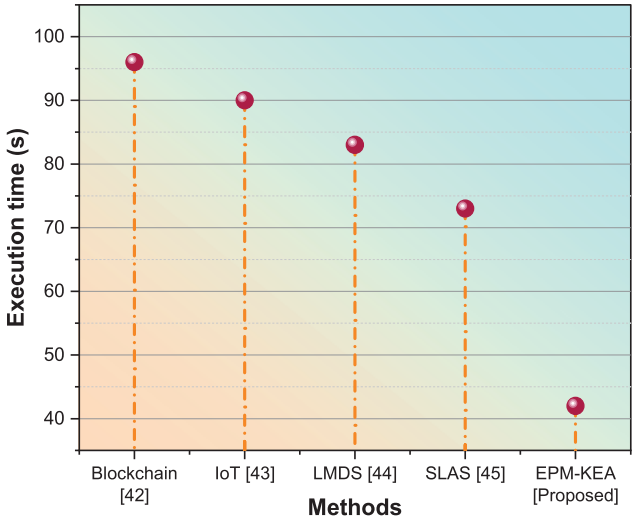

Figure 8: Execution time

The execution time for blockchain was estimated at 96 s, while IoT was evaluated with an 89-s execution time. LMDS was assessed using an 83-s execution time, and SLAS was considered with a 73-s execution time. The proposed technique, EPM-KEA, was evaluated with an execution time of 42 s. Comparing the suggested EPM-KEA technology to current methods such as blockchain, IoT, LMDS, and SLAS, it exhibited a shorter execution time for data processing.

4.4 Security Level

The term "security level" denotes the degree to which minimally adequate protective security measures must always be maintained for a specific duration, primarily due to the heightened risk of a security event. Table 4 and Fig. 9 illustrate the representation of the security level.

Table 4: Values of security level

Methods	Security level (%)
Blockchain [42]	39
IoT [43]	54
LMDS [44]	75
SLAS [45]	90
EPM-KEA [Proposed]	**97**

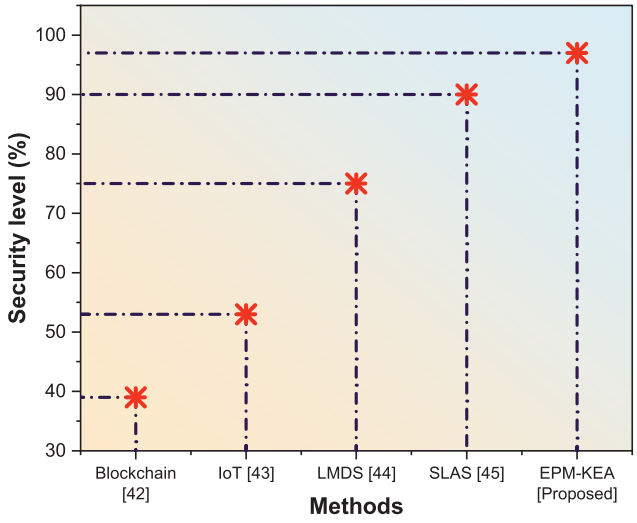

Figure 9: Security level

Cloud storage places significant importance on ensuring security. The compromised data is assessed by dividing it with the entirety of the original text to ascertain its value. The security level is expressed as follows:

$$\mathrm{GG}_{(\mathrm{gggg})} = \frac{\mathrm{gg}^{'}_{(zzzz)}}{\mathrm{gg}^{''}_{\mathrm{qqqq}}} \tag{5}$$

where $\mathrm{GG}_{(\mathrm{ggg})}$ denotes the security analysis, the hacked data $HH^{'}_{(zztt)}$ is and the number of the original text is $HH^{''}_{(qqdd)}$.

The compromised data is assessed by dividing it with the entirety of the original text to ascertain its value. The security level is expressed as follows:

$$\mathrm{GG}_{(\mathrm{gggg})} = \frac{\mathrm{gg}^{'}_{(zzzz)}}{\mathrm{gg}^{''}_{\mathrm{qqqq}}} \tag{6}$$

where $\mathrm{GG}_{(\mathrm{ggg})}$ denotes the security analysis, the hacked data $HH^{'}_{(zztt)}$ is and the number of the original text is $HH^{''}_{(qqdd)}$.

The coexistence of consumer firms' data within the same network poses a fundamental challenge to data security in cloud computing. The proposed approaches exhibit a higher level of protection, whereas the existing methods demonstrate a lower level of security.

When comparing the suggested EPM-KEA technology with current methods such as blockchain, IoT, LMDS, and SLAS, it is observed that the execution time for data processing is reduced. Blockchain achieves a security level of 39%, IoT achieves 54%, LMDS achieves 75%, SLAS achieves 90%, and the proposed method, EPM-KEA, achieves 97%.

4.5 Energy Consumption

Energy consumption encompasses all the energy required to carry out activities, create something, or occupy a structure. In data encryption, energy consumption refers to the amount of electricity or fuel used. Table 5 and Fig. 10 illustrate energy usage. Blockchain was estimated to have an energy usage of 81%.

Table 5: Energy consumption

Methods	Energy consumption (%)
Blockchain [42]	81
IoT [43]	62
LMDS [44]	92
SLAS [45]	73
EPM-KEA [Proposed]	**53**

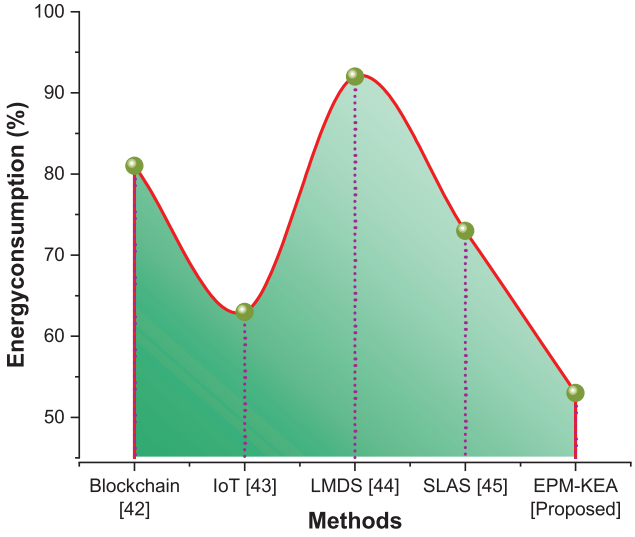

Figure 10: Energy consumption

IoT demonstrated an energy usage of 62%. LMDS accounted for 92% of energy usage during the evaluation. SLAS exhibited an energy usage of 73%. The suggested approach, EPM-KEA, was tested with a 53% energy usage. In comparison to current methods, the recommended approach consumes less energy.

When comparing the existing techniques with the suggested ones, blockchain, IoT, LMDS, and SLAS demonstrate remarkable efficiency.

4.6 Discussion

Data stored on the blockchain cannot be altered once created, which is one of the technology's significant advantages and drawbacks. The economic and logistics sectors derive benefits from this phenomenon. Immutability necessitates a uniform distribution of network nodes, which is unattainable without it. Should a single organization exercise control over more than 50 percent of a blockchain network's nodes, the network faces a potential risk [42]. Additionally, numerous lightweight authentication techniques currently in use exhibit various security flaws, particularly the absence of forward secrecy [43]. By leveraging blockchain technology, computational costs can be reduced while maintaining a higher level of security [44]. IoT devices' limited storage and processing power pose challenges in implementing complex cryptographic processes [45]. To address these issues, this research introduces a novel cloud-based encryption method, the Enhanced Parallel Multi-Key Encryption Algorithm (EPM-KEA). The primary motivation behind encryption techniques is to safeguard and store vast amounts of data in the cloud.

5 Conclusion

In conclusion, the rapid development of cloud computing, driven by its potential for cost reductions, has emphasized the rising relevance of cloud services in various industries, with healthcare data security emerging as a critical issue. The processing cost of encryption techniques might be a barrier when dealing with time-sensitive medical data. Using robust encryption techniques, such as EPM-KE, is a heartening step in the right direction, especially when protecting data stored in the cloud, which poses specific issues. Safeguarding Patients' Confidential Health Information Online, Cryptographic algorithms implement it to ensure the confidentiality and integrity of transmitted data. To ensure the security of patient data stored in the cloud, irreversible hash values. However, owing to the security holes in today's technologies, a thorough examination of wireless network security is necessary. Compared to traditional techniques, the system performed well, indicating that resolving these security issues might lead to more widely accessible cloud storage alternatives for preserving healthcare data. This research shows how important it is to strengthen data security measures as the cloud computing sector grows. Further development and expansion of the EPM-KEA encryption protocol will be necessary to strengthen cloud-based healthcare data security. Integration with emerging technologies like homomorphism encryption, constant threat monitoring, and dynamic key management will all improve resilience.

Acknowledgement: Not applicable.

Funding Statement: Not applicable.

Author Contributions: Conceptualization, SKG and USB; methodology, SKG; software, WA; validation, SK, SB, and SKG; formal analysis, SK and SB; investigation, USB; resources, SKG; data curation, WA; writing—original draft preparation, SKG; writing—review and editing, USB; visualization, SKG and USB; supervision, SK; project administration, SKG. All authors have read and agreed to the published version of the manuscript.

Availability of Data and Materials: Not applicable.

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

References

[1] A. Gumaei, R. Sammouda, A. M. S. Al-Salman, and A. Alsanad, "Anti-spoofing cloud-based multispectral biometric identification system for enterprise security and privacy-preservation," *J. Parallel. Distr. Comput.*, vol. 124, no. 2–3, pp. 27–40, 2019. doi: 10.1016/j.jpdc.2018.10.005.

[2] A. Kumar, "A novel privacy preserving HMAC algorithm based on homomorphic encryption and auditing for cloud," in *Proc. 2020 Fourth Int. Conf. I-SMAC*, India, Oct. 2020, pp. 198–202.

[3] A. Zhang and X. Lin, "Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain," *J. Med. Syst.*, vol. 42, no. 8, pp. 1–18, 2018. doi: 10.1007/s10916-018-0995-5.

[4] A. Abugabah, N. Nizamuddin, and A. A. Alzubi, "Decentralized telemedicine framework for a smart healthcare ecosystem," *IEEE Access*, vol. 8, pp. 166575–166588, 2020. doi: 10.1109/ACCESS.2020.3021823.

[5] J. B. Awotunde, R. G. Jimoh, S. O. Folorunso, E. A. Adeniyi, K. M. Abiodun and O. O. Banjo, "Privacy and security concerns in IoT-based healthcare systems," in *The Fusion of Internet of Things, Artificial Intelligence, and Cloud Computing in Health Care*. Cham: Springer International Publishing, 2021, pp. 105–134.

[6] C. Zhou, A. Fu, S. Yu, W. Yang, H. Wang and Y. Zhang, "Privacy-preserving federated learning in fog computing," *IEEE Internet Things*, vol. 7, no. 11, pp. 10782–10793, 2020. doi: 10.1109/JIOT.2020.2987958.

[7] B. Chen, T. Xiang, D. He, H. Li, and K. K. R. Choo, "BPVSE: Publicly verifiable searchable encryption for cloud-assisted electronic health records," *IEEE Trans. Inf. Foren. Secur.*, vol. 18, pp. 3171–3184, 2023. doi: 10.1109/TIFS.2023.3275750.

[8] D. Teodoro, E. Sundvall, M. João Junior, P. Ruch, and S. Miranda Freire, "ORBDA: An open EHR benchmark dataset for performance assessment of electronic health record servers," *PLoS One*, vol. 13, no. 1, pp. e0190028, 2018. doi: 10.1371/journal.pone.0190028.

[9] G. Sun, S. Sun, J. Sun, H. Yu, X. Du and M. Guizani, "Security and privacy preservation in fog-based crowd sensing on the internet of vehicles," *J. Netw Comput. Appl.*, vol. 134, no. 6, pp. 89–99, 2019. doi: 10.1016/j.jnca.2019.02.018.

[10] P. Gautam, M. D. Ansari, and S. K. Sharma, "Enhanced security for electronic health care information using obfuscation and RSA algorithm in cloud computing," *Int. J. Inf. Secur. Privacy*, vol. 13, no. 1, pp. 59–69, 2019. doi: 10.4018/IJISP.

[11] H. Deng, Z. Qin, L. Sha, and H. Yin, "A flexible privacy-preserving data sharing scheme in cloud-assisted IoT," *IEEE Internet Things*, vol. 7, no. 12, pp. 11601–11611, 2020. doi: 10.1109/JIOT.2020.2999350.

[12] C. F. L. Hickman *et al.*, "Data sharing: Using blockchain and decentralized data technologies to unlock the potential of artificial intelligence: What can assisted reproduction learn from other areas of medicine?," *Fert. Steril.*, vol. 114, no. 5, pp. 927–933, 2020. doi: 10.1016/j.fertnstert.2020.09.160.

[13] J. Han, Y. Li, and W. Chen, "A lightweight and privacy-preserving public cloud auditing scheme without bilinear pairings in smart cities," *Comput. Stand Inter.*, vol. 62, no. 5, pp. 84–97, 2019. doi: 10.1016/j.csi.2018.08.004.

[14] J. Li, H. Yan, and Y. Zhang, "Identity-based privacy-preserving remote data integrity checking for cloud storage," *IEEE Syst. J*, vol. 15, no. 1, pp. 577–585, 2020. doi: 10.1109/JSYST.2020.2978146.

[15] J. Xu *et al.*, "Health chain: A blockchain-based privacy-preserving scheme for large-scale health data," *IEEE Internet Things*, vol. 6, no. 5, pp. 8770–8781, 2019. doi: 10.1109/JIOT.2019.2923525.

[16] J. A. Alzubi, "Blockchain-based LamportMerkle digital signature: Authentication tool in IoT healthcare," *Comput. Commun.*, vol. 170, no. 1, pp. 200–208, 2021. doi: 10.1016/j.comcom.2021.02.002.

[17] J. Domingo-Ferrer, O. Farras, J. Ribes-González, and D. Sánchez, "Privacy-preserving cloud computing on sensitive data: A survey of methods, products, and challenges," *Comput. Commun.*, vol. 140, no. 1, pp. 38–60, 2019. doi: 10.1016/j.comcom.2019.04.011.

[18] K. Fan, H. Xu, L. Gao, H. Li, and Y. Yang, "Efficient and privacy-preserving access control scheme for fog-enabled IoT," *Future Gener. Comput. Syst.*, vol. 99, no. 1, pp. 134–142, 2019. doi: 10.1016/j.future.2019.04.003.

[19] K. R. Sanjay, S. S. Babu, and Y. Vijayalakshmi, "Enhancing the security of cloud data using hybrid encryption algorithm," *J. Amb. Intell. Hum. Comput.*, vol. 10, pp. 1–10, 2019.

[20] L. Tan, K. Yu, N. Shi, C. Yang, W. Wei and H. Lu, "Towards secure and privacy-preserving data sharing for COVID-19 medical records: A blockchain-empowered approach," *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 1, pp. 271–281, 2021. doi: 10.1109/TNSE.2021.3101842.

[21] M. Tahir, M. Sardaraz, Z. Mehmood, and S. Muhammad, "CryptoGA: A cryptosystem based on genetic algorithm for cloud data security," *Clust. Comput.*, vol. 24, no. 2, pp. 739–752, 2021. doi: 10.1007/s10586-020-03157-4.

[22] M. Zhang, Y. Chen, and J. Huang, "SE-PPFM: A searchable encryption scheme supporting privacy-preserving fuzzy multi-keyword in cloud systems," *IEEE Syst. J.*, vol. 15, no. 2, pp. 2980–2988, 2020. doi: 10.1109/JSYST.2020.2997932.

[23] P. Velmurugadass, S. Dhanasekaran, S. S. Anand, and V. Vasudevan, "Enhancing Blockchain security in cloud computing with IoT environment using ECIES and cryptography hash algorithm," *Mater. Today: Proc.*, vol. 37, pp. 2653–2659, 2021.

[24] R. Gupta, I. Gupta, D. Saxena, and A. K. Singh, "A differential approach and deep neural network-based data privacy-preserving model in cloud environment," *J. Amb Intell. Hum. Comput.*, vol. 13, pp. 1–16, 2022.

[25] S. Ganapathy, "A secured storage and privacy-preserving model using CRT for providing security on cloud and IoT-based applications," *Comput. Netw.*, vol. 151, pp. 181–190, 2019.

[26] S. Guo, T. Xiang, and X. Li, "Towards efficient privacy-preserving face recognition in the cloud," *Signal Process.*, vol. 164, no. 2, pp. 320–328, 2019. doi: 10.1016/j.sigpro.2019.06.024.

[27] Y. Song, H. Wang, X. Wei, and L. Wu, "Efficient attribute-based encryption with privacy-preserving key generation and its application in industrial cloud," *Secur. Commun. Netw.*, vol. 2019, pp. 1–9, 2019.

[28] Y. Wang, A. Zhang, P. Zhang, and H. Wang, "Cloud-assisted EHR sharing with security and privacy preservation via consortium blockchain," *IEEE Access*, vol. 7, pp. 136704–136719, 2019. doi: 10.1109/ACCESS.2019.2943153.

[29] M. Banerjee, J. Lee, and K. K. R. Choo, "A blockchain future for internet of things security: A position paper," *Digital Communications and Networks*, vol. 4, no. 3, pp. 149–160, 2018. doi: 10.1016/j.dcan.2017.10.006.

[30] Y. Wang, Y. Ding, Q. Wu, Y. Wei, B. Qin and H. Wang, "Privacy-preserving cloud-based road condition monitoring with source authentication in VANETs," *IEEE Trans. Inform. Foren. Secur.*, vol. 14, no. 7, pp. 1779–1790, 2018. doi: 10.1109/TIFS.2018.2885277.

[31] Z. Guan *et al.*, "APPA: An anonymous and privacy preserving data aggregation scheme for fog-enhanced IoT," *J. Netw. Comput. Appl.*, vol. 125, no. 2, pp. 82–92, 2019. doi: 10.1016/j.jnca.2018.09.019.

[32] Z. Xu, C. Xu, W. Liang, J. Xu, and H. Chen, "A lightweight mutual authentication and key agreement scheme for medical Internet of Things," *IEEE Access*, vol. 7, pp. 53922–53931, 2019. doi: 10.1109/ACCESS.2019.2912870.

[33] C. Zhang, X. Luo, Q. Fan, T. Wu, and L. Zhu, "Enabling privacy-preserving multi-server collaborative search in smart healthcare," *Future Gener. Comput. Syst.*, vol. 143, no. 3, pp. 265–276, 2023. doi: 10.1016/j.future.2023.01.025.

[34] J. Zhang, B. Chen, Y. Zhao, X. Cheng, and F. Hu, "Data security and privacy-preserving in edge computing paradigm: Survey and open issues," *IEEE Access*, vol. 6, pp. 18209–18237, 2018. doi: 10.1109/ACCESS.2018.2820162.

[35] Y. Zhang and D. Wang, "Integrating blockchain technology and cloud services in healthcare: A security and privacy perspective," in *Proc. Indian Nati. Sci. Acad.*, 2023, pp. 1–14.

[36] A. Sarker, A. C. Canto, M. M. Kermani, and R. Azarderakhsh, "Error detection architectures for hardware/software co-design approaches of number-theoretic transform," *IEEE Trans. Comput.-Aided Des. Integr. Circ. Syst.*, vol. 42, pp. 2418–2422, 2022.

[37] M. Mozaffari Kermani and R. Azarderakhsh, *Integrating Emerging Cryptographic Engineering Research and Security Education*. American Society for Engineering Education (ASEE), Washington DC, pp. 20036–2479, 2015.

[38] A. Sarker, M. M. Kermani, and R. Azarderakhsh, "Efficient error detection architectures for postquantum signature falcon's sampler and KEM SABER," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 30, no. 6, pp. 794–802, 2022. doi: 10.1109/TVLSI.2022.3156479.

[39] A. C. Canto, J. Kaur, M. M. Kermani, and R. Azarderakhsh, "Algorithmic security is insufficient: A comprehensive survey on implementation attacks haunting post-quantum security," arXiv preprint arXiv:2305.13544, 2023.

[40] A. K. Sangaiah, A. Javadpour, F. Ja'fari, P. Pinto, and H. M. Chuang, "Privacy-aware and AI Techniques for healthcare based on K-Anonymity model in internet of things," *IEEE Trans. Eng. Manag.*, vol. 70, pp. 1–15, 2023.

[41] M. Zhang, Y. Chen, and W. Susilo, "PPO-CPQ: A privacy-preserving optimization of clinical pathway query for e-healthcare systems," *IEEE Internet Things*, vol. 7, no. 10, pp. 10660–10672, 2020. doi: 10.1109/JIOT.2020.3007518.

[42] N. Deepa and P. Pandiaraja, "E health care data privacy preserving efficient file retrieval from the cloud service provider using attribute-based file encryption," *J. Amb. Intell. Hum. Comput.*, vol. 12, no. 5, pp. 4877–4887, 2021. doi: 10.1007/s12652-020-01911-5.

[43] N. A. Al-gohany and S. Almotairi, "Comparative study of database security in cloud computing using AES and DES encryption algorithms," *J. Inf. Sec. Cyber. Res.*, vol. 2, pp. 102–109, 2019.

[44] P. PremPriya and J. Katiravan, "Privacy-preserving and energy-centered QoS for IoT using XOR-RSA and BM-SSA," *Wirel, Pers, Commun.*, vol. 122, pp. 1671–1694, 2022.

[45] P. Singh, M. Masud, M. S. Hossain, and A. Kaur, "Blockchain and homomorphic encryption-based privacy-preserving data aggregation model in smart grid," *Comput. Electr. Eng.*, vol. 93, no. 1, pp. 107209, 2021. doi: 10.1016/j.compeleceng.2021.107209.