Journal of Harbin Engineering University
ISSN: 1006-7043

Vol 45 No. 12
December 2024

Sustainable Framework for Enhancing Cloud Computing Security Against Data Breaches Inspired by Shannon's Theory

[1]Anil Kumar , [2]Pinki Nayak, [3]Deepak Bhardwaj

[1.] anilbest2005@gmail.com, ADGIPS, Shastri Park, Delhi, INDIA

[2.] pinki.nayak.dua@gmail.com, ADGIPS, Shastri Park, Delhi, INDIA

[3.] 707.deepak@gmail.com, ADGIPS, Shastri Park Delhi, INDIA

Abstract:

As the digital landscape evolves with distributed system technologies, cloud computing has emerged as a revolutionary force in the IT sector, offering remote services hosted by third parties for data storage, processing, and management. This shift brings with it significant security challenges, particularly concerning sensitive and confidential data stored in the cloud. While encryption is a prevalent method for data protection, various algorithms—such as RSA, ECDSA, and HMAC—also play a role in ensuring security, integrity, and authorized access. However, these techniques have limitations.

This paper proposes a security mechanism based on Shannon's theory, structured in two layers. The first layer employs Shannon's principles of diffusion and confusion through logical operations (NOR, NAND, and Shift) to divide the original plain text and key into equal parts. The second layer draws inspiration from the central dogma of molecular biology, simulating natural processes for genetic-based cryptography.

The proposed algorithm aims to provide a robust security level that outperforms existing techniques in cloud computing. While cloud service providers implement security controls, users also bear the responsibility of safeguarding their own data. This dual approach enhances overall security in the cloud computing environment.

Objective: The objective of a **Sustainable Framework for Enhancing Cloud Computing Security Against Data Breaches Inspired by Shannon's Theory** would be to develop a security framework that integrates the principles of Claude Shannon's information theory to address data breaches in cloud computing environments. This framework would focus on creating more secure, efficient, and reliable systems for protecting sensitive data stored and processed in the cloud.

The **objective** of this framework is to combine the theoretical foundation provided by Shannon's information theory with practical, sustainable solutions for improving cloud computing security. It would focus on data confidentiality, integrity, authentication, resilience to attacks, and scalability, while promoting energy efficiency and sustainability in cloud security measures.

Methods:

Process of the Proposed Framework:

i. **Key Generation:** The initial step involves generating the necessary cryptographic keys for encryption and decryption.

ii. **Conversion of Plaintext to Ciphertext**

a) **First Layer:** This layer uses logical operations like NOR, XNOR, and bit shifting to transform the plaintext into ciphertext.

b) **Second Layer:** Drawing inspiration from the Central Dogma of Molecular Biology (CDMB), this layer adds an additional level of complexity to the encryption, further strengthening the security process.

iii. **Key Generation (Continued):**

a) Two specific sequences, such as AUGC and UCGA, are chosen to assist in the encryption process.

b) The process of security key generation is then carried out as per the framework's design, ensuring robust cryptographic protection for the data.

Results: The proposed framework, which leverages a genetic algorithm-based approach for cloud computing, demonstrates superior resistance to data breaches when compared to traditional symmetric encryption methods such as AES, DES, and Blowfish. The evaluation is conducted based on several factors, including encryption time, encryption throughput, and the size of the encrypted ciphertext, all of which are measured relative to the size of the plaintext and the time required for converting between plaintext and ciphertext.

Conclusion: The proposed technique utilizes logical-mathematical functions and genetic algorithms inspired by ribonucleic acid (RNA) to strengthen data breach confidentiality. The process begins by applying logical operations such as NOR, XNOR, and bit shifting, which divide the original plaintext and key into equal segments, introducing diffusion and confusion within the cipher. This forms the first layer of encryption, ensuring a basic level of secrecy. To further bolster privacy, the second layer incorporates concepts from the Central Dogma of Molecular Biology (CDMB), enhancing the cryptographic process and providing an added layer of security.
Discussion: A **Sustainable Framework for Enhancing Cloud Computing Security Against Data Breaches**, inspired by Shannon's information theory, provides a structured approach to addressing the complex challenges of securing cloud data. Shannon's work, particularly his concepts of **confidentiality, integrity, and authentication**, lays the foundation for robust encryption and security measures in cloud environments.
Keywords: cloud computing, RSA, ECDSA, HMAC, Shannon's Theory, Genetic Algorithm

Introduction:

Cloud computing shifts the management of IT resources from on-premises data centers to cloud vendors, who handle everything from hardware procurement and installation to virtualization, operating system setup, firewall configuration, and data storage management. This allows businesses to access a range of software and platform services without the burden of maintaining their own infrastructure.

Cloud computing enables users to rent necessary services for specific time periods, representing a new paradigm in the digital landscape. It offers on-demand services at low costs, aiming to deliver fast and user-friendly computing and data storage solutions in a cloud environment [1]. Cloud computing provides greater flexibility and reliability, improving performance and efficiency while lowering IT costs. Businesses can access applications and data from any internet-enabled device instead of depending on in-house servers or software. Although cloud computing is crucial for modern business, it also presents various challenges and risks. To maximize its advantages, providers, developers, and end users must proactively tackle these issues.

Significant challenges in cloud computing encompass user privacy, data security, vendor lock-in, service availability, disaster recovery, performance, scalability, energy efficiency, and programmability.

To improve cloud computing security, various techniques are available that ensure data center security and privacy, as well as confidentiality in data transfer. These methods convert messages into ciphertext, allowing only the intended recipient to access the hidden information.

Cryptographic mechanisms encompass various methods that can be employed to deliver essential security services [2]. Encryption protocols, digital signatures, and hash functions are essential components of cryptography, which secures confidential information. These methods can be categorized into symmetric algorithms, asymmetric algorithms, and hybrid algorithms, each playing a vital role in encrypting and decrypting data to ensure its confidentiality and integrity [3,4].

Current cartographic schemes face various protection challenges and often require significant time for key generation, retrieval, and data encryption and decryption. RSA, an asymmetric algorithm, utilizes a public-private key pair for signature generation and verification. As a form of public key cryptography, RSA employs both keys to secure data in the cloud, representing a significant advancement in cryptography. Known as an asymmetric algorithm, it operates with two keys along with a secret key. In this scheme, both plain text and ciphertext are treated as integers between 0 and n-1, with n typically set at 1024 bits [5-6]. The Elliptic Curve Digital Signature Algorithm (ECDSA) is a widely used digital signature algorithm that ensures integrity, authenticity, and non-repudiation. However, since the private key in traditional ECDSA is stored in plaintext, it can be vulnerable to attackers. To enhance the security of the private key against white-box attacks, this article introduces a white-box implementation of ECDSA that employs lookup table technology and a "cloud plus side" mode to better protect the private key [7].

HMAC, or Hash-based Message Authentication Code, is a cryptographic hash function that combines a message and a secret key, hashing them together to create an authentication code. This method utilizes a cryptographic hash function, such as SHA, to ensure

data integrity and authenticate the message using the security key necessary for generating the code. Unlike standard hash functions, which can produce authentication codes without constraints, HMAC's security is influenced by the cryptographic strength of the hash function, the size of the hash output, and the quality of the key. While HMAC does not independently provide message integrity, it serves as a critical component within protocols designed to ensure message integrity and protect against man-in-the-middle attacks. HMAC supports various hash algorithms, including MD5, SHA-1, and SHA-256 [8]

PROBLEM STATEMENT

A cloud data storage service involves several key participants: the user (U), who needs to store large amounts of data; the cloud server (CS), managed by the cloud service provider (CSP) and equipped with substantial storage; and the trusted third-party auditor (TPA), who accesses the CSP at the user's request. When the user uploads data, copies are sent to both the CSP and the TPA. To ensure the correctness of the stored data, an auditing process is conducted by the TPA, which must be able to audit efficiently without altering the original data. The auditing relies on the data stored with the TPA [9].

Key requirements for this process include:

1. **Public Audibility**: The TPA should be able to verify the data's correctness without needing a copy of the data.
2. **Privacy Preservation**: The TPA must not be able to access the actual data content during the auditing process.
3. **Lightweight Operation**: The auditing process should involve minimal communication and computational overhead for the TPA.

Cloud service providers offer a secure hosting platform for clients to deploy their services. However, security implementations can vary significantly from one cloud provider to another. It's important to note that clients do not completely relinquish their responsibilities for securing their data and applications. The proposed algorithm is based on Shannon's theory, emphasizing the need for robust security measures even within the cloud environment.

Literature review

Since its introduction to the market in 2000, cloud computing has been an active field of study. Cloud computing offers services such as virtual data storage, collaboration, servers, networks, applications, and tools with minimal resource commitment. The central concern of cloud computing is the protection of information due to the vast volume of data stored in the cloud and communication systems' development, meaning that data can be hacked or destroyed by unauthorized access [10]. Cloud computing faces various security issues, some of which are service disruption, DoS attacks, compromised authentication, outside malicious insiders, security threats, system vulnerabilities, multi-tenancy issues, data integrity, and data privacy [11]. Cloud technology guarantees the protection of data and handles cryptographic keys to prevent data compromise or data failure. As there are many malicious users in the cloud, data protection could be at risk; cloud Service also has to maintain data security to prevent unwanted access to data in cloud storage. Incidents of data breaches or lack of data are widespread these days [12] These authors analyzed data protection and privacy issues in cloud computing by concentrating on data isolation and secure privacy. Data security problems are of paramount significance to the extent and data of IaaS, PaaS, and SaaS, which are core challenges in cloud computing. Data integrity is a critical enabler for cloud users. In addition to storing data, cloud technology typically offers data management facilities. In data integrity, Many scholars have also done a lot of work on cloud data integrity and privacy issues, some of which have been discussed [13]. Encryption is the key technology that satisfies the criteria of security [14]. Various algorithms based on symmetric/asymmetric core technologies and genetic techniques such as RSA, DES, etc. were adopted, developed, and applied [15]. Cryptographic algorithms can be contrasted based on design, versatility, scalability, limitations and security, execution time, and memory requirements [16]. introduced the use of hybrid encryption approaches to enhance the privacy of the information stored on cloud servers such: as Blowfish, RSA, AES, Eclipse IDA, and DSA, This study focuses on not using third parties to encrypt customer data, but on allowing consumers the authority to decide ways of encrypting their data" [17]. The authors identified previous studies devoted to cloud data security and performed a survey. They suggested a hybrid protection encryption approach using Blowfish and MD5 to offer improved security on the cloud server [18]. A comparison of IDAs, SHA-512, 3DES, and AES-

256 made by Ref. [19], consists of on-premise data encoding and decoding. This algorithm achieves a much higher level of protection and performance for large and small data files. This author [20] proposed a New Lightweight Cryptographic Algorithm for Enhancing Data Security that can be used to secure applications on cloud computing. The algorithm is a 16-byte (128-bit) block cipher and wants 16 16-byte (128-bit) key to encrypt the data. The authors [21] proposed a feature-based hierarchical encryption technique using semantic ontology for public auditing on cloud computing.

Many different researchers have focused research on the improvement of cloud data security. Quantum cryptography offers unconditional security based on the principles of quantum computers. The authors reviewed and implemented a well-known branch of quantum cryptography which includes theory and implementation such as quantum key distribution[22]. A study of quantum cryptography and its application such as encryption and key distribution is used for avoiding the access control problem. The author proposed an encryption technique and key distribution protocol for the Categorical Quantum Mechanics (CQM) for the graphical language for CQM [23]. In the twenty-first century, identity-based theft is the most risky in cybercrime, and the number of hackers is exponentially increasing day by day. Quantum cryptography is used to provide the security and confidentiality for the network security. The authors implemented a model that uses identity-based authentication and used to confirm the user's identity before getting access and also used quantum identity-based authentication and BB84 protocol for securing the cloud data [24]. In the field of mobile cloud computing, quantum cryptography also plays an important role in the security of mobile cloud data. Quantum key distribution for cloud mobile users using two phases is proposed by the multiplexing technique used for the transformation of the quantum distribution network using the classical optical network. It is also used as an authentication protocol for access control and then quantum keys are transferred to the cloud mobile user’s storage area and the mobile user can easily access the storage area through the quantum secret key. All the experiments are performed using the real quantum cryptography environment which proves the validity of quantum cryptography for mobile cloud computing [25]. Several traditional cryptographic techniques failed concerning confidentiality and integrity across the worldwide network. The author implemented a model on the AVISPA which provided confidentiality in the presence of an attacker and also compared it with the existing cryptographic techniques [26]. Verifiable quantum computation resolves the problem of authentication and privacy while cloud computing clients interact with quantum computers. Li et al. [27] implemented a model based on a cryptographic calculation which is used for the distributed structure of cloud computing and used cluster state in grid distributed manner and the random key is always used by the cloud client which builds trust for the confidentiality to the users. Winick et al. [28] proposed a safe, effective, and hard-grained numerical computation method for generating key rates using Quantum Key Distribution (QKD) protocols and interpreted by generating higher key rates in comparison to other research. Cloud computing needs a visible solution for securing computing resources. The current security technique has a certain presumption which may be broken with few efforts. To provide high security for cloud storage has made using quantum cryptography which is an unconditional security technique. The author implemented and proposed a new security model based on the BB84 protocol for data distribution which is more beneficial for providing security to cloud data storage and also consider cloud servers, owner, and clients. This technique provided secure communications using the proposed model and provides a comparative study of the success and failure rates of public and private clouds [29]. Cloud computing has become a more promising technology in the field of information technology so the protection of cloud data is more important. The theft of identity authentication is the more serious concern of cloud computing so the author proposed a novel security protocol for authenticating the user through quantum cryptography [30].

In the public and private cloud storage accessibility, availability, and cost-effectiveness are the most important factors of the cloud environment. The transmission of information is the biggest concern of the cloud and is still not safe as a result of this aspect many cloud users lose their personal information. Olanrewaju et al. [31] proposed a novel security

technique that is an integrated service of advanced quantum cryptography with cloud computing. Access authentication is the decidable property of cloud computing that decides the cloud user's access. Qiu L et al. [32] investigated quantum cryptography to develop access control and used BB84, identity authentication, and digital certificate protocols for cloud data security. The data is growing in exponential order and security breaches are also increasing, and the difficult part for cloud providers is providing security to users. The author proposed a Mathematical model for generating encryption and decryption of data. For encryption, an encrypted message may clone three layers, and all three layers sum up and generate stronger ciphertext for the message [33].

Cloud computing changed the working style in the recent era of technology. It is an emerging technology that is rapidly changing technology for provide security and getting attention every time, and different large organizations are showing interest and shifting data in cloud storage because cloud storage has a unique property that attracts more organizations due to its flexibility of storage capacity. A novel security model has been proposed based on a DNA encryption algorithm that crops the security of cloud storage [34]. The DNA sequence with cloud computing storage is also used for the medical treatment of a patient. Wang et al [35] presented a method to store patient information related to deceases and biological information in cloud storage and identify patients with biological sequence, so the doctor easily identifies patients' past checkups and medicines and suggests medicines according to past medical information and present condition of the patient.

In Shannon's theory of confusion and diffusion, confusion aims to obscure the relationship between the ciphertext and the encryption key by making it as complex and intricate as possible. This complexity makes it difficult for an adversary to discern any patterns or relationships that could aid in decrypting the ciphertext without knowledge of the key.

On the other hand, diffusion involves spreading the statistical structure of the plaintext across the entirety of the ciphertext. This means that small changes in the plaintext result in significant changes throughout the ciphertext. Diffusion helps to prevent the recovery of information about the plaintext from any local characteristics or patterns in the ciphertext, thereby enhancing the security of the encryption scheme. Together, confusion and diffusion work synergistically to strengthen the security of cryptographic systems by making them resistant to various cryptanalytic attacks, such as frequency analysis or differential cryptanalysis. By incorporating these principles into encryption algorithms, cryptographic systems can achieve higher levels of security and confidentiality for sensitive data transmission and storage [36].

Proposed Framework for Conceptual Cryptography

Proposed Framework for Conceptual Cryptography aims to establish a comprehensive approach to understanding and implementing cryptographic principles. This framework integrates various cryptographic techniques and theories, providing a structured methodology for enhancing data security and privacy in diverse applications. By emphasizing the conceptual foundations of cryptography, the framework seeks to guide both practitioners and researchers in developing more effective and resilient cryptographic systems.

Conceptual cryptography is founded on RNA cryptography, which conceals confidential data within RNA molecules, addressing data breaches in cloud computing. This framework prioritizes critical parameters such as storage space, speed, and security against unauthorized access and attacks from hackers. It leverages logical-mathematical functions (such as NOR, XNOR, and shifting) alongside genetic algorithms to further enhance security mechanisms, effectively hiding confidential data within these mathematical constructs.

Conceptually, both cloud computing clients and cloud servers are responsible for protecting the integrity of sensitive data. The genetic algorithm is utilized to generate encryption and decryption keys, which are then integrated with a cryptographic algorithm to ensure the integrity and security of data in the cloud. The proposed cryptographic framework is designed to safeguard data from unauthorized access, enhancing overall security in cloud computing environments.

The requirements for a genetic algorithm based on Shannon's theory are as follows:

The conversion of plaintext to ciphertext must utilize the full character set used in the genetic algorithm encoding. This involves first converting the input text

from a file into binary, followed by replacing the binary data with nucleic acid coding to encode each character. This process integrates genetic algorithm principles and genetic coding with encryption techniques, enhancing the security and robustness of the ciphertext and making it more resilient to cryptographic attacks.

ii. A dynamic table must be generated to track the status of binary data alongside its corresponding RNA molecules.

iii. Unique sequences should be generated to encrypt each character of the input text for RNA sequencing. This requires creating a mapping between characters and their corresponding unique RNA sequences.

iv. **Mutation and Crossover Operations**: Inspired by genetic algorithms, these operations modify and combine encryption techniques, introducing randomness and variability into the encryption process. This approach significantly enhances the complexity and effectiveness of the encryption, making it more resistant to cryptanalysis and better protecting sensitive information from unauthorized access or decryption.

	A` 0	U `	C`	G `	U `	G `	C`	A`		
A `	0 0 0 0	0 0 0 1	0 0 1 1	0 0 1 0	0 0 0 1	0 0 1 0	0 0 1 1	0 0 0 0	K 1 `	S k 1 `
U `	0 1 0 0	0 1 0 1	0 1 1 1	0 1 1 0	0 1 0 1	0 1 1 0	0 1 1 1	0 1 0 0		
C `	1 1 0 0	1 1 0 1	1 1 1 1	1 1 1 0	1 1 0 1	1 1 1 0	1 1 1 1	1 1 0 0	K 2 `	
G `	1 0 0 0	1 0 0 1	1 0 1 1	1 0 1 0	1 0 0 1	1 0 1 0	1 0 1 1	1 0 0 0		
C `	1 1 0 0	1 1 0 1	1 1 1 1	1 1 1 0	1 1 0 1	1 1 1 0	1 1 1 1	1 1 0 0	K 3 `	S k 2 `
A `	0 0 0 0	0 0 0 1	0 0 1 1	0 0 1 0	0 0 0 1	0 0 1 0	0 0 1 1	0 0 0 0		
G `	1 0 0 0	1 0 0 1	1 0 1 1	1 0 1 0	1 0 0 1	1 0 1 0	1 0 1 1	1 0 0 0	K 4 `	
C `	1 1 0 0	1 1 0 1	1 1 1 1	1 1 1 0	1 1 0 1	1 1 1 0	1 1 1 1	1 1 0 0		

v. **Simulating Biological Processes**: This involves leveraging principles from biology to strengthen cybersecurity defenses and mitigate the risks associated with data breaches in the digital landscape. By mimicking biological mechanisms, the framework can improve its resilience against attacks.

vi. **Dynamic Encryption Process**: The encryption parameters, algorithms, or keys are constantly adjusted in response to evolving security threats, system conditions, or regulatory requirements. This dynamic approach ensures that the encryption remains robust and adaptable in the face of changing security landscapes.

The dynamic encryption process utilizes a genetic algorithm rooted in Darwin's theory of natural selection [37-38], while Shannon's theory serves as the foundation for the encryption and decryption methods within the proposed cryptography framework. This combination enhances the adaptability and security of the encryption process.

The proposed cryptography framework employs a two-stage encryption process that operates in a layered manner.

First Stage / Layer: This initial phase involves utilizing specific functions to split the text and its corresponding key into equal parts.

Second Stage / Layer: This stage employs a genetic technique that simulates the natural process of genetic coding, drawing on the Central Dogma of Molecular Biology (CDMB) for cryptographic purposes. This approach reduces the complexity of permutations and combinations while maintaining data security in cloud computing.

A similar process is reversed when downloading data from cloud storage, ensuring secure access to the information.

Process of the Proposed Framework:

i. **Key Generation**: The first step involves creating the necessary keys for encryption and decryption.

ii. **Conversion of Plain Text to Cipher Text**: a) **First Layer**: This layer employs logical operations such as NOR, XNOR, and shifting to transform the plaintext. b) **Second Layer**: This layer is based on the Central

Dogma of Molecular Biology (CDMB) to further enhance the encryption process.

iii. **Key Generation**: a) Two sequences are selected, such as AUGC and UCGA, to facilitate the encryption process. b) The security key generation process from the proposed framework is outlined below.

Table 1: Proposed key combination of Gen Sequence in binary:

Each RNA molecule consists of two long strands made up of nucleotides arranged in a random order, with ribose sugars attached to nitrogenous bases and phosphate groups. The nitrogenous bases include adenine, guanine, uracil, and cytosine. The strength of the nucleotide-based genetic scheme is directly related to the randomness it provides, which helps create a robust and reliable coding scheme for encryption.

c) Convert the key generation process into binary format.

Table 2: key generation to binary:

d) Each key is divided into four equal parts, represented as hexadecimal numbers (K1, K2, K3, and K4).

e) Logical operations (NOR, XNOR) are applied between every two keys (i.e., hexadecimal numbers) to generate the main key:

- SK1’=K1’⊕K2’+K2’SK1' = K1' \oplus K2' + K2'SK1’=K1’⊕K2’+K2’
- SK2’=K3’⊕K4’+K3’SK2' = K3' \oplus K4' + K3'SK2’=K3’⊕K4’+K3’
- KK1’=SK1’ (XNOR) SK2’+SK2’KK1' = SK1' \text{ (XNOR) } SK2' + SK2'KK1’=SK1’ (XNOR) SK2’+SK2’

Each time the key is sent to the receiver, its value will be randomly changed.

Each time the key is transmitted to the receiver, its value will be randomly altered to enhance security.

Encryption Process:

f) **First Layer - Logical-Mathematical Function**: i. Convert the input file's alphabet to ASCII, then from ASCII to binary.

ii. Read the binary values from the input file (referred to as plaintext) and convert each character to its corresponding ASCII digit.

iii. Convert the input file into octal values, then to hexadecimal values, and finally to their corresponding binary values.

iv. Split the binary value block into four 64-bit sub-blocks, labeled M1', M2', M3', and M4'.

v. **I1: Iteration 1**: Perform a NOR operation between each key and sub-key block:
(M1’⊕K1’,M2’⊕K2’,M3’⊕K3’,M4’⊕K4’)(M1' \oplus K1', M2' \oplus K2', M3' \oplus K3', M4' \oplus K4')(M1’⊕K1’,M2’⊕K2’,M3’⊕K3’,M4’⊕K4’)
(Sum of each nucleotide and its key)

vi. **I2: Iteration 2**: Use the output from the previous NOR operation:
(M1’⊕K1’,M2’⊕K2’,M3’⊕K3’,M4’⊕K4’)(M1' \oplus K1', M2' \oplus K2', M3' \oplus K3', M4' \oplus K4')(M1’⊕K1’,M2’⊕K2’,M3’⊕K3’,M4’⊕K4’)
Then, swap the parts (M1', M2') and (M3', M4') during the encryption process.

vii. **I3: Iteration 3**: Combine (M1’+M2’)(M1' + M2')(M1’+M2’) to create MP1 and (M3’+M4’)(M3' + M4')(M3’+M4’) to create MP2.

viii. Perform a NOR operation:
(SK1’⊕MP1’)(SK1' \oplus MP1')(SK1’⊕MP1’)

ix. Perform a NOR operation on the output:
(SK1’⊕MP1’⊕MP1’)(SK1' \oplus MP1' \oplus MP1')(SK1’⊕MP1’⊕MP1’)

x. Perform a NOR operation:
(SK2’⊕MP2’)(SK2' \oplus MP2')(SK2’⊕MP2’)

xi. Perform a NOR operation on the output:
(SK2’⊕MP2’⊕MP2’)(SK2' \oplus MP2' \oplus MP2')(SK2’⊕MP2’⊕MP2’)

xii. Combine MP1' and MP2'.

xiii. Perform XNOR operations between KK’KK'KK’ and (MP1’+MP2’)(MP1' + MP2')(MP1’+MP2’) to produce cipher level 1.

g) **Layer 2 - Genetic Algorithm**: i. Convert the binary value (cipher level 1) into RNA bases: 'A' = 00, 'U' = 01, 'G' = 10, and 'C' = 11.

ii. **Transcription**: Simulate a biological transcription process.

iii. **Translation**: Simulate the biological translation processes, e.g., A' - U', U' - A', G' - C', and C' - G'.

iv. **Reverse Transcription**: Simulate the biological reverse transcription process.

v. Convert the ciphertext back to binary and upload it to the cloud

Decryption Process: The decryption process is the reverse of the encryption process and occurs after the user requests data from the cloud and confirms their authentication. It consists of two stages:

	A`	U`	C`	G`	U`	G`	C`	A`		
A`	A`A`	A`U`	A`C`	A`G`	A`U`	A`G`	A`C`	A`A`	K1`	Sk1`
U`	U`A`	U`U`	U`C`	A`G`	A`U`	A`G`	A`C`	A`A`		
C`	C`A`	C`U`	C`C`	C`G`	C`U`	C`G`	C`C`	C`A`	K2`	
G`	G`A`	G`U`	G`C`	G`G`	G`U`	G`G`	G`C`	G`A`		
C`	C`A`	C`U`	C`C`	C`G`	C`U`	C`G`	C`C`	C`A`	K3`	Sk2`
A`	A`A`	A`U`	A`C`	A`G`	A`U`	A`G`	A`C`	A`A`		
G`	G`A`	G`U`	G`C`	G`G`	G`U`	G`G`	G`C`	G`A`	K4`	
C`	C`A`	C`U`	C`C`	C`G`	C`U`	C`G`	C`C`	C`A`		

a) **Decrypt the Second Layer**: This stage utilizes the genetic algorithm based on the Central Dogma of Molecular Biology (CDMB).

b) **Decrypt the First Layer**: This stage involves reversing the logical-mathematical functions, such as NOR, XNOR, and shifting, while splitting the original plaintext and key into equal parts.

Results and Discussion

The proposed framework, based on a genetic algorithm scheme for cloud computing, demonstrates greater robustness against data breaches compared to existing symmetric encryption techniques such as AES, DES, and Blowfish. This evaluation is based on criteria including encryption time, encryption throughput, and the length of the encrypted ciphertext, all measured against the size of the plaintext and the time required for conversion between plaintext and ciphertext.

Encryption Time: The analysis reveals that the encryption process time increases linearly with the number of characters or the size of the file. Importantly, the time needed for decryption is shorter than that for encryption, suggesting that the computational complexity of the proposed framework is significantly lower.

In this framework, the encryption time is affected by several factors, including:

I. **Key Size**: Larger keys typically result in longer encryption times, as more complex algorithms are required to maintain security.

II. **Logical Operations**: The use of logical operations (e.g., NOR, XNOR) in the encryption process adds computational overhead, which contributes to the overall encryption time.

III. **Data Size**: As the size of the input data grows, the encryption time increases linearly, reflecting the need to process more data.

Ultimately, the efficiency of the encryption process, as informed by Shannon's principles, demonstrates that while increased randomness and complexity can enhance security, they also necessitate careful management of encryption time to maintain performance in practical applications.

Decryption Time: In the proposed framework, the time to recover the original data from the ciphertext is calculated using the formula: Time consumed=end time−start time\text{Time consumed} = \text{end time} - \text{start time}Time consumed=end time−start time.

The proposed technique achieves faster decoding times compared to other encryption algorithms, making it adaptable and effective for secure communication in a cloud computing environment.

Throughput: The efficiency of an algorithm can be evaluated directly through its throughput. Performance is directly proportional to throughput; higher performance results in higher throughput. Throughput can be calculated using the formula: Throughput=Plain Text SizeEncoding Time\text{Throughput} = \frac{\text{Plain Text Size}}{\text{Encoding Time}}

Throughput =Plain Text Size / Encoding Time

Overall, the proposed scheme offers a promising solution for enhancing data security in cloud computing.

Decryption time can also be examined through the framework of Shannon's theory, which highlights the significance of entropy and information security in cryptography. In Shannon's view, effective cryptographic systems should minimize the predictability of both plaintext and ciphertext, thereby increasing security.

When analyzing decryption time in relation to Shannon's theory, several factors come into play:

I. **Algorithm Complexity**: The decryption process typically requires operations that are inversely related to those used during encryption. If the encryption method maximizes uncertainty and complexity, decryption may be quicker due to more efficient algorithms designed to reverse these processes.

II. **Key Utilization**: According to Shannon, the relationship between the key size and decryption time is crucial. A well-structured key management strategy can streamline decryption, ensuring that even with complex encryption methods, the decryption time remains manageable.

III. **Data Structure**: The manner in which data is structured during encryption influences how quickly it can be decrypted. For example, if data is organized to facilitate rapid access and processing, decryption can occur more efficiently.

IV. **Entropy and Redundancy**: Shannon's theory posits that redundancy in data can be exploited to speed up decryption. By recognizing patterns or repetitions, the decryption process can be optimized.

In this framework, it is observed that the decryption time is often less than the encryption time, indicating a lower computational complexity. This efficiency aligns with Shannon's principles, as the decryption process focuses on restoring the original data without the need to reintroduce the same level of complexity used during encryption. Ultimately, while security is paramount, maintaining a balance between encryption complexity and decryption efficiency is key to effective cryptographic design.

Conclusion

With the rapid advancement of computing technologies, cloud computing offers effective and flexible solutions for computational and storage needs based on application requirements. Cloud service providers deliver data and computational services on demand. However, challenges regarding data security and privacy remain significant concerns. These providers often store sensitive and confidential data, raising issues of trust.

The proposed technique leverages logical-mathematical functions and genetic algorithms based on ribonucleic acid (RNA) to enhance data breach secrecy. This method begins with the exploration of logical operations such as NOR, XNOR, and shifting, which split the original plaintext and key into equal parts, incorporating characteristics of diffusion and confusion in the cipher. This approach ensures first-layer secrecy. To further enhance privacy, the second layer incorporates principles from the Central Dogma of Molecular Biology (CDMB) for cryptographic purposes, providing an additional level of security.

References

[1] F.M. Groom, “The basics of cloud computing,” in Enterprise Cloud Computing for Non Engineers, 2018.

[2] F. Thabit, A. Prof, S. Alhomdy, A.H.A. Al-hadal, Exploration of Security Challenges in Cloud Computing: Issues, Threats, and Attacks with Their Alleviating Techniques Exploration of Security Challenges in Cloud Computing: Issues, Threats, and Attacks with Their Alleviating Techniques 12th, vol. 10, Journal of Information and Computational Science, USA, 2020, pp. 35–56, 1, December, Submitted for publication.

[3] M. Zhou, R. Zhang, W. Xie, W. Qian, A. Zhou, Security and Privacy in Cloud Computing: A Survey, 2010, https://doi.org/ 10.1109/ SKG. 2010.19.

[4] S. Yi, Z. Qin, Q. Li, Security and privacy issues of fog computing, A survey (2015), https://doi.org/10.1007/978-3-319-21837-3_67.

[5] Simarjeet Kaur, “Cryptography and Encryption in Cloud Computing”, VSRD International Journal of Computer Science and Information Technology, Vol. 2(3), 2012, pp: 242-249.

[6] Vishwa Gupta, Gajendra Singh, Ravindra Gupta, "Advanced Cryptography algorithm for improving data security", International Journal of Advanced Research in Computer Science and Software Engineering, Vol 2, Issue 1, Jan 2012.

[7] Jie Zhou et all, "White-Box Implementation of ECDSA Based on the Cloud Plus Side Mode", Hindawi Security and Communication Networks Volume 2020, Article ID 8881116, 10 pages https://doi.org/10.1155/2020/8881116

[8] S. Ezhil Arasu, B. Gowri, S Ananthi, "Privacy-preserving Public Auditing in Cloud using HMAC Algorithm", International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878 (Online), Volume-2 Issue-1, March 2013

[9] C. Wang, Q. Wang, K.Ren, and W.Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage", in Proc. Of IEEE INFOCOM'10,March 2010

[10] M. Ali, S.U. Khan, A.V. Vasilakos, Security in cloud computing: opportunities and challenges, Inf. Sci. (2015), https://doi.org/10.1016/ j.ins. 2015.01.025.

[11] N. Kshetri, Privacy and security issues in cloud computing: the role of institutions and institutional evolution, Telecommun. Pol. (2013), https://doi.org/10.1016/ j.telpol.2012.04.011.

[12] D. Chen, H. Zhao, Data Security and Privacy Protection Issues in Cloud Computing, 2012, https://doi.org/10.1109/ICCSEE.2012.193.

[13] 13. S. Pearson, A. Benameur, Privacy, Security and Trust Issues Arising from Cloud Computing, 2010, https://doi.org/10.1109/CloudCom.2010.66.

[14] 14. A. Bhardwaj, G.V.B. Subrahmanyam, V. Avasthi, H. Sastry, Security Algorithms for Cloud Computing, 2016, https://doi.org/10.1016/ j.procs.2016.05.215.

[15] P. Dixit, A.K. Gupta, M.C. Trivedi, V.K. Yadav, Traditional and hybrid encryption techniques: a survey, in Lecture Notes on Data Engineering and Communications Technologies, 2018.

[16] S. Chowdhury, S.R. Ghosh, A. Paul, Design and implementation of a novel cryptographic technique for network security using genetic algorithms (gas), Int. J. Innov. Knowl. Concepts 119 (7) (2019).

[17] Naccache David, Reiter Michael, Cryptology and network security, Network 9 (10) (2012) 1–256, 9783319268231, 3319268236.

[18] 18. S.S. Khan, P.R. Tuteja, Security in cloud computing using cryptographic algorithms, Int. J. Innov. Res. Comput. Commun. Eng. (2015), https://doi.org/10.15680/ ijircce.2015.0301035.

[19] P. N. S. V. Keer, S. I. Ali, "Hybrid approach of cryptographic algorithms in cloud computing.".

[20] S. B. J. Fursan Thabit, Alhomdy, "A new lightweight cryptographic algorithm for enhancing data security in the cloud," Glob. Transitions Proc.

[21] A. Kalaivani, B. Ananthi, S. Sangeetha, Enhanced hierarchical attribute-based encryption with modular padding for improved public auditing in cloud computing using semantic ontology, Cluster Comput. (2019), https://doi.org/10.1007/ s10586-018-2346-1

[22] Zhang H, Ji Z, Wang H, Wu W. Survey on quantum information security. China Comm. 2019 Oct; 16(10): 1-36.

[23] Zhou L, Wang Q, Sun X, Kulicki P, Castiglione A. Quantum technique for access control in cloud computing II: Encryption and key distribution. J NetwComput Appl. 2018 Feb 1; 103: 178-84.

[24] Sharma G, Kalra S. Identity-based secure authentication scheme based on quantum key distribution for cloud computing. Peer PeerNetw Appl. 2018 Mar; 11(2): 220-34.

[25] Han J, Liu Y, Sun X, Song L. Enhancing data and privacy security in mobile cloud computing through quantum cryptography. In 2016 7th IEEE I Conf on Soft Eng and Service Sci (ICSESS) 2016 Aug 26: 398-401. IEEE.

[26] Mustafa I, Khan IU, Aslam S, Sajid A, Mohsin SM, Awais M, et al. A lightweight post-quantum lattice-based RSA for secure communications. IEEE Access. 2020 May 19; 8: 99273-85.

[27] Li J, Zhao Y, Yang Y, Lin Y. Verifiable Quantum Cloud Computation Scheme Based on Blind Computation. IEEE Access. 2020 Mar 19; 8: 56921- 6.

[28] Winick A, Lütkenhaus N, Coles PJ. Reliable numerical key rates for quantum key distribution. Quantum. 2018 Jul 26; 2:77.

[29] Murali G, Prasad RS. CloudQKDP: Quantum key distribution protocol for cloud computing. In2016 I Conf on InfComm and Emb Sys. 2016 Feb 25: 1-6. IEEE.

[30] Fatima S, Ahmad S. Quantum key distribution approach for secure authentication of cloud servers. Int J Cloud App Comp. 2021 Jul 1; 11(3): 19-32.

[31] Olanrewaju RF, Islam T, Khalifa OO, Anwar F, Pampori BR. Cryptography as a service (CaaS):

quantum cryptography for secure cloud computing. Indian J Sci Technol. 2017 Feb; 10(7): 1-6.

[32] Qiu L, Sun X, Xu J. Categorical quantum cryptography for access control in cloud computing. Soft Comput. 2018 Oct; 22(19): 6363-70.

[33] Matthews RA. The use of genetic algorithms in cryptanalysis. Cryptologia. 1993 Apr 1; 17(2): 187- 201.

[34] Sugumar R, Leelavathy L. Ensure Data Security and Privacy using DNA Symmetric Encryption Method in Cloud. J InfComput Sci. 2020; 10(3): 676-689.

[35] Wang B, Song W, Lou W, Hou YT. Privacy-preserving pattern matching over encrypted genetic data in cloud computing.IEEEIntConfIntell. ComputCommun. 2017 May 1: 1-9. Doi:10.1109/INFOCOM.2017.8057178

[36] C.E. Shannon, A mathematical theory of communication, Bell Syst. Tech. J. (1948), https://doi.org/10.1002/j.1538-7305.1948.tb01338.x.

[37] M.R. Biswas, K.M.R. Alam, S. Tamura, Y. Morimoto, A technique for DNA cryptography based on dynamic mechanisms, J. Inf. Secure. Appl. 48 (2019) 102363, https://doi.org/10.1016/j.jisa.2019.102363.

[38] H.M. Mousa, DNA-genetic encryption technique, Int. J. Comput. Netw. Inf. Secure. 8 (7) (2016) 1–9, https://doi.org/10.5815/ijcnis.2016.07.01.