ISSN: 0067-2904

A Key Based Hybrid Approach for Privacy and Integrity in Multi-Cloud

Mariam Duraid Abdul-Jabbar[1]*, Yousra abdul alsahib S.aldeen[2]
[1] *Collage of Science,Computer Science ,University of Baghdad, Baghdad, Iraq*
[2] *Collage of Science for women , Computer Science ,University of Baghdad, Baghdad, Iraq*

Received: 3/9/2022 Accepted: 26/12/2022 Published: 30/11/2023

Abstract

Before users store data in the cloud, many security issues must be addressed, as they will have no direct control over the data that has been outsourced to the cloud, particularly personal and sensitive data (health, finance, military, etc.). This article proposes a system based on chaotic maps for private key generation. A hybrid encryption for fast and secure cryptography. In addition to a multi-cloud storage with Pseudonymized file names to preserve user data privacy on the cloud while minimizing data loss. As well as a hash approach to check data integrity. AES in combination with RSA and fragmenting the file is used for the encryption. Integrity is cheeked using SHA-3. The experiments demonstrated that the key generation strategy may provide efficient keys in a shorter amount of time. Furthermore, the keys for the proposed approach passed NIST randomness testing. When cipher text fragmentation and encryption are combined, the average entropy value was (7.99). In addition, as file sizes grew, the total system's execution time increased only slightly.

Keywords: Cloud Computing (CC), Key generation, fragmentation, data integrity, encryption.

نهج هجين للحفاظ على الخصوصية وتكامل البيانات في الحوسبة السحابية

مريم دريد عبدالجبار[1]*, يسرى عبدالصاحب سيف الدين[2]
[1]علوم الحاسوب, كلية العلوم, جامعة بغداد, بغداد, العراق
[2] علوم الحاسوب, كلية العلوم للبنات, جامعة بغداد, بغداد, العراق

الخلاصة

قبل أن يقوم المستخدمون بتخزين البيانات في السحابة ، يجب معالجة العديد من مشكلات الأمان ، حيث لن يكون لديهم سيطرة مباشرة على البيانات التي تم الاستعانة بمصادر خارجية لها في السحابة ، وخاصة البيانات الشخصية والحساسة (الصحة ، والتمويل ، والجيش ، وما إلى ذلك). تقترح هذه المقالة نظامًا يعتمد على الخرائط الفوضوية لتوليد المفاتيح السرية ، والتشفير الهجين لتشفير السريع والآمن ، والتخزين متعدد السحابة بأسماء الملفات ذات الأسماء المستعارة للحفاظ على خصوصية بيانات المستخدم على السحابة مع تقليل فقدان البيانات ، بالإضافة إلى نهج التجزئة للتحقق من سلامة البيانات. أظهرت التجارب أن استراتيجية توليد المفاتيح قد توفر

*Email: mariam.doraid1201a@sc.uobaghdad.edu.iq

مفاتيح فعالة في فترة زمنية أقصر. علاوة على ذلك ، اجتازت مفاتيح النهج المقترح اختبار العشوائية NIST.
عندما يتم الجمع بين تجزئة النص المشفر والتشفير ، يكون متوسط قيمة الانتروبيا (7.99). بالإضافة إلى ذلك
، مع زيادة حجم الملفات ، يزداد وقت تنفيذ النظام الإجمالي بشكل طفيف فقط.

1. Introduction

Cloud computing is defined as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. According to the United States National Institute of Standards and Technologies (NIST), five basic qualities, three service models, and four deployment types make up this cloud model [1] .Cloud storage is a novel phrase coined by cloud computing technology and created by it. It is a storing pool concept that includes all types of storage devices, clustering applications, distributed systems, and software applications that store and access data for users. The use of the cloud is novel. More users (individuals, corporations, government agencies, and others) are benefiting from significant advances in cloud storage while also increasingly focusing on its services and applications. With the advancement of technology for networking and a growing need for IT services, an increasing number of enterprises and individuals are opting to outsource significant amounts of data to the cloud for processing and storage to save money on infrastructure [2].

Customers appreciate the convenience of cloud storage; however, cloud computing service providers have been gathering personal information such as identification, address, and sensitive information for the company's use from these services. To ensure that this data remain private in the face of curious adversaries and malevolent cloud service provider workers, privacy techniques have been employed [3]. The guarantee that digital data remains undamaged and that it can only be accessed or changed by authorized individuals is known as data integrity. For digital forensics and data reassurance, the integrity verification approach is crucial. Since data storage is location-independent, data integrity verification is a key issue in cloud computing. To check data integrity more quickly, the signature scheme and hash algorithms are commonly utilized [4].

Users' sensitive information deserves the highest level of privacy and security before being outsourced to the cloud. Encryption is a typical solution in this situation [5]. Various methods have been employed to verify data integrity, but hash value comparison has grown in popularity in recent years [6]. It is important to enter the initial data hash in a secured environment [7].

Multi-cloud, practitioners and specialists may refer to multi-cloud as a cloud-of-clouds. This term refers to the fact that the cloud computing environment must be expanded to include several unified and linked cloud service providers. It also means that, to avoid dependencies, sensitive data should not be supplied to a single Cloud Service Provider (CSP). It is a cloud scheme that allows enterprises to use several cloud computing platforms to perform multiple tasks. It empowers the organization to choose the services that best suit their requirements, and businesses commonly employ multiple CSPs for different aspects of their operations or use cases. Because they all come from multi-cloud, inter-cloud and cloud federation are frequently used interchangeably with hybrid cloud [8].

Cryptography can assist in increasing security-conscious enterprises adoption and use of cloud computing. It can help Cloud technology at the first level of security, which is secure storage. Encryption is the process of transforming data into unreadable forms in order to secure the safety of data transmissions. Cryptography nowadays is thought to contain three types of

algorithms: Symmetric-key, asymmetric-key, and hashing algorithms. The key challenges in Cloud computing are file system security, data safety, network traffic, backups, and host security. Encryption can address these concerns to some level [9].

We propose a hybrid encryption method to meet the privacy-preserving criteria, which is defined as the use of different cryptographic algorithms at the same time to increase data security. Hybrid cryptography [10] is a technique that combines symmetric and asymmetric algorithms. To offer and assure data integrity, combine file fragmentation with a Hash value.
The objective of the study:

- To offer a private mechanism for generating random keys.
- Create a data privacy-preserving hybrid-encryption with multi-cloud storage system that is quick and secure.

There are five sections to the rest of this article. Section 2 provides an overview of the literature and associated studies, focusing on encryption for privacy and hash value computing for integrity. The algorithms used in this work are presented in section 3, and flowcharts and the methodologies are then described in Section 4. Section 5contains the experimental result and evaluations. Section 6 includes the conclusion, and the future work.

2. Related Works

This section includes three subsections that briefly cover recent strategies and research for the privacy preservation and data integrity of sensitive and personal data or files that are uploaded or processed in the cloud:

A- Privacy-Preserving

OM PRAKASH JENA et al. in [11] presented a method for maintaining cloud privacy and security using a hybrid encryption methodology. The best asymmetric and symmetric encryption methods and technologies, respectively, are Elliptic Curve Cryptosystem (ECC) and Advanced Encryption Standard (AES). The AES-ECC hybrid cryptosystem combines the speed of the AES algorithm with the symmetrical session key exchange of the ECC technique. The suggested method minimizes the delay factor while also being computationally efficient, secure, and robust.

Santoso et al. in [12] used a 256-bit key produced by the Secure Hash Function (SHA) 256 function to combine two cryptographic techniques, AES (Advanced Encryption Standard) and Twofish. The technique makes data posted or downloaded in the Cloud system more secure.

K.Jaspin et al. in [13] described a security method that encrypts and decrypts files to improve security. They encrypt the files that users upload to the cloud using the double encryption method . The file is encrypted using the AES method first, then the RSA algorithm. The relevant keys are generated throughout the algorithm's execution. The level of security is raised with this method. They looked at the data confidentiality, security level, information protection, speed, and cipher text size, among other things. This method is more efficient since it satisfies all the criteria that conventional methods failed to meet. Drobox was used to store the file's content, which was in an encrypted format.

B- Data Integrity

Shivarajkumar Hiremath et al. in [14] proposed an effective public auditing approach employing Third Party Auditor(TPA) to evaluate the integrity of data stored in the cloud. The suggested auditing solution encrypts data with the AES algorithm and generates verification information or message digests for data integrity checks with the Secure Hash Technique (SHA-

2). The suggested technique is provably secure, according to the research, and TPA audits files of various sizes in a predictable amount of time.

Gaopeng Xie et al. in [15] improved on the shortcomings of previous system and proposed a blockchain-based cloud data integrity verification methodology. In their study, they suggested a lattice signature mechanism to resist quantum computing and supplied the cuckoo filter to reduce the computational load of the user verification phase. Finally, to replace traditional centralized audits, a decentralized blockchain network is incorporated to distribute and certify verification findings, boosting the scheme's transparency and security. According to security analysis, this technique can withstand cyberattacks, and testing results show that it is highly efficient, particularly during the user verification step.

C- Privacy-Preserving and Data Integrity

Mamun et al. in [16] proposed a hybrid AES/RSA method for calculating and ensuring the security of encrypted data with third-party confirmation. This is a proposal for a secure authentication system that protects both message privacy and validity of parties' communication . The fundamental goal of the encryption scheme is to prevent unwanted access.

Vikas et al. in [17] described a cloud data security solution that uses a combination of Secure Hash (SHA512) for integrity and Secure Hash (SHA512) for confidentiality to provide data at rest with secrecy and integrity. The AES random key generation algorithm is used to generate the 128-bit secret key in a secure manner. The RSA public key algorithm is used to encrypt this key. The SHA-512 algorithm is used to calculate the file's hash. The data is encrypted with AES and saved on a cloud server using an RSA key pair generator to generate a private key. The goal is to offer data owners with a high level of protection when storing sensitive data in the cloud.

Shani Raj and B. Arunkumar in [18] described a lightweight distributed cloud data encryption approach based on multi-cloud features .Multiple cloud computing providers provide storage services in a heterogeneous environment. To provide secrecy, safe data storage, and file sharing, the suggested system employs a multi-cloud environment. When compared to established procedures, quantitative results show that the suggested mechanism is practicable.

Most current systems rely on a trusted third party, a single cloud for storage, and encryption employing asymmetric techniques that take a long time to encrypt/decrypt or are subject to assaults. As a result, an effective and safe plan for safely storing data on the cloud must be devised, ensuring data privacy and data integrity verification, as well as avoiding data loss as much as feasible.

3. Preliminaries

This study proposes a solution based on the production of private keys using a chaotic map (described in subsection A) and cryptographic methods (described in part B).

A- Chaotic maps

Logistic map: - The follows is the most commonly investigated and used chaotic system:

$$u_{n_{+1}} = \mu \times u_n \times (1 - u_n) \quad (1)$$

The abovementioned Equation (1) is referred to as a logistic map. The above equation's behavior is controlled by the μ and its range is (0, 4). When the Logistic system's values are changed from 0-3, there is no chaos. The Logistic map's initial seed is u0, and its output sequence is un, which can be pseudo-random or not depending on the value. When you get to

3.569945672, a standard logistic map starts to become chaotic. To deal with the dispersion and confusion, a logistic map = 3.9999 is utilized [19].
Two-Dimensional Logistic-Adjusted-Sine Map (2d-lasm):- Defined mathematically as:

$$x_{i+1} = sin(\pi\mu(y_i + 3)x_i(1 - x_i)) \quad (2)$$

$$y_{i+1} = sin(\pi\mu(x_{i+1} + 3)y_i(1 - y_i)) \quad (3)$$

Where [0, 1] is a parameter of x, y value ranges. 2D-LASM is made up of Sine and Logistic maps. Before being fed into the Sine map's input, scaling is used to the logistic equation xi(1 xi). Then, the phase plane is increased from 1D to 2D. The output pairs (xi+1, yi+1) of 2D-LASM are spread across the 2D phase plane as a result of two inputs interacting in an interactive way. Its outputs are difficult to predict since it has a more complex structure than Sine and Logistic maps [20].

B- The Cryptography algorithms

Message-Digest Algorithm (MD5):- MD5 is a hashing (message-digest) algorithm. It accepts any amount of data as input and produces digested output with a length of 128 bits that is specified. The MD method has a 512-bit block size that is partitioned into 16 32-bit subblocks [21].

Advanced Encryption Standard (AES):- is a block cipher with a 128-bit block length. The method's initial input is saved in a 4x4 byte matrix named State, on which actions are performed. There are three different key lengths to choose from: 128 bits, 192 bits, and 256 bits. For key lengths of 128, 192, and 256 bits, the number of rounds is 10, 12, and 14, respectively. Substitute Bytes, ShiftRows, MixColumns, and AddRoundKey are all included in each round [22] [23] .

Rivest–Shamir–Adleman (RSA):- Named with the initials for Rivest–Shamir–Adleman. The RSA technique offers asymmetric cryptography. Rivest, Shamir, and Adleman, three mathematicians, introduced the RSA encryption technique for the first time in 1978. The RSA algorithm, unlike symmetric cryptosystems, contains two distinct keys, one of which is a public key and the other a private key. Only the corresponding private key can decrypt data encrypted with a public key; data encrypted with a private key can only be decrypted with the matching public key [24].

Winternitz One-Time Signature Plus (WOTS+):- is a one-time signature mechanism based on the Winternitz signature. Winternitz signatures are one-time digital signatures that may be used in conjunction with existing hash-based digital signatures that can sign multiple messages. It was proposed by Hülsing in 2013. It has been proven to be extremely unforgeable in the standard model under selected message attacks, and has a smaller signature size than older WOTS schemes [25] [26].
Secure Hash Algorithm 512 (SHA-512):- The SHA 512 algorithm, which is a one-way hash function, was devised by Ron Rivest. In general, the SHA 512 hash function provides the same hash process as the SHA 2 hashing algorithm. The SHA 512 hash algorithm generates message digests of a 512-bit size and a block length of 1024 bits. This cryptographic technique accepts any message length as input and generates a message digest with a length of 512 bit. Due to its long hash value, which makes it more resistant to assault than any other hash function, SHA 512 is regarded as a fast and strong hash function [27]

4. Privacy- Data Integrity Proposed System

The proposed system based on key generation, data encryption, and fragmentation will be addressed in this section, which includes both file uploading and downloading. The solution uses hybrid cryptography for uploading privacy and downloading integrity checks in a multi-cloud context.

4.1 Upload file:

Figure 1 represent the file uploading workflow and the system architecture.

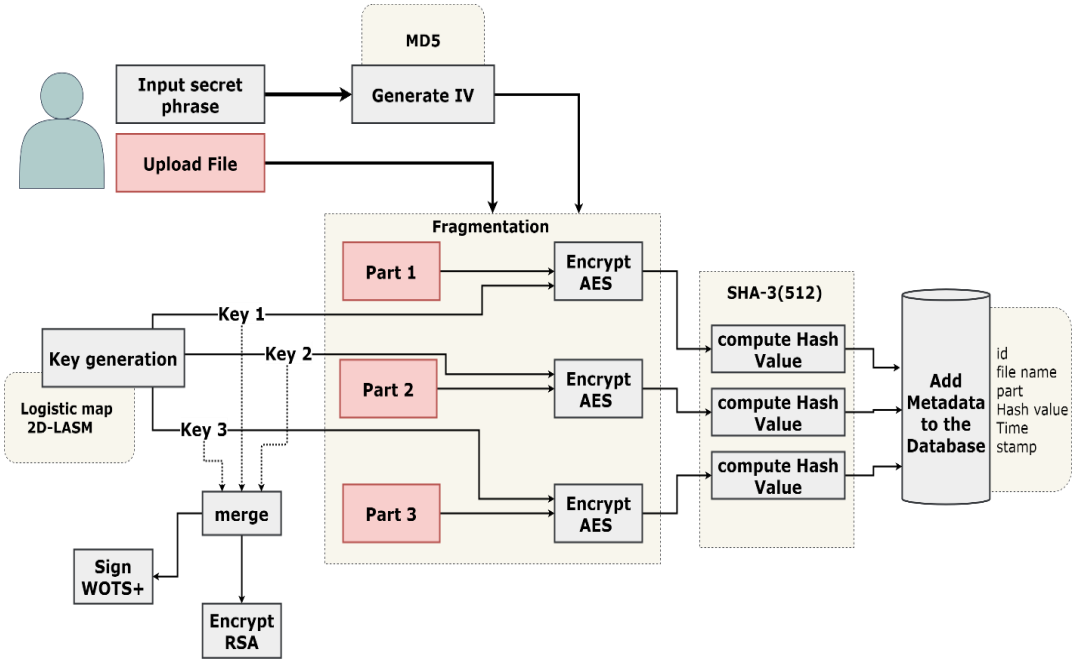

Figure 1: Proposed system architecture

1) Key generation: in this stage, three random numbers are generated, one using a logistic map and the other two using a 2D-LASM. Then all three numbers are XORed and transformed into characters as shown in Figure 2. This procedure is repeated until the key size is 256 bits long. This phase is repeated three times to generate three distinct keys, which are then merged to produce the final key.

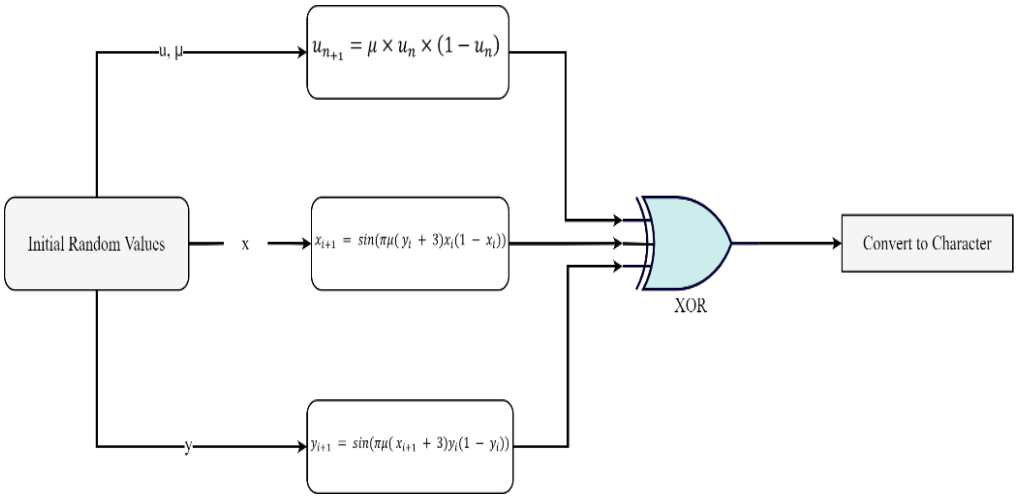

Figure 2 random number generation process

2) AES 128-bit Initial Vector (IV) generation: The AES 128-bit 1st IV is created by hashing a secret word supplied by the user with MD5. The 2nd IV generated by calculating the hash value for the generated 1st IV, and the 3rd by hashing the 2nd result. Each IV is then used as parameter for the next part.

3) Fragmentation: Separating data into parts increases cloud data privacy by limiting the possibility that an attacker will gain access to all of it (parts will be meaningless). However, splitting data into a large number of parts may generate overhead. Thus, the data is divided into three equal portions in this study, which improves encryption and reduces time.

4) Encryption: To improve security while reducing time complexity. A hybrid approach is used to carry out the data encryption process. This hybrid approach utilizes the symmetric AES algorithm, which is fast and difficult to break due to its larger key size (in this paper, a 256-bit key is used). Each generated key of the three keys is used to encrypt one of the parts with its generated IV. The asymmetric RSA algorithm is used to encrypt the merged keys which is a combination of the three generated keys, to secure the secret key transmission. Figure 3 show an example of processing result:

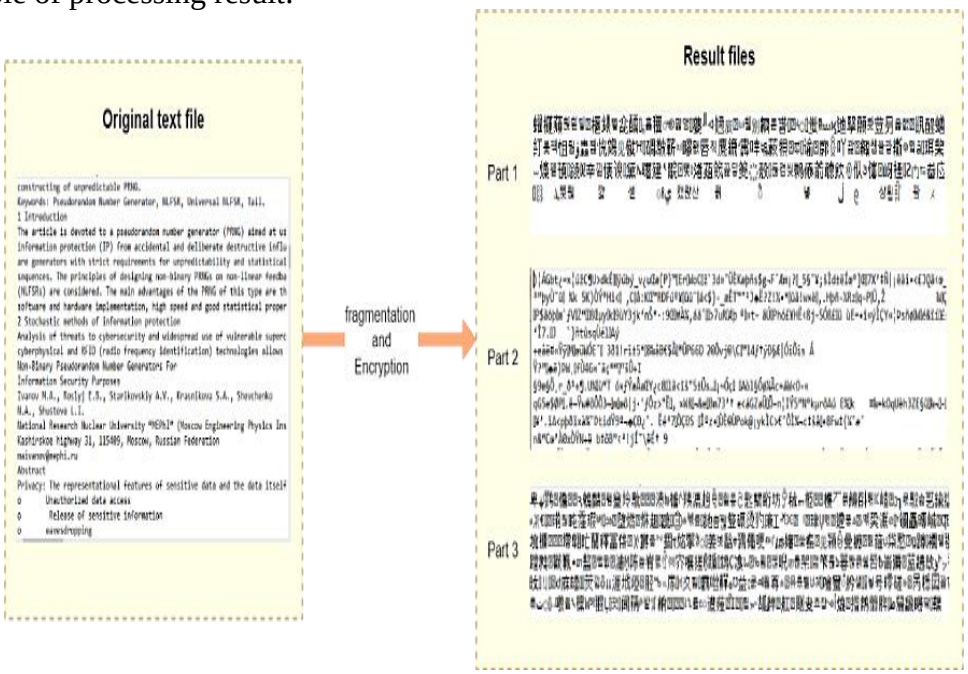

Figure 3: A result example

5) Computing hash values: for each encrypted part, the hash value is computed using SHA-3 (512-bit) before being sent to the cloud storage. The results are utilized for integrity checks. These hash values are saved in a lookup table alongside other file metadata, such as file name, part number, timestamp, and an ID, which will be used to Pseudonymize (change file name) the file part by changing its name to the ID before sending it to cloud storage. The three portions are distributed across three distinct cloud storages, making it easier and safer than storing a single entire file on the cloud. Transparency is provided, as well as a reduction in uploading time and the risk of losing all data at once.

6) Digital signature: For the merged keys, the post-quantum W-OTS+ is employed to generate a digital signature.

4.2 Download file:

1- The user selects a file
2- the parts pseudonym is retrieved from the lookup table.
3- the parts are downloaded from multi-cloud storage and checked for integrity by computing the hash value and comparing it to the value saved in the lookup table.

Which is the mechanism of checking a part's integrity shown in the Figure 4:

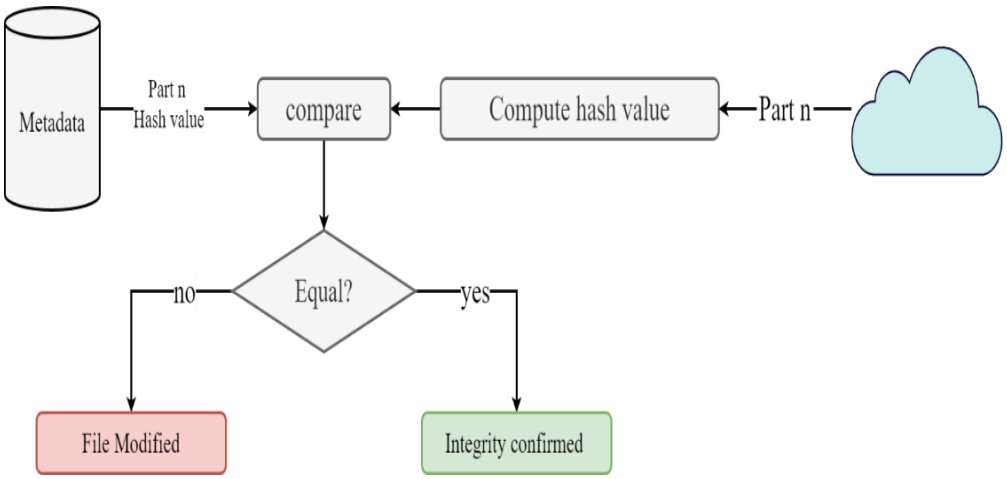

Figure 4 Integrity checking

5. Results and Discussion

Examination results for the proposed system involved three parts: the NIST test for randomness, cipher text entropy, and system execution time.

Windows 10 was used to run and test the proposed system (laptop computer). x64-based computer with Intel(R) Core(TM) i5-5300U CPU @ 2.30 GHz, 8 GB Random Access Memory (RAM), 64-bit operating system(OS), and Intel(R) Core(TM) i5-5300U CPU @ 2.30 GHz.

A- NIST test

The NIST Test Suite consists of 15 statistical tests to that are used to validate the randomness of the generated Pseudo Random Number Generator (PRNG). In this paper, a 12 tests was used to examine the private random generated 256-bit key and 14 tests for the final merged key with hybrid chaotic maps because these tests are the most suitable for the generated sequence size, and the binary sequence success in the test when the value>=0.01, Table shows the results.

Table 1: NIST test of private key generation

Test name	P-value(256-bit)	Result
Frequency	0.1691314447026715	Pass
Frequency within a Block	0.3855343441745786	Pass
Run	0.7004768311479884	Pass
Longest Run	0.1190728723337719	Pass
(Spectral)	0.4220007050375904	Pass
Non-Overlapping Template Matching	0.0537656961481751	Pass
Serial test	0.4989610874592239	Pass
Approximate Entropy Test	1.0	Pass
Cumulative Sums (Forward)	0.2363349604766558	Pass
Cumulative Sums (Reverse)	0.2672152143830609	Pass

Random Excursions	P-value	Chi-Squared	
	0.9625657732472964	1.0	Pass
Random Excursions Variant	P-value	count	
	1.0	6	Pass

The results in table 1 indicate that the randomness of the generated private key is good, and the highest value is the approximate entropy test.
The test was also applied to the merged key and the result are represented in Table 2.

Table 2: NIST test for merged key

Test name	P-value(256-bit)	Result
Frequency	0.1309655569884592	Pass
Frequency within a Block	0.8917931772546183	Pass
Run	0.8917931772546183	Pass
Binary Matrix Rank Test	0.039104615860550376	Pass
(Spectral)	0.13443822042726827	Pass
Non-Overlapping Template Matching	0.982122103944362	Pass
Overlapping Template Matching Test	0.48841560242748283	Pass
Linear Complexity Test	0.1246475556641696	Pass
Serial test	0.1246475556641696	Pass
Approximate Entropy Test	0.9971132680230932	Pass
Cumulative Sums (Forward)	0.24686390426495647	Pass
Cumulative Sums (Reverse)	0.1932908193693051	Pass
Random Excursions	0.8048081134311252	Pass
Random Excursions Variant	0.9357741458363251	Pass

These results show that the merged key also passed the tests with a good results, and the best obtained result was the approximate entropy.

B- Entropy

Entropy is a measure of unpredictability; the higher the entropy value, the more randomness in the file. For encryption testing, a suitable entropy number is closer to 8. Table 2 shows a comparison of the entropies of three different size text files containing letters, numbers, and symbols with their cipher text result from the proposed system.

Table 3: Entropy results

Text file size (kb)	Entropy of the plain text	Entropy of the cipher text
15	4.60335	7.989
30	4.727	7.9945
60	4.611	7.9966

The entropy result of the cipher text is close to 8, and there is a high difference between the entropy of the plain text and the result cipher-text.

C- Executions Time

In this subsection, the encryption and fragmentation performance by the time taken to execute and output the result cipher text are analyzed.

Figure 5 shown the execution time of fragmentation and AES encryption on three text files of different sizes

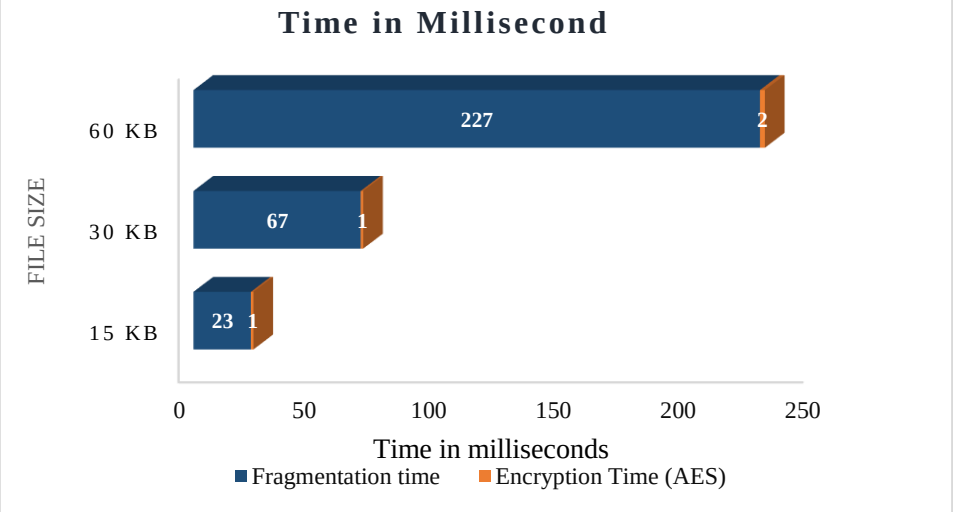

Figure 5 Fragmentation and Encryption Execution time

Figure 6 depicts the overall system execution time for the three text files, taking into account the processes that are unaffected by file size. The approximate fixed values are IV generation=0ms, Key generation =6ms, RSA=670ms, and wots+=156 ms. Because RSA is much slower than AES, it was used to encrypt the merged AES keys, which output size is 768-bit. The hybrid encryption added extra security in less time and using the iv generating process added more privacy in addition to the key. The fragmentation process with different key encryption led to less data loss, increased the entropy for the file, and helped to figure the malicious cloud storage. The pseudonymization kept the file name private from anyone accessing the cloud, thus it is useful with public cloud specifically.

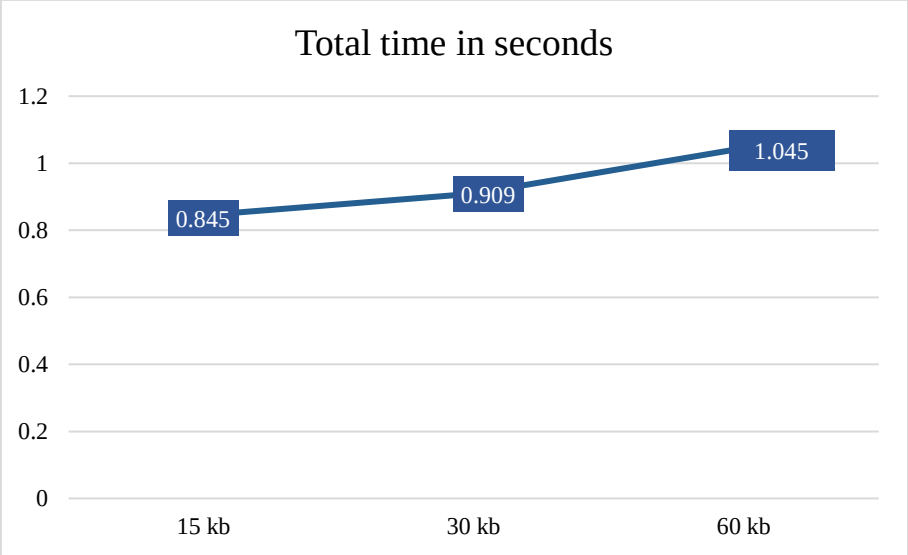

Figure 6: Total execution time

6. Conclusions and Future Works

Cloud computing has several severe drawbacks despite all its capabilities and advantages. The most significant drawback is that it targets users' sensitive and personal data, thus jeopardizes the privacy and data integrity. This paper proposes a system architecture based on chaotic maps for private key generation, hybrid encryption for safe and fast encryption. In addition to a multi-cloud storage with Pseudonymized file names to keep user data private in the cloud and limit data loss as much as possible, as well as a hash technique to ensure data integrity. Our key generation technique can produce efficient keys while requiring less time to apply, according to the findings of our experiments. Furthermore, the keys generated by the proposed technique satisfy the NIST randomness tests, and the system's execution time increases significantly as the file size grows larger; the average entropy value for fragmentation and encryption of the cipher text was (7.99).

The suggested system can accommodate text files and, in the future, might be modified to accept all types of data files, including images, video, and audio. Reducing encryption time/decryption time can be achieved by employing lightweight encryption techniques and set up an experiment against an attack that isn't implemented in the experimental results. Finally, authentication and data availability should be considered.

References

[1] Mell, P., & Grance, T., "The NIST Definition of Cloud Computing," 2011. [Online]. Available: http://faculty.winthrop.edu/domanm/csci411/Handouts/NIST.pdf.

[2] Shao, B., Bian, G., Wang, Y., Su, S., & Guo, C., "Dynamic Data Integrity Auditing Method Supporting Privacy Protection in Vehicular Cloud Environment," *IEEEACCESS,* Vols. 6,, pp. 43785-43797, 2018..

[3] Yang, P., Xiong, N., & Ren, J., "Data Security and Privacy Protection for Cloud Storage: A Survey," *IEEEACCESS,* vol. 8, pp. 131723-131740, 2020.

[4] Gangadevi, K., & Devi, R. R., "A survey on data integrity verification schemes using blockchain technology in Cloud Computing Environment," *IOP Conference Series: Materials Science and Engineering* , vol. 1110, no. 1, p. 012011), 2021.

[5] R. Bingu, S. Jothilakshmi and N. & Srinivasu, "A Comprehensive Review on Security and Privacy Preservation in Cloud Environment," *Sustainable Communication Networks and Application,* vol. 93, pp. 719-738, 2022.

[6] K. Gangadevi and R. R. Devi, "A survey on data integrity verification schemes using blockchain technology in Cloud Computing Environment," *IOP Conference Series: Materials Science and Engineering,* vol. 1110, no. 1, p. 012011, 2021.

[7] G.O.Ogunleye and S.E.Akinsanya, "Elliptic Curve Cryptography Performance Evaluation for Securing Multi-Factor Systems in a Cloud Computing Environment," *Iraqi Journal of Science,* vol. 63, no. 7, pp. 3212-3224, 2022.

[8] Nzanzu, V. P., Adetiba, E., Badejo, J. A., Molo, M. J., Takenga, C., Noma-Osaghae, E., ... & Suraju, S., "Monitoring and resource management taxonomy in interconnected cloud infrastructures: a survey," *TELKOMNIKA Telecommunication Computing Electronics and Control,* vol. 20, no. 2, pp. 279-295, 2022.

[9] Nigoti, R., Jhuria, M., & Singh, S., "A Survey of Cryptographic Algorithms for Cloud Computing," *(IJETCAS),* vol. 123, no. 13, pp. 141-146, 2013.

[10] Alharbi, M. F., Aldosari, F., & Alharbi, N. F., "Review Of Some Cryptographic Algorithms In Cloud Computing," *IJCSNS,* vol. 21, no. 9, pp. 41-50, September 2021.

[11] Jena, O. P., Tripathy, A. L. A. K. A. N. A. N. D. A., Swagatam, S. A. M. B. I. T., Rath, S. M. I. T. A., & TRIPATHY, A. R., "DUAL ENCRYPTION MODEL FOR PRESERVING PRIVACY IN CLOUD," *Advances in Mathematics: Scientific Journal,* no. Spec. Issue, pp. 6667-6678, 2020.

[12] Santoso, K. I., Muin, M. A., & Mahmudi, M. A. , "Implementation of AES cryptography and twofish hybrid algorithms for cloud," *Journal of Physics: Conference Series,* vol. 1517, no. 1, p. 012099, 2020.

[13] Jaspin, K., Selvan, S., Sahana, S., & Thanmai, G., "Efficient and Secure File Transfer in Cloud Through Double Encryption Using AES and RSA Algorithm," *International Conference on Emerging Smart Computing and Informatics (ESCI),* vol. 2021, no. April , pp. 791-796, 2021.

[14] Hiremath, S., & Kunte, S., "A Novel Data Auditing Approach to Achieve Data Privacy and Data Integrity in Cloud Computing," *International Conference on Electrical, Electronics, Communication, Computer and Optimization Techniques (ICEECCOT),* vol. 2017, pp. 306-310, 2017.

[15] Xie, G., Liu, Y., Xin, G., & Yang, Q., "Blockchain-Based Cloud Data Integrity Verification Scheme with," *Hindawi ,Security and Communication Networks,* vol. 2021, p. 15, 2021.

[16] Al Mamun, S., Mahmood, M. A., & Amin, M. A., "Ensuring Security of Encrypted Information by Hybrid AES and RSA Algorithm with Third-Party Confirmation," *5th International Conference on Intelligent Computing and Control Systems (ICICCS),* vol. 2021, no. May, pp. 337-343, 2021.

[17] Soman, V. K., & Natarajan, V., "Analysis of Hybrid Data Security Algorithms for Cloud," *Second International Conference on Networks and Advances in Computational Technologies -springer,* vol. 2021, pp. 231-242, 2021.

[18] Raj, S., & Arunkumar, B., "Enhanced encryption for light weight data in a multi-cloud system," *Distributed and Parallel Databases- Springer,* vol. 2021, no. April , pp. 1-10, 2021.

[19] Firdous, A., Rehman, A. U., & Missen, M. M. S., "A Gray Image Encryption Technique Using the Concept of Water Waves, Chaos and Hash Function," *IEEEAccess,* vol. 9, pp. 11675-11675, 22 January 2021.

[20] Hua, Z., & Zhou, Y., "Image encryption using 2D Logistic-adjusted-Sine map," *Information Sciences,* vol. 339, pp. 237-253, 2016.

[21] Bermani, A. K., Murshedi, T. A., & Abod, Z. A., "A hybrid cryptography technique for data storage on cloud computing,," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 24, no. 6, pp. 1613-1624, 2021.

[22] Abdulazeez, A. M., & Tahir, A. S, "Design and Implementation of Advanced Encryption Standard Security Algorithm using FPGA," *International Journal of Scientific & Engineering Research,* vol. 4, no. 9, pp. 1988-1993, 2013.

[23] Kochar, T., Nandi, S., & Biswas, S., "A Single chip implementation of AES cipher and Whirlpool hash function," *2009 Annual IEEE India Conference-IEEE.,* vol. 2010, pp. 1-4, 2009.

[24] Lin, R., & Li, S., "An Image Encryption Scheme Based on Lorenz Hyperchaotic System and RSA Algorithm," *Security and Communication Networks,* vol. 2021, no. Apr, p. 18, 2021.

[25] A. Hülsing, "W-OTS+ – Shorter Signatures for Hash-Based Signature Schemes," in *Progress in Cryptology -- AFRICACRYPT 2013*, vol. 7918, Youssef, Amr, Nitaj, Abderrahmane and A. Hassanien, Eds., Berlin-Heidelberg, Springer, 2013, p. 173–188.

[26] Roh, D., Jung, S., & Kwon, D., "Winternitz Signature Scheme Using Nonadjacent Forms," *Security and Communication Networks,* vol. 2018 , no. Jun, p. 12, 2018.

[27] Sumagita, M., Riadi, I., Sh, J. P. D. S., & Warungboto, U. , "Analysis of Secure Hash Algorithm (SHA) 512 for Encryption Process on Web Based Application," *International Journal of Cyber-Security and Digital Forensics (IJCSDF),* vol. 7, no. 4, pp. 373-381, 2018.