DOI: https://doi.org/10.33103/uot.ijccce.22.1.10

Framework For Modeling and Simulation of Secure Cloud Services

Teaba W. Khairi
Department of Computer Science, University of Technology, Baghdad, Iraq
teaba.w.khairi@uotechnology.edu.iq

Abstract— *Many companies recognize the importance of cloud computing all around the world. However, various worries keep businesses from adopting cloud computing. Data security, privacy, and trust difficulties are among them. Recently, there have been rapid developments in the progression of cloud computing services. This paper focuses on the design and implementation of the secure cloud services framework by providing secure and trusted storage for user data. Proposed framework generated an encryption key based on a chaotic map generator and encrypted user data. proposed work shows that integration of key with defensive options is more efficient than approaches from those categories of using external keys. A test has been applied on the frame work in cloud slime services and show the effectiveness of the proposed solution to provide secure cloud services. Our model of cloud services show valid ad promising performance with multiple users trail.*

Index Terms— *logistic map , cloud services frame , chaoticmap.*

I. INTRODUCTION

The widespread use of high-speed Internet and the widespread availability of low-cost machines are transforming the high-performance computing paradigm. Simultaneously, businesses must examine massive volumes of data to forecast future trends and justify their business strategies' acceptance. Without a readily available cloud infrastructure, the subsequent extensive data analysis and massive storage requirements are impossible. As a result, cloud computing is a new paradigm that is fast gaining traction. It provides virtualized, scalable resources as Internet-based services [12].

Hybrid, private, and public clouds are the three types of cloud computing that exist. A public cloud is one in which cloud providers use the internet to generate resources such as storage and applications. The data center architectures exclusively owned by a firm are referred to as private clouds. Provisioning, scalability, adaptability, monitoring, and automation are some of the services provided by the cloud provider [6]. A private cloud aims to reap the benefits of cloud architecture without sacrificing control over the data center's upkeep. On the other hand, the hybrid strategy involves businesses using the public cloud while keeping internal control over a private, managed data center [1].

The sharing of data with a Cloud Service Provider (CSP) is viewed as adopting cloud computing by companies and people. Both Cloud Service Users (CSUs) and CSPs lose ownership of their data when using the cloud paradigm. Experts in cloud security have highlighted reservations about storing highly private data in the infrastructure [13]. Loss of control, for example, refers to a situation in which a cloud user's control over their data is eroded as data is transferred from local servers to remote cloud servers

Received 16/August/2021; Accepted 18/October/2021

ISSN (Print) 1811-9212 *ISSN (Online) 2617-3352*

DOI: https://doi.org/10.33103/uot.ijccce.22.1.10

[19]. On the other hand, cloud computing is thought to be hacker-proof, making it a popular choice for storing sensitive information [2], [3], [10].

An introduction of the innovative idea of building a model to provide secure cloud services by exploiting user data and knowledge within the concept of the infrastructure of a service. In this situation, given the work that has been described in this paper, the question now is whether or not private cloud storage could protect user data and camouflage the threat actor.

The Cloud Service threat profile is described below. An attacker can convert these threats into exploits and compromise the corresponding infrastructure or Cloud Services application in the right circumstances [9], [11]. The following is how the rest of the paper is organized: The following section discusses the current options. The third section explains the proposed solution. The forth section Depicts a secure cloud computing environment implantation. Finally, in section 5, the conclusion and future research directions are discussed.

II. RELATED WORK

Cloud providers appear to be unaware of the confidentiality and security requirements for data stored on their servers. On the other hand, the user has no control over the system security apparatus or the other services that share the same resources. This raises a slew of security and privacy concerns [15].

In this section an initial display of the current solution that is proposed to provide secure cloud frame work.

Chinnasamy et al. utilized modeling techniques and developed tools with the purpose of establishing a secure cloud storage system for healthcare data. Asymmetric algorithms are used to encrypt the data, whereas symmetric algorithms are used to encrypt the keys. The technique has drawbacks due to its inability to manage processes and distribute users' encrypted and decrypted keys.

The model incorporates the keys of user of each transaction and generates these keys to provide secure cloud storage. For those reasons, a proposed to work on the keys generation as a final means of representing the secure cloud provider [4].

M. Abibulla et al. demonstrated that ordinary four sorts of keys used: SymmetricKey, AsymmetricKey, PublicKey, PrivateKey & PreShared Key. The Advanced Encryption Standard (AES) algorithm can in turn lead to a minimal probability of cracking the same. This paper also showed how to exploit cryptography as a programmed mathematical tool that plays a pivotal role in network security. In this regard, the identification of transaction of each user request and develop the method of visual to encrypt and decrypt the image [5].

Interestingly, the methodology was an integrate over the AES algorithm, mentioned above as the solution is capable of providing secure cloud services upon postulate the encryption characteristics but not just confined to user data with visual method.

The research article by Kukatlapalli, Cherukuri R.C., and colleagues developed a methodology for ensuring secrecy for protected data using access control methods. Access specifiers assist us in determining the scope of permissions granted to users for properly using data records. There are certain disadvantages to this method in that the findings are complex owing to the complexity of the access control mechanism [6].

Other similar studies by Shehzad A. C., Taeshik S., and others established that even the Cyber-Physical System (CPS) is "a NetworkedSystem comprised of cyber (communication and computing) and physical components (actuators and sensors)." Computing and communication capabilities are being more

Received 16/August/2021; Accepted 18/October/2021

DOI: https://doi.org/10.33103/uot.ijccce.22.1.10

incorporated into physical creatures and things. A trusted authority may utilize the secure authentication technique to create a key agreement between the user and the cloud server. One drawback is that end-to-end frameworks are tailored for each task, and each feature adds significant overhead to the "CloudNetwork" [7].

III. APPROACHES AND METHODS

Cryptography in Logistic Map theory: Cryptography with many algorithms and with deterministic chaos has been developed. Thus, the main advantage that the chaos provides is the ability to produce multialgorithm solutions, owing to the potential development of the unlimited numbers of an algorithm [16]. The approach of the multialgorithm results from the use of dissimilar algorithms for the encryption processes of the different blocks of the data, which also participate considerably in solving the problem of a short-cycle length, which is related to chaotic iterations [14], [9], [20].

A logistic map is a one-dimensional map that may be used to describe "nonlinear discrete systems in a simple manner." The logistic map may be explained using "the recursive function," as shown below:

$$\mathbf{X_{n+1} = L\,(r - Xn)\,Xn = (1 - Xn)} \tag{1}$$

r represents the parameter and **X_n [0, 1]**. Looking at the logistics map, **L: [0 ، 1] → [0 ، 1]**, based on Eq. **(1)**, the parameter **r** is located in the interval **(0, 4]** [17].

The Lyapunov exponent that can be presented by Eq. (2):

$$\mathbf{LE= \frac{1}{n} \sum_{i=1}^{n} ln|f'(xi)|} \tag{2}$$

Accordingly, it is now possible to confirm the dynamic behavior of the various values of parameter **r** that are mentioned above [17].

a. **Logistic Maps with Multiple Parameters:** Recently, many techniques that are related to information encryption have used chaotic maps with 1 dimension due to it being highly efficient and simple. However, it contains various shortcomings, including small key spaces and poor security. Therefore, logistics maps with one or many parameters have been employed to overcome those shortcomings. The map provided here is based on the parameter r, which was set to 4 from 3.57, and "the chaotic behavior" is depicted in the map, as seen in *Fig. 1* and *Fig. 2* [18].

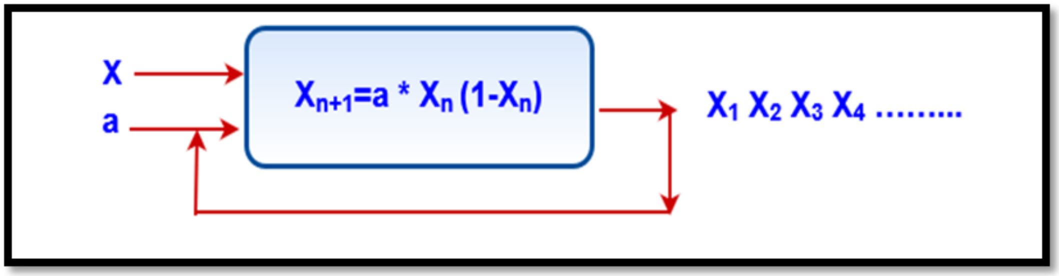

X
a
X_{n+1}=a * X_n (1-X_n)
X_1 X_2 X_3 X_4 ....

FIG. 1. LOGISTIC MAP WITH 1 PARAMETER [17]

Here, **a = (0.4]** and **0 < X_n < 1**.

Following extraction of the "values from the model," as can be seen in the formula in *Fig. 5*, "where 0 < X < 1, all of these values will be transferred, which are then extracted, to a binary system," as follows:

Received 16/August/2021; Accepted 18/October/2021

DOI: https://doi.org/10.33103/uot.ijccce.22.1.10

if $X_{n+1} < 0.5$ 0, if $X_{n+1} \geq 0.5$ 1

b. Two-parameter logistic map

Fig. 2 represents a logistic map with 2 parameters.

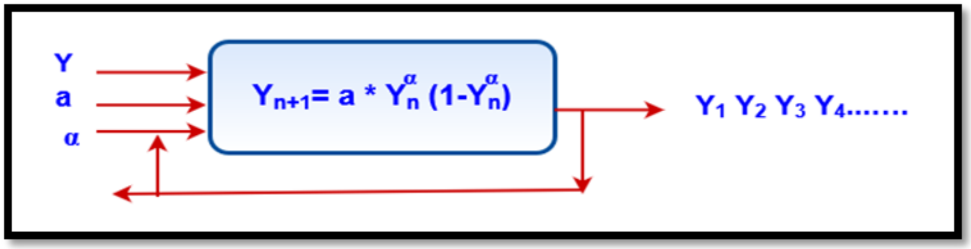

Y
a
α
$Y_{n+1} = a * Y_n^\alpha (1-Y_n^\alpha)$
Y_1 Y_2 Y_3 Y_4.......

FIG. 2. LOGISTIC MAP WITH 2 PARAMETERS [17]

Here, **a = (0.4], *α*= 0.5,** and **$0 < Y_n < (0.5)^2$**.

As with the first formula, an extraction procedure will be used to the values from the second formula, transferring them all to a "binary system": **if $Y_{n+1} < 0.5$, if Yn+1 ≥ 0.5 1**

IV. BUILD SECURE CLOUD SERVICES FRAMEWORK

Now a description of the way dynamic display is generated for the framework. The purpose of this article is to provide a framework for the provision of safe cloud services. The proposed solution manipulates each user request and secures user data by encrypting it using a logistic map. This prevents the case from being characterized as unclear that the user's account is likely to be hacked and the computer is controlled by a risky player. A secure user request is characterized in this work by its use of secure virtual resources.

"Security for virtual work" in cloud computing must be on-demand and simple to use. The transmission of data and its storage are two distinct processes. It may create a complete working platform by renting both virtual clod slim and the data security service. This may be accomplished via the following factors:

Propose a generic security architecture for virtual work on cloud computing. Create a transparent encryption system that is built on a hybrid of authentication and relay clouds.

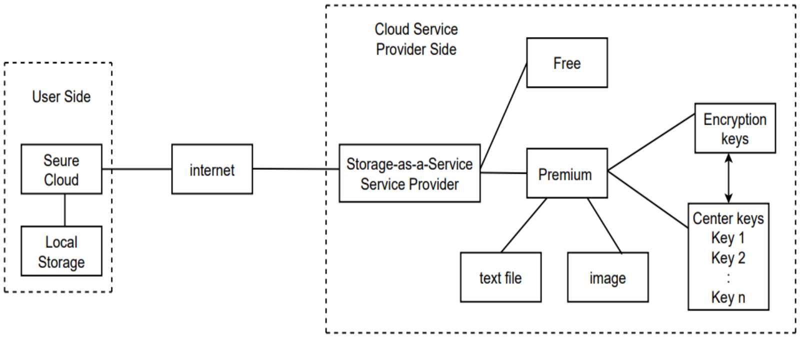


FIG. 3. FRAMEWORK OF SECURE CLOUD SERVICES

Received 16/August/2021; Accepted 18/October/2021

ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

The initial layer of this architecture, shown in *Fig. 3*, is transparent encryption, which encrypts all data on virtual machines, whether they are in storage clouds, clients, or during transmission.

The second tier consists of a storage cloud that stores online data for clients, a cloudslim tunnel that connects clients to the storage cloud, and clients that act as an interface between the cloud platform and its customers. Additionally, it may be a thick client that stores a portion of the user's data and installs service software to provide the service. The client may be a thin client, which serves as a single point of contact between cloud computing and its users.

User request: User requests could come in a variety of forms and shapes. People, businesses (organizations), Non-Governmental Organizations (NGOs), governments, and third-party security evaluators are among the clients. The Protection Administration Interface is how Cloud Clients engage with the cloud environment (PMI).

Secure cloud service as Infrastructure: "Cloud Storage" implies it is a virtual space used to store large amounts of data. However, users are concerned that do not have a control over their data; this control is taken over by cloud providers, prompting users to question their data security in the cloud . One of the most severe security issues is protecting data in the cloud. Only authorized personnel can access the data, while "data integrity" refers to data that has not been altered. The process of validating a user's authorization is known as authentication. The availability of data when it is requested is referred to as data availability.

Virtual Database: A virtual database gives a one-to-many based on a hash map database that is built around several vendor endpoints that represent the same class of data. It is considered as a way to handle every user request. Depending on the users, the data produced from the user upload will be kept in a sequence of vectors. Each vector will eventually contain data and display a well-organized object structure for rapid and efficient manipulation. A creation of data structure code is to read and append data from the user data to a vector. Following the collection of a large settings site, user data is loaded into a high voltage vector for each data storage parameter. Each vector generates a unique structure for the user's data inside an index in a hash table within the segment object. The proposed framework performed two steps that resulted in the creation of a hash table using the method described below:

- The hash table of an object can have numerous segments.
- The object can be recognized, and the cluster of data that will be deposited in each section is already known. At this point, a clear vision for the user request and portion of the user task has a central cluster [8].

Another essential aspect is that the procedure outlined above will allow us to acquire the user's data, in this example, the data uploaded by the user. As a result, caught the picture and text user data and the storage is needed for the task step within the user request, which can be used to store data for the model. To clarify, after a user completes a task, the following step is to create a process in the cloud resources. Then, for the processes saves the system resources. Another stage is to create a process in the operating system on the user's machine and preserve system resources because the methods are stored as the user performs a function. As previously stated, completing the operation only takes the form of a vector. For this reason, our framework can be used to predict user behavior based on the user task. Above all is recognition for the user's request within a task on a specific day and time.

Built-In Key Management: Encryption is another critical aspect of the database. Encryption requires the use of two keys, one of which is referred to as the master key, and the other as the data encryption keys. This encryption method safeguards the data's privacy. The author elaborates on the security measures in

Received 16/August/2021; Accepted 18/October/2021

DOI: https://doi.org/10.33103/uot.ijccce.22.1.10

this article by allowing the control to be placed closer to the data and by offering the options for tightening the security of current applications.

Premium cloud storage Services: Premium refers to secure services that our framework offers. Data loss causes issues with data integrity and confidentiality. According to a study conducted by International Data Corporation (IDC), most Cloud Info Services CIOs are concerned about losing control as a significant security issue connected with cloud computing . When the hosting CSP management controls user data, it becomes more vulnerable to damage, especially during provider transitions. When data is hosted on a remote cloud service, it is likely to lose its anonymity. Encryption methods are useful in preventing data loss in cloud architectures.

The asymmetric and symmetric encrypting methods are among the finest. The only fundamental issue with this system is the critical giver, although homophobic encryption has recently overcome some issues. Cloud users can entrust the keys or arbitrary encryption schemes to the cloud provider and control the keys themselves. Without a doubt, encryption techniques have become a necessary component of protecting data confidentiality

Transparent Encryption Model: Transparent encryption is accomplished using the e technology. It is composed of two layers: an application layer and a kernel layer. Application Control Module: This module is in charge of data interchange with the rest of the application layer components. It conducts activities such as retrieving authentication results from the identity management module, retrieving and updating keys from the key management module, and constructing security plans for the security strategy module based on client requirements.

Chaotic maps' properties have attracted the attention of cryptographers working on new encryption methods. These chaotic maps may be likened to a variety of cryptographic characteristics of ideal ciphers, including confusion, diffusion, balance, and avalanche property, since it exhibit many important traits such as unpredictability, mixing, and sensitivity to starting condition/system parameters. To meet the requirement of secure picture sharing, this study uses a novel image encryption method based on chaotic logistic maps.

Key Generator: Two logistic maps can be used to simulate nonlinear discrete systems that are basic. As demonstrated below, it is feasible to explain the logistic map using the recursive function:

Due to their high efficiency and simplicity, chaotic maps with one dimension have been used in numerous approaches connected to information encryption in recent years. However, it has a number of flaws, including narrow key areas and inadequate security. Deficient systems have been addressed by the use of logistic maps with one or more parameters. Using the r-value, which is equal to 4, the map revealed the chaotic behavior, as seen in *Fig. 4*. Here, formulae 1 and 2 must be combined to create a hybrid logistic function. After that, the X and Y values were added to this hybrid function, and these values were retrieved from the hybrid formula, were then converted to a binary system, as is shown in *Fig. 4*. By making comparison to the results from both formulas 1 and 2, as well as from the hybrid, it can be seen that the results indicated that the most valuable formula was the hybrid, which contained a number of random keys .in addition that a logistic map function is non periodic and the length of key is over limited which means the time interval is couldn’t not be manipulated

Received 16/August/2021; Accepted 18/October/2021

ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.22.1.10

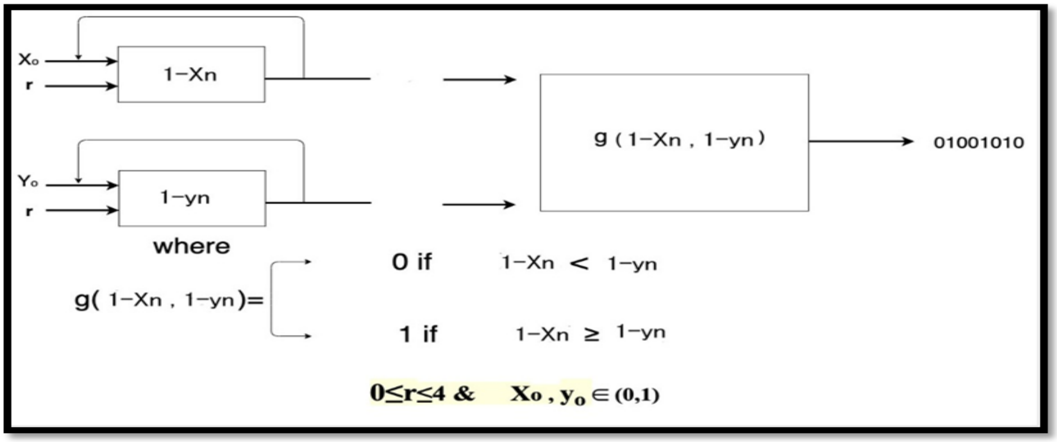


FIG. 4. LOGISTIC MAP KEY GENERATOR

Image Encryption: To accomplish the goal of image encryption, the proposed method makes use of "two chaotic logistic maps," as shown in *Fig. 2*. The proposed approach makes use of "two chaotic logistic maps," as follows:

Throughout the process, that maintains a constant "system parameter for both logistic maps (4.000)," which corresponds to a very chaotic situation. On the other hand, both maps' "starting conditions (X0 and Y0)" are created via exact mathematical manipulations of session keys, as shown in the algorithm below:

Algorithm for Encrypted Image;

```
Input: plain Image
Output: encrypted Image
Step1: assume the plain Image 256*256 “which is a body of image ‘without header”
Step2:  generate a key from chaotic map generator
Step 3: let J is a vector of plain Image staring with J(0)
Step 4: compute J as J (k) = J(k-1) XOR  J(k) =1,2…… 256*256 -1
Step 5: End
```

Text file Encryption: Cryptographic solutions are thought to be among the most effective in solving data loss. It is a secure technique for transferring and storing data in a format that can only be processed and read by the intended recipients. The hash function, which is based on local memory, can address issues relating to data integrity. The recalculation of the data received is compared to data stored locally to help the server authenticate answers.

Proof of retrievability (POR) is a system that allows a (prover) or backup service or an archive to provide clear evidence of a CSU's (verifier) ability to retrieve a target file [6]. It is designed, in particular, to ensure that data files are kept and consistently delivered by the archives in sufficient quantities for the CSU to retrieve them entirely. Essentially, a POR is a Proof of Knowledge (POK) cryptographic model designed to work with a "bitstring," another term for a huge file. The POR, unlike the POK, does not require the CSU to be familiar with the target file. Thus, existing cryptographic techniques play a critical role in assisting CSUs in retrieving files with good integrity and privacy. Furthermore, the encryption technology allows the CSUs to ensure that files are neither modified nor deleted by the archives before it retrieved by using an advanced AES 256 hash.

Received 16/August/2021; Accepted 18/October/2021

DOI: https://doi.org/10.33103/uot.ijccce.22.1.10

V. TESTING AND VALIDATION

For the implementation of the approach, "User Interface (UI)": Allows a user on the Cloud Service User's premises to request and receive services for which he or she is permitted. "Application (App)": Responsibilities include processing user requests at the Cloud Service User's and, if required, the Cloud Service Provider's facilities. The approach was evaluated under five ITU-T guidelines parameters: secrecy, data integrity, responsibility clarity, secure transmission, and protection consistency.

Confidentiality: The main difficulty in existing systems is protecting the User's data from malevolent cloud service providers. When data from the CSU is transferred to the CSP for processing, security becomes an issue. As the user has no control over the data that has already been transferred, it becomes vulnerable to attackers on the provider's premises.

The suggested approach includes mechanisms for safeguarding the user's data's confidentiality. "The UI (User Interface) component of the CSU environment will be a subset of it." All processing requests will be made through the UI, and no processing will occur on the provider's premises.

As illustrated in *Fig. 5* which indicate the main interface of slim clod tool that used to implementation phase, the test of the framework using a scenario in which a user attempts to upload data via cloud thin simulator services.

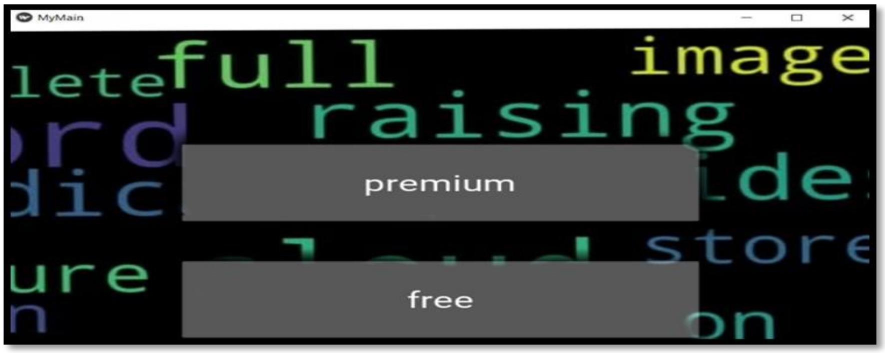


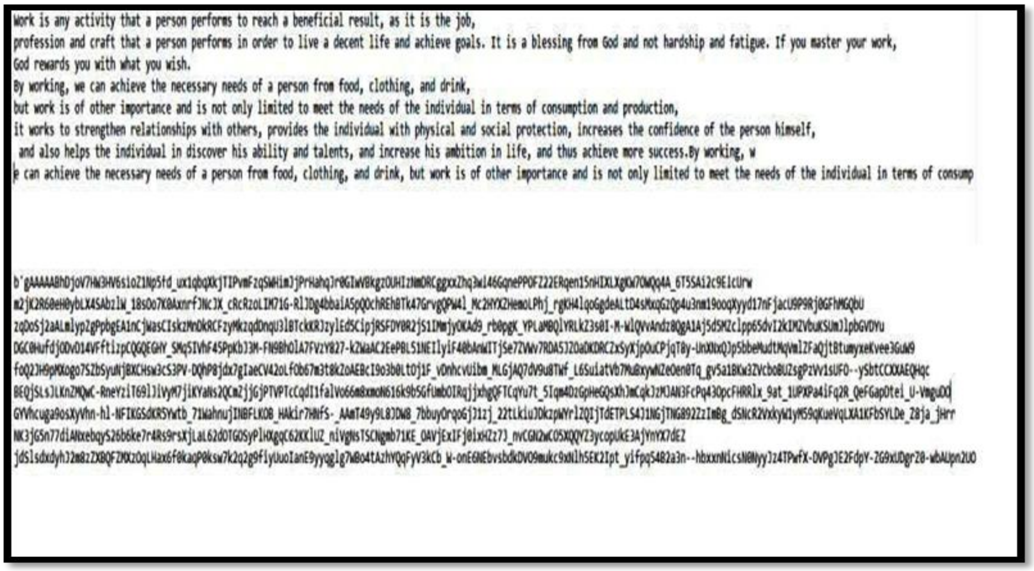
FIG. 5. SIMULATOR OF SECURE CLOUD SERVICE

As the user logins to the services, the proposed framework provides two kinds of services, which are free normal services and premium secure services, which are shown in *Fig. 5*. *Fig. 6* shows the premium services with two encryption methods.

Secure text data: since the user uploads the text file, the frame work provides the encryption solution to protect the user's data from any attack, including passive and active**.** *Fig. 6* shows the encrypted and decrypted data as a text file which users upload to cloud services

Received 16/August/2021; Accepted 18/October/2021

DOI: https://doi.org/10.33103/uot.ijccce.22.1.10



```
Work is any activity that a person performs to reach a beneficial result, as it is the job,
profession and craft that a person performs in order to live a decent life and achieve goals. It is a blessing from God and not hardship and fatigue. If you master your work,
God rewards you with what you wish.
By working, we can achieve the necessary needs of a person from food, clothing, and drink,
but work is of other importance and is not only limited to meet the needs of the individual in terms of consumption and production,
it works to strengthen relationships with others, provides the individual with physical and social protection, increases the confidence of the person himself,
 and also helps the individual in discover his ability and talents, and increase his ambition in life, and thus achieve more success.By working, w
e can achieve the necessary needs of a person from food, clothing, and drink, but work is of other importance and is not only limited to meet the needs of the individual in terms of consump
```

```
b'gAAAAABhDjoV7HW3HV6sioZ1Np5fd_ux1qbqXkjTIPvmFzqSWHimJjPrHahqJr0GIwVBkgzOUHIzNmDRCggxxZhq3wi46GqnePPOFZ22ERqen1SnHIXLXgKW7OWQq4A_6T5SAi2c9E1cUrw
m2jK2R60eH0ybLX4SAbzlW_18sOo7K0AxnrfJNcJX_cRcRzoLIM71G-RlJDg4bbaiASpQOchREhBTk47GrvgQPW4l_Mc2HYX2HemoLPhj_rgKH4lqoGgdeALtD4sMxqGzQp4u3nm19ooqXyyd17nFjacU9P9Rj0GFhMGQbU
zqDoSj2aALmlyp2gPpbgEA1nCjWasCIskzMnDkRCFzyMkzqdDnqU3lBTckKRJzylEd5CipjRSFDY0R2jS1IMmjyOKAd9_rb0pgK_YPLaMBQlYRLkZ3s0I-M-WlQVvAndz8QgA1Aj5d5MZclpp65dvI2kIMZVbuKSUmJlpbGVDYu
DGC0HufdjODvO14VFftizpCQGQEGHY_SMq5IVhF45PpKbJ3M-FN9BhOlA7FVzY827-kZWaAC2EePBL51NEIlyiF40bAnWITjSe7ZVWv7RDA5J2OaDKDRC2xSyXjpOuCPjqT8y-UnXNxQJp5bbeMudtMqVml2FaQjtBtumyxeKvee3GuW9
foQ2JH9pMXogo7SZbSyuNjBXCHsw3cS3PV-DQhP8jdx7gIaeCV42oLfOb67m3t8kZoAEBcI9o3b0LtOj1F_vOnhcvUibm_MLGjAQ7dV9u8TWf_L6SuiatVb7MuBxywNZeOen0Tq_gv5a1BKw3ZVcboBUZsgPzVV1sUFO--ySbtCCXXAEQHqc
BEQjSLsJLKnZMQwC-RneYziT69lJiVyM7jiKYaNs2QCmZjjGjPTVPTcCqdI1falVo66m8xmoN616k9b5GfUmbOIRqjjxhgQFTCqYu7t_5Iqm4DzGpHeGQsXhJmCqkJzMJAN3FcPq43OpcFHRRlx_9at_1UPXPa4iFq2R_QeFGapOtei_U-VmguDd
GYVhcuga9osXyVhn-hl-NFIKGSdKR5Ywtb_71WahnujINBFLKOB_HAkir7HNfS-_AAmT49y9L8JDW8_7bbuyOrqoGjJ1zj_22tLkiuJDkzpWYrlZQIjTdETPLS4J1NGjTNG8922zImBg_dSNcR2VxkyW1yM59qKueVqLXA1KFbSYLDe_Z8ja_jHrr
NK3jG5n77diANxebqyS26b6ke7r4Rs9rsXjLaL62dOTGOSyPlHXgqC62KKlUZ_niVgNsTSCNgmb71KE_OAVjExIFj0ixHZz7J_nvCGN2wCO5XQQYZ3ycopUkE3AjYnYX7dEZ
jdSlsdxdyhJ2m8zZXBQFZMXzOqLHax6f0kaqP0ksw7k2q2g9fiyUuoIanE9yyqglg7WBo4tAzhYQqFyV3kCb_W-onE6NEbvsbdkDVO9mukc9xNlh5EK2Ipt_yifpqS4B2a3n--hbxxnNicsN0NyyJz4TPwfX-OVPgJE2FdpY-ZG9xUDgrZ0-wbAUpn2UO
```

FIG. 6. TEXT FILE ENCRYPTION AND DECRYPTION

Secure Image: In *Fig. 7* shows a user uploading an image. It shows conventional, encrypted, and decrypted images. The encrypted image is indistinct, and the pure image information is unidentified by the software. Thus, there are problems with restoring the image, it is hidden, and it is impossible to detect its information. When the right key is used, the encrypted image may be decoded efficiently.

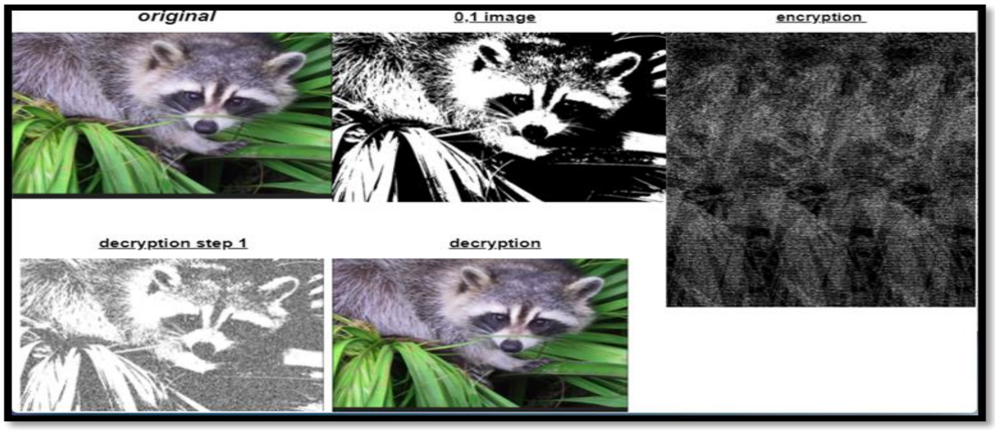


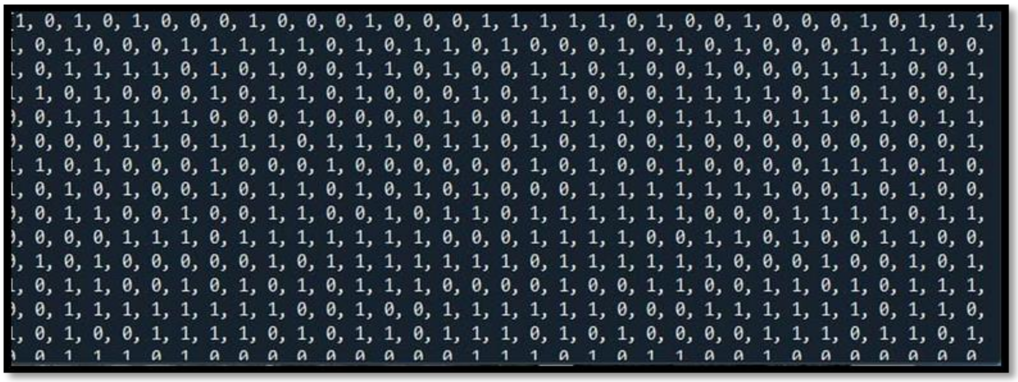
FIG. 7. ENCRYPTION IMAGE AND DECRYPTION

Random key generator: A random key was generated using Python code, as shown in *Fig. 8*. A full explanation of the methods involved in creating a random key was also included in the paper. It was necessary to determine the key generation strategy by analyzing how sensitive the key was to alterations of any type that would result in the production of new encryption. One bit in the key can be changed, resulting in the keys being completely dissimilar. The National Institute of Technology and Standards provided a statistical research kit that was used to test the proposed methodology (NITS).

The P-values were determined for each test of randomness in the NITS. The NITS has 15 tests to verify the randomness of the series and P-values were identified for each test.

Received 16/August/2021; Accepted 18/October/2021

DOI: https://doi.org/10.33103/uot.ijccce.22.1.10



```
[1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1,
1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0,
1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1,
1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1,
0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1,
0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1,
1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0,
1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0,
0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1,
0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0,
0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1,
1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1,
0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0,
1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1,
0  0  1  1  1  0  1  0  0  0  0  0  0  0  0  0  1  1  1  0  1  0  1  1  0  0  1  0  0  0  0  0  0  0
```

FIG. 8. KEY GENERATION THROUGH LOGISTIC MAP

These experiments can be used to measure binary sequence randomness, including cryptographic generators for cipher text or pseudorandom numbers. A P-value is calculated in both of these experiments and can be used to find out whether or not the test has been completed. If the (p-value) is higher than certain confidentiality (a) threshold for any measure, it is (passes). If (P-value α) it appears to be the string is random, the string appears not random otherwise. For the tests, a significance level (α) can be chosen. Usually, (α) is chosen in the range [0.001 – 0.01]. When the value of (α)= (0.01), it means that one string in (1000) strings will be rejected by the test. A (P- value≥ 0.001), would mean that the string would be considered to be random with a confidence of (99.9%). A (P-value<0.001), would mean that the string is non-random with a confidence of 99.9%.

Cloud services performance: testing the model in clod slim with multiple data users uploading. *Fig. 9* displays the numbers of users that did a successful trial of storing data in the framework with reliable and secure data storage.

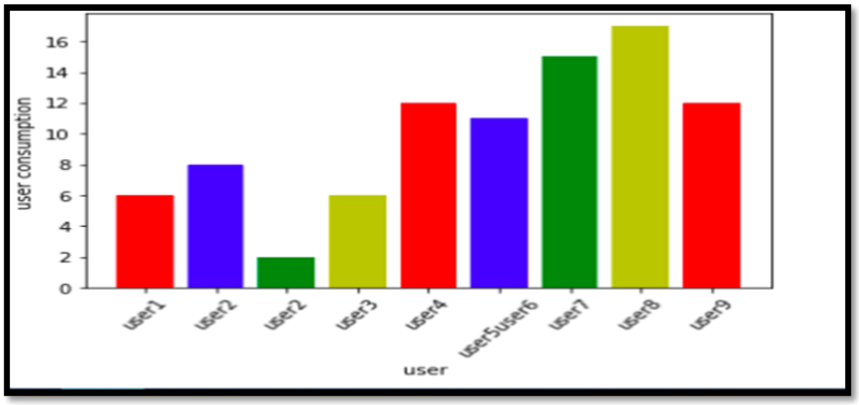


FIG. 9. USER TRAIL IN OUR PROPOSED SYSTEM

VI. CONCLUSION

In cloud environments, the security of cloud consumers' data is lacking. Therefore, security considerations in cloud environments were the subject of this research. Using encryption techniques can make the cloud more secure and reliable. Furthermore, the generation of the encryption keys in the proposed cloud framework is to deliver secure cloud services instead of external keys. Since the proposed framework can generate and manage the unique keys for encryption – decryption and pass all

Received 16/August/2021; Accepted 18/October/2021

DOI: https://doi.org/10.33103/uot.ijccce.22.1.10

statistical tests that approved for validate keys our approach does not need to be updated for this strategy to be used, making it quick to implement and easy for the users. The tested results show valued performance of our solution with secure and effective storage cloud services.

REFERENCES

[1] Y. Alagrash, F. Alghayadh, A. Alshammari, and D. Debnath, "Cloud computing: a framework for balancing accountability and privacy based on multi-agent system," in *2019 Cybersecurity and Cyberforensics Conference (CCC)*, 2019, pp. 6-12: IEEE.

[2] P. S. Pawar, M. Rajarajan, S. K. Nair, and A. Zisman, "Trust model for optimized cloud services," in *IFIP international conference on trust management*, 2012, pp. 97-112: Springer.

[3] S. Challa, A. K. Das, P. Gope, N. Kumar, F. Wu, and A. V. Vasilakos, "Design and analysis of authenticated key agreement scheme in cloud-assisted cyber–physical systems," *Future Generation Computer Systems*, vol. 108, pp. 1267-1286, 2020.

[4] P. Chinnasamy and P. Deepalakshmi, "Design of secure storage for health-care cloud using hybrid cryptography," in *2018 second international conference on inventive communication and computational technologies (ICICCT)*, 2018, pp. 1717-1720: IEEE.

[5] M. Abibulla, M. S. Hafiz, and I. M. Khader, "Design and Implementation of High-Speed AES and Visual Cryptography with Modified Mix Column on FPGA–A Survey," *Perspectives in Communication, Embedded-systems and Signal-processing-PiCES*, pp. 4-6, 2021.

[6] K. P. Kumar, "Symbiotic view of Provenance in Cyber Infrastrcuture and Information Security," *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, vol. 12, no. 2, pp. 3261-3267, 2021.

[7] S. A. Chaudhry, T. Shon, F. Al-Turjman, and M. H. Alsharif, "Correcting design flaws: An improved and cloud assisted key agreement scheme in cyber physical systems," *Computer Communications*, vol. 153, pp. 527-537, 2020.

[8] F. Alghayadh, Y. Alagrash, and D. Debnath, "Privacy and trust in cloud computing," *International Journal of Advance Research, Ideas and Innovations in Technology*, vol. 4, no. 4, 2018.

[9] A. Singh, P. Agarwal, and M. Chand, "Image encryption and analysis using dynamic AES," in *2019 5th International Conference on Optimization and Applications (ICOA)*, 2019, pp. 1-6: IEEE.

[10] O. M. Al-Hazaimeh, M. F. Al-Jamal, N. Alhindawi, and A. Omari, "Image encryption algorithm based on Lorenz chaotic map with dynamic secret keys," *Neural Computing and Applications*, vol. 31, no. 7, pp. 2395-2405, 2019.

[11] H. Xiang and L. Liu, "An improved digital logistic map and its application in image encryption," *Multimedia Tools and Applications*, vol. 79, no. 41, pp. 30329-30355, 2020.

[12] A. K. Chauhan, A. Kumar, and S. K. Sanadhya, "Quantum Free-Start Collision Attacks on Double Block Length Hashing with Round-Reduced AES-256," *IACR Transactions on Symmetric Cryptology*, pp. 316-336, 2021.

[13] Y.-Q. Zhang, J.-L. Hao, and X.-Y. Wang, "An efficient image encryption scheme based on S-boxes and fractional-order differential logistic map," *IEEE Access*, vol. 8, pp. 54175-54188, 2020.

[14] S. M. Ismail *et al.*, "Generalized fractional logistic map encryption system based on FPGA," *AEU-International Journal of Electronics and Communications*, vol. 80, pp. 114-126, 2017.

[15] N. Ayati, R. Sadeghi, Z. Kiamanesh, S. T. Lee, S. R. Zakavi, and A. M. Scott, "The value of 18 F-FDG PET/CT for predicting or monitoring immunotherapy response in patients with metastatic melanoma: a systematic review and meta-analysis," *European journal of nuclear medicine and molecular imaging*, vol. 48, no. 2, pp. 428-448, 2021.

[16] S. Sanadhy, A. Kumar, and A. Chauhan, "Quantum free-start collision attacks on double block length hashing with round-reduced AES-256," 2021.

[17] A. H. N. Drebee, A. E. Topcu, and Y. Alagrash, "Healthcare Security Based on Blockchain within Multi-parameter Chaotic Map," in *2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, 2020, pp. 0770-0778: IEEE.

[18] L. Moysis, A. Tutueva, C. Volos, D. Butusov, J. M. Munoz-Pacheco, and H. Nistazakis, "A two-parameter modified logistic map and its application to random bit generation," *Symmetry*, vol. 12, no. 5, p. 829, 2020.

[19] A. Cook *et al.*, "Internet of cloud: Security and privacy issues," in *Cloud Computing for Optimization: Foundations, Applications, and Challenges*: Springer, 2018, pp. 271-301.

[20] M. Annaby, M. Rushdi, and E. Nehary, "Color image encryption using random transforms, phase retrieval, chaotic maps, and diffusion," *Optics and Lasers in Engineering*, vol. 103, pp. 9-23, 2018.

Received 16/August/2021; Accepted 18/October/2021