International Journal of Data Informatics and Intelligent computing (IJDIIC)
Vol. 2, No. 1, March 2023, pp. 11~31
DOI: 10.59461/ijdiic.v2i1.34

Information Security: A Coordinated Strategy to Guarantee Data Security in Cloud Computing

Kofi Immanuel Jones[1], R. Suchithra[1]
[1]Department Computer Science and Information Technology, Jain University, Bengaluru, Karnataka, India

Article Info

Article history:

Received November 27, 2022
Revised January 02, 2023
Accepted February 10, 2023

Keywords:

Cloud Security
Encryption
Message authentication code
Virtualization
Secured socket layer

ABSTRACT

This paper discusses different techniques and specialized procedures which can be used to effectively protect data from the owner to the cloud and then to the user. The next step involves categorizing the data using three encryption parameters provided by the user, which are Integrity, Availability, and Confidentiality (IAC). The data is secured through various methods such as SSL and MAC protocols to ensure data integrity checks, searchable encryption, and splitting the data into three parts for cloud storage. Dividing the data into three portions not only enhances security but also facilitates easier access. Access to the encrypted data requires the user to provide the login information and password of the owner. This paper also studies critical security issues like unauthorized servers, brute force attacks, threats from cloud service providers, and loss of user identity and password.

Corresponding Author:

Kofi Immanuel Jones
Computer Science and Information Technology
Jain University
Bangalore, India
Email: kofijones37@gmail.com

1. INTRODUCTION

Modern businesses rely heavily on networks and communication infrastructure to transmit important and confidential information. As a result, it is crucial to ensure that such information is appropriately handled and secured. This makes the priority of protecting business and operations more important. Information security can be described as the manner of protecting the information, the system that has been put in place, and the hardware that has been used to store, used, and transmit the information in other to ensure the integrity, confidentiality, and availability of data and to make sure that operating procedures are protected[1]. Many businesses, particularly small and medium-sized ones, have come to understand the advantages of moving their applications to the cloud. The introduction of cloud computing technology has enabled many businesses to build and deploy software more efficiently and effectively in the cloud, saving money on the expense of buying and maintaining the infrastructure. "Cloud computing" is a concept for instant, on-demand network access to a pool of programmable computing resources (including networks, servers, storage, applications, and services). It makes it possible for these resources to be quickly provisioned and released with minimum administrative effort or service provider involvement[2].

This research project has been set up by combining several methodologies and using them to carry out the mission of cloud data security. The combination of these techniques acts as a wall against the security issues that have been continuously causing gaps in the effective operation and expansion of the cloud. This model's description offers a comprehensive perspective of how the data is processed at various stages. The way in which this model is defined gives a thorough overview of how data processing works at various levels. Data transferred to the cloud is encrypted because encryption is the model's primary fundamental protection strategy. Data is encrypted when it is transformed into cipher text, a form that is difficult for

outsiders to decipher but which can be opened by a legitimate decryption key held by a legitimate user. Furthermore, the approach effectively deals with security issues by enforcing strict authentication protocols, utilizing cryptographic signatures, storing encrypted data in the cloud based on sensitivity levels, creating an index, employing MAC for ensuring data integrity, and implementing keyword search for accessing stored data in the cloud. The proper operation of cloud computing is promoted by a defined approach that is developed in light of each of these considerations.

According to this computing architecture, after being supplied by the owner in an encrypted form and stored there in various amounts depending on the level of sensitivity, the user can get data from the cloud upon request. But to achieve that, you must first pass the authentication tests and then search the data using a keyword that the owner provided. The phrase "cloud" refers generally to the off-site, off-site storage of user data by a third party. By connecting the user's computer and online database over the internet, information is saved to the remote database rather than the user's computer's hard disk or other storage devices. By setting up the cloud's machines to work simultaneously, the concept of virtualization enables separate programs to leverage the combined computing power as though they were running on a cloud[3]. In this model, customers can connect to the cloud to obtain on-demand, reasonably priced information technology resources. Similar to how renters use offices, housing, or storage facilities, IT resources are effectively rented and shared among many tenants. The company's data center or server is replaced by the cloud services, which are offered online. Two examples of cloud computing services designed to make use of an organization's existing infrastructure are Amazon EC2 and Google App Engine. When compared to the traditional IT architecture, these cloud technologies provide a number of potential advantages, especially when factoring in service efficiency and effectiveness. The concern over security has been a major barrier to the uptake of cloud computing from the user's perspective[4]. This cloud model, which encourages availability, consists of three service models, four deployment models, and five characteristics[5].

The Three Functional Units ;f The Cloud Computing Model:

- Provider of cloud service: It is a company that oversees cloud storage servers (CSS). It offers powerful computational power and remarkable storage capacity for the clients' data.
- Client/owner: These are organizations that have massive data files in the cloud that the cloud maintains and supplies power to compute for. A company or a person can be the client or owner.
- User: This unit, which is associated with the client or owner, manages the Owners' data that is kept in the cloud. A user may also be an owner.

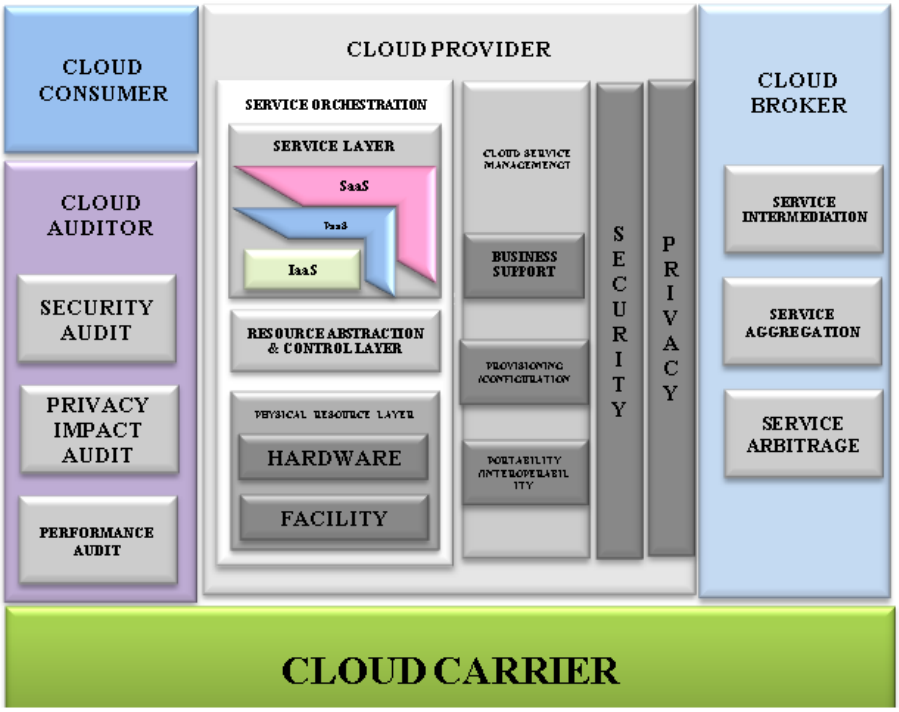


Fig.ure 1. 1NIST Cloud Computing Reference Architecture

Figure 1 depicts an indisputable example of a cloud computing reference design. The seven levels of the Open Systems Interconnection (OSI) paradigm, including the economic, commercial, and governmental

components, are all depicted in the graphic. It is essential to comprehend this knowledge[6]. As is evident, cloud computing is a comprehensive and sophisticated solution with numerous points of weakness[7]. Cloud computing may leverage the concept of firewalls, virtual private networks, and the enforcement of specific security standards to safeguard the confidentiality of customer data within a network's perimeter or peripherals. Being able to guarantee that only authenticated users have the system's privileges, and that secure conduct is expected has made security an essential part of any architecture of cloud computing.[8]. To ensure data protection, the cloud incorporates firewalls, virtual private networks, and other security measures within its own infrastructure. While the cloud concept involves pooling resources with other cloud providers, critical business or client data can be accessed through the cloud and third-party clouds. Due to various architectural designs using cloud computing, issues about architectural security is evolving. Outsourcing is the primary focus of cloud computing, so two key issues can be brought up here. Because the owner does not have control over the system, outside attackers (or any unauthorized user) can access the crucial data. As the data is being kept on his premises, the cloud service providers themself may breach the owner[9]. Any breach of security must be viewed as extremely serious and may have serious repercussions. Many business owners will feel secure moving to cloud computing if concerns about cloud privacy are further addressed with strong regulation and governance for cloud operations in place. Due to outsourcing, computing systems have been organized by combining various strategies that can be used to carry out the duties of cloud data security. The combination of these many strategies has been used as a wall against the security barriers that have been continuously causing gaps in the cloud's expansion and methodical operations. Encryption is the primary security technique used in this analysis, and any data transmitted to the cloud is done so in encrypted form[10].

Data is encrypted after it has been converted into encrypted data, a form of encryption that is difficult for unauthorized users to decipher but that can be unlocked by authenticated users with the right decryption key. Additionally, the study uses strict authentication standards, cryptographic signatures, and cloud storage of encrypted information to effectively handle security issues. In this digital system, the owner transfers encrypted information to a cloud, where it is preserved in various locations based on its level of sensitivity and may be retrieved by the user from the cloud[11].

Whether the data is in the cloud or in transit, this article has been set up to provide total protection for it during the full cloud computing process. As a result, numerous techniques and understandable protocols have been put in place to protect sensitive information from unauthorized parties. This paper is divided into two parts. The first step is the process of exchanging and securely storing data in the cloud. The second stage explains how to generate requests for access to data, double authentication, cryptographic signature verification, and integrity. It also covers the recovery of data or information from the cloud. After they have successfully navigated all essential security procedures, authorized users can subsequently be granted access to the data.

2. RELATED WORK

This section highlights several recent studies that looked into cloud computing cryptography despite the fact that the security issues with cloud technology have been the focus of countless studies. Three categories are used to classify common cryptographic algorithms: The International Data Encryption Standard (IDEA), the Advance Encryption Standard (AES)[12], and the Data Encryption Standard (DES)[13]. Due to the significance of cloud computing security, numerous research have been done on the topic. For instance [14] suggest "Security study and performance evaluation of a new lightweight cryptographic method for cloud computing". The authors suggest performing a security audit and effectiveness evaluation of a new, lightweight cryptographic method to enhance data security in the cloud. The study concentrates on assessing the efficiency and security of the cryptographic algorithm design in the cloud computing environment, employing various techniques such as computational complexity, key sensitivity analysis, statistical methods, image histograms, and entropy analysis.

Their experiment's findings show that NLCA performs well in terms of computational time parameters and unpredictability and that substantially less memory is required for NLCA security analysis results. The Avalanche Test further demonstrates that the NLCA algorithm will result in a significant number of bits changing with a (single bit) shift in the key or original text. Additionally, it is clear from the results of Picture Entropy and Image Histogram that the suggested approach, NLCA, is the best option for image encryption. Novel Hybrid Encryption Mode (NHEM), a novel crypto approach introduced by Quazi Warisha [15]., blends many cutting-edge cryptologic approaches into it and offers the highest level of protection for cloud data. The Advanced Encryption Standard (AES) and Message Digest (MD5) algorithms are two extremely potent algorithms that are combined in the NHEM proposal's hybrid algorithm.

In addition to the aforementioned techniques, some researchers propose using advanced methods to enhance cloud computing security. For instance [16] suggest using blockchain technology to secure cloud computing. In a proposed blockchain-based ecosystem for new data, when a majority of peers approve a new

block, the system adds it to the chain, and the newly generated blocks are distributed to all network peers. This approach offers a high level of cloud computing security due to the inherent security of blockchain technology. However, despite its numerous advantages, the blockchain-based solution has several challenges, including the inability to update data once it is added to the chain, which may affect data integrity. For instance, it may be illegal to do so in accordance with data protection regulations (such as GDPR1), which mandate that sensitive personal information should only be retained for the "shortest time practicable" and have a deadline for doing so. Moreover, changes or mistakes cannot be undone because it requires the consent of much more than half of the peers. Another issue with the suggested approach is that while many cloud technology data are enormous data, like images, and the method does not adequately work for preserving all cloud computing data, blockchain is designed to carry small transactional data. The effectiveness and efficiency of various symmetric cryptography methods were compared in a different study (such as execution time and memory usage)[17]. They discovered that Blowfish and DES (Data Encryption Standard) require less time and memory for encryption and decoding. Both a Traditional Encryption Algorithm and a Modified Advancing Encryption Standard are proposed 18]. With a patch size of a 4 by 4 matrix, AES employs group iteration. Each element consists of 8 bits. The following changes are made based on the AES algorithm framework to make the algorithm more suitable for encryption, increase security, and enhance encryption effectiveness.

2.1. Improved Key Sequence Generation Method

Chaotic dynamical systems are characterized by pseudorandomness and extreme sensitivity to beginning conditions and system parameters. As a result, it offers a useful method for image information encryption. To construct the key sequence, the new technique uses the following skew tent map.

$$F_a(x) = \begin{cases} x/a, x \in (0,a). \\ (1-x)/(1-a), x \in (a,1) \end{cases} \quad (1)$$

A ∈ [0,1] indicates that the system is chaotic. The relationship of this recurrent trajectory sequence for mapping is falling off quickly because the circulation of chaotic parameters is uniform and has good pseudo-random features. The steps for constructing oblique tent mapping-based pseudo-random sequences are as follows: A single M x N image must be used to encrypt R rounds. It first evaluates the oblique tent mapping to get the R sequence. $X_r x_{r,0}, x_{r,1}, \cdots, x_{r,MN-1}, 1 \le r \le R$. Expanding X to a 0-255 integer sequence. $K_r k_{r,0}, k_{r,1}, \cdots, k_{r,MN-1}$ based on the equation below.

$k_{r,i} = \text{x}x_{r,i} \times 255\text{y}$.
where xy represents a round-to-infinite number.

2.2. Improved Encryption and Decryption

$$C[i][j] = \begin{cases} D[i][j] \bigoplus k_{r,i\times N+j}, i = M-1, j = N-1. \\ D[i][j] \bigoplus (k_{r,i\times N+j} \bigoplus D[i+1][0]), \\ \qquad\qquad i \neq M-1, j = N-1. \\ D[i][j] \bigoplus (k_{r,i\times N+j} \bigoplus D[i][j+1]), others. \end{cases} \quad (2)$$

Where as $i \in [0, M-1]$, $j \in [0, N-1]$, $D[i][j]$ are pixels with plain text.
$C[i][j]$ is derived from the cipher pixel.

2.3. Key Tree

25	28	255	65
66	91	58	212
242	255	84	49
195	79	8	196
78	60	79	89

(a) 5x4 matrix

25	13	242	79
41	10	49	97
201	3	23	136
250	137	102	191
83	102	252	58

(b) row diffusion result

25	13	242	79
66	24	25	176
242	13	71	233
195	140	125	72
78	238	97	248

(c) column diffusion result

The matrix of plaintext is encrypted from left to right. Both right to left and top to bottom decoding operations are performed on the ciphertext matrix. The plaintext and key are merged after

the XOR procedure. Even though the initial conditions are the same for both photos, the resulting key sequences differ.

2.4. Improved Column Mixing

Each pixel in AES undergoes a shift and XOR operations as part of the column mixing process, MixColumns, which uses a matrix. In order to improve pixel association and reduce computing cost, the updated method modified the MixColumns matrix operations to use straightforward addition and subtraction. The specific actions are as follows: as shown in Equation (3), the first pixel remains constant for each row while the current pixel for each column is upgraded with the values of nearby pixels beginning with the second pixel; as shown in Equation (4), the existing pixel for each row remains constant while the existing pixel is modified with nearby pixels beginning with the second pixel. Each column's first pixel remains constant.

$$MixColumns = \begin{cases} D[i][j] = D[i][j], j = 0. \\ D[i][j] = (D[i][j] - D[i][j-1] \\ \qquad \mod 256, others. \end{cases} \quad (3)$$

$$MixColumns = \begin{cases} D[i][j] = D[i][j], i = 0. \\ D[i][j] = (D[i][j] - D[i-1][j] \\ \qquad \mod 256, others. \end{cases} \quad (4)$$

The tables above display the outcome of the procedure using a 5 x 4 matrix as an example. We may infer from this image that changing D[0][0] will have an impact on every pixel. Changes to D[M-1][N-1] have no impact on other pixels in the same round. Therefore, each line and each column should move to the left and upward, respectively, throughout the row and column transformation processes. After multiple rounds of encryption, there is a clear diffusion effect. Each pixel only requires two additive operations in the improved row and column mixed operations, which not only decreases computing complexity but also strengthens the connections between the pixels. After numerous encryption rounds, it can produce a greater mixing effect.

A thorough summary of the state of the art in Advanced Encryption Standards (AES) research is given in this literature review. The review covers on the various aspects of AES, such as its implementation, performance, and security. AES is one of the most secure encryption algorithms currently in use, and the review finds that it performs very well. AES is also simple to use and effective to install. This review's overall conclusion shows that AES is a dependable and safe encryption technology that works well for a variety of applications.

3. METHOD

This stage discusses the systems and practices for storing and safeguarding data, which begin with sharing it safely and in an encrypted form on the cloud. Classifications, Encryption, And Index Building, and Message Authentication Code (MAC), which provide a step-by-step detail of action on the data, can be further divided into sub-sections.

3.1. Classification

As shown in Figure 1, a mechanism has been created to store data in the three types of the cloud (Private, Public, and Hybrid), according to three cryptographic properties: Confidentiality, Availability, and Integrity. The sensitivity rating (SR) will be calculated using the recommended algorithm that is shown below when the client lists these parameters. As long as the information in the cloud is set up to be stored, this technique can be used. The validity of the information determines the value of integrity, whereas the level of privacy required at every phase of the data processor determines the value of secrecy. Also, the data must be secure against unauthorized alteration and dependable. The importance of availability is determined by how often the data is accessed, and it must be made available immediately upon request.

Algoritham 1. **Rijndael Algorithm**

1 Data, a protection section, and a D [ ] array with n integer elements.
Where D[ ] is an array of n-dimensional integers made up of C, I, goA, SR, and R.

2 Output: Data that has been categorized for the relevant part.

3 For i=1 to n
C [i]= Confidentiality's value.
I [i]= Integrity value.
A[i]= Availability value.
Calculate SR[i]=(C[i]+(1/A[i])*10+I[i])/2

4 For j=1 to 10
For i=1 to n
IF SR [i]==1||2||3 then
S[i]=3
IF SR[i]==4||5||6 then
S[i] =2
IF SR [i]==8||9||10 then
S[i] =1

/* Integrity and availability are directly inversely correlated with security, while security and confidentiality are directly correlated with each other. * /

Rijndael was selected by the National Institute of Standards and Technology (NIST) to replace the existing industry standard, recognized as DES (Data Encryption Standard)[19]. AES is a type of symmetric encryption, which allows the same information to be encrypted and decrypted with the same key. Keys of 128 bits, 196 bits, or 256 bits in size can be utilized with AES. Some scholars recommend employing advanced techniques to enhance cloud computing security, including the use of blockchain technology proposed[20]. In their proposed blockchain-based ecosystem for new data, the system adds a new block to the chain when a majority of peers approve it, and the newly generated blocks are distributed to all network peers. This approach provides a high level of cloud computing security due to the inherent security of blockchain technology. However, there are some challenges with this solution, such as the inability to update data once it is added to the chain, which may impact data integrity.

Rijndael's finite field is a particular Galois field that is used by AES for several crucial operations. It uses GF(2^8) specifically with the irreducible polynomial $x^8 + x^4 + x^3 + x + 1$. The field with p^n elements is designated by the Galois field GF(p^n), where p is a prime and n is a positive integer. For instance, all integers from 0 to 7 are present in the field GF(8) (or GF(2^3)). The fact that all of the elements of the field GF(p^n) are polynomials with non-negative coefficients evaluated at P and degrees smaller than n is a crucial characteristic of Galois fields. *P* is referred to as the field's characteristic. Let's take another look at GF(8) or GF(2^3). GF(2^3) contains the following numbers: {0, 1, 2, 3, 4, 5, 6, 7}. These numbers can also be written as {0, 1, 2, 2 + 1, 2^2, 2^2+ 1, 2^2+ 2, 2^2+ 2 + 1}, {0, 1, x, x+ 1, x^2, x^2 + 1, x^2 + x, x^2 + x+ 1} with x = 2

How Does AES Function?

You must first learn how AES transports data between several phases in order to comprehend how it functions. A single block of data is carried by a 4x4 matrix since each cell in a block of 16 bytes contains one byte.

Table 1. State Array

0	**1**	**2**	**3**
4	**5**	**6**	**7**
8	**9**	**10**	**11**
12	**13**	**14**	**15**

The framework in the preceding figure is described by state arrays. The initial key is similarly increased by (n+1) keys, whereby n refers to the number of encryption rounds. Thus, there are 16 rounds in a 128-bit key's generation, yielding a total of 11 keys (10+1)[21].

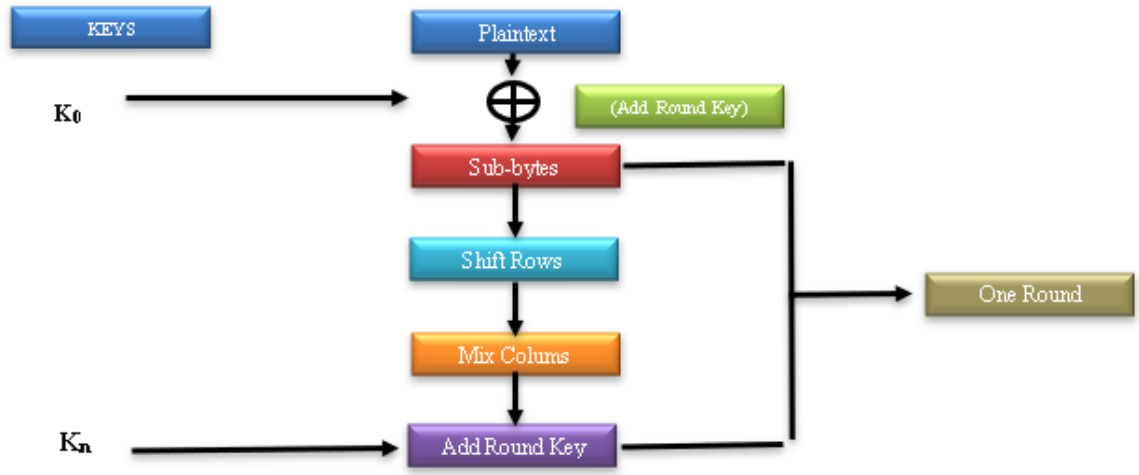


Figure 2. Stages in AES

Figure 2 Each block must go through the aforementioned processes in turn. It puts the encrypted blocks together to create the final ciphertext once each block has been successfully encrypted separately. The steps are as follows:

Add Round Key: The first key generated (K_0) by the XOR function is used to pass the block data contained in the state array. As an input to the following phase, it sends the generated state array.

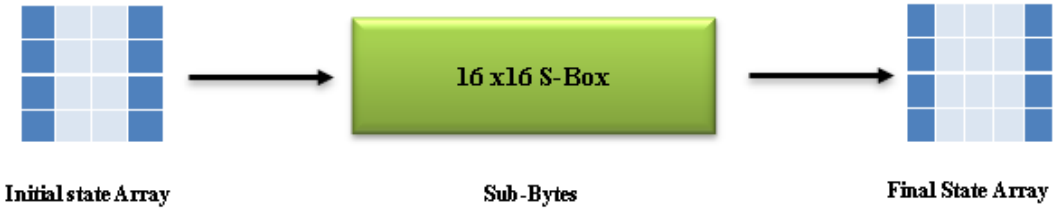
0	1	2	3
4	5	6	7
8	9	10	11
12	13	14	15

⊕

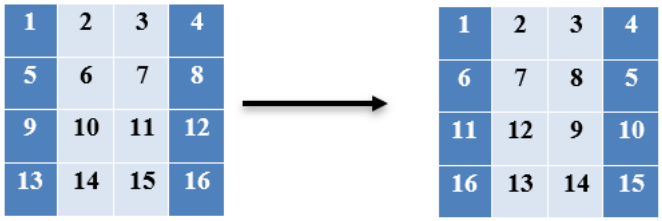
XOR

K_0	K_1	K_2	K_3
K_4	K_5	K_6	K_7
K_8	K_9	K_{10}	K_{11}
K_{12}	K_{13}	K_{14}	K_{15}

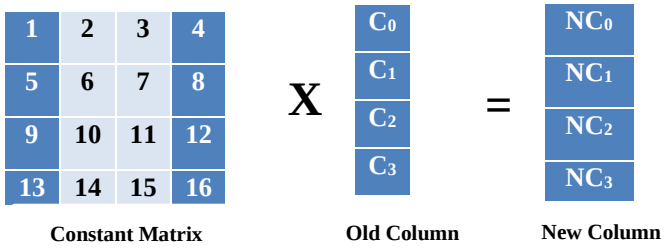
Sub-Bytes: At this phase, the bytes of the state array are divided into two equal parts and transformed to hexadecimal. To develop new values for the final state array, these components, which are made up of rows and columns, were transformed using a substitution box (S-Box).



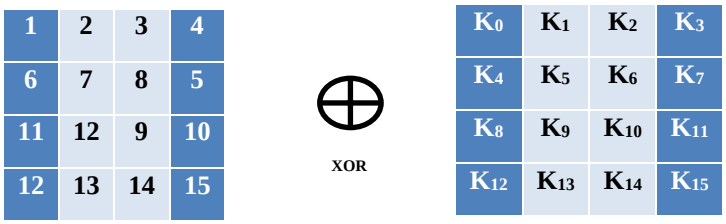
Shift Rows: There is a change in the row's components. First-row skip is present. The elements in the second row are shifted to the left by one position. The last row is also moved three positions to the left, as well as the parts of the third row move two spaces in succession.



Mix Columns: The process involves the multiplication of a fixed matrix with each column in the state array to generate a new column for the subsequent state array. After multiplying each column by the same fixed matrix, the next state array can be obtained. However, in the final round, this operation is not performed.



Add Round Key: The relevant key for this stage is combined with the state array obtained from the previous step using the XOR operation. The resulting state array becomes the new state array for the next round, unless it is the final round, in which case it becomes the ciphertext for that specific block.



The owner's main responsibility in the algorithm mentioned above is to classify the data according to cryptographic criteria namely C, I, and A. In this instance, D [ ] stands for the data, and the user must provide C, I, and A values. Using the suggested formula as a result the Sensitivity Rating (SR) value is determined and is displayed above. The data is assigned to one of the three models using this "SR" value. The S3 [Public], S2 [Private], or S1 [Owner's] areas in the cloud Restricted Access] as depicted in Figure 3.

To achieve a high level of security, AES uses S-boxes in conjunction with substitution and permutation. Uses for AES here include encryption of sensitive data stored in databases and safe data transmission over the internet [22]. The Counter Mode CTR) is the most popular statistical model for encryption and decryption in AES. The plaintext is encrypted in CTR mode, a stream cipher mode of operation, one block at a time with the same key and nonce. Each block's ciphertext is unique since the nonce is increased for each block. Since the same key and nonce can be used for several blocks of data, CTR mode is an effective way to encrypt data[23].

Counter Mode (CTR):

Ciphertext = Plaintext XOR (Keystream XOR Nonce)

Let Plaintext = P, Keystream = K, Nonce = N

Ciphertext = P XOR (K XOR N)

C = P XOR (K XOR N)

Galois/Counter Mode (GCM):

For cryptographic block ciphers, the Galois/Counter Mode (GCM) mode of operation offers both confidentiality and authentication. GCM offers extremely effective authenticated encryption that combines the AES algorithm's confidentiality with a GHASH function's authentication.

Ciphertext = Plaintext XOR (Keystream XOR Nonce XOR MAC)

Let Plaintext = P, Keystream = K, Nonce = N, MAC = M

Ciphertext = P XOR (K XOR N XOR M)

C = P XOR (K XOR N XOR M)

As a symmetric block cipher, the Rijndael algorithm requires the use of the same cryptographic key for both encryption and decryption. It is a well-known encryption technology that works with keys that are 128, 192, and 256 bits long. For both hardware and software implementations, it is a safe algorithm.
A plaintext input and a cryptographic key are required for the algorithm to function. The data is subsequently encrypted using the procedures listed below:
1. The plaintext is separated into 128-bit blocks (16 bytes).
2. After that, each block goes through several rounds of data modification using a set of routines.
3. The outcomes are XORed with a round key produced from the initial cryptographic key after each round.
4. The rounds are carried out once more to fully encrypt the data. The number of rounds is determined by the key's size.
5. The ciphertext that has been encrypted is the algorithm's output.
A simple reversal of the encryption process is what happens during decryption. Blocks of the ciphertext are separated, rounds are applied in reverse order, and the original plaintext is then retrieved.

3.2. Encryption and Index Building

Since searching over encrypted data is a challenging problem since cloud data is kept in an encrypted format, an index must first be created using the index builder illustrated in Figure 3 so that we may conduct searches over the encrypted data as the data is being retrieved. One simple method for creating an index is to list all the files that include each word W (the keyword of interest) individually. Creating an index makes it possible to retrieve files more quickly[24].

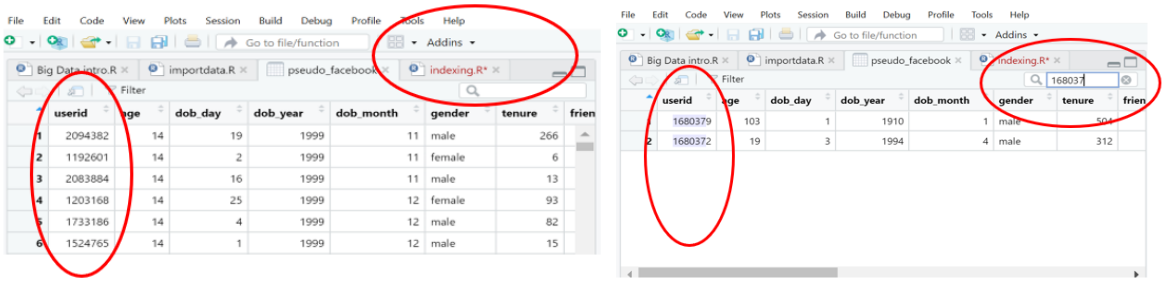


Figure 3. Retrieval of data using index in R studio

The index should also be encrypted to offer security against the disclosure of any type of information to the cloud. This index primarily consists of a list of keywords, each of which is followed by a list of links to the relevant documents. These keywords are intriguing words that the user might want to employ in the future. One of the suggested methods is to create an index of clear documents and encrypt both the index and the documents in which the encrypted information is being stored in the cloud[25].

Even if hackers, cybercriminals, and other online snoops manage to intercept plain text before it reaches its intended receivers, it cannot be read readily thanks to encryption. Once the message reaches its intended audience, each person has a unique key that can be used to decode the content and restore it to plain, readable language.

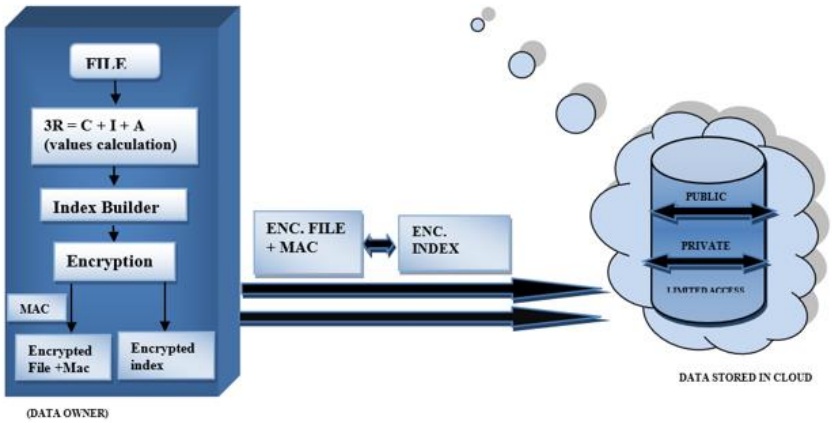


Figure 4. Data Owner & Data Stored in Cloud

Information that is understandable is rendered useless through the process of encryption. There is a key used in Secure Socket Layer (SSL) encryption that only enables authorized users in order to have the capacity to decipher the data. As illustrated below, this model encrypts the data and index using 128-bit SSL encryption[26].

128-bit SSL (F,k_2)-F”

As previously demonstrated, any key will be used (k_2) to secure the file F, creating the encrypted file F'. Only the same key (k_2) can be used to decrypt F'. Figure 4 depicts the movement of data from the owner to the cloud. When utilizing SSL, 128-bit encryption, as an example, we can see that the key length is 2^{88} bits longer than the previous 40-bit standard SSL encrypts data. There are 2^{88} more as a result of just that shift combination. Because of this, it is far more difficult for hackers to decipher the code. The range of values exceeds trillions. 256-bit encryption with SSL is, therefore safe. 128-bit encryption is typically sufficient. It is capable of a brute force attack due to its complexity[27].

The majority of attacks would be rendered useless due to the necessary processing power, among other things. Yet as technology advances, it's projected that the current industry standard for SSL could eventually need to switch to 256-bit encryption. There is a trade-off between cost and key size as the key size grows, though not dramatically[28]. Data that is communicated received, and saved by utilizing a device can be protected with encryption. This can include text messages saved to your phone's memory as well as financial data transmitted via your online account. Symmetric encryption and asymmetric encryption are the two basic categories of encryption systems[29].

Asymmetric encryption uses two keys for encryption and decryption while symmetric encryption only requires a single password. The data is encrypted using a public key that is dispersed among users. The data is decrypted using a private key, which is not shared. As a result of encrypting document references and keywords in each list found in the index, the data should then be encrypted. This is the process of turning relevant knowledge into irrelevant or obscure information. Secure Socket Layer (SSL) technology allows the system to provide a key, making it possible for only an authorized individual to have the ability to decrypt the data. By utilizing R Studio, you can generate an index of the data sets kept in the R environment. It entails making a list of all the variables, their values, and any functions that were applied to the data. The data can then be easily located and accessed for additional analysis using this index. By classifying the data into useful categories, it also provides effective access to the information. By making it possible to find and double-check data values, index building can also contribute to ensuring data integrity.

Data sent over the internet is secured and protected using the Secure Socket Layer (SSL) encryption cryptographic technique. It functions by creating an encrypted link between the two communicating endpoints to allow for the secure sharing of sensitive data[30]. To secure the data transferred between the two endpoints, SSL combines public-key and symmetric-key encryption. The symmetric key is used to decrypt the data once it has been encrypted using the public key. A further feature of SSL is authentication, which verifies the legitimacy of both communication parties and the authenticity of the data being communicated[31]. This is accomplished by validating each end's identification and confirming that the data hasn't been tampered with.

3.3. Message Authentication Code

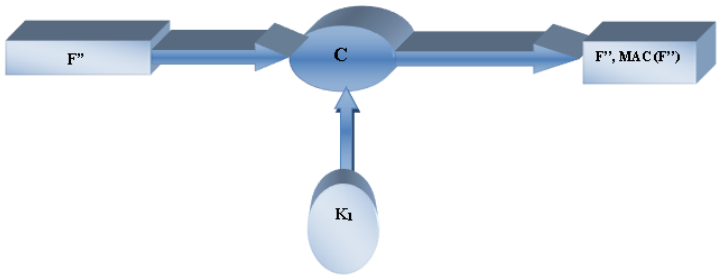


Figure 5. MAC Generation

A message authentication code (MAC) is generated once the data has been encrypted, and it is transmitted to the cloud together with the encrypted data. A secret key is used to construct MAC, a compact fixed-size block of data depending on the message or file F's variable length. When recovering the file, the user or owner of the data can use a tool called a cryptographic checksum to determine whether data has been altered during transmission[32].

The method of using key K_1 to create the MAC for file F" and transferring the encrypted data alongside the MAC to the other side is shown in Figure 5. Following the development of the Message Authentication Code, the model has data prepared for transfer to the cloud for storage, as shown in Fig. 5.

The data will now be distinguished based on the calculated Sensitivity Rating, with SR≤3 going into public sections (S3), 3<SR≤6 into private sections (S2), and 6<SR≤10 into owner's limited access sections. This is because the encrypted data once reaching the cloud is to be stored in separate parts (S1). In other words, a cryptographic hash function is used to create a Message Authentication Code (MAC). A shared secret key and a message that has to be authenticated are combined to create the MAC. The message and shared secret key are then combined, and the result is fed into a cryptographic hash function, which outputs a MAC. The message is then sent to the recipient with the MAC attached. The recipient can then construct their own MAC and compare it to the one included in the message using the shared secret key. The message is authenticated if the two MACs match[33].

3.4. Retrieval of Data (Phase Two)

Figure 6. Process of Registration.

As soon as data has been securely stored in the cloud, it must be retrieved using the finest methods and tools available. To get data, a user should first sign in with the company or owner by receiving a login name and password, which is illustrated in Figure 6. A password and username can only be obtained if the user registers with the organization. The organization will then send the username to the cloud so it may be stored in its directory[34]. When the user needs to access the data in this model, He makes a request to the cloud along with the username. If the request is appropriate for the public section, Cloud confirms it. Without authentication, access is granted, and following retrieval, only the section's public key can be used to decrypt the data. For a username and password, the user should register with the organization[35]. The cloud looks for the user-provided username in its user directory whenever a request is submitted for a private or limited access section.

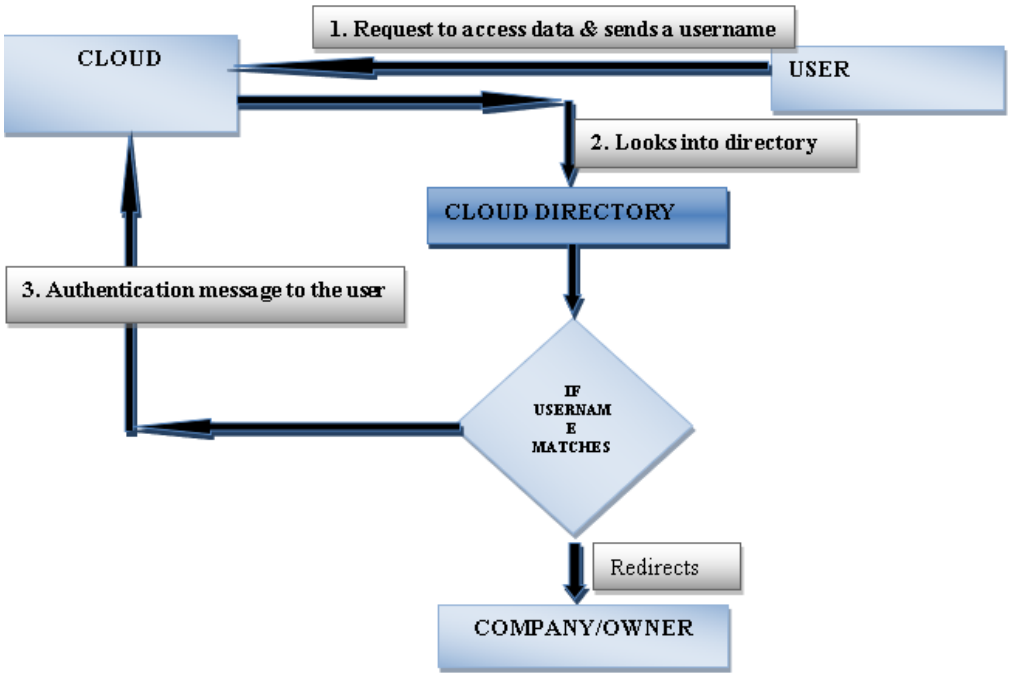


Figure 7. Requesting Access

The transmission of these requests is shown in Figure 7, which is provided below. The following conditions must be met in order to gain entry to the sectional database utilized in this model:

- There is no read/write functionality in the lower section, so the user who has access to the upper section is not permitted to access it. For instance, if a user has access to data in the public portion but not the private or limited access sections, they will not have access to the same owner's data in those areas.
- Anyone who has been given admission to the lower section is also permitted entry to the higher section. For instance, if a user has access to information in the limited access part, they will also have access to information belonging to the same owner that is available in the private section.

As seen in Figure 8, if the usernames match, the cloud will communicate the user identity to the owner or company for authentication. The biggest problem at this time is that the main authentication procedure is only retained with the owner because it is so vital that even the cloud cannot be trusted.

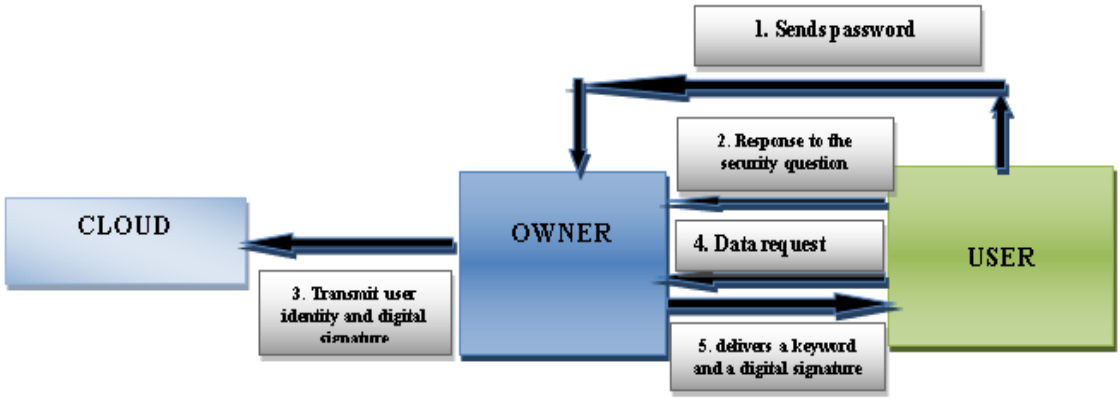


Figure 8. Process of Authentication

Figure 8 depicts user authentication and the request for data from the owner. When requesting authentication, a user must first send the owner their password. The owner will then ask the user for a verification code following the completion of this stage, and the user will need to provide a valid response in order to be verified. To ensure that only authorized users can access specific data for a particular session, the owner provides the user's identity along with a digital signature. The owner then sends the user the "Digital Signature," the keyword for the required data, and a master key to decrypt the data stored in the cloud. The user then requests information from the owner. As illustrated in Figure 8, the user sends a request to the cloud for data that matches the keyword, along with the owner's digital signature and keyword.

Using the keyword, the cloud performs the search request after first verifying the digital signature. In essence, retrieving files from encrypted data may be done quickly and securely without disclosing any sensitive data to the cloud. We have an already preserved encrypted index, as was previously mentioned. It has a list of keywords as well as a collection of hyperlinks to the documents that include those keywords. When the cloud accepts a keyword to search over encrypted files and discovers a match, the user-encrypted sequence of matching positions is delivered from the index. Before requesting that a pertinent file or document be retrieved from the cloud, the user can first utilize the decoding key given to them by the data owners to access the encrypted contents. The cloud answers to the user's request for an encrypted file by providing it. Following that, the user can decrypt the data by using the decryption key for file F that the owner has already provided. It may be difficult for the cloud to determine whether the demand for encrypted text retrieval and the request for a search are connected if it is included in other retrievals.

In other words, before granting access to cloud-based data and services, a user or device's identity is verified through the process of "authentication." Verifying the identity of the user or device is usually the goal of authentication, whether it be done via a login and password or two-factor authentication. The service provider subsequently checks the credentials against a list of valid credentials that are maintained. If the credentials are correct, the device or user is authenticated and given access to the information and services. Another method of authentication known as "two-factor authentication" calls for the user or device to submit additional information. This additional information can take the form of a one-time passcode or biometric information like a fingerprint[36].

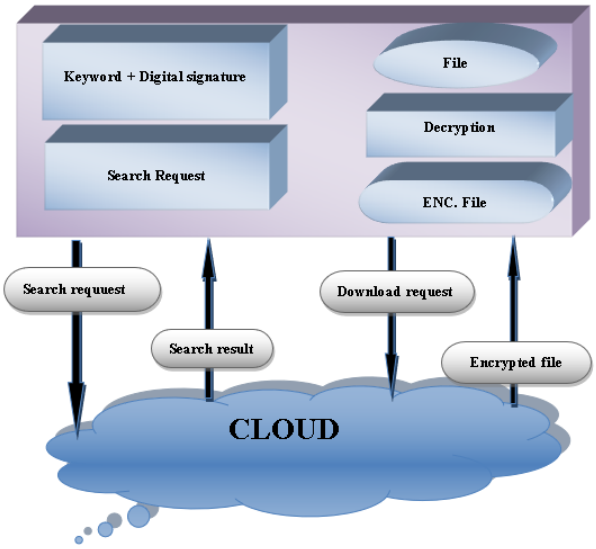


Figure 9. Process of retrieving

The user creating the search request and obtaining the encrypted file from the cloud are both depicted in Figure 9. Now that the user has acquired his or her data from the cloud, a concern or uncertainty about its integrity develops. Since this model employs MAC to check for integrity, the user can ensure the data integrity by calculating the Message Authentication Code of an encrypted file received using a secret key that has already been disclosed to the user and comparing it to the MAC received with the encrypted file.

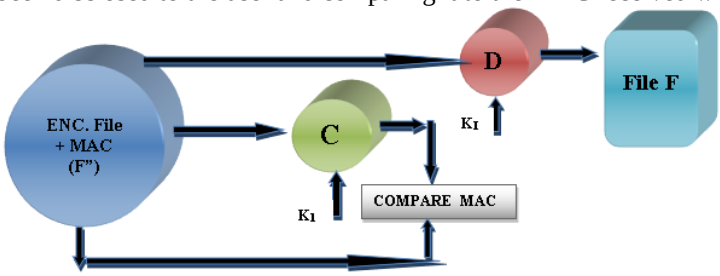


Figure 10. Comparison of MAC

Here, the procedure for verifying data integrity can be conducted out as shown in Figure 10. As shown in Figure 10, once the user has retrieved encrypted information, Key (k_1) is used to ascertain its MAC^, which is then contrasted with the MAC that was transmitted together with the encrypted files. It is shown that the data has not been altered at any point while traversing the entire data set if MAC^=MAC, or the MAC of encrypted files calculated by both the owner as well as the user is equal. The user can, however, decode the encrypted file they got using the key (k_1). The retrieval procedure comes to an end with this stage, and we can see that the model took all the necessary steps and safeguards to safeguard the data during the whole working process against potential threats like leakage of data, unauthorized entry, and tampering of data, among other things.

4. SECURITY EVALUATION

This study looks at how to secure data throughout the cloud computing system and highlights the procedures below where information can be particularly vulnerable to threats such as data leakage, user privacy, manipulation, and secrecy. All these security concerns will be successfully addressed in this study.

4.1. Server Unauthorization

A hacker can easily gain access to an internet-based network and pretend to be the owner of the data's cloud server, which results in data loss, just as the data is programmed to transmit via a network to the cloud. SSL Certification is then utilized to prevent data loss in this scenario. Each certificate, which serves as a credential to only one particular domain or server in the internet world, is issued by Certificate Authorities (CAs). The cloud server's identity information was then made accessible to the owner, and a duplicate of its SSL certificate was subsequently delivered to the owner. A message is delivered to the server, accompanied

by a cryptographically signed acknowledgment from the server, to start an SSL encrypted session, which allows encrypted data transfer between the browser and server. The certificate is validated by the owner. The information and keywords will still be saved in the cloud encrypted.

4.2. Brute Force Attack

While being sent to the cloud across an internet network, data can be attacked by a number of unauthorized interceptors. SSL offers encryption to prevent data readers from accessing transmissions of cloud-based data. It is simple to break using a modern computer that can quickly combine enormous numbers to find every potential key in an approach called a "brute force attack". As a result, I utilize 128-bit SSL encryption in this model, which provides a greater key size than that of the preceding SSL (40-bitbit) and can be adjusted to 256-bit encryption if necessary. A brute force attack is now largely worthless due to 128-bit SSL's complexity. The owner does one encryption, and SSL performs the other, under this model. Most attacks would be rendered useless due to the necessary computing power, among other considerations. As a result, this approach helps convince clients that their information is safe while in transit in addition to protecting it where it stays.

4.3. Threat From Cloud Vendor

The "cloud" is the domain where data is kept after being transferred by its owner. Due to the strong security measures used by the cloud service provider, the information stored in the cloud may be secure from every third party who is not authorized. Yet, the provider of cloud services has the option of betraying the owner in the interim. Anything can happen when data is saved to the cloud because its owner has little or no influence over it. The provider of cloud services can deal with any data leaks by disclosing the information to competitors. The cloud service provider cannot be fully trusted in this regard. The encryption of cloud-stored data is the greatest option in this circumstance. Via SSL certificates, data is encrypted. The optimal technique for using this strategy is to encrypt data stored in the cloud. Under this paradigm, private communications transmitted via a public network are encrypted using SSL Certificates. SSL employs an infrastructure of public keys and comprises of a secret key that decrypts data once it has been encrypted, allowing only the keyholders to see it. An attacker would find it extremely difficult to use brute force to decrypt the data with 128-bit SSL encryption.

4.4. Alteration of Data

Any unauthorized interceptor poses a constant risk of altering the data. Although this model has taken every care to prevent data tampering, including the use of encryption, keywords, and SSL encryption, data must still be validated after transmission. This model makes use of the MAC (Message authentication code). A MAC is created by the owner of the encrypted data before to transmission and is sent together with the encrypted data. On the reverse hand, a receiver can determine the MAC of the data they download or receive and correlate it to the MAC created by the data's owner. The user is confident that the data is real and hasn't been tampered with if both MAC codes are identical.

4.5. User Information and Password Loss

Authentication is necessary for the cloud computing infrastructure to prevent unwanted access. The data may be in danger if a user misplaces or unintentionally shares his username and password with an unauthorized person. The owner will in this case offer a security question, the answer to which is only known by the authorized user, preventing the unauthorized user from accessing the data even if they are aware of the user’s name and password.

Servers that have not received approval or authorization from a cloud provider are considered to be unauthorized servers. These servers can be used to access data, apps, and other resources that are not intended for public usage. As a result, security is a top concern when it comes to unauthorized servers. These servers can be used by an attacker to obtain confidential data, interfere with services, or carry out malicious activities. The following actions should be considered while evaluating the security of unauthorized servers:

- Limit access to unregistered servers: Only authorized users should be able to access unauthorized servers. In order to guarantee that only individuals with authorization have access, access control lists (ACLs) and other security measures can be made.
- Monitor server activity: It's critical to monitor server activity on unauthorized servers. This includes keeping an eye out for suspicious activity like unauthorized access attempts, data espionage, or other hostile conduct.

- Implement strong authentication mechanisms: To further safeguard unauthorized servers, strong authentication methods should be applied. This entails two-factor authentication, user certificates, and other security procedures to guarantee that only authorized users can access the system.
- Encrypted and secure data storage should be used when storing information on unapproved servers.

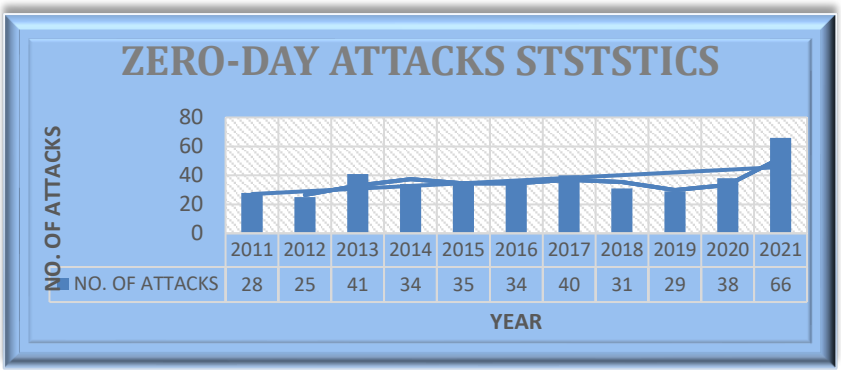
By asking the user to provide a second factor, such as a one-time code delivered to their mobile device, when logging in, two-factor authentication (2FA) helps to defend against brute force assaults.
A strong password should be at least 8 characters long and include a mix of numbers, letters, symbols, and capital and lowercase letters. Account lockout rules, which lock an account after a predetermined number of unsuccessful login attempts, can also aid in preventing brute force assaults. Additionally, CAPTCHAs can ALSO aid to avoid brute force attacks by asking the user to verify that they are a human before allowing them to log in. Additionally, encrypting your data with a powerful encryption scheme like AES256 can prevent cloud vendors from accessing it without the encryption key. Make sure the cloud provider you select has a clear security policy in place and is dedicated to keeping your data safe. Regularly check your cloud accounts for suspicious activity, such as unauthorized data access or modifications to user rights. A good method for preventing unauthorized access to your data is two-factor authentication. Requiring a second authentication method gives your accounts an added degree of security. It is practically impossible for cloud vendors to access your data without your authorization by using virtual private networks, which also build an encrypted tunnel for it.

4.6. Functionality Assessment

An efficient cloud data protection system ought to be capable to overcome challenges by shielding the owner's information from all risks associated with cloud computing, allowing the advantages of cloud computing to maximize their potential and progress in the directions they were meant for. This model describes security measures that can be effectively used to prevent zero-day attacks. Table 1 illustrates the total number of zero-day attacks recorded from 2011 to 2021 according to the Purplesec Cyber Security Experts.

Table 1. Statistics Of Zero-Day Attacks according to the Purplesec Cyber Security Experts.

Year	No. of Zero-Day Attacks
2011	28
2012	25
2013	41
2014	34
2015	35
2016	34
2017	40
2018	31
2019	29
2020	38
2021	66
Total	401



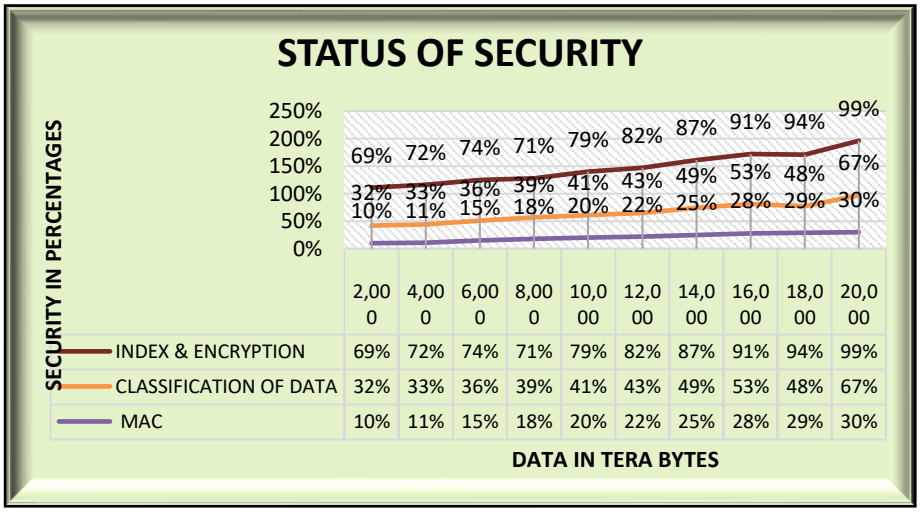
(a)Statistics of Zero-Day attacks from 2011-2021

In the third quarter of 2021, the percentage of zero-day malware climbed by 3% to 67.2%. A number of 83 zero-days were reported in 2021, an increase of 55% from the 2020s' 36 zero-days. Between 2016 and 2020, 12 to 25 zero-day attacks were discovered per year, or roughly 21 on average. In 2019, 80% of all catastrophic data breaches were caused by zero-day attacks. According to estimates, zero-day assaults made up 42% of all attacks in 2021. According to FireEye, there were more than 306 zero-day vulnerabilities discovered in 2020, up from 287 in 2019 . Trend Micro reported that zero-day attacks were responsible for 27% of all cyber-attacks in 2020. According to Kaspersky, zero-day exploits were responsible for 5.3% of all cyber-attacks in 2020. A recent report from Check Point released in October 2020 revealed that zero-day attacks rose by 77% in the first half of 2020 compared to the same period in 2019.

5. RESULTS AND DISCUSSION

After the installation of security parameters such as MAC, Data Classification, and Index & Encryption technique, Graph (b) displays the security status. The installation of Index and Encryption mechanism offers the greatest security than the use of Data Classification, which offers greater protection than MAC. When all three security considerations are combined, namely MAC, Data Classification, Index & Encryption, is taken into consideration, the security of data pertaining to the owner is very excellent overall. It leads to extremely good security of the suggested model, which is depicted as a peak value in Graph (b). The data integrity saved in the cloud is safeguarded by Message Authentication Codes (MAC), which offer a safe way to confirm that the data hasn't been altered since it was transferred there. A hash value that is used to authenticate the message is calculated by MACs using a shared secret key between the sender and the receiver.

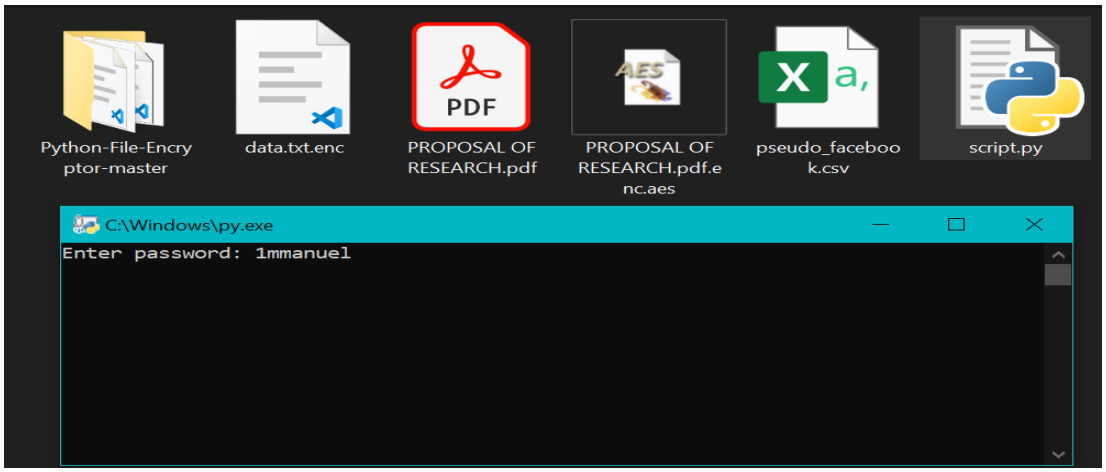
Data were classified into multiple categories according to their level of sensitivity in order to establish the best security precautions to take in order to safeguard it. Confidential, sensitive, and public are just a few examples of the various levels of sensitivity. This aids cloud service providers in applying the right security safeguards to safeguard the data according to its level of sensitivity. This research study claims that by encrypting the data with a key, Index & Encryption techniques offer the highest security protections for data kept in the cloud. This implies that only those with access to the key can access the data. Data is stored and searched relatively fast and effectively using indexing techniques. Because it enables them to easily locate data when needed, this is significant for cloud service providers.



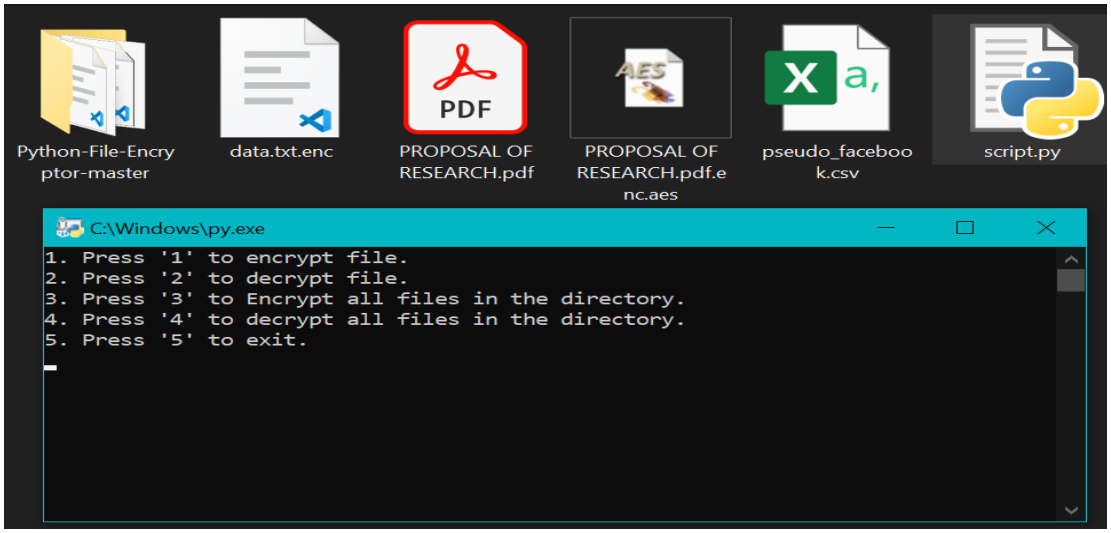
(b) Security Analysis of Mac, Classification & Index & Encryption

6.1. Dataset

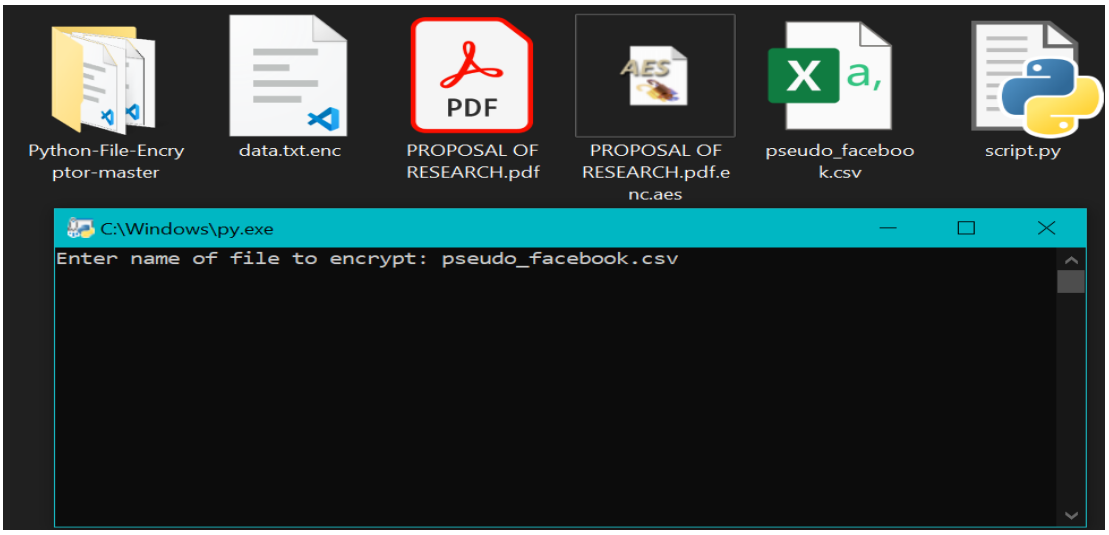
We made use of the Kaggle dataset pseudo facebook.csv. The dataset has almost 0.9 million entries, 15 columns, and 1397896 rows, thus it falls within the large dataset category. User-id, age, dob day, dob year, dob month, gender, tenure, friend count, friendship initiated, likes, likes received, mobile likes, mobile likes received, www likes, and www likes received are the three labels that make up the majority of it. The AES encryption for this model was done using Python and Pycryptodome, while the index creation was done using R Studio. Python 2.6 and 2.7, Python 3.4 and later, PyPy, and a self-contained Python package containing low-level cryptographic primitives known as PyCryptodome are all supported. In PyCryptodome, a fork of PyCrypto, more algorithms have been added along with improvements to the original PyCrypto library. For most of the algorithms in this library, pure Python is used whenever possible and C extensions are only used for components that are strictly necessary to performance (such as block ciphers).

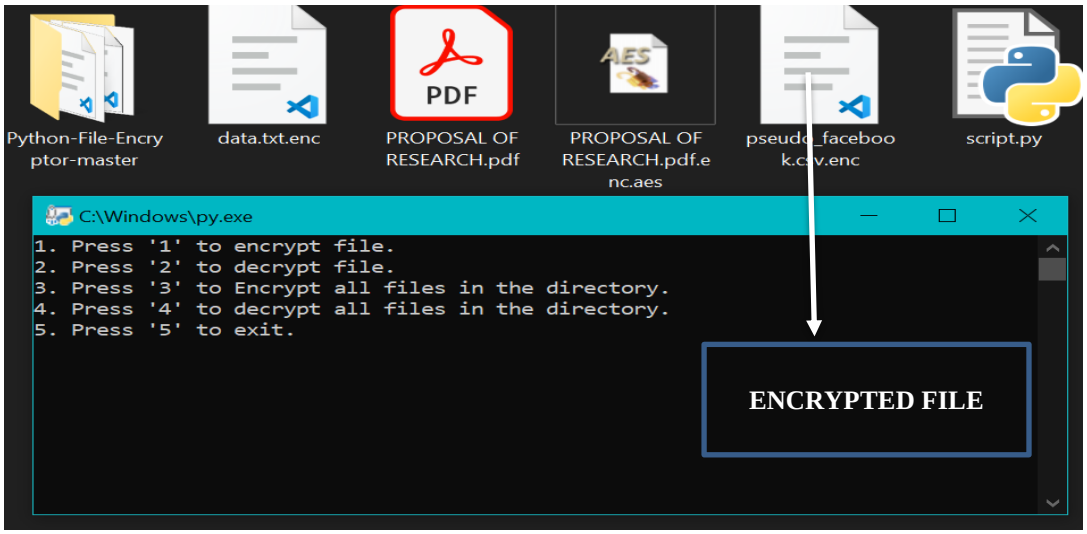


AES encryption using python and pycryptodome (unencrypted documents)

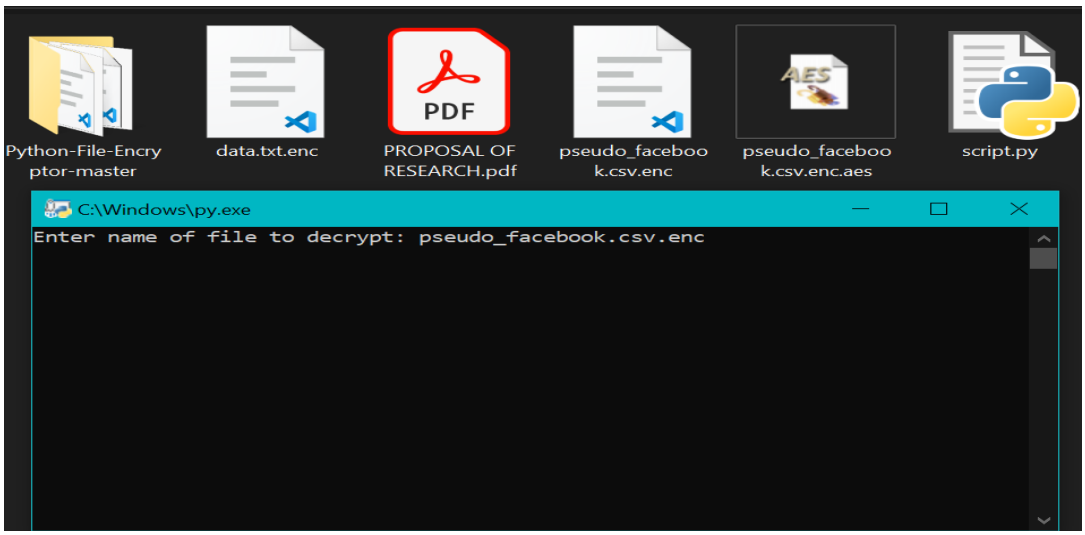


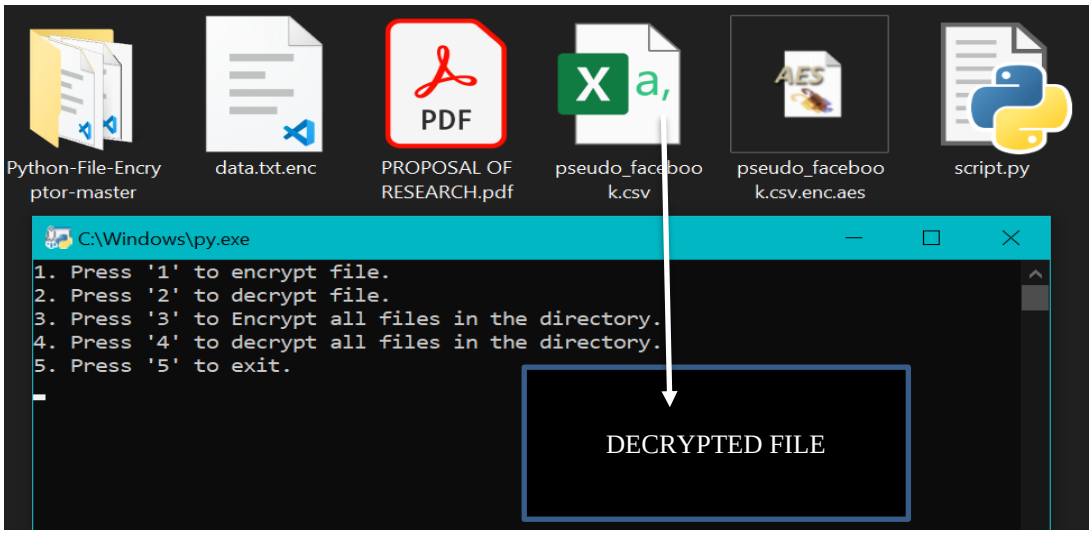
The pseudo_facebook.csv file is to be encrypted




Python-File-Encryptor-master
data.txt.enc
PROPOSAL OF RESEARCH.pdf
PROPOSAL OF RESEARCH.pdf.enc.aes
pseudo_facebook.csv.enc
script.py
C:\Windows\py.exe
1. Press '1' to encrypt file.
2. Press '2' to decrypt file.
3. Press '3' to Encrypt all files in the directory.
4. Press '4' to decrypt all files in the directory.
5. Press '5' to exit.
ENCRYPTED FILE


pseudo_facebook.csv.enc
C: > Users > admin > Music > test files > pseudo_facebook.csv.enc
This document contains many invisible unicode characters
Disable Invisible Highlight
CIPHERTEXT OF THE PSEUDO_FACEBOOK.ESV FILE


Python-File-Encryptor-master
data.txt.enc
PROPOSAL OF RESEARCH.pdf
pseudo_facebook.csv.enc
pseudo_facebook.csv.enc.aes
script.py
C:\Windows\py.exe
Enter name of file to decrypt: pseudo_facebook.csv.enc



6. CONCLUSION

This paper offers a solution for data protection, checking the authenticity and integrity using the best practices in the sector. It discusses categorizing data into distinct groups, index builders, SSL encryption, Message Authenticate Codes (MAC), double user authentication—first by the user's owner, then by the cloud—and cloud-based digital signature verification. By discussing solutions to numerous problems, including data tampering, data leakage, and unwanted access even from the cloud service provider, it makes data accessible. Additionally, this document offers increased flexibility and capability to meet the demands of today's complex, diversified networks. It also offers a way for users to search for information in the cloud and retrieve it.

REFERENCES

[1] Humayun, R. (2021) "Review on Cloud Computing and Cloud Security issues." Available at: https://doi.org/10.36227/techrxiv.13727878.v1.

[2] Author links open overlay panelM.G. Avram and AbstractWith the rapid development of processing and storage technologies and the success of the Internet (2014) Advantages and challenges of adopting cloud computing from an enterprise perspective, Procedia Technology. Elsevier. Available at: https://www.sciencedirect.com/science/article/pii/S221201731300710X (Accessed: March 10, 2023).

[3] Bertino, E. (2016) "Data Security and privacy: Concepts, approaches, and Research Directions," 2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC) [Preprint]. Available at: https://doi.org/10.1109/compsac.2016.89.

[4] Chen, D. and Zhao, H. (2012) "Data Security and Privacy Protection Issues in cloud computing," 2012 International Conference on Computer Science and Electronics Engineering [Preprint]. Available at: https://doi.org/10.1109/iccsee.2012.193.

[5] Sood, S.K. (2012) "A combined approach to ensure data security in cloud computing," Journal of Network and Computer Applications, 35(6), pp. 1831–1838. Available at: https://doi.org/10.1016/j.jnca.2012.07.007.

[6] Harmening, J. and DeVitto, R. (2020) "Cloud Security Access Control: Distributed Access Control," Cloud Computing Security, pp. 157–166. Available at: https://doi.org/10.1201/9780429055126-15.

[7] Neto, A. (2023) SAAS implementation challenges and Pitfalls, SaaSholic. Available at: https://saasholic.com/saas-implementation-challenges-and-pitfalls/ (Accessed: March 10, 2023).

[8] Alzahrani, A., Alalwan, N. and Sarrab, M. (2014) "Mobile cloud computing," Proceedings of the 7th Euro American Conference on Telematics and Information Systems [Preprint]. Available at: https://doi.org/10.1145/2590651.2590670.

[9] Overby, E., Bharadwaj, A. and Sambamurthy, V. (2006) "Enterprise agility and the enabling role of Information Technology," European Journal of Information Systems, 15(2), pp. 120–131. Available at: https://doi.org/10.1057/palgrave.ejis.3000600.

[10] Staff, D. (2021) Should your email live in the cloud? A comparative cost analysis, Datamation. Available at: https://www.datamation.com/white-papers/should-your-email-live-in-the-cloud-a-comparative-cost-analysis/ (Accessed: March 10, 2023).

[11] Cloud security and privacy:an enterprise perspective on risks and compliance (no date) Guide books. Available at: https://dl.acm.org/doi/10.5555/1594881 (Accessed: March 11, 2023).

[12] Tezcan, C. (2021) "Optimization of Advanced Encryption Standard on graphics processing units," IEEE Access, 9, pp. 67315–67326. Available at: https://doi.org/10.1109/access.2021.3077551.

[13] Reyad, O. et al. (2021) "Key-based enhancement of Data Encryption Standard for Text Security," 2021 National Computing Colleges Conference (NCCC) [Preprint]. Available at: https://doi.org/10.1109/nccc49330.2021.9428818.
[14] Thabit, F., Alhomdy, S. and Jagtap, S. (2021) "Security analysis and performance evaluation of a new lightweight cryptographic algorithm for cloud computing," Global Transitions Proceedings, 2(1), pp. 100–110. Available at: https://doi.org/10.1016/j.gltp.2021.01.014.
[15] Et.al, Q.W. (2021) "Energetic data security management scheme using hybrid encryption algorithm over cloud environment," Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(6), pp. 201–208. Available at: https://doi.org/10.17762/turcomat.v12i6.1289.
[16] Prabhdeep Singh, & Ashish Kumar Pandey. (2022). A Review on Cloud Data Security Challenges and existing Countermeasures in Cloud Computing. International Journal of Data Informatics and Intelligent Computing, 1(2), 23–33. https://doi.org/10.5281/zenodo.7464700
[17] Wani, A.R., Rana, Q.P. and Pandey, N. (2018) "Performance evaluation and analysis of Advanced Symmetric Key cryptographic algorithms for cloud computing security," Advances in Intelligent Systems and Computing, pp. 261–271. Available at: https://doi.org/10.1007/978-981-13-0589-4_24.
[18] Manju Bargavi, M.Senbagavalli, Tejashwini.K.R, & Tejashvar.K.R. (2022). Data Breach – Its Effects on Industry. International Journal of Data Informatics and Intelligent Computing, 1(2), 51–57. https://doi.org/10.5281/zenodo.7469630
[19] SafeHouse (2021) AES: How the most advanced encryption actually works, Medium. CodeX. Available at: https://medium.com/codex/aes-how-the-most-advanced-encryption-actually-works-b6341c44edb9 (Accessed: March 11, 2023).
[20] Padmavathi, R.A. and Dhanalakshmi, K.S. (2021) "An advanced encryption standard in memory (AESIM) efficient, high-performance S-box based AES encryption and decryption architecture on VLSI," Wireless Personal Communications, 123(4), pp. 3081–3101. Available at: https://doi.org/10.1007/s11277-021-09278-2.
[21] Abikoye, O.C. et al. (2019) "Modified advanced encryption standard algorithm for information security," Symmetry, 11(12), p. 1484. Available at: https://doi.org/10.3390/sym11121484.
[22] Khompysh, A. et al. (2022) "Design of substitution nodes (s-boxes) of a block cipher intended for preliminary encryption of confidential information," Cogent Engineering, 9(1). Available at: https://doi.org/10.1080/23311916.2022.2080623.
[23] Lee, W.-K. et al. (2022) "Efficient implementation of AES-CTR and AES-ECB on gpus with applications for high-speed frodokem and exhaustive key search," IEEE Transactions on Circuits and Systems II: Express Briefs, 69(6), pp. 2962–2966. Available at: https://doi.org/10.1109/tcsii.2022.3164089.
[24] Rajesh, N., Selvakumar, A.A.L. Association rules and deep learning for cryptographic algorithm in privacy preserving data mining. Cluster Comput 22 (Suppl 1), 119–131 (2019). https://doi.org/10.1007/s10586-018-1827-6.
[25] Coppersmith, D. (1994) "The Data Encryption Standard (DES) and its strength against attacks," IBM Journal of Research and Development, 38(3), pp. 243–250. Available at: https://doi.org/10.1147/rd.383.0243.
[26] Smid, M.E. and Branstad, D.K. (1988) "Data Encryption Standard: Past and Future," Proceedings of the IEEE, 76(5), pp. 550–559. Available at: https://doi.org/10.1109/5.4441.
[27] Bourbakis, N. and Alexopoulos, C. (1992) "Picture data encryption using scan patterns," Pattern Recognition, 25(6), pp. 567–581. Available at: https://doi.org/10.1016/0031-3203(92)90074-s.
[28] ADLEMAN, L.E.O.N.A.R.D.M. et al. (1999) "On applying molecular computation to the Data Encryption Standard," Journal of Computational Biology, 6(1), pp. 53–63. Available at: https://doi.org/10.1089/cmb.1999.6.53.
[29] Schaefer, E.F. (1996) "A Simplified Data Encryption Standard algorithm," Cryptologia, 20(1), pp. 77–84. Available at: https://doi.org/10.1080/0161-119691884799.
[30] Aayush, A., Aryan, Y. and Muniyal, B. (2022) "Understanding SSL protocol and its cryptographic weaknesses," 2022 3rd International Conference on Intelligent Engineering and Management (ICIEM) [Preprint]. Available at: https://doi.org/10.1109/iciem54221.2022.9853153.
[31] Khan, N.A. et al. (2022) "Employing public key infrastructure to encapsulate messages during transport layer security handshake procedure," 2022 Applied Informatics International Conference (AiIC) [Preprint]. Available at: https://doi.org/10.1109/aiic54368.2022.9914605.
[32] Wen, C. et al. (2021) "Advanced Data Encryption using 2D materials," Advanced Materials, 33(27), p. 2100185. Available at: https://doi.org/10.1002/adma.202100185.
[33] Oberti, F. et al. (2022) "Lin-mm: Multiplexed message authentication code for local interconnect network message authentication in road vehicles," 2022 IEEE 28th International Symposium on On-Line Testing and Robust System Design (IOLTS) [Preprint]. Available at: https://doi.org/10.1109/iolts56730.2022.9897819.
[34] Chang, H. and Choi, E. (2011) "User authentication in cloud computing," Communications in Computer and Information Science, pp. 338–342. Available at: https://doi.org/10.1007/978-3-642-20998-7_42.
[35] Choudhury, A.J. et al. (2011) "A strong user authentication framework for cloud computing," 2011 IEEE Asia-Pacific Services Computing Conference [Preprint]. Available at: https://doi.org/10.1109/apscc.2011.14.
[36] Khan, N., Zhang, J. and Jan, S.U. (2022) "A robust and privacy-preserving anonymous user authentication scheme for public cloud server," Security and Communication Networks, 2022, pp. 1–14. Available at: https://doi.org/10.1155/2022/1943426.

BIOGRAPHIES OF AUTHORS

Kofi Immanuel Jones Received his B.Sc in Geology from the Fourah Bay College University of Sierra Leone in 2016. He is currently pursuing His MSc in Computer Science and Information Technology at Jain University Bangalore. He can be contacted at email: kofijones37@yahoo.com

Suchithra R. Has 19 years of experience in teaching and research. Published papers in Science and Scopus, four patents, published three book chapters. She is currently working as Head of the Department of Computer Science and Information Technology at Jain University. She can be contacted at email: r.suchithra@jainuniversity.ac.in