A Systematic Survey of Cloud Data Security Techniques

ARULJOTHI R[1], DR JEMIMA PRIYADARSINI R[2]
[1]*Research Scholar, Department of Computer Science, Bishop Heber College (Autonomous), Trichy, Tamil Nadu. Affiliated with Bharathidasan University, Trichy*
[2]*Associate Professor, Department of Computer Science, Bishop Heber College (Autonomous), Trichy, Tamil Nadu. Affiliated with Bharathidasan University, Trichy*

Abstract*— Cloud computing is a well-equipped platform for providing computing resources to the demanded consumers. The providing resources from the cloud are virtual. The main purpose of cloud usage is to store data and applications on the cloud server because the cloud provides an efficient storage system to store the user's data and applications. The cloud service providers from the cloud data centreto monitor and maintain the cloud servers. Overall, the cloud provides many benefits to users, and at the same time, it also has many data security challenges. The data stored in the cloud are in public storage, which may lead to data security vulnerability. The security vulnerability leads to data loss or data disclosure by illegitimate users. Many researchers contributed to addressing the data security issues in the cloud by delivering many security methods to defend the data in the cloud storage. This paper surveyed the list of techniques proposed for addressing security issues and excavated more to explore the details of the techniques. The paper compares the techniques based on their performance in addressing cloud data security. The paper also suggests which technique can be further enhanced to improve data security in the cloud. The finding and interpretation of this paper are given to suggest where and which technique can be more useful and malleable for cloud data security.

***Index Terms*— Cloud Computing, Security, Data Storage, Encryption, Cryptography**

I. INTRODUCTION

Today's computing world has advanced with many new technologies like Machine learning, Data Science, etc.; wherever the technologies rule the IT world today, cloud computing is the only technology behind all to provide space to process the data and applications and provide facility to operate new inventions [1]. Cloud extends many conveniences to the computing users to uninterrupted use of the computing resources. Cloud is in the form of public access and private access. Cloud computing providers manage and control public access to cloud data centres [2]. Cloud can be used in different ways; users can use it as an application service, developers can use it as a platform service to host their applications, or business users can use it as an infrastructure service to get the required virtual computer server from the cloud [3]. So, the cloud can be used in the said ways. During this time of using the cloud, the user stores some data or applications in the cloud storage. The point to note in this scenario is how the data or application is secure from other users in the cloud. Or how is data secured from the administrators in the cloud data centres? How can it be secured from the intended hackers or intruders from unauthorised disclosure of the user's data? The most noticeable area of the cloud is how the cloud could provide security to data or applications stored by the users [4]. Many reviews and surveys are taken to report the necessity of the security requirement in the cloud [5]. Cloud computing is a delightful target for several computing requirements. Still, data security plays the most important role in the cloud and the main preoccupation on the Internet to serve all its services and advantages[6].

Cloud Security Report 2022 [7] indicates that cloud security continues to be a major concern for cybersecurity professionals. With a two percentage point increase from last year, 95 per cent of organisations are moderately or extremely concerned about their security posture in a public cloud environment. Figure 1 shows the cloud security concern level of companies.

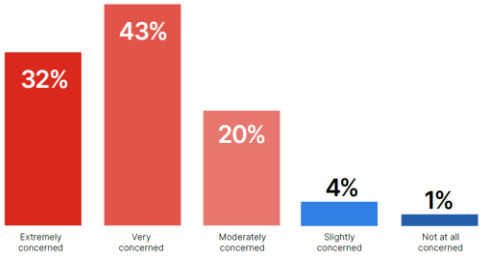

Figure 1. Cloud Security Concerns of Companies [7]

Security professionals are looking for ways to improve the security of public clouds. Cybersecurity professionals are asked which controls would increase their confidence in adopting cloud services. There are three checks at the top of the list: Resting Data Encryption (54%), Compliance Automation (46%), and Establishing and Enforcing Security Policies (46%).In addition, over three-quarters (78%) of respondents consider it extremely helpful to have a single cloud security platform with a dashboard to consistently and comprehensively protect data across their cloud footprint [7].The report says that data security in the cloud is a more important concern. The secret of data over the network could be reached using the cryptographic technique, which is the procedure of encryption and decryption [8].

Cryptography is an ancient technique to secure the data travelled and stored in the network. Security can be serviced in different ways like confidentiality, integrity and availability or authentication. For example, encryption is the system by which the original data are transformed from a plain data form to an encoded form (cipher text) that another entity can only decode if they have access to a decryption key. Decrypting is the reverse encryption process for converting encrypted text into clear text. The three most common encryption and decryption methods are symmetric, asymmetric, and hybrid algorithms for encrypting and decrypting data in cloud storage [9].

Symmetric encryption is an encryption system in which the sender and recipient of a message share only one common key, which is used to encrypt and decrypt the message. Data Encryption Standard (DES) and Advanced Encryption Standard (AES) are symmetric algorithms used in cloud computing. A symmetrical encryption uses two different but related keys. One is a public key used for encrypting, and the other is the private key used for decrypting. The private key is fictional to be private so that only the authenticated receiver can decrypt the message. The RSA algorithm is an example of an asymmetrical encryption technique used for cloud computing. Hybrid encryption combines two or more encryption schemes and includes a mixture of symmetric and asymmetric encoding to take advantage of the strengths of each type of encryption [10].

There are many ways to protect data in cloud storage. This paper chooses some related research works that have proposed a security technique for protecting the data in the cloud environment. Each proposed technique has its characteristics, and compiled details of each technique are given in the comparison table at the end of this paper.

II. DATA VULNERABILITY IN THE CLOUD

Cloud is more convenient for storing and retrieving data via the Internet. However, the data is more vulnerable and should be safe from other users and hackers. The vulnerability to the data is a concern of protecting the data. The cloud has many possibilities to disclose the data without the data owner's knowledge. Therefore, protection against data disclosure is the main concern in the cloud environment. Therefore, a security vulnerability is the most significant area in the cloud computing environment [11]. The security concerns are end-user data protection, network bandwidth traffic, file storage systems, and host-machine security, which cryptography can resolve to some extent and thus helps organisations reluctant to accept Cloud Computing [12]. Various security vulnerabilities that arise in the cloud are listed below,

- *Ensure secure data transfer:* In a cloud environment, physical location and scope are not under the control of the end-user regarding the location of resources.
- *Ensure a secure interface:* the integrity of information when transferring, storing and recovering must be ensured over the unsecured Internet.
- *Data separation:* Privacy issues arise when cloud providers access personal data or when limits between personal and enterprise data are not clearly defined.
- *Secure Stored Data:* It is an enquiry on monitoring the encoding and decoding by either the end-user or the Cloud Service provider.
- *User Access Control:* Compliance auditors and security managers must provide web data logs for web-based transactions.

III. CRYPTOGRAPHY FOR CLOUD

Cryptography is the traditional way to protect the data in the network. It can be used in different security services such as authentication, confidentiality, integrity and availability. Authentication is the confirmation that the incoming user is registered or unregistered. Confidentiality ensures that legitimate users can only access the data. Integrity ensures that legitimate users can only update or modify the content of the data. Finally, available ensures that the required service is always available to the users. The main service concentrated on in this survey article is to ensure the confidentiality of the data stored in the cloud. Because when confidentiality is ensured 100%, there is no possibility of other vulnerabilities [13].

The encryption techniques ensure the confidentiality of the data. There are two techniques to ensure confidentiality in cryptography: symmetric cryptography and asymmetric cryptography. Symmetric encryption converts the original data into unintelligible data, which can't be understandable by anyone until it is decrypted.

Generally, it is compulsory to have a key and encryption technique for encrypting the data. Symmetric encryption uses the same key for encryption and decryption, and it can also be referred to as single or secret key cryptography. However, only symmetric encryption has the speed and computational efficiency in handling the encryption of large volumes of data [14]. For example, a source produces a communication in plaintext, X = [X1, X2, X3,…. XM]. For encryption, a key is generated at the message source. Then the key is also provided to the destination using some secure channel. With the data X and the encryption key K as input to the encryption, the encryption algorithm produces the encrypted text Y = [Y1, Y2,….YN]. It is written as Y = EK(X). First, the encrypted text Y is produced from the encryption procedure, where E indicates the encryption technique and Kdenotes the encryption key. Next, on the other side, the receiver receiving the message is decrypted using the same key used at the time of encryption to get the original message X = DK[Y]. Here D denotesthe decryption technique. Figure 2 depicts the symmetric cryptographic system's functional diagram.

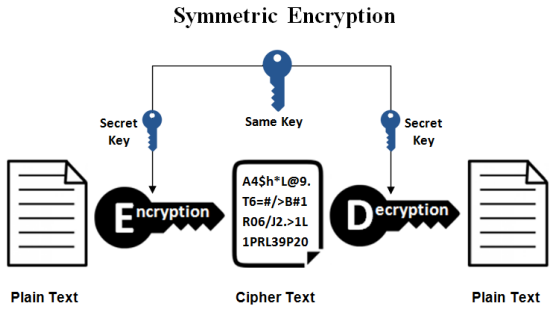

Figure 2. Symmetric Cryptography [15]

Another way of cryptography is asymmetric encryption. In asymmetric encryption, two keys are used for encryption and decryption. The two keys are related keys, which are the public key and the private key. The public key is used for encryption by the sender, and the private key is used for decryption by the receiver. For example, A wants to send a message to B, A encrypts the data using B's public key, and B decrypts data using B's private key on the receiving side. Here, the scenario is that the private key is only known to the receiver and is not shared with other users in the communication. By the literature, asymmetric encryption is taken more time to encrypt and decrypt the small size of data [16]. An example of asymmetric encryption is RSA. RSA is used for the encryption of a small amount of data. In [17], the key used for symmetric encryption is encrypted by the RSA. The diagram of the asymmetric cryptographic system is shown in Figure 3.

s

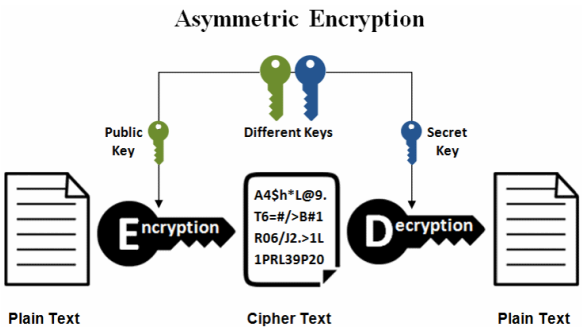

Figure 3. Asymmetric Cryptography [15]

IV. SYMMETRIC CRYPTOGRAPHY FOR CLOUD

Cloud dominates IT enterprises by way of its computing services. Data storage is one of the services provided by cloud computing. Cloud storage primarily

supports small and medium-sized businesses (SMEs) by reducing their capital investments and maintaining storage servers. Most SMEs are outsourcing their data to cloud storage. Enterprises' data forwarded to the cloud must be kept in public cloud storage. Safety and security are the main problems when it comes to cloud storage. The confidentiality setting assures the security of data storage. Arockiam L et al. [18] proposed a security service algorithm called AROcrypt to ensure data security in the cloud storage environment. The paper discussed the cloud environment's security as a Service (SEaaS). The AROcrypt security service algorithm proposed by the CSP.

It's a symmetrical cryptographic algorithm. It uses four keys to encrypt, and the same keys are used to decrypt. Initially, the given characters are converted to ASCII values. Then, a square matrix is formed according to the number of characters in the plain text. The maximal matrix size is 25X25.Next, the square matrix is split into three matrices called Top Matrix (UMAT), Diagonal Matrix (DMAT) and Bottom Matrix (UMAT).Next, apply encryption to individual UMAT, DMAT and UMAT matrices using K1, K2 and K3 keys, respectively. Next, another square matrix is built using a numeric value. Now the text is read on a column-by-column basis. The order in which the column is interpreted is based on the K4 key. Next, the ASCII code values are converted to character values. The AROcrypt process only non-numerical data. Finally, the algorithm is evaluated in the simulation environment, and the author claimed that AROcrypt produced better results.

Manikandasaran, S. S. et al. [19] proposed a security technique based on the obfuscation technique called MONcrypt. The obfuscation is also used to secure the network's data and application. Generally, the obfuscation technique does not use any key to obfuscate the data, but the proposed techniques by the authors use keys to obfuscate the data. The obfuscation process has many mathematical calculations to convert and is applied to numerical data. The MONcrypt is executed in the obfuscation module in the proposed scenario. The MONcrypt is invoked when the users upload data to the cloud storage. Initially, the plain text values are arranged as an array of numerical values T = T(1), t(2), T(3),…T(n). The mathematical function, namely pow(), is applied to the plain text T(i). The pow () function is used to find square value T(i)(D(i) = pow(T(i), 2)). D(i) value is divided by 256 to find the count(i) value and also to get the reminder value in RD(i). The count(i) represents the number of times the D(i) is divided by 256. RD(i) value is between 0 to255. Finally, the obfuscated text is generated by converting the RD(i) into an ASCII character value. Users' data are forwarded after the completion of this obfuscation module. This technique is evaluated in a simulation environment and takes minimal time to obfuscate the data.

Balamurugan S. et al. [20] proposed an algorithm called ESSAO that is executed before the data are uploaded to the cloud storage. The ESSAO is an obfuscation technique. ESSAO uses a different mathematical function to obfuscate the users' data. The procedure of the ESSAO is as follows, the users' data are taken as plaintext (PT). Consider the numerical values in the PT to obfuscate. Find the length(N) of PT. Determine the position (POS) of each value in PT. Multiple (MUL) PT with its positional value. • Find a Square (SQU) of each value in the MUL. • Get the key K from the KaaS cloud service. Apply the Key K on SQU values. For each value in the SQU, key K is incremented by 1. Find the Reverse (REV) value of SQU.Find the Modulus (MOD) of REV by 256, and the quotient value is the Secret Key (SK). Convert the MOD value into ASCII code. ASCII converted value is the obfuscated text (OT). ESSAO converts all the characters in the plaintext into ASCII decimal code, and these values are computed with the following mathematical functions such as multiply (), pow(), reverse(), modulus() and ascii(). This technique is evaluated in a simulation environment and takes minimal time to obfuscate the data.

Veeraragavan N. et al. [21] proposed a security technique called EEA, which encrypts the data for storage in the cloud. The following steps represent the procedures of the EEA. First, users' data (Plain Text) are converted into ASCII codes. Then, ASCII codes of the Plain Text (PT) are converted into binary bits. Bit values are used throughout the execution of the algorithm. A Prime Number (*PRM_NO)* is generated based on the number of bits in the PT. Then, the total number of bits is divided into fixed-size blocks. The size of each block is equal to the generated *PRM_NO*.

Key Generation as a Service(KGaaS) is a cloud service for generating keys for encryption algorithms; it generates keys K1 and K2 for encryption. K GaaS uses Random Number Generation (RNG) to generate keys for encrypting and decrypting EEA. Each block of bits is rotated from right to left at K1 times. Merge each rotated block into a single block and find two's complements. Compute the XOR with K2 and divide data into8 bits blocks. Convert the 8 bits block into the corresponding decimal value. Finally, the decimal value is converted into ASCII character code to produce the cipher text. The technique is tested in a simulation environment and produces better results.

Kalaichelvi et al. [22] proposed an enhanced AES algorithm. The EnAES preserves the confidentiality of data stored on the cloud. It embraces three mechanisms, namely, data partition, shuffling and an encryption technique. The EnAES to ensure data confidentiality. The first mechanism in the proposed AES is partitioning a big volume of data into multiple chunks. Secondly, to provide security, these chunks are shuffled to change the order of the generated chunks before they get encrypted by EnAES in the shuffling mechanism. Finally, the hash function is used in metadata creation and is maintained safely on the Data Owners' (DO) side. The hash function offers two roles to the proposed system: 1) It maintains the integrity of data, and 2) The indices generated using the hash function are used to retrieve the data back to the original form on the client side. The first and the second mechanisms together are known as the PaShu module. It serves as a base layer of security, and it happens on the Do's side. Subsequently, the shuffled chunks are encrypted by EnAES to provide data confidentiality. After these mechanisms are applied to the data, the shuffled and encrypted data chunks are transferred to the cloud. When Data User (DU) needs to access the cloud-stored data, the transaction takes place on the client side to access the shuffled and encrypted data. The transaction between the DOs and the DUs helps to identify the authorized user. Then the identified authorised users fetch the shuffled and encrypted data chunks from the cloud with their genuine credentials. On the DUs side, the proposed algorithm proposes an efficient retrieval scheme using appropriate decryption methods and a system to rearrange and merge the data chunks to get the original data.

As a result, EnAES CCSA provides substantial data security and a proficient retrieval scheme by incorporating data confidentiality.

K. Balaji et al. [23] proposed that an ESCET is a symmetric block cipher technique. It uses 160-bit keys for encryption and decryption. The technique runsvariable numbers of rounds according to the key. The 160- bit key is divided into five subkeys that are SK1 to SK5.The SK1 8-bit subkey denotes the number of rounds the encryption or decryption is carryout. The SK2 8-bit subkey is used with PT for finding product value. The SK3 8-bit subkey denotes the number of the circular shift of the decimal PT values. The SK4 128-bit subkey for finding XoR with 128-bit value. The SK5 is an 8-bit subkey used for finding 8-XoR operation. Unlike existing encryption techniques, the number of rounds is not fixed. Instead, rounds are changed based on the SK1 value. This is because the cryptography operations of substitutions and permutations confuse and diffuse the cryptanalyst. The main key, 160-bit, is generated from the input data given by the user to upload. Therefore, convergent encryption first generates the key from the data uploaded to the cloud. This technique is proposed for security and to reduce duplicate data in the cloud.

S. Arul Oli et al. [24] proposed symmetrical encryption for securing non-numerical data in cloud storage. When the user wants to hide only the non-numerical data that are more sensitive, then this proposed encryption might be very comfortable. This algorithm uses three keys for encryption and decryption. Among the three keys, two keys are integer, and one is string type. The proposed technique uses the square matrix to manipulate the plaintext and process user data at three levels. First, the data are split based on even and odd columns in the matrix. Second, the Key K1 and K2 are applied to the data alternatively. Third, data are filled in a square matrix column-wise and read row-wise based on the order of characters in the key K3. Finally, the ciphertext is produced for the submitted plaintext. Decryption is done while reversing the process of encryption steps with the same keys. This technique is tested and produces better results.

S. Arul Oli et al. [25] proposed a technique based on the obfuscation technique. Generally, obfuscation is a

technique like encryption, butit uses different mathematical methods or some critical programming logic to hide original data. The proposed technique obfuscates the data before they are uploaded into the cloud. The proposed technique uses different methods like ascii(), binary(), rotate(), two complex() and decimal() to obfuscate the original data. It also uses a key which is used to rotate the values. This algorithm is only used to obfuscate the numerical data. The strength of the technique is measured in the simulation environment, and it shows better improvement in security.

RSugumaret al. [26] proposed a symmetrical encryption algorithm called SEA. The SEA encrypts the data before sending it to the cloud storage. SEA is a cloud service, and keys generation is a cloud service. SEA uses two keys for both encryption and decryption. Keys used for encryption are not communicated to CSPs who provide storage. Keys are confidentiality stored on the user's side for decrypting the data. The proposed encryption algorithm is provided as a security service from a CSP. It is a symmetric encryption algorithm. Users' data are in Plaintext (PT), submitted for encryption. Initially, SEA counts the number of characters in the PT and divides the PT into PT1 andPT2. Next, PT1 and PT2 are converted into ASCII code values. A square matrix MAT[R][C] is formed for the total number of characters in PT. From MAT[R][C], CT1 and CT2 are derived. The keys K1 and K2 are applied on CT1 andCT2, respectively. Finally, convert CT1 and CT2 into ASCII code to produce the Cipher Text (CT). The simulation is conducted to evaluate the technique.

S. Balamurugan et al. [27] proposed a security technique for protecting data from security attacks. First, the plaintext is converted into binaries. Next, the binaries are divided into blocks fetched from the odd and even position bits in the plaintext. Four keys are used for encryption and decryption K1, K2, K3 and K4. The keys K1 and K2 are applied on the odd and even block bits, respectively. The two blocks of data are merged and filled in a square matrix. The matrix size is based on the original text's total numbers. The matrix is divided into two sub-matrices. The odd columns indexed are formed as one matrix, and even columns indexed are formed as another. The keys K3 and K4 have been applied to the even columns indexed matrix, and odd columns indexed matrix, respectively. The two sub-matrices are merged as one matrix. The matrix values are read row by row. Finally, convert the ASCII code into character code to produce ciphertext. To retrieve the original text, do the reverse process of this encryption procedure. This approach produces better results.

L. P. George et al. [28] proposed an algorithm called GLEnc that only encrypts the non-numerical data. The user selects the GLEnc algorithm from the cloud environment. The algorithm immediately requests the key from the Secret Key as a Service (SKaaS) and provides a powerful key management algorithm. The SKaaS forward three randomly generated keys, K_1, K_2 and K_3, to the user's side. The user submits the plain text for encryption. First, the algorithm calculates the size of the plain text. Next, the algorithm converts the plain text into a corresponding binary. They are further divided into blocks based on alternative odd and even position bits. The odd or even blocks are split into 8-bit blocks. The keys K_1 and K_2 are applied to the data. Each 8-bit in the odd block is rotated at K_1 times from left to right. Simultaneously, the even blocks 8-bits are rotated at K_2 times from left to the right. Then the 1's complements are calculated in the odd and even blocks. The XOR of key K_3 on every eight bits value is calculated in the odd and even blocks. The key K_3 is incremented by one for every upcoming eight-bit value in the odd and even blocks. The odd and even blocks are merged in the same position as in the plain text. The merged block of bits is divided into 8-bit blocks. Every 8-bits is converted into an equivalent decimal. These decimal values are converted into ASCII character code to produce the ciphertext. The entire process of GLEnc encryption occurred at the service called by the user's end.

So, the intruder or the service provider is unaware of the original plain text. Hence, the security of personal data is increased, and the GLEnc algorithm reduces the time frame.

L. P. George et al. [29] proposed an obfuscation technique GLObfus to obfuscate the data. In particular, GLObfus is developed to secure digital data. User data are input into the proposed obfuscation method and receive the scrambled data once GLObfus process the data.In the GLObfus method, the user

provides the data in the original format. This method considers only the numerical values of the user's data. The data size is determined based on the information entered by the user. Initially, obfuscation is a procedure started by interchanging the odd and even positional values. The value of the position indicator subtracts the numerical values. Next, figure out the square of the subtracted values. A 'K' key is generated from the key service in the proposed framework and applied to square values. Next, the squared values are divided by 256 to get the mod value. The value of the quotient is retained as its secret key. Finally, the mod values are converted into ASCII characters. The ASCII character code is the obfuscated data. The key used in obfuscation is kept secure to de-obfuscate the data. The proposed method uses a single for obfuscation. However, it uses two keys for de-obfuscation. During the obfuscation, the data are divided by 256, and the module's values are found. The co-efficient value generated in this step is considered another key. It is also kept secure to de-obfuscate the data.

George Amalarethinamet al. [30] proposed a symmetric key encryption technique MAGcipher. To enforce stronger security for the various data stored in the cloud, it is possible to split the data into two Clouds, one being the Public Cloud, where information is accessible by the general public, and the other one is the usage of Private Cloud, where sensitive and mission-critical data is stored. Hence it is highly mandatory to apply robust measures for data protection in a hybrid cloud. It is responsible for cloud service providers to maintain the security of the data in the cloud. But in the public cloud environment, there is a possibility that the service provider can access the data without the knowledge of the data owner. To avoid the data being accessed by the service providers, users should handle encryption procedures ahead of the data being uploaded to the public cloud. The proposed algorithm MAGcipheris symmetric encryption and is executed before the data are uploaded to the cloud storage. MAGcipher uses different mathematical functions to encrypt the user's data.The encryption process involves a series of operations, including key insertion, complement computation, finding XOR, splitting, joining and merging. The necessity for these operations is relevant to the fact that the process of finding the key to decrypt the encrypted text becomes extremely difficult. It complicates the hacker by trying different keys to attack, making the plain text vulnerable. Decryption is the reverse process of encryption. Key plays a vital role in the secrecy of the data in the cloud. Key is generated from the cloud key provider as a service.

A. Fairosebanuet al. [31] proposed that PUCSCipher encodes the data as a 64-bit block. It is performed for the number of turns according to the key. The encryption rounds are not fixed; it is changed to various input data. The key to the encryption is 196 bits. From the 196-bit key, a subkey is derived as subkey2.Permutation stands for bit transposition. After permutation, the 64-bit is divided into two 32-bit halves. For example, subkey 3 is 64 bits divided into 32 bits. Therefore, both 32-bit are XoRed with sub-key 3.Following XoR, both 32 bits are swapped. After swapping, two 32-bits are fused into 64-bits, and a single round is finished. The same turn continues with the number of times indicated by subkey 1.When all turns are finished, the 64-bit is XoRed with sub-key 4 and generates the 64-bit ciphertext.

Many symmetric cryptosystems are proposed to protect the data in the cloud environment. Similarly, many asymmetric encryptions are also proposed for securing the data in the cloud. The following section describes the list of such algorithms.

V. ASYMMETRIC CRYPTOGRAPHY FOR CLOUD

The asymmetric cryptosystem is the method of using two keys for encryption and decryption of the cloud environment. Many researchers are tried to propose asymmetric-based encryption. For example, S. Kaushik et al. [32] proposed a hybrid symmetric encryption approach to provide more security for the owner's data other than any single symmetric encryption algorithm. This hybrid approach makes data more secure and protects it from any malicious activity attended by intruders. The proposed framework methodology combines transposition as primary and substitution as secondary ciphercryptographic techniques to encrypt confidential data before storing it over a cloud server. Both of these algorithms use the plaintext in its original form and perform encryption ordecryption

using a symmetric cryptographic algorithm only. Allthe keys used in any cryptographic operation are generated and distributed only by the key generator. This is a hybrid approach of symmetric and asymmetric key cryptography algorithms. The Data Encryption Standard (DES) and RSA are implemented to provide multilevel encryption and decryption at both sender and receiver sides, increasing cloud storage security and consuming more time for encryption and decryption.

Hossein Abroshan [33] proposed a combined cryptography approach when dealing with data in a cloud environment. However, a complex cryptographic algorithm is not useful in cloud computing, as computational speed is essential in that environment. Therefore, this solution utilises an enhanced Blowfish algorithm in combination with an elliptical curve algorithm. Blowfish encrypts the data, and the elliptical curve algorithm encrypts its key, increasing safety and performance. In addition, a digital signature technique serves to ensure the integrity of the data.

Quisi-Aphetsi Kester et al. [34] proposed a hybrid method of encryption of digital images based on an asymmetric encryption algorithm and a visual cryptographic algorithm. The encryption key used was based on a public key-exchange algorithm. This paper produced a hybrid digital encryption algorithm based on public key and visual cryptography. The ciphering of the plain image was done using the image encryption algorithm but dependent on the keys engaged. The public key was deduced based on a randomly chosen private key of n length with the engagement of a forward hash function algorithm [35]. For the image to be encrypted and decrypted, the two or more parties involved must choose a random private key and generate a public key from it. Theycan therefore interchange the public keys to communicate. The algorithm that generated the public key wasa forward hash function, making it difficult for anadversary to generate the private key easily. The exchanged keys were used to encrypt the image. The algorithm depended on a shared secret key (generated from the combination of a public key and a private key).

V. P. Bansal et al. [36] proposed a hybrid Crypto system using RSA and Blowfish algorithm. This hybrid cryptosystem is considered for cloud computing, where a digital signature is a must for user authentication. So, this technique provides features of both symmetric and asymmetric cryptography. Also, blowfish is unpatented, so this crypto system is also cost-efficient. Therefore, the hybrid RSA and Blowfish technique is proposed, which can be used for cloud computing on FPGAs. Cloud computing on FPGAs is useful because it is fast, compact, cheap, and easy to implement. Furthermore, the hybrid technique shown above has the properties of both symmetric and asymmetric techniques. The symmetric technique is fast, secure, has less memory consumption, and is simple in construction. The asymmetric technique is also known as public key cryptography. It is mainly considered for authentication purposes. The asymmetric techniques are encrypted by a public key but decrypted by only the authenticated user with the private key. The main problem is that key size must be kept high, so it cannot be found by direct key substitution. Therefore, it makes the process much slower. But, this hybrid technology allows the use of a small key for asymmetric technique because direct substitution doesn't work as it is the combined process with blowfish. So, the speed of the process is much faster than the separate process. The blowfish also becomes more secure as it needs both RSA and blowfish keys for decryption. So, the rounds of blow fish (Feistel network) can also be reduced to 8 rounds or 4 rounds which results in better speed than previous algorithms.

I. G. Amalarethinamet al. [37] proposed an Enhanced RSA algorithm, an asymmetric key algorithm using two dissimilar keys for encryption and decryption processes. The Key size can be varied to make the encryption process strong. Hence it is difficult for the attackers to intrude on the data. However, increasing key size correspondingly increases the time for encryption and decryption. The proposed algorithm reduces the time it takes to encrypt and decrypt by dividing the file into blocks and increasing the key's size. It opens the door to storing data in the cloud for users without inconvenience. Stage 1: This stage is used for generating two keys, namely, Public Key E and Private Key D. Generally RSA algorithm uses two prime numbers. In addition, the proposed ERSA

algorithm includes two more prime numbers, PR1 and PR2. The next step of the algorithm computes two 'N' values as N1 and N2. Four prime numbers are multiplied and computed as N1. For N2computation, it uses two prime numbers. This is done to increase the complexity of the encryption part. The third step of stage 1 calculates the Euler Totient value of r. The public key E is chosen so that the GCD of E and the Euler Totient value of r equals 1. The final step of stage 1 computes the private key D. Stage 2: This stage converts plaintext to cipher text. This process uses the Public key E andN1 values, where N1 is a product of four prime numbers. Thus the cipher text C is generated after the completion of Stage 2.Stage 3: In stage 3, the original plain text is retrieved using the values of cipher text and decryption keys D and N2.N2 is computed using only two prime numbers. The calculated N1 value is used for the encryption process as public key pair (E, N1). The private key pair composed of D and N2 is used for decryption. The proposed work still enhances the speed of encryption and decryption processes by dividing the files into blocks that are to be encrypted.

N. Jahan et al. [38] proposed a system that can humiliate the discovery of the key for dispensing a file that guarantees security by dispensingan asymmetric key and sharing it in the cloud environment. Users do the integrity check themselves instead of using third-party services' compression or hash functions. Upon receipt of the data by the user, each hash is compared to other hash values to verify differences in the data. The encryption and decryption time is computed and compared with the previous document, and experience shows that our calculation took about 80% less time. In this method, the keys are used and distributed using a modified Diffie-Hellman distribution scheme for encrypting and decrypting the data. The data is gathered in the cloud safely. Here, a cryptographic compression function is used to check data integrity. The public key cryptographic system and cryptographic compression function are both one-way functions. The compression function is also known as the Hash function. Hashing converts an input of any length into a fixed-sizestring or text using a mathematical function. This means any text can be converted into numbers or letters through an algorithm, no matter how long it is. The message to be minced is referred to as input. The algorithm used to do so is called the hash function, and the output is called a hash value. Many formulas can be used to hash a message, but acryptographic hash function needs some qualities to be considered useful. Each hash value on output has to be unique. This means that it should be impossible to produce the same hash value by entering different entries; as a result, the same message will always produce the same hash value. The hash speed is also an important factor. The hash function should quickly produce the hash value. Cryptographic compression or hash is used in data or user verifications and authentication. A strong cryptographic compression function is very difficult to contrary the result of the compression and reproduces the original file or data. Cryptographic compression or hash functions represent large quantities of data with a signal ID. To access entry-level control, the users check the integrity using the hash function rather than any third party.

Adee, R. et al. [39] proposed a four-step data security model based on Rivest–Shamir–Adleman, Advanced Encryption Standard, and identity-based encryption algorithms alongside Least Significant Bit steganography. The four stepsare data protection and security through encryption algorithms, steganography, data backup and recovery, and data sharing. This proposed approach ensures more cloud data redundancy, flexibility, efficiency, and security by protecting data confidentiality, privacy, and integrity from attackers[40].

VI. FINDINGS AND INTERPRETATION

Cloud makes users feel compatible in keeping their data, but it has many security-related vulnerabilities. Different published articles related to addressing the security challenges in the cloud are considered for the survey. The survey analysis of various security techniques shows that the symmetric techniques are used more and show less time consumption since it uses a single key for encryption and decryption. Therefore, the speed level of symmetric algorithms seems to be better than the asymmetric algorithm. Compared to security, the RSA algorithm shows a high level of security since it uses the factoring of a high prime number for key formation. The survey shows that AES and DES algorithms show less encryption/decryption time, whereas RSA shows the

longest encryption/decryption time. Table 1 shows the comparison security techniques consider for the survey with different parameters as shown in the table. The table shows that most techniques are symmetric and block cipher encryption.

Moreover, most of the techniques use substitution and permutation operations to make confusion and diffusion to the cryptanalyst. The techniques are categorised into two encryption and obfuscation. Comparing the two approaches, obfuscation approaches take low computation time than encryption. However, the data may be hacked from the cloud administrator's side, known as an insider attack. Therefore, most of the proposed security techniques are encrypted the data on the client side to avoid this attack. One or two techniques proposed are hybrid, which may increase the security but slower the encryption and decryption time. The hybrid approaches are shown the computation time as high. Not all block ciphers use the Feistel structure.

Further, most of the proposed algorithms are processed non-numerical and numerical data. Obfuscation approaches only consider the numerical data. In the cloud environment, data may be in transit or at rest. The asymmetric cryptosystem may be useful for data in small sizes, such as passwords, keys, etc. because it provides high security but takes more time. It is not advisable to use asymmetric cryptosystems for large sizes of data. Symmetric cryptosystems are better suited for data stored in the cloud environment. Symmetric encryption is a block cipher that can encrypt and decrypt large volumes of data in less time than asymmetric encryption. Therefore, securing the data stored in the cloud is more suitable when using the symmetric cryptosystem. Further, the researchers should concentrate on the symmetric cryptosystem and enhance its procedure to improve the strength of the security. Table 1 shows the comparison of different literatures with respect to necessary parameters.

Table 2. Comparison of Literatures

Techniques	Type of Operation	Keys Used	Data Proc essed	Types of data	Approaches	Encryption at	Feistel Structure	Computation Time
[16]	Substitution & Permutation	Symmetric	Block	Non-Numerical	Encryption	Client Side	No	Medium
[17]	Substitution	Symmetric	Block	Numerical	Obfuscation	Client Side	No	Low
[18]	Substitution	Symmetric	Block	Numerical	Obfuscation	Client Side	No	Low
[19]	Substitution	Symmetric	Block	Both	Encryption	Server Side	No	Medium
[20]	Substitution & Permutation	Symmetric	Block	Both	Encryption	Server Side	No	Low
[21]	Substitution	Symmetric	Block	Both	Encryption	Client Side	No	Medium
[22]	Subst	Sym	Block	Num	Obfus	Client	No	Low

	itution	metric		erical	cation	Side		
[23]	Substitution	Symmetric	Block	Numerical	Obfuscation	Client Side	No	Low
[24]	Substitution & Permutation	Symmetric	Block	Both	Encryption	Client Side	No	Medium
[25]	Substitution & Permutation	Symmetric	Block	Both	Encryption	Server Side	No	Medium
[26]	Substitution	Symmetric	Block	Non-Numerical	Encryption	Client Side	No	Medium
[27]	Substitution	Symmetric	Block	Numerical	Obfuscation	Client Side	No	Low
[28]	Substitution & Permutation	Symmetric	Block	Both	Encryption	Client Side	No	Low
[29]	Substitution	Symmetric	Block	Both	Encryption	Client Side	No	Medium
[30]	Substitution	Symmetric & Asymmetric	Block	Both	Encryption	Server Side	Yes	High
[31]	Substitution & Permutation	Symmetric & Asymmetric	Block	Both	Encryption	Server Side	Yes	High
[32]	Substitution	Asymmetric	Block	Both	Encryption	Server Side	No	High
[34]	Substitution & Permutation	Symmetric & Asymmetric	Block	Both	Encryption	Server Side	Yes	High
[35]	Substitution	Asymmetric	Block	Both	Encryption	Server Side	No	High
[36]	Substitution	Asymmetric	Block	Both	Encryption	Server Side	No	High

[37]	Substitution & Permutation	Symmetric & Asymmetric	Block	Both	Encryption	Server Side	Yes	High

CONCLUSION

Cloud is more important in storing and maintaining the data in its servers. Data security is a major concern when the cloud keeps the data. No proper guidance describes that the data are secured from cloud storage. There are many other researchers have come out with their explanations and results. This paper surveyed the already developed security techniques pointed out in today's scenario. The survey presented the nature of cryptography techniques for addressing and ensuring the confidentiality of the data stored in the cloud. Many articles are considered for the survey. A comparison of each technique with different parameters is given. Finally, the finding and interpretation of this paper are given to suggest where and which technique can be more useful and malleable for cloud data security. The paper also suggests which technique can be further enhanced to improve data security in the cloud.

REFERENCES

[1] Felix Bentil, Isaac Lartey, Cloud Cryptography - A Security Aspect, International Journal of Engineering Research & Technology (IJERT), Vol. 10 Issue 05, May-2021, pp. 448-450.

[2] Sarkar, S.; Choudhary, G.;Shandilya, S.K.; Hussain, A.; Kim, H.Security of Zero Trust Networks inCloud Computing: A ComparativeReview. Sustainability, 14, 11213, 2022, pp. 1-21.

[3] Miss Ruchira Gajanan Mankar,Prof. Prashant P. Patil Cloud Computing – Cryptography, Journal of Emerging Technologies and Innovative Research (JETIR), Volume 8, Issue 7, 2021, pp.231-234.

[4] Prof.S.S Dhule1, Durga Nehare2, Komal Ballewar3, Punam Bangade4, Riddhi Raut5, Mamta Sidam6, Punam Pawar, Implementation of Cryptographic Algorithm for Cloud Data Security, International Journal of Aquatic Science, Vol 12, Issue 02, 2021, pp.5359-5364.

[5] G R Tsochev1, R I Trifonov1, Cloud computing security requirements: A Review, IOP Conf. Series: Materials Science and Engineering 1216 (2022) 012001, pp.1-8.

[6] Arockiam, L., S. Monikandan, and G. Parthasarathy. "Cloud computing: A survey." Journal of Computer and Communication Technology: Vol 8.1 (2017): 4, pp. 21-28.

[7] Holger Schulze, 2022 CLOUD SECURITY REPORT, Fortinet, Cybersecurity Insiders, 2022, pp. 1-27.

[8] Mohammad Anwar Hossain, Ahsan Ullah, Newaz Ibrahim Khan, Md FerozAlam, Design and Development of a Novel Symmetric Algorithm for Enhancing Data Security in Cloud Computing, Journal of Information Security, Volume 10, 2019, 199-236.

[9] Smita Sharma, R.P. Singh, The Cryptography Based Security Algorithm For Protecting Sensitive Information in Cloud Environment, International Journal Of Scientific & Technology Research, Volume 8, Issue 11, November 2019, pp. 2281-2287.

[10] Da Rocha, M., Valadares, D., Perkusich, A., Gorgonio, K., and Will, N., Secure Cloud Storage with Client-side Encryption using a Trusted Execution Environment, In Proceedings of the 10th International Conference on Cloud Computing and Services Science, 2020, pp. 31-43.

[11] Manikandasaran, S. S., and L. Arockiam. "Security Attacks and Cryptography Solutions for Data Stored in Public Cloud Storage." IRACST-International Journal of Computer Science and Information Technology & Security (IJCSITS), ISSN 2249 (2016): 9555, pp. 498-503.

[12] Akashdeep Bhardwaj, G.V.B. Subrahmanyam, Vinay Avasthi, Hanumat Sastry, Security Algorithms for Cloud Computing, Elsevier

Procedia Computer Science, Volume 85, 2016, pp. 535-542

[13] Arockiam, L., and S. Monikandan. "Data security and privacy in cloud storage using hybrid symmetric encryption algorithm." *International Journal of Advanced Research in Computer and Communication Engineering* 2.8 (2013): 3064-3070.

[14] Tim Mather, Subra Kumaraswamy, and Shahed Latif "Cloud Security and Privacy", O"Reilly Media, Inc, pp 61-71, 2009.

[15] SvetlinNakov,Practical Cryptography for Developers, ISBN: 978-619-00-0870-5, 2018.

[16] Tim Mather, Subra Kumaraswamy, and Shahed Latif, "CloudSecurity and Privacy", O"Reilly Media, Inc, pp 61-71, 2009.

[17] Zaid Kartit, Ali Azougaghe, H. Kamal Idrissi, M. El Marraki, M. Hedabou, M. Belkasmi and A. Kartit, Applying Encryption Algorithm for Data Security in Cloud Storage, Springer, The International Symposium on Ubiquitous Networking, LNEE 366, 2016, pp.141-154.

[18] Arockiam, L., and S. Monikandan. "AROcrypt: A confidentiality technique for securing enterprise's data in cloud." Int J Eng Tech 7.1 (2015): 245-253.

[19] Manikandasaran, S. S., Lawrence Arockiam, and PD Sheba KeziaMalarchelvi. "MONcrypt: a technique to ensure the confidentiality of outsourced data in cloud storage." International Journal of Information and Computer Security 11.1 (2019): 1-16.

[20] Balamurugan, S., S. Sathyanarayana, and S. S. Manikandasaran. "ESSAO: Enhanced security service algorithm using data obfuscation technique to protect data in public cloud storage." Indian Journal of Science and Technology 9.17 (2016): 1-6.

[21] Veeraragavan, N., L. Arockiam, and S. S. Manikandasaran. "Enhanced encryption algorithm (EEA) for protecting users' credentials in public cloud." 2017 International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET). IEEE, 2017, pp. 1-6.

[22] Kalaichelvi, R., and S. S. Manikandasaran. "ENAES CCSA to preserve confidentiality of outsourced data in public cloud." *2017 International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET)*. IEEE, 2017. pp. 1-6.

[23] K. Balaji, Manikandasaran S S, ESCET: Enhanced Symmetric Convergent Encryption Technique To Provide Secured Deduplicated Data In Public Cloud Storage, Webology,Volume 18, Number 6, 2021, pp. 5811-5825.

[24] S. Arul Oli and L. Arockiam, "Confidentiality Technique for Data Stored in Public Cloud Storage", International Journal of Engineering Research and Technology (IJERT), Vol. 5, Issue 2, February 2016, ISSN: 2278-0181, pp. 44-48.

[25] S. Arul Oli and L. Arockiam, "Enhanced Obfuscation Technique for Data Confidentiality in Public Cloud Storage", In Proceedings of International Conference on Mechanical Engineering and Electrical Systems (ICMES 2015 at NTU Singapore), MATEC Web of Conferences, Vol. 40, No. 09003, , January 2016, pp.1-5.

[26] Ramalingam Sugumar and Sharmila Banu Sheik Imam, Symmetric Encryption Algorithm to Secure Outsourced Data in Public Cloud Storage, Indian Journal of Science and Technology, Vol 8(23), IPL0284, September 2015, pp. 1-5.

[27] S. Balamurugan, Dr. Sanjay Pande, Symmetric Cryptosystem to Enhance Data Security in Public Cloud Storage, International Journal of Applied Engineering Research ISSN 0973-4562 Volume 10, Number 16 (2015) pp 37515-37522.

[28] L. P. George, D. I. George Amalarethinam and A. S. Chandran, "GLEnc Algorithm to Secure Data in Public Cloud Environment," IEEE International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2018, pp. 2018-2022.

[29] Amalarethinam, George & George, Lalu. (2020). GLObfus: An Enhanced Data Security Method to Protect Numerical Data in Public Cloud Storage. International Journal of Computer Theory and

Engineering. Vol. 12, No. 5, October 2020, pp. 113-117.

[30] Dr. D.I. George Amalarethinam , J. Madhu Priya, MAGcipher: An Enhanced Cryptography Encryption for securing the Data in Hybrid Cloud, International Journal of Advanced Science and Technology, Vol. 29, No. 5s, (2020), pp. 585-590.

[31] A. Fairosebanu1, Dr. A. Nisha Jebaseeli, Enhanced Symmetric Encryption Technique for Securing Users' Data in Public cloud Environment, IJCSNS International Journal of Computer Science and Network Security, VOL.22 No.4, April 2022, pp. 785-791.

[32] S. Kaushik and A. Patel, "Secure Cloud Data Using Hybrid Cryptographic Scheme," 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), 2019, pp. 1-6.

[33] Hossein Abroshan, A Hybrid Encryption Solution to Improve Cloud Computing Security using Symmetric and Asymmetric Cryptography Algorithms, International Journal of Advanced Computer Science and Applications,Vol. 12, No. 6, 2021, pp. 31-37.

[34] Quisi-Aphetsi Kester, Laurent Nana, Anca Christine Paseu, A New Hybrid Asymmetric Key-exchange and Visual Cryptographic Algorithm for Securing Digital Images, IEEE International Conference on Adaptive Science and Technology, 2013, pp. 1-5.

[35] Ghassan Sabeeh Mahmood, Dong Jun Huang, and Baidaa Abdulrahman Jaleel, A Secure Cloud Computing System by Using Encryption and Access Control Model, Journal of Information Processing System, Vol.15, No.3, June 2019, pp. 538-549.

[36] V. P. Bansal and S. Singh, "A hybrid data encryption technique using RSA and Blowfish for cloud computing on FPGAs," 2015 2nd International Conference on Recent Advances in Engineering & Computational Sciences (RAECS), 2015, pp. 1-5.

[37] I. G. Amalarethinam and H. M. Leena, "Enhanced RSA Algorithm with Varying Key Sizes for Data Security in Cloud," 2017 World Congress on Computing and Communication Technologies (WCCCT), 2017, pp. 172-175.

[38] N. Jahan and M. A. Mahmood, "Securely Distributing Files in Cloud Environment by Dispensing Asymmetric Key Management System applying Hashing," 2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS), 2021, pp. 1105-1110.

[39] Adee, R.; Mouratidis, H. ADynamic Four-Step Data SecurityModel for Data in Cloud ComputingBased on Cryptography andSteganography. Sensors 2022, 22, 1109, pp. 1-23.

[40] M.Sowmiya, S.Prabavathi, Symmetric and Asymmetric Encryption Algorithms in Cryptography, International Journal of Recent Technology and Engineering (IJRTE), Volume-8 Issue-1S2, May 2019, pp. 335-357.