International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT217250

A Review of Encryption Techniques Used in Cloud Computing

Parth Tandel*, Abhinav Shubhrant, Mayank Sohani
Mukesh Patel School of Technology Management and Engineering, Shirpur, Maharashtra, India

ABSTRACT

We can say that we are surrounded by the computing world from every nook and corner. Cloud Computing is deemed as the most fundamentally changing phenomenon happening in Information Technology. But with great perks, comes great challenges as well, especially in the field of data security and privacy protection. The Cloud Service Providers take over chunks of private data from users for providing better functionalities. But for the sake of privacy and protection, this sensitive data should be encrypted and then outsourced to the cloud consoles.

Since traditional cloud computing is performed on plaintext, many encryption algorithms were applied in the cloud for security purposes and 'encrypted' data was stored in the cloud from then on. This change gives fruition to a new type of encryption technique called Homomorphic Encryption. Primarily, the paper will focus on a subtype of Homomorphic Encryption called Fully Homomorphic Encryption. The objective of the paper is to propose a method to convert the sequentially processing Fully Homomorphic Encryption into parallel processing Fully Homomorphic Encryption using a Parallel Computing concept called Partitioning and thereby producing a better performing Fully Homomorphic Encryption.

Keywords : Cloud Computing, Encryption, Homomorphic Encryption, Fully Homomorphic Encryption, Parallel Computing, Parallel Processing, Partitioning.

Article Info
Volume 7, Issue 2
Page Number: 231-243

Publication Issue :
March-April-2021

Article History
Accepted : 05 April 2021
Published : 11 April 2021

I. INTRODUCTION

Cloud Computing is a technology which lets smooth, voluntary (on-request) network access to shareable and configurable computing resources and data that can be provisioned, manipulated and delivered with the least amount of administration or cloud service provider's involvement. Before getting into the security concerns, let us take a look at the three major services and benefits of Cloud Computing [1].

Software as a Service (SaaS) - It is called SaaS that

distributes a software operated by third party companies, thus allowing users to access the software over the network. For instance, if a student needs office software like MS PowerPoint for a specific period, he / she does not have to purchase the whole product, rather he / she only has to pay for the software resources needed by the buyer. Example – Dropbox and Google Workspace.

Platform as a Service (PaaS) – In traditional terms, PaaS literally paves the way or offers software developers a forum to create their goods or services over the Internet or a network. For example, if a developer now uses MacOS and needs to operate in a Windows environment, then that platform is provided by CSP. Example – Microsoft Azure, GAE (Google App Engine) and AWS Elastic Beanstalk.

Infrastructure as a Service (IaaS) – This service facilitates virtual storage for the users. The data is actually stored in the Cloud Service Provider's servers. Since the corporate world is consuming a lot of data today, IaaS's use has increased extensively. Example – GCP (Google Cloud Platform/Google Compute Engine), Microsoft Azure and AWS (Amazon Web Services) [1].

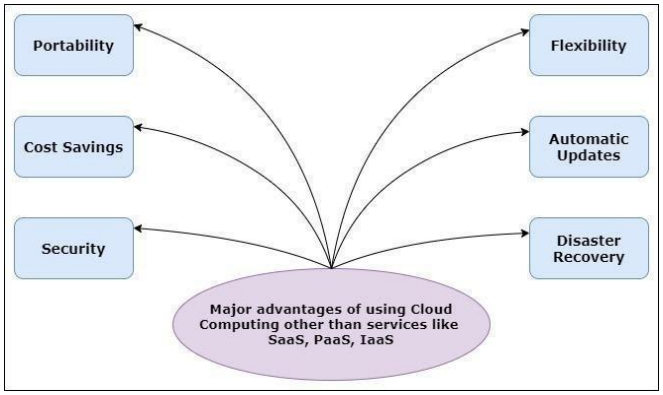

Fig. 1. Various advantages of using Cloud computing other than SaaS, PaaS, IaaS

The major deal breaker when it comes to using a technology like Cloud Computing is Security. That is, the potential data breach by third-party vendors while putting sensitive data on the cloud. The repercussions of not having secured data: A chance of attack on the data either by simple manipulations or the whole chunk of data may be compromised [1].
Some other vital controls that harms Cloud Security w.r.t. compliance standards are given below [2]:

- Encryption of data and key administration
- Security of the media
- Recognize, authenticate and approve
- Virtualization and Resource Abstraction
- Interoperability and portability
- Security programme
- Identifying and managing security threats
- Anonymity, e-discovery and ethics
- Planning of emergencies
- Operations and maintenance of the Data Center
- Answer incident
- Enforcement, Transparency and Audit
- Awareness and Training

To remedy these issues, an obvious solution of cryptography was introduced to the cloud. Simply stating, Cryptography is the art of hiding any kind of information or data and keeping it secure and limited to approved eyes only. To successfully pull Cryptography, two techniques play a major role in it. Encryption converts different formats of data into unreadable format called ciphertext. Decryption is the other side of the coin which converts that ciphertext into original plain text [1].

II. REVIEW OF LITERATURE

2.1 Hybrid Homomorphic Encryption Scheme

The partial homomorphic encryption systems can only be supported by property homomorphic. In the meantime, all the properties of homomorphic encryption systems will help. To create a completely new scheme of homomorphic encryption, one supports multiplication and other supports addition

operations only, supports all operations from two partial homomorphic encryption schemes. The algebraic architecture must be maintained in the hybrid homomorphic encryption method [3].

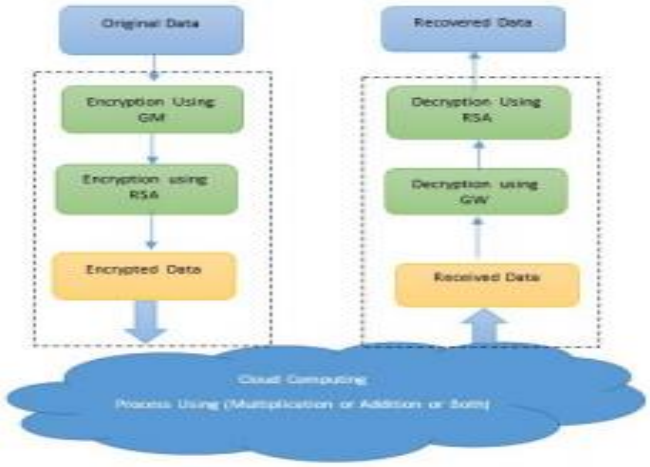

Fig. 2. Method Hybrid Homomorphic Encryption scheme [3].

2.2 Modified RSA algorithm to achieve FHE

The addition algorithm not only multiplication aspect characteristic, but it also contains the adding characteristic for complete homomorphic encryption, in that the new algorithm completely adapts to the homomorphic cloud computing encryption algorithm. In the RSA encryption method, the plaintext string is first of all treated as an extremely high number, while the symmetric encryption uses a number sequence in the mathematical field in order to accomplish the purpose of encryption by using a sequence of modular arithmetics[4].

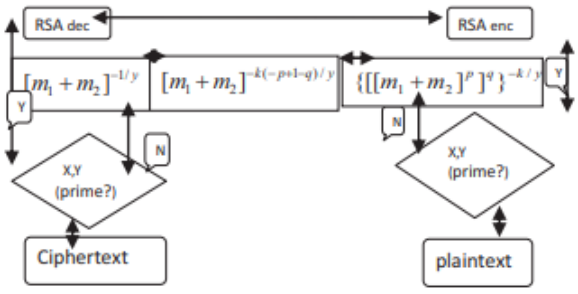

Fig. 3. Flow of the processes of Modified RSA algorithm[4].

Then, during encryption, the value of the private key & public key created contains the prime integer; combines it with the Pascal's theorem of triangle and the model of the RSA Algorithm and inductive methodology for creating a new crypto-system that estimates the homomorphic calculation of several ciphertext operation(e.g., additions, multiplications)[4].

2.3 Secured way of Parallel Processing on Cloud Data using Fully Homomorphic Encryption

Security in the cloud is subject to several techniques. User data may often be lost to storage in the cloud. The data partitioning approach is presented for user's data protection purposes. The method of partitioning data provides user data on the cloud with improved protection. The data of this user is initially divided into several sections based on size (with the same shorts), stored on different cloud servers after partitioning of the data of the user (text file), as well as created public keys for saving and retrieving data. This approach provides user data with greater protection[5].

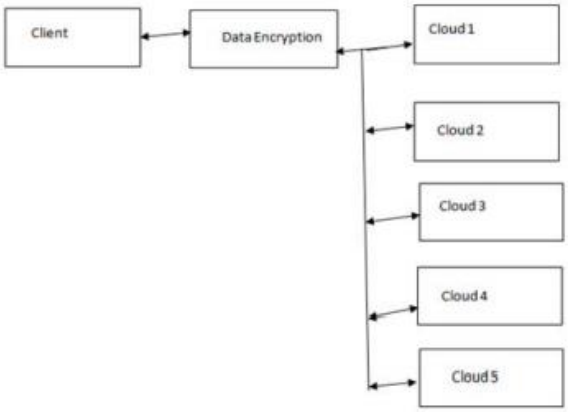

Fig. 4. Data Partition method block diagram[5].

This simultaneous treatment results in better performance. In cloud related computing, security of data is also a big problem in today's world. It also highlights another work using the Data Partitioning Approach to enhance client data protection in the

cloud. Client data is split on various servers into several chunks of the same size and store. And it creates attention on the side of the customer; to obtain and store data in the cloud the public key is used. The Gentry's algorithm is used to achieve FHE[5].

Improving the time taken in processing ultimately means processing Fully Homomorphic Encryption simultaneously reduces the time taken in processing of the encrypted data in cloud activity. The partitioning of data approach gives the user data on the cloud more stability. This process creates a public key; and then used in the storage of cloud data. Data for customers is divided into several pieces of chunks of the same size. Each portion is stored on various servers. The approved user should enter a public key when downloading the data from the cloud. The data confidentiality is shown by this process[5].

2.4 Hybrid Homomorphic Encryption

A machine was created for an encryption/decryption programme that is running in a private cloud. EDM provides schemes for encryption and decoding, manages the Paillier and RSA algorithms, and converts basic text calculation operations to instructions on the ciphertext calculation. The arrangement is listed below, assuming it works in all the right settings[6].

[1] The EDM produces P-PK, P-SK, P-SK, RSA public key R-PK, R-SK private key and the Paillier public key. Then the EDM will upload the keys to the server of the public cloud.

[2] Customers apply the private cloud server calculation requests. The server analyses and breaks down customer requests to operations and operations.

[3] The Pailliers are encrypted using P-PK to process the encryption based on the kind of the operation, add and sub operand, multiplication and division operand by RSA using R-PK. The RSA operand is encrypted. The EDM then moves the add and sub plain text to the multiplication and division method of the ciphertext text.

[4] The private cloud uploads the data to the cloud server and processes the calculations without understanding the basic texts and processes.

[5] The private cloud gets data, analyses and categorises data by the form of activity from the public cloud. The EDM would then decode the add-on and sub-results with P-SK, multiply and divide with R-SK.

[6] Customers receive the results of their private cloud server calculation requests[6].

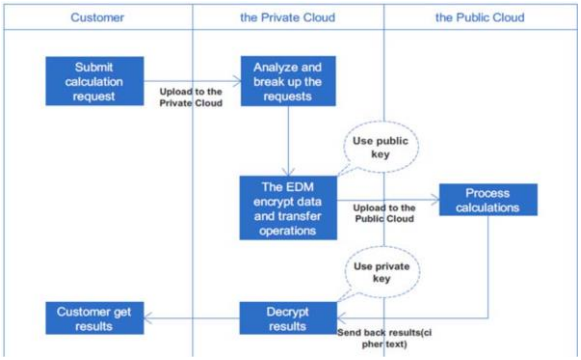

Fig. 5. Hybrid cloud computing scheme[6].

OThe test results indicate that the homomorphic device is capable of producing key, encrypt, process and effectively decode results for sizes 512, 1024, and 2048 and text of less than 64k in duration. The homomorphic framework operates with a slightly long processing time for the text of length 64 KB or the size 4096, but the text of size less than 64 KB. The homomorphic device can no longer handle these operations for the key size 4096 and for the text length 64 KB. The length of the text shall not impact the period of key generation and decryption[6].

2.5 Analysis of various encryption algorithms : DES, 3DES, AES, RSA and Blowfish

The chosen approach is basically dependent on the application requirements such as time of response,

bandwidth, confidentiality and credibility. However, the limitations and strengths of each cryptographic algorithm. We are presenting the results of the implementation and study of several encryption algorithms in this article[7].

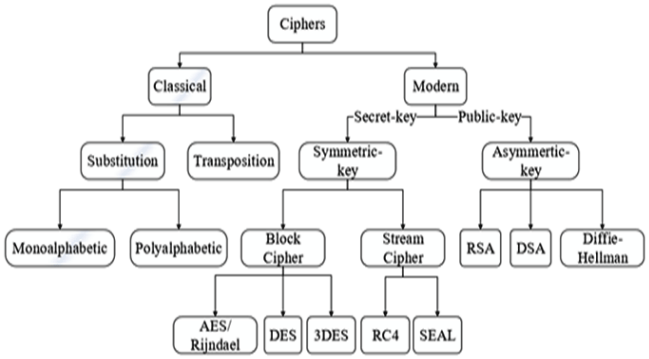

Fig. 6. Classification of various encryption methods[7].

AES (Advanced Encryption Standard) [8]:

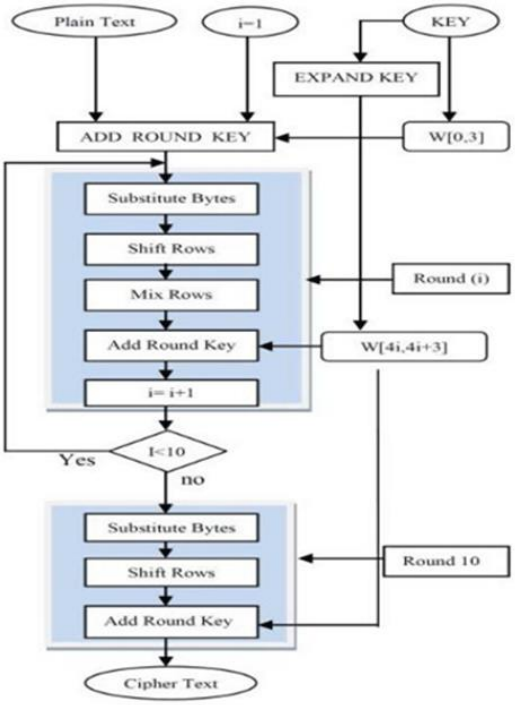

Fig 6(a). Work flow of AES[8].

DES (Data Encryption Standard) :

Block's size is 64 bit length and key length is 56 bits. If a weak key is used, it is prone to key attack. The NSA started with a 64-bit key and then restricted DES with a 56-bit key length. DES discards 8-bit of a 64-bit key, and then uses the compressed 56-bit drive key to encrypt 64bit data , making it versatile in various modes[7].

RSA (Rivest-Shamir-Adleman) [7]:

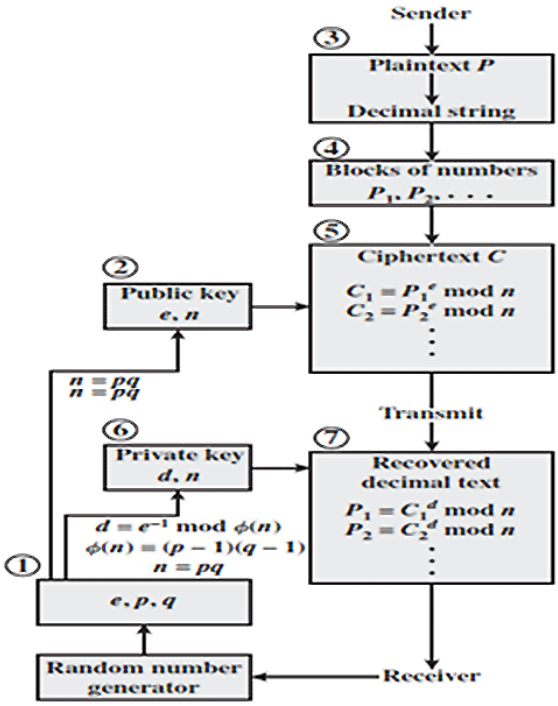

Figure 6(b). Work flow of RSA[7].

Blowfish :

It has a feistel network structure. Blowfish is a symmetrical block chip which can be used as an informal DES or Concept substitute. It requires a 32-bit to 448-bit variable-length key and is suitable for both residential and industrial use. It was substantially analysed and is gaining popularity steadily as a robust coding algorithm. It has the issue of weak keys[9]. As individuals store their personal and important information in the clouds, it is important to safely store the data. For data protection such as AES, RSA and Blowfish, a variety of

algorithms exist[10]. We should take into account the use of Blowfish and AES algorithms to escape attack and can be implemented on top of all IPv4 and IPv6 related internet protocols[9].

AES can not be struck rather than by the Brute Force. But attack by the Brute Force isn't an easy task even for a great machine. The key size used by an AES algorithm is 128, 192 or 256 bits, resulting in trillions of permutations and combinations[10]. The AES selection process was based on high speed and low RAM specifications. So AES works well on a large range of hardware from 8-bit intelligent cards to high-performance computers. AES is also much quicker than conventional algorithms, which is why AES is taken on in our work[11].

2.6 Cloud Storage multi-authority access control with ABE

Data can usually be classified by its sensitivity into three groups. In order to maintain power of their data , the data owners select one type from three levels. CSP is the Cloud Computing Environment service provider. CSP encrypts the PRTP Date group. The PRNTP data is encrypted using the Access Authentication Method (AAS). The central authority issues consumers internationally[12].

- Privacy Not Required (PNR): Data owners believe the data is not vulnerable in this category and that protection does not require the data to be encrypted, but that data is transmitted via SSL to the network for a simple security reason[13].
- Privacy Required with Trusted Provider (PRTP): The data owner is skeptical about vulnerability and relies on the provider for decryption.
- Privacy Required with Non Trusted Provider (PRNTP): The data owner in this group believes that the data is particularly vulnerable and must be shielded from untrusted CSPs. As data owners don't believe in CSP, the data would be provided in order to encrypt and secure the security and integratedness of the data through Access Authentication Schemes (AASs)[13]. The data is also housed in cloud computing. AAS is an agency of a third party that works safely for all of its above activities. In order to ensure the protection of employees' records, AASs must provide new safety algorithms[12].

PRTP and PRNTP groups may be selected to have power over results. To secure the data, RHA, HAS and current FH-CPABE are used for encrypting in these data groups. For PRNTP data type, since AAS does not trust the data owner, the data is encrypted by the AAS using the proposed RHA, HAS and FH-CPABE. The data owner has little interest in CSP. A CSP is used in encrypting data for the PRTP data type because the data owner is confident in CSP. Crypting data using the RHA, HAS, and FH-CPABE suggested is achieved using CSP[12].

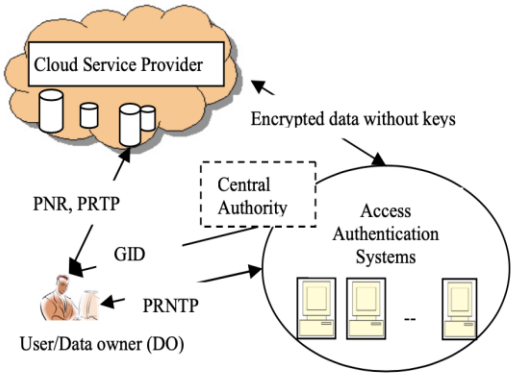

Fig. 7. Block Diagram[12].

Role Hierarchy Algorithm can be used for anonymity, data security, fine seed and multi-authority access control for user data in cloud storage to achieve hierarchy structure. Cloud storage The RHA algorithm is designed to create a user hierarchy depending on the attributes assigned. The develop hierarchy is used for the layout of the hierarchy of access to fine seeds. For hierarchical file encryption, HAS and the current FH-CPABE are used. Performance and protection are calculated with

respect to the time taken to encrypt and decode the proposed scheme. Compared to the current FH-CPABE, the proposed arrangements are effective , safe and achieve excellent access, and multi-authority access control by HAS[12].

2.7 Combination of RSA & AES Encryption Algorithm

A framework implemented with encryption strategies using the AES and RSA algorithms is to apply protection features, which uses an AES 128 bit hidden key and an RSA 1024 bit key. Uploading leads to the development of public keys in RSA ns and e, private key in RSA ds, and the hidden AES key. The user will need to save his / her private key and hidden AES key. The user will first be saved in a temporary directory as he / she attempts to upload the data to the cloud[14].

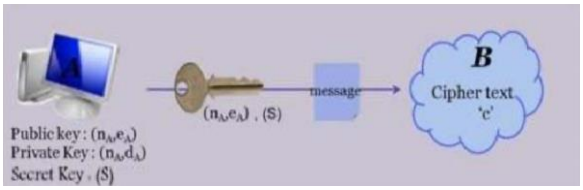

Fig. 8. Upload mechanism[14].

Now, when you are involved in accessing or storing data in the cloud, the name of the file should be user-defined to be accessible, and it should provide all the keys which are kept secret and only accessible to the user[14].

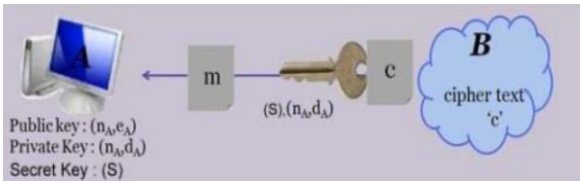

Fig. 9. Download mechanism[14].

Upload Module:

- Authentication: With the special username and password the user authenticates to the cloud.
- Upload: The user can retrieve its files in a safe manner with this module. The encrypted version of this data (file) is uploaded via this portal in his cloud document directory.
- Generating keys by considering time as a parameter.
- Data is first stored in the server temporary file in the cloud after uploading. Crypt the data using the user's public key and save the encrypted data type in user records. Then provisional files are unlinked[14].

Download Module:

- When a user decides to download his protected info, he is asked with the hidden private key to type his user name. The cloud decrypts the data using the user's private key.
- Download: In this way, Cloud can supply the customer with his original data to the Decrypted Data[14].

Results of the proposed scheme:

- The use of a hybrid encryption algorithm provides high security.
- There are RSA and AES keys so the private key is not expected from the public key.
- Hybrid encryption contributes to a high degree of text file protection which allows intruders nearly difficult to access original files.
- When a person signs out or leaves the machine idle. In that situation, a trespass user may be asked to access the private key if they want to retrieve the data from the device. In any case, if a test user calculates the private key and then attempts to download it will receive the information. The initial data won't be received.
- The user must always enter the keys for a safe download of the data, since the cloud administrator doesn't know the keys. The principal benefit of the framework is that the customer data can not even be reached by the

cloud administrator. In the event that the data is attempted, the encrypted version will be shown[14].

2.8 3-way security mechanism using Digital Signature, Diffie Hellman Key Exchange and AES.

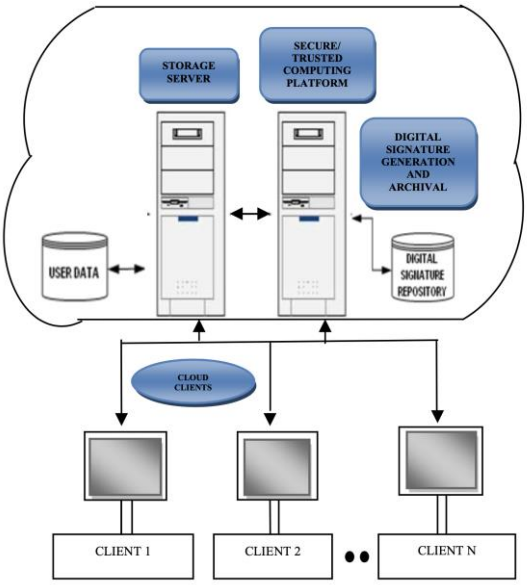

Fig. 10. Discussed Architecture[15].

In this architecture, a three-way security mechanism is used. First of all, Diffie Hellman's algorithm is used for key exchange generations. After that, the authentication digital signing algorithm is used to encrypt or decrypt the data file of the consumer. All this is achieved to provide a storage system that is trustworthy in order to deter server end data modifications. There are two independent repositories, one for an encryption method that is known as a (trustworthy) computing network, and one for the storing of user data files[15].

When the user needs to upload a file on the cloud server, the client first swaps keys using the Diffie Hellman key exchange when signing in. Use the AES to encrypt the user's data file, and only just transfer to a (cloud) storage server. If the recipient now needs to import the same file from the cloud server. In this case , users first have to share the encryption keys, pick the downloaded file, authenticate with the digital signature, use the AES method for decrypting the stored file, and the client may access the file. AES is then used for decrypting[15].

2.9 A different approach to Encryption/Decryption

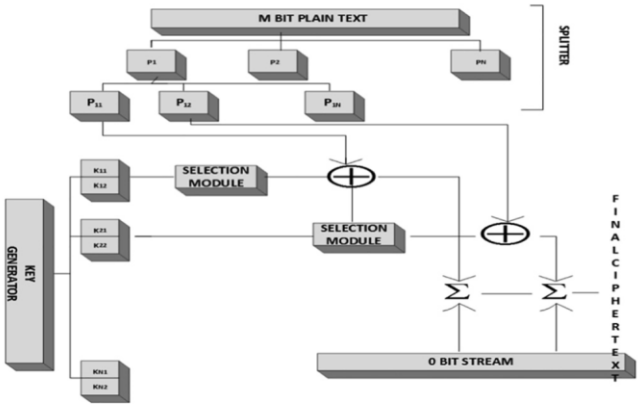

Fig. 11. Block Diagram[17].

The 'm' byte text is separated into 128-bit blocks in this encryption method. This is further divided by the splitter into 16-bit blocks. The key generator produces two random 128-bit keys and is divided into 16-bit blocks. The first 16 bits of the keys are EXOR and the matching MSB bit key fits the basic MSB text block and if it is the same, the first key is chosen, or the next key from the module of selection is chosen. The cypher from the first EXOR function will be used to pick the EXOR key for the next block, which will then be matched with EXOR for key selection with the random key. EXOR, with plain text, is the key selected and the mechanism proceeds to encrypt the entire 'm' bit. The key generator produces separate keys for each 128-bit plaintext block. Finally, between the created cyphers and the0-bit stream an OR operation is performed to get the entire cypher text [16][17]. The two randomly generated keys and ciphertext is EXOR for decryption and the plain text is recoverable. An 8-bit selection of chosen keys with a number of random keys is introduced, and this 8-bit

selection can be used to pick the 16-bit from the 128-bit random keys[17].

The algorithm is evaluated using different algorithms with multiple parameters including time, size and the avalanche effect. The algorithm performs better than current algorithms in any of these parameters. The time taken to check on the encrypted is decreased by the algorithm by a substantial amount of time relative to the others[17].

Table 1. Analysis of various encryption algorithms and concepts used in Cloud Computing based on specific parameters.

Techniques and Algorithms	Encryption time	Decryption time	File size	Text size	Memory consumption	Additive and Multiplicative Properties	Key size	Operation time	Execu' time	Network Bandwidth	Entropy	Avalanche effect	Circuit calculation complexity and safety index	Storage, computation and comm' cost	Access control
DES [1][7][11][16]	✓		✓		✓				✓	✓					
3DES [1][7][16]	✓		✓		✓				✓	✓					
AES [1][7] [8][9][11][16]	✓		✓		✓				✓	✓	✓	✓		✓	
Blowfish [1] [7][9][16]	✓		✓		✓				✓	✓	✓	✓			
Multiple PHE oriented FHE [3]	✓	✓		✓											
Modified RSA [4]						✓									
Gentry's Algorithm with FHE [5]	✓	✓			✓										
Hybrid HE [6]				✓			✓	✓							
RSA [7][9][11][16]					✓				✓	✓	✓	✓			
MD5 [8]									✓					✓	
RSA+AES [10][14]							✓		✓						
Homomorphic Encryption[11][16] [18]	✓	✓											✓		
MAAC using ABE[12]	✓	✓			✓										✓
RSA+IDEA[13]	✓														
Digital Signature with Diffie Hellman Key Exchange & AES [15]															✓
Proposed Key Generation and Encryption Phase using XOR bitwise operations [17]	✓											✓			
ABE [19][20]	✓														✓

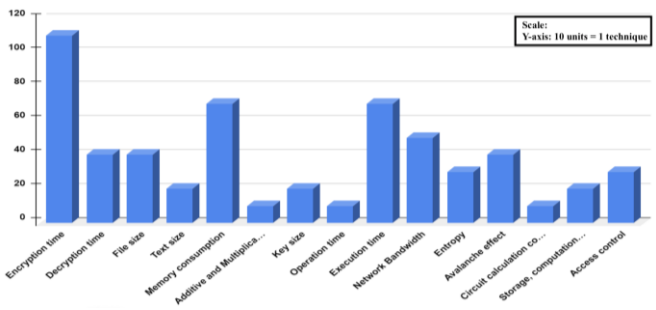

Fig. 12. Proportion of various parameters used in cloud encryption techniques

2.10 Parallel Processing and Partitioning.

FHE carries out cloud data (Fully homomorphic encryption) on one or more nodes and hence acquiring comparatively more time memory to compute than the one operation performed in simple text (unencrypted data). One of the obvious approaches to solve this issue would be Parallel Processing. It reduces processing time in cloud computing by imposing parallelism on encrypted data. As the name implies, parallel processing allows several nodes to work concurrently, so that the desired operation takes comparatively less time than the sequential process. Hence this approach will increase the performance of the traditional FHE [5].

Let's speak about some parallel processing approaches. Conversion of a sequential algorithm to a parallel algorithm is one approach. If the problem already has a sequential algorithm, the inherent parallelism in the algorithm can be identified. It is a kind of parallelism which naturally occurs within an algorithm without special effort or algorithm shift. However, it is not fruitful or effective to use inherent parallelism in a sequential algorithm. A Parallel Algorithm to solve a similar but distinct problem is a safer and more successful solution for some problems. Another solution is the conception and substitution of a brand new parallel algorithm with the current algorithm.

Parallel Programming (Multiprocessors)
Process Creation
Synchronization
Lock and Unlock
Wait and Signal (Increment and Decrement)
Fetch and Add
Barrier
Deadlock

Parallel Computation
Partitioning
Assignment or Scheduling

Table 2. Tabular Representation of Parallel Programming Concepts

Also, the approach of Parallel processing can be used for Data partitioning method which tackles the security drawback of FHE. Client data can be separated into several sections of similarly sized chunks and stored on various servers. A public key is created on the client side to store and retrieve originally cloud-divided data. This can be

accomplished by a parallel processing principle known as partitioning. The processing time is computed according to the time taken (on multiple nodes) to perform the operations applied simultaneously and to transmit the data. [5].

There are two methods of partitioning the task for parallel processing. They are : static partition and dynamic partition.

- Static Partitioning - The static partitioning technique separates tasks before execution and avoids conflict between processes. Input data then takes decisions including the exercise time and amount of data provided to systems, such as the amount of parallel calculation actually occurs. Therefore, during execution, certain processes cannot be kept working.
- Dynamic Partitioning - The dynamic partition approach divides up the tasks while running. As a consequence, systems are more busy and the input data isn't affected. The disadvantage is the amount of communication and coordination between processes that is required for implementation.

Another classification of partitioning is done on the basis of processes.

- Data Partitioning (Data Parallelism) – The processes can be generated in such a way that every process carries out the same operation on several sections of the data. This partitioning is also called homogeneous multitasking because it creates multiple mirror processes. This approach derives parallelism from problem data organisation. Every part will be processed simultaneously with the data structure divided into pieces of information. An individual data item or the set of items may be a bit of information. In solving mathematical problems that handle large arrays and vectors, data partitioning is especially helpful. It is also useful for non-numerical topics, such as combinatorial search and sorting algorithms. Data Partitioning is especially suitable for creating multicomputer algorithms since a processor primarily calculates using its own local data and rarely with different processors.
- Function Partitioning (Control/Function Parallelism) - Processes may be generated to perform a different data operation, which is called Function Partitioning. This partitioning is known as heterogeneous multi-tasking, just as data partitioning is known as multitasking in a homogeneous manner, as many separate processes carry out various data tasks.

Illustration of both the above discussed partitioning - Consider four vectors P, Q, S and T for the following computation.

$Y[n] = (P[n] / Q[n]) - (S[n] / T[n])$, for n=1 to 5

- Data Partitioning - Five identical processes are generated such that n is run by each process. Thus, the computation of each of the Y[n] using several similar processes simultaneously was carried out in parallel.
- Function Partitioning – A and B are two processes which are derived and then we compute $h = P[n] / Q[n]$ and send the value of h to B. B then calculates $f = S[n] / T[n]$ and inherits h from A for performing the calculation $Y[n] = h + f$. This is done for each index n. In this way, the functions of division are performed in parallel processing at the same time. This method typically organises the programme in such a way that the processes uses parallel processing while coding and not in the data.

Advantages of data partitioning over function partitioning:

1. More amount of parallel processing
2. Processes are given balanced/equal load
3. Subtle implementation

On the basis of Task Execution	On the basis of Process Creation
Static Partitioning	Data Partitioning
Dynamic Partitioning	Function Partitioning

Table 3. Classification of Partitioning

2.11 Potential development in Cloud Computing.

In cloud infrastructure, there are a lot of defence technology and encryption frameworks. A structure for growth, as shown in Figure 12, different policies / technologies may be used and the purpose of security and personal privacy protection easily achieved[19][20].

- Stable user security search technology. The mapping partnership is measured by the use of patterns to detect data security in order to provide real-time information on behavioural privacy, privacy of your identities and privacy of your location.
- Integrate unified confidentiality metrics. The span involves multi-source data fusion, user conduct and fine-tuned access management in the search process from the life cycle of cloud data. As these privacy protection technology has metrics for measurement, a multi-dimensional privacy protection evaluation framework, search accuracy and timeliness are needed [18].
- Cloud CPF technology for information fusion and intelligence extraction. Since Cloud data content is multidimensional and multi-granular, as well as because of the variety of analysis needs of users, the extraction of content is required to produce knowledge collections.
- Coordinate the relationship between trust and involvement of various stakeholders in the cloud. The involvement of various parties complicates the protection/privacy problem in cloud computing, when various parties' protection priorities can be somewhat different and sometimes conflicting [18].
- Cloud networking and big data. The input, analyses and output of the high-performance data stream in a short time is needed to be continuously processed in real time. An powerful and simple cryptographic something-ratio will reduce the cost of computation to ensure security and secrecy.
- Multiple integrated cloud computing. Since multiple cloud computing systems may be considered autonomous, they are compliant with these structures. The approach to address compatibility issues in various countries should be considered.
- Integration of different emerging paradigms of network infrastructure. Blockchain can be used for building the stable layer between cloud storage, fog computing and the internet. A stable, credible, and efficient infrastructure is transformed into cloud computing[18].
- Security of privacy on confident cloud systems. The security on a private computing network covers the whole life cycle of computing data processing.
- Mobile running systems, a single stable framework. Various cloud-based systems and equipment have common features and security concepts, allowing multi-party unification to minimise expense and increase performance.
- Related administration policies and legislation. Without the consent of citizens, cloud computing can sell information collected to a third party. Cloud infrastructure also requires new regulatory strategies by the government to balance priorities and privacy risks[19][20].

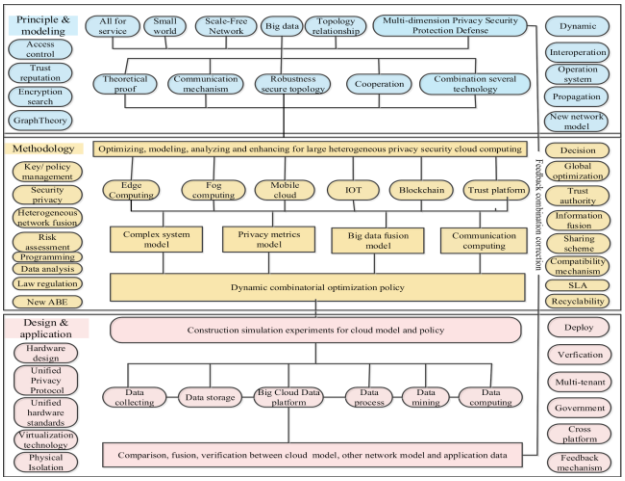

Fig. 13. Development of Cloud Computing [20].

III. CONCLUSION

In cloud computing, the power of computation and resources are much greater than just one computer where data calculations are carried out by computer clusters. The use of cloud storage to process large volumes of data is popular. For cloud computing, however, businesses are worried about data privacy. The privacy related problems in cloud related computing was described in this paper. Fully Homomorphic Encryption can be a resolution for solving data privacy in the cloud that processes information which is encrypted and returns the encrypted results. Beside so, generally Fully Homomorphic Encryption is slower and the faster schemes of Fully Homomorphic Encryption are needed to extend this way of processing things easily. We could practically implement partitioning methods with Fully homomorphic encryption as proposed in the third section. Also, we could implement other parallel programming concepts as. Lastly, we could also implement a whole new algorithm merged with FHE to achieve parallel processing. We could also implement algorithms with FHE with the sole purpose of tackling security issues and not the 'time and memory' drawback.

IV. REFERENCES

[1]. G. S. Vennela, N. V. Varun, N. Neelima, L. S. Priya and J. Yeswanth, "Performance Analysis of Cryptographic Algorithms for Cloud Security," 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT), Coimbatore, 2018, pp. 273-279, doi: 10.1109/ICICCT.2018.8473148.

[2]. A. Hendre and K. P. Joshi, "A Semantic Approach to Cloud Security and Compliance," 2015 IEEE 8thInternational Conference on Cloud Computing, New York, NY, 2015, pp. 1081-1084, doi:10.1109/CLOUD.2015.157.

[3]. Z. H. Mahmood and M. K. Ibrahem, "New Fully Homomorphic Encryption Scheme Based on Multistage Partial Homomorphic Encryption Applied in Cloud Computing," 2018 1st Annual International 8 Conference on Information and Sciences (AiCIS), Fallujah, Iraq, 2018, pp. 182-186, doi: 10.1109/AiCIS.2018.00043.

[4]. P. Sha and Z. Zhu, "The modification of RSA algorithm to adapt fully homomorphic encryption algorithm in cloud computing," 2016 4th International Conference on Cloud Computing and Intelligence Systems (CCIS), Beijing, 2016, pp. 388-392, doi: 10.1109/CCIS.2016.7790289.

[5]. R. S. Patil and P. Biradar, "Secure Parallel Processing on Encrypted Cloud Data Using Fully Homomorphic Encryption," 2018 4th International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), Mangalore, India, 2018, pp. 242-247, doi: 10.1109/iCATccT44854.2018.9001284.

[6]. X. Song and Y. Wang, "Homomorphic cloud computing scheme based on hybrid homomorphic encryption," 2017 3rd IEEE International Conference on Computer and Communications (ICCC), Chengdu, 2017, pp. 2450-2453, doi: 10.1109/CompComm.2017.8322975.

[7]. Nazeh Abdul Wahid MD, Ali A, Esparham B, Marwan MD (2018) A Comparison of Cryptographic Algorithms: DES, 3DES, AES, RSA

and Blowfish for Guessing Attacks Prevention. J Comp Sci Appl Inform Technol. 3(2): 1-7. DOI: 10.15226/2474-9257/3/2/00132.

[8]. Akashdeep Bhardwaj, G.V.B. Subrahmanyam, Vinay Avasthi, Hanumat Sastry, Security Algorithms for Cloud Computing, Procedia Computer Science, Volume 85, 2016, Pages 535-542, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2016.05.215.

[9]. Alrubaee, Saif. (2019). Security Algorithms in Cloud Computing- Review Paper. 10.13140/RG.2.2.27320.19200.

[10]. Kartit, Zaid & Azougaghe, Ali & Idrissi, H. & El marraki, Mohamed & Mustapha, Hedabou & Belkasmi, Mostafa & Ali, Kartit. (2016). Applying Encryption Algorithm for Data Security in Cloud Storage. 10.1007/978-981-287-990-5_12.

[11]. Nasarul Islam.K.V et al, International Journal of Computer Science and Mobile Computing, Vol.6 Issue.7, July- 2017, pg. 90-97, ISSN 2320–088X

[12]. Praveen S. Challagidad, Mahantesh N. Birje, Efficient Multi-authority Access Control using Attribute-based Encryption in Cloud Storage, Procedia Computer Science, Volume 167, 2020, Pages 840-849, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2020.03.423.

[13]. K. K. Chennam, L. Muddana and R. K. Aluvalu, "Performance analysis of various encryption algorithms for usage in multistage encryption for securing data in cloud," 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), Bangalore, 2017, pp. 2030-2033, doi: 10.1109/RTEICT.2017.8256955.

[14]. V. S. Mahalle and A. K. Shahade, "Enhancing the data security in Cloud by implementing hybrid (Rsa & Aes) encryption algorithm," 2014 International Conference on Power, Automation and Communication (INPAC), Amravati, 2014, pp. 146-149, doi: 10.1109/INPAC.2014.6981152.

[15]. P. Rewagad and Y. Pawar, "Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing," 2013 International Conference on Communication Systems and Network Technologies, Gwalior, 2013, pp. 437-439, doi: 10.1109/CSNT.2013.97.

[16]. Pansotra, Er & Singh, Simar Preet. (2015). Cloud Security Algorithms. International Journal of Security and Its Applications. 9. 353-360. 10.14257/ijsia.2015.9.10.32.

[17]. D. K. Shukla, V. K. R. Dwivedi and M. C. Trivedi, Encryption algorithm in cloud computing, Materials Today: Proceedings, https:// doi.org/10.1016/j.matpr.2020.07.452

[18]. Min Zhao E, Yang Geng, Homomorphic Encryption Technology for Cloud Computing, Procedia Computer Science, Volume 154, 2019, Pages 73-83, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2019.06.012.

[19]. P.P., Kumar, P.S., Alphonse, P.J.A., Attribute based encryption in cloud computing: A survey, gap analysis, and future directions, Journal of Network and Computer Applications (2018), doi: 10.1016/j.jnca.2018.02.009.

[20]. PanJun Sun, “Security and privacy protection in cloud computing: Discussions and challenges,” Journal of Network and Computer Applications (2020), doi: https://doi.org/10.1016/j.jnca.2020.102642

Cite this article as :

Parth Tandel, Abhinav Shubhrant, Mayank Sohani, "A Review of Encryption Techniques Used in Cloud Computing", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 7 Issue 2, pp. 231-243, March-April 2021. Available at

doi : https://doi.org/10.32628/CSEIT217250

Journal URL : https://ijsrcseit.com/CSEIT217250