International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 09 | Sep 2021 www.irjet.net p-ISSN: 2395-0072

Different Approaches to Cloud Cryptography

Dhairya Shah[1], Anuj Sarda[2], Ritik Shah[3], Manav Punjabi[4], Jainum Sanghavi[5]

[1]*Student, Dept. of Information Technology, K. J. Somaiya College of Engineering, Maharashtra, India*
[2]*Student, Dept. of Information Technology, K. J. Somaiya College of Engineering, Maharashtra, India*
[3]*Student, Dept. of Information Technology, K. J. Somaiya College of Engineering, Maharashtra, India*
[4]*Student, Dept. of Information Technology, K. J. Somaiya College of Engineering, Maharashtra, India*
[5]*Student, Dept. of Information Technology, K. J. Somaiya College of Engineering, Maharashtra, India*

Abstract – *One of the most revamping domains today, Cloud computing offers a plethora of services that are accessed around the globe at an individual and an organization level. Cloud computing handles critical data and data can be accessed from anywhere in the world through internet. Therefore, security is an important feature of cloud computing. In this paper, we will focus on cryptography and a secure authentication of cloud computing. It provides extra security for data/files and prevents hackers from getting original files/data even if they get valid credentials. In this survey, we have discussed approaches to secure cloud data using symmetric key and asymmetric key cryptography algorithms.*

***Key Words*: Cryptography, Cloud computing security, Algorithms, Authentication, CIA.**

1.INTRODUCTION

A. What is cloud?

It is a virtual environment where users upload and access data whenever and wherever they want. When data is stored on the cloud, it is not available on the computers hard-drive but on servers of the service provider. Cloud has three main service model – Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS).

B. What is Symmetric Key Encryption?

In symmetric key cryptography, the receiver needs to have the private key, same as the user, with it when the data is being transmitted. The security depends on the secrecy of a single key. The individual who performs encryption sends the key to the receiver, who then uses it to decrypt the cipher information. Examples are AES, DES. In Cloud Computing, this role is performed by the service provider.

C. What is Asymmetric Key Encryption?

Asymmetric Key Encryption In this method, a public key, known to everyone in the communication, is used to encrypt the user data. Another key, called the private key is used for decryption of the encrypted text and is only known to the receiver. Both the keys are generally related but it is not easy to guess one from the other. Examples are RES and Diffie Hellman. Although it is slow, it is better in terms of security when compared to Symmetric Key cryptography as there is no need of key distribution.

2. SECURITY ISSUES IN CLOUD

Data Security is an important factor to be taken care while working or using cloud. Simply putting data on the cloud does not guarantee security. Data can get lost and once that happens there is no physical storage from where it can be restored or taken backup from. So cloud computing must incorporate the CIA Triads for ensuring and enhancing security

A. Confidentiality – Limits access to information to any intruder.

B. Integrity – Integrity assurances that the Message remains unaltered when sent from sender to receiver.

C. Availability – Information is available by authorized people whenever they require.

Encryption of data using cryptography involves the conversion of data into an intricate non penetrable format to send it to the receiver and decryption is the process of converting the data back to its original form at the receiver's end. This paper also sheds light upon symmetric and asymmetric encryption for securing Cloud. [6]

3. IMPORTANCE OF CLOUD SECURITY

A cloud user stores their sensitive data to the cloud. Thus it becomes cloud service providers responsibility to establish secure communication mechanism. With cryptanalysis reaching new levels day by day, the impending decryption of a single layer encryption won't take long. Most of the services used by individuals and organizations like E-mail, social media, Online data storage are contingent upon the security of Cloud. [10]

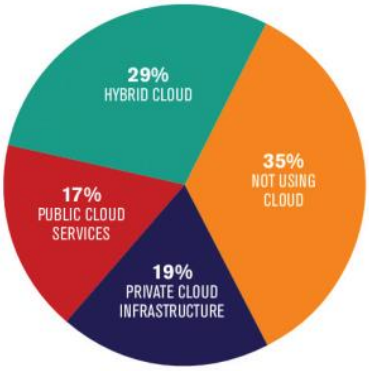

Fig - 1: Cloud Computing Usage [9]

Cloud security challenges:

- **Regulatory compliance:** this occurs when the company denies its audit
- **Data location:** you don't really know where the data is located
- **Recovery:** if the data is crashed then how would they recover it

Some of the **RISKS** to a cloud are-

- Data Protection
- Loss of Data
- Traffic hijacking
- Isolation of Resources
- Malicious Insider as security concern
- Data breaches
- Insecure interfaces as well as APIs
- Denial of service

4. PROPOSED SYSTEMS IN PAPERS

- **USER AUTHENTICATION AND CLOUD ENCRYPTION PROTOCOL**

General Authentication System:

User needs to enter his/her credentials (id and password) to get access to the data files. After successful login, the exchange of data can take place. When the user uploads data to the cloud, the data undergoes encryption and is stored in the cloud.

Drawback –

If someone gets the credentials of the user, he/she can get access to the user's data. A method should be devised so that even if an intruder gets in the system, it will not be able to access any data.

USER AUTHENTICATION PROCESS

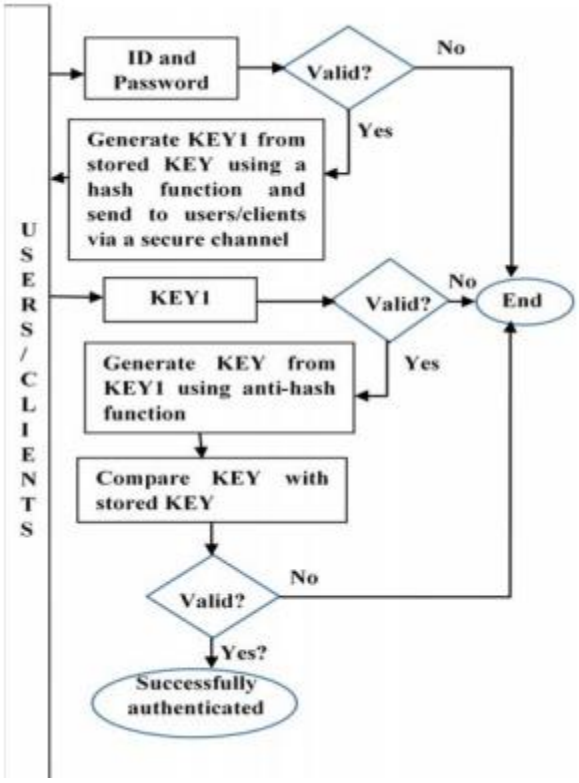

Fig - 2: Users Authentication Process [3]

Advantages –

1. Hackers will fail
   a) if invalid credentials are provided
   b) if he/she is unable to supply the KEY1, which is sent to the user via a secure channel.
2. Extra security is provided by the anti-hash function which validates the KEY1.

If users need to access data from the cloud, the files are decrypted and then sent to the user.

CLOUD END ENCRYPTION

Fig - 3: Cloud end auto encryption [3]

This protocol can be used in Data Analytics fields such as **health and educational data**. [3]

- **DES WITH RSA ENCRYPTION ALGORITHM**

As discussed earlier, securing data becomes more and more difficult if the algorithm is not revamped periodically. To maintain the security of the data and forthright a secure communication, authentication is essential. The proposed idea can be understood in three parts:

Security Analysis:

The paper undermines the use of premised based Data management system. Premise based DMS is the concept of handling cloud data and authentication on an individual level which becomes a daunting task. Furthermore, the drawbacks of a premise based DMS include - a very complex architecture of logistics, storage, indexing that is difficult to implement; Necessity of software licences; and lack of required level of security. Ergo, a Cloud based DMS is proposed where multilevel encryption is implemented on the cloud data to achieve the CIA triad of security of the databases of the users.

System architecture:

Named as Cloud-based DMS, the proposed model equips us with Software as a Service(SaaS) which strikes of all the major drawbacks of premise-based DMS like its intricate architecture and requirement of high capital. Cloud-based DMS is allegedly said to be more scalable and more secure with quick recovery of files and a multilayer encryption. Available with very little prerequisites, Cloud DMS can be used by almost every level of data owners.

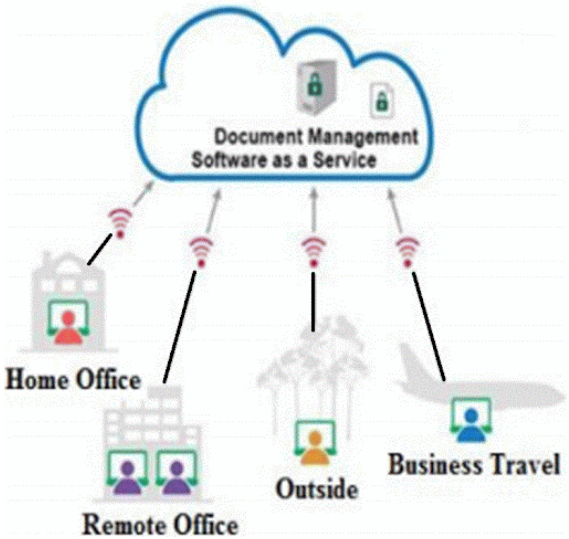

Fig – 4: Architecture of Cloud-Based DMS [8]

Proposed Algorithm

The DES algorithm falls under Symmetric key block cipher which takes in a 64 bit plain text and produces a 64 bit ciphered text. This is done through various shifts and permutations of 16 rounds and was considered one of the most secure algorithms.

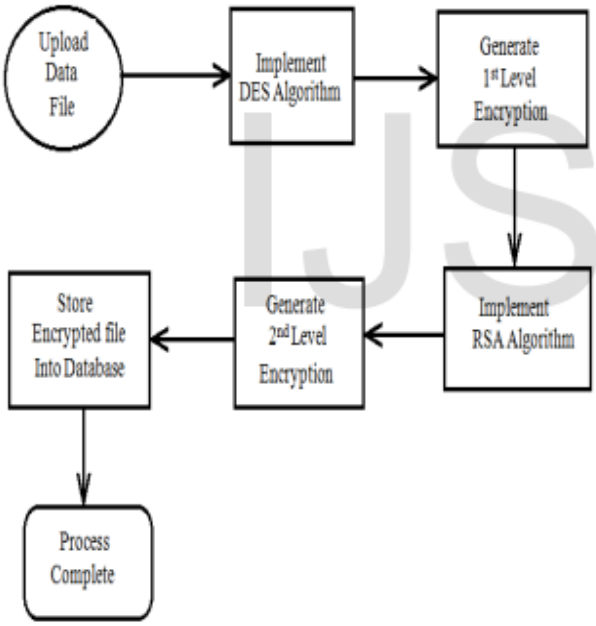

Fig – 5: Block diagram of Multilevel Encryption [8]

The Second algorithm, RSA is an asymmetric key algorithm having two keys (public and private. It is fundamentally based on the principle of modular exponents that are used as public and private keys where only one is used for decryption and one is used for encryption. In asymmetric key algorithms, there is no threat of sending the private key to the other end for decryption.

The model suggested by a paper is a two layer encryption model which uses DES, the symmetric key algorithm to achieve the first layer of encryption. This first layer is then secured with a second layer of encryption using RSA, the asymmetric key algorithm. With a two layer encryption using different algorithms, the data is completely scrambled and difficult to penetrate. [8]

- **AES-256 WITH RSA ENCRYPTION ALGORITHM**

This paper also backs the theory of previous one that a to cope up with the improving cryptanalysis, a single algorithm might not be sufficient. Ergo, the proposed model suggests the use of two different algorithms; one symmetric and one asymmetric. Both the papers choose RSA as the asymmetric algorithm but the key difference is the symmetric algorithm. This model suggests the use of AES – 256 instead of DES algorithm. AES is said to be even more secure than triple DES hence to improve the security, AES is used.

This paper also uses multilevel(2) encryption. The plaintext is first encrypted using AES algorithm with which the first level is achieved. The ciphered text of this encryption is then encrypted using the RSA algorithm which gives us the second layer of encryption. While decrypting, the final ciphered text is decrypted using private key of RSA algorithm. This gives us back the first level of encryption which is then decrypted using the private key of AES algorithm and the data is back to its original form with the receiver.

- **AES WITH RSA ENCRYPTION AND DECRYPTION ALGORITHM**

This will initiate a way for cloud users sharing of particular files with particular users(Read, Write, Execute). Any cloud providers can adopt this service in their functionalities.

1. **ENCRYPTION STEPS:**

Step 1: Take user input like name of user, what rights user wants to allow i.e R for read, W for write, X for execution or any other similar to them and secret code .

Step 2: Generate 128 bit key by encrypting secret code provided by user using AES algorithm

Step 3: merge all data provided by user using this formula. First 4 letters of username + 128 bit AES generated key + Permission letter

Step 4: encrypt final key generated in step 4 with RSA

Step 5: Provide that key to user for communication

Generated key can be provided to intended user. When user will try to access data with this key reverse engineering should be performed at cloud provider server. Below are steps that should be performed.

2. **DECRYPTION STEPS:**

Step 1: Decrypt provided key with RSA algorithm

Step 2: From decrypted result, take first 4 letters that is name of user to whom access is to be allowed, and take last letter that is type of permission to be given.

Step 3: In-between is the 128 bit AES key

Step 4: decrypt key found in step 3 using AES decryption algorithm and generate secret code

Step 5: If secret code is valid then allow the defined permission to user.

Explanation:

As per the key generation steps discussed above, first we will have to take a secret code from user, then we will generate 128 bit key using an AES algorithm. Then we will have to take a name of user for whom key is being generated and permission that we want to provide. Then we will merge details using formula defined in step 3. Final outcome will be encrypted again with RSA algorithm. Resultant key will be provided to user who can further provide that key to another user.

Cloud user stores their sensitive data to the cloud thus it becomes a priority of cloud service provider to establish such a communication mechanism which is highly secure and which covers all security feature. Our proposed algorithm satisfies all these security parameters. With our proposed algorithm, Confidentiality could be implemented with the use of first four letters of intended user name as well as sharing of final key to the intended user only. Thus, limits access to information to any intruder. However, use of more advanced system like access mode and locking period (the time over which the data is accessible to the intended user) ensures integrity and availability of data in more secure and healthy manner. The successful authentication is possible only if data must reach to the destination where it is meant to be and accessible to only who is genuinely allowed seeing. The use of asymmetric (AES) and symmetric (RSA) algorithm ensures that even if any intruder gets an access to the data, he will not be able to reveal the secret key (the one which was shared). Thus all the security key objectives can be achieved by implementing the current system. [1]

- **ALGORITHM FOR DATA SECURITY USING ELLIPTIC CURVE CRYPTOGRAPHY**

There is a lot of buzz about cloud computing nowadays as the years are passing every company is shifting to cloud computing which is due to many benefits that cloud computing provides. Also the pace at which it is developing it adds new features every day making it more reliable and robust. One aspect which drives people away is security of their data. This paper talks about a approach to secure the data using elliptic curve cryptography [10]

The Method:

Elliptic curve cryptography is a public key cryptography. In this method, there are 6 steps.

Step1: decide the values for constants in algorithm

Step2: generate the key. In this step both the parties generate their private and public keys

Step3: generate the digital signature using cryptographic hash function

Step4: encryption takes place

At receiver end:

Step5: decryption takes place

Step6: signature verification

- **DIFFIE HELLMANN WITH ELLIPTIC CURVE CRYPTOGRAPHY ENCRYPTION ALGORITHM**

To remove the security threats, we have used two encryption techniques in this paper: **Diffie Hellmann Key Exchange and Elliptical Curve Cryptography**. By using these two techniques we have created a new architecture which ensures integrity and safety of the data. The steps in our system are:

1. **Establishment of Connection:**

For the new user logging in our system, the user has to make a new account in our system. To establish the connection for the first time HTTPS and SSL protocols are used.

2. **Account Creation:**

When the connection is built for the first time, the account is created by the user by filling in the account details used to create the account in the system. These information are stored in the server and the connection is built using the Diffie Hellmann Key Exchange protocol. Then the generation of the user id takes place by the server, which is used as uniquely to identify the user. For the ECC this id is used as a public and private key, and it is also equivalent to Diffie Hellmann stream. This user id is then sent to the user by a secure channel.

The user is also asked to keep this id secretly, as it is the basic tool for the authentication process, which will be used every time to login into the server.

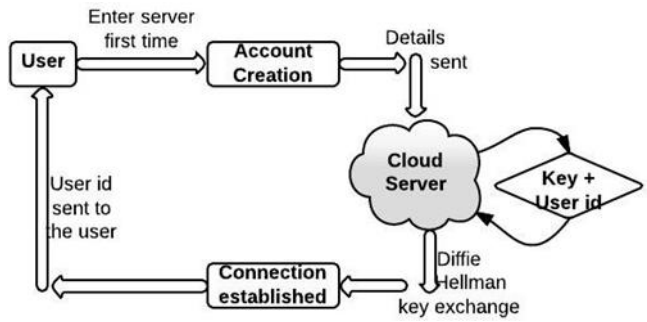

Fig – 6: Account creation process [5]

3. **Authentication:**

When the user is directed to the home page of the server, the establishment of the connection takes place using the SSL. Using the user id and other user details the authentication of the user is done.

Using the Diffie Hellmann equivalent stream of the user id the user validity is done by the cloud server. By matching the key, the connection is established by the protocol again and the logging in process of the user is completed. The encryption of the Ecc algorithms and the private key is done at the back end.

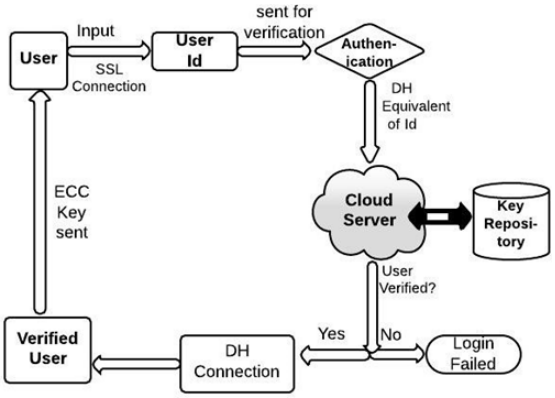

Fig – 7: Authentication of user [5]

4. **Data Exchange:**

There are two steps involved in the data exchange:

A. **Client Side:** For fetching of the data by the user from the repository of the server, the query is formed into a file and encryption is done on the file using the public key. Then the user gets the data for further processing.

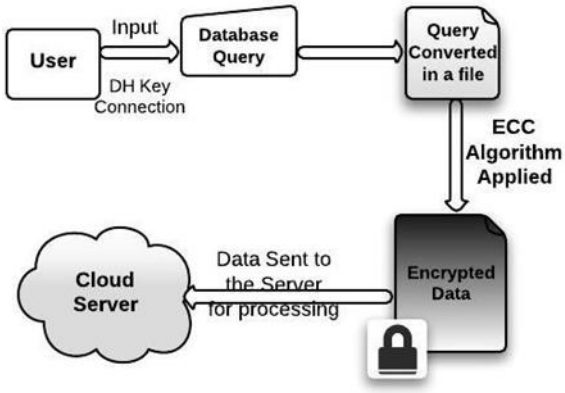

Fig – 8: Data Processing view of Client [5]

B. **Server Side:** The encrypted data is received by the server. Using the private key, the decryption process is done and query of the user is processed. The obtained result is again sent back to the client side after encrypting it. [5]

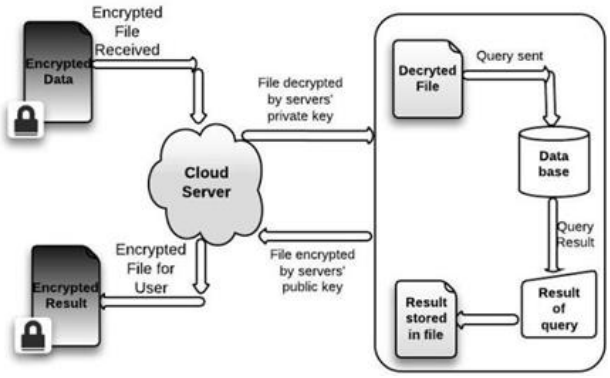

Fig – 9: Data Processing view of Server [5]

5. CONCLUSION

After analysing various approaches we can understand the necessity of securing cloud data to prevent the inexorability of cryptanalysis. This can be done through various symmetric key and asymmetric key cryptography algorithms. Many developed methods provide extra levels of user authentication and cloud end encryption. This prevents the hackers from gaining control, even if they get the user credentials. All the methods cover the main security concerns of cloud computing services through Software-as-a-Service and algorithms like AES, DES, ECC, RSA and Diffie-Hellmann. Through these approaches, Confidentiality, Integrity and Security of the Cloud is maintained. The proposed systems are effective enough so that the security can be attained and cloud users can efficiently share their data. The cloud service provider must provide these systems for secure sharing of data so as to achieve the key security objectives.

6. FUTURE SCOPE

No encryption algorithm can completely be relied on for a long period of time. The impending doom of the strongest encryption being cracked by cryptanalysis cannot be prevented and the algorithm becomes redundant. Ergo, as strong and imponderable these proposed ideas are, they are only temporary. There is still more research going on for the decryption process of these algorithms as they must be more exacted than they currently are and it can be done by improving the decryption of the applied multilevel algorithms.

7. REFERENCES

[1] Kajal Chachapara, TIT Engineering & Technology, Sunny Bhadlawala, Department of Computer Science & Engineering "Secure sharing with cryptography in cloud computing", RGPV University Bhopal, India, AISECT University Bhopal, India, Nirma University International Conference on Engineering (NUiCONE), 2013

[2] Akanksha Upadhyaya, Monika Bansal, Rukmini Devi Institute of Advanced Studies "Deployment of Secure Sharing: Authenticity and Authorization using Cryptography in Cloud Environment", International Conference on Advances in Computer Engineering and Applications (ICACEA) IMS Engineering College,Ghaziabad, India, 2015

[3] SM Jahidul Islam, Zulfiker Haider Chaudhury, Saiful Islam "A Simple and Secured Cryptography System of Cloud Computing", IEEE Canadian Conference of Electrical and Computer Engineering (CCECE), 2019

[4] Sameer A. Nooh. "Cloud Cryptography: User End Encryption", International Conference on Computing and Information Technology, University of Tabuk, Kingdom of Saudi Arabia, 2020

[5] Neha Tirthani, Gangesan R. " Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography", The International Association for Cryptologic Research (IACR), 2014

[6] B.Harikrishna, Dr.S.Kiran, R.Pradeep kumar Reddy "Protection on Sensitive Information in Cloud - Cryptography algorithms", International Conference on Communication and Electronics Systems (ICCES), 2016

[7] Eng. Hashem H. Ramadan, Moussa Adamou Djamilou, "Using Cryptography Algorithms to Secure Cloud Computing Data and Services", American Journal of Engineering Research (AJER) 2017.

[8] Miss Shakeeba S. Khan M.E. Scholar, Dept. of Computer Sci. & Engg "Security in Cloud Computing using Cryptographic Algorithms ", International Journal of Scientific & Engineering Research, Volume 7, Issue 2, February-2016.

[9] Aws Naser Jaber,Mohamad Fadli Bin Zolkipli, "Use of Cryptography in Cloud Computing", Kuantan, Malaysia:IEEE(2013)

[10] Veerraju Gampala, Srilakshmi Inuganti, Satish Muppidi, "Data Security in Cloud Computing with Elliptic Curve Cryptography" ,Volume-2,Rajam, Andhra Pradesh,India:International Journal of Soft Computing and Engineering (IJSCE)(July 2012)