THREE WAY MECHANISM TO ENHANCE THE DATA SECURITY ON CLOUD

[1]Ms. Isha Chawla, [2]Mr. Pawan Luthra, [3]Mrs. Daljeet kaur
[1]Researcher, [2]Assistant Professor, [3]Assistant Professor
SBS State Technical Campus Ferozepur, India
Email:[1]ishachawla1992@gmail.com, [2]pawanluthra81@gmail.com,
[3]daljeetkaur617@gmail.com

Abstract – The cloud computing is one of the developing segmenting of IT industry as well as a promising concept to the end users.Cloud computing is an internet based service which allows its consumers to store large amount of data on the cloud in multitenant environment and use as and when required, from any part of the world via any terminal equipments. As Cloud computing is a shared facility and is accessed remotely, the data stored in it is vulnerable to various attacks by hackers or crackers and becomes difficult to maintain its security and privacy. As a solution to these problems our research paper provides a "Three Way Mechanism" system as it ensures all the three protection scheme of authentication, data security and verification, at the same time. In this paper, we make use of digital signatures and Diffie Hellman key exchange melded with (AES) Advanced Encryption Standard encryption algorithm to protect confidentiality of data stored in cloud. Even if the key in transmission is hacked by untrusted party, the facility of Diffie Hellman key exchange make it useless, since key in transit is of no use without user's private key, which only belonged to the legitimate user. The model we have implemented makes it tough for hackers to crack the security system, thereby protecting data stored in cloud.

Index Terms– Cloud Computing, Security, Authentication, AES, Digital Signatures.

I. INTRODUCTION

Clouds provide a powerful computing platform that enables individuals and organizations to perform variety levels of tasks such as: use of online storage space, adoption of business applications, development of customized computer software, and creation of a "realistic" network environment.Cloud computing virtually and dynamically distributes the computing and data resources to a variety of users, based on their needs, with the use of virtualization technologies and uses public and private APIs (Application Programming Interface) to provide services to its consumers.It provides better utilization of resources and hence results in reduced service access cost. Cloud is used as the medium to store massive data of users. Data outsourcing user can get the information from anywhere more efficiently and has no burden on data storage and avoid extra expense on software, hardware and information resources and the maintenances and usage will be more efficient. The data storage is made public by sharing it on cloud. Cloud services are provided by different cloud providers like Google, Microsoft, IBM, Amazon etc. cloud storage is used as a core technology of many online services [2]. The data stored in the cloud

are accessible anywhere and therefore there are some security requirements are [3] :

- **Authentication**: It is used for identification of intended user.
- **Privacy/ Confidentiality**: Only legitimate users can view the data during transmission.
- **Integrity**: Data is protected from any kind of alteration.
- **Non–repudiation**: Assurance that someone cannot deny something or we can say that the communication between two parties cannot be denied and ensure the authenticity of their signature on a document or the sending of a message that they originated.

Cryptography is the science of enciphering and deciphering of messages that is the art of hiding and transforming information into scrambled format [4]. Encryption is the main aspect of cryptography for the secure transmission of data over the internet and also data can be stored in the same format on the cloud storage to enhance its security[3].

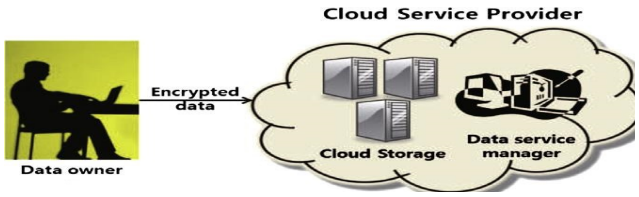

Fig. 1. Data Stored in Encrypted Format on Cloud [5]

Our paper focus on three security control mechanism viz authentication Encryption and data verification technique in to a single system wherein digital signature provides authentication, encryption algorithm provides session encryption key and is used to encrypt user data file , which is to be saved in cloud and lastly trusted computing to verify integrity of user data.

II. LITERATURE REVIEW

Dan Boneh1,Craig Gentry2, and Brent Waters1[6] has described two public key broadcast encryption systems for stateless receivers. Broadcast encryption so defined , a scheme in which broadcaster encrypts a message for some subset of users listening on a broadcaster channel . Any user other than of S cannot receive any information about the contents of the broadcast. In the paper, they have constructed fully collusion secure broadcast encryption systems with short ciphertexts and private keys for arbitrary receiver sets. Their first construction provided a system in which both the broadcast message and user private keys are of constant size and broadcast ciphertext contains only two group elements. Each user's private key is just a single group element. Thus, when broadcasting to small sets, generates far shorter ciphertexts than the trivial solution and in the second system both the public key and the ciphertext are of size O(√n). This means that user can attach the public key to the encrypted broadcast and still achieve ciphertext size of O(√n) [6].

Dongyoung Koo [a], Junbeom Hur [b], Hyunsoo Yoon [a] [7]
have proposed a scheme for data retrieval using attribute-based encryp-tion(ABE). This proposed scheme was best suited for cloud storage systems with massive amount of data.
In this paper, they have proposed a new searchable encryption scheme that exploited ABE with scrambled attributes to handle the securityproblems specifically, the presence of redundant encrypted data for the same message, poor expressiveness regarding access policy, and the concentration of computational overhead on the searching entity. In ABE, the access policy can be represented as Boolean expressions which consist of logical operators such as AND or OR with various attributes describing who is eligible to access the data content. Under this approach, the retriever makes index terms from its private key satisfying the access policy made up of keywords associated with the content, where these index terms are only used for data accessing in the cloud storage system. Therefore, the Cloud Service Provider cannot learn which keywords are associated to the retriever's query. This scheme was suitable for one-to-many content distribution without a sacrifice of the nature of ABE. The main advantage of this was in case of one-upload-many-download situation [7].
According to Parvez khan Pathan, Basant Verma[3], Encryption is the main aspect of cryptography for the secure transformation over

the cloud storage system and also Avalanche effect is the phenomenon that describes the effect in the output cipher text if a single or few bits are changed in the plain text. This change that occurs at the output should be sufficient if we want to create a secure algorithm. In this Paper, they are showing a new encryption key model and there decryption part which will improve avalanche effect as well as execution time as compared with various encryption algorithms. The model so proposed will secure information from all the anomalies which constantly follow-up over public network. In this paper they have defined the study of TEA encryption and MTEA encryption algorithms with their weaknesses and also comparing both these algorithms with their proposed model which will improve the avalanche effect of data thereby improving data security[3].

Authors Kamlesh Kumar Hingwe , S.Mary Saira Bhanu[10], has described about Database as a service (DBaaS) security of Cloud Computing. According to this paper, in DbaaS cloud service providers provide services for storing customers data. As the data are managed by an un-trusted storage server, the service is not fully trustworthy. So, the proposed framework performed database encryption, query encryption and also supports range query over encrypted databases. The proposed framework focused on securing database as well as storing sensitive information without any leaks or alteration. A double layered encryption is used for sensitive data and a single layer encryption is used for non-sensitive data. Order Preserving Encryption (OPE) is used for single layer encryption. OPE maintains the order in encrypted database and so range query can be performed over encrypted database using encrypted query. OPE has a drawback of revealing a personel information and so for sensitive data, a double layered encryption using Format Preserving Encryption (FPE) followed by OPE, symmetric key encryption algorithm is proposed. Symmetric key is used for both OPE and FPE [10].

Authors R.Sivaranjani, R.Radhika[8], have proposed Cloud Security Framework (CSF), been structured to provide complete security to the data throughout the process of cloud computing. In system, multiple mechanisms and available techniques are applied to shield the critical information from unauthorized parties. The proposed Cloud Security Framework (CSF) is divided into two phases. First phase deals with process of transmitting and storing data securely into the cloud. Second phase deals with the retrieval of data from cloud and shows the generation of requests for data access, double authentication, verification of digital signature and integrity, thereby providing authorized user with data on satisfying all security mechanisms[8].

From the literature review, it is observed that there are some limitations and constraints in the security of data stored on the cloud. So, our work is trying to overcome these security issues and is providing the three way protection scheme in the form of authentication, encryption and data verification in single architecture or system.

III. SYSTEM OVERVIEW

A new "Three Way Security Mechanism " system that was proposed by *Mr.Prashant Rewagad,Ms. Yogita Pawar[1]*, is now designed and implemented in our paper to enhance the security of data stored on cloud. Firstly, Diffie Hellman algorithm is used to generate keys for key exchange between client and server. Then digital signature is used for authentication, thereafter AES encryption algorithm is used to encrypt or decrypt user's data file. All this is implemented to provide trusted and secure computing environment in order to avoid data alteration at the server end to preserve data integrity. For the same reason two separate servers are maintained, one for encryption process known as (secure/ trusted) computing platform and another known as storage server for storing user data text files [1].

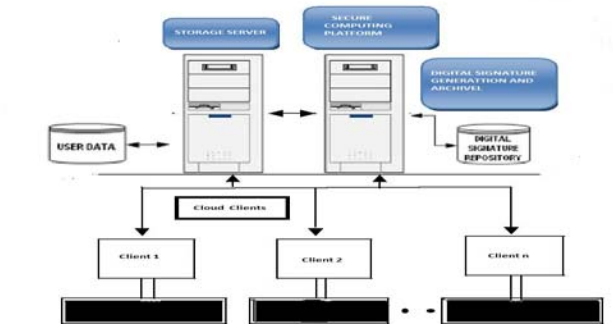

Fig.2. System Architecture [1]

Execution Steps during the process [1] :

- Sign up by the user on the cloud .
- Login from client on the cloud storage
  Key Exchange – Diffie Hellman
  Digital Signature –SHA-I
- Uploading / Downloading Data Encryption- AES
- Data is stored / retrieved from Storage server
- . Logout.

When a user wants to upload a file to the cloud server, first keys are exchanged among client and server using Diffie Hellman key exchange algorithm at the time of login, then the client is authenticated using digital signature. Finally user's data file is encrypted using AES and only then it is uploaded to another cloud Storage server. Now when client is in need of same file, it is to be downloaded from cloud server and for that when user login, first encryption keys are exchanged, file to be downloaded is selected, authentication takes place using digital signature and then the same algorithm, AES is used to decrypt the saved file and client can access that text file [1].

IV. DETAILED INSIGHT INTO THE SYSTEM

Our paper focus on protecting the data of client stored on cloud storage at robust places from any modification or malfunctioning by the third untrusted parties by proper authentication of legitimate user using key exchange process and digital signatures. To secure the data from hackers it has been stored in encrypted format on cloud side that further increases its security to great extend.

A. Diffie Hellman : Key Exchange Algorithm

Diffie Hellman was the first public key algorithm ever invented, in 1976. Client and server want to generate a key to use for subsequent message exchange to avoid any attack on data so the steps followed in this algorithm are[11] :

Step1: Two numbers are set: p, large prime and g, a primitive element of Z_n. These two numbers do not need to be kept secret that is client and server can exchange these two numbers in open.

Step2: Client choses a large random integer x and sends to server

$$X=g^x \bmod p$$

Step3: Server choses a large random integer y and sends Client

$$Y=g^y \bmod p$$

Step 4: Client computes

$$k=Y^x \bmod p$$

Step5: Server computes

$$k=X^y \bmod p$$

k is the final key and need to be same. Therefore, k should be same with server and client and is equal to $g^{xy} \bmod p$. In order to attack this scheme, an intruder would need to know how to calculate x from X or y from Y [11].

B. AES (Advanced Encryption Standard): Encryption Algorithm

AES has also been called Rijndael on its inventors' names Joan Daemen and Vincent Rijmen. The AES encryption and AES decryption occurs in blocks of 128 bits . The maximum block size can be 256 bits however the key size has no maximum limit. The AES cryptography uses the same key to encrypt and decrypt data. The user simply need to select AES encrypt or AES decrypt and the encryptor will do the rest. It is one of the perfect cryptography algorithms to protect personal data. The encrypt AES tool converts the input plain text to cipher text in a number of repetitions based on the encryption key. The AES decrypt method uses the same process to transform the cipher text back to the original plain text using the same encryption key [9].

Process of AES algorithm shown below:

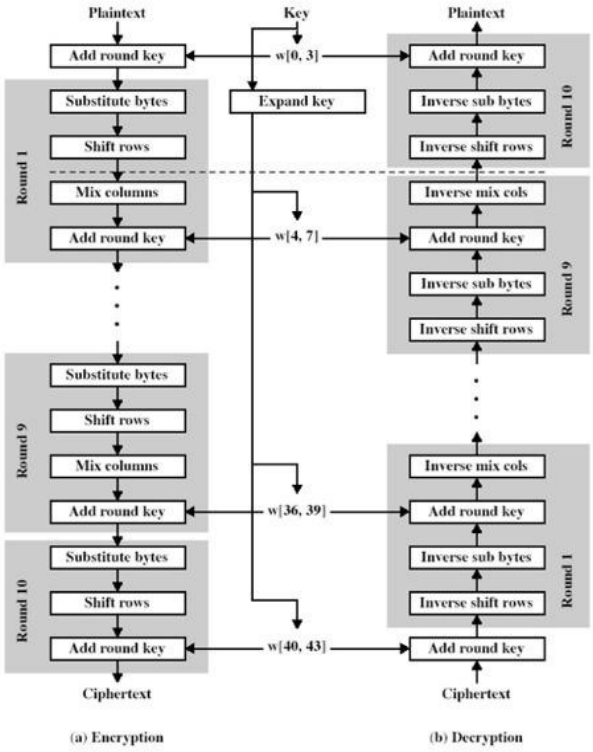

Fig.3. AES Algorithm[9]

V. EXPERIMENTAL SETUP

CloudSim is the simulator tool that is used to carry out experiment. Other minimum requirements that need to be specified are :

A. **Hardware Specifications** :

- Pentium Core.
- RAM Size 128mb.
- Processor 1.2GHz

B. Software Specifications :

- Supporting OS: Windows XP, VISTA, LINUX: Red Hat, Ubuntu, Fedora.
- Java Development Kit - jdk1.6.0_02.
- Java Runtime Environment - jre1.6.0_06.
- Netbeans
- Web Browser like Google chrome with Java Plug-in installed.
- Wireless connectivity driver.
- SOAP
- Glassfish Server

VI. RESULT ANALYSIS

1. Firstly, the client or user registers himself with username / id and password on the cloud inorder to use it as data storage medium.

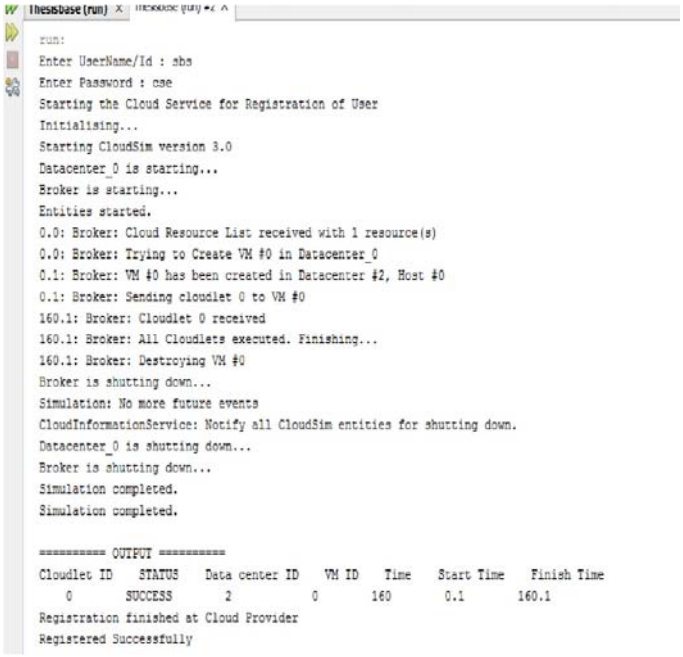

Fig.4. Registration by the Client on Cloud

2. After Registration the client will login on to the cloud with valid username and password. Diffie Hellman Key Exchange Algorithm will run to produce Cloud and client secret and public keys and Login will be finished.

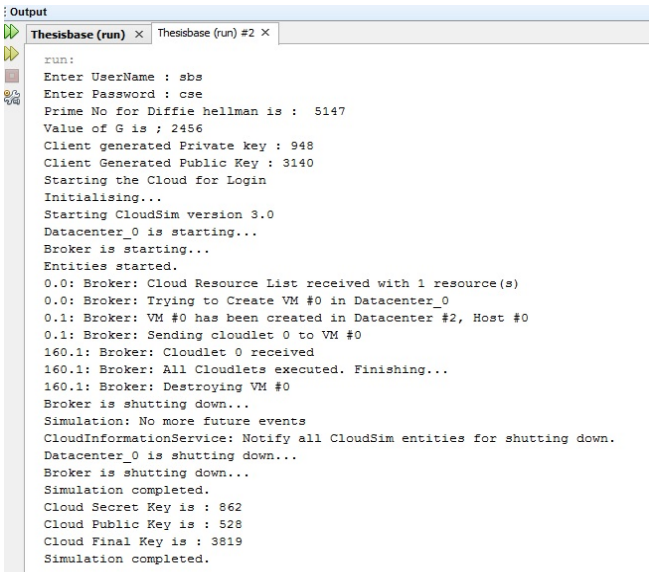

Fig.5. Login on the cloud by the client

3. When the userid and password is correct then client's identity will be verified and this will be done by generation of Digital Signatures at cloud and client side.

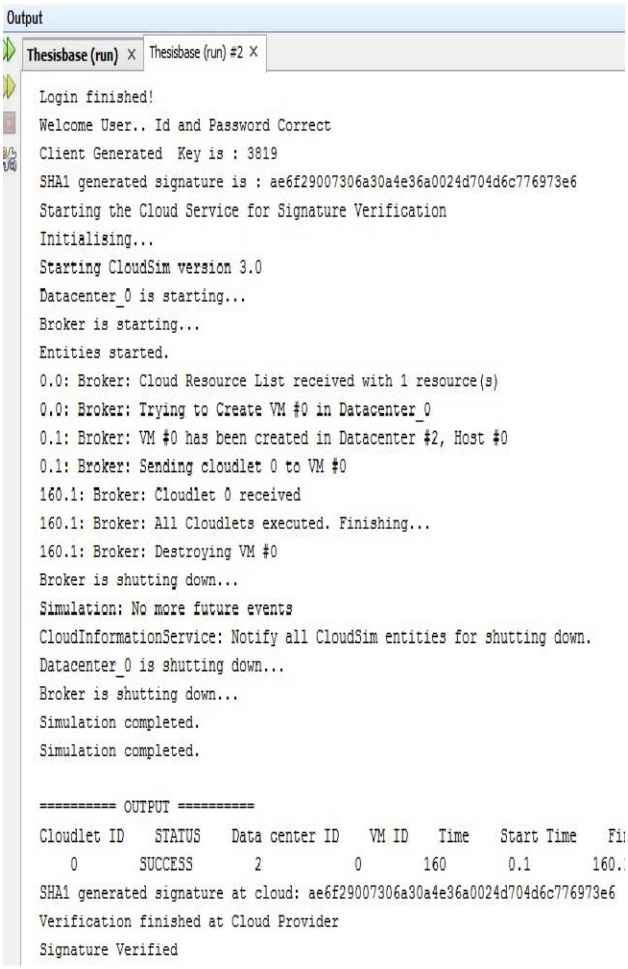

Fig. 6. Digital Signature Generation for verification

4. After the verification and authentication of legitimate user on the cloud is done if the client want to upload the data file then the path will be specified and data will be uploaded in encrypted form on cloud storage by AES Algorithm and also files can be retrieved from cloud in decrypted manner on client machine using the same.

Fig.7. Encryption of data by AES

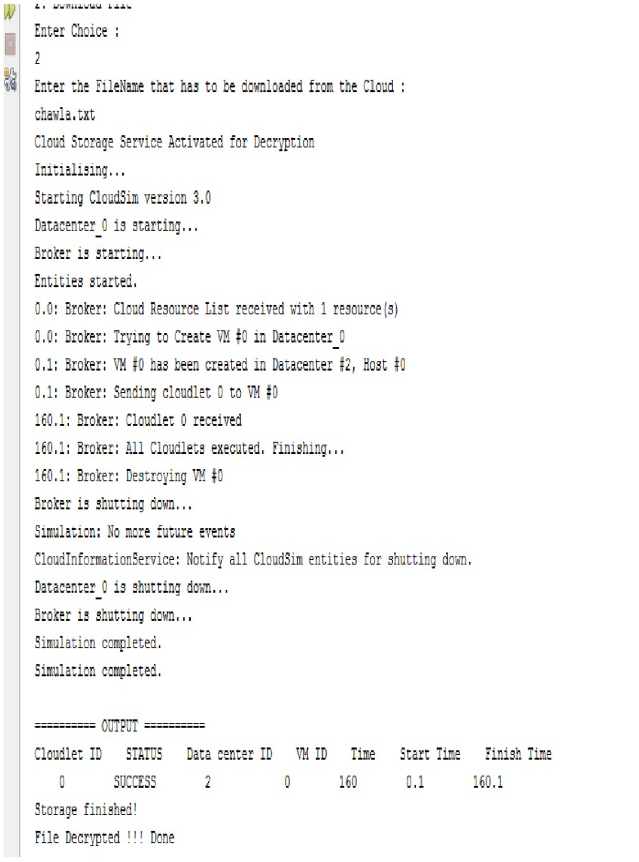

Fig.8. Decrytion of data by AE

VII. CONCLUSION AND FUTURE WORK

In this paper, we have implemeted a new three way mechanism security architecture that enhances the security of data stored at robust places on the cloud. It has incorporated the authentication, encryption and verification in a single standalone system which allows only intended users to use that data, thereby preserving its availability, confidentiality and integrity.
In Future, we can extend our system by different algorithms to generate keys and also "One Time Password" can be applied in addition to key exchange algorithm for authentication so as its security further gets increased.

REFERENCES

[1] 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 Int. Conf. Commun. Syst. Netw. Technol.*, pp. 437–439, Apr. 2013.

[2] R. Subbu and R. Nirmalan, "Survey on Imparting Data in Cloud Storage Using Key Revocation Process," vol. 4, no. 11, pp. 293–297, 2014.

[3] P. Pathan and B. Verma, "Hyper Secure Cryptographic Algorithm to Improve Avalanche Effect for Data Security," vol. 1, no. 2, pp. 140–145.

[4] N. Professional and S. Associate, "A SECURE AND ROBUST CRYPTO SYSTEM BASED ON UNIQUE DYNAMIC KEY," 2014.

[5] A. Celesti, M. Fazio, M. Villari, and A. Puliafito, "Adding long-term availability, obfuscation, and encryption to multi-cloud storage systems," *J. Netw. Comput. Appl.*, Oct. 2014.

[6] D. Boneh, C. Gentry, and B. Waters, "Collusion Resistant Broadcast Encryption with Short Ciphertexts and Private Keys," no. 1, pp. 258–275, 2005.

[7] D. Koo, J. Hur, and H. Yoon, "Secure and efficient data retrieval over encrypted data using attribute-based encryption in cloud storage," *Comput. Electr. Eng.*, vol. 39, no. 1, pp. 34–46, Jan. 2013.

[8] R. Sivaranjani and R. Radhika, "A Framework to Enhance Cryptographic Parameter for Data In Cloud," vol. 2, no. 1, pp. 3508–3513, 2014.

[9] M. E. K. M. C. A, M. Phil, J. M. Sc, M. Phil, and D. Ph, "Secure Login Using Encrypted One Time Password (Otp) and Mobile Based Login Methodology," vol. 2, no. 10, pp. 14–17, 2013.

[10] K. K. Hingwe and S. M. S. Bhanu, "Two layered protection for sensitive data in cloud," *2014 Int. Conf. Adv. Comput. Commun. Informatics*, pp. 1265–1272, Sep. 2014.

[11]http://www.cse.scu.edu/~tschwarz/coen350/diffiehellman.html.