Achieving Cloud Security Using Hybrid Cryptography Algorithm

Tripathi Jyoti[1], Prof. Gayatri Pandi (Jain)[2]

[1] *Research scholar, Computer Engineering, L.J .Institute of Engineering & Technology, Gujarat, India*

[2] *Assistant professor, Computer Engineering, L.J .Institute of Engineering & Technology, Gujarat, India*

ABSTRACT

Clouds are large pools of easily usable and accessible virtualized resources. These resources can be dynamically reconfigured to adjust to a variable load (scale), allowing optimum resource utilization. Cloud Computing security concerns, especially data security and privacy protection issues, remain the primary inhibitor for adoption of cloud computing services concentrate on security issue. In this paper using SHA-512 and MAES hybrid algorithm using hash code which will enhance user authentication process; only authorized person can access the data. Here, the data is encrypted using Modify advanced encryption standard, so data is successfully and securely stored on cloud. Proposed system is highly efficient against malicious data an provide high security and higher execution time .

Keyword : - *Cloud Security ,MAES, SHA-512, Encryption,*

1. INTRODUCTION

Cloud Computing definition is using web-based applications and/or server services that you pay to access rather than software or hardware that you buy and install locally. Using the internet for communication and transport hardware, software and networking services to clients, to general public, enterprises, corporations and businesses markets.

1.1 Types of Cloud Computing

The Public Cloud deployment model represents true cloud hosting. In this deployment model, services and infrastructure are provided to various clients e.g. Google.

The Private Cloud This model doesn’t bring much in terms of cost efficiency: it is comparable to buying, building and managing your own infrastructure. Still, it brings in tremendous value from a security point of view. E.g. Bank.

The Hybrid Cloud is an infrastructure that includes links between one cloud managed by the user typically called “private cloud” and at least one cloud managed by a third party (typically called “public cloud”). Although the public and private segments of the hybrid cloud are bound together, they remain unique entities. This allows a hybrid cloud to offer the benefits of multiple deployment models at once.

1.2 Introduction to Security

Security and Privacy

It is the biggest concern about cloud computing. Since data management and infrastructure management in cloud is provided by third-party, it is always a risk to handover the sensitive information to cloud service providers. Although the cloud computing vendors ensure highly secured password protection accounts, any sign of security breach may result in loss of customers and businesses.

2. LITERATURE SURVEY

In[1] the Authors has purposed consumers, store their personal files or data on cloud server and consumers use that data or files whenever needed. Many consumers store or place their personal data on the cloud, so security and privacy are very important issue in cloud. These two issues can lead to a number of security concerns related to data transmission, integrity control, access control, identity management, logging and auditing, etc. Yet, research in the area of cloud computing receiving great attention from industry, academia and government.

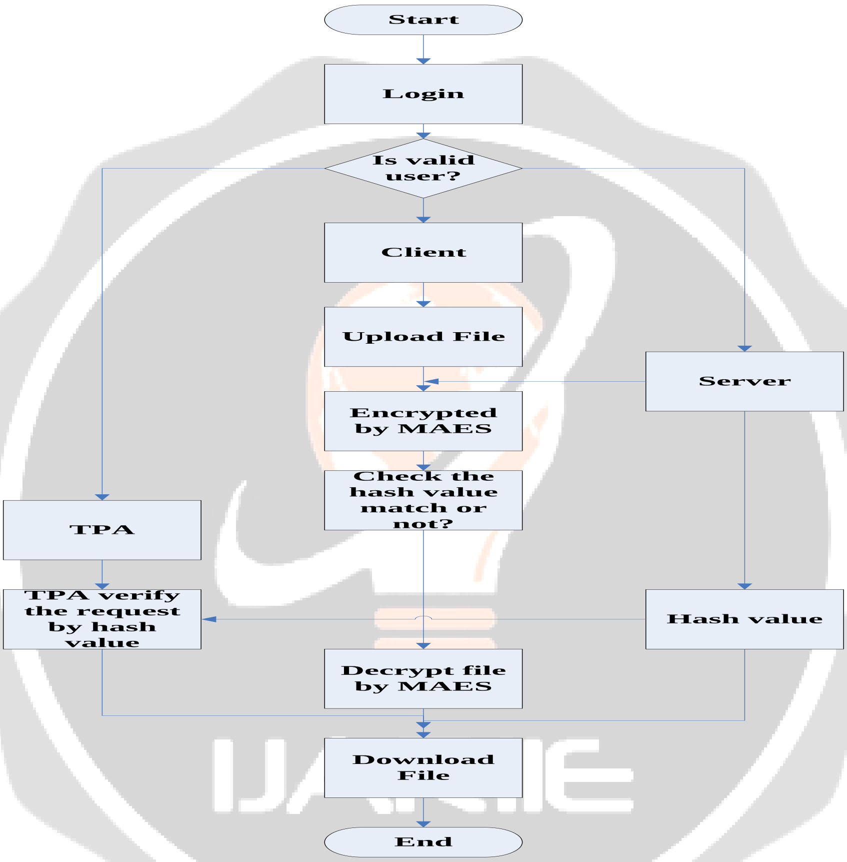

Fig -1 Algorithm Workflow [1]

This proposal is concerned to overcome the security trade-off and improve the performance of data transmission and increases the security through Third Party Auditor and Identity Based Encryption. Provide security in the cloud with the help of the Third Party Auditor. This is done to enhance the hardness in security by the IBE encryption algorithms by adding some more security codes. Encryption is the vital part of information sharing .Put our efforts into an encryption area for IBE algorithm with digital abstract algorithm MD5 so that we can make security harder by giving a hybrid algorithm. Password after that it will be verified by the server. Then the user uploads the file which is encrypted with the help of the IBE. The server generates hash values of user uploaded files. Then users send requests to the TPA for audit their file. The user request consists of request ID and request Status.

After that, the server sends the hash value and ID of that file which user wants to audit. Then, TPA verifies user requests by hash value send by the server, then audit the user files. When users want to download file the decryption process is started.

In[2] the Authors has purposed Certain Cloud Service Providers (CSPs) may operate dishonestly with the cloud users' data, they may sneak the data from cloud and sell it to third parties in order to earn profit Thus even though outsourcing data on cloud is inexpensive and reduces long duration storage and maintenance complexity, there is least assurance of data integrity, privacy, security and availability on cloud servers. Focuses on the integrity verification strategy for outsourced data. The proposed scheme combines the encrypting mechanism along with integrity verification strategy. The encrypting scheme used here is public key cryptographic algorithm like ElGamal and SHA-256 hash function is employed for ensuring data storage correctness on untrusted server.

since the stored data is on cloud server i.e. at a remote location, how to get the verification about the stored data. Since the cloud users do not have physical check over outsourced data, this makes data integrity checking in cloud environment a significant job.

In[3] the Authors presented Cryptography and steganography techniques are more popular now a day's for data security. Use of a single algorithm is not effective for high level security to data in cloud computing. In this proposed system AES, blowfish, RC6 algorithms are used to provide block wise security to data File is spited into eight parts. Each and every part of file is encrypted using different algorithm. All parts of file are encrypted simultaneously with the help of multithreading technique**.** Cloud owner and cloud user are included into system architecture as show .Cloud owner upload the data on cloud server. File is split into octet. Every part of file is encoded simultaneously using multithreading technique. Encoded file is stored on cloud server. Keys used for encryption are stored into cover image. Cloud computing is the multi user environment .In this more than one user can access file from cloud server. Cloud user request for file. On request of file user also get stego image using email which consist of key information. Reverse process is used for decode the file·In hybrid algorithm three keys are used. For data upload on cloud mandatory keys are AES secret key and RSA public key. Private key of RSA and AES secret key are essential to download data from cloud. Advantages of hybrid algorithm are data integrity, security, confidentiality and availability. data integrity purpose hash value is generated. Hash values are garneted after encryption and before decryption. If both hash values matches than that data is in correct form.

Cloud storage issues are solved using cryptography and steganography techniques. Block wise Data security is achieved using AES, RC6, Blowfish and BRA algorithms. Key information security is accomplished using LSB technique. Data integrity is accomplished using SHA1 hash algorithm. Low delay parameter is achieved using multithreading technique. With the help of proposed security mechanism data integrity, high security, low delay, authentication and confidentiality parameters are accomplished.

In[4] the Authors has purposed the most challenging issue today in cloud servers is to ensure data security and privacy of the users. Hybrid encryption RSA along with Advanced Encryption Standard or AES to ensure efficiency, consistency and trustworthiness in cloud servers. During communication along with its application in cloud computing and to enhance the security of cipher text or encrypted data in cloud servers along with minimizing the consumption of time, cost and memory size during encryption and decryption. Presents hybrid encryption algorithm along with AES which is an improvement over simple RSA we can conclude that as the exponent size increases beyond 1024 bits, there is a significant difference between Original RSA and the proposed algorithm. Moreover, it is efficient in terms of Brute Force attack, Timing Attack as well as Mathematical attacks as described above. The complexity of simple RSA is dependent on how large exponent is chosen while the complexity of proposed algorithm is less since symmetric ciphers has complexity O(1) and it makes use of that. It takes less time and memory as compared to RSA as RSA needs to store the computations. Hence, proposed algorithm is much more efficient.

In [5] the Authors presented Many business peoples are getting attracted towards cloud computing model because of the features easy to manage, device independent, location independent. But this cloud models comes with many security issues. A business person keeps crucial information on cloud, so security of data is crucial issue as probability of hacking and unauthorised access is there. Also availability is a major concern on cloud. This paper, discusses the file distribution and SHA-1 technique. When file is distributed then data is also segregated into many servers. So here the need of data security arises. Every block of file contains its own hash code, using hash code which will enhance user authentication process; only authorized person can access the data. Here, the data is encrypted using advanced encryption standard, so data is successfully and securely stored on cloud. Third party auditor is used for public auditing. This paper discusses the handling of some security issues like Fast error localization, data integrity, data security. The proposed design allows users to audit the data with lightweight communication and computation cost. Analysis shows that proposed system is highly efficient against malicious data modification attack and server colluding attack. Performance and extensive security analysis shows that proposed systems are provably secure and highly efficient.

3. COMPARATIVE STUDY

Table- 1: Comparative Study

Paper Title	Algorithm Used	Strong Points	Weak Points
"Achieving Cloud Security using Third Party Auditor, MD5 and Identity-Based Encryption" **Publish paper :** IEEE - 2016	RSA and MD5	Overcome the security trade-off and improve the performance of data transmission and increase the security	MD5 hashes are no longer consider cryptography secure
"Secure Cloud Auditing over Encrypted Data" **Publish paper :** IEEE - 2016	ElGaman and SHA-256	Improve integrity verification strategy for outsourced data	RSA requires more time decryption process
"Secure File storage in Cloud Computing using Hybrid Cryptography Algorithm" **Publish paper :** IEEE - 2016	AES,RC6, Blowfish	Provide block wise security to data.	AES, DES, Blowfish are provide low delay for data encode decode but provides low security.
"Secure algorithm for cloud computing and its applications" **Publish paper :** IEEE - 2016	RSA and AES	Minimizing the consumption of time, cost and memory size during encryption and decryption.	RSA is a computationally costly. AES is better than RSA in terms of time complexity but not more useful to distributing key
"Enhancing Distributed Data Storage Security for Cloud Computing Using TPA and AES algorithm" **Publish paper :** IEEE - 2015	AES and SHA-1	Highly efficient against malicious data modification attack and server colluding attack.	Overhead is high, Time complexity is low, Collision occur

4. PROPOSED SYSTEM

Here using MAES algorithm and SHA-512 technique. When file is distributed then data is also aggregated into many servers. So here the need of data security arises. Every block of file contains its own hash code, only authorized person can access the data. Here, the data is encrypted using Modify advanced encryption standard, so data is successfully and securely stored on cloud. Third party auditors used for public auditing. Handling of some security issues like Data integrity and data security.

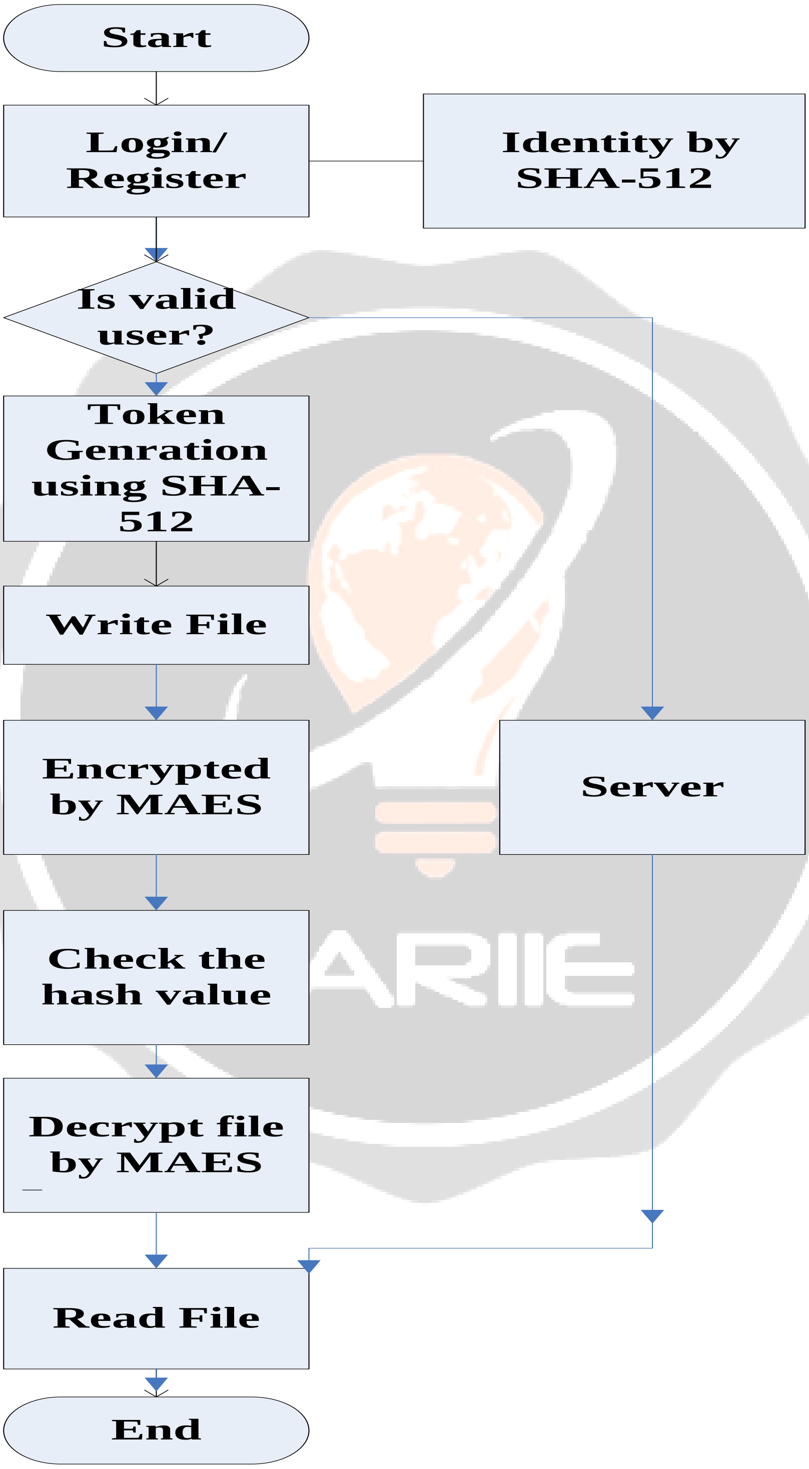

Fig 2. Proposed Method

5 conclusion

The **approaches also relate** to likely problems and abuses arising from a greater reliance on Cloud **computing,** and how to maintain security in the face of such attacks. Namely, the new threats require new constructions to maintain and improve security. Algorithm tools to control and understand privacy leaks, perform authentication, and guarantee availability in the face of attacks. Hybrid Algorithm provide higher degree of confidentiality and **intrigrity.**

6. REFERENCES

1) Bhale Pradeepkumar Gajendra, Vinay Kumar Singh, More Sujeet "Achieving Cloud Security using Third Party Auditor, MD5 and Identity-Based Encryption"IEEE(2016) DOI: 10.1109/CCAA.2016.7813920 PP 1304-1309

2) Sarah Shaikh, Deepali Vora"Secure Cloud Auditing over EncryptedData"IEEE(2016)DOI: 10.1109/CESYS.2016.7889842 pp 1-5

3) Punam V Maitri, Aruna Verma"Secure File storage in Cloud Computing using Hybrid CryptographyAlgorithm"DOI**:**10.1109/WiSPNET.2016.7566416 IEEE(2016) pp 603-610

4) Akshita Bhandari, Ashutosh Gupta, Debas Das**"**Secure algorithm for cloud computing and its applications"IEEE(2016)DOI:10.1109/CONFLUENCE.2016.7508111 pp 188-192

5) Nivedita Shimbre, Prof. Priya Deshpande"Enhancing Distributed Data Storage Security for Cloud Computing Using TPA and AES algorithm"IEEE(2015)DOI: 10.1109/ICCUBEA.2015.16 pp 35-39 Ms. Pooja Deshmukh, Ms. Vaishali Kolhe "Modified AES Based Algorithm for MPEG Video Encryption" IEEE(2014) DOI: 10.1109/ICCUBEA.2014.16 pp 441-446

6) Puneet Kumar, Shashi B. Rana "Development of modified AES algorithm for data security", 0030-4026/© 2015 Published by Elsevier GmbH.

7) D L. Ponemon " Security of Cloud Computing Users", vol. 34-No. 2, International Journal of Computer Theory and Engineering(2010)

8) Yunchuan Sun, Junsheng Zhang, Yongping Xiong, and Guangyu Zhu" Data Security and Privacy in Cloud Computing" Volume 2014, Article ID 190903, 9 pages

9) Pengfei You, Yuxing Peng, Weidong Liu, Shoufu Xue "Security Issues and Solutions in Cloud Computing" IEEE(2012) DOI**:** 10.1109/ICDCSW.2012.20 pp 573-577

10) Akashdeep Bhardwaja*, GVB Subrahmanyamb , Vinay Avasthic , Hanumat Sastryd "Security Algorithms for Cloud Computing" Science Direct(2016) pp 535-542

11) Shakeeba S. Khan, Prof.R.R. Tuteja "Security in Cloud Computing using Cryptographic Algorithms" International Journal of Innovative Research in Computer and Communication Engineering Vol. 3, Issue 1, January 2015 pp 148-153

12) Ms. Pooja Deshmukh, Ms. Vaishali Kolhe "Modified AES Based Algorithm for MPEG Video Encryption" IEEE(2014) DOI: 10.1109/ICCUBEA.2014.16 pp 441-446