Enhancing the Data Storage Security in Cloud Computing with Cryptography Security Principles

J.Velmurugan[1] E.Ajitha[2] A.Jayanthi[3] R.Sangeetha[4] P.Aniz Fathima[5]
[1,2,3]Assistant Professor [4,5]UG Student
[1,2,3,4,5]Department of Information Technology Engineering
[1,2,3,4,5]Vel Tech Hightech Dr.Rangarajan Dr.Sakunthala Engineering College, Chennai - Avadi

Abstract— The number of cloud users and the amount of sensitive data on cloud is increasing massively, so there is a serious need to provide security to the data stored in cloud. Cloud computing allows the user to store the massive amount of data in cloud and to make use of it on demand. One of the greatest challenges in cloud is data security. Since there is a serious security issue in cloud, users are more concerned about the sensitive data, which they store in cloud. Thus to implement the strong security to the data stored in cloud, we implement AES algorithm to provide confidentiality of data. Third party auditor (TPA) and Merkle Hash tree are used to provide integrity of the data. The scheme steganography is used, thereby hiding the sensitive data within the images. All these techniques are collaborated together, to implement strong security to the issues made to the data, which we store in cloud.

Key words: Advanced encryption standard, cloud computing, merkle hash tree, TPA, steganography

I. INTRODUCTION

The important service provided by the cloud computing is cloud storage, which makes it possible for the cloud users to move their data to the cloud. But due to the untrusted cloud server, the cloud users are worrying about the data, they store in cloud. Since the data storage location is virtual to them. To protect the outsourced data, several cryptographic aspects are described below

A. Advanced Encryption Standard(Aes):

AES uses the key size of 128,192 and 256 bits.it is referred to AES-128, AES-192 and AES-256 based on its key length. Encryption and decryption algorithm takes an input of single 128-bit blocks. The encryption process consists of 10 block of processing with 128-bit keys.

B. Third Party Auditor(Tpa):

It audits the data stored in the cloud,to minimize the overhead to the client. The main use of Third party auditor is to check the integrity of the data stored in the cloud and to reduce the overhead of the client.

C. Merkle Hash Tree:

Merkle hash tree is used for authentication purpose. It checks the data, to ensure whether the stored data remains unaltered and undamaged. It is the process of dividing the file into small pieces and apply hash algorithm to it and then combine it back

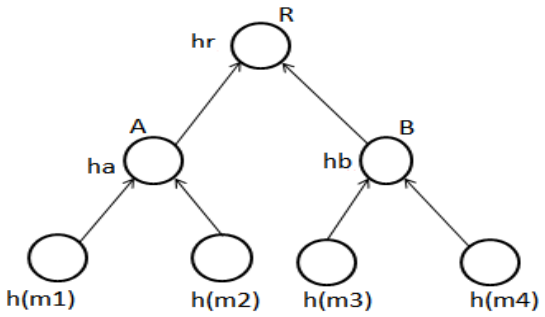

Fig. 1: Merkle Hash Tree (MHT)

D. Steganography:

It is the process of hiding the sensitive data within the images. This scheme guarantees the data security, which is stored in cloud.

Key principles of security:

1) Confidentiality: protecting the data from disclosure to unauthorized users
2) Integrity: correctness of data or protecting information from being modified by unauthorized users

II. EXISTING SYSTEM

In this paper [1], simple data protection model has been proposed, where data is encrypted using AES, before it is being stored in cloud to provide confidentiality and security. Longer the key length, shorter the encryption in symmetric crptosystem.even it provides more protection, there will be more issues in power and time.so they have used “high grade advanced encryption standard” .It is the symmetric encryption algorithm with key length of 128-bits.here the key is not stored after the encrypted data, because there is a chance of getting compromised. so physical key management server can be used in the data consumer side to store the keys. In AES, the encryption process consists of 10 rounds of processing with 128-bit keys. There are no serious weak keys in AES. they have used AES encryption technique to provide security mainly because it is consistent in both hardware and software platforms. it requires less memory for implementation. it support any block size and key size.

In [2], to provide security for the data-at-rest in cloud computing, effective and novel approach is proposed by means of hiding data within images. Here explicit dynamic data support is proposed, by storing the data within the image. This scheme guarantees the data security when it is residing on the data center. The problem statement with data-at-rest is loss of control. Two methods to overcome this problem are through encryption methodology. The proposed model is to secure data-at-rest not only by physically storing files, it is through steganography. This steganography implementation uses three cloud service providers.CSP-1 is to store all the images which will be used for steganography.CSP-2 contains

the encryption algorithm.CSP-3 in which, where all computation take place.

In [3], AES algorithm is used instead of RSA algorithm, since AES algorithm requires very less time for encryption and decryption process and this algorithm requires very less buffer space. Here they have make use of public auditing. to test the integrity of the data, which is being stored in the cloud. this scheme make use of third party auditor(TPA).here they encrypted the data before being stored in cloud, thereby providing confidentiality. To make sure, the data stored in cloud is unaltered and undamaged, this paper uses Merkle hash tree. So far we have concerned only about auditing the static data, so what about dynamic data operation. so they have implemented dynamic Merkle hash tree in order to support dynamic data operation and to provide data integrity.

In [4], to make sure the correctness and integrity of the data stored in cloud,third party auditor(TPA) is used. The main use of TPA is that, it eliminates the burden of client by auditing the data stored in cloud. The use of auditing process will help the owner to test the risk of the cloud data services. There are three auditing, public auditing, private auditing and batch auditing. This paper supports batch auditing for TPA. the main concern behind using TPA is that, it should audit the data stored in cloud without requiring the local copy of entire data and should not insists any overhead to the cloud user

In [5], sobol sequence and elliptical cryptographic curve has been used to allow TPA to check the data stored in cloud without the use of original data. To provide confidentiality, they encrypt the data before being stored in cloud. But to provide integrity, we need to have a local copy of data or should have to receive it from server. Because of this problem, we cannot use straight forward cryptographic primitives and naïve way. In this paper, they introduced "Remote data integrity checking". It is a protocol, in which user generates metadata. Then he challenges the server for integrity. Server generates responses, that it still has data uncorrupted to the user. This protocol has three phases, 1.setup 2.verification 3.Dynamic data operation and verification. Dynamic data operation and verification, not only user access the data, they also modify, update or delete data in the cloud. In setup phase, key generation, encryption, Meta data generation has been carried out. In verification phase, challenge, proof generation, proof check has been done. In dynamic data operation, user request for an update to the server. Then the server updates itself. Here dynamic data operation and verifications are needed.

In [6], distributed scheme is used to provide security in the cloud, in order to prevent access of the data from unauthorized user. This scheme securely stores the data and identifies any problem in the cloud. It performs updating, deleting and appending. Here distributed protocol is used, since the user may insert, delete or modify the data that they have stored in cloud, in order to ensure their correctness. This paper illustrates, when the owner stores the data or file into the cloud server through cloud service provider. Before the owner stores the data into the cloud, they encrypt the file using some sort of security key and then stores safely in cloud. So when any other user tries to access that data, they should have the security key to retrieve it now, the user sends the key request, if it is approved by the data owner, they response with the secret key. The user then accesses the file from the cloud using secret key. If there is an unmatched secret key, file cannot be accessed. To provide more security, they block the IP address of the system, who tries to illegally access the file. The main module in this paper is client module. The client first request the server. Based on the request, server sends the corresponding file to the client. But before this, client authorization is done.

In [7], to provide data security in cloud, some services and access controls are provided. Here the data owner is seriously involved in fine grained data access control to cloud server by disclosing the data contents. Here, they have designed a mechanism for dynamic data verification and operation, in order to conceal (I) correctness of data: this makes the users to trust the cloud, that the stored data is safe. (ii) Localization of data error: when there is any issue in data stored in the cloud. This is used to effectively locate the malfunctioning server. (iii) Dynamic data support: to provide correctness of the data, not only when user stores their data in cloud, but also when they modify, update and delete the data stored in cloud.(iv)Dependability: minimizing the effects made by data loss or server failures.(v) to allow the user to check the data correctness with minimal burden

In [8],the main concern in this paper is optimal storing and retrieval of data with security. In this, user uploads the data on the cloud. This paper provides security to the data, not only by making encryption, but also by providing data to the user, only after successful authentication. it also provides security for the data in transit. In this paper, AES algorithm is used to encrypt the data. Also it provides locking mechanism to allow only the authorized user to access the data by using authenticated name and mail-id

In [9], this paper makes use of merkle hash tree and Advanced Encryption standard (AES) algorithm to maintain data integrity at untrusted server. Here we use AES instead of RSA, to improve the performance. To reduce the overhead of the user in verifying the stored data, we introduced an entity called Third party auditor (TPA) .the novelty of this project is that, this assures recovery of data, when there is data loss, by providing recovery mechanism. in this paper, once the user stores his file in the cloud ,deletes the local copy of the data and strongly relies only on the cloud for data maintenance. to assure the security of client data, auditing mechanism should be implemented. To overcome these problems, AES based storage integrated is proposed in this paper.

In [10], a secure and performance data storage in cloud is called cryptonite. Here we are using merkle hash tree to improve integrity of data and to enhance the bandwidth. A secure data repository is created and placed above the cloud infrastructure. The use of this repository is created and placed above the cloud infrastructure. The use of this repository is, the user can store and share their data on the cloud without giving access of the plain text to unauthorized user, cloud service provider and also to repository itself. cryptonite is introduced with the se of RSA and AES for encryption process. To provide data integrity, SHA algorithm is used. The performance of the system is improves by using Merkle hash tree.

III. PROPOSED SYSTEM

In our project, three entities are used, namely cloud server, user(both data owner and data user) and third party

auditor(TPA).User provided with the access key upon registration in addition to username, password, primary key and secondary key, in order to tighten the security. Once the cloud user is registered with the cloud, then they can upload and download the files which they stored in the cloud, with the proper authorization. Once the data has been uploaded by the data owner, Third party auditor (TPA) is used check the integrity of data stored in cloud and also it can be shared by other data users. In Existing system shared keys are generated, when user tries to share or access the data owner's files and then the data is authorized for usage. But in our proposal system, both the shared key and access key of the user is verified by the cloud server, before they make access to the data stored in the cloud. Once the user is verified as an authorized user, the request is made to the data owner by the cloud server. Data owner creates the mutual key, upon approval of data sharing. The mutual key is strongly encrypted using steganography scheme and then passed to the data user via mail. Where as in existing, mutual key is simply passed in unsecured manner. In this, we have used AES algorithm to encrypt the data with the key size of 128-bit key size. The encrypted data is then applied with steganography for security purpose. it is then resulted in hash code after passing it through Merkle hash tree followed by the hash algorithm. In our approach, security is more tightened by considering every aspect of technology with security principles.

IV. ARCHITECTURE DIAGRAM

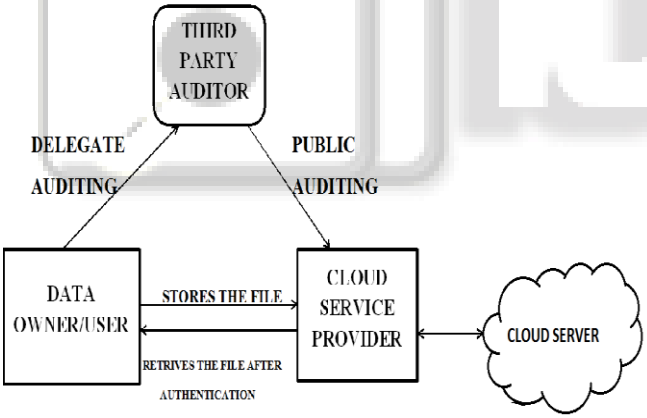

Fig. 2:

A. Performance of AES Algorithm:

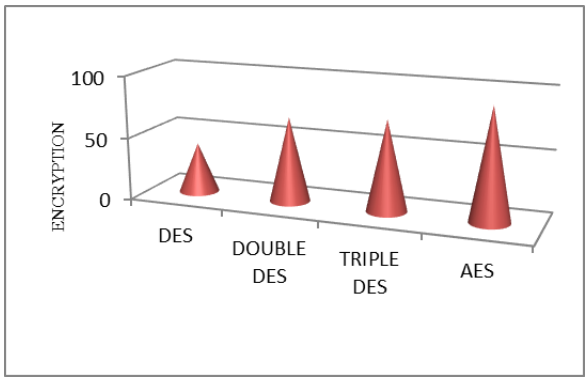

Fig. 2: Encryption time by AES

V. CONCLUSION

By this paper, we made a detailed survey on how the stored data will be secure in cloud. Also we have proposed an approach that ensures the security principles such as confidentiality and integrity of data in cloud. The major analysis made in this paper is that, how to secure the data from an unauthorized access. By our proposal system, we are expected to get 98% data security approximately. The serious data security issue can be compromised by using enhanced encryption algorithms.

REFERENCES

[1] Sachdev Abha Thakral, and Mohit Bhansali ,"Enhancing cloud computing security using AES algorithm "International journal of computer applications (0975-8887) volume 67-No.9, April 2013.

[2] Mrinal Kanti Sarkar and Trijit Chatterjee,"Enhancing data storage security in cloud computing through steganography" ACEEE nit's on Network security, vol.5, NO.1, January 2014.

[3] Poonam M. Pardeshi and Deepali R. Borade, "Enhancing Data Dynamics and Storage Security for Cloud Computing using Merkle Hash Tree and AES Algorithms"International Journal of Computer Applications (0975 – 8887) Volume 98 – No.21, July 2014.

[4] Miss. Nupoor M. Yawale and Prof. V. B. Gadichha,"Third Party Auditing (TPA) for Data Storage Security in Cloud "International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 11, November 2013

[5] 5.K. Yang and X. Jia, "An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing," IEEE Trans. Parallel and Distributed Systems, vol. 24, no. 9, pp. 1717-1726, Sept. 2013.

[6] Deepanchakaravarthi Purushothaman and Dr.Sunitha Abburu,"An Approach for Data Storage Security in Cloud Computing", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 1, March 2012.

[7] Manoj Kokane, Premkumar Jain and Poonam Sarangdhar," Data Storage Security in Cloud Computing", International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 3, March 2013.

[8] Sudeepa R and Dr. H S Guruprasad,"Effective Secure Storage and Retrieve In Cloud Computing"IRACST - International Journal of Advanced Computing, Engineering and Application (IJACEA), ISSN: 2319-281X, Vol. 3, No.3, and June 2014.

[9] Poonam M. Pardeshi and Prof. Bharat Tidke," Improving Data Integrity for Data Storage Security.In Cloud Computing", Poonam M. Pardeshi et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (5), 2014, 6680-6685.

[10] Anjali Almale, Prof. Y. B. Gurav and Prof. S. V. Phulari," Optimized Cryptonite System for Secure DataStorage on Cloud using Merkle Hash Tree", International Journal of Application or Innovation in Engineering & Management (IJAIEM),Volume 3, Issue 6, June 2014.

