Scientific Journal of Impact Factor (SJIF): 5.71
e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 5, Issue 03, March -2018

A SURVEY ON DESIGN AND IMPLEMENTATION OF CLOUD STORAGE SECURITY SYSTEM

[1]Nithyashree C M, [2]Dr.Sheela S V

[1]*PG student, Information Science and Engineering, BMSCE*
[2]*Associate Professor, Information Science and Engineering,BMSCE*

Abstract: *The data storage is one of the primary function of the cloud computing. It provides storage to enterprises as well as end users there by reducing cost of server maintenance. In this paper the cloud security challenges are specified and the system proposed to overcome those problems is given. One of the proposed system is taken into account for explaination.A framework of the third party auditor is first proposed. Based on the system model, a key management plan and an authentication procedure are given which can guarantee the security of cloud storage. In addition to this, two types of key loading methods are briefed to advance the performance of key management. In order to generate a system with balanced load, AES encryption algorithm is taken to decrease the computation load on the userside.Through analyses, the given proposed system achieves both security and overall good performance*

I. INTRODUCTION

The increasing technologies in IT field have made cloud storage to become the vast using technique to store data. so, the lot of enterprises are providing users these services like Google drive from Google[1].Cloud storage is reliable, scalable,multi-tenant still there is a security issue in the cloud for storing the data.

Providers such as Amazon, IBM, Microsoft have established data centres for hosting applications of cloud computing. One of the primary application of cloud computing is data storage. In cloud storage, the data is stored on multiple third-party servers rather than single dedicated server [11].

Cloud storage financial and security-based advantages. Financially, virtual resources used in the cloud are cheaper than physical dedicated resources used for network and personal computers. As in case of security, data in the cloud are not vulnerable to accidental erasure or hardware crashes because the data is duplicated across multiple machines [11].

The server clusters in the cloud helps in achieving data redundancy and data distribution by producing multiple copies of documents which has these objectives: high scalability and high usability. High scalability is achieved by increasing the cloud storage to larger cluster of hundred for nodes for the processing purpose. High usability, it means cloud storage can authorize node failure and do not affect the entire system operation [12].

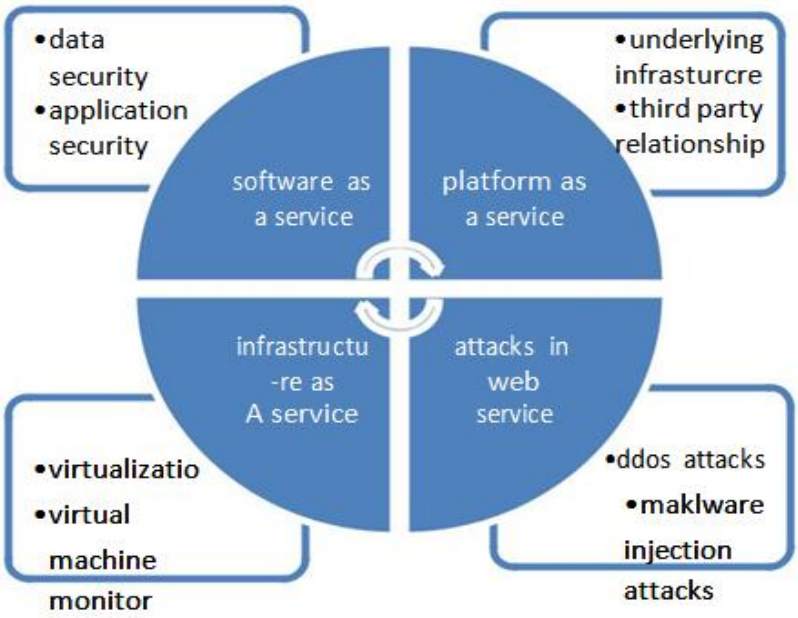

Fig 1: Schematic diagram for Cloud security challenges.

According to survey in recent years, cloud computing gains 12% of the software market in last 5 years and gains the value up to $90 billion. Even though cloud has more advantage it lacks in providing efficient security for data. If this problem of security is considered than cloud computing reaches 50% of software market [2].fig 1 depicts the layer of cloud such as service layers, storage layer and network layer ,with the cloud security challenges.

In this paper, the different techniques used by various authors to secure data in cloud storage and how they implemented it are given.

II. LITERATURE SURVEY

The security problems can be tackled in various ways, many researchers come up with solutions in different ways. The methods are categorized in two groups. one is based on cryptographic methods and other is based on protocol/frameworks.

A. ensuring security by cryptographic techniques

Li et al. in [9] propose a security structure for cloud storage based on the homomorphic encryption scheme. Bhandari et al. in [3] propose a framework using AES, RSA, and HMAC techniques to improve the data storage security in the cloud. Arockiam and Monikandan in [8] propose an efficient cloud storage confidentiality to ensure data security. They use obfuscation and encryption as two different techniques to protect the cloud storage data.

B. Ensuring Security by Framework or Protocol

Feng et al. in [10] propose a protocol which is a novel fair multiparty non-repudiation, provides a fair non-repudiation storage and is having ability of preventing rollback attacks. Shimbre and Deshpande in [6] propose a framework to ensure data security using the AES algorithm and third party auditor. Singh and Verma in [4] propose a framework using AES, SHA-1, and Station-to-Station Key Agreement protocol to overcome security issues like privacy, authentication, and integrity. Omer Mushtaq in [5] introduces quad layered framework for data security, data privacy, data breaches and process associated aspects. Ju-Shu and Min-Te in[1] proposed a framework with third party auditor,key management scheme and an authentication process to secure data in cloud storage.

III. METHODOLOGY

In the previous section the various methods of securing cloud data are listed. In this section the two methods are explained briefly.

In [1], the authors of the paper proposed a third party auditor framework along with key management and authentication process. In addition to this, authors given two types of key loading methods to improve key management performance and the AES encryption algorithm is taken up to reduce the computation load at user side there by creating a balanced load system. At last through analysis and simulation, they have shown that the system proposed achieves both security and overall good performance.

As a preparatory author has given four main functions:

A. B-tree

B-Tree is a self-balancing search tree in data structure which keeps data in a sorted sequence so that insertion, deletion and retrieving of data is done in logarithmic time. It is commonly used in file system and data structure and it is a convenient data structure.

B. Advanced Encryption Standard

It is a symmetric-key algorithm which uses a single key for both encryption process and decryption process. Symmetric key block cipher. It can have 128 bit, 192 bit or 256-bit key size. When a key is longer it is hard to break and it requires more computational time. Four step are performed in each round sub bytes, Mix Columns, ShiftRows and AddRoundKey[13].These four steps mix and shift the data, then re-encrypt it.AES algorithm is very safe security-wise. It needs more than 2126.0 operations to recover an AES 128 key, 2189.9 for AES-192, and 2254.3 for AES-256 [7].

C. Secure Hash Algorithm (SHA)

A cryptographic hash function is a hash function which takes an input (or 'message') and returns a fixed-size alphanumeric string. The string is called The ‘hash value’ extremely easy to calculate a hash for any given Data. The Secure Hash Algorithms are a family of cryptographic hash functions published by the National Institute of Standards and Technology (NIST) as a U.S. Federal Information Processing Standard(FIPS)[14].the versions of are SHA-0,SHA1,SHA-2and SHA-3.

D. Password-Based Key Derivation Function 2

In cryptography, PBKDF1 and PBKDF2 (Password-Based Key Derivation Function 2) are key derivation functions with a sliding computational cost, aimed to reduce the vulnerability of encrypted keys to brute force attacks.PBKDF2 utilizes a pseudorandom function, such as a cryptographic hash, hash-based message authentication code (HMAC), or cipher, to a provided password or passphrase along with a salt value. The process is repeated number of times to produce a derived key, which can then be used as a cryptographic key.

IV. PROPOSED SCHEME

With the existing security system of cloud storage, the user is unable to recognize the verification is safe or not as no other opponents are involved. In order to ensure the security of a system by verification and file encryption, author proposed a new scheme to encounter those issues.

A. Design Goals

In this section, the expectations and design goals of system are provided.

- The author built third party auditor to see the identity of the users instead of using CSP to verify users. By the help of this third party auditor, the unauthorized and malicious users are prevented by accessing data of other users.
- For storing the encrypted file and its key in the same place may cause problem so a new place is required to store the keys.
- As the keys are stored in different place the separate data structure is required to handle the computations like insertion and storing.
- Instead of server handling all the load balancing this is tells us that some amount of load should be handled by client. By this the sever will not become a bottleneck in performance measures.
- An efficient encryption and decryption algorithm should be given so that the it should be able to defend any attack.

B. System Model

As shown in Fig. 2, authors divide all the participating components in their system into three parts: the user, cloud service provider (CSP), and third party auditor (TPA). The user, is first confirmed by TPA and then he is permit to access the cloud storage, together with upload and download his file. The cloud service provider (CSP) provides the storage service to all its users for keeping encrypted file and take part in the registration procedure of users. It does not take part in the authentication process and the key management. Finally, the third party auditor (TPA), is responsible for the verification of users' identity. On the whole, TPA is only used for the authentication safety. It does not hear any information regarding user's file. However, in this scheme, the encrypted file key will be stored in TPA instead of CSP. By doing this, malicious users and CSP itself cannot able to decrypt the encrypted file even if they are able to access it. Hence, this system has not only safer verification but also good key management.

Fig 2.system model

C.Data Structure for Key Management

A the encrypted file and their keys are kept in different location, whenever a user wants to download or upload a file, he have to send the key to TPA or request TPA for the corresponding key of the file. Thus, it is anticipated that there will more insertions and searches for keys. In order to hold this kind of circumstances with minimum computational time and memory usage, the conventional array or tree structure is not good enough. To deal with these issues, they take up B-trees as their data structure for key and user's account management in TPA. The reason to choose B-trees is that it absolutely meets the requirements mentioned earlier. The overall design of data structure is shown in Fig.3.

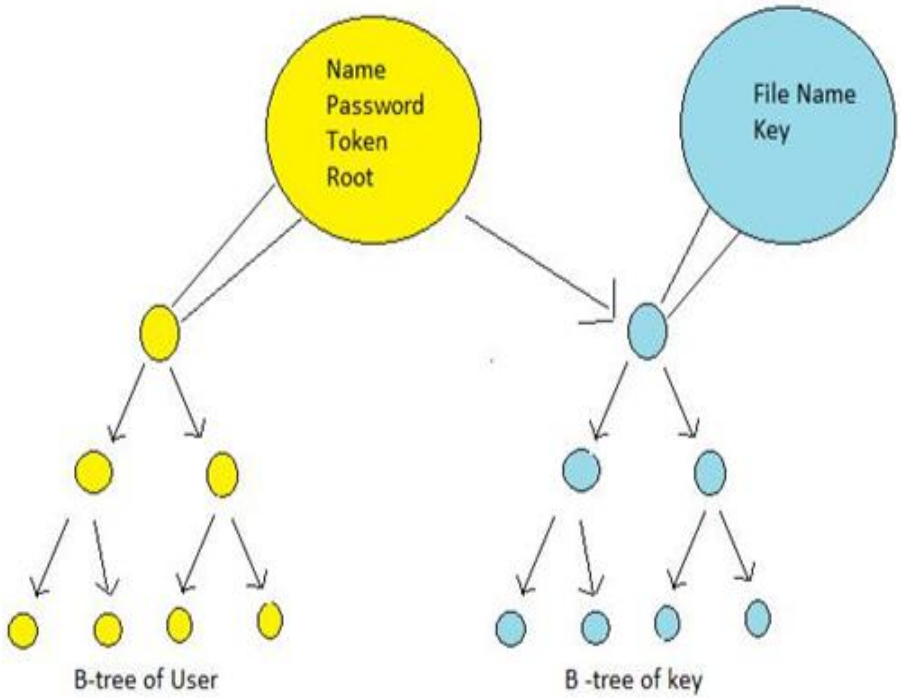

Fig. 3. B-tree for user and key management

D.Authentication Process

In this section, how the user gets authentication based on authors model and data structure is discussed.

First the user send the information of his username and password to TPA.then TPA uses this users name to search his node in users account B-tree. If tree node is present then this user is already registered in the system. Otherwise it an error and then TPA will ask the user to submit his name again.

If the user already exists in the system, TPA verifies if the information user gave matches that in tree node. If the password is wrong, TPA will ask the user to submit correct information again. If the user is legitimate, TPA produces a token for authentication by means of SHA and sends the pair of username and authentication token to CSP for the registration. When CSP hears this information, it knows that this user will request to access the cloud storage system with the particular given token. CSP stores the pair of user name and authentication token, and acknowledges TPA. If TPA receives the acknowledgment from CSP, it sends the authentication token back to the user. After the user receives the token, he can send it to the CSP to access the system. CSP then checks if the user name and authentication token have registered before or not. Finally, CSP grants the user entry permission if the user's information is legitimate and the user authentication process is completed. The complete authentication process is shown in fig 4.

Fig. 4. Authentication process

E.Cryptographic Techniques and Key Management

The authors have already introduced the data structure and authentication process of their scheme, so now the cryptographic techniques are elaborate in this section.

The performance is improved by using symmetric encryption but it has one drawback of sharing the key with other parties. In this paper ,the author assumed that during transmission the key is safe and they focused on key management. With the scheme proposed, they can give guarantee that unauthorized user cannot access the encryption key. Thus, they used encryption mechanism to safeguard the proposed scheme.

F.Encryption/Decryption Process

In this section, we will see the how encryption and decryption are illustrated which are used for schemes'. And the communication during the process between users,CSP and TPA.

The encryption process is first discussed. As illustrated in Fig. 4, when a user desires to upload a file to the cloud storage, first produce a random 32

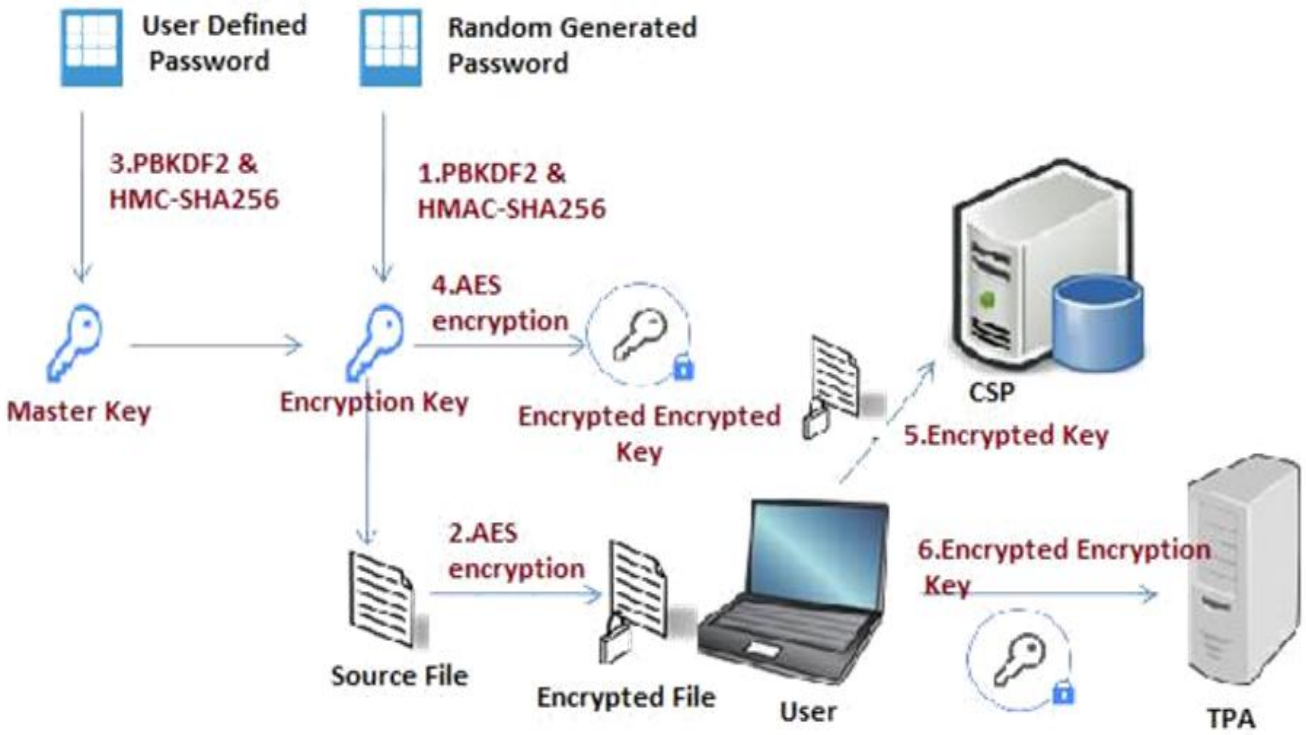

Fig 4.Encryption process

bytes password and employ PBKDF2 with the HMAC-SHA256 to obtain an encryption key. Then encrypt the source file by using AES encryption with the derived encryption key. The operation mode here used is Cipher Block Chaining (CBC). After the encryption is completed, they let user give a password to generate a master key with PBKDF2 once more. This master key is required to encrypt the encryption key. Finally, send the encryption file to CSP to accumulate it in cloud and send the encrypted encryption key to TPA separately.

The decryption process is fairly similar to the encryption process. When the user wants to download a file from the cloud storage, he gets the encryption file from the CSP and sends a request to the TPA for the encryption key of the file. after the user receives the encryption encrypted key and encrypted file. he can use the password to derive the master key and decrypt the encryption key with it. then the user is able to get the source file after decrypting the encrypted file with encryption key. The fig.4, shows the encryption process.

V. RESULT

In this section, the security of the scheme is analyzed and the performance is given.

A. Security Analysis

The proposed system has come up with providing functions such as file encryption, authentication process, key management, strong key generation and the third party auditor in the system. As a second authentication (taken care by CSP),the system uses one-time authentication token to guarantee that same confirmed user accesses the cloud storage. The file encryption is done to ensure the security of user's file. To ensure the strong key generation, the PBKDF2 can guarantee the strength of the derived key and for key management , TPA helps in key storage so that CSP or unauthenticated users cannot access encryption keys.

VI. CONCLUSIONS:

The cloud computing has developed the cloud storage which has been increasingly growing among the enterprises and ordinary users. However, there is a concern about security issues which may become the reason for users to unwilling to store data in the cloud. In inclusion to security issues, the cloud storage overall performance will also affect users' tendency to migrate to the cloud. In this paper, the author has proposed a framework using TPA with AES key management to solve the security concerns of cloud storage. An authentication process which is made by the TPA is first proposed to prevent accessing files by unauthenticated users and the authentication token is used for double authentication. Furthermore, a key management method is proposed to take care two important goals. first, the encryption keys are stored in TPA instead of CSP to avoid the CSP from accessing the source file, and second, the master key is designed to guard the encryption keys in TPA.

To advances the overall performance of the framework, two types of key loading methods are used to handle regular key insertions and searches. For file encryption and file decryption on the user side, AES encryption algorithm is taken to ensure not only security but also performance of the system. The analyses validate the security, the performance and the computational load of the proposed framework.

VII. REFERENCES

[1]. Ju-Shu Chueh and Min-Te Sun, "Design and Implementation of Security System for Cloud Storage," in network operations and management symposium (APNOMS) 2017 19th Asia- pacific,2017.

[2]. Mr.S.Hendry Leo Kanickam, Dr.L.Jayasimman, Dr. A.Nisha Jebaseeli, "A Survey on Layer wise Issues and Challenges in Cloud Security," in World Congress on Computing and Communication Technologies (WCCCT),2016.

[3]. A. B. . A. G. . D. Das, "A framework for data security and storage incloud computing," in International Conference on Computational Techniques in Information and Communication Technologies (ICCTIC), 2016

[4]. D. S. . H. K. Verma, "A new framework for cloud storage confidentiality to ensure information security," in Colossal Data Analysis and Networking(CDAN), 2016.

[5]. M. Omer Mushtaq, Furrakh Shahzad, M. Owais Tariq, Mahina Riaz, Bushra Majeed, "An Efficient Framework for Information Security in Cloud Computing Using Auditing Algorithm Shell (AAS)," International Journal of Computer Science and Information Security (IJCSIS), Vol. 14, No. 11, November 2016.

[6]. N. S. . P. Deshpande, "Enhancing distributed data storage security for cloud computing using tpa and aes algorithm," in Computing Communication Control and Automation (ICCUBEA), 2015

[7]. B. T. . H. Wu, "Improving the biclique cryptanalysis of aes," Lecture Notes in Computer Science, vol. 9144, pp. 39–56, 2015.

[8]. L. A. . S. Monikandan, "Efficient cloud storage confidentiality to ensure data security," in International Conference on Computer Communication and Informatics (ICCCI), 2014.

[9]. J. L. . S. C. . D. Song, "Security structure of cloud storage based on homomorphic encryption scheme," in Cloud Computing and Intelligent Systems (CCIS), 2012.

[10]. J. F. . Y. C. . D. S. . W.-S. K. . Z. Su, "Enhancing cloud storage security against roll-back attacks with a new fair multi-party non-repudiation protocol," in Consumer Communications and Networking Conference, 2011.

[11]. J.Wu, L.Ping, X.GE,Y.Wang, Jianqing FU, "Cloud Storage as the Infrastructure of Cloud Computing," in International Conference on Intelligent Computing and Cognitive Informatics,2010.

[12]. Jiabin Deng, JuanLi Hu, Anthony Chak Ming LIU, Juebo Wu, "Research and Application of Cloud Storage," in intelligent system and application (ISA),2010.

[13]. N. R. Wagner, The Laws of Cryptography: Introduction to the Advanced Encryption Standard (AES), 2001.

[14]. I. T. L. N. I. of Standards and Technology,"Federal information processing standards publication secure hash standard (shs).

