Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 1, January 2014, pg.401 – 407

RESEARCH ARTICLE

AES and DES Using Secure and Dynamic Data Storage in Cloud

[1]Prasanth SP, [2]Gowtham B

[1]Information Technology & V.S.B.Engineering College, Tamilnadu, India

[2]Information Technology & V.S.B.Engineering College, Tamilnadu, India

[1] gowthambruse@gmail.com; [2] prasanthitboss@gmail.com

Abstract---Cloud computing is the usage of both hardware and software as a service through the internet. When it comes to software as a service, it itself depends on the hardware to execute the instructions and hence can carry out the user's request. When the data is accessed through the internet in the cloud, security on the data being transferred will be the major concern. Since cloud computing is scalable and the servers are located in a distributed manner, security is still increasing higher. Users of the cloud can access the cloud from anywhere, from any device, so the device is also to be secured from security attacks. Data that are stored in the cloud is also in the risk of security attacks. To ensure security for the data that are stored in the cloud the Digital Signature Algorithm (DSA) is used to ensure the integrity of the file and Advanced Encryption Standard (AES) algorithm to encrypt and decrypt the files in the cloud storage. Public auditability can also be implemented by using the public key that is created during the file creation or editing process. Secure Hash Algorithm-1 hash function is used to create the message digest in the Digital Signature Algorithm, any other hash functions can be used in the place of SHA-1 like SHA-2, MD5 etc. Advance Encryption Standard Algorithm (AES) is used in the application to encrypt the data stored in the cloud, so that the files stored in the cloud will be free from all the users of the cloud including the administrator of the cloud and the files can be verified to check the integrity of the file.

Keywords— Security; data storage; dynamic data; public auditability

I. INTRODUCTION

Cloud Computing uses the internet and cloud server combined to provide scalability, flexibility, remote usage of services and data storage for the clients in a simple way. Moreover the cloud can be accessed from any device, anywhere on the world. Data that are stored on the cloud can be managed using various applications provided by the cloud provider, also the users of the cloud can create their own application to manage their data. Clients are freed from the data storage burden, maintenance and data can be accessed globally as the data are stored and managed by the Cloud Providers (CP). Software that is running on the cloud is scalable; used by the clients to connect with the cloud and manipulate the data and services of the cloud.

Though Cloud Computing gives more advantages in terms of storage and services. Software of the users, data and databases that are resided on the cloud are under security risks. As CP is individual organizations, data stored in the cloud are not under the direct control of the users of the cloud. Moreover the cloud provider may hide the data loss errors to the users. CP are working hard to secure the data from security breaches, but still the cloud data are under attack. Attackers may steal the cloud data or modify it; hence the security and data integrity of the data are at high risk. CP may also become a threat to the cloud data, if CP is compromised. CP may hide various kinds of failures like Byzantine failure which may occur in the server, so as to keep good name with the clients of the cloud. Also they may delete the rarely used files. These things will become a major problem to clients. If these problems continue to exist in the cloud environment then the cloud clients will lose their faith will the CP.

Though the data are stored in the cloud in a distributed manner, can be accessed from anywhere; maintaining data integrity is highly expensive due to I/O cost for the client to download the data and check it locally. Also the client's cloud data may be of huge size to audit it by the clients in a manual manner. Corrupted data due to failures in the cloud can't be retrieved. Hence clients need to check the file integrity periodically to ensure safety of their cloud data. Checking the data integrity day by day manually is a tedious process as discussed above. Therefore to check the integrity of the data, to maintain the data securely, need to create a system which is capable of checking the data integrity with low cost of I/O, that is to check the data in the cloud itself and to send only the result of the data integrity verification.

Also need to create a system that is capable of maintaining the data in a cryptographic manner so that only the cloud clients can create, edit and delete his data; even the CP can't know what is present in the data. Clients can also appoint a Third Party Auditor (TPA) to check the integrity of the data, in other words public auditability can be done. TPA is one who checks the integrity of the files on behalf of the cloud clients. TPA can check the data integrity without the need of the actual data of the clients. TPA checks the data integrity and provides the result to the clients. Public auditability can be done by using the public key of the files that was generated during the creation of the files; public key of that particular file will change when the client dynamically edit the content in the cloud. TPA will reduce the burden of the client in checking the integrity of the file.

Dynamically editing the cloud files is also a major concern in the previous designs of the cloud as the files need to be downloaded to the local machines, edited locally and uploading to the cloud. Maintaining unique contents in the local and cloud files is a tedious process, as editing and uploading it every time the file is edited locally. To face this issue synchronization of local files is done, every time a file edited. Synchronization is the process of maintaining unique contents of the files and the files itself between the local and cloud storage. When the data is dynamically edited in the cloud, new security issues will rise which will lead to the data security issues. Therefore a system has to be created which is capable of editing the files in a dynamic way and have to be free from security risks.

II. PROBLEM STATEMENT

A. System Model

System contains the cloud storage, security applications in the cloud as Software as a Service (SAAS), TPA, clients which is shown in the Fig. 1. All the above said entities will communicate through the internet for communication between them. Clients are the

users of the cloud who frequently access the files in the cloud storage. Clients may use any device of their own to access the cloud like a mobile phone, laptop, personal computer, tablet etc. Internet connection is required for the clients to access the cloud. TPA are who work for the clients, generate the result of the auditing task and submit them to the clients periodically. Cloud Storage are used to store the files of the clients in a distributed manner, multiple copies of the files maintained in the cloud servers with the unique contents of the files, that is the files are synchronized with all the cloud servers.

Applications which are used to edit, view, cryptography purposes and file specific applications like photo, video editor, development applications etc. are available in the cloud that are used to manage the files in the cloud storage. In cloud computing the large files of the users are stored in the remote location thereby reduce the overhead of maintaining a large storage space and computation mechanism to manage it. Though the files are stored in a remote place and can be retrieved and used whenever the user needs it, there is a problem of checking the integrity of the files, because to check the integrity of the file, the client needs to download and verify the file manually. Hence the clients should have a mechanism to check the integrity of the files periodically, instead of checking it manually by downloading and checking it. Also the client can appoint a TPA to check the integrity of the files, if the client is busy and the TPA needs only the public key of the file to verify.

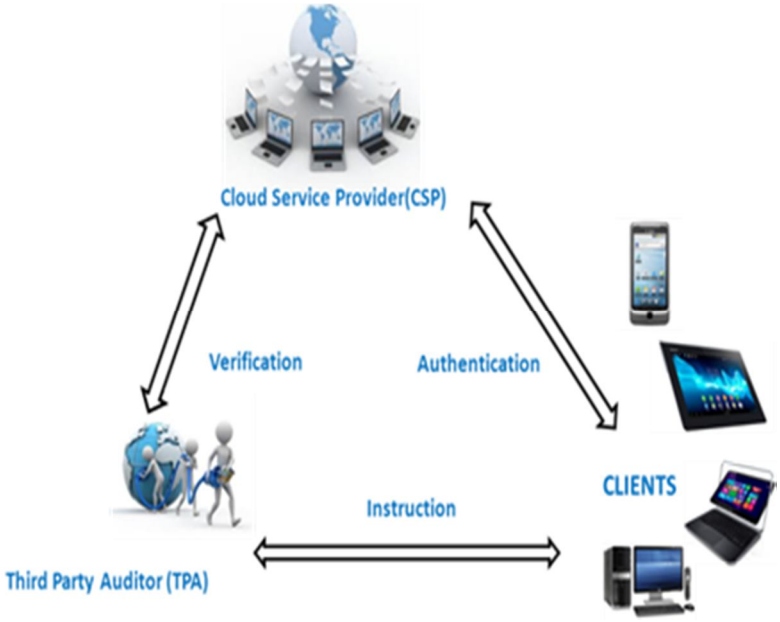

Fig 1. System model

B. **Design Goal**

Dynamic editing: Editing the files in the cloud storage directly without the need to download it manually and uploading it after editing. Large files can be edited easily as the files are modified in the server itself. Time, network bandwidth and hence computation cost can be highly reduced.

Public auditability: Clients who are busy with their day to day work can appoint a TPA to monitor the files of the clients. TPA needs only the public keys of the files that are need to be verified. TPA after auditing all the files in the cloud storage sends the auditing process to the client for final verification.

Security: Files stored in the cloud storage has to be free from attackers. TPA should not know about the content of the files while auditing the files of the client. CA also should not be able edit the files of the client. Files have to be in the encrypted format. Only the client with the valid authentication has to be able to view and edit the files. User-friendly: Clients, TPA have to use the application as easy as possible.

C. Security Model

The system is modeled in a way that the security is not compromised in any way; even the Cloud Administrator can't be able to hack the data of the clients. Data is encrypted by using Advanced Encryption Standard (AES) algorithm and signature for the data is created and can be verified by using the "Digital Signature Algorithm (DSA)". Whenever the client modifies the data, the modified data is stored after encryption and the signature, public key for that file is modified. Data of the clients are encrypted using the 128 bit key, and signed using 1024 bit key. Hence the security of the system is perfect.

III. PROPOSED SCHEME

Integrity of the files can be maintained by verifying the file integrity in a periodic manner, Public Auditability can be done and even the Cloud Administrator can't obtain the content of the files. Data stored in the cloud are at high secure protection that no one can compromise the system.

A. Definitions

The proposed scheme is built based on the algorithms AES and DSA. Encryption of the file during creation or modification is explained in the Fig. 2.

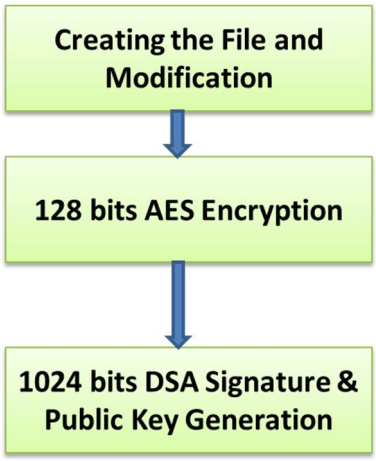

Fig. 2. File encryption and signature creation while modification or creation

When the file is created or modified and saved, file is subject to 128 bit AES encryption that is the file undergone AddRoundKey then 10 rounds of SubBytes, ShiftRows, MixColumns, AddRoundKey and finally undergone a single round of subBytes, ShiftRows, AddRoundKey. After the AES algorithm encryption is over, the file is given to a message digest function "SHA1" and the digest is created using it. Digest is then encrypted using the 1024 bits private key to form the signature. Public key is created with the private key before the encryption is carried out.

While the client is opening a file and verify, the action as depicted in the Fig. 3. Will take place.

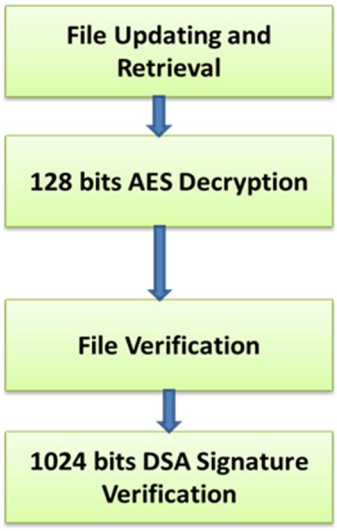

Fig. 3. File AES decryption during file content retrieval and verification using DSA

When the client or TPA verifies a particular file, 1024 bits public key and signature is used for verification. The file is given to the message digest function; here "SHA1" digest function is used to create the digest. File and the signature are combined decrypted with the public key that was created during the encryption of the file and the expected digest is created in this process. If the digest and expected digest are the same then the integrity fo the file is true that is no one has modified the client file. If both the digest is not the same, then the integrity of the file is not verified.

B. **Construction**

According to the proposed scheme (Fig. 4) the file is created initially, after that the file is modified, that is content of the file is inserted, deleted or modified.

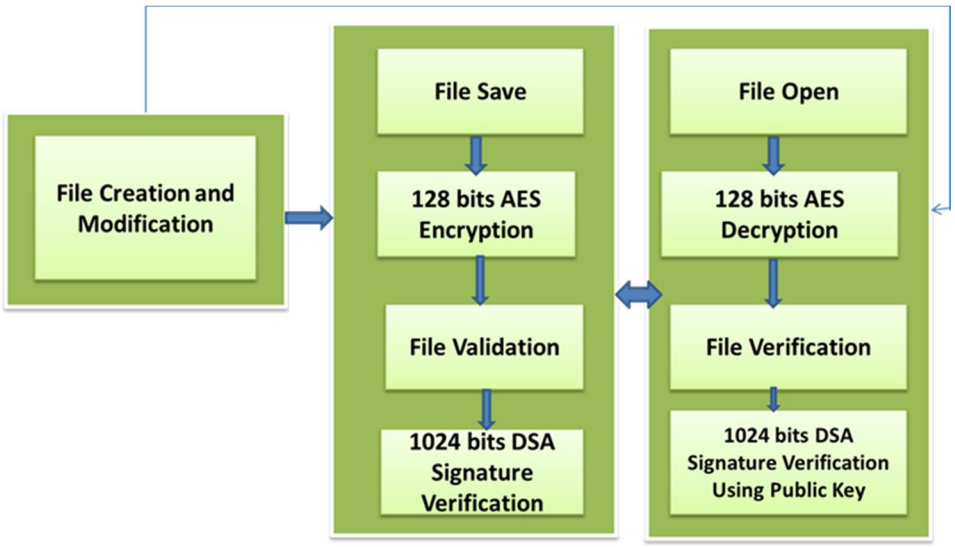

Fig. 4. Proposed scheme

Then the file is saved at which the AES algorithm is used to encrypt the file content with the 128 bits key which has 10 rounds of operation, other key sizes 192 or 256 bits can also be used. DSA is used next to create the signature and key pairs (private and public keys) which are of 1024 bits each. Some days after saving the file the client may open it for viewing or modification, during that AES decryption is done for that particular file and the content of the file is displayed to the user. When the user or the TPA verify the file; the signature, public key of the file created during file saving process is used for verification. If the verification result is true, then the integrity of the file is maintained, that is the file is not modified by any attackers.

IV. CONCLUSION

In this paper, DSA and AES algorithms are used to secure the data and to check the integrity of the file. TPA can also be appointed to check the integrity of the files. Files stored in the cloud storage are hence secured not only from the attackers but also from the cloud administrators.

V. ACKNOWLEDGEMENT

I would like to thank Mr.P.G.Kathiravan Assistant Professor in VSB Engineering College, Karur for guiding me to bring this paper successful.

REFERENCES

[1] Qian Wang, Student Member, IEEE, Cong Wang, Student Member, IEEE, Kui Ren, Member, IEEE, “Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing” - VOL. 22, NO. 5, MAY 2011.

[2] Hsiao-Ying Lin, Member, IEEE, and Wen-Guey Tzeng, Member, "A Secure Erasure Code-Based Cloud Storage System with Secure Data Forwarding" - VOL. 23, NO. 6, JUNE 2012.

[3] Cong Wang, Qian Wang, and Kui Ren, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing" – 2010.

[4] Zhifeng Xiao and Yang Xiao, Senior Member, "Security and Privacy in Cloud Computing" – 2012.

[5] Cong Wang, Student Member, IEEE, Qian Wang, Student Member, IEEE,Kui Ren, Senior Member, IEEE, Ning Cao, and Wenjing Lou, Senior Member, "Toward Secure and Dependable Storage Services in Cloud Computing" - VOL. 5, NO. 2, APRIL-JUNE 2012.

[6] Sivadon Chaisiri, Student Member, IEEE, Bu-Sung Lee, Member, IEEE, and Dusit Niyato, Member, "Optimization of Resource Provisioning Cost in Cloud Computing" - VOL. 5, NO. 2, APRIL-JUNE 2012.

[7] Zhiguo Wan, Jun’e Liu, and Robert H. Deng, Senior Member, "A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing" - VOL. 7, NO. 2, APRIL 2012.

ABOUT THE AUTHOR

	**S.P.Prasanth** received the B.Tech in Information Technology from Nandha Engineering College in 2012 and M.Tech in Information Technology in VSB Engineering College in 2012 under Anna University, Chennai. His Area of Interest includes Pattern matching, Image enhancement, and Cloud Computing. He published Two International journals, Presented International and National Level conferences, attended Various National Workshops and Seminars.
	**Gowtham B** is Currently Pursuing B.Tech(IT) in V.S.B.Engineering College and his area of interest includes Cloud Computing and Cryptography and Network Security. He Presented Various Symposiums, attended Various National level Workshops and Seminars.

