International Engineering Journal For Research & Development

Vol.4
Special Issue

E-ISSN NO:-2349-0721

Impact factor : 6.03

DATA INTEGRITY AUDITING WITHOUT PRIVATE KEY STORAGE FOR SECURE CLOUD STORAGE

Miss. Pradnya G. Kalbande
Information Technology Department
PRMIT & R, Badnera
Amravati, Maharashtra
kalbande2695@gmail.com

Prof. S. S. Kulkarni
Information Technology Department
PRMIT & R, Badnera
Amravati, Maharashtra
sskulkarni@mitra.ac.in

Abstract—

Using cloud storage services, user can store their large amount of data such as confidential documents, mails etc in the cloudto avoid the expenditure of local data storage and maintenance. So that cloud server is mostly being used, to ensure the integrity of the data stored in the cloud. However data security is one of the major barriers to adoption in cloud storage. In multinational companies, employees can share their data such as files, documents, mails and so on. Even user can able to upload their data on cloud storage without worrying about to check or verify integrity. User can store data and used on demand .User needs to employ his private key to generate the data authenticator for realizing the data integrity auditing. Thus user needs to store his private key and also memorize the password to activate the private key. But sometimes private key and password will be forgotten or hack by third party. In order to overcome this problem, we proposed a new paradigm called Data Integrity Auditing without Private Key Storage for Secure Cloud Storage and design such a scheme. In this, we use digital signature scheme in order for the websites, security organizations, banks and so on to verify user's validity

Keywords—Cloud storage, data integrity auditing, Digital signature scheme

Introduction (*Heading 1*)

Cloud Storage can provide a powerful and on- demand data storage services for users to store their huge amount of data [1]. By using the cloud services. Users can outsource their data to the cloud, which bring the great benefits to users. However, once the users upload their data such as document to the cloud as the purpose to share between employees, once they share data they will lose the physical control of their data since they no longer keep their data in local. Thus, the integrity hardware or software failures and human errors in the cloud [2].

Cloud computing is widely embraced by many organization and individual because of its various dazzle advantages like huge size data storage, low price service and flexible way to access the data [3][4] . Cloud Computing could be describe as the use of Computing resources both hardware and software provided over a network, requiring minimal interaction between users and provider. There are three service models are commonly implemented in the cloud such as, Software as a service (SaaS), platform as a services (PaaS) , and infrastructure as a service (IaaS). Cloud computing is remodeling the very nature of how businesses use information technology. In this data is being centralized or outsourced to the cloud server storage. From users a perspective, including both user and enterprises, by uploading data to the cloud server in a flexible on demand manner brings appealing benefits. The benefits such as free from the burden for storage and the security management, global data access over independent geographical locations, and saving of capital expenditure on maintaining security [6]

Data integrity auditing is sometimes we need to have on cloud storage, but there are different threats to harm the shared data. The threats like a hacker which placing a backdoor on storage using applications. Hackers can be change permissions on the confidential documents, modify files or changing the order form to email a copy of everyone's credit card and other information while leaving it appear to be functionally normal without any problem [5].

The system model considered is having cloud data storage or file storage involving three different entities. As illustrated in figure 1 [7]. The entities are cloud users , cloud server storage and data auditing system such as TPA (third party auditor). The first entity users such as a cloud user who store the huge amount of data in the form of files and documents on the cloud storage. Files may be in different types such as binary files, data files,

log files, hidden files. Second entity that is cloud server storage, which fully managed by the cloud service provider or hosting for the data storage space and different resources like network connection, backup facilities and different level security. Third entity is TPA (Third Party Auditor) having expertise and knowledge of integrity auditing process [8].

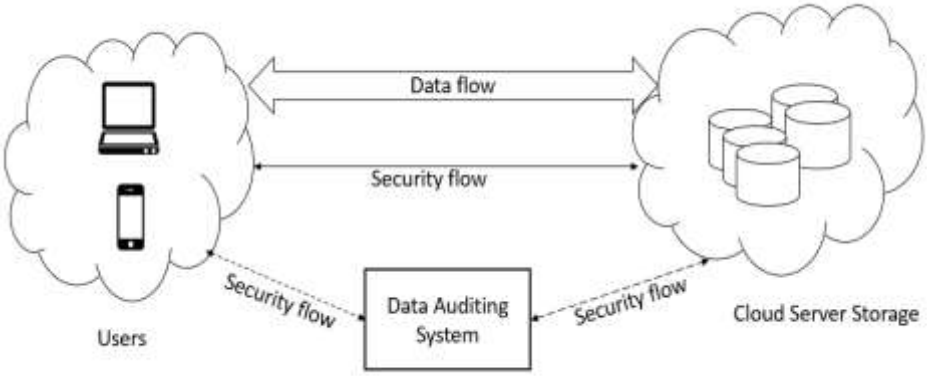

Figure 1. Cloud architecture

Users upload and download their data that is uploading their files dynamically from storage device space on the cloud server for its applications purpose. Users always need to be ensuring that data stored over the server is correct and maintained properly. Users data could be hacked changed or modify internal or external unauthorized entities. To avoid this computational resources and ensure data integrity and security of data which has been share, user resort to TPA to audit the data on behalf of user on cloud server.

There are different scheme has been proposed to ensure the data integrity auditing. We design a new signature scheme which not only support blockless verifiability, but also is compatible with the linear sketch, our proposed scheme achieves desirable security and efficiency. All types of signature scheme emphasis on secure and best verification methods. They are used in order for the websites, security organization, banks and so on to verify user's validity.

This template, modified in MS Word 2007 and saved as a "Word 97-2003Document" for the PC, provides authors with most of the formatting specifications needed for preparing electronic versions of their papers. All standard paper components have been specified for three reasons: (1) ease of use when formatting individual papers, (2) automatic compliance to electronic requirements that facilitate the concurrent or later production of electronic products, and (3) conformity of style throughout a conference proceedings. Margins, column widths, line spacing, and type styles are built-in; examples of the type styles are provided throughout this document and are identified in italic type, within parentheses, following the example. Some components, such as multi-leveled equations, graphics, and tables are not prescribed, although the various table text styles are provided. The formatter will need to create these components, incorporating the applicable criteria that follow.

PROPOSED WORK

This section present integrity auditing scheme which provides a complete outsourcing solution of data. After introducing notations considered and brief preliminaries, started from an overview of proposed data integrity auditing scheme. Finally, the proposed how to generalize integrity auditing keeping data privacy scheme and its support of dynamic data. Figure 2 illustrate the overview of the integrity auditing scheme.

In the following figure two users such as cloud service provider and user. Here there are two cloud such as application cloud and the auditing cloud. Assume a multinational company in which number of employees has been work . They need to share their files or documents between employees. To provide the security to the shared document, so that digital signature generation scheme has been used. In that, first of all user upload their files or documents. They used different algorithm to achieve the desirable security, the algorithm such as SHA (Secure Hash Algorithm) and AES (Advanced Encryption Standards) algorithm.

The Advanced Encryption Standard (AES) algorithm is one of the most common and widely symmetric block cipher algorithm used in worldwide. This algorithm has an own particular structure to encrypt and decrypt sensitive data and is applied in hardware and software all over the world. In private and public sectors to protect sensitive data from intruders or hackers , because of the security of electronic data is crucial issue. Cryptography

is one of the most significant and popular techniques to secure the data from attacker by using two vital processes that is Encryption and Decryption. Modern cryptography provide the confidentiality, integrity, nonrepudiation and authentication [8]. There are different numbers of algorithm for encrypt and decrypt sensitive data. There are three main types of cryptography algorithm such as symmetric cryptography in which same key is used for both that is for both encrypt the data and also decrypt the data. Second one is Asymmetric cryptography in which two different keys are used to encrypt and decrypt the sensitive data. Finally, cryptographic hash function using no key instead key it is mixed the data [9].

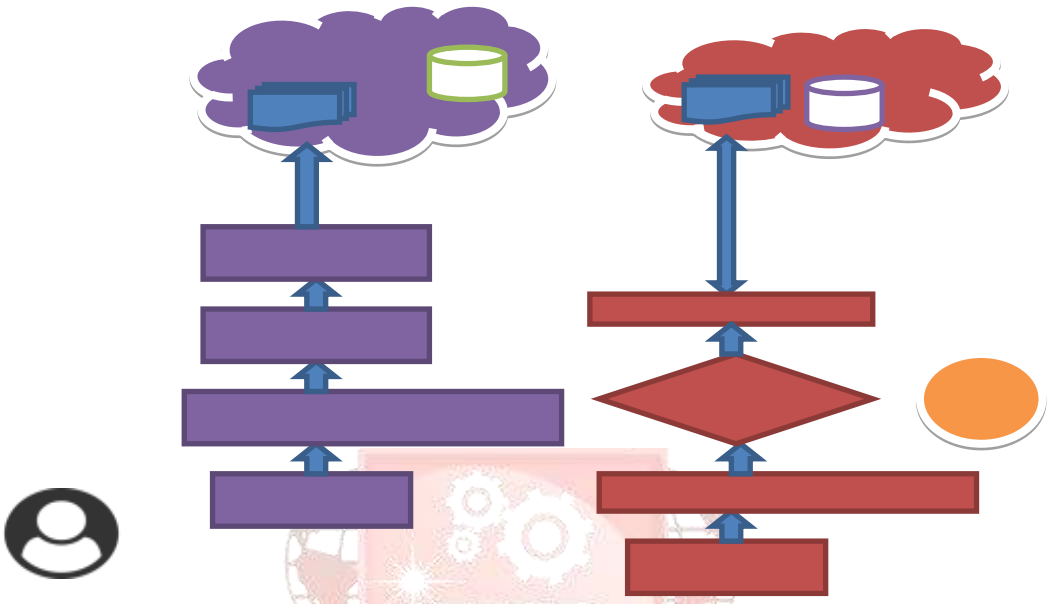

Figure 2. Overview of data integrity auditing

Here we are using the digital signature generation scheme to provide the security to the sensitive data. As given in the figure user are upload there document for the purpose to share the document to other authorized user. When the authorized user upload there document, after that generate a hash value and secrete key of the document. For the hash value generation used the secure hash algorithm. After that document encryption has been take place to encrypt the document and avoid the external intruder to access the data. The encrypted file has been stored in the data base of the application cloud. When the other authorized user request for the particular document, if that user has the access permission to access the document he can easily access. But if the user does not have access permission, then the auditing cloud discard there request.

When the user request for document, first of all check their access permission, whether the user is authorized or not. Then the secrete key is verified, secrete key is in the form of some important details of the user. Integrity is verified automatically even more the detail has been update after every 7 days automatically. Then the document will be decrypt by the decryption process. During encryption of document, hash value of the document will be generating that will stored in both the cloud such as application cloud and auditing cloud. During decryption of document both the hash value will be checked, whether that are matched or not. If the both hash value will be matched then the document are download by other user.

Here also we focus on the document integrity, the documents will be also stored in the database of auditing cloud as a backup on auditor server. The backup documents will be stored in compressed format on auditor server, when needed it will access. In case if the integrity failed during auditing, system will restore the document from backup server.

APPLICATION

Digital signature is very important tools to implement secure and correct sign between two connected partners. Data has been shared between them, but there is a need of integrity to verify the data and securely reached their destination. Today, traditionally physical signature procedure is out-dated. Communication between the two partners of a company is significant issue that must be secure, and be aware from attacker than become stole the data.. Usually digital signature scheme are categorized in four aspects [10].

1. Schemes with Increased Efficiency

2. Schemes with Increased Security
3. Schemes with Anonymity Services
4. Schemes with Enhanced Signing and Verification Capabilities

When a digital signature is generated, important thing is the security of signature scheme, and that always be update as per accessing purpose. The important parameter to evaluate the digital signature scheme is difficulty of implementation. Implementation of parameter is really hard to implement and this parameter based on the computer platform, used locations, security of scheme and so on. The following figure 3 shows the steps of generating digital signature.

Digital signature is a cryptographic primitive which is fundamental in authentication, authorization and non-repudiation. Also the important work of digital signature is to proves its owners identity and also find out he or she can't repudiate his or her sign. In this digital signature is implemented by hash functions and also used public and private key algorithms.

As we showed in figure 3, when the original message is generated by user that upload some files or document and sent for signing to other end of user and those user need to be authorized. The message become hashed by the hash function and also performing private key algorithm, digital signature is generated and is appended to message as "digital signature".When the other end authorized user receives signed message, user can ensure from its validity. This procedure called verification that is performed by public- key algorithm.

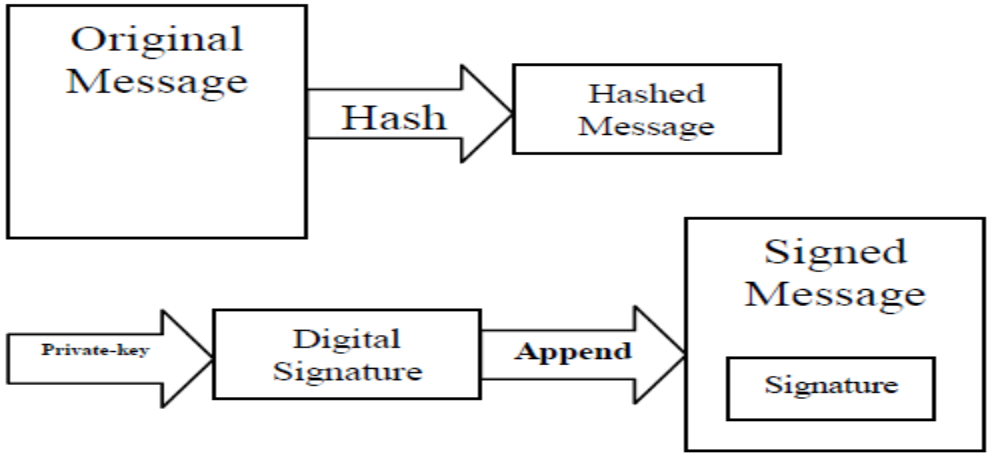

Figure 3. Step of generating digital signature

Digital SIGNATURE SCHEME

In this section we defined different types of Digital Signature Schemes and procedures of their implementation. Every schemes have based on different algorithm which describes the different methods of implementation. Following is the types of scheme that are available and explain as follows,

A. Batch Scheme
B. Forward-Secure Scheme
C. Blind Scheme
D. Proxy Scheme

A. Batch Scheme

This is one of the type of implementation scheme is classified on Increased Efficiency that provides synchronous signing with number of large scale computations. Batch is proposed a procedure for a number of signing digital messages that number of signing message batched together at single message. After performing different cryptographic algorithms, messages are signed and split in single signed message that can be sent to requestors. For example, suppose that we need thousands of signing verification in the same time, in this case Batch Digital Signature Scheme is suitable. This scheme is used random number to generate and verify the validity of signer or user for the purpose to protect the data from attackers. For reconstructing verification functions, attacker is needed to know the random numbers but it seems infeasible in practice.

B. Forward-Secure Scheme

This Forward-Secure Scheme can be categorized in Scheme with Increased Security. This security level is very high as compared to other schemes because in this scheme maintains the validity of the key, even after used that key during encryption and decryption. Idea behind Forward Secure Scheme is T (total time of verifying public key) that are splits the time in to equal periods that any period have special different secrete key for the encryption and decryption message. By using secret key and key update algorithm, public key is remain constant even if next secrete key for next process is generate. To generate and verify steps of signature generation and verification, there will be generate two random and primes numbers P1 and P2 and used them to generate digital signature successfully [10].

C. Blind Scheme

Blind Scheme is classified on anonymity Services that in this scheme receiver does not know identity of the sender, without knowing the details of both sender and receiver data will be insecure between them. During sharing the data sender must get sign from signer but signer can't know sender identity and only sign this message. Suppose that two person are share their data between them, consider the two persons such as person x and person y. Person x sends a message for signing to the person y and person y must sign this send it again to sender without knowing senders is identity.For this scheme to implement includes three steps that should be execute sequent. First step is called blinding, in this, consists of changing message M into the form of f(M). Function f is the blinding function that changes its message identity. Second stage is called Signing, in this stage at the receiver end without knowing the identity of the sender they sign the message and send back to sender. Last stage is called Unblinding, in this stage function is performed to the message and sign will verify [10].

CONCLUSION

In this paper, we explore how to employ fuzzy private key to realize data integrity auditing without storing private key. We proposed the scheme to achieve data integrity auditing scheme without private key storage for secure cloud storage. In the proposed scheme , we utilize Digital Signature Scheme that is achieved by hash algorithm and Advanced encryption standard algorithm as a user's fuzzy private key to achieve data integrity auditing without private key storage. Digital Signature scheme supporting blockless verifiability and the compatibility with the linear sketch. The main purposed is to secure the websites, security organization and so on at the huge level

E-ISSN NO:2349-0721

References

H. Dewan and R. C. Hansdah, "A survey of cloud storage facilities," in 2011 IEEE World Congress on Services, july 2011, pp. 224-231

K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," IEEE Internet Computing, vol. 16, no 1, pp. 69-73, jan 2012.

P. Melland , T. Grace, "The NIST Definition of cloud Computing , Technical report", Nat'l Inst. Of Standards and Technology, 2009.

H. Tian, Y. Chen, C. Chang, "Dynamic-Hash-Table Based Public Auditing for Secure Cloud Storage", Vol. PP, Issue: 99, IEEE Transactions on Service Computing, Manuscript ID, DEC 2016.

P. Mell and T. Grance, "Draft NIST working definition of cloud computing," Referenced on June. 3rd, 2009 Online at http://csrc.nist.gov/groups/SNS/ cloud-computing/index.html 2009.

M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the clouds: A berkeley view of cloud computing," University of California, Berkeley, Tech. Rep.

Cong Wang ,Sherman S.M Chow, Qian Wang, Kui Ren and wening Lou, "Privacy-Preserving Public Auditing for Secure cloud storage" in IEEE transaction on computers vol 62 No 2 February 2013

Abdullah, A. M., & Aziz, R. H. H. (2016, June). New Approaches to Encrypt and Decrypt Data in Image using Cryptography and Steganography Algorithm., International Journal of Computer Applications, Vol. 143, No.4 (pp. 11-17).

Singh, G. (2013). A study of encryption algorithms (RSA, DES, 3DES and AES) for information security. International Journal of Computer Applications, 67(19).

Mehran Alidoost Nia#1, Ali Sajedi#2, Aryo Jamshidpey, "An Introduction to Digital Signature Schemes"