Privacy-Preserving Public Auditing in Cloud Using HMAC Algorithm

S.Ezhil Arasu, B.Gowri, S.Ananthi

***Abstract*—Cloud computing is the arising technology to minimize the user burden in the updation of data in business using internet. Instead of local data storage and maintenance, the user is assisted with the cloud storage so that the user can remotely store their data and enjoy the on-demand high quality application from a shared pool of resources. The data stored must be protected in the cloud storage. To enhance the correctness of data, auditing process is done which is carried out by TPA(Third Party Auditor). The TPA must be efficient to audit without demanding the local copy of data. In this paper we have proposed a method that uses the keyed Hash Message Authentication Code (HMAC) with the Homomorphic tokens to enhance the security of TPA**.

***Index Terms*— Cloud storage, Integrity, Third Party Auditor.**

I. NTRODUCTION

Cloud computing is a long dreamed vision of computing utility, which enable the sharing of services over the internet. Cloud is a large group of interconnected computers, which is a major change in how we store information and run application. Cloud computing is a shared pool of configurable computing resources, on-demand network access and provisioned by the service provider[1]. Cloud computing is used by many software industries now a days as a new technology. Cloud computing gives flexibility to the user, when users put their data in the cloud, they need not manage the information stored in cloud storage. Cloud computing lets you access all your application and document from anywhere in the world. The advantage of cloud computing are cost saving, unlimited storage capacity, improved performance. Reduced software cost, increased data reliability and flexibility. Disadvantage of cloud computing is the security, stored data might not be secure it may get lost.

II. CLOUD SERVICES

Cloud computing is anything that involves services over the internet. These services are broadly classified into three categories: software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS). Cloud software as a service (SaaS) is the on-demand service developed for end users, provider will license the software for their own use. As the software is managed over the central location over the web, the user need not required to handle the upgrades. E.g-gmail. And the next service is cloud platform as a service (PaaS) is designed for the application developers, which provide all the facilities for developing the web applications easily with more features without the complexity of buying and maintaining the software and the infrastructure. E.g-Google App Engine. Finally the cloud infrastructure as a service (IaaS) is way of delivering the cloud computing infrastructure which provision the storage, service and network. As it is fully outsources service it is not necessary to purchase the server, software and other equipments for the business and the service providers benefit from cost saving. E.g-amazon web service.

Revised Manuscript Received on 30 March 2013.
* Correspondence Author

S.Ezhil Arasu*, Computer Science and Engineering, Anna University/ SNS College Of Technology/ Organization Name, Coimbatore, India.
B.Gowri, Computter Science and Engineering, Anna University/ SNS College Of Technology/ Organization Name, Coimbatore, India.
S.Ananthi, Computer Science and Engineering, Anna University/ SNS College of Technology/ Organization Name, Coimbatore, India.

III. DEPLOYMENT MODEL

The deployment models of cloud computing are public, private and hybrid cloud. Public cloud is generally for public owned by an organization. Public cloud (off-site and remote) describes cloud computing where resources are dynamically provisioned on an on-demand, self-service basis over the internet, via web application/web services, open API, from a third-party provider who bills on a utility computing basis. A private cloud environment is often the first step for a corporation prior to adopting a public cloud initiative. Private cloud are two types on-premise private cloud and externally hosted private cloud. Externally hosted private cloud is cheaper than the on-premise private cloud, externally hosted private cloud are hosted with single organization or specific third party specializing in cloud. The combination of private and public cloud id the hybrid cloud. A hybrid cloud environment consist of computing resources on-site(on premise) and off-site(public cloud). By integrating public cloud services, user can leverage cloud solutions which are too costly to maintain the specific function in on-premise like virtual server disaster recovery.

IV. CHARACTERISTICS

Cloud computing includes four basic characteristics:
On-demand self service: Computing capabilities is provisioned automatically.
Broad network access: Capabilities available over the net using desktop, laptop and mobile phone.
Resource pooling: Computing resources provided are pooled together to serve multiple clients.
Rapid elasticity: Capability to quickly in or out provisioning services.
Measured services: Automatically control and optimize resources based on metering capabilities.

V. PROBLEM STATEMENT

Cloud data storage service includes the user(U), who has the large data to be stored in cloud; the cloud server(CS), managed by cloud service provider(CSP) with significant storage; the third party auditor(TPA), trusted to access the CSP according to users request. When user store the data, the copy is sent to both the CSP and TPA. To verify the correctness of data stored in cloud, auditing process is done. Here the auditing process is carried out TPA, it must efficiently audit without bringing any changes to the original data. For auditing, the data which is in TPA is used.

Public auditability: Allow the TPA to verify the correctness of data without demanding the copy of data.

Privacy preserving: To ensure that TPA cannot retrieve the data content during the auditing process.

Lightweight: To allow TPA to perform auditing with minimum communication and computation overhead[2].

VI. RELATED WORK

Related works were carried out by Yan Zhu et al [3]. about the data which the user puts into the cloud will be sent to the Cloud Service Provider(CSP) and a copy of it is also sent to the Third Party Auditor (TPA) which checks for the correctness of the data. Dynamic audit service is done for verifying the integrity of un-trusted and outsourced storage. Here periodic sampling is done to minimize the computation cost of TPA and storage service provider.

The related works carried out by Qian Wang et al [4]. studied that so as to ensure the credibility of the data that is being used during the auditing process a remote integrity checking protocol is used. This protocol is suitable for integrity protection of the data stored in cloud. It supports dynamic operations like insertion, deletion and updation of data. To achieve efficient data dynamic, and to improve the storage by manipulating the classic merkle hash tree for block tag authentication[4].

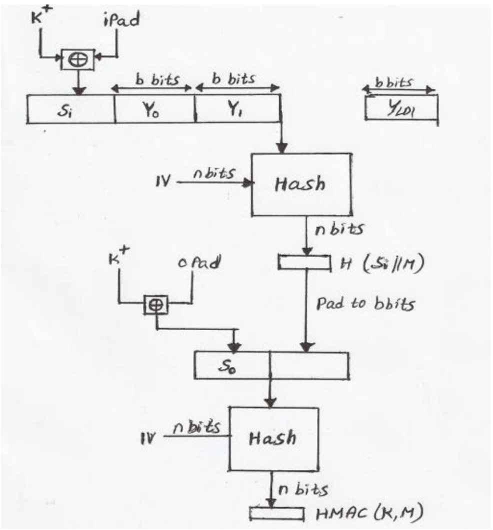
Further Nandeesh et al [5]. carried out future work on the physical possession of the outsourced data in cloud computing storage creates new security risk. To secure TPA based storage using homomorphic tokens and distributed erasure coded data, which allow to audit the cloud storage with minimum computation cost. To achieve efficient data dynamic operations, we improve the storage on outsourced data including data modification, deletion and updation. To provide redundancy parity vector and guarantees data dependability using erasure-correcting code in the distribution preparation[6].

Mururalikrishnan Ramane et al [7]. studied further about the public auditing schemes are used efficiently in auditing the data stored in cloud, it solves the issue of restricting TPA to access of the data openly. This scheme verifies the metadata rather than actual data which provides secure cloud storage that supports privacy preserving public auditing.

Dalia Attas et al [8]. studied further on cloud computing to ensure the integrity of the data stored in the cloud storage, TPA supported with digital signature is used for efficient auditing. This doesn't affect the original data and also audits without demanding local copy of data. Checking is done in the cloud service provider(CSP) and TPA. The digital signature first performs hash function using message-digest algorithm(MD5)[9]. Compute encryption with private key on the other hand decryption by using public key with hash value containing reverse order of its original data.

VII. HMAC

Hash based message authentication code is cryptographic hash function which is all about the concatenation of message and the key and hash them together. It is the method of calculating message authentication code with cryptographic hash function by using secret cryptographic key. The hash algorithm used to generate the authentication code is SHA. The authentication code used to verify the data integrity and authentication of the message using the security key which is necessary for producing the code. The authentication code produced by the normal hash function can be reproduced without any normal constraints. The cryptographic strength of the hash function, the size of the hash output and the size and quality of the key determines the cryptographic strength of HMAC. HMAC doesn't serve the purpose of being a provider of message integrity by itself. It is one of the components in the protocol that provides message integrity. Though the HMAC is not designed to encrypt the message itself it serves as a protection shield for man in the middle attack. HMAC supports hash algorithms like MD5,SHA –1, SHA – 256 and etc.



Structure of HMAC

Which implement the function:

$HMAC_k$ = Hash [(K^+ XOR opad)] | | Hash [(K^+ XOR ipad) | | M)]

K^+ is K padded with zeros on the left so that the result is b bits in length

ipad is a pad value of 36 hex repeated to fill block

opad is a pad value of 5C hex repeated to fill block

M is the message given as input to HMAC[10].

The output of the HMAC is the binary authentication code which equals in the length to that of the hash function digest. The security of the HMAC is directly proportional to the underlying hash function. Hence security of HMAC is said to be weaker if the underlying hash function is MD5 and stronger if the underlying hash function is SHA – 512. The threats of the HMAC are said to be forgery and the key recovery attacks, but these threats need large number of message pairs for the analysis.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Data integrity being one of the most important feature in the cloud computing. So as to ensure the data integrity message authentication code is used along with the hash function like Secured Hash Algorithm(SHA). The hash function is chose based on speed and security concerns. The SHA generates a separate key using a hash function by passing the original message to the hash function. This process is carried out by both the user and the auditor. The data integrity is verified by comparing the values that are received from the hash function by the user and the auditor. The hash function does the process of condensing arbitrary size message to fixed size by processing the message in blocks through compression function which are either custom or block cipher based[11]. HMAC is a symmetric process which makes use of secret and hash algorithm for the generation of authentication code. The authentication code is the core factor which ensures data integrity and authenticity because a secret key is necessary to reproduce the authentication code. HMAC is used because it ensures the usage of hash functions without any modifications and these hash functions can be used in any software that is widely available. The HMAC provides the advantage of preserving the original performance of the hash function without subjecting it to any degradation.

VIII. HMAC SPECIFICATION

To compute a MAC over the data ‘text’ using the HMAC function,the following opereation is Performed;

$MAC\ (text)_t = HMAC(K,text)_t = H((K_o \downarrow opad)||H((K_o \downarrow ipad) \ || \ text))_t$

Step by step process in the HMAC algorithm,which is depicted in

Step 1 If the length of K = B: set K_0 = K. Go to step 4.

Step 2 If the length of K > B: hash K to obtain an L byte string, then append (B-L) zeros to create a B-byte string K_0 (i.e., K_0 = H(K) || 00…00). Go to step 4.

Step 3 If the length of K < B: append zeros to end of K create a B-byte string K_0 (e.g., if K is 20 bytes in length and B = 64, then K will be appended with be appended with 44 zero bytes 0x00).

Step 4 Exclusive-Or K_0 with ipad to produce a B-byte string: K_0 ↓ ipad .

Step 5 Append the stream of data ‘text’ to to the string resulting from step 4:(ko↓ ipad)||
Text.

Step 6 Apply H to the stream generated in step 5:H((ko↓ipad)||text).

Step 7 exclusive-or K_o with opad :ko ↓ opad.

Step 8 Append the result from step 6 to step 7: (k_o ↓ opad) || H((K_O ↓ ipad) || text).

Step 9 Apply H to the result from step 8: H((k_o ↓ opad)|| H((k_o ↓ ipad) || text)).

Step 10 Select the leftmost t bytes of the result of step 9 as the MAC.

IX. CONCLUSION

In the cloud storage, user put their data in the cloud and no longer posses the data locally. One of the key issue is to detect the modification and corruption during the auditing process by TPA. The third party auditing allow to save time and computation resources with reduced online burden of the user. Security for the data stored in cloud during the auditing process can be provided by HMAC along with the homomorphic tokens with erasure coded data.

ACKNOWLEDGMENT

The authors would like to thank the Editor in chief the Associate Editor and anonymous Reference for their comments.

REFERENCES

1. P. Mell and T. Grance, “Draft NIST working definition of cloud computing”.
2. C. Wang, Q. Wang, K.Ren, and W.Lou, “Privacy-Preserving Public Auditing for Secure Cloud Storage”, in Proc. Of IEEE INFOCOM’10,March 2010.
3. Y. Zhu,Z. Hu,Gail-J Ahn, H. Hu,Stephen S. Yau, Fellow, IEEE, Ho G. An, and Shimin Chen,”Dynamic Audit Services for Integrity Verification of Outsourced Storages in Clouds”,in Proc.of IEEE SAC’11 March 2011.
4. Q. Wang, C. Wang, Kui Ren, W.Lou and Jin Li, “Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing”, in IEEE transaction on parallel and distributed system May 2011.
5. Nandeesh.B.B, Ganesh Kumar R, Jitendranath Mungara”Secure and Dependable Cloud Services for TPA in Cloud Computing” International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-1, Issue-3, August 2012.
6. M. A. Shah, M. Baker, J. C. Mogul, and R. Swaminathan, “Auditing to keep online storage service honest”, in Proc. Of HotOS’07, CA, USA: USENIX Association, 2007, pp.1-6.
7. Muralikrishnan Ramane and Bharath Elangovan, “A Metadata Verification Scheme for Data Auditing in Cloud Environment”, International Journal on Cloud Computing: Services and Architecture(IJCCSA), Vol.2, no.4, August 2012.
8. Dalia Attas and Omar Batrafi “Efficient integrity checking technique for securing client data in cloud computing”, October 2011.
9. S. Balakrishnan, G. Saranya, S. Shobana, S. karthikeyan, “Introducing Effective Third Party Auditing(TPA) for Data Storage in Cloud” IJCST Vol. 2, Issue 2, June 2011.
10. Cryptography and Network Security Chapter 12 – *Hash* Algorithms.http://vlsi.byblos.lau.edu.lb/classes/csc736/Notes/Lecture12.pdf
11. *DSA*, Hash functions *and HMACs*
12. http://www.cs.rutgers.edu/~vinodg/teaching/spring-2008-cs442/slides/lecture6.pdf.

AUTHOR PROFILE

Ezhil Arasu.S pursuing final year B.E in Computer Science and Engineering in Anna University, Chennai from SNS College of Technology. His area of interests is Cloud Computing.

Gowri.B pursuing final year B.E in Computer Science and Engineering in Anna University, Chennai from SNS College of Technology. Her area of interests is Cloud Computing.

Ananthi S received MCA degree from Bharthidasan university Trichi in 2003 and M.E degree in Computer Science and Engineering from Anna University, Coimbatore. India in 2011. She is at present working as a Assistant Professor in the department of Computer Science and Engineering at SNS College of Technology, Coimbatore, India. Her area of interest include cloud computing and mobile computing