ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 11, November 2014

AN ANALYSIS OF THIRD PARTY AUDITING TECHNIQUES IN CLOUD COMPUTING

Ramya.D[1], Dr.Raja.K[2], Srinivasan.S[3]

P.G Student, Dept of Computer Science and Engineering, Alpha College of Engineering, Chennai, Tamilnadu, India[1]

Dean Academics, Alpha College of Engineering, Chennai, Tamilnadu, India[2]

Research Scholar, Research & Development Center, Bharathiar University,Coimbatore, India &

Associate Professor, Department of M.C.A,K.C.G College of Technology, Chennai, Tamilnadu, India [3]

Abstract: The usage of Cloud computing is increases rapidly in many enterprises. It provides a framework to cloud users. It aims to provide a resource based on-demand. It avoids online usage burden of accessing data through internet. Cloud storage supports to maintain data securely in cloud. To enhance data correctness of cloud, auditing is done by Third Party Auditor (TPA). The TPA can check integrity of data in cloud periodically. During auditing, an auditor does not reveal the information of the user to others. A method that uses the keyed Hash Message Authentication Code (HMAC) with the Homomorphic encryption to enhance the security of TPA.

Keywords: TPA, HMAC, Homomorphic encryption, Security.

I. INTRODUCTION

Cloud computing provides service to the user over the internet. Cloud is interconnected with group of computers, which is used to store information and run their applications in cloud platform. It provides infrastructure, platform and software as services to cloud user. Through cloud computing, we can access any file, document of user from anywhere in the world. Mainly, cloud can be used for cost savings, high scalability and large storage space. But a major issues in cloud computing is security.

II. CLOUD SERVICES

Cloud computing services can be classified into infrastructure as a service (Iaas), platform as a service (PaaS) and software as a service (SaaS).

Infrastructure as a service provides the storage, service and network. By using this service, it is not necessary to buy the server, software and other hardware equipment's for an organization and also it saves the cost of the cloud user. E.g. Amazon web service.

Next service is Platform as a service which is designed for developers which has all facilities to develop any applications. It avoids complexity of the user to purchase and maintain the software and the infrastructure. E.g. Google App Engine.

Finally Software as a service, user can use the software for their own use based on their needs and service provider will license that software. E.g. Gmail.

III. DEPLOYMENT MODEL

Cloud computing deployment model can be classified into three models. They are public, private and hybrid cloud. The physical infrastructure of public cloud is owned and managed by service provider. Resources are dynamically provisioned to user based on-demand through virtualization. The physical infrastructure of private cloud is owned and managed by organization for particular business. Hybrid cloud is the integration of public cloud and private cloud.

IV. DATA IN THE CLOUD

Cloud user who has store and utilize huge amount of data in the cloud. Cloud service provider who manages and maintain information in cloud. The third party auditor who audits the cloud file based on user requests. Auditing is necessary to check the data correctness of detail which is stored in the cloud. Without affecting the client original data, auditing is performed. Cloud service provider will also trust the third party auditor. TPA checks user data in cloud using HMAC. By mapping hash value of user file checks integrity of that data. And Homomorphic encryption is used for security purpose.

The following section (v) and (vi) describes about working functions of Hash based message authentication code and Homomorphic encryption.

V. HMAC

Hash based message authentication code is cryptographic hash function where the message and key are hash them together. By using secret key, we can calculate the hash

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 11, November 2014

function of message authentication code. SHA is a hash algorithm with is used to generate the authentication code for the message. It is used to check the message authentication by using secret key and verify the data integrity. The strength of HMAC is determined by strength of hash function, hash output size and key size. HMAC supports for has algorithms like MD5, SHA-1, SHA-256, etc.

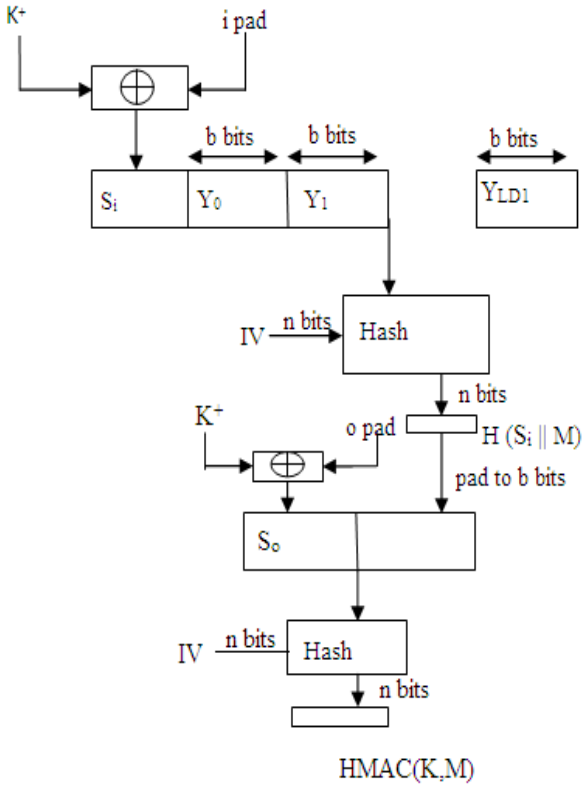

Fig: 5.1 Structure of HMAC

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[1].

The output binary authentication code which equals in the length to that of the hash function digest.

The data integrity of the file is checked by comparing the value of hash function in both user and auditor. In HMAC, the generation of authentication code uses secret and hash based algorithm. This code ensures the usage of hash function is expanded in many places. It conserves the performance of hash function.

VI. HOMOMORPHIC ENCRYPTION

A Homomorphic Encryption system is used to perform operations only on encrypted data not on decryption data. While performing operations, it does not know the users private key. It knows only the users secret key.

While performing the calculation on raw data it should be same as decryption data.

Definition: An encryption is Homomorphic, if: from Enc(a) and Enc(b) it is possible to compute Enc(f (a, b)), where f can be: +, ×, ⊕ and without using the private key. Homomorphic encryption has Additive Homomorphic encryption and multiplicative Homomorphic encryption.

Additive Homomorphic encryption is the Pailler[2] and multiplicative Homomorphic encryption is the RSA[3] and ElGammal cryptosystems[4].

For calculating any calculation in the cloud fully Homomorphic encryption is used based on encrypted data not on decrypted data. Fully Homomorphic encryption is an important for cloud for providing Cloud Computing security and keeps the data more confidential. Decryption is also based on client secret key.

By working with cloud server uses virtual platform ESX and a VPN network that links to the client. By simulating different scenarios using the Computer Algebra System Magma tools[5].

It focusing on

- The size of the public key and its impact on the size of the encrypted message.
- The server delay of the request treatment according to the size of the encrypted message.
- The result decrypting time of the request according to the cipher text size sent by the server.

VII. CONCLUSION

Third party auditor is used to detect modification of file during auditing time. It is used to reduce online burden of users. For security purpose TPA uses HMAC and Homomorphic algorithm for encrypt the user data. HMAC uses hash value for checking user original file with cloud stored file. And fully Homomorphic encryption used for data confidentiality. Future enhancement of this paper is to check integrity verification of cloud using dynamic audit protocol.

ACKNOWLEDGMENT

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

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 11, November 2014

REFERENCES

[1] Cryptography and Network Security Chapter 12 – Hash Algorithms.http://vlsi.byblos.lau.edu.lb/classes/csc736/Notes/Lecture 12.pdf

[2] Pascal Paillier. Public-key cryptosystems based on composite degree residuosity classes. In 18th Annual Eurocrypt Conference (EUROCRYPT'99), Prague, Czech Republic , volume 1592, 1999.

[3] R. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public key cryptosystems. Communications of the ACM, 21(2) :120-126, 1978. Computer Science, pages 223-238. Springer, 1999.

[4] TaherElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transactions on Information Theory, 469-472, 1985.

[5] WiebBosma, John Cannon, and Catherine Playoust. The Magma algebra system I: The user language. J. Symbolic Comput., 24(3-4): 235-265, 1997. Computational algebra and number theory, London, 1993.

[6] 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.

[7] Y. Zhu,Z. Hu,Gail-J Ahn, H. Hu,Stephen S. Yau, Fellow, IEEE, Ho G. An, and ShiminChen,"Dynamic Audit Services for Integrity Verification of Outsourced Storages in Clouds",inProc.of IEEE SAC"11 March 2011.

[8] Q. Wang, C. Wang, KuiRen, 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.

[9] MuralikrishnanRamane and BharathElangovan, "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.

[10] Dalia Attas and Omar Batrafi "Efficient integrity checking technique for securing client data in cloud computing", October 2011.

[11] 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.

[12] Ronald L. Rivest, Leonard Adleman, and Michael L. Dertouzos. On Data Banks and Privacy Homomorphisms, chapter On Data Banks and Privacy Homomorphisms, pages 169-180. Academic Press, 1978.