IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

A Survey paper on Public Integrity Auditing for Shared Dynamic Cloud Data Using HMAC Algorithm

Prof. Sunita Patil[1], Prof. Supriya Bhosale[2], Prof. Shubhangi Sonawane[3]

Asst. Prof, Department of IT, DYPCOE, Talegaon, India[1,2,3]

Abstract: This paper presents various disputes associated with public Auditing and security for storing user's data on untrusted cloud. There is a huge amount of research being made to discover the disputes with these cloud service providers and cloud security. In this paper system proposes a HMAC algorithm to enhanced public integrity auditing Shared Dynamic Cloud Data. Typically message authentication code is used in between sender and receiver that share secrete key in order to authenticate information transmitted between this parties. This standard defines a MAC that uses a cryptographic hash function in conjunction with a secret key in order to authenticate information transmitted between these parties. The main goal of this paper is to proposal a secure and an effective cloud data storage system to decrease the bandwidth and to increase the data integrity. The key is part of HMAC, since it is shared secrete known between two parties only and only they can create .The main intention of these is to overcome the length extension attack and to protect the original performance of the hash function without incurring a significant degradation.

Keywords: Cloud Computing; Hash Message Authentication Code (HMAC); Message Authentication Code (MAC); integrity.

I. INTRODUCTION

Cloud Computing delivers us a means by which we can contact the applications as services, over the Internet. It permits us to generate, configure, and modify applications online With Cloud Computing users can contact database resources via the internet from anywhere for as long as they want without worrying about any repairs or management of actual resources.

A. Basic Concept

The term Cloud denotes to a Network or Internet. In further words, we can say that Cloud is something, which is existing at remote location. Cloud can deliver services over network, i.e., on public networks or on private networks. There are four types of cloud as following [1]

- Public Cloud: The Public Cloud permits systems and services to be simply accessible to the general public. Public cloud may be less secure because of its openness.
- Private Cloud: The Private Cloud permits systems and services to be accessible within an organization. It offers improved security because of its private nature.
- Community Cloud: The Community Cloudpermits systems and services to be accessible by group of organizations.
- Hybrid Cloud: The Hybrid Cloud is combination of public and private cloud. However, the serious activities are performed using private cloud while the non-critical activities are performed using public cloud.

B. Advantages and Disadvantages of Cloud Computing:

➢ Advantages:-

- Lower computer costs
- Improved performance
- Reduced software costs
- Instant software updates
- Improved document format compatibility
- Unlimited storage capacity
- Increased data reliability
- Universal document access
- Latest version availability
- Easier group collaboration
- Device independence

➢ Disadvantages:-

- Requires a constant Internet connection
- Does not work well with low-speed connections
- Features might be limited
- Can be slow
- Stored data can be lost
- Stored data might not be secure

II. LITERATURE SURVEY

[1]" New Public Integrity Auditing Scheme for Cloud Data Storage Using Mac And Symmetric Key Cryptographic Algorithms"

IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

Extracting idea for Dissertation: - From this paper propose system uses public integrity auditing mechanism with the help of Message Authentication Code (MAC) generation and symmetric cryptographic techniques. The main intention of this paper is to design a secure and an efficient cloud data storage system to reduce the bandwidth and to improve the data integrity.

[2]"Public Integrity Auditing for Shared Dynamic Cloud Data with Group User Revocation"

Extracting idea for Dissertation: -From this paper proposed system referred we figure out the collusion attack in the exiting scheme and provide an efficient public integrity auditing scheme with secure group user revocation based on vector commitment and verifier-local revocation group signature. We design a concrete scheme based on the our scheme definition. Our scheme supports the public checking and efficient user revocation and also some nice properties, such as confidently, efficiency and traceability of secure group user revocation. Finally, the security and experimental analysis show that, compared with its relevant schemes our scheme is also secure and efficient.

[3] "Group User Revocation and Integrity Auditing of Shared Data in Cloud Environment"

Extracting idea for Dissertation: - From this paper proposed system referred concept of auditing the integrity of shared data with dynamic groups in cloud. A new user can be added into the group and an existing group member can be revoked by preserving privacy including data backup based on vector commitment and verifier-local revocation group signature. This scheme supports the public validation and efficient user revocation.

[4] "A Review on Cryptographic Hashing Algorithms for Message Authentication"

Extracting idea for Dissertation: - HMAC is an improvisation of NMAC and is more secure. But on the other hand, HMAC is much slower than NMAC. Also, NMAC involves the use of two keys whereas HMAC involves the use of a single key.

III.PROPOSED SOLUTION

The major function of the paper is to solve the challenges presented above. In this paper, the problem of designing public integrity auditing based shared dynamic data with group user revocation is analysed. The main goal of this paper is to proposal a secure and an effective cloud data storage system to decrease the bandwidth and to increase the data integrity.

The key is part of HMAC, since it is shared secrete known between two parties only and only they can create .An efficient and secure public integrity auditing scheme is proposed for cipher-text base with the help of multi-user operation. The main intention of these is to overcome the length extension attack. In cryptography a length extension attack is a type of attack where an attacker can use Hash (message1) and the length of message1 to calculate Hash (message1 ‖ message2) for an attacker-controlled message2.

This attack can be done on hashes with construction H(secret ‖ message)[1] when message and the length of secret is known. Since HMAC doesn't use the construction H(key ‖ message), HMAC hashes are not prone to length extension attacks.

IV.HMAC ALGORITHM STRATEGY

For implementation HMAC Algorithm is used. The detail strategy of algorithm is as following.

A) Basic Concept:-

As shown in Fig.1 for generation of HMAC it is required that there must be message and secrete key. When message and secrete key gets combined it produce Hash H and then create HMAC. Then sender transmits message and HMAC to the receiver.

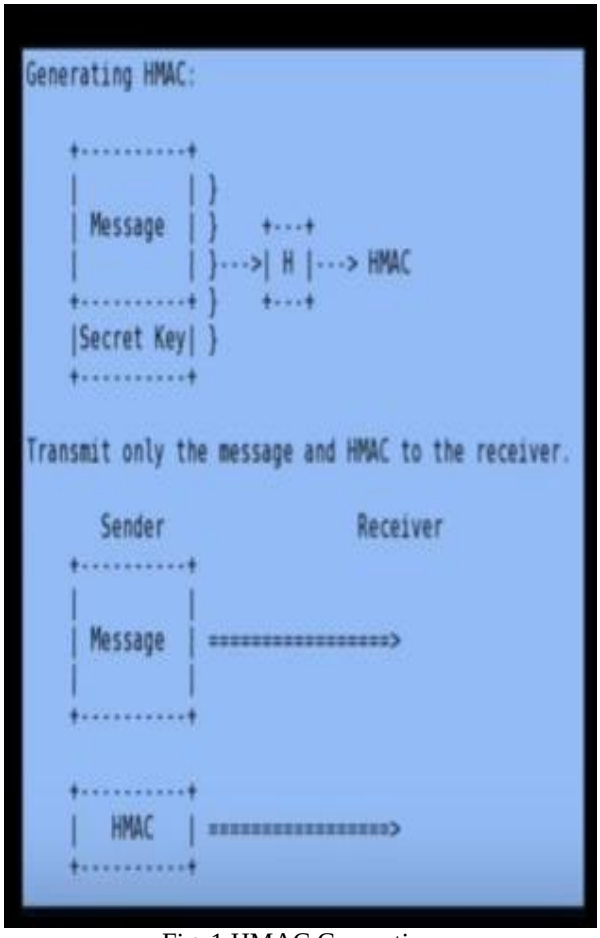

Fig. 1 HMAC Generation

IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

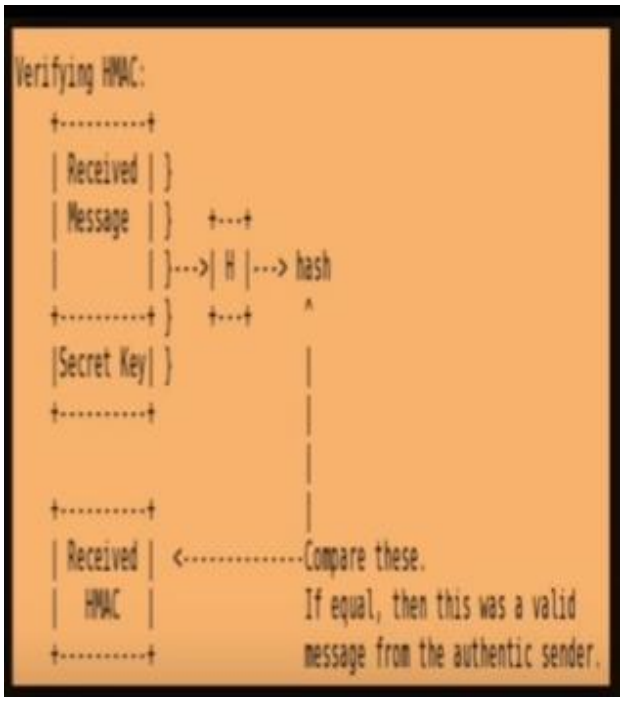

Fig.2 Verification of HMAC

As shown in Fig.2 on receiver site when receiver receive message it will calculate Hash H from HMAC of it with it own secrete key. This secrete key must be known between sender and receiver. Once it is calculated it is compared received HMAC with Hash H. If it is equal then it is valid message form authentic sender. It means there is no alteration for this message

B) HMAC Algorithm:-
HMAC Parameters and Symbols
B - Block size (in bytes) of the input to the Approved hash function.
H - An Approved hash function.
ipad - Inner pad; the byte x‘36’ repeated B times.
K - Secret key shared between the originator and the intended receiver(s).
K0 - The key K after any necessary pre-processing to form a B byte key.
L - Block size (in bytes) of the output of the Approved hash function.
opad - Outer pad; the byte x‘5c’ repeated B times.
text - The data on which the HMAC is calculated; text does not include the padded key. The length of text is n bits, where $0 \leq n < 2^B - 8B$.
x ‘N’ - Hexadecimal notation, where each symbol in the string ‘N’ represents 4 binary bits.

C) HMAC specification:-
To compute a MAC over the data ‘text’ using the HMAC function, the following operation is performed:
MAC(text) = HMAC(K, text) = H((K0⊕opad)|| H((K0 ⊕ipad) || text))

Step by step process in the HMAC algorithm.

- Step 1. If the length of K = B: set K0 = 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 K0 (i.e., K0 = H(K) || 00...00). Go to step 4.
- Step 3. If the length of K < B: append zeros to the end of K to create a B-byte string K0 (e.g., if K is 20 bytes in length and B = 64, then K will be appended with 44 zero bytes x’00’).
- Step 4. Exclusive-Or K0 with ipad to produce a B-byte string: K0 ⊕ipad .
- Step 5. Append the stream of data 'text' to the string resulting from step 4: (K0 ⊕ipad) || text
- Step 6. Apply H to the stream generated in step 5: H ((K0 ⊕ipad) || text) .
- Step 7. Exclusive-Or K0 with opad: K0 ⊕opad
- Step 8. Append the result from step 6 to step 7: (K0⊕opad) || H ((K0 ⊕ipad) || text).
- Step 9. Apply H to the result from step 8: H((K0 ⊕opad) || H((K0 ⊕ipad) || text)).

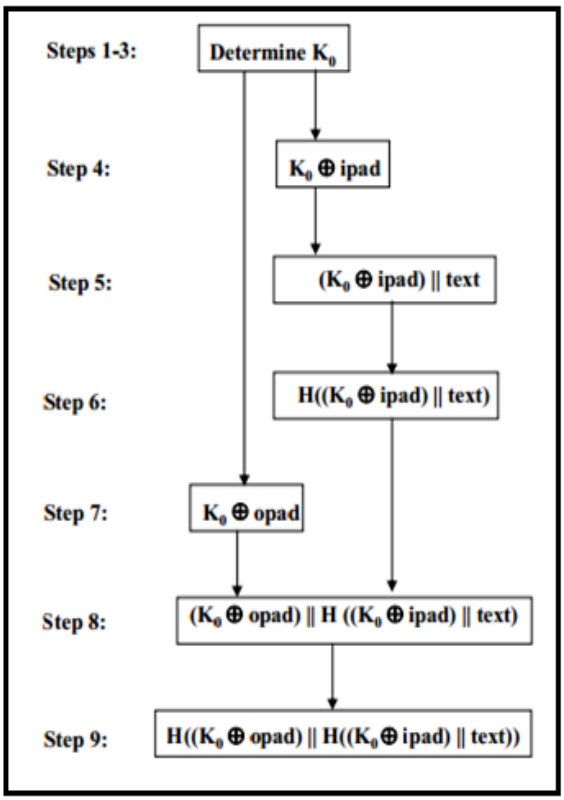

Fig.3 HMAC Algorithm

V. SYSTEM ARCHITECTURE

In this architecture, the two different algorithms such as, HMAC algorithm is used for code generation and the symmetric key cryptography algorithm is used for encryption and decryption.

Initially the hash key is created for the user input and the block of the data is encrypted. Consequently, the hash key is also encrypted and the file is uploaded in the cloud. If the data is already exists, it is identified that the upload file

IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

is duplicated. Otherwise, it will divided into various blocks, after that the availability of the blocks is also verified. If the block is not exists, it will be given to the Cloud Service Provider (CSP). Hence, the file is downloaded from the server and to access that file, the hash key and data blocks are need to be decrypted. After successful creation of cloud setup, users need to get registered with the system through user registration process. During registration process users need to fill their personal information such as user Name, Emailed etc. but the system guarantees Identity privacy. User has to browse file for uploading. Before uploading files, Data Owner assigns File ID to selected data files.

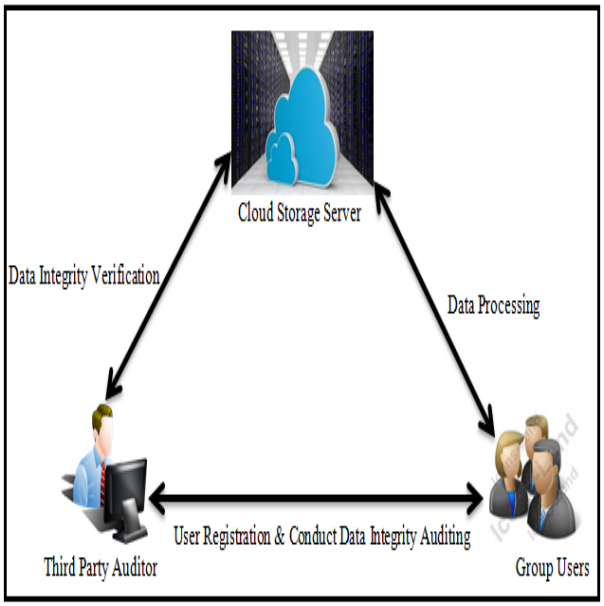

Fig.4 System Architecture

Fig.4 shows the system architecture, where the three different units are used such as, cloud storage server, group user and a Third Party Auditor (TPA).

- Group User: - The group users have, who have an access to change the data.
- Cloud Storage Server: - The cloud storage server is semi-trusted that delivers the data storage services to group users.
- Third Party Auditor:-The TPA can be any entity in the cloud that conducts the data integrity in the cloud server.

In this proposed system architecture, the data owner can encrypt and upload its data in the remote cloud storage server. Also, the cloud service provider achieves an originality organization to deliver a secure, reliable and scalable atmosphere to user. When a group of user is initiate as malicious or expired, the data owner can securely revoke a group of user. Hence, it is difference from other group of users. Here, the TPA can expertly verify the data integrity in the storage server.

VI. CONCLUSION

The main goal of this paper is to proposal a secure and an effective cloud data storage system to decrease the bandwidth and to increase the data integrity. This paper proposed a new public integrity auditing scheme for cloud data storage using HMAC Algorithm. The key is part of HMAC, since it is shared secrete known between two parties only and only they can create .The main intention of these is to overcome the length extension attack and to protect the original performance of the hash function without incurring a significant degradation. HMAC is much faster to compute. Also, HMAC might still be secure, even if the underlying hash function is broken. From this analysis, it is observed that the proposed system provides the better results. Extensive studies show that proposed scheme satisfies the desired security necessities and assurances efficiency, security and scalability as well.

ACKNOWLEDGMENT

I would like to express my gratitude to all those who gave me the possibility to complete this project. I deeply indebted to my friends whose help, stimulating suggestion and encouragement helped me in the all-time.

REFERENCES

[1] Ms. A. Emily Jenifer, Ms. S. Karthigaiveni " New Public Integrity Auditing Scheme for Cloud Data Storage Using Mac And Symmetric Key Cryptographic Algorithms"IJAER,ISSN 0973-4562, Vol.11 No. 3.
[2] Tao Jiang Xiaofeng Chen and Jianfeng Ma, "Public Integrity Auditing for Shared Dynamic Cloud Data with Group User Revocation" IEEE Transactions On Computers, Vol. 65, No. 8, August 2016 .
[3] PushkarZagade,"Group User Revocation and Integrity Auditing of Shared Data in Cloud Environment" International Journal of Computer Applications (0975 – 8887) Volume 128 – No.12, October 2015
[4] NishantSahani,"A Review on Cryptographic Hashing Algorithms for Message Authentication" International Journal of Computer Applications (0975 – 8887) Volume 120 – No.16, June 2015.
[5] S. Kamara and K. Lauter, "Cryptographic cloud storage, " in Financial Cryptography and Data Security, ed: Springer, 2010, pp. 136-149.
[6] Xuefeng Liu, Yuqing Zhang, Boyang Wang, and Jingbo Yan. 2013, Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud, IEEE Transactions On Parallel And Distributed Systems, Vol. 24, No. 6.
[7] 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, 2010, A View of Cloud Computing, Comm. ACM, vol. 53, no. 4, pp. 50-58.
[8] A. E. C. Cloud, "Simple Storage Service, " ed
[9] http://cryptowiki.net/,"The framework for identification protocols".
[10] R. Gennaro, C. Gentry, and B. Parno, "Non-interactive verifiable computing: Outsourcing computation to untrusted workers, " in Advances in Cryptology–CRYPTO 2010, ed: Springer, 2010, pp. 465-482.
[11] Z. Hao, S. Zhong, and N. Yu, "A privacy-preserving remote data integrity checking protocol with data dynamics and public verifiability, " IEEE transactions on Knowledge and Data Engineering, vol. 23, pp. 1432-1437, 2011.
[12] "hmac tutorial" , ZarigaTongy.