ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

Security Enhancement Using Homomorphic Encryption in Cloud Computing

Thomas P Noel[1], Caroline Mary.A[2]

Department of Computer Technology, Sri Krishna Arts and Science College, Coimbatore, India

ABSTRACT*:* Using cloud storage, user can store their data efficiently and the sharing of data is also important task in the cloud computing. Moreover, data owner and user check the integrity of data in the cloud server. Accordingly, this schema presents an efficient data and signature verification based on the cryptographic domain. Homomorphic algorithm is introduced in this paper for data integrity and verification process. In the server side, MD5, Homomorphic algorithm is used whereas in Client side MD5 and Homomorphic algorithm is used. First, MD5 algorithm is used to encrypt the original data; Homomorphic algorithm is used both for encryption and decryption in server and client side.The main idea is that one can aggregate any set of secret keys and make them as compact as a single key, but all keys should be aggregated. In other words, the secret key holder can release a fixed-size aggregate key for convenient choices of cipher text set in cloud storage, but the other encrypted files outside the set remain confidential. We can share the data efficiently and securely .The proposed method Homomorphic algorithm with DES provides better result than the existing method.

I. INTRODUCTION

Cloud computing is one of the important technologies where data owner belongs to the cloud service provider providing computing resources to their customers to protect or host their data. In cloud computing several types of services deliver models are available like: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) [1-3].

For internet purpose it is one of the efficient techniques, cloud gives very effective challenging techniques it is useful for protect the security [4]. But Even though there is some problem in cloud computing is data integrity due to several reasons is; cloud computing user loosed their data; failure of software and hardware parts in cloud computing service [5].

Cloud computing is one of the new technology it provides various advantage to the user.With the help of this cloud computing, user utilize the data and the storage tasks to the cloud servers [6]. Private Key is used in cloud computing process, in server side the signature is generated with the helpof private key; it is useful for storing the data as well as for verification purpose [7-8].

The problem of data integrity and data verification is handled through Homomorphic Encryption. The data is given by data owner A and it is verified in client side through encryption and decryption algorithm [9]. First the data is encrypted through MD5 and it gives HASH value and again it encrypted through Homomorphic encryption algorithm and produced signature in the server side. In client side produced signature is decrypted through Homomorphic algorithm and the given data is encrypted through MD5 algorithm.

II. LITERATURE SURVEY

(Rahul Bhatnagar et al., 2013) [10] Proposed technical components for security in cloud computing. The author provide more security topics for standardized cloud security, the related topics are e. Storage Security, Data and Privacy Protection, Virtualization Security, Security Architecture/Model and Framework, Security Management and Audit Technology.

(Anjana et al., 2013) [12] Proposed some important security services including key generation, encryption and decryption are provided in Cloud Computing system. Here author improved the security through RSA algorithm. Here the TPA is the trusted entity that has expertise and capabilities to assess cloud storage security on behalf of a data owner upon request. The main aim of these techniques to improve the security through RSA algorithm and the data is access through authorized person only.

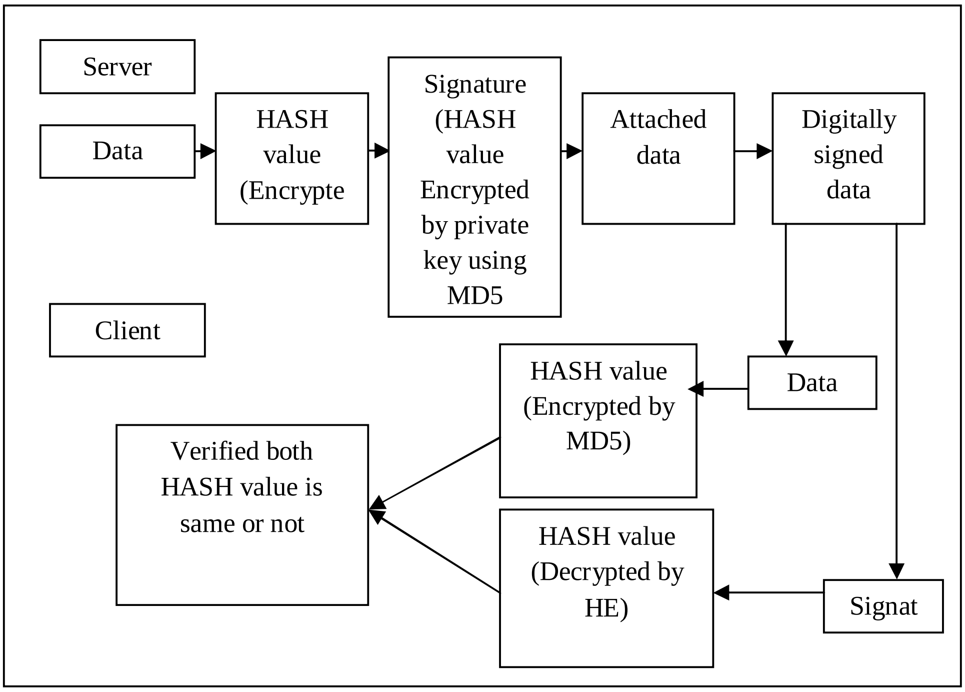
DOI: 10.15680/IJIRCCE.2016. 0409145

Faraz et al., 2013) [11] proposed a hybrid method for increase the security and reliability in cloud server with least execution time and cost for both encryption and decryption. This method uses Hybrid Encryption based on the strengths of Efficient RSAand RSA Small-e (HE-RSA). In this technique, dual encryption technique is used for increasing the security level of cloud computing.

Cloud computing is used in many web applications because of its flexible nature. In cloud computing security level is high, even though some threats are taken place. To overcome this, (Saravanan et al., 2012) [13] implement the method for providing security by implementingRSA algorithm using cloud SQL to the data that will be stored in the third party area.

III. METHODOLOGY

The proposed system consists of two phase that in server side and client side. In server side; first Generate HASH value using MD5.MD5 generate the digital signature using Homomorphic algorithm and finally obtained digital signature and their respective public key is given to client side. Figure 1 illustrates the block diagram of proposed system.


Server
Data
HASH value (Encrypte
Signature (HASH value Encrypted by private key using MD5
Attached data
Digitally signed data
Client
HASH value (Encrypted by MD5)
Data
Verified both HASH value is same or not
HASH value (Decrypted by HE)
Signat

A. SERVER SIDE:

1. Message digest 5:

MD5 is used to encrypt the original data. MD5 is the improved version of MD4. MD5 is used to produce 128-bit hash value for the original data. It divides the input data into 16 32 bit sub blocks. Then finally it forms 32-bit blocks, then it concatenate into single 128 bit hash value. First the message is padded, it is single 1-bit and it is combined to the end of the message simultaneously followed by many zeros. Initialized four 32 bit variables are

$A = 0x01234567, B = 0x9abcdef, C = 0xfedcba98 \; and \; D = 0x76543210.$

The above variable A, B, C and D are called as chaining variables. First MD5 algorithm starts with 512-bit blocks in their message. The four variables are copied into different variables such as a gets A, b gets B, c gets C and d gets D. the main loop in this MD5 algorithm contains four rounds, and each rounds contains several 16 operations. Nonlinear function is performed by each operation on three variables and it adds the result to the fourth variable, a sub block of text and constant. Then the result is rotated to the right and adds the number of bits to any one of the variable and finally replace the result to any one of the given variable.

$L(T,U,V) = (T \wedge U) \vee (-T \wedge V)$ (2)
$M(T,U,V) = (T \wedge V) \vee (U \wedge -V)$ (3)
$N(T,U,V) = T \oplus U \oplus V$ (4)
$O(T,U,V) = U \oplus (T \vee -V)$ (5)

The above equations denotes four nonlinear functions and their four operations are $\oplus$ performs XOR function, $\wedge$ performs AND function, $\vee$ performs OR operation and – performs NOT function.

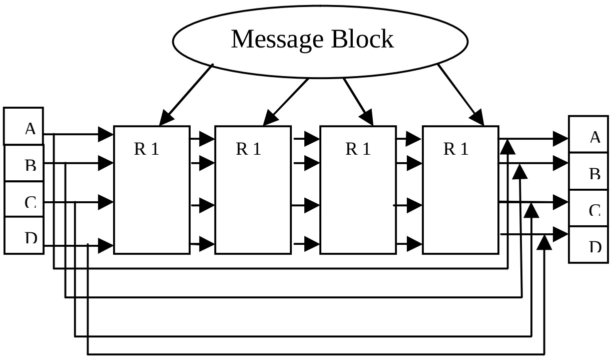


Figure 2: MD5 Main Loop

2. *Homomorphic Encryption and Decryption algorithm:*

This function takes complex mathematical operation for data encryption without revealing the content of the original data. Consider two plaintexts P and P2 and C1 & C2 are their corresponding Ciphertext, HE allows computation of P1ΘP2 from C1 and C2 without revealing P1 or P2. This function is based on addition or multiplication and it is based on the functionΘ.HE consists of three algorithms such as key generation, encryption, and decryption and evaluate.

Key Generation λ:
Step 1: Given a security parameter λ as an input.
Step 2: output is consisting of secret key sk and public keypk.
Encryption(pk, π):
Step 1: Public key pk and a plain text π are given as an input.
Step 2: Output Cipher text ψ.
Decryption(sk, ψ).
Step 1: Input-a secret keysk and a Ciphertextψ.
Step 2: corresponding plaintext π is obtained in output.
Evaluate(pk, C, ψ):
Step 1: Input a public key pk, a circuit C with t inputs and a setψ of t Ciphertext $\psi_1, \ldots, \psi_2$.
Step 2: Output-a Ciphertextψ.

B. CLIENT SIDE:

Step 1: In the client side, the combination of data and the signature is send by the data owner A to the client user B.
Step 2: Separate the data and signature from server side.

Step 3: Data is again encrypted through MD5 algorithm and hash value is produced.
Step 4: Signature is decrypted through Homomorphic algorithm
Step 6: Obtained both HASH value from Homomorphic algorithm and MD5 algorithm are checked whether it is equal or not.
Step 7: If it satisfies the condition then client side gets the original data send by data owner or server side.

IV. EXPERIMENTAL RESULTS

In this paper, experimental results are evaluated by comparing the proposed method of Homomorphic algorithm and DES with based storage system through performance metrics such as throughput, Encryption time, Decryption time, total execution time, memory utilization and cost. The experimental results are carried through cloudsim platform.

Comparison of Homomorphic algorithm And DES with existing algorithm

Performance Metrics	DES	HE
Throughput (ms)	20	50
Encryption time (ms)	1000	500
Decryption time (ms)	500	250
Total Execution time (ms)	1500	750
Memory (MB)	250	100
Cost	HIGH	LOW

The above table gives the description about the comparison between Homomorphic algorithms with DES with existing algorithm.From the table clearly observed that the DES with HE method provides better result than DES with SEC method through performance metrics.

V. CONCLUSION

There are two process are happen in this paper are in server and client side. First the data is encrypted by using MD5 and produces HASH value, again this HASH value is encrypted by Homomorphic algorithm and produces signature in server side. In the verification process, the given data is encrypted by MD5 and the signature is decrypted by Homomorphic algorithm and verified whether both HASH values are equivalent or not. Through this encryption and decryption methods, it increases the security level of both the client and the data owner.

REFERENCES

[1] L. Youseff, M. Butrico, and D. Da Silva,
"Towards a unified ontology of cloud computing," in Proc. 2008 Grid Computing Environments Workshop.
[2] Amazon Inc., "Amazon elastic compute cloud (Amazon EC2)," 2011. Available: http://aws.amazon.com/ec2/
[3] "Windows Azure." Available: http://www.windowsazure.com/en-us/.
[4] Qian Wang, Cong Wang, Kui Ren, Wenjing Lou and Jin L, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing", IEEE transactions on parallel and distributed systems, vol. 22, no. 5, may 2011
[5] TAN Shuang, TAN Lin, LI Xiaoling and JIA Yan, "An Efficient Method for Checking the Integrity of Data in the Cloud", China Communications • September 2014.
[6] M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, M. Zaharia, Above the cloud: a Berkeley view of cloud computing, Berkeley University, 2009.
[7] H. Shacham and B. Waters, "Compact proofs of retrievability," in Proc. of ASIACRYPT'08. Springer-Verlag, 2008, pp. 90–107.

[8] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, “Provable data possession at untrusted stores,” in Proc. of CCS’07. New York, NY, USA: ACM, 2007, pp. 598–609.

[9] A. Juels and B. S. Kaliski, Jr., “Pors: proofs of retrievability for large files,” in Proc. of CCS’07. New York, NY, USA: ACM, 2007, pp. 584–597.

[10]Rahul Bhatnagar, SuyashRaizada, PramodSaxena, SECURITY IN CLOUD COMPUTING,International Journal For Technological Research In Engineering, ISSN (Online) : 2347 4718, December – 2013.

[11]AnjanaChaudhary,Ravinder and Manish “A Review: Data Security Approach in Cloud computing by using RSA Algorithm”, International Journal of Advance Research in Computer Science and Management Studies, Volume 1, Issue 7, December 2013.

[12]N. Saravanan, A. Mahendiran, N. Venkata Subramanian and N. Sairam, “An Implementation of RSA Algorithm in Google Cloud using Cloud SQL”,Research Journal of Applied Sciences, Engineering and Technology 4(19): 3574-3579, 2012.

[13]FarazFatemiMoghaddam, Maen T. Alrashdan, and OmidrezaKarimi, “A Hybrid Encryption Algorithm Based on RSA Small-e and Efficient-RSA for Cloud Computing Environments

BIOGRAPHY

THOMAS P NOEL is a MS.c student in the computer Technology Department, Sri Krishna Arts and Science college. My research interests are Computer Networks , cloud computing.

CAROLINE MARY.A is an Assistant professor in Computer Technology Department, Sri Krishna Arts and Science college. My research interests in Cryptography and Network security.