International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 10 (2018) pp. 7388-7391


# Increase Security of Data With Respect to Both Confidentiality and Integrity over Cloud

**Rubal Deep Gill**
*Assitant Professor, Departement of Computer Science, SKIT, M&G, India.*

**Neha Kapur**
*(Ex)Asst. Professor, Departement of Information Technology, SKIT, M&G, India.*

**Harpreet Singh Gill**
*Asst. Professor, Departement of Computer Science, SKIT, M&G, India.*

**Abstract**

The main purpose of security architecture is to maintain system's policy, confidentiality, availability, integrity, accountability and assurance. Cloud computing is a platform of delivering information from computing power to computing infrastructure, business process, application, storage and personal collaboration to an end-user as a service whenever they require it. The correctness of data and security of Cloud Computing Systems is a significant concern to organizations and industry. The main goals of security procedures are to provide practical effort of securing the cloud data, platform and application as well as to provide an secure environment for cloud-end users. Authentication, data integrity and confidentiality are the major issues in cloud computing security.

In this paper, our core concern is to provide solutions for these aspects. Third party can misuse and waste the cloud resources. He/she can capture the data and then modify, update or delete it. A user can rely on a trusted cloud auditor to check for the authentication and integrity of his/her data and make that data confidential. For this, we apply a strong cryptographic hash function (SHA-2) on a plain-text message along with shared variable. Our proposed scheme is used to generate the shared variable. Confidentiality of the data is provided by AES symmetric block cipher encryption

## INTRODUCTION

**C**loud is computing infrastructure which serves the need of computing of business or individuals by providing resources on sharing basis. It is a way to access reliable computing resources like networks, servers, memory and other services etc. It provides low cost services, scalability, high level of abstraction and security, thus improving business process and efficiency of business [1],[2].

Three types of services are provided by cloud:-

a) Software as a Service (SaaS) : it is a model which provides Software or application as a service to the user that is available on cloud [3].
b) *Platform as a service (PaaS)*: it is a model in which user can deploy his/her applications on platform like system software, middleware, operating system or database etc. provided by cloud [4].
c) *Infrastructure as a Service (Iaas):* this model provides infrastructure of cloud like storage space, network and server capacity etc. to the end user on rental basis for increasing organization capabilities [3],[5].

Security services enhance the security of information/data of the system being transferred over the cloud in terms of authentication, access control, confidentiality, data integrity and provide specific kind of protection to the resources. Authentication ensures that the communication between the parties is authentic and both the parties are valid. Confidentiality provides the security of a message. Data integrity assures that there is no modification in data transferred between the sender and the receiver. There are different challenges regarding security over cloud.

- Data integrity
- Data confidentiality
- Authentication
- Trustworthy cloud service provider

Cloud server providers (CSP) run the cloud software that provides the services to the cloud end-user through network access. Service deployment, service management, security and privacy are the main activity areas for cloud service provider, thus requires Trustworthy cloud service provider. There are many reasons why CSPs are not always trustworthy like, for saving money and storage space, CSPs may discard the data that has not been accessed for long time (which belongs to ordinary client) or sometimes even hide data losses or corruptions to maintain a reputation.
Cloud auditor is a main actor that plays a vital role in cloud computing security. Security audit makes an assessment of the security controls in the information system as well as verification of the compliance with regulation and security policy

## PROPOSED WORK

We want to provide authentication, data integrity and confidentiality to data on cloud. So we follow given approach:

- A approach that is based on Diffie-Hellman key exchange algorithm- is used to share random variable (S_Var) which is known to both end-user and auditor. It also provides entity authentication to both [6].
- A symmetric key cryptographic algorithm Advance Encryption Standard (AES) is used to generate cipher text .
- Secure Hashing Algorithm (SHA-2) is used to generate a message digest by passing the original message along with shared variable (S_Var) to the hash function. This is done by both the end- user and the auditor and the value obtained from the hash function is compared and hence the data integrity is verified.

The following steps are used for creating shared variables:

Both end-users share two variable f1, f2.

i. User A creates a random no α and calculate $(f1)^{\alpha}$ mod (f1-1)(f2-1) and send it to second communicating party B.

ii. B creates a random no β and calculate $(f1)^{\beta}$ mod(f1-1) (f2-1) and send this calculated value to A.

iii. Then user A calculate:

$$S\_Var1 = ((f1)^{\beta} \bmod (f1-1)(f2-1))^{\alpha} \bmod (f1-1)(f2-1)$$

iv. Then user B calculate:

$$S\_Var2 = ((f1)^{\alpha} \bmod (f1-1)(f2-1))^{\beta} \bmod (f1-1)(f2-1)$$

So in this way, both users share a number.

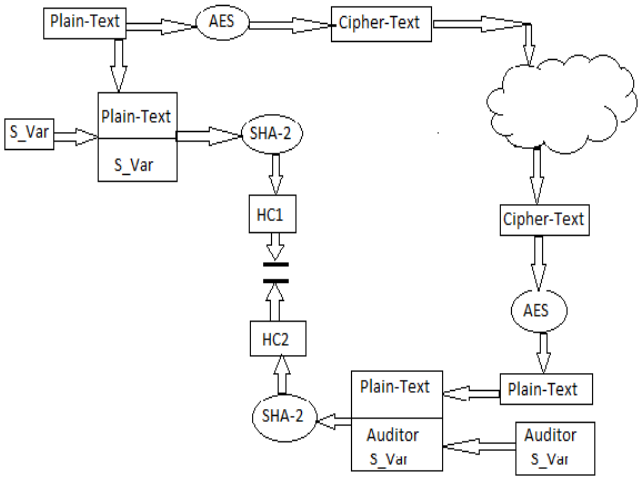


**Figure 1:** Methodology

Our approach has the following steps according to Fig 1:

1. A shared variable (S_Var) is generated using above described approach that is known to both end-users and cloud service auditor.
2. Now, Plain-text is encrypted using symmetric cryptographic algorithm-Advance Encryption Standard (AES) and the corresponding cipher text is stored on cloud.
3. S_Var is appended with plain-text and a hash function SHA-2 is applied on it, resultant hash code (HC1) is send to auditor. This step provides authentications to both end-user.
4. The Cipher-text is fetched by auditor from cloud. This cipher-text is decrypted using the decryption algorithm and generate the plain text.
5. This generated plain text is appended with S_Var and apply same hash function on it and generates the hash code (HC2).
6. The comparison between these two hash codes provides the following results-
   a) if HC1 = HC2, this concludes that plain-text has not been changed during transit and plain-text indeed came from the authorized person.
   b) if HC1 ≠ HC2, means plain-text has been changed.

### Algorithms used in this work :

***a.*** **SHA-*2***

SHA-2 (Secure Hash Algorithm) is one of a number of **cryptographic hash functions** with digest length of 256 bits, generates an almost-unique, fixed size 256-bit (32-byte) hash. A message is processed by blocks of 512 = 16×32 bits, each block requiring 64 rounds [7].

### Algorithm structure of SHA-2

*Step 1: Padding bits:* Padding bits(1 and 0)are added to make the length of message equals to the value that is 64 bits less than the exact multiple of 512.

*Step 2: Appending length as 64 bit unsigned:* The length of the original message is added to the message after the padding bits in the form of 64 bits. After that the final message (exact multiple of 512 bits) is divided into blocks of 512 bits.

*Step 3: Buffer initiation*: Here 8 Chaining variables A-H (works as buffer) are used those are specified in [8], each of size 32 bits are used to store the intermediate and final results of 256 bits (hash code) of the whole process.

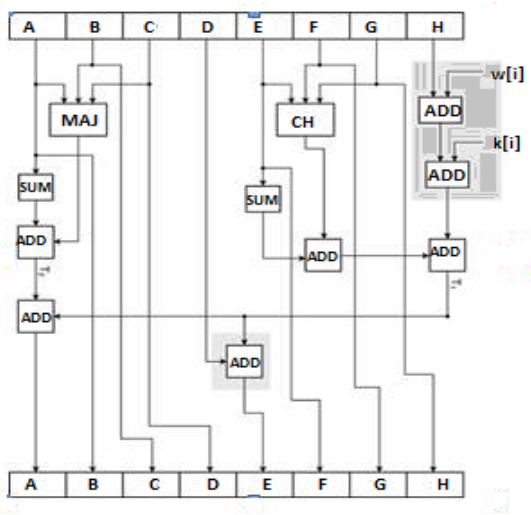


**Figure 2:** Single iteration of SHA-2

*Step 4: Processing of message:* current 512 bit block is divided into 16 sub-blocks (W[i]) of 32 bits. There are total 64 rounds, each round takes A-H variables and sub-block (W[i]) as a input and performs the operation according to fig. 2 [8].

*Step 5: Output:* After the execution of 64$^{th}$ round, A-H variables generates the 256- bits hash code as a output.

### b. Advance Encryption Standard (AES)

AES takes 128-bit plain-text and generate 128-bit cipher-text using symmetric key. Key size may be 128,192 or 256-bits. if the key size used is 128-bits then the number of rounds is 10 whereas it is 12 and 14 for 192 and 256-bits respectively.

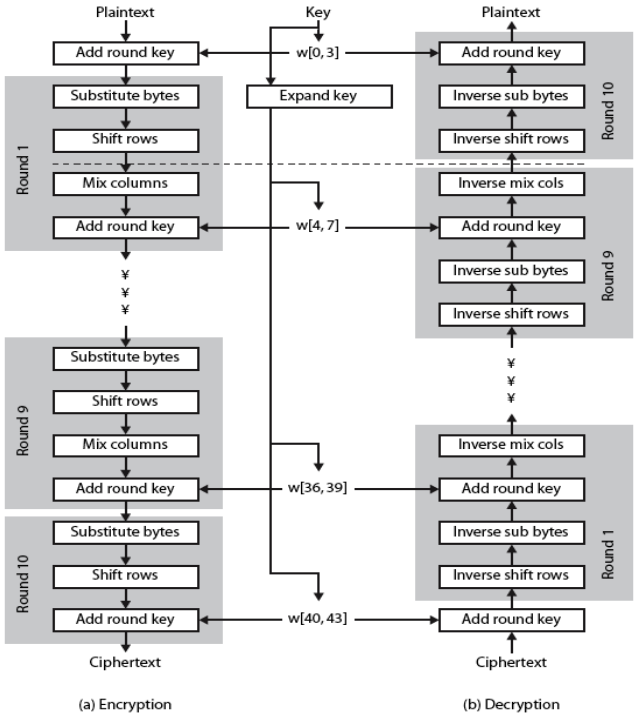


**Figure 3:** Working of AES

1. According to fig 3, Perform the following one-time initialization process which includes given steps-
   a. *Key Expansion* – This step expands the 16-byte (128-bit) key into 11 array (176 byte) to get the actual key block. Each array is two dimensional 4 x 4 array. First array of expanded key is only used in one-time initialization process and other arrays are used in 10 rounds.
   b. *Perform one-time initialization* - 16-byte plain-text is stored into a 2-D 4x4 array. This array is known as state.
   c. *Perform XOR operation* – First array is key block of expanded key is XORed with state, resultant array is again stored in state array.
2. Each round consist of broad level of given steps-
   a. *S-box substitution* - S-box substitution is applied to each of plain-text.
   b. *Circular–left Rotation* – Row K of the plain-text block (state) is circular left rotated by k-bytes.
   c. *Apply Mix-column operation* – in this step, Matrix multiplication is performed between the state array and a constant matrix using Galois field, resultant array is copied into state array.
   d. *Perform XOR operation* - State array is XORed with key block array of key expansion.

## RESULTS AND ANALYSIS

For example, if our message is "hello world" and SHA-1 and SHA-2 generates hash code as:

SHA-1 (in Hex):

2aae6c35c94fcfb415dbe95f408b9ce91ee846ed

SHA-2 (in Hex):

b94d27b9934d3e08a52e52d7da7dabfac484efe37a5380ee9088f7ace2efcde9

EX 2: Cryptography

SHA-1 (in Hex):

b804ec5a0d83d19d8db908572f51196505d09f98

SHA-2 (in Hex):

b584eec728548aced5a66c0267dd520a00871b5e7b735b2d8202f86719f61857

Ex3: Have A Nice Day!

SHA-1 (in Hex):

f3579afc7643a7e1442261bf755f93555993e9e3

SHA-2 (in Hex):

66495c275c0c6c3adaa073b2f92c188bf0966f1c19c4907504651440f755ccc0

Ex4: Good day

SHA-1 (in Hex):

fd4f11f202ff82750dc4a133aa67747832388fe

SHA-2 (in Hex):

368c062b4f03c1f469b2015740f0fa91622454a042cc552fac3f1a458d9c4dc7

SHA-1 generates 40 characters hash code whereas SHA-2 generates 64 characters hash code. SHA-2 is more secure as it generates longer hash-code than SHA-1 which will take a longer time to decipher.

## CONCLUSION

Cloud computing system is a paradigm to meet multiple objectives such as performance, cost, reliability, maintainability, security and in order to make balance among all these objectives cloud security-design principles must be compatible with characteristics like reliability and performances. In order to overcome the threat of integrity, user can entrust third party auditor to assess the risk of outsourced data, whenever needed .For this, we used SHA-2 on plain-text along with shared variable which is cryptographic hash function to verify integrity of data and validating the identity of the originator. We used AES algorithm for encryption and decryption of message to verify the confidentiality of data. This concept will definitely help in achieving the objectives of cloud for security.

## REFERENCES

[1] Abdulwadood Sabeeh, Abdul Wadood Alshawi "International Journal of Research in Computer and Communication Technology, VOL 4, Issue 4, April - 2015

[2] Rajkumar Buyya “Introduction to the IEEE Transactions on Cloud Computing” IEEE TRANSACTIONS ON CLOUD COMPUTING, VOL. 1, NO. 1, JANUARY-JUNE 2013.

[3] L.Badger, T Grance, R. P. Comer and J. Voas, DRAFT cloud computing synopsis and recommendations, Recommendations of National Institute of Standards and Technology(NIST), May-2012.

[4] D. A. Menasce and P. Ngo, “Understanding cloud computing: Experimentation and capacity planning,” in Proc. of computer measurement group conf., pp. 1-11, December 2009.

[5] IBM Global Services, Cloud computing: defined and demystified explore public, private and hybrid cloud approaches to help accelerate innovative business solutions ,April-2009.

[6] K.Govinda, E.Sathiyamoorthy, “Data Auditing in Cloud Environment using Message Authentication Code”, International Conference on Emerging Trends on Advanced Engineering Research(ICETT),2012.

[7] Ricardo Chaves, Leonel Sousa, “Improving SHA-2 Hardware Implementation”, International Association for Cryptographic Research, 2008.

[8] Robert P. McEvoy, Francis M. Crowe, Colin C. Murphy and William P.Marnane, “Optimisation of the SHA-2 Family of Hash Functions on FPGAs”, IEEE Emerging VLSI Technologies and Architectures, Vol. 00, 2-3 March, 2006.