International Journal of Scientific Research & Engineering Trends
Volume 5, Issue 3, May-Jun-2019, ISSN (Online): 2395-566X

Third Party Auditing In Cloud Storage

Akshay Bhonde Bipin Kumar Bilal Momin Prathamesh Shete Asst. Prof. Sulbha Ghadling
Dept. of Computer Science
NMIET, Pune, MH, India

***Abstract*- Remote data integrity checking (RDIC) enables an cloud server, to provide a proof to a verifier that it is really storing data owner's data securely. A lot of RDIC protocols have been proposed in the literature, but most of the constructions are complex key management, which rely on expensive public keys infrastructure (PKI), which might hinder the deployment of RDIC in practice. In this paper, a new construction of identity-based (ID-based) RDIC protocol by making use of cryptographic primitive to reduce the system complexity and the cost for establishing and managing public key authentication framework in PKI-based RDIC schemes. It is an ID-based RDIC security model, which includes security against a malicious cloud server and zero knowledge privacy against a third party verifier. The ID-based RDIC protocol doesn't leak any information of the stored data to the verifier during the RDIC process. The new construction is proved to be secure enough against the malicious server in the generic group model and achieves zero knowledge privacy against a verifier. Immense security analysis and implemented results demonstrates the proposed protocol is provably secure and practical in the real-world applications.**

***Keywords*- Digital Document System, Encryption, Decryption, Cloud.**

I. INTRODUCTION

Cloud Computing is one of the net-based computing, where exclusive offers are added to an enterprises computer systems and devices through the internet which helps in saving users both time and money. Cloud computing may be very promising for the information Technology (IT) programs however, there are still a few issues to be solved for example to keep private customers and corporations records and deploy applications inside the Cloud computing surroundings. Facts safety is one of the most massive barriers to its adoption and it's far accompanied by using troubles such as compliance, privacy consider, and felony subjects.

The facts confidentiality could be addressed by increasing the reliability and trustworthiness in Cloud. Consequently various parameters like security, integrity, privacy, confidentiality of the statistics and other stored documents on the cloud have to be considered which essential requirements from customer's point of view are. To attain all of these necessities, new techniques or techniques need to be evolved and implemented. Records auditing is delivered in Cloud computing to address relaxed statistics garage. Auditing is a technique of verification of consumer facts which can be carried out both via the user himself or by using a TPA.

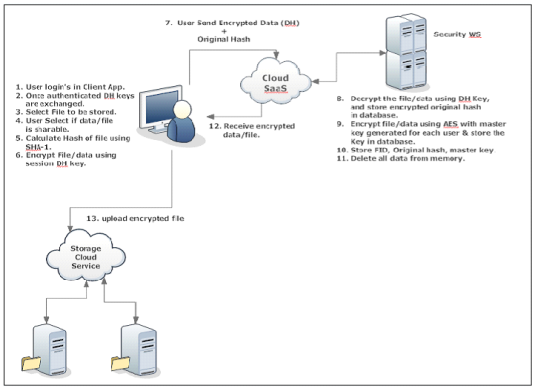

Fig. 1 Proposed System Architecture (Uploading/Encryption Phase)

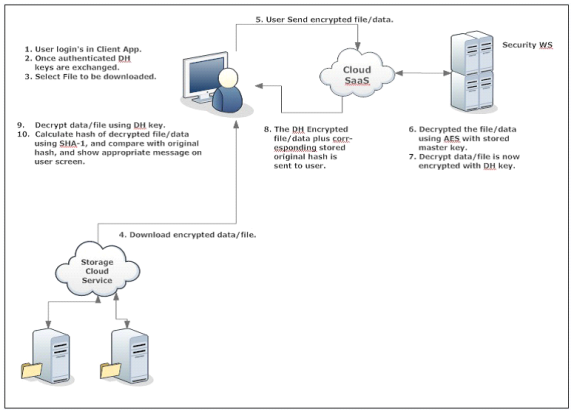

Fig. 2 Proposed System Architecture (Downloading/Decryption Phase)

© 2019 IJSRET

International Journal of Scientific Research & Engineering Trends
Volume 5, Issue 3, May-Jun-2019, ISSN (Online): 2395-566X

II. PROPOSED WORK

Encrypting the file before outsourcing can partially address the data-privacy issue but leads to losing the flexibility of the protocols, since privacy preserving RDIC protocols can be used as a building block for other primitives. A new construction of identity-based RDIC protocol by making use of key-homomorphism cryptographic primitive to reduce the system complexity and the cost for establishing and managing the public key authentication framework in PKI-based RDIC schemes which reduce the system complexity and the cost for establishing and managing the public key authentication framework in PKI-based RDIC schemes.

In data integrity checking with public-verifiability, an external auditor (or anyone) is able to verify the integrity of the cloud data. In this scenario, data privacy against the third party verifier is highly essential since the cloud users may store confidential or sensitive files say business contracts or medical records to the cloud.

Advantages of Proposed System

- No need to carry all document files everywhere.
- Avoid damage and loss of confidential documents.
- Users will get notified if at all any of his documents might get manipulated

III. IMPLEMENTATION

1. Algorithms

1.1 AES Algorithm

AES is cipher cryptographic algorithm. Also meant the substituting permutation network. It contains the several operations such as the given input replaced by the special substitution shifting the rows and adding bit into it. This algorithm has an own particular structure to encrypt and decrypt sensitive data and is applied in hardware and software all over the world. It is extremely difficult to hackers to get the real data when encrypting by AES algorithm.

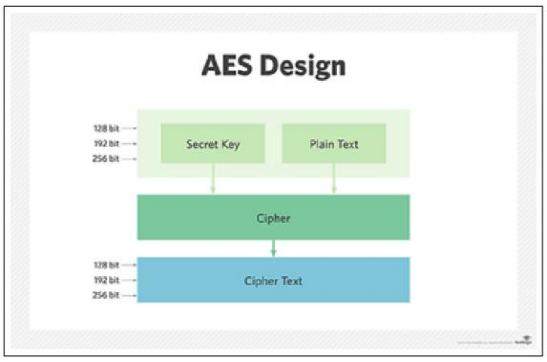

Fig. 3 Working of AES Algorithm.

2. Encryption Process- Following are the working of the encryption pro-cess of AES algorithm.

2.1 Byte Substitution- Byte substitution by based on the table of input is in bytes and the result also will be the matrix of four columns and rows.

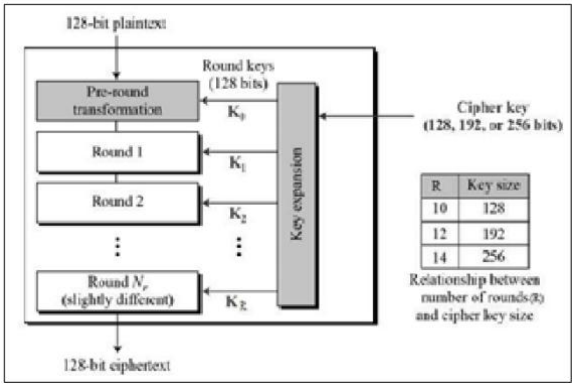

Fig.4 Byte Substitution In AES Algorithm.

2.2 Shift Rows- The shifting processing carried out in the matrix by shifting the rows to the left one by one. In the shifting process if any entries are fall of then those entries shifted or reinserted right side of the row. It is important for the encryption of the data given as the input. The rst row in the matrix is not shifted. While the second row shifted to one position from current position to the left. Then third row shifted two positions to the left. Fourth row is shifted three positions to the left. One by one row shifted to the left and any rows fall of, it reinserted to the right. New matrix will the same number of bytes 16 but shifted as above with each other.

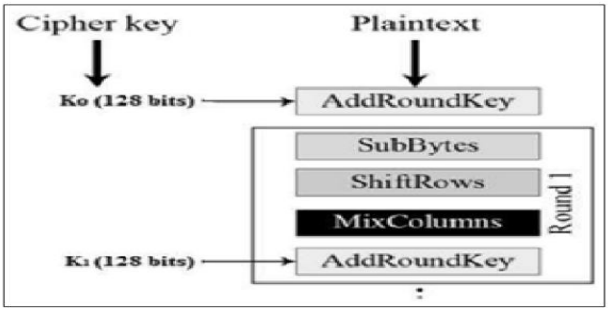

Fig. 5 Shift Rows In AES Algorithm

3. Mix Columns- Mix 4 bytes by using the functions using math. In this it get the four byte of inputs and writes the newly generated bytes in which it replaces the existing data. It will write the other matrix of newly generated data.

4. Add Round Key- The 16 bytes matrix are now considered as 128 bits and are XOR'ed to the 128 bits of the round key. If this is the last round then the output is cipher text. Otherwise, the resulting 128 bits are interpreted as 16 bytes and begining of another similar round.

5. Decryption Process- The decryption process is exactly the reverse order of the AES encryption steps. In which the steps consist of the reversed order processes.

© 2019 IJSRET

- Add round key
- Mix columns Shift rows
- Byte substitution

6. SHA Algorithm

Security Hash Algorithm (SHA) developed in 1993 by the NIST and NSA designed to be used for secure hashing in Digital Signature Standard in the US. It is one of the most popular encryption methodologies. A special mathematical function called "Hash" performs one-way encryption. SHA-l is a revised version of SHA designed by NIST and published as a FIPS. In comparison to MD5, SHA-l processes input data in 512-bit blocks and generates a 160-bit message digest. Whereas MD5 generated message digest of 128 bits. The procedure is used to send a non secret but signed message from sender to receiver. In such a case following steps are followed:

- Sender inputs a plaintext message into SHA-l algorithm and obtains a 160-bit SHA-l hash.
- Then Sender signs the hash with his private key and sends both the plaintext message and the signed hash to the receiver.
- After receiving the message, the receiver computes the SHA-l hash himself and also applies the sender's public key to the signed hash to obtain the original hash H.

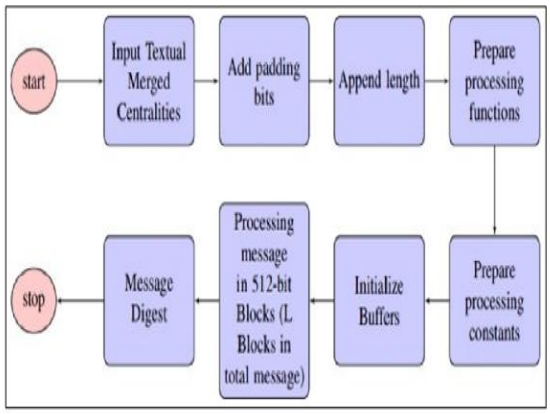

Fig. 6 Working Of SHA-1

IV. MATHEMATICAL MODEL

1. Cryptographic Parameters of Mathematical Model

F = (m1, . . . ,mn)p users data which should be stored in the server storage where n is the number of blocks and p is a high prime number. fkey() { pseudo random function (PRF), denied as: 0, 1 key p. key() { pseudo random permutation (PRP), denied as: 0, 1log2(n) key 0, 1log2(n) MACkey() { message authentication code (MAC) function, denied as: 0, 1 key 0, 11 H(), h() { map-to-point hash functions, denied as: 0, 1 G, where G is some group.

Let G1, G2 and GT to be the multiplicative cyclic group of line p and G1 G2 GT was a bilinear map. Let g be the generator G2.H() which was a secure map-to-point hash function: 0,1 G1 which mapped the integer (chains) uniformly into G1. Hash function () G1 p mapped the element groups G1 into p [14].

V. MATHEMATICAL DESCRIPTION OF TPA MODEL OPERATION

In the process of settings, the user launched the algorithm KeyGen and generated both public as well as private parameters. Randomly selected x p, random element u G1 and calculated u g x and w u x . The private parameter was sk=(x) and the public were vk = (v,q,g,u). On data F = (m1, . . . ,mn)the user launched the algorithm SigGen by which he calculated the sign i for each data block mi: i (H(i) umi) xG1, for i=(1, . . . ,n). Then the summary of all signs was = i1 I nfori=(1, . . . , n). Consequently, the user sent F, on a server and deleted the local copy.

During the audit, the message \chal" has been created. It specified the blocks position which was sneeded to be checked during the audit phase. The third audit side randomly selected a subset s c elemental I=S1 , . . . , Sc sets [1, n]where Sq=kprp(q) where q=(1, . . . ,c) and kprp was the third permutation key for each audit chosen by audit side. For each element iI, TAP has chosen randomly the value i. Then it has sent the message chal=(i, i)i I to the server. After receiving the message \chal", the server launched the algorithm GenPro which generated an answer as a proof of correctness of data storage.

The Server selected a random element r p through r = fkprf(chal) where kprf was a randomly chosen key by the server by the use of the pseudo-random function for every unit. Then it calculated R= (w)r = (ux) rG1. Linear combinations of chosen blocks speci ed in the message \chal" was ' = vimi, for iI. For ' and r server calculated = '+r(R) p. Then server calculated aggregated signature = i Ii viG1, for i I. Finally, the server has sent the answer , , R to third audit side. After receiving the answer from the server, TAS launched the algorithm VerifyProof by which it verified the accuracy of the answer by calculating in the verifying equation: e((Rh(R)),g) e i=si H(i)vi . u , v) Random mask R did not have any effect on accuracy verification. Simultaneously, the third side did not have any access to data of customer F, privacy has been maintained, Cong et al., (2010).

VI. WORKING

TPA (Third-Party Auditor) module, the auditor will regularly check the integrity of the files. This integrity checking helps to maintain the integrity of the file.

The actions performed under TPA Module are as follows:

1. Check Integrity.
2. Send Notification.

© 2019 IJSRET

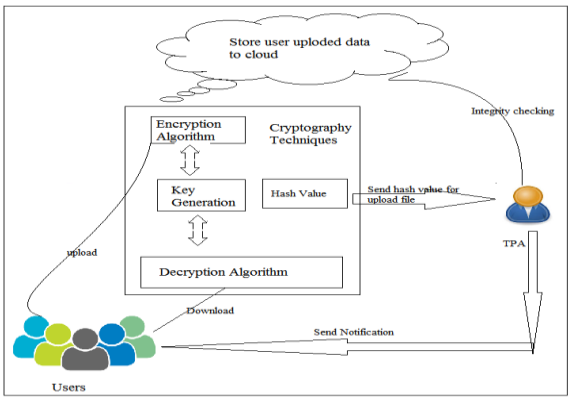

Fig.7 System Architecture.

VII. CONCLUSION

Cloud computing is a emerging technology. We addressed the construction of an efficient audit service for data integrity in clouds. A secured privacy maintaining public auditing scheme is been proposed which preserves privacy and public auditing for cloud, this is achieved by using a TPA (Third Party Auditor), which performs the auditing without retrieving the original data, therefore privacy is preserved. The data is encrypted and then saved in the cloud storage, preserving the confidentiality of information is maintained. TPA verifies the data integrity in the cloud. TPA also performs multiple auditing tasks which helps to overcome the limitations of the prevailing auditing scheme. This proposal is to perform an effective auditing scheme focusing on AES algorithm in cloud computing.

REFERENCES

[1] A. F. Barsoum and M. A. Hasan, “Provable multi-copy dynamic data possession in cloud computing systems,” IEEE Trans. Inf. Forensic Security, vol. 10, no. 3, pp. 485–497, Mar. 2015.

[2] J. Yu, K. Ren, C. Wang, and V. Varadharajan, “Enabling cloud storage auditing with key-exposure resistance,” IEEE Trans. Inf. Forensics Security, vol. 10, no. 6, pp. 1167–1179, Jun. 2015.

[4] T.Subha1 and Dr.S.Jayashri**,"** Efficient Privacy Preserving Integrity Checking Model for Cloud Data Storage Security**",** @2016 IEEE.

[5] Shulan Wang, Kaitai Liang, Joseph K. Liu, Member, IEEE, Jianyong Chen, Jianping Yu, Weixin Xie Attribute-Based Data Sharing Scheme Re-visited in Cloud Computing, 2016.

[6] Muhamad Abdullah. Advanced Encryption Standard Algorithm to Encrypt and Decrypt Data, 2017.

© 2019 IJSRET