IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727
PP 01-04
www.iosrjournals.org

Third Party Auditing for Cloud Data Security with AES Algorithm

G.Siva Brindha[1], Dr.M.Gobi[2]

[1]*(Department of computer science, Chikkanna Govt. Arts College, Tiruppur,India)*
[2]*(Department of computer science, Chikkanna Govt. Arts College, Tiruppur,India)*

Abstract: *The purpose of this work is to develop an auditing scheme which is at ease, efficient to apply and own the skills which include privacy preserving, public auditing, keeping the statistics integrity alongside confidentiality. Thus the new auditing scheme has been developed consisting of three entities. Data proprietor, TPA and cloud server. The data proprietor performs diverse operations consisting of splitting the document to blocks, encrypting those using AES. It verifies the integrity of records on demand of the users in cloud. The cloud server is used handiest to save the encrypted blocks of facts. This proposed auditing scheme uses AES algorithm for encryption.*

Keywords: *Cloud Computing, TPA methods, AES Algorithm encryption and decryption.*

I. Introduction

1. Cloud Computing: Using the cloud saves both users time and money. Cloud Computing is defined as a type of net-based totally computing, in which exclusive offerings are added to an enterprise's computer systems and devices through the internet [1]. Cloud computing may be very promising for the information Technology (IT) programs; however, there are still a few issues to be solved for private customers and corporations to keep 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, privateness, consider, and felony subjects. Consequently, one of the critical desires is to preserve security and integrity of records saved within the cloud because of the essential nature of Cloud computing and big quantities of complicated statistics it consists of. The customers concerns for security must be rectified first to make cloud environment honest, in order that it enables the customers and employer to adopt it on big scale [1]. The most troubles in cloud records protection include records privateness, information protection, information availability, information place, and cozy transmission. Threats, records loss, provider disruption, out of doors malicious assaults, and multi tenancy troubles are the security demanding situations blanketed in the cloud. Statistics integrity inside the cloud device means retaining the integrity of saved records. The records should not be misplaced or changed via unauthorized users. Cloud computing carriers are relied on to keep records integrity and accuracy of records. Authentication and get admission to manipulate techniques are used to ensure statistics confidentiality. The facts confidentiality could be addressed by growing the cloud reliability and trustworthiness in Cloud computing. Consequently security, integrity, privateness and confidentiality of the stored statistics on the cloud have to be considered and are essential requirements from person's point of view [1]. 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 (information proprietor) or by using a TPA.

2. Third Party Auditor (TPA): Third Party auditor allows keeping the integrity of statistics stored on the cloud. The verifier's role is classified into: first one is private audit ability, in which most effective consumer or statistics owner is authorized to test the integrity of the stored records. Second one is public audit ability, which allows anyone, now not simply the consumer, to mission the server and plays facts verification tests with the help of TPA [4]. The TPA is an entity which is used so that it is able to act on behalf of the consumer. It has all the important understanding, skills, expertise and expert abilities which can be required to deal with the paintings of integrity verification and it additionally reduces the overhead of the consumer.

3. Advanced Encryption Standard (AES): The more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES). AES is regularly used encryption algorithm. This algorithm is based on several substitutions, permutations and linear transformations, each executed on data blocks of 16 byte. AES remains the preferred encryption standard algorithm. It is found at least six times faster than triple DES.

II. Literature Survey

Cloud computing faces many problems on integrity and privacy of user's data stored in the cloud. Hence it requires some secure and efficient methods which can ensure the integrity and privacy of data stored in the cloud. Wang et al. has proposed a privacy preserving public auditing protocol which makes use of an independent TPA to audit the data. It utilizes the public key based homomorphism linear authenticator (HLA) with random masking techniques. But this protocol is vulnerable to existential forgeries known as message attack from a malicious cloud server and an outside attacker [5].

Wang et al. proposed a new improved scheme which is more secure than the protocol. It is a public auditing scheme with TPA, which performs data auditing on behalf of users. It uses HLA which is constructed from Boneh-Lynn-Shacham short signature referred as BLS signatures [6].

Tejaswani et al. has finished integrity of records the usage of a Merkle hash tree by using TPA and the confidentiality of facts is executed the usage of RSA primarily based cryptography set of rules [7].

III. Objective

Cloud computing is a web based computing which enables sharing of offerings. Cloud Computing is a technology for next generation Information and Software enabled work that is capable of changing work environment. It is interconnecting the large-scale computing resources to effectively integrate, and to computing sources as a provider to users Cloud computing permits users to apply applications without set up any utility and get entry to their personal files and alertness at any computer with internet or intranet get admission to. Many customers place their facts inside the cloud, so correctness of records and protection is a top subject to make certain the correctness of information, we keep in mind the task of allowing a third party auditor (TPA), on behalf of the cloud patron, to affirm the integrity of the facts stored inside the cloud..In Cloud Computing, Data storage security and provide privacy preserving auditing protocol is motivated by public auditing system. Third party auditor is a kind of inspector. TPA ought to efficaciously audit the cloud data storage without soliciting for the neighborhood reproduction of information. It needs to have zero information about the records saved within the cloud server. It need to no longer introduce any extra online burden to the cloud person [2].This kind of auditing service not only helps to save owner's data computation resources but also provide a transparent yet Cost effective method for data owners to gain trust in the cloud.

IV. Existing System

Cloud Computing is a trustworthy mechanism of logical entities like stored data and security resources in internet. To protect data from intruders data centers uses security techniques to deny the accessing of stored data. Security is good and better to achieve privacy –preserving public auditing system for cloud data storage. On behalf of cloud client, using a dynamic audit service (TPA) for integrity verification of untrusted and outsourced storages. Service providers are able to devote resources to solving security issues.

1. Drawbacks of existing system: Cloud storage provides safety and security to save the users data. In some exists, users file were kept open without encryption on the cloud storage system i.e. TPA demands retrieval of user data here privacy is not preserved. User privacy is a big concern.

V. Proposed System

A powerful public auditing protocol is needed to overcome the obstacle of the present auditing scheme. The proposed machine is advanced to affirm the correctness of cloud records via TPA, periodically or on call for without retrieving the entire data or without introducing additional on line burden to the cloud customers and cloud servers. It assures that no facts content material is leaked to TPA all through the auditing manner. It maintains storage correctness of records, integrity and confidentiality of saved facts. The proposed scheme consists of three primary entities; they're data owner, cloud server storage and TPA. The information proprietor or the person is liable for splitting the document into blocks, encrypting the ones the use of AES Algorithm. The AES algorithm is a symmetric block cipher, in which both the sender and the receiver use a same key for both encryption and decryption. The information block duration is fixed to be 128 bits, while the period can be 128, 192, or 256 bits. In addition, the AES algorithm is an iterative set of rules. Every iteration may be referred to as a round, and the full variety of rounds is 10, 12, or 14 when key duration is 128,192, or 256, respectively. In this case the entire data block is processed in parallel during each round using substitutions and permutations.

A number of AES parameters depend on the key length. For example, if the key size used is 128 then the number of rounds is 10 whereas it is 12 and 14 for 192 and 256 bits respectively. At present the most common key size likely to be used is the 128 bit key. This description of the AES algorithm therefore describes this particular implementation.

Key selection: Sender and receiver agree upon a 128 bit key. This key is used for encryption and decryption. It is a symmetric key encryption method, so they want to share this key in a comfortable way. The key is represented as blocks k [0], k [1]...k [15]. Where each block is 8 bits prolonged (8*16=128 bits).

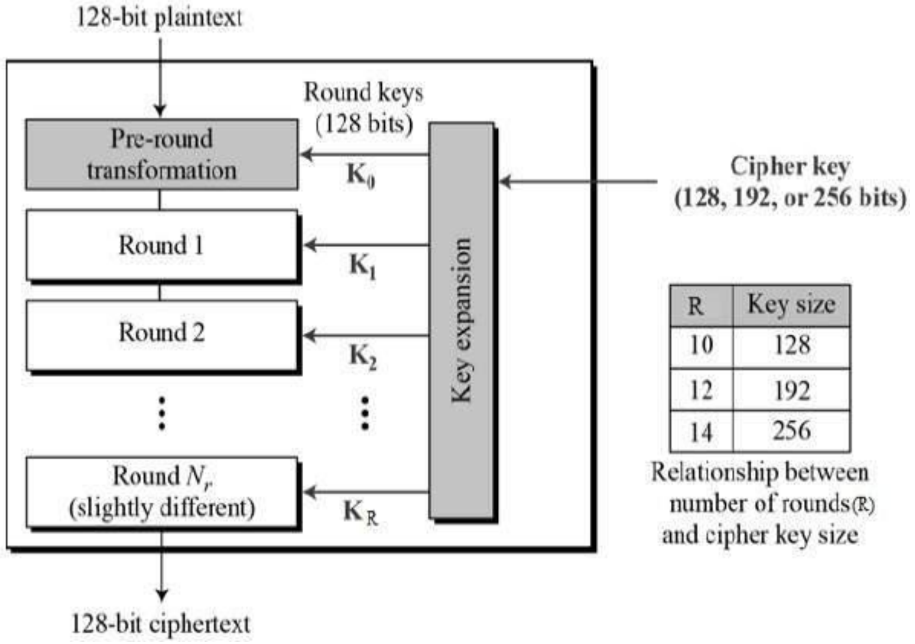
The algorithm starts Add round key with 9 rounds of four stages and a tenth round of three stages for encryption and decryption is inverse of encryption. The four stages are as follows:

1. Substitute Bytes - A simple substitution of each byte on state. Uses one fixed table (S-box) 16 input bytes are substituted. Each byte of state is replaced by byte indexed row (left 4 bits) and column (right 4 bits).

2. Shift Rows- This is a simple permutation. The first row of state is not altered. The second row is shifted 1 bytes, third row is shifted 2 bytes and fourth row is shifted 3 bytes to the left in a circular manner. The result is a new matrix consisting of the same 16 bytes.

3. Mix Column - It operates on each column individually. Each column of four bytes is transformed using a matrix multiplication using GaloisField-GF (28). Each value in the column is eventually multiplied against every value of the matrix. The result is another new matrix consisting of 16 new bytes.

4. Add Round Key - In the AddRoundKey step, the sub key is combined with the state. For each round, a sub key is derived from the main key; each sub key is the same size as the state. The sub key is added by combining each byte of the state with the corresponding byte of the sub key using bitwise XOR.



R	Key size
10	128
12	192
14	256

Relationship between number of rounds(R) and cipher key size

Fig.1 Advanced Encryption Standard

VI. Working Methodology

The system provides encryption/decryption by a trusted third party over the network. The trusted third party which provides these security services does not store any data at its ends and stores only master key for each client for data encryption and decryption. To enhance the security, the communication between client and security server is secured using AES. This division of responsibility has big effect, as no single provider has access to other data and security key. Audit can be both static and dynamic. In static auditing , auditing is done periodically to verify the integrity of data. Samples are taken from the data and it is verified for integrity of data. In dynamic auditing, auditing is done on dynamic data. The dynamic data operations are modification, insertion and deletion.

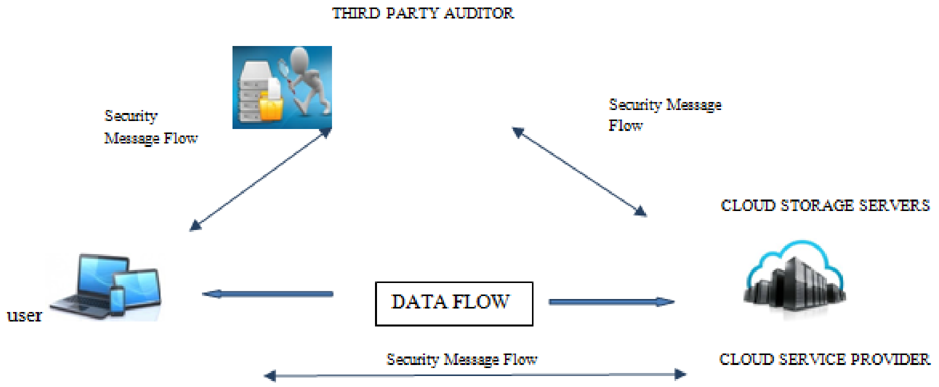


Fig. 2 The architecture of cloud data storage service

VII. Conclusion

Cloud computing is a emerging technology. A secured privacy maintaining public auditing scheme is been proposed. Preserving privacy and public auditing for cloud is achieved by using a TPA (Third party Auditor), which does 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 performs multiple auditing tasks to overcome the limitations of the prevailing auditing scheme. This proposal is to perform an effective auditing scheme focuses on AES algorithm in cloud computing.

References

[1]. Zissis, Dimitrios, and Dimitrios Lekkas. Addressing cloud computing security issues. Future Generation computer systems 28.3 (2012): 583-592.

[2]. Cong Wang, Sherman SM Chow, Qian Wang, Kui Ren, and Wenjing Lou. Privacy Preserving Public Auditing for Secure Cloud Storage. http://eprint.iacr.org/2009/579.pdf

[3]. Mell, Peter, and Tim Grance. The NIST definition of cloud computing. (2011).

[4]. Balakrishnan S, Saranya G, et al. (2011). Introducing Effective Third Party Auditing (TPA) for Data Storage Security in Cloud, International Journal of Computer Science and Technology, vol 2(2), 397–400.

[5]. Qian Wang, Cong Wang, Kui Ren, Wenjing Lou, and Jin Li. Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing. Parallel and Distributed Systems, IEEE Transactions on, 22(5):847–859, 2011.

[6]. Cong Wang, Sherman SM Chow, Qian Wang, Kui Ren, and Wenjing Lou. Privacy Preserving Public Auditing for Secure Cloud Storage. http://eprint.iacr.org/2009/579.pdf

[7]. Tejaswini, K. Sunitha, and S. K. Prashanth. Privacy Preserving and Public Auditing Service for Data Storage in Cloud Computing. Indian Journal of Research PARIPEX, 2(2), 2013.

[8]. Cloud Security Alliance,"Top Threats to Cloud Computing" http://www.cloudsecurityalliance.org 2010.

[9]. P. Oreizy, N. C. Wang, Q. Wang, K. Ren, and W.Lou. "Privacy Preserving Public Auditing for Storage Security in Cloud Computing" proc.IEEE INFOCOM 10, Mar 2010.

[10]. S. Sivachitralakshmi,T. Judgi, "A Flexible Distributed Storage Integrity AuditingMechanism in Cloud Computing", International Conference on Computing and Control Engineering (ICCCE 2012), 12 & 13 April, 2012.

[11]. R.Ushadevi, V. Rajamani, "A Modified Trusted Cloud Computing Architecture based on Third Party Auditor (TPA) Private Key Mechanism", International Journal of Computer Applications (0975 – 8887) Volume 58– No.22, November 2012.

[12]. M. A. Shah, R. Swaminathan, and M. Baker, "Privacypreserving audit and extraction of digital contents," Cryptology ePrint Archive, Report 2008/186, 2008.