INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 08, August 2024, pp: 525-529

THIRD PARTY AUDITING(TPA) FOR SECURITY STORAGE DATA IN CLOUD COMPUTING

Rasha Rokan Ismail[1]

[1]Diyala university, Diyala, Diyala, Iraq.

DOI: https://www.doi.org/10.58257/IJPREMS35742

ABSTRACT

Cloud computing considered one of the most important areas of research today, because its ability to reduce costs which related with computing while increase flexibility and scalability for computing services. When the users use the cloud computing, the data of users are stored on far place to the cloud servers and enjoy the on-demand cloud services from a shared pool, without the burden of maintenance, data storage and costs. In cloud computing the consumers can share resources, information and services during use of internet. Several security issues arises when using the cloud computing such as data confidentiality, authentication and integrity. This paper aims to offer a secure, effective, and flexible method to ensure security storage in cloud computing by Third Party Auditing , and providing users with a more secure experience of a cloud computing environment . by using modified Advanced Encryption Standard(AES).

Keywords: Cloud Computing, Security, AES, Third Party Auditing TPA

1. INTRODUCTION

Cloud computing is era technology that provide virtualized significant pool of computing resources. The consumer in cloud computing can use these resources everywhere, anywhere, on-demand and depend on the principle of pay per use. There are two type of models in cloud computing are: services models (SaaS, PaaS, and IaaS), and deployment models (Public, Private, Community, and Hybrid cloud). The cloud computing also include five essential characteristics defined by NIST are: (On-Demand, Broad Network Access, Rapid Elasticity, Measured Service, and Resource pooling). When using cloud computing many security concerns arises, these concerns should be taken in account like breach of the privacy and confidentiality of consumers' data by unauthorized parties. Cryptography is the best way to secure data in cloud computing. It becomes difficult for an intruder if the data existent in cloud is in encrypted form, as the data files or encrypted data blocks are useless for any person unless he knows the perfect method for decrypting it. In this paper I will use the modification of AES algorithm which was proposed by Ali AdulGader et al in [1] to provide data security , integrity data and authentication.

Cloud computing describes the combination of logical entities like data, software which are accessible via internet. Client data is generally stored in banks of servers spread across the globe. The clients concern about data security,data integrity, and sharing data with specific band of men and women must be addressed. You can find multiple means of achieving this, example encrypting data on client machine and then storing the information to cloud storage server, computing hash of the information on client machine and storing hash of data in client machine, client trying out the responsibility of sharing the trick key about encryption with specific band of people. Therefore it becomes moretedious for client to keep these information and share such information, more over in the event the device which stores such information is lost or stolen it pose a threat to the total data. Another way could be same storage cloud provider providing the service for secured sharing, hashing, encryption/decryption, but since administrative can have use of both services for maintainance, the security service provided by the cloud storage provider, the information might be compromised. The forementioned approches burdens the client by which makes it additionally accountable for securing it data before storing it to the cloud storage. [2][3][4].

2. THIRD PARTY AUDITOR (TPA)

The Cloud users send the data to Cloud service provider through the network. The user data may contains very sensitive data like user personal information, Bank details, Password, Important key Word, Business client details etc.Cloud service providers normally use Secure Socket Layer (SSL), Point to Point Tunneling protocol (PPTP), VPN for secure transaction. We are having history that attackers and intruders have win over this type of security services.While transferring the data between user and the cloud service providers very hard to avoid malicious attack. But usersneed assurance legally about the security over their data. For this we need a authentication mechanism based on the third party. This third party should common for both cloud user and the Cloud Service Providers. This third partymonitor the activities of cloud user and cloud service provider. Normally cloud service providers and client will havea Service Level Agreement (SLA). This is a legal agreement between Cloud service provider and the client. Both

parties have to follow the rules and regulations mentioned in the SLA. This agreement includes the Cloud service provider's quality of service, Standard of the service, service monitoring and controlling. The Cloud service may givelot

of commitment and service offers to the cloud user due to market competition. But any point of time he has to follow it. The cloud service providers for their own benefits they will hide the data errors from the cloud user. To avoid this problem and to maintain the security standard we need a Third Party Auditor (TPA).The TPA will monitor the both client and Service Provider side activities. TPA will follow the auditing norms and techniques, also they will have list of auditing strategies. The TPA should familiar with the SLA between cloud service provider and cloud user. TPA will play promising role between this two parties. TPA having ability to check the integrity of the data which stored in the cloud. The auditing should not affect the privacy of the cloud users. Here the cloud user mainly concern about their data security. Data Security comprises of Data integrity, Data Availability, Data Confidentiality. As the data is stored In order to verify the data integrity at un trusted servers become a big concern with cloud environment. Data security means protecting the data from the unwanted actions from unauthorized users and protecting from destroy forces. The forces may in any form of hardware failure, software failure, network failure, system failure, external forces, natural calamities etc. The unauthorized user may be intruder. We have to monitor the all user activities, if we found any unauthorized function from any user, immediately we should block the particular user before damaging the data. Data Integrity means maintaining the accuracy and consistency over the cloud user data at any point of time. The cloud user may store key information in the cloud storage, the accuracy of the user data information should be accurate in any point of time. Data Confidentiality means maintaining the secrecy about the user data. Confidentiality is a set of rules and promises to maintain the secrecy over some cloud user data information. The Cloud Service Provider should not enclose that information to anybody in any point of time. The auditing process consists of three different type of phases. Planning, Execution and Reporting. In planning stage the TPA have to finalize the following important tasks, Content to audit, Time schedule of the auditing, duration of auditing, area of auditing, audit team size etc. The audit time and team size depends up on the size of the content.

Execution is the important phases. In this phase we have to analysis the security threats in the cloud storage, monitor the previous threats and determine the level of previous threats. Also have to do the data integrity check. Reporting is the report of execution phase, this report will help the Cloud service provider to improve their service. The third party audit report mention the complete details about the cloud user activities and performance of the cloud service

providers. According to this audit report Cloud Service Providers can monitor the activities of the user, if any user acting like the attacker we can cancel the agreement. At the same time Cloud Service Provider can improve the serviceefficiency of the service by this audit report. Because this audit report indicate the both user and cloud service provider performance.[5][6][7]

3. 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 [8]. 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 [9]. 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 [10].

4. 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

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 08, August 2024, pp: 525-529

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.

Our objective is to build a security service which will be provided with a trusted 3rd party, and would lead to providing only security services and wouldn't store any data in its system. Detailing it further:

1. To construct Web service system which would provide data integrity verification, provide encryption/decryption ofthe consumer data.

2. Defining access list for sharing data securely with specific band of individuals.

3. To construct thin client application which would call this web service before uploading/downloading the data to and from cloud.

5. 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.

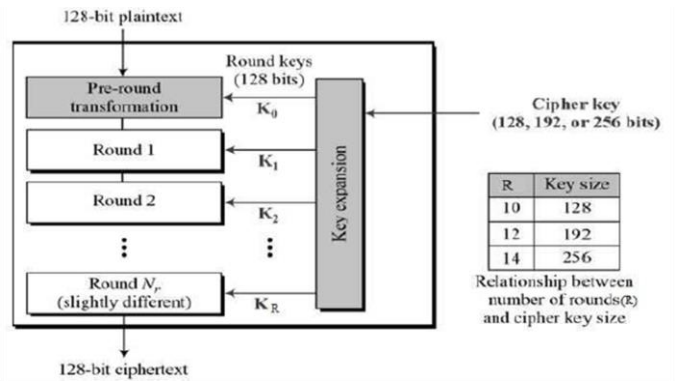
Key selection: Sender and receiver agree upon a 128 bit key. This key is used for encryption and decryption. It is a symmetric key encryption method, so they want to share this key in a comfortable way. The key is represented as blocks k [0], k [1]...k [15]. Where each block is 8 bits prolonged (8*16=128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



R	Key size
10	128
12	192
14	256

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

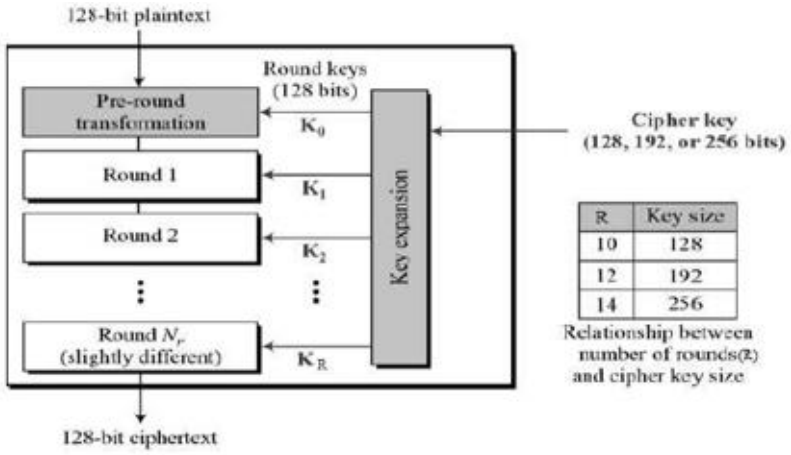
INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 08, August 2024, pp: 525-529



R	Key size
10	128
12	192
14	256

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

Fig.1 Advanced Encryption Standard

6. 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

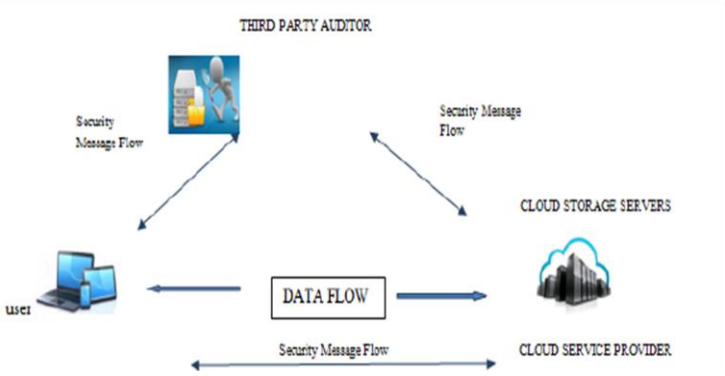


Fig. 2 The architecture of cloud data storage service

7. 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.

8. REFERENCES

[1] [1] P. Mell and T. Grance, “Draft NIST working definition of cloud computing”.

[2] [2] A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, M. Zaharia, “Above the clouds: A berkeley view of cloud computing,” University of California, Berkeley, Tech. Rep, 2009.

[3] [3] G.Ateniese et al., ―Provable Data Possession at Untrusted Stores,‖ Proc. ACM CCS _07, Oct. 2007, pp. 598–609.

[4] [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] [5] Yu, S., Wang, C., Ren, K., Lou, W.: Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing. In: Proc. IEEE INFOCOM. pp. 534–542 (2010)

[6] [6] Mohammed A. AlZain, Ben Soh and Eric Pardede AlZain, M.A.; Soh, B.; Pardede, E. A New Approach Using Redundancy Technique to Improve Security in Cloud Computing. International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012.

[7] [7] Akhil Behl, Emerging Security Challenges in Cloud Computing . Congress on Information and Communication Technologies (WICT), 2011 World.

[8] [8]. 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.

[9] [9]. 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

[10] [10]. Tejaswini, K. Sunitha, and S. K. Prashanth. Privacy Preserving and Public Auditing Service

[11] [11]. 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.

[12] [12]. 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

[13] [13]. Ahmed, W. S., & Itwayya, A. A. (2023). A new technology to make smaller power grids work better. International Journal of Electrical and Electronics Engineering, 10(8), 176–184. https://doi.org/10.14445/23488379/ijeee-v10i8p117

[14] [14]. Al-Chaabawi, N. J. H., Ahmed, W. S., & Itwayya, A. A. (2023). Evaluation of memristor behaviour with global logic gates. AIP Conference Proceedings. https://doi.org/10.1063/5.0170813