Methodology for Data Auditing and Privacy Preserving in Cloud Using Fuzzy RSA Algorithm

Patel Tanvi Dhansukhbhai[#1], Puneet Dwivedi [*2]

[#1]*M.Tech Scholar, Department of Computer Science and Engineering, RKDF University, Bhopal, India*
[*2]*Assistant Professor, Department of Computer Science and Engineering, RKDF University, Bhopal, India*

Abstract: ***In cloud computing domain, Attribute Based Encryption ABE is one of the significant theory of cryptographic strategy. Here we proposed algorithm MD5 in Fuzzy RSA cryptographic is applied in attribute based cloud data integrity authentication, and in this process data holder uploads the coded files at the cloud server and then sent the auditing request to Third Party Auditor for the authentication purpose. In this algorithm data signature or hash values are created for the encrypted files with the help of public key encryption which includes homomorphic algorithm for the integrity of the information.***

Keywords: Cloud Computing, Data Integrity, Data Auditing, Data sharing, Security, ABE

I. INTRODUCTION

Services provided by cloud computing include software as a service (SaaS), platform as a service (PaaS) and hardware as a service (HaaS). Amazon, Google, Microsoft, IBM companies key corporations in cloud computing. At the instant, several users are outsourcing their knowledge to the websites of these companies. A cloud computing system, it's useful to divide it into 2 sections: the front end and also the back end. They connect to one another through a network, typically the internet. The front end is that the side the computer user, or client, sees. Cloud computing devices need to construct a copy of all its customers' info and keep it on distinctive gadgets. The copies enable the significant server to get entry to backup machines to retrieve data that otherwise would be out of attain. Making copies of facts as a backup is named redundancy.

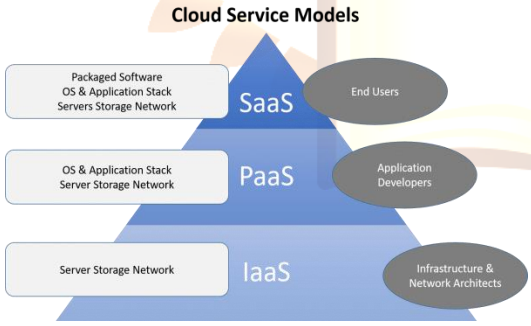

Figure 1: Cloud Computing Models

There are different types of clouds that you can subscribe to depending on your needs. As a home user or small business owner, you will most likely use public cloud services. Public Cloud - A public cloud may be accessed via any subscriber with a web connection and get entry to the cloud area. Private Cloud - A private cloud is mounted for a selected cluster or business enterprise and limits get right of entry to merely that organization. Hybrid Cloud - A hybrid cloud is a combination of at least 2 clouds, wherever the clouds covered are a combination of public, non-public, or community. As every coin has two sides, cloud computing also comprised of pros and cons. Cloud computing provides services and resources to the user to store their data or process their applications. SaaS applications are web bases applications that are delivered via the Internet through a Web browser. So, security challenges in SaaS applications are not different from any web application technology. Multi-Tenancy is a single instance of server delivered to all customers or cloud users. This approach enables more efficient and scalable use of the resources. Since sensitive data from multiple tenants is likely to be stored at same data servers. So, the security risk associated with data is very high. In any web based applications, data is often processed in plaintext. Similarly in SaaS, user data security is of prime concern. The SaaS provider is responsible for the data security while processing and storing it at cloud server. Cloud computing has emerged with concept of virtualization. So, virtual machine security is similarly important as physical machine security. VMs residing over same server shares processing unit, memory unit, I/O unit, and all others desired resources. This sharing possibly cause the security degradation of all virtual machines. As cloud computing helps multitenant structure, so, network additives are shared by means of exceptional tenants by way of aid pooling.

In recent years, the issue of data validation in cloud computing has gained importance and many researchers have proposed numerous protocols. The systems, which include data owners and cloud servers, are called private control systems. The

protocol that enables a third party to regulate data owners is termed a public surveillance system. this method includes data owner, CSS and an external reviewer. There are different models of a control protocol. These models are discussed below:

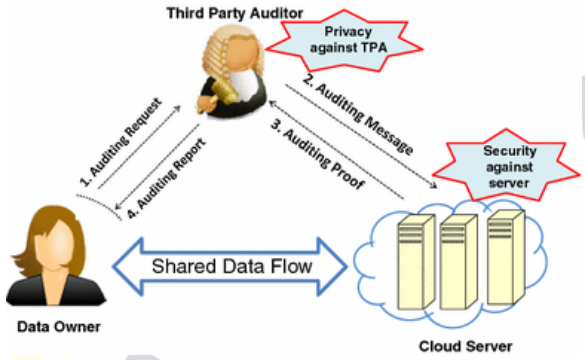

Figure 2: Basic Data Integrity Models

II. LITERATURE REVIEW

In this scenario, an authoritative review service is needed to periodically review data integrity in the cloud. In recent years, the review of data integrity on the remote server has attracted a lot of attention from researchers without having to access complete data. Patil et al. [1] used Merkle Hash Tree (MHT) for scheduling encoded information to provide structured privacy and dynamic public auditing. This technique lowers the evaluation cost and information exchanging cost. With the security of information integrity this also provides the function like input, enhance and remove.

Yong Yu et al. [2] in this research work security against false cloud server is provided by using ID based RDIC protocol which does not left any information about the stored data in the auditor which imparts the secured data against the fraud or false cloud server. Thus introduced protocol is safe and secured and used in real applications.

Sasikala [5] without downloading the complete information it provide the benefit for users to check the integrity of the exchanged data. This research provides a brief study on RDIC protocols in a cloud environment and considers the classification of RDIC protocols such as Provable Data Possession (PDP), Proof of Retrievability (POR), Proof of Ownership (POW) and ID-based RDIC protocols. R.Swathi and T.Subha [7] introduced an initial step naming improving data storage privacy in cloud using Certificate less public auditing scheme which is used to create key value. Key Generation Center (KGC) will create only the partial key which will not compromise user's private key. The KGC generates a private and public key based on a partially generated private key in order to verify the cloud data reliability of users who upload data to the server, which is then checked during the auditing process. It then sends the report to the users after it has been reviewed. Yong Yu et al. [8] To simplify key management issues, an attribute-based cloud information integrity auditing protocol was proposed. The proposed approach needs much less calculation in checking the auditing reaction, resulting in reduced time consumption.

Yannan Li [10] To our knowledge, fuzzy identity-based auditing is the first method of its kind to address the dynamic key management problem in cloud data integrity checking. Author introduced the primitive of fuzzy identity-based data auditing, in which a user's identity can be interpreted as a set of descriptive attributes. In the selective-ID security model, the author proved the security of the built protocol using the computational Diffie-Hellman assumption and the discrete logarithm assumption. Ming-quan et al. [11] proposed homomorphic encryption scheme primarily based on elliptic curve cryptography for privateness safety of cloud computing. this set of rules achieves better efficiency in phrases of computation and communication price in comparison to RSA &paillier scheme.

III. PROPOSED METHODOLOGY

The audit system at present should work with an objective to design a strong audit protocol that is public and deals with all of its challenges. The proposed protocol has been made in such a way that it will have a close look on the data stored with help of TPA. The three building blocks of the system that is proposed include: Third Party Auditor, owner of the data and cloud server storage. It is the responsibility of the data owner that their data is properly hashed and concatenation is applied on them. Also they must make sure that their file is divided into blocks, encrypting the data. Once the data is received, harsh algorithms for file blocks that are encrypted gets generated.

An algorithm similar to that utilized by the client is generated. A perfect match proves that the data is maintained in its original state and is not attacked by any external source. An if it does not, then it is a sign that the data was improperly managed and was attacked. The owner of the data then receives the result.

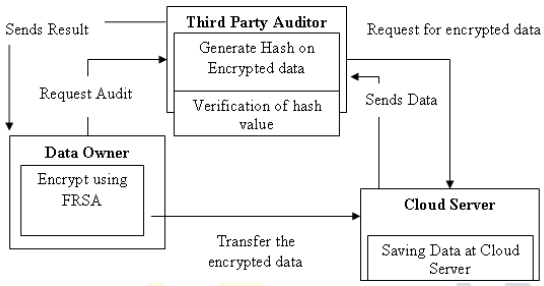

Figure 3: Proposed Flow Chart

PDP is a probabilistic detection protocol that performs cloud data integrity testing by randomly sampling data blocks rather than the entire file, which is more efficient than deterministic auditing protocols, particularly for large files.

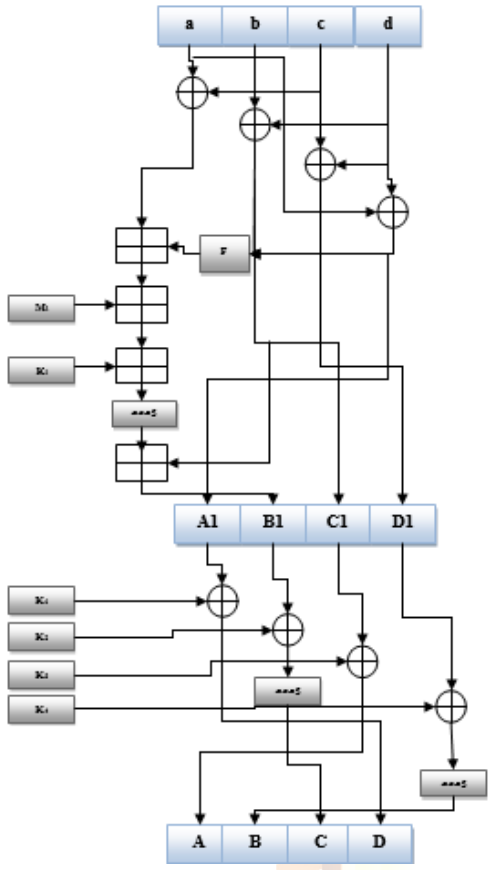

Figure 4: Process block of M-MD5

Step 1: Input data
Step 2: Encrypt data using Fuzzy RSA (FRSA).
Step 3: Divide encrypted data file into blocks of different sizes i.e. 10KB upto 100KB block size
Step 4: Generate Digital Signature of each block using M-MD5 algorithm
Step 5: Send the encrypted data blocks to the cloud data server to store these blocks.
Step 6: If user wants to check integrity of stored data or wants to audit data
{
Data owner send request to TPA
Cloud Server sends data blocks to TPA
TPA generates hash code on these blocks and send the audit report to dataowner.
}
Step 7: Exit
M-MD5 algorithm is a type of integrity-checking hashing algorithm that divides data into 512-bit blocks, which are divided into 16 words of 32 bits, and produces a fixed-size hash value of 128 bits.

The proposed MD5 algorithm flowchart, where Mi is the extended message word of round i. The round constant of the round I is called Ki. is an abbreviation for addition modulo. F is a varying non-linear function. K1, K2, K3, and K4 are the four parts of the original key.

IV. CONCLUSION

The proposed protocol preserves the confidentiality of statistics file attributes, making the main management issue in conventional cloud facts control systems easier to solve. This implementation of the proposed system demonstrates the system's usability and efficacy. On behalf of data owners, the Third Party Auditor (TPA) challenges the data server for data file integrity. Processing costs rise as block sizes grow in both GenProof and VerifyProof, but the end result is more effective in terms of existing work. During the real-time processing such light weight algorithm will help in fast auditing and does not need to download authentication data independently any more.

REFRENCES

[1] J. M. Patil and S. S. Chaudhari, "Efficient Privacy Preserving and Dynamic Public Auditing for Storage Cloud," 2019 International Conference on Nascent Technologies in Engineering (ICNTE), 2019, pp. 1-6, doi: 10.1109/ICNTE44896.2019.8945817.

[2] Yong Yu, Man Ho Au, Giuseppe Ateniese, Xinyi Huang, Willy Susilo "Identity-Based Remote Data Integrity Checking With Perfect Data Privacy Preserving for Cloud Storage" IEEE Transactions on Information Forensics and Security, Volume: 12, Issue 4, 2017, pp. 767 - 778.

[3] S. Suganya"Improving Cloud Security by Enhancing Remote Data Integrity Checking Algorithm" Innovations in Power and Advanced Computing Technologies (i-PACT) IEEE, April 2017.

[4] T.Subha"Efficient Privacy Preserving Integrity Checking Model for Cloud Data Storage Security", International Conference on Advanced Computing (ICoAC), IEEE, January 2017.

[5] C. Sasikala"A Study on Remote Data Integrity Checking Techniques in Cloud", International Conference on Public Key Infrastructure and its Applications (PKIA), IEEE, Nov. 2017.

[6] Samundiswary. S "Public Auditing for shared data in cloud with safe user revocation", International conference of Electronics, Communication and Aerospace Technology (ICECA), IEEE, 2017.

[7] R.Swathi and T.Subha, "Enhancing Data Storage Security in Cloud using Certificateless Public Auditing", International Conference on Computing and Communications Technologies (ICCCT), IEEE, February, 2017, pp. 348-352.

[8] Yong Yu, Yannan Li, Bo Yang, Willy Susilo, Guoming Yang and Jian Bai, "Attribute-Based Cloud Data Integrity Auditing for Secure Outsourced Storage". IEEE Transactions on Dependable and", IEEE Transaction on Emerging Topics in Computing, Vol. 14, No. 8, 2017.

[9] Khalid El Makkaouia,Abderrahim Beni-Hssaneb, AbdellahEzzatia, Anas El-Ansari, "Fast Cloud RSA Scheme for Promoting Data Confidentiality in the Cloud Computing", Procedia Computer Science, Volume 113, 2017, pp. 33–40.

[10] Y. Li, Y. Yu, G. Min, W. Susilo, J. Ni, K-K. R. Choo. "Fuzzy Identity-Based Data Integrity Auditing for Reliable Cloud Storage Systems", IEEE Transactions on Dependable and Secure Computing, Volume 16, issue 1, 2017, pp. 72-83.

[11] Ming-quanHong,Wen-bo Zhao, Peng-yu Wang, "Homomorphic Encryption Scheme Based on Elliptic Curve Cryptography for Privacy Protection of Cloud Computing", IEEE International Conference on Intelligent Data and Security (IDS), April 2016.