iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** XII **Month of publication:** December 2018

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue XII, Dec 2018- Available at www.ijraset.com

Third Party Auditing in Cloud Storage

Akshay Bhonde[1], Bipin Kumar[2], Bilal Momin[3], Prathamesh Shete[4], Prof. Amruta Jadhav[5]
[1, 2, 3, 4, 5]*Computer Department, Pune University*

Abstract: ***Remote data integrity checking (RDIC) enables a cloud server, to provide a proof to a verifier that it is really storing a 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 the 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 leaks no information of the stored data to the verifier during the RDIC process. The new construction is proven secure against the malicious server in the generic group model and achieves zero knowledge privacy against a verifier. Immense security analysis and implementation results demonstrate that 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 cloud reliability and trustworthiness in Cloud computing. Consequently security, integrity, privacy and confidentiality of the stored statistics and other documents on the cloud have to be considered which are essential requirements from customer's point of view. 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.

II. LITERATURE SURVEY

"Identity-Based Remote Data Integrity Checking With Perfect Data Privacy Preserving for Cloud Storage" by Yong Yu, Man Ho Au, Member, IEEE, Giuseppe Ateniese, Xinyi Huang, Willy Susilo, Yuanshun Dai, and Geyong Min. This paper addresses the file sharing and key distribution in a private cloud storage using three main ideas: [1] It can make the clients verify whether their outsourced data is kept intact without downloading the whole data.[2] In some application scenarios, the clients have to store their data on multi-cloud servers.[3] At the same time, the integrity checking protocol must be efficient in order to save the verifier's cost. "Enhanced Privacy of a Remote Data Integrity Checking Protocol for Secure Cloud Storage" by Halo et al states that the data integrity checking (RDIC) enables a server to prove to an auditor the integrity of a stored file. The auditor could be a party other than the data owner; hence, an RDIC proof is based usually on publicly available information. To capture the need of data privacy against an un-trusted auditor, Hao et al. formally defined "privacy against third party verifiers" as one of the security requirements and proposed a protocol satisfying this definition. "Identity-Based Distributed Provable Data Possession in Multi-cloud Storage" by Huaqun Wang, School of Information Engineering, Dalian Ocean University, Dalian, China. The proposed ID-DPDP protocol is provably secure under the hardness assumption of the standard CDH (computational Diffie-Hellman) problem. In addition to the structural advantage of elimination of certificate management, our ID-DPDP protocol is also efficient and flexible. Based on the client's authorization, the proposed ID-DPDP protocol can realize private verification, delegated verification, and public verification. Encrypt/Decrypt Data: The Advanced Encryption Standard (AES) algorithm is one of the block cipher encryption algorithms that were published by National Institute of Standards and technology (NIST) in 2000. The main aims of this algorithm were to replace DES algorithm after appearing some vulnerable aspects of it. NIST invited experts who work on encryption and data security all over the world to introduce an innovative block cipher algorithm to encrypt and decrypt data with powerful and complex

©IJRASET: All Rights are Reserved

structure. One of the most crucial aspects that NIST was considered to choose algorithm it is security. The main reasons behind this was obvious because of the main aims of AES was to improve the security issue of DES algorithm. AES has the best ability to protect sensitive data from attackers and is not allowed them to break the encrypt data as compared to another proposed algorithm. This was achieved by doing a lot of testing on AES against theoretical and practical attack.

III. EXISTING SYSTEM

Privacy preserving for the user data stored in a storage server like cloud server forms a complex task with performance and the maintenance issue alongside the security overheads. Storing data in the cloud has become a trend. An increasing number of clients store their important data in remote servers in the cloud, without leaving a copy in their local computers. Sometimes the data stored in the cloud is so important that the clients must ensure it is not lost or corrupted. Hence, a lot of work has been done on designing remote data integrity checking protocols, which allow data integrity to be checked without completely downloading the data. However, several issues aren't been fully investigated.

IV. LIMITATIONS

A. Data can be manipulated during upload or downloading of documents.
B. Most of the RDIC protocols create an issue of generating key to protect the privacy of user data stored in cloud.

V. PROPOSED SYSTEM

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.

A. Advantages Of Proposed System

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

VI. SYSTEM ARCHITECTURE

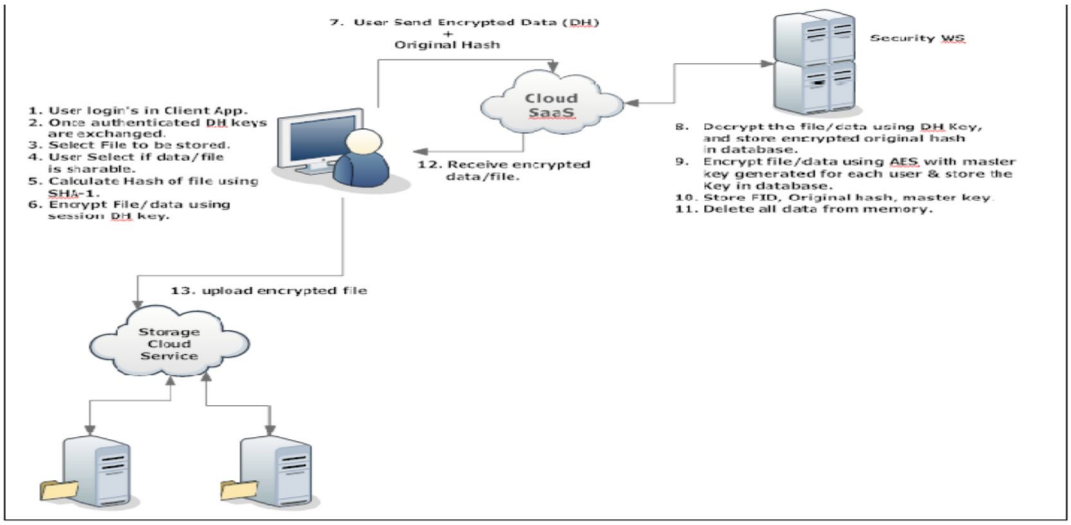


Figure1. Proposed System Architecture (Uploading/Encryption Phase)

©IJRASET: All Rights are Reserved

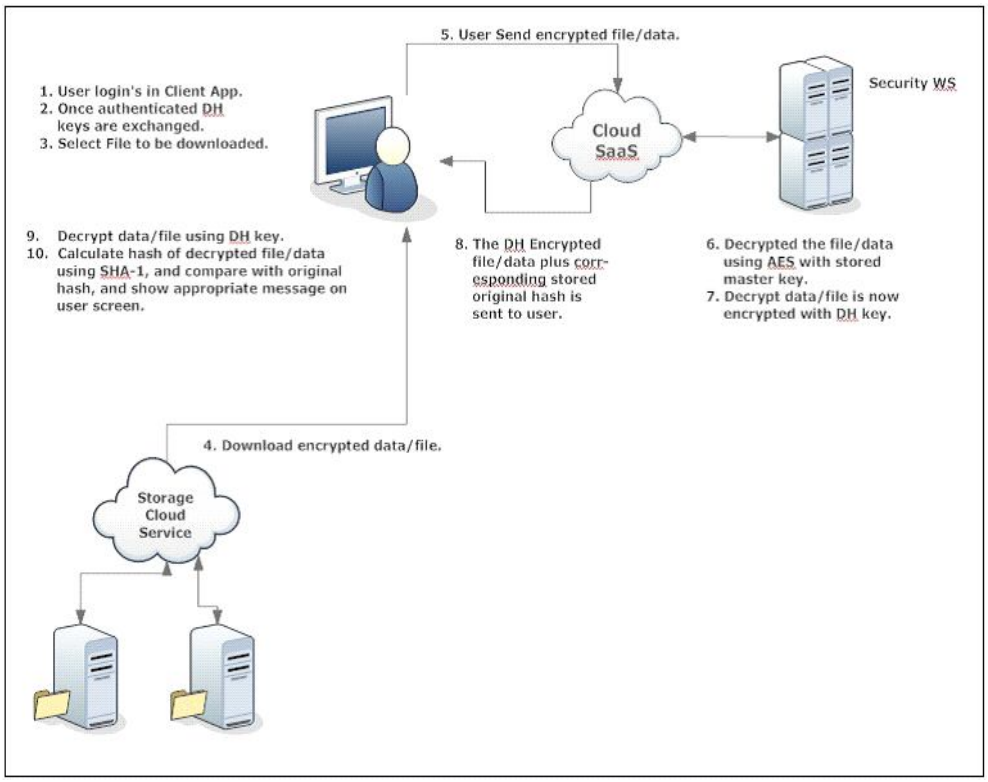


Figure2. Proposed System Architecture (Downloading/Decryption Phase)

VII. CONCLUSION

Cloud computing is an 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 help 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] "Identity-Based Remote Data Integrity Checking With Perfect Data Privacy Preserving for Cloud Storage" by Yong Yu, Man Ho Au, Member, IEEE, Giuseppe Ateniese, Xinyi Huang, Willy Susilo, Yuanshun Dai, and Geyong Min.

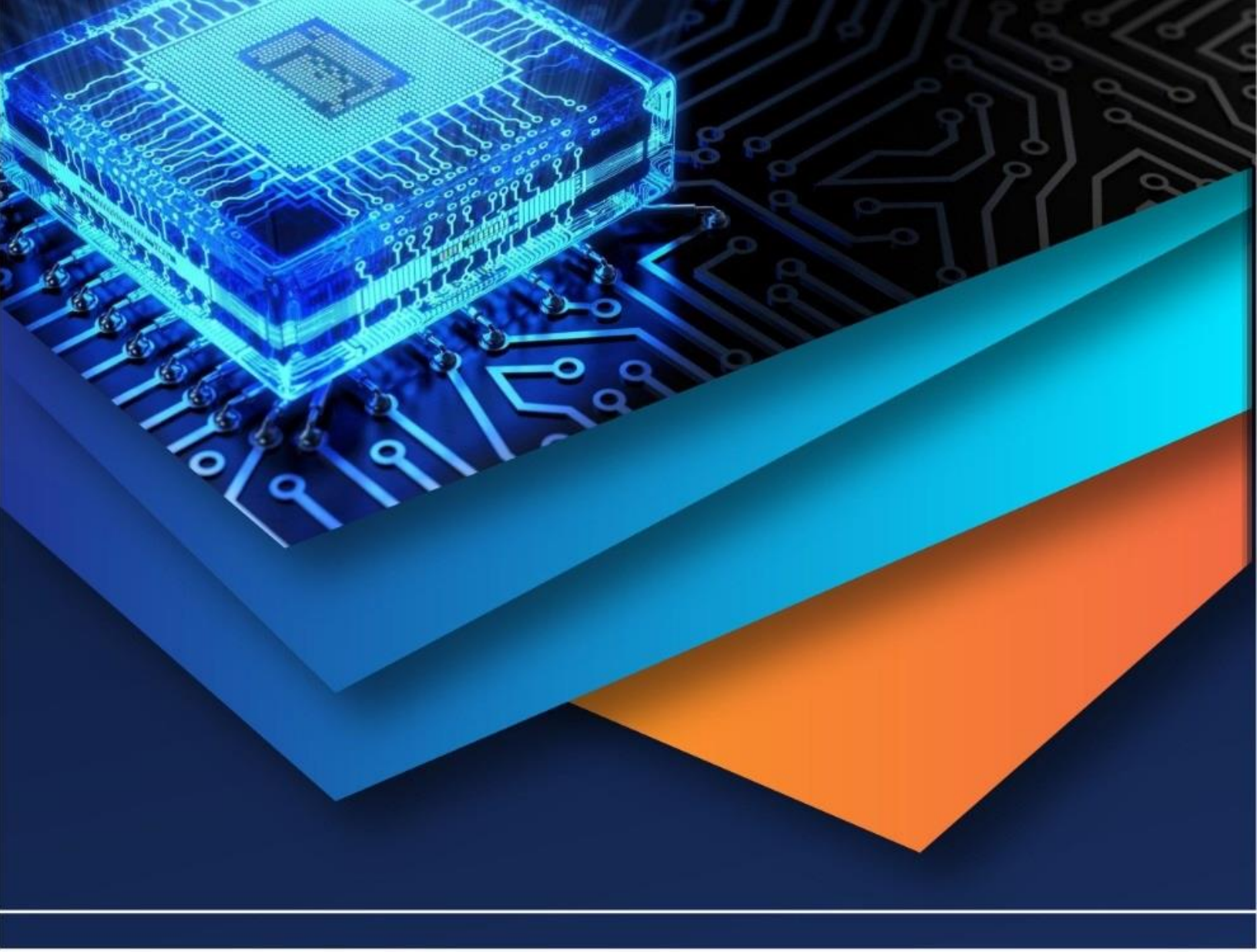
[2] "Enhanced Privacy Of A Remote Data Integrity Checking Protocol For Secure Cloud Storage" by Hao et al states that emote data integrity checking (RDIC) enables a server to prove to an auditor the integrity of a stored file.

[3] "Identity-Based Distributed Provable Data Possession in Multi-cloud Storage" by Huaqun Wang, School of Information Engineering, Dalian Ocean University, Dalian, China.

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

[5] C. Wang, Q. Wang, K. Ren, N. Cao, W. Lou, "Toward Secure and Dependable Storage Services in Cloud Computing," IEEE Transactions on Services Computing, 5(2), pp. 220-232, 2012.

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)