International Journal of Research
Available at https://pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 20
September 2018

A New Primitive Secure Identity-Based Authentication Framework for Data Storage in Cloud

Naziya Yasmeen & S G Nawaz Hod
[1] M.Tech Student, Dept of CSE, SKD Engineering College, Affiliated to JNTUA, AP, India
[2] Associate Professor & HOD, Dept of CSE, SKD Engineering College, Affiliated to JNTUA, AP, India

ABSTRACT:
The fact that users no longer have physical possession of the possibly large size of outsourced data makes the data integrity protection in Cloud Computing a very challenging and potentially formidable task, especially for users with constrained computing resources and capabilities. Thus, enabling public auditability for cloud data storage security is of critical importance so that users can resort to an external audit party to check the integrity of outsourced data when needed. Up to the date, a number of Remote data integrity checking (RDIC) protocols have been proposed but most of the constructions suffer from the issue of a complex key management, they depend on the expensive public key infrastructure (PKI), which might delay the deployment of RDIC in performance. In this paper, a new approach of identity-based (ID-based) RDIC protocol is proposed by using key-homomorphic cryptographic primitive to reduce the system complexity and the cost for establishing and managing the public key authentication framework. The proposed ID-based RDIC protocol doesn't leaks any information of the stored data to the verifier during the RDIC process. The new method is demonstrated with secure against the malicious server in the generic group model and achieves zero knowledge privacy against a verifier.

Keywords: Cloud storage, data integrity, privacy preserving, identity-based cryptography.

I. INTRODUCTION

The emergence of cloud computing brings a revolutionary innovation to the management of the data resources. Within this computing environments, the cloud servers can offer various data services, such as remote data storage and outsourced delegation computation etc. For data storage, the servers store a large amount of shared data, which could be accessed by authorized users. For delegation computation, the servers could be used to handle and calculate numerous data according to the user's demands. However, there is a vast variety of barriers before cloud computing can be widely deployed. A recent survey by Oracle referred the data source from international data corporation enterprise panel, showing that security represents 87% of cloud users fears. One of the major security concerns of cloud users is the integrity of their outsourced files since they no longer physically possess their data and thus lose the control over their data. Moreover, the cloud server is not fully trusted and it is not mandatory for the cloud server to report data loss incidents. Indeed, to ascertain cloud computing reliability, the cloud security alliance (CSA) published an analysis of cloud vulnerability incidents. The investigation revealed that the incident of data Loss & Leakage accounted for 25% of all incidents, ranked second only to "Insecure Interfaces & APIs". Take Godaddy's cloud crash disaster as an example. In 2017, Godaddy's cloud services crash permanently destroyed some data of cloud users. The data loss was apparently small relative to the total data stored, but anyone who runs a website can immediately understand how terrifying a prospect any data loss is. Sometimes it is insufficient to detect data corruption when accessing the data because it might be too late to recover the corrupted data. As a result, it is necessary for cloud users to frequently check if their outsourced data are stored properly.

The size of the cloud data is huge, downloading the entire file to check the integrity might be prohibitive in terms of bandwidth cost, and hence, very impractical.

Moreover, traditional cryptographic primitives for data integrity checking such as hash functions, authorization code (MAC) cannot apply here directly due to being short of a copy of the original file in verification. In conclusion, remote data integrity checking for secure cloud storage is a highly desirable as well as a challenging research topic.

II. LITERATURE SURVEY

1) Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, Enabling public verifiability and data dynamics for storage security in cloud computing.

Cloud Computing has been envisioned as the next-generation architecture of IT Enterprise. It moves the application software and databases to the centralized large data centers, where the management of the data and services may not be fully trustworthy. This unique paradigm brings about many new security challenges, which have not been well understood. This work studies the problem of ensuring the integrity of data storage in Cloud Computing. In particular, we consider the task of allowing a third party auditor (TPA), on behalf of the cloud client, to verify the integrity of the dynamic data stored in the cloud. The introduction of TPA eliminates the involvement of client through the auditing of whether his data stored in the cloud is indeed intact, which can be important in achieving economies of scale for Cloud Computing. The support for data dynamics via the most general forms of data operation, such as block modification, insertion and deletion, is also a significant step to- ward practicality, since services in Cloud Computing are not limited to archive or backup data only. While prior works on ensuring remote data integrity often lacks the support of either public verifiability or dynamic data operations, this paper achieves both. We first identify the difficulties and potential security problems of direct extensions with fully dynamic data updates from prior works and then show how to construct an elegant verification scheme for seamless integration of these two salient features in our protocol design. In particular, to achieve efficient data dynamics, we improve the Proof of Retrievability model by manipulating the classic Merkle Hash Tree (MHT) construction for block tag authentication. Extensive security and performance analysis show that the proposed scheme is highly efficient and provably secure.

2) C. Wang, Q. Wang, K. Ren, and W. Lou, Privacy-preserving public auditing for data storage security in cloud computing.

Cloud Computing is the long dreamed vision of computing as a utility, where users can remotely store their data into the cloud so as to enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources. By data outsourcing, users can be relieved from the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the possibly large size of outsourced data makes the data integrity protection in Cloud Computing a very challenging and potentially formidable task, especially for users with constrained computing resources and capabilities. Thus, enabling public auditability for cloud data storage security is of critical importance so that users can resort to an external audit party to check the integrity of outsourced data when needed. To securely introduce an effective third party auditor (TPA), the following two fundamental requirements have to be met: 1) TPA should be able to efficiently audit the cloud data storage without demanding the local copy of data, and introduce no additional on-line burden to the cloud user; 2) The third party auditing process should bring in no new vulnerabilities towards user data privacy. In this paper, we utilize and uniquely combine the public key based homomorphic authenticator with random masking to achieve the privacy-preserving public cloud data auditing system, which meets all above requirements. To support efficient handling of multiple auditing tasks, we further explore the technique of bilinear aggregate signature to extend our main result into a multi-user setting, where TPA can perform multiple auditing tasks simultaneously. Extensive security and performance analysis shows the proposed schemes are provably secure and highly efficient.

3) Y. Zhu, H. Hu, G. J. Ahn, S. S. Yau, Efficient audit service outsourcing for data integrity

Cloud-based outsourced storage relieves the client's burden for storage management and maintenance by providing a comparably low-cost, scalable, location-independent platform. However, the fact that clients no longer have physical possession of data indicates that they are facing a potentially formidable risk for missing or corrupted data. To avoid the security risks, audit services are critical to ensure the integrity and availability of outsourced data and to achieve digital forensics and credibility on cloud computing. Provable data possession (PDP), which is a cryptographic technique for verifying the integrity of data without retrieving it at an untrusted server, can be used to realize audit services. In this paper, profiting from the interactive zero-knowledge proof system, we address the construction of an interactive PDP protocol to prevent the fraudulence of prover (soundness property) and the leakage of verified data (zero-knowledge property). We prove that our construction holds these properties based on the computation Diffie-Hellman assumption and the rewindable black-box knowledge extractor. We also propose an efficient mechanism with respect to probabilistic queries and periodic verification to reduce the audit costs per verification and implement abnormal detection timely. In addition, we present an efficient method for selecting an optimal parameter value to minimize computational overheads of cloud audit services. Our experimental results demonstrate the effectiveness of our approach.

III. EXISTING METHOD:

Ateniese et al. proposed two concrete PDP constructions by making use of RSA-based homomorphic linear authenticators. Due to its necessity and practicability, remote data integrity checking has attracted extensive research interest in recent years. Shacham and Waters proposed the notion of compact proofs of retrievability by making use of publicly verifiable homomorphic authenticators from BLS signature. This scheme also relies on homomorphic properties to aggregate a proof into a small authenticator value and as a result, the public retrievability can be achieved.
Ateniese et al. considered dynamic PDP scheme for the first time based on hash functions and symmetric key encryptions. This scheme is efficient but has only limited number of queries and block insertion cannot explicitly be supported. Erway et al. extended the PDP model to dynamic PDP model by utilizing rank-based authenticated skip lists. Wang et al. improved the previous PDP models by manipulating the Merkle Hash Tree (MHT) for block tag authentication. A recent work due to Liu et al. showed that MHT itself is not enough to verify the block indices, which may lead to replace attack.

DISADVANTAGES OF EXISTING SYSTEM:

- MHT itself is not enough to verify the block indices, which may lead to replace attack.

International Journal of Research
Available at https://pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 20
September 2018

- ❖ A formal security model is not provided.
- ❖ But their model works only in public key infrastructure (PKI) based scenario instead of the identity-based framework

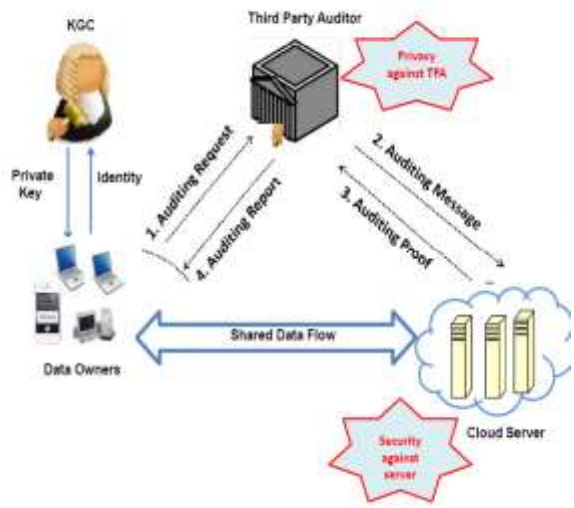
IV. PROPOSED METHOD:

- ❖ In an ID-based signature scheme, anyone with access to the signer's identity can verify a signature of the signer. Similarly, in ID-based RDIC protocols, anyone knowing a cloud user's identity, say a third party auditor(TPA), is able to check the data integrity on behalf of the cloud user. Thus, public verifiability is more desirable than private verification in ID-based RDIC, especially for the resource constrained cloud users. In this case, the property of zero-knowledge privacy is highly essential for data confidentiality in ID-based RDIC protocols.
- ❖ Our first contribution is to formalize the security model of zero knowledge privacy against the TPA in ID-based RDIC protocols for the first time.
- ❖ We fill the gap that there is no a secure and novel ID based RDIC scheme to date. Specifically, we propose a concrete ID-based RDIC protocol, which is a novel construction that is different from the previous ones, by making use of the idea of a new primitive called asymmetric group key agreement.
- ❖ To be more specific, our challenge-response protocol is a two party key agreement between the TPA and the cloud server, the challenged blocks must be used when generating a shared key, which is a response to a challenge from the TPA, by the cloud server.

ADVANTAGES OF PROPOSED METHOD:

- ❖ This is the first correct security proof of ID-based RDIC protocol. Thus, the new security proof method itself may be of independent interest.
- ❖ We show the practicality of the proposal by developing a prototype implementation of the protocol.

SYSTEM ARCHITECTURE



V. MODULES

1. Attribute Authority:

Authority will have to offer the key, as per the user's key request. Every users request can have to be raised to authority to induce access key on mail. There are 2 complementary forms of attribute-based secret writing. One is key-policy attribute-based secret writing (KP-ABE) and the alternative is ciphertext-policy attribute-based encryption (CPABE). In a KP-ABE system, the decision of access policy is created by the key distributor rather than the encipherer, which limits the usefulness and usability for the system in sensible applications.

2. Cloud Server:

Cloud server will have the access to files that square measure uploaded by the information owner Cloud server needs to decipher the files offered underneath their permission.

Furthermore information user can have to decipher the info to access the initial text by

International Journal of Research
Available at https://pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 20
September 2018

providing the individual key. File has been decrypted successfully and provided for shopper.

3. Data owner:

Data owner can have to register initio to induce access to the profile. Data Owner can transfer the file to the cloud server in the encrypted format. Random encryption key generation is happening whereas uploading the file to the cloud. Encrypted file will be hold on the cloud.

4. Data Consumer:

Data shopper can be initio raise for the key to the Authority to verify and decipher the enter the cloud. Data shopper will access the file primarily based on the key received from mail id. As per the key received the consumer will verify and decipher the info from the cloud.

VI. CONCLUSION

In this paper, a new approach of identity-based (ID-based) RDIC protocol is implemented by using key-homomorphic cryptographic primitive to reduce the system complexity and the cost for establishing and managing the public key authentication framework. The implemented ID-based RDIC protocol doesn't leaks any information of the stored data to the verifier during the RDIC process. The new method is demonstrated with secure against the malicious server in the generic group model and achieves zero knowledge privacy against a verifier.

REFERENCES

[1] J. Liu, K. Huang, H. Rong, H. M. Wang, Privacy-preserving public auditing for regenerating-code-based cloud storage, IEEE Trans. on Information Forensics and Security, 10(7): 1513–1528, 2015.
[2] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, Enabling public verifiability and data dynamics for storage security in cloud computing. Proc. of ESORICS2009, LNCS 5789, 355–370, 2009.
[3] C. Wang, Q. Wang, K. Ren, and W. Lou, Privacy-preserving public auditing for data storage security in cloud computing. Proc of IEEE INFOCOM 2010, 525–533, 2010.
[4] C. Wang, K. Ren, W. Lou, and J. Li, Toward publicly auditable secure cloud data storage services. IEEE Network, 24, 19-24, 2010.
[5] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, Enabling public audibility and data dynamics for storage security in cloud computing. IEEE Trans. Parallel Distrib. Syst., 22, 847-859, 2011.
[6] C. Wang, S. S.Chow, Q. Wang, K. Ren, and W. Lou, Privacy-preserving public auditing for secure cloud storage. IEEE Trans. on Computers, 62, 362-375, 2013.
[7] K. Yang, and X. Jia. An efficient and secure dynamic auditing protocol for data storage in cloud computing. IEEE Trans. on Parallel and Distributed Systems, 24(9): 1717-1726, 2013.
[8] Y. Zhu, G. J. Ahn, H. Hu, S. S. Yau, H. G. An, C. J. Hu, Dynamic audit services for outsourced storages in Clouds. IEEE Trans. Services Computing, 6(2): 227-238, 2013.
[9] Y. Zhu, H. Hu, G. J. Ahn, S. S. Yau, Efficient audit service outsourcing for data integrity in clouds. Journal of Systems and Software, 85(5): 1083-1095, 2012.
[10] H. Wang, Y. Zhang, On the knowledge soundness of a cooperative provable data possession scheme in multicloud storage, IEEE Trans. on Parallel and Distributed System, 25(1): 264–267, 2014.