A Survey Paper on Identity Based Remote Data Integrity Checking

Dipak Pawar[1] Rajesh Kasar[2] Tejswee Gaikwad[3] Naresh Jadhav[4]
[1,2,3,4]Department of Information Technology
[1,2,3,4]SND COE & RC, Yeola, Dist- Nashik, State- Maharashtra, India

Abstract— In this 21 Century (RDIC) enables a data storage server to prove to a verified that it is actually storing a Customer or User data truthfully. up to now, a number of RDIC protocols have been planned in the literature, but most of the construction undergo from the issue of a difficult key management, that is, they rely on the cheap public key Infrastructure, which might hinder the deployment of RDIC in practice. In this paper, we propose a new construction of identity-based (ID-based) RDIC protocol by making use of key-homomorphism cryptographic primitive to reduce the system complexity and the cost for establish and manage the public key authentication template in PKI based RDIC schemes. We formalize ID-based RDIC and its security model including security against a malicious cloud server and zero knowledge privacy against a third party verified. The proposed ID-based RDIC protocol leaks no information of the stored data to the verified during the RDIC process. The new construction is prove secure against the malicious server in the generic group mode and achieves zero knowledge privacy against a verified. Wide security study and execution results demonstrate that the proposed protocol is prove secure and practical in the real-world applications.

Key words: RDIC, PKI, CSA, TPA

I. INTRODUCTION

Cloud computing [1], which has received considerable attention from research communities in academia as well a industry, is a distributed computation model over a large pool of shared-virtualized computing resources, such as storage processing power, applications and services. Cloud users are provisioned and release recourses as they want in cloud computing environment. This kind of new computation mode represents a new vision of providing computing services as public utilities like water and electricity. Cloud computing brings a number of benefits for cloud users. For example, (1 Users can reduce capital expenditure on hardware, software and services because they pay only for what they use; (2) User can enjoy low management overhead and immediate access to a wide range of applications; and (3) Users can access their data wherever they have a network, rather than having to stay nearby their computers.

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' fears1. One of the large security issues of cloud users is the integrity of their outsourced files since they no longer physically hold 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 report data loss incidents. Certainly, to ascertain cloud computing trustworthiness, the cloud security alliance (CSA) published an analysis of cloud exposure incidents. The investigation [2] revealed that the incident of data Loss & Leakage accounted for 25% of all incidents, ranked second only to "Insecure Interfaces & APIs". Take Amazon's cloud crash disaster as an example2. In 2011, Amazon's huge EC2 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.

Occasionally, Cloud data is very Big in size, downloading the entire File and then check the integrity might be excessive in terms of Bandwidth cost, and hence, very not practical. 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 highly secure cloud large storage as well as Small is a highly desirable as well as a Challenging research topic.

Blum proposed an auditing issue for the first time that enables data owners to verify the integrity of remote data without explicit knowledge of the entire data [3]. Recently, remote data integrity checking becomes more and more significant due to the development of distributed storage systems an online storage systems. Provable data possession (PDP) [4], [5] at untrusted stores, introduced by Ateniese et al., is a novel technique for "block less validating" data integrity over remote servers. In PDP, the data owner generates some metadata for a file, and then sends his data file together with the metadata to a remote server and deletes the file from its local storage to generate a proof that the server stores the original file correctly, the server computes a response to a challenge from the verifier. The verifier can verify if the file keeps unchanged via checking the correctness of the response. PDP is a practical approach to checking the integrity of cloud data since it adopts a spot-checking technique. Specifically, a file is divided into blocks and a verifier only challenges a small set of randomly chosen clocks for integrity checking. According to the example given by Ateniese et al. [4], for a file with 10; 000 blocks, if the server has deleted 1% of the blocks, then a verifier can detect server's misbehavior with probability greater than 99% by asking proof of possession for only 460 randomly selected blocks. Ateniese et al. proposed two concrete PDP constructions by making use of RSA-based homomorphism linear authenticators. Waters proposed the notion of compact proofs of irretrievability by making use of publicly verifiable homomorphism authenticators from BLS signature. This scheme also relies on homomorphism properties to aggregate a proof into a small authenticator value and as a result, the public irretrievability can be achieved.

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

II. LITERATURE SURVEY

Cong Wang, Sherman SM Chow, Qian Wang, Kui Ren, and Wenjing Lou, Privacy Preserving Public Auditing for Secure Cloud Storage Using cloud storage, users can remotely store their data and enjoy the on-demand high-quality applications and services from a shared pool of configurable computing resources, without the burden of local data storage and maintenance. However, the reality that users no long Time have physical Access of their outsourced data makes the data integrity guard in cloud computing a redoubtable task, especially for users with embarrassed computing resources. Sometimes, users should be able to just use the cloud storage as if it is local Storage, without any worry about the necessity to verify its integrity. Thus, allow open audit capability for cloud storage is mostly critical so that users can option to a third-party auditor (TPA) to check the truthfulness of their outsourced data and be worry free. To securely introduce an effective TPA, the auditing process should bring in no new vulnerabilities toward user data privacy, and introduce no additional online burden to user. In this paper, they proposed a secure cloud storage system supporting privacy-preserving public auditing. They furthered extend their result to enable the TPA to perform audits for multiple users simultaneously and efficiently. Big security and presentation analysis show the designed schemes are provably secluded and highly able. Their preliminary research conducted on Amazon EC2 instance. 13 RDIC with Data Privacy protect further demonstrate the fast performance of the design.

Tejaswini, K. Sunitha, and S. K. Prashanth. Privacy Preserving and Public Auditing Service for Data Storage in Cloud Computing. The cloud computing model represents a new paradigm shift in internet based services that deliver highly scalable distributed computing platforms in which computational resources are occurred red as a service. Security is considered one of the top ranked open issues in adopting the cloud computing model includes data Integrity. Wang planned a enabling community audit capability and data dynamics for storage protection in cloud computing. They achieved the integrity guarantee of data storage with support of public audit ability and dynamic data operations. However their protocol lacks in providing privacy of data which is one of the issue for the cloud data storage. In this they proposed a privacy preserving public variability for integrity of data storage in cloud computing. They have used RSA public cryptography to provide congeniality of data. Their scheme is more secure than existing system

III. PROPOSED SYSTEM

Always, data owners or user themselves can check the integrity of their cloud data by running a two-party RDIC protocol However, the auditing result from either the data owner or the cloud server might be regarded as biased in a two part scenario. The RDIC protocols with public verifiability enable anyone to audit the integrity Of the outsourced data. To make the explanation of the publicly provable RDIC protocols visibly, we assume there exists a third party auditor (TPA) who has skill and capabilities to do the verification work. With this in mind, the ID-based RDIC architecture is illustrated in Fig 1. Four different entities namely the KGC, the cloud user, the cloud server and the TPA are involved in the system. The KGC generates secret keys for all the users according to their identities. The cloud user has large amount of files to be stored on cloud without keeping a local copy, and the cloud server has significant storage space and computation resources and provides data storage services for cloud users. TPA has expertise and capabilities that cloud users do not have an is trusted to check the integrity of the cloud data on behalf of the cloud user upon request. Each entity has their own obligations and benefits respectively. The cloud server could be self-interested, and for his own benefits, such as to maintain a good reputation, the cloud server might even decide to hide data corruption incidents to cloud users. However, we assume that the cloud server has no incentives to reveal the hosted data to TPA because of regulations and financial incentives. The TPA's job is to perform the data integrity checking on behalf the cloud user, but the TPA is also curious in the sense that he is willing to learn some information of the users' data during the data integrity checking procedure.

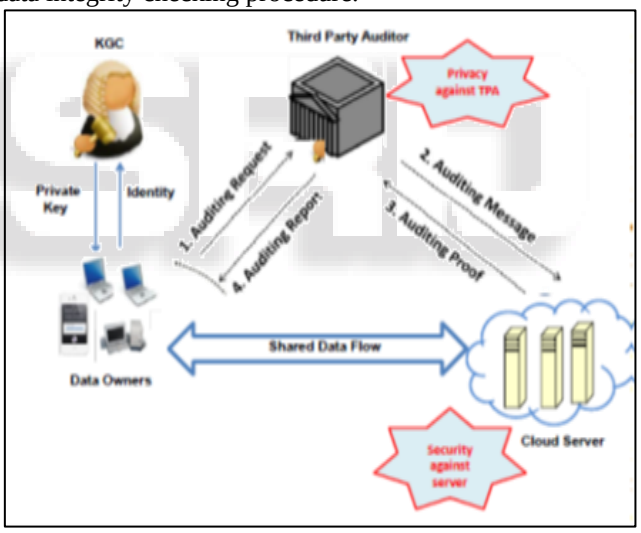

Fig. 1: System Architecture

IV. CONCLUSION

In this Research paper, we investigate an innovative prehistoric called identity-based remote data integrity checking for protected cloud storage. We dignified the security model of two imperative properties of this primitive, namely, reliability and perfect data privacy. We provided a new construction of this primitive and showed that it achieves soundness and ideal data privacy. Both the numerical analysis and the implementation program. For New Center Excellent Talents in Fujian University (JA14067) and the Fundamental Research Funds for the Central Universities under Grant ZYGX2015J059.

REFERENCES

[1] Q. Wu, Y. Mu, W. Susilo, B. Qin, J. Domingo-Ferrer, Asymmetric group key agreement. Proc. of Eurocrypt 2009, LNCS 5479, 153–170, 2009.
[2] L. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin, Z. Dong, Roundefficient and sender-unrestricted dynamic group key agreement protocol for secure group communications. IEEE Transactions on Information Forensics and Security, 10(11): 2352–2364, 2015.
[3] Shoup, Lower bounds for discrete logarithms and related problems, Proc. of Eurocrypt 1997, 256–266, 1997.
[4] Y. Yu, Y. Zhang, Y. Mu, W. Susilo, Provably Secure Identity based Provable Data Possession. Proc. of ProvSec 2015, LNCS 9451, 1–16, 2015.
[5] D. Boneh, B.Lynn, and H. Shacham, Short signatures from the weil pairing. Journal of Cryptology, 17, 297–319, 2004.
[6] D. Chaum, T. P. Pedersen, Wallet databases with observers. Proc. Of Crypto 1992, 89–105, 1993.
[7] J. C. Cha, and J. H. Cheon, An identity-based signature from gap Diffie- Hellman groups, in: Processing of PKC 3003, LNCS 2567, 2003, pp. 18-30.

