ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
Vol. 2, Issue 2, February 2015

Concise Survey on Privacy Preserving Techniques in Cloud

B.Banu priya[1], V.Sobhana[2], Prof.Mishmala Sushith[3]

Department of IT, Kalaignar Karunanidhi Institute of Technology, Coimbatore, TamilNadu, India[1,2,3]

Abstract: In this paper we have made a concise survey on various privacy preserving techniques in cloud. Homomorphic Authenticable Ring Signature (HARS), privacy-preserving public auditing System for data storage security are discussed. Public key cryptosystem, the MD5 Message-Digest Algorithm are depicted. Proof-Of-Retrievability system for public verifiability is described. Dynamic Provable Data Possession (DPDP) to enlarge the PDP model is discussed in detail. LT codes based cloud storage service (LTCS) to empower efficient decoding, Merkle Hash Tree (MHT) for the block tag Authentication is discussed.

Keywords: Privacy Preserving, Public Auditing, DPDP, PDP, Cloud Computing.

I.INTRODUCTION

Cloud computing is the practice of using a network of remote servers hosted on the Internet to store, manage, and process data rather than a local server or a personal computer. The privacy preserving supports the public auditing without the retrieval access of entire data blocks. The privacy preserving public auditing is used to integrate the homomorphic authenticated with random masking technique. proof-of-retrievability system is used for public verifiability. Several privacy preserving techniques in the cloud has been dealt detail in this paper.

II.NEED FOR CLOUD COMPUTING

The cloud computing explained in hardware point of view and software point of view. The advantages of SAAS in cloud is also explained. The authors listed the various Conditions that influence the organizations to become the cloud computing providers. The location for the data centers need to be selected properly in order to reduce the electricity cost. Many new types of applications have been developed with the help of cloud computing. The obstacles and opportunities for the cloud computing is been explained. The bottle necks are used in cloud. The software like application software, hardware systems are been explained in this paper [2].

III.HOMOMORPHIC AUTHENTICATORS IN CLOUD PRIVACY

The first privacy preserving public auditing mechanism to audit the shared data in cloud. Ring signature are been Used to construct the homomorphic authenticators. The Third Party Auditor (TPA) can audit but do not know the user on each block. Batch auditing can be used to audit multiple task. The Ring Signature used in the construction of ORUTA will increase the size of storage space. Homomorphic Authenticable Ring Signature (HARS), a novel idea is used in this paper. The HARS is been extended from the classic ring signature scheme [1] .The new paradigm for cloud computing. Data protection as a service is the paradigm designed in this paper. The authors also used two different approaches to data privacy they are full-disk encryption and computation on encrypted data. In the full-disk encryption (FDE) the entire physical disks are encrypted for the simplicity and speed. The fully homomorphic encryption (FHE) is used for computation on cipher texts. When comparing FDE and FHE, the FDE has high performance than FHE. The access control list is used for the user access. The same phenomenon can be used in the batch process, but it has a different logging granularity. Some of the challenges in this paper are how to migrate for existing applications and can technology be standardized across platforms [3]. The privacy-preserving public auditing system for data storage security in cloud computing. The privacy preserving supports the public auditing without the retrieval access of entire data blocks. The privacy preserving public auditing can be used to integrate the homomorphic authenticated with random masking technique. They proposed this scheme as setup phase and audit phase. The public auditing scheme has four algorithms they are KeyGen, SigGen, GenProof, VerifyProof. The privacy preserving public auditing supports for batch auditing. Third Party Auditor (TPA) can handle multiple auditing delegations between different users request. But the individual auditing is very difficult in TPA. So the author deals that we can use TPA to perform the multiple auditing tasks in a batch process concurrently. The auditing system in the cloud server is been illustrated in fig 1.The block of message is sent to the auditor for checking integrity [4].

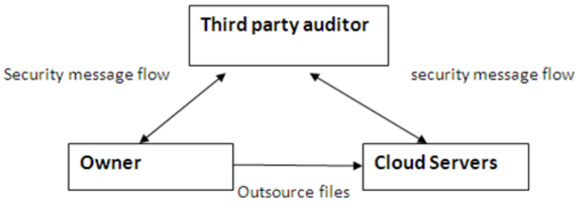

Figure: 1. Third Party Auditor (TPA)

The scheme proof-of retrievability system. The author used BLS signatures and secure in the random oracle model to build the first scheme. This scheme is used to let on public verifiability. The second scheme frames on the pseudo random functions (PRFs), this is used only for private verification. The proof-of-storage scheme is used to boost the response length of the simple MAC-based scheme using homomorphic authenticators. In this paper the author built two contributions. The first one is on the PRFs. The second one is based on the BLS signatures. In the first scheme the user breaks the erasure encoded file. In the second scheme it is publicly verifiable. This uses BLS signatures to authenticate values that can be publicly verifiable [8].

Copyright to IARJSET
DOI 10.17148/IARJSET.2015.2206

IV.THE MD5 ALGORITHM AND LT CODES

The MD5 Message-Digest Algorithm describes that algorithm takes the input as message of arbitrary length and produces output as 128-bit “finger print” or “message digest” of the given input. This algorithm can be used for digital signature applications. So that large type of files can be “compressed” in a secure way before the encryption can be made with private key under the public key cryptosystem for example RSA. There are five steps to compute the message digest of the message. The message is extended so that the bit length is congruent to 448, modulo 512. A 64-bit representation is made with B and the result is added with the previous step. The algorithm consists of four word buffer to compute the message digest. The four auxiliary functions need to be defined first. It takes input as three 32-bit words and produce output as one 32-bit word. The message digest produce output as A,B,C,D. Starts with low-order byte A and end with high-order of byte D [7]. The designed LT codes based cloud storage service (LTCS). The author has examined the problem of secure and reliable cloud storage. The author has used low complexity LT codes to empower efficient decoding for data users in the data retrieval process. The fast belief propagation decoding algorithm is been used for the adequate data retrieval. The LTCS has less storage cost and faster data retrieval than network coding-based storage services. The future work of this paper is to detect the decidability. The LT codes generate vast number of encoded packets by performing bitwise XOR algorithm on a subset of original packets [13].

V.PRIVACY PRESERVING TECHNIQUES

The author proposed two schemes for the secure outsourced computation over cloud data encrypted under the multiple keys. The author used to non-colluding cloud servers that are used to compute polynomial functions over the multiple users. The author also demonstrated those schemes experimentally through applications in the machine learning. These schemes are applicable for the privacy preserving. The cloud data must be encrypted with multiple keys to preserve the privacy. Existing secure computation use only single key but in this paper the author used multiple keys for computations [5]. The suggested a new encryption method. The method uses the public key cryptosystem. The public key cryptosystem means each user keeps their public file in an encryption procedure E. The user keeps the secure details of the decryption procedure D. Encryption is used to provide privacy. The signed messages have to be re-blocked for the encryption process. The author used a threshold value (h) for the public key cryptosystem. The cipher text is recursively deciphered to produce a value less than h. There are no techniques to prove that the encryption scheme is more secure. The only way is to break it. The author says that the paper needed to be examined in more detail [6]. The presented a framework and efficient constructions for Dynamic provable Data Possession(DPDP) which enlarge the PDP model to support the provable updates to stored data. In this model the data is reprocessed by the client and metadata used for verification purposes is produced.PDP can be applied only to the case of static, archival storage that is file can be expand and never changes. Author defined an update as either insertion of a new block or modification of an existing block or deletion of any block. Their update operation is to perform modifications as per the client wish. The DPDP solution is related on a new variant of authenticated dictionaries. The security for the constructions is provided using the standard assumptions. The DPDP scheme is very much useful in distributed applications [9]. The classic Merkle Hash Tree (MHT) construction for the block tag authentication. This scheme provides wide range of security and the performance analysis. The bilinear map is a map e it is commutable, bilinear and non degenerate. The MHT is a authentication structure that is used to prove that the set of elements are unimpaired and unchanged. The author have used BLS signature as a support. The direct addition of PDP or POR schemes to pillar data dynamics have security problems. The experiments display that the scheme is capable in aiding data dynamics with provable verification. The Merkle Hash Tree is been illustrated in the fig 2. Leaves are hashes of the data blocks. Nodes are hashes of their children [10].

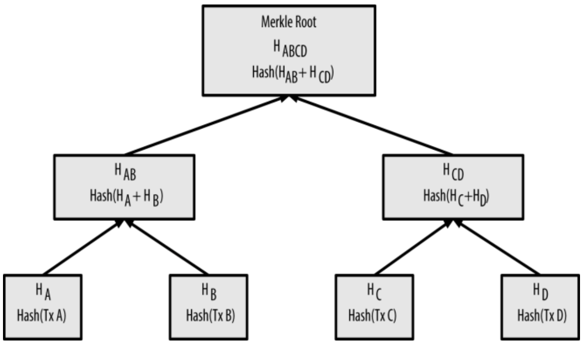

Figure: 2. Merkle Hash Trees

The Remote Data Checking (RDC) is a way of approach to the users and provide that data to be utilized at intrusted servers have complete rest over some time. RDC is used as an avoidance tool. It grants clients to regularly audit if data has been impaired and as a overhaul of tool damage can be recognize. The author have used a approach to compute repetition established on network coding, which attempt suspicious deal, because of its remarkable slow interaction roof to repair corrupt servers. Network coding is used to minimize the combine cost of both prevention and repair phase. The author proposed a new concept called RDC a novel secure and efficient RDC for network coding based distributed storage systems. RDC-NC is used to reduce new attacks. This implementation is low-cost for both clients and servers [11]. The dynamic audit service for validating the integrity in untrusted and outsourced storage. The audit service is positioned on the techniques, fragment structure, random sampling and index hash table for the abnormal detection. This paper directs only the issues of integrity checking and auditing. For supporting the dynamic data operations the author have recommended a simple index-hash table(IHT) that is used to report the changes of file blocks. The author has conferred two algorithms for the tag generation process. KeyGen, TagGen are the two algorithms. This scheme reduces the

DOI 10.17148/IARJSET.2015.2206

computation costs for the third party auditors and storage service providers [12]. They established a certificate less public auditing mechanisms for confirming the data integrity in the cloud. In this system model it contains a key generation center. The KGC is a trusted party required in the framework of certificate less schemes. It develops a partial private key of an entity to provide data security every block is appended with a signature. The certificateless signatures do not have the key escrow problem, which is an disadvantage in Identity Based Signatures (IBS). This scheme is block less verifiable and non adaptable. By using the certificateless signature scheme the author have built the entire certificates public auditing mechanism for the cloud users. By using this mechanism the public verifies not only audit data integrity but also capable of excluding the security risks established PKI. Experimental results have shown that the (HA-CLS) mechanism is efficient [14]. The proposed a privacy preserving technique by which the end user can remotely store their data and using undamaged perfection applications and services from a shared pool of configurable computing resource without the task of local data storage and maintenance. If the end user can use local cloud storage to make analytical importance then end user can hangout to TPA to control the incorruption of utilize data and to be worry free. In this paper author has extend their result to implement TPA to perform audits for several end users concurrently. By using this technique the performance and security both are very efficient [15]

CONCLUSION

Several methods for privacy preserving is discussed in this paper. This paper deals with certificate less public auditing mechanisms for confirming the data integrity in the cloud. Remote Data Checking (RDC) an avoidance Tool is discussed in detail. Public key cryptosystem the MD5 Message-Digest Algorithm are discussed. LT codes based cloud storage service (LTCS) are studied in detail. Certificateless public auditing mechanisms are depicted in this paper.

REFERENCES

[1] B. Wang, B. Li, and H. Li, “Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud,”Proc. IEEE Fifth Int’l Conf. Cloud Computing, pp. 295-302, 2012.

[2] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A.Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, “A View of Cloud Computing,”Comm. ACM,vol. 53, no. 4, pp. 50-58, Apr. 2010.

[3] D. Song, E. Shi, I. Fischer, and U. Shankar, “Cloud Data Protection for the Masses,”Computer, vol. 45, no. 1, pp. 39-45, 2012.

[4] C. Wang, Q. Wang, K. Ren, and W. Lou, “Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing,”Proc. IEEE INFOCOM, pp. 525-533, 2010.

[5] B. Wang, M. Li, S.S. Chow, and H. Li, “Computing EncryptedCloud Data Efficiently under Multiple Keys,”Proc. IEEE Conf. Comm. and Network Security (CNS ’13), pp. 90-99, 2013.

[6] R. Rivest, A. Shamir, and L. Adleman, “A Method for Obtaining Digital Signatures and Public Key Cryptosystems,”Comm. ACM,vol. 21, no. 2, pp. 120-126, 1978.

[7] The MD5 Message-Digest Algorithm (RFC1321). https://tools.ietf.org/html/rfc1321, 2014.

[8] H. Shacham and B. Waters, “Compact Proofs of Retrievability,”Proc. 14th Int’l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (ASIACRYPT ’08), pp. 90-107, 2008.

[9] C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia,“Dynamic Provable Data Possession,”Proc. 16th ACM Conf. Com-puter and Comm. Security (CCS’09), pp. 213-222, 2009.

[10] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, “Enabling Public Verifiability and Data Dynamic for Storage Security in Cloud Computing,”Proc. 14th European Conf. Research in Computer Secu-rity (ESORICS’09), pp. 355-370, 2009.

[11] B. Chen, R. Curtmola, G. Ateniese, and R. Burns, “Remote Data Checking for Network Coding-Based Distributed Storage Sys-tems,”Proc. ACM Workshop Cloud Computing Security Workshop(CCSW’10), pp. 31-42, 2010.

[12] Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S.S Yau,“Dynamic Audit Services for Integrity Verification of Outsourced Storages in Clouds,”Proc. ACM Symp. Applied Computing(SAC’11), pp. 1550-1557, 2011.

[13] N. Cao, S. Yu, Z. Yang, W. Lou, and Y.T. Hou, “LT Codes-Based Secure and Reliable Cloud Storage Service,”Proc. IEEE INFO-COM, 2012.

[14] B. Wang, B. Li, and H. Li, “Certificateless Public Auditing for Data Integrity in the Cloud,”Proc. IEEE Conf. Comm. and Network Security (CNS’13), pp. 276-284, 2013.

[15] C. Wang, S.S. Chow, Q. Wang, K. Ren, and W. Lou, “Privacy-Pre-serving Public Auditing for Secure Cloud Storage,”IEEE Trans.Computers, vol. 62, no. 2, pp. 362-375, Feb. 2013.

DOI 10.17148/IARJSET.2015.2206