International Journal of Research in Advent Technology, Special Issue, March 2019
E-ISSN: 2321-9637
International Conference on Technological Emerging Challenges (ICTEC-2019)
Available online at www.ijrat.org

New Systematic Remote Data Assume Audit Scheme in Cloud Storage

[1]Ch. Bindu Sri, [2]M. Mytri Madhurya
[1] *M.Tech, Assistant Professor,* [2] *M.Tech, Assistant Professor,*
[1] *email: chbindusri123@gmail.com,* [2] *email: mytrimadhurya7@gmail.com*
N.V.R.College of Engineering & Technology

Abstract: A growing number of data owners choose to outsource data files to the cloud. Cloud service provider tries to provide a promising service for data storage, which saves the users costs of investment and resource. Today, technical research works focus on Remote data possession Checking protocols permit to check that a remote server can access an uncorrupted file with the help of third party verifiers. The model makes client independent from initiating verification request and keeping the track of previous records which reduces client's time. To verify the correctness of data in cloud storage, this paper proposes an efficient ECC based Provable Data Possession (EPDP) Protocol with data dynamics. The proposed protocol preserves confidentiality of data stored in cloud storage and allows data owner to verify the integrity of data without retrieving the whole original data. Large number of clients like to store data onto public cloud server (PCS) due to increase in advancement in cloud computing. 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 effective TPA eliminates the involvement of the client through the auditing of whether his data stored in the cloud is indeed intact. The proposed scheme is highly efficient and resilient against the malicious data modification attack, server clouding attacks and failures.

Index Terms: cloud data storage, data integrity, cryptography, proxy based public key cryptography, Third Party Auditor

1. INTRODUCTION

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction [1]. The cloud provides server-based applications and all data services to the user, with output displayed on the client device [3]. Memory allocated to the client system's web browser is used to make the application data appear on the client system display, but all computations and changes are recorded by the server and final results including files created or altered are permanently stored on the cloud servers [4]. The central trouble of remote data security is ensuring integrity of remotely located data which is out of client reach [5]. Even though the benefits of cloud are significant and tremendous one unique aspect that impedes the adoption of cloud by many individuals and enterprises is concern over data security [6]. Ensuring confidentiality and integrity of the outsourced data is very important since data are stored on shared servers at remote site [7]. We provide remote Data Integrity Check using Proxy Server with Partial Data method is used to address the problem. Our algorithm is efficient and very flexible. Based upon the real client's authorization, our protocol can realize private data integrity check using partial data [8]. To fully ensure the data integrity and save the cloud users' computation resources as well as online burden it is of critical importance to enable public auditing service for cloud data storage users may resort to an independent third party auditor (TPA) to audit the outsourced data when needed [9].

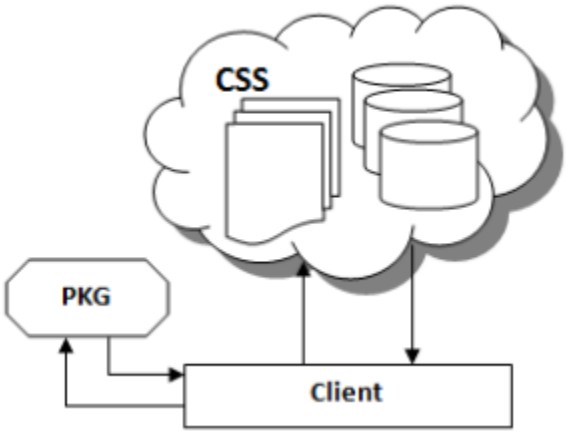

Figure 1: System Model

2. RELATED WORK

The propose allowing a TPA to keep online storage honest by first encrypting the data then sending a number of pre computed symmetric keyed hashes over the encrypted data to the auditor[10]. The auditor verifies both the integrity of the data file and the server possession of a previously committed decryption key [11]. The malicious cloud server may damage the client's data in order to gain more benefits and to maintain their reputation. Many researchers proposed the equivalent system model and security model to work on security issue. Latest work was proposed [12]. Proposed attestable data possession (ADP) paradigm[11]. In ADP model, the checking can verify the remote data integrity without retrieval or download of the complete data. ADP is a probabilistic evidence on remote data integrity check by inputting random set of blocks from the public clouds servers, which significantly reduces I/O costs [13]. One of the biggest concerns with cloud data storage is that of data integrity verification at un-trusted servers. For example, the storage service provider, which experiences Byzantine failures occasionally, may decide to hide the data errors from the clients for the benefit of their own [14]. They extend the PDP model to support provable updates to stored data files using rank-based authenticated skip lists. This scheme is essentially a fully dynamic version of the PDP solution [15]. To support updates, especially for block insertion, they eliminate the index information in the computation in Attendee's PDP model and employ authenticated skip list data.

3. SYSTEM STRUCTURAL MODELING

The cloud environment and the multilevel security system required to protect the data stored in cloud server's responsibilities of a data owner in securing data discussed exhaustively [16]. There are many clients but only one server web layer directly has business logic layer in it and it interacts with database, then it can handle only one client at a time. Hence we use separate business logic layer which interacts with database layer [17]. The cloud is large amount of data files to be stored in the cloud the cloud server (CS), which is managed by cloud service provider (CSP) to provide data storage service the third party auditor (TPA), who has expertise and capabilities that cloud users do not have and is trusted to assess the cloud storage service security on behalf of the user upon request [18]. The proposers proposed a on spot verification approach to undertaking ownership of data records and engaged error correcting coding technology to ensure constraint on their scheme is that the number of challenge is utilized the homomorphism signature to design an improved scheme [19].

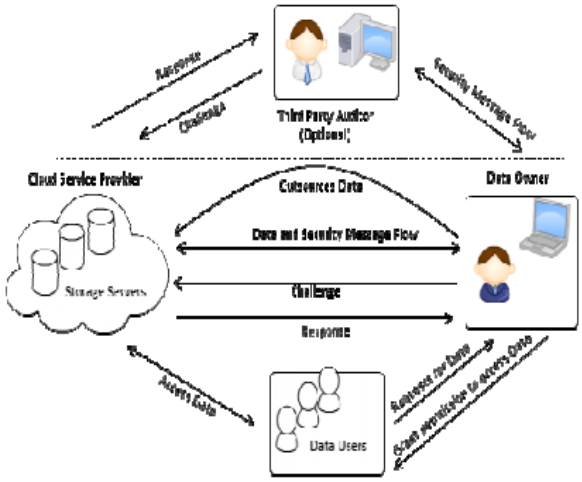

Fig. 2. Cloud Data Storage overview

4. PROPOSED SYSTEM PROTOCOL

To ensure the correctness of storage, an efficient Provable Data Possession protocol using Elliptic Curve Cryptography is proposed our model is effective and efficient in providing authentication, authorization during the access of the data and also ensures the integrity of the data stored on the public cloud [20]. Our method called remote data integrity check using partial data provides security for the client's data during data uploading and provides security for the data stored in remote place by integrity checking of the data stored in remote place with the partial data [21]. Cloud Storage Server (CSS): an entity, which is managed by Cloud Service Provider (CSP), has significant storage space and computation resource to maintain the clients' data Privacy-preserving to ensure that the TPA cannot derive users data content from the information collected during the auditing process.

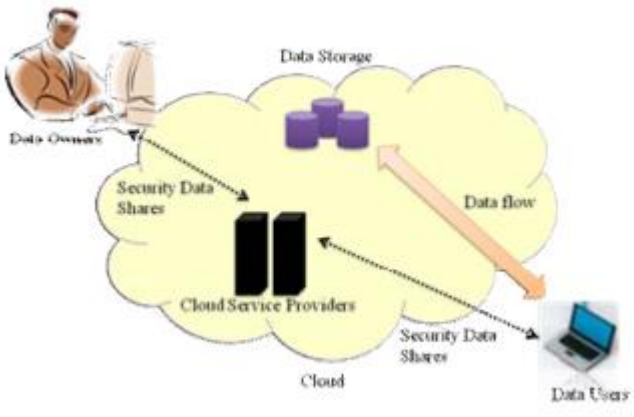

Fig.3 Proposed System

5. ALGORITHM

The Advanced Encryption Standard, or AES, is a symmetric block cipher to protect classified information and the world to encrypt sensitive data. Security Competing algorithms were to be judged on their ability to resist attack, as compared to other submitted ciphers, though security strength was to be considered the most important factor in the competition [22]. AES comprises three block ciphers: AES128, AES-192 and AES-256. Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128, 192 and 256 bits, respectively [23].

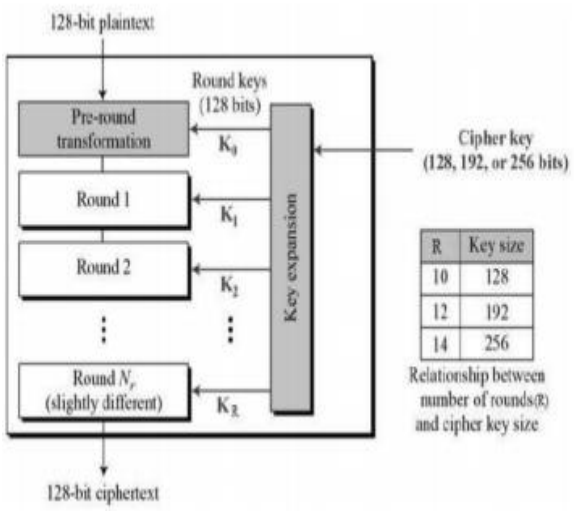

Fig 4: Schematic Representation of AES Structure

The process of decryption of an AES cipher text is similar to the encryption process in the reverse order. Each round consists of the four processes conducted in the reverse order.

- Add round key
- Mix columns
- Shift rows
- Byte substitution

The sub-processes in each round are in reverse manner, unlike for a Feistel Cipher, the encryption and decryption algorithms need to be separately implemented, although they are very closely related.

Key Generation Phase

The key generation algorithm, Gen Key is executed by data owner to generate secret and public key pair. A secret and public key pair (sk, pk) as output. Data owner selects a random integer k from [1,n-1],and P=kG is computed, where k is the secret key and P is the public key [24]..

Algorithm : GenKey

1. Procedure: GenKey(1k)→(sk,pk)
2. Select a random integer k ϵ [1,n-1]
3. Compute P=kG
4. sk← k, pk←P
5. End Procedure

Third Party Auditor

In the cloud paradigm, by putting the large data files on the remote servers, the clients can be relieved of the burden of storage and computation. As clients no longer possess their data locally it is of critical importance for the clients to ensure that their data are being correctly stored and maintained [25]

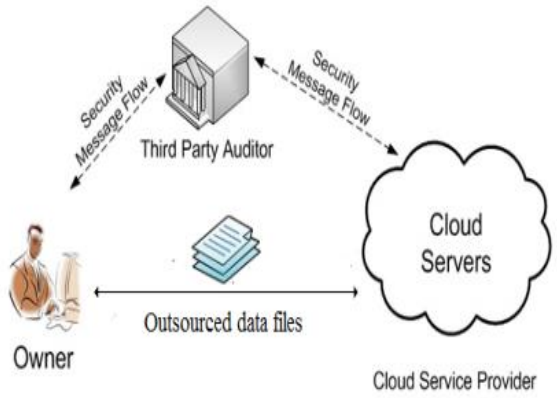

Figure.5 Third Party Auditor Architecture

A. Integrity Verification

The verifier before storing the file at the archive, preprocesses the file and appends some Meta data to the file and stores at the archive. At the time of verification the verifier uses this Meta data to verify the integrity of the data. TPA will does the equality check between the SigGen() and SigAvil() Ack will be sent to the Client depend upon the equality checking [26].

Dynamic Data Operation with Integrity Security

Now we show how our scheme can explicitly and efficiently handle fully dynamic data operations like Data Modification including data insertion and data deletion (D) for cloud data storage. We assume that the file F and the signature Sig() have already been generated and properly stored at server [27]. In case those clients do not necessarily have the time, feasibility or resources to monitor their data, they can delegate the monitoring task to a trusted TPA.

6. PERFORMANCE ANALYSIS

The proposed protocol is proved to be correct and is also sound correctness the outsourced data is stored honestly in cloud storage server, then whenever the server receives a challenge from verifier could

compute proof for the challenge that will always be accepted by the verifier. The schemes proposed is based on bilinear pairing which involves computation cost for multiplication operation, exponentiation operations and bilinear pairs. Since the proposed EPDP protocol is built without pairing, the computation cost. The computation cost for each algorithm and the proposed new protocol. From the analysis, it is determined that the computation cost is minimized and thereby the comparison result proves the efficiency of the proposed protocol.

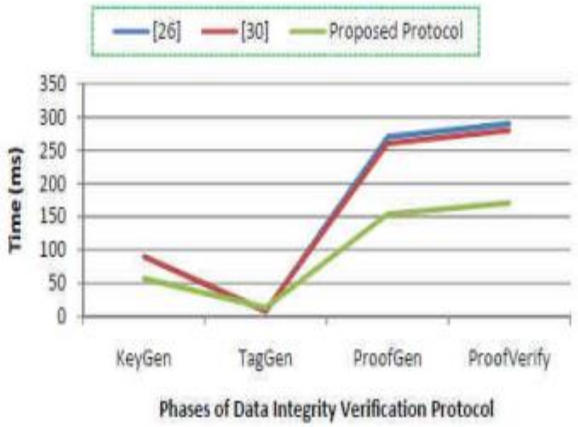

Fig. 6. Comparison between the proposed protocol

7. CONCLUSION AND FUTURE WORK

Our system supports data dynamics i.e., using our new data structure, the data owner can perform insert, modify or delete operation on file blocks with high efficiency. The focus is on stopping data being disclosed by un-trusted service providers when data owners distribute their database entries along with error recovery. To achieve the assurances of cloud data integrity and availability and enforce the quality of dependable cloud storage service for users. The approach focuses on file break flexibility and automation in random challenge generation. To ensure confidentiality and integrity of data outsourced to cloud storage, in this paper, an efficient provable data possession protocol using elliptic curve cryptography is proposed. In our discussion, we went up with too many phases like setup, tag generation etc. It becomes too congested from the point of view of the architecture. The same can be solved using automatic key generation algorithms or virtual key generation systems. Service level agreement (SLA). It is important to note that our proof of data integrity protocol just checks the integrity of data i.e. if the data has been illegally modified or deleted.

REFERENCES

[1] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic,"Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility," Future Gener. Comp. Sy., vol. 25, no. 6, pp. 599 – 616, 2009.

[2] Q.Wang, C.Wang, K.Ren, W.Lou and J.Li "Enabling public auditability and data dynamics for storage security in cloud computing",IEEE Trans. Parrael Disrib. Syst, vol.22, pp. 847-859, 2011.

[3] Y.Deswarte, J.J.Quisquater and A.Saidane, "Remote integrity checking", Proc. 6th Work. Conf. Integr. Int. Control Inf. Syst. (IICIS), vol. 16, pp. 1-11, 2003.

[4] G.Ateniese, R.Di.Pietro, L.V.Mancin and G,Tsudik "Scalable and efficient provable data possession," Proc. 4th Int. Conf. Secur. Privacy Commun. Netw. (SecureComm), vol. 9, 2008.

[5] L.Chen, S.Zhou, X.Huang and L.Xu "Data dynamics for remote data possession checking in cloud storage," Comput. Electr. Eng, vol. 39, pp. 2413-2424, 2013

[6] F. Seb´e, J. Domingo-Ferrer, A. Mart´ınez-Ballest´e, Y. Deswarte, J. Quisquater, "Efficient Remote Data Integrity checking in Critical Information Infrastructures", IEEE Transactions on Knowledge and Data Engineering, 20(8), pp. 1-6, 2008.

[7] H.Q. Wang, "Proxy Provable Data Possession in Public Clouds," IEEE Transactions on Services Computing, 2012.

[8] Y. Zhu, H. Hu, G.J. Ahn, M. Yu, "Cooperative Provable Data Possession for Integrity Verification in Multicloud Storage", IEEE Transactions on Parallel and Distributed Systems, 23(12), pp. 2231-2244, 2012.

[9] Y. Zhu, H. Wang, Z. Hu, G. J. Ahn, H. Hu, S. S. Yau, "Efficient Provable Data Possession for Hybrid Clouds", CCS'10, pp. 756-758, 2010.

[10] R. Curtmola, O. Khan, R. Burns, G. Ateniese, "MR-PDP: Multiple Replica Provable Data Possession", ICDCS'08, pp. 411-420, 2008.

[11] A. F. Barsoum, M. A. Hasan, "Provable Possession and Replication of Data over Cloud Servers", CACR, University of Waterloo, Report2010/32, 2010.

[12] Z. Hao, N. Yu, "A Multiple-Replica Remote Data Possession Checking Protocol with Public Verifiability", 2010 Second International Symposium on Data, Privacy, and E-Commerce, pp. 84-89, 2010.

[13] A. F. Barsoum, M. A. Hasan, "On Verifying Dynamic Multiple Data Copies over Cloud Servers", IACR eprint report 447, 2011. Available at http://eprint.iacr.org/ 2011/447.pdf.

[14] A. Juels, B. S. Kaliski Jr., "PORs: Proofs of Retrievability for Large Files", CCS'07, pp. 584-597, 2007.
[15] B.-C. Chen and H.-T. Yeh, ―Secure proxy signature schemes from the weil pairing,‖ J. Supercomput., vol. 65, no. 2, pp. 496–506, 2013.
[16] K. Huang, J. Liu, M. Xian, H. Wang, and S. Fu, ―Enabling dynamic proof of retrievability in regeneratingcoding-based cloud storage,‖ in Proc. IEEE ICC, Jun. 2014, pp. 712–717.
[17] C. Wang, Q. Wang, K. Ren, and W. Lou, ―Privacy-preserving public auditing for data storage security in cloud computing,‖ in Proc. IEEE INFOCOM, Mar. 2010, pp. 1–9.
[18] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, ―Enabling public auditability and data dynamics for storage security in cloud computing,‖ IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 5, pp. 847–859, May 2011.
[19] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, ―Toward secure and dependable storage services in cloud computing,‖ IEEE Trans. Services Comput., vol. 5, no. 2, pp. 220–232, Apr./Jun. 2012.
[20] Y. Zhu, G.-J. Ahn, H. Hu, S. S. Yau, H. G. An, and C.-J. Hu, ―Dynamic audit services for outsourced storages in clouds,‖ IEEE Trans. Services Comput., vol. 6, no. 2, pp. 227–238, Apr./Jun. 2013.
[21] J. Kincaid, "MediaMax/TheLinkup Closes Its Doors,"at http://www.techcrunch.com/2008/07/10/ mediamaxthelinkup-closes-its-doors/, July 2008.

[22] M. Naor and G. N. Rothblum, "The complexity of online memory checking," in Proc. of FOCS'05, Pittsburgh, PA, USA, 2005, pp. 573–584.
[23] E.-C. Chang and J. Xu, "Remote integrity check with dishonest storage server," in Proc. of ESORICS'08. Berlin, Heidelberg: Springer-Verlag, 2008, pp. 223–237.
[24] M. A. Shah, R. Swaminathan, and M. Baker, "Privacy-preserving audit and extraction of digital contents," Cryptology ePrint Archive, Report 2008/186, 2008.
[25] A. Oprea, M. K. Reiter, and K. Yang, "Space-efficient block storage integrity," in Proc. of NDSS'05, San Diego, CA, USA, 2005.
[26] T. Schwarz and E. L. Miller, "Store, forget, and check: Using algebraic signatures to check remotely administered storage," in Proc. of ICDCS'06, Lisboa, Portugal, 2006, pp. 12–12.
[27] Q. Wang, K. Ren, W. Lou, and Y. Zhang, "Dependable and secure sensor data storage with dynamic integrity assurance," in Proc. Of IEEE INFOCOM'09, Rio de Janeiro, Brazil, Appril 2009, pp. 954–962.