A Blockchain based Access Control System for Cloud Storage

V. Subedha[1], S. Harish[2], V. G. Abishekraj[3]
[1]*Professor & HoD, Department of CSE, Panimalar Institute of Technology, Chennai, India*
[2,3]*Student, Department of CSE, Panimalar Institute of Technology, Chennai, India*

***Abstract*: Multi-user system for access control to datasets stored in an untrusted cloud environment. Cloud storage like any other untrusted environment needs the ability to secure share information. Our approach provides an access control over the data stored in the cloud without the provider participation. The main tool of access control mechanism is cipher text-policy attribute-based encryption scheme with dynamic attributes. Using a block chain based decentralized ledger, our system provides immutable log of all meaningful security events, such as key generation, access policy assignment, change or revocation, access request. We propose a set of cryptographic protocols ensuring privacy of cryptographic operations requiring secret or private keys. Only cipher texts of hash codes are transferred through the block chain ledger. The prototype of our system is implemented using smart contracts and tested on Ethereum block chain platform.**

***Keywords*: blockchain, cloud storage**

1. Introduction

Cloud computing encourages users to outsource their data to cloud storage. Data outsourcing means that users lose physical autonomy on their own data, which makes remote data integrity verification become a critical challenge for potential cloud users. To free user from the burden incurred by frequent integrity verifications, Third Party Auditor (TPA) is introduced to perform verifications on behalf of user for data integrity assurance. However, existing public auditing schemes rely on the assumption that TPA is trusted, thus these schemes cannot be directly extended to support the outsourced auditing model, where TPA might be dishonest and any two of the three involved entities (i.e. user, TPA, and cloud service provider) might be in collusion. In this paper, we propose a dynamic outsourced auditing scheme which cannot only protect against any dishonest entity and collision, but also support verifiable dynamic updates to outsourced data. We present a new approach, based on batch-leaves-authenticated Merkle Hash Tree (MHT), to batch-verify multiple leaf nodes and their own indexes all together, which is more appropriate for the dynamic outsourced auditing system than traditional MHT-based dynamism approaches that can only verify many leaf nodes one by one. Experimental results show that our solution minimizes the costs of initialization for both user and TPA (compared to existing static outsourced auditing scheme), and incurs a lower price of dynamism at user side.

2. Literature Survey

Revisiting Attribute-Based Encryption with Verifiable Outsourced Decryption.

Author: Suqing Lin, Rui Zhang, Hui Ma, and Mingsheng Wang, Year: 2015.

Description: Attribute-based encryption (ABE) is a promising technique for fine-grained access control of encrypted data in a cloud storage, however, decryption involved in the ABEs is usually too expensive for resource-constrained front-end users, which greatly hinders its practical popularity. In order to reduce the decryption overhead for a user to recover the plaintext, Green et al. suggested to outsource the majority of the decryption work without revealing actually data or private keys. To ensure the third-party service honestly computes the outsourced work, Lai et al. provided a requirement of verifiability to the decryption of ABE, but their scheme doubled the size of the underlying ABE ciphertext and the computation costs. Roughly speaking, their main idea is to use a parallel encryption technique, while one of the encryption components is used for the verification purpose. Hence, the bandwidth and the computation cost are doubled. In this paper, we investigate the same problem. In particular, we propose a more efficient and generic construction of ABE with verifiable outsourced decryption based on an attribute based key encapsulation mechanism, a symmetric-key encryption scheme and a commitment scheme. Then, we prove the security and the verification soundness of our constructed ABE scheme in the standard model. Finally, we instantiate our scheme with concrete building blocks. Compared with Lai et al.'s scheme, our scheme reduces the bandwidth and the computation costs almost by half.

An Algorithmic Approach to Improving Cloud Security: The MIST and Malachi Algorithms.

Author: Cara Tunstall, Kuo-pao Yang, Justin LeJeune, Year: 2016.

Description: Cloud Computing is ever increasing in popularity in the computer science field. Because of this increased usage, the importance of data integrity and strong security has become paramount. This paper expounds upon security measures and methodologies for strengthening the cloud, including two new security algorithms. According to the Cloud Security Alliance paper, “The Notorious Nine: Cloud Computing Top Threats 2013”, the nine biggest threats to cloud computing are data breaches, data loss, account or service traffic hijacking, insecure interfaces and Application Programming Interfaces (APIs), denial of service, malicious insiders, abuse of cloud services, insufficient due diligence, and finally shared technology vulnerabilities [1]. All nine of these issues would be lessened by properly implementing stricter security on cloud systems. A combination of security measures in concurrence is the basis of the security improvements asserted forthwith. The security algorithms introduced in this paper, the MIST and Malachi are two new ways to protect users’ data through account security.

Data Security in Cloud computing and Outsourced Databases.

Author: ShankarNayak Bhukya ,Dr.Suresh Pabboju , Dr. K Venkatesh Sharma, year: 2016.

Description: We introduce a model for provable data possession (PDP) that allows a client that has stored data at an untrusted server to verify that the server possesses the original data without retrieving it. The model generates probabilistic proofs of possession by sampling random sets of blocks from the server, which drastically reduces I/O costs. The client maintains a constant amount of metadata to verify the proof. The challenge/response protocol transmits a small, constant amount of data, which minimizes network communication. Thus, the PDP model for remote data checking supports large data sets in widely distributed storage systems. It is also superior in performance by minimizing the use of expensive publickey cryptography in metadata management. We present the architecture and implementation of various SHAROES components and our experiments demonstrate performance superior to other proposals by over 40% on a number of benchmarks.

New Proofs of Retrievability using Locally Decodable Codes

Author: Julien Lavauzelle, Franc¸oise Levy-dit-Vehel, year: 2016.

Description: Proofs of retrievability (PoR) are probabilistic protocols which ensure that a client can recover a file he previously stored on a server. Good PoRs aim at reaching an efficient tradeoff between communication complexity and storage overhead, and should be usable an unlimited number of times. We present a new unbounded-use PoR construction based on a class of locally decodable codes, namely the lifted codes of Guo et. al. Our protocols feature sublinear communication complexity and very low storage overhead. Moreover, the various parameters can be tuned so as to minimize the communication complexity (resp. the storage overhead) according to the setting of concern.

Compact Dualmode Microwave Electroporation and Dielectrometry Tool.

Author: Henry D. Herce, S¨onke Schmidt, Martin Sch¨ußler, Zhen Luo and Rolf Jakoby, YEAR: 2017.

Description: In this paper, a novel tool is introduced for microwave assisted electroporation at 18 GHz, suitable for the integration in a lab-on-a-chip. In contrast to conventional electroporation, microwave electroporation has the advantage of lower field strengths, and can therefore, provide higher cell viability rates. Moreover, with this applicator it is possible to monitor the membrane poration process in situ optically, and by obtaining broadband dielectric spectroscopy at the same time. The concept of microwave assisted electroporation is proofed with SF9 insect cells. After an exposure of 25 minutes with an input power of 24dBm at 18 GHz, successful uptake was detected due to microwave membrane poration.

Public Auditing for Secure Data Storage in Cloud through a Third Party Auditor Using Modern Ciphertext

Author: Henry D. Herce, S¨onke Schmidt, Martin Sch¨ußler, Zhen Luo and Rolf Jakoby, year: 2017.

Description: Outsourced data in cloud and computation results are not always trustworthy because data owners lack physical possession and control over the data as a result of virtualization, replication, and migration techniques. Protecting outsourced data from security threats has become a challenging and potentially formidable task in cloud computing; hence, many schemes have focused on ameliorating this problem and on enabling public auditability for cloud data storage security. These schemes drop into two categories: total computation cost and burden on client side. Researchers have used bilinear map technology with public key cryptography. Although this technology is highly efficient, computation time is long and overhead cost is high. The client needs to perform numerous computations to ensure the integrity of data storage. To reduce auditing cost, we propose an efficient and robust scheme to maintain data integrity in cases that involve public auditing. Our scheme adopts modern cipher cryptography with a cryptographic hash function. We consider allowing a third party auditor to preprocess data on behalf of cloud users before uploading them to cloud service providers and then verifying data integrity afterward. Our proposed scheme has important security characteristics, such as privacy, key management, low cost computation, key exchange, low overhead cost, no burden on client side, inability of cloud service providers to create correct verifier respond without data, and one-time key. Finally, efficiency analysis shows that our scheme is faster and more cost-efficient than the bilinear map-based scheme.

An Efficient Provable Data Possession Scheme with Data Dynamics

Author: Chaoling Li, Yue Chen, Pengxu Tan, Gang Yang, Year: 2017.

Description: Ateniese et al proposed an efficient Provable Data Possession scheme which uses only hash and symmetric-key cryptographic functions, but it cannot support block insertion. To achieve full data dynamics, a SN-BN table which maps the logical indices of blocks to their physical ones is introduced. The SN (Serial Number) is used to determine which blocks are included in tags, while the corresponding BN (Block

Number) is used to retrieve the actual data blocks. Therefore, the remaining tags need not to be recomputed with new blocks while a block is inserted. Therefore, it can support full data dynamics including block modification, deletion, insertion and appending. Because of its high efficiency and full dynamics, our scheme is very suitable for applications in which some resource-constrained clients are used to check the data possession and the data needs to be updated after being outsourced.

Strong Key-Exposure Resilient Auditing for Secure Cloud Storage

Author: Jia Yu, and Huaqun Wang, year: 2017.

Description: Key exposure is one serious security problem for cloud storage auditing. In order to deal with this problem, cloud storage auditing scheme with key-exposure resilience has been proposed. However, in such a scheme, the malicious cloud might still forge valid authenticators later than the key-exposure time period if it obtains the current secret key of data owner. In this paper, we innovatively propose a paradigm named strong key exposure resilient auditing for secure cloud storage, in which the security of cloud storage auditing not only earlier than but also later than the key exposure can be preserved. We formalize the definition and the security model of this new kind of cloud storage auditing and design a concrete scheme. In our proposed scheme, the key exposure in one-time period doesn't affect the security of cloud storage auditing in other time periods. The rigorous security proof and the experimental results demonstrate that our proposed scheme achieves desirable security and efficiency.

3. Existing System

In existing framework, the cost of initialization in existing outsourced auditing scheme Fortress is high, during the Store Protocol (i.e., the data pre-processing step), the whole of user's outsourced data must be downloaded by TPA from cloud. Given that TPA will concurrently provide auditing proxy services for many different cloud users, and the total size of outsourced data of all users will be considerable in cloud. In this case, it must be a very heavy communication cost for TPA, by downloading all outsourced data from CSP, to accomplish above initialization for every user. In practice, to make an outsourced auditing scheme more easily accepted from the perspective of a real TPA, the design of forcing TPA to fetch the whole outsourced data from CSP is a limitation that should be avoided.

Disadvantages:

The Major disadvantages of the existing system are waste of space and the need to buy large volumes of data.

4. Proposed System

Cloud computing has become more and more popular, receiving increasing attentions in academic field and IT industry. All kinds of advantages of cloud computing are attractive, such as ubiquitous access of network service, pay as you go billing model, on-demand configurations of software and hardware resources, cost saving of IT infrastructure investment. Despite these benefits, many potential cloud users have yet to join the cloud, and many are for the most part putting only their less sensitive data in the cloud [1]. Actually, the concerns of cloud users seem to make sense. Cloud Security Alliance (CSA) regards Data Loss as the top of the list among the notorious nine cloud computing top threats [2], showing the importance and significance for user to discover data corruption in cloud as early as possible and then immediately take actions to avoid the irretrievable losses.

The proposed concept of block chain based access control system for cloud storage deals with the drawbacks of the private auditing i.e., Third Party Auditor. Third Party Auditor could change the corrupted file in the cloud data by generating two types of database in server. As one database data is corrupted, the third party auditor can change the corrupted data by changing original data in second database.

Advantages:

The major advantage of the proposed concept of block chain based access control system for cloud storage is that it allows for data storage even in the absence of data owner. Another advantage of this proposed concept is that the regeneration problem of authenticators is resolved.

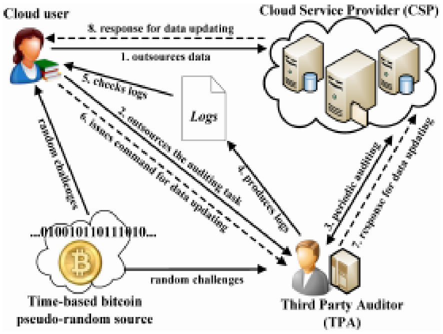

Fig. 1. Architecture

5. Module description

1. User interface design
2. File owner uploading
3. File requesting
4. Third party auditor response
5. File retrieval

1) *User interface design*

To connect with server user must give their username and password then only they can able to connect the server. If the user already exits directly can login into the server else user must register their details such as username, password & Email-id, in the server. Server will create the account for the entire user to maintain upload and download rate. Name will be set as user id. Logging in is usually used to enter a specific page.

2) *File Owner Uploading*

This is the module for uploading owner's files or documents into the virtual machines. These constraints serve a dual purpose as they can introduce high-level policies and assist in administration tasks. The user sends the file to cloud send the Data so upload the file or Data. Given that we rely on network services for our most security-critical data. A source wants to securely send a message to a set of receivers over a cloud network with unit-capacity edges, in the presence of a cloud user.

3) File Requesting

The file is only view format so the file is share and download purpose in Request send to the data owner, the data owner is check the request and user was authorized person so data owner response and key provide to the user.

4) Third Party Auditor Response

The malicious cloud might still forge valid authenticators later than the key-exposure time period if it obtains the current secret key of data owner. In this paper, we innovatively propose a paradigm named strong key exposure resilient auditing for secure cloud storage, in which the security of cloud storage auditing not only earlier than but also later than the key exposure can be preserved.

5) File Retrieval

TPA can audit the integrity of the challenged blocks without retrieving these actual blocks from the cloud. But the homomorphic tags can only be computed by user herself to against malicious CSP/TPA. Fortress builds upon the scheme of where the homomorphic tag of data block is constructed by using the corresponding block index.

6. Conclusion

In the context of cloud storage and remote data auditing, how to defend against a dishonest TPA is an important issue raised by recent research. Compared to traditional public auditing schemes, outsourced auditing scheme under a stronger security model aims to protect against any dishonest entity and collusion. In this paper, we propose a new authenticated data structure that is based on Merkle Hash Tree and referred to as BLA-MHT. By supporting the batch-verifications upon multiple leaf nodes, this novel data structure is more efficient than existing MHT-based approaches, and thus is appropriate for the dynamic outsourced auditing system. Based on BLA-MHT, we also propose a new scheme to achieve both dynamic updates and outsourced auditing. Compared to the state of the art, the experiments validate the effectiveness of our scheme.

7. Future Enhancements

Future concept is more advanced than the proposed concept as the data owner and third party auditor need not be change the data at each time the file has been corrupted. Future concept provide proxy based data auditing thus when the file in the cloud have been corrupted the proxy itself enhance protocol to change the corrupted file with original file present in the cloud. Similarly, it provides multiple keyword to check the file stored in cloud.

References

[1] R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka, and J. Molina, “Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control,” Proc. 2009 ACM Workshop on Cloud Computing Security (CCSW '09), pp. 85-90, 2009.

[2] Cloud Security Alliance (CSA), “The Notorious Nine Cloud Computing Top Threats in 2013,” https://cloudsecurityalliance. org/download/the-notorious-nine-cloud-computing-top -threats-in-2013, Feb. 2013.

[3] G. Ateniese, R.C. Burns, R. Curtmola, J. Herring, L. Kissner, Z.N.J Peterson, and D.X. Song, “Provable Data Possession at Untrusted Stores,” Proc. 14th ACM Conf. Computer and Comm. Security (CCS ’07), pp. 598-609, 2007.

[4] A. Juels and B.S. Kaliski Jr, “PORs: Proofs of Retrievability for Large Files,” Proc. 14th ACM Conf. Computer and Comm. Security (CCS ’07), pp. 584-597, 2007.

[5] 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.

[6] 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 and Distributed Systems, vol. 22, no. 5, pp. 847-859, May 2011.

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

[8] D. Cash, A. Küpçü, and D. Wichs, “Dynamic Proofs of Retrievability via Oblivious Ram,” Proc. 32nd Int’l Conf. Theory and Applications of Cryptographic Techniques: Advances in Cryptology (EUROCRYPT ’13), pp. 279-295, 2013.

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

[10] 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 Computing, vol. 6, no. 2, pp. 227-238, April-June 2013.