A Survey on Authorized Encrypted Search for Information Retrieval of Distributed System by Journal Purpose Application

Sagar Borude[1] Arvind Kedar[2] Rahul Yeloe[3] Prof. S. S. Khatal[4]
[1,2,3]Student [4]Assistant Professor
[1,2,3,4]Department of Computer Engineering
[1,2,3,4]Savitribai Phule Pune University, Pune, Maharashtra, India

Abstract— Data integrity maintenance is the major objective in cloud storage. It includes audition using TPA for unauthorized access. To implements this work for protecting the data and regeneration of data if someone mishandles it. This job will be assigned to a Proxy server. The data of the users will be stored in public and private area of the cloud. So that only public cloud data will be accessed by user and private cloud will remain more secured. Once any unauthorized modification is made, the original data in the private cloud will be retrieved by the Proxy server and will be returned to the user. Cloud storage generally provides different redundancy configuration to users in order to maintain the desired balance between performance and fault tolerance. Data availability is critical in distributed storage systems, especially when node failures are prevalent in real life. This research work explores secure data storage and sharing using proposed AES 128 encryption algorithm and Role Base Access Control (RBAC) for secure data access scheme for end user. This work also carried out backup server approach it works like proxy storage server for ad hoc data recovery for all distributed data servers. The experiment analysis has proposed in public as well as private cloud environment.

Keywords: RBAC, SHA256 encryption scheme; secure user access policy; Proxy Key Generation, Role Base Access Control (RBAC), advanced encryption standard (AES)

I. INTRODUCTION

The most straightforward method of addressing data privacy concerns is to encrypt data before uploading to the cloud. Subsequently, only the authorized client who has the key or permissions can decrypt the data. Accordingly, in an Organization system, data owners are usually required to encrypt their records. As a practical consideration, data owners also need to provide corresponding access policies to access their records and determine which keywords they can search. However, it is nontrivial to achieve the aforementioned requirements over encrypted data. A wireless network consists of spatially distributed autonomous sensors to monitor physical or logical conditions, and to cooperatively pass their data through the network to a main location. The development of wireless networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on. Special characteristics of WSNs, such as resource constraints on energy and computational power and security have been well-defined and widely studied. What has received less attention, however, is the critical privacy concern on information being collected, transmitted, and analyzed in a WSN. Such private and sensitive information may include payload data collected by network and transmitted through another network to a centralized data processing server.

System depict the principle plan objectives of the proposed plan including key circulation, information secrecy, access control and effectiveness as takes after: Key Distribution: The prerequisite of key transportation is that clients can safely get their private keys from the gathering director with no Certificate Authorities. In other existing plans, this purpose is skillful by expecting that the communication channel is secure, on the other hand, in our plan, system can accomplish it without this solid thought. Access control: First, collect individuals can make use of the cloud asset for information stockpiling and information sharing. Second, unapproved clients can't get to the cloud asset whenever, and disavowed clients will be unfitted for utilizing the cloud asset again once they are renounced [5].

II. LITERATURE SURVEY

Wei Li, KaipingXue, YingjieXue, and Jianan Hong, "TMACS: A Robust and Verifiable Threshold Multi-Authority Access Control System in Public Cloud Storage". In this paper, from another perspective, we conduct a threshold multi-authority CP-ABE access control scheme for public cloud storage, named TMACS, in which multiple authorities jointly manage a uniform attribute set. In TMACS, taking advantage of (t, n) threshold secret sharing, the master key can be shared among multiple authorities, and a legal user can generate his/her secret key by interacting with any t authorities. Security and performance analysis results show that TMACS is not only verifiable secure when less than t authorities are compromised, but also robust when no less than t authorities are alive in the system. Furthermore, by efficiently combining the traditional multi-authority scheme with TMACS, we construct a hybrid one, which satisfies the scenario of attributes coming from different authorities as well as achieving security and system-level robustness.

Jianan Hong, KaipingXue and Wei Li, 'Comments on "DAC-MACS: Effective Data Access Control for Multi-Authority Cloud Storage Systems"/Security Analysis of Attribute Revocation in Multi-Authority Data Access Control for Cloud Storage Systems'. In the above paper, Yang et al. have proposed a multi-authority ciphertext-policy attribute-based encryption-based data access control for cloud storage, in which the authors claimed that the mechanism in dealing with attribute revocation could achieve both forward security and backward security. Unfortunately, our further analysis and investigation show that their work adopts a bidirectional re-encryption method in ciphertext updating, so security vulnerability appears. Our proposed attack method demonstrates that a revoked user can still decrypt new cipher

texts that are claimed to require the new-version secret keys to decrypt.

Taeho Jung, Xiang-Yang Li, Zhiguo Wan, and Meng Wan, "Control Cloud Data Access Privilege and Anonymity with Fully Anonymous Attribute-Based Encryption". In this paper, we present a semi-anonymous privilege control scheme AnonyControl to address not only the data privacy, but also the user identity privacy in existing access control schemes. AnonyControl decentralizes the central authority to limit the identity leakage and thus achieves semi-anonymity. Besides, it also generalizes the file access control to the privilege control, by which privileges of all operations on the cloud data can be managed in a fine-grained manner. Subsequently, we present the AnonyControl-F, which fully prevents the identity leakage and achieve the full anonymity. Our security analysis shows that both AnonyControl and AnonyControl-F are secure under the decisional bilinear Diffie-Hellman assumption, and our performance evaluation exhibits the feasibility of our schemes.

Kan Yang and Xiao huaJia, "Expressive, Efficient, and Revocable Data Access Control for Multi-Authority Cloud Storage". In this paper, we design an expressive, efficient and revocable data access control scheme for multi-authority cloud storage systems, where there are multiple authorities co-exist and each authority is able to issue attributes independently. Specifically, we propose a revocable multi-authority CP-ABE scheme, and apply it as the underlying techniques to design the data access control scheme. Our attribute revocation method can efficiently achieve both forward security and backward security. The analysis and simulation results show that our proposed data access control scheme is secure in the random oracle model and is more efficient than previous works.

T. Jung, X. Li, Z. Wan, and M. Wan, "Privacy preserving cloud data access with multi-authorities".This paper presents an anonymous privilege control scheme AnonyControl to address not only the data privacy problem in cloud storage, but also the user identity privacy issues in existing access control schemes. By using multiple authorities in cloud computing system, our proposed scheme achieves anonymous cloud data access and fine-grained privilege control. Our security proof and performance analysis shows that AnonyControl is both secure and efficient for cloud computing environment.

III. PROPOSED SYSTEM

In proposed system we use three different entities data Owner, User, TPA, cloud server and attacker is untrusted entity. In this module first data owner upload the data file to cloud server using cryptography algorithm once data has store into database, owner gets the notification about file storage successfully [8]. The data owner having a full access of specific data file he can share or access, so data owner can share the any file to any user who can request for file then it will automatically access to particular user only normally; but in that one more access policy is their when Owner share particular file that time user can't access these file without key, so user can request for key to TPA and TPA can accept the user's request if it is trusted then TPA grant access and send key to user & that time user access particular file [9]. The shared user can access each file to anytime by cloud server. In first phase if data owner revokes any user from access the file then he can't access such file. If he can try to generate any collusion attack using SQL injection queries, even our system will prevent such attacks. Second data owner can share and revoke file to individual user to specific user, and third once any user revoke system will automatically generate proxy key generation that means existing keys will expire. Finally, if any un-trusted user can alter or hack any file from server that time our system easily recovers that file and give access to user. The overall approach improves the system efficiency as well security on drastic level [10].

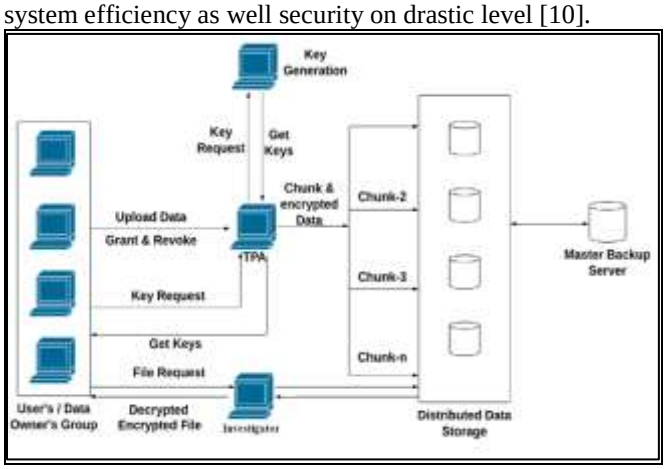

Fig. 1: System Architecture

IV. CONCLUSION

In this work system propose a secure Role Base Access Control (RBAC) data sharing scheme for untrusted environment in the cloud. In our scheme, the users can securely get their private keys from middleware authorities, TPA provide and secure communication between multi users. Also, our scheme is able to provide the secure revocation for untrusted user. The proxy key generation has also proposed in this work. When data owner revokes any specific end user system automatically expired the existing keys and generates new keys for all shared users. The system can achieve highest level security as well as privacy through such approaches [7].

It's a revocable decentralized data access control system can support efficient attribute revocation for multi-authority cloud storage systems. It eliminates decryption overhead of users according to attributes. This secure attribute based encryption technique for robust data security that is being shared in the cloud. This revocable multi-authority data access scheme with verifiable outsourced decryption and it is secure and verifiable. This scheme will be a promising technique, which can be applied in any remote storage systems and online social networks etc.

ACKNOWLEDGMENT

I would prefer to give thanks the researchers likewise publishers for creating their resources available. I'm conjointly grateful to guide, reviewer for their valuable suggestions and also thank the college authorities for providing the required infrastructure and support.

REFERENCES

[1] Sagar Borude, Arvind Kedar, Rahul Yeloe, Prof. S. S. Khatal, "Authorized Encrypted Search for Information Retrieval of Distributed System Journal Purpose Application". Proceedings of paper at International Journal of Research and Analytical Reviews (IJRAR), Volume 8 | Issue 2 | May 2021, pp. 799-803.
[2] [1]Prof. Sunil Khatal, Analyzing the role of Heart Disease Prediction System using IoT and Machine Learning
[3] Sunil S. Khatal , Health Care Patient Monitoring using IoT and Machine Learning
[4] Wei Li, KaipingXue, YingjieXue, and Jianan Hong, "TMACS: A Robust and Verifiable Threshold Multi-Authority Access Control System in Public Cloud Storage", IEEE Transactions on parallel and distributed systems, VOL.24, NO. 06, October 2017.
[5] Jianan Hong, KaipingXue and Wei Li, "Comments on "DAC-MACS: Effective Data Access Control for Multi-Authority Cloud Storage Systems"/Security Analysis of Attribute Revocation in Multi-Authority Data Access Control for Cloud Storage Systems", IEEE transactions on information forensics and security, VOL. 10, NO. 06, June 2017.
[6] Taeho Jung, Xiang-Yang Li, Zhiguo Wan, and Meng Wan, "Control Cloud Data Access Privilege and Anonymity with Fully Anonymous Attribute-Based Encryption", IEEE transactions on information forensics and security, VOL. 10, NO. 01, January 2017.
[7] Kan Yang and Xiao huaJia, "Expressive, Efficient, and Revocable Data Access Control for Multi-Authority Cloud Storage", IEEE Transactions on parallel and distributed systems, VOL. 25, NO. 07, July 2014.
[8] S. Kamara and K. Lauter, "Cryptographic cloud storage," in Proceedings of the 14th Financial Cryptography and Data Security, Springer, 2010, pp. 136-149.
[9] R. Ostrovsky, A. Sahai, and B.Waters, "Attribute-based encryption with non-monotonic access structures," in Proceedings of the 14th ACM conference on Computer and communications security, ACM,2014, pp. 195-203.
[10] N. Attrapadung, B. Libert, and E. Pana_eu, "Expressive key policy attribute based encryption with constant-size ciphertexts," in Proceedings of the 14th International Conference on Practice and Theory in Public Key Cryptography. Springer, 2011, pp. 90-108.
[11] T. Jung, X. Li, Z. Wan, and M. Wan, "Privacy preserving cloud data access with multi-authorities," in Proceedings of The 32nd IEEE International Conference on Computer Communications. IEEE, 2013, pp. 2625-2633.
[12] Z. Liu and Z. Cao, "On efficiently transferring the linear secret sharing scheme matrix in ciphertext-policy attribute-based encryption," IACR Cryptology ePrint Archive, vol. 2010, p. 374, 2010
[13] S. Patil, P. Vhatkar, and J. Gajwani, "Towards secure and dependable storage services in cloud computing," International Journal of Innovative Research in Advanced Engineering, vol. 1, no. 9, pp. 57-64, 2014.

