iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** V **Month of publication:** May 2022

DOI: https://doi.org/10.22214/ijraset.2022.42489

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue V May 2022- Available at www.ijraset.com

Data Security of Dynamic and Robust Role Based Access Control from Multiple Authorities in Cloud Environment

Vikas Nagrale[1], Mayur Yalji[2], Ashutosh Kumar[3]
[1, 2, 3]*Computer Science, Savitribai phule Pune University*

Abstract: ***Data integrity maintenance is the major objective in cloud storage. It includes audition using TTP for unauthorized access. This work implements 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, Elgamal encryption scheme; secure user access policy; Proxy Key Generation, Role Base Access Control (RBAC), advanced encryption standard (AES), etc.

I. INTRODUCTION

In existing system, a user can be a Data Owner and a Data Consumer simultaneously. Authorities are assumed to have powerful computation abilities, and they are supervised by government offices because some attributes partially contain users' personally identifiable information. The whole attribute set is divided 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. Further, by efficiently combining the traditional multi-authority scheme with TMACS, construct a hybrid one, which satisfies the scenario of attributes coming from different authorities as well as achieving security and system-level robustness [1]. In security analysis of attribute revocation in multi-authority data access control for cloud storage systems proposed the mechanism in dealing with attribute revocation could achieve both forward security and backward security. Analysis and investigation show that the work adopts a bidirectional re-encryption method in cipher text updating, so security vulnerability appears. Also 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 [2]. In a semi anonymous privilege control scheme Anony Control 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. The AnonyControl-F, which was fully prevents the identity leakage and achieve the full anonymity. Author's security analysis shows that both AnonyControl and AnonyControl-F are secure under the decisional bilinear Diffie–Hellman assumption, and author's performance evaluation exhibits the feasibility of scheme [3]. Cipher-text Policy Attribute-based Encryption (CP-ABE) is regarded as one of the most suitable technologies for data access control in cloud storage, because it gives data owners more direct control on access policies. However, it is difficult to directly apply existing CP-ABE schemes to data access control for cloud storage systems because of the attribute revocation problem.

©IJRASET: All Rights are Reserved

For that designed an expressive, efficient and revocable data access control scheme for multi-authority cloud storage systems, where multiple authorities coexist and each authority was able to issue attributes independently. Specifically, it proposed a revocable multi-authority CP-ABE scheme, and applies it as the underlying techniques to design the data access control scheme [4]. Sharing data in a multi-owner manner while preserving data and identity privacy from an untrusted cloud is a challenging issue, due to the frequent change of the membership. For that proposes a secure multi-owner data sharing scheme, named Mona, for dynamic groups in the cloud. By leveraging group signature and dynamic broadcast encryption techniques, any cloud user can anonymously share data with others. Meanwhile, the storage into N disjoint sets and controlled by each authority, therefore each authority is aware of only part of attributes. A Data Owner is the entity who wishes to outsource encrypted data file to the Cloud Servers. The Cloud Server, who is assumed to have adequate storage capacity, does nothing but store them. Newly joined Data Consumers request private keys from all of the authorities, and they do not know which attributes are controlled by which authorities. When the Data Consumers request their private keys from the authorities, authorities jointly create corresponding private key and send it to them. All Data Consumers are able to download any of the encrypted data files, but only those whose private keys satisfy the privilege tree Tp can execute the operation associated with privilege p. The server is delegated to execute an operation p if and only if the user's credentials are verified through the privilege tree Tp.

II. EXITING SYSTEM

Wang et al. proposed the notion of "zero knowledge public auditing" to resist off-line guessing attack.

Yu et al. recently enhanced the privacy of remote data integrity checking protocols for secure cloud storage, but their model works only in public key infrastructure (PKI) based scenario instead of the identity-based framework.

Wang proposed another identity-based provable data possession in multi-cloud storage.

For providing the integrity and availability of remote cloud store, some solutions and their variants have been proposed. In these solutions, when a scheme supports data modification, we call it dynamic scheme, otherwise static one (or limited dynamic scheme, if a scheme could only efficiently support some specified operation, such as append). A scheme is publicly verifiable means that the data integrity check can be performed not only by data owners, but also by any third-party auditor. However, the dynamic schemes above focus on the cases where there is a data owner and only the data owner could modify the data.To support multiple user data operation, Wang et al. proposed a data integrity based on ring signature.

To further enhance the previous scheme and support group user revocation, Wang et al. designed a scheme based on proxy re-signatures. Another attempt to improve the previous scheme and make the scheme efficient, scalable and collusion resistant is Yuan and Yu, who designed a dynamic public integrity auditing scheme with group user revocation. The authors designed polynomial authentication tags and adopt proxy tag update techniques in their scheme, which make their scheme support public checking and efficient user revocation. The cloud storage service (CSS) relieves the burden for storage management and maintenance. However, if such an important service is vulnerable to attacks or failures, it would bring irretrievable losses to the clients because their data or archives are stored in an uncertain storage pool outside the enterprises. These security risks come from the following reasons: First, the cloud infrastructures are much more powerful and reliable than personal computing devices, but they are still susceptible to internal threats (e.g., via virtual machine) and external threats (e.g., via system holes) that can damage data integrity; second, for the benefits of possession, there exist various motivations for cloud service providers (CSP) to behave unfaithfully toward the cloud users; furthermore, disputes occasionally suffer from the lack of trust on CSP because the data change may not be timely known by the cloud users, even if these disputes may result from the users' own improper operations

III.CONCLUSIONS

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 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. 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.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

IV. MOTIVATION

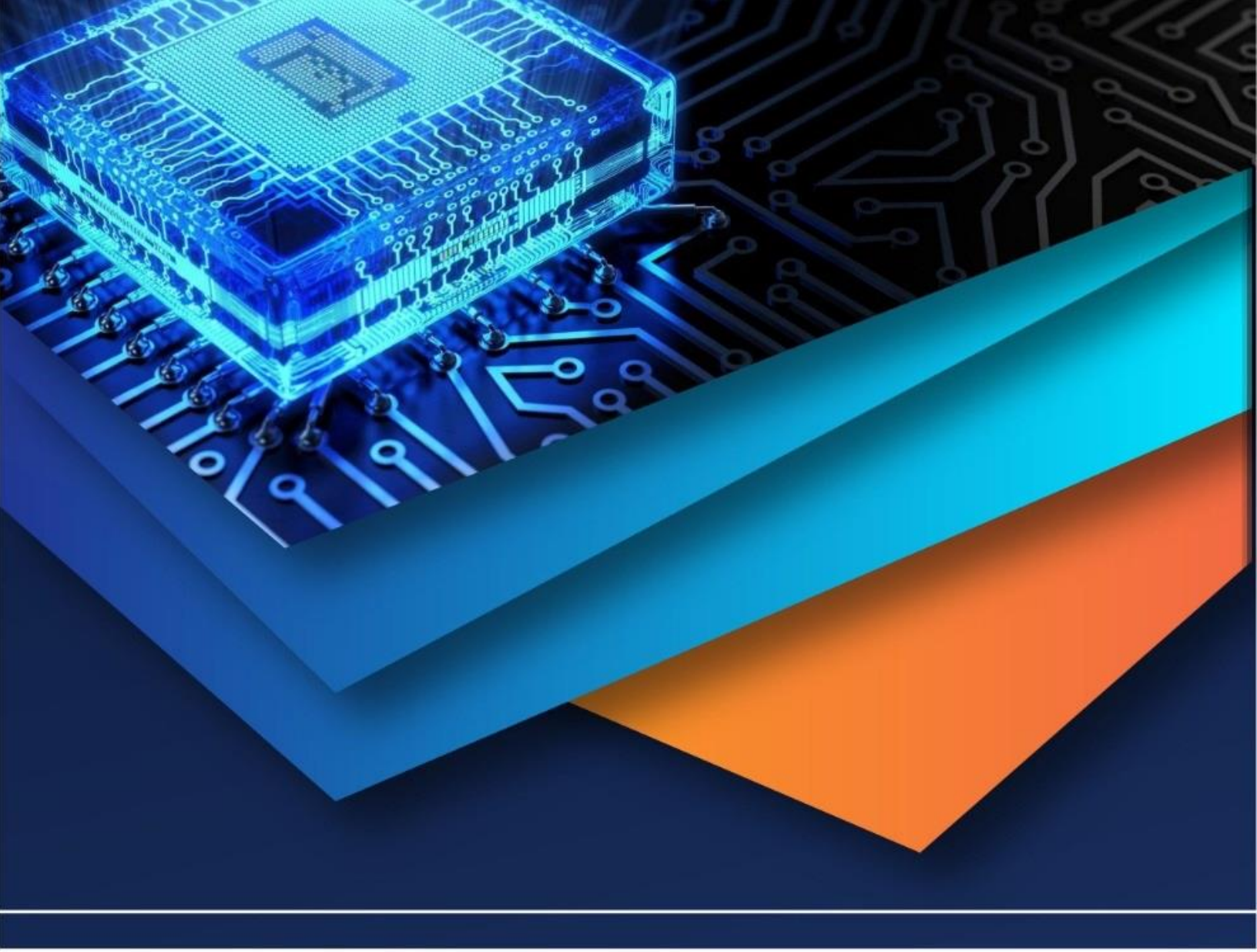
In existing system, a user can be a Data Owner and a Data Consumer simultaneously. Authorities are assumed to have powerful computation abilities, and they are supervised by government offices because some attributes partially contain users' personally identifiable information. The whole attribute set is divided into N disjoint sets and controlled by each authority, therefore each authority is aware of only part of attributes. A Data Owner is the entity who wishes to outsource encrypted data file to the Cloud Servers. The Cloud Server, who is assumed to have adequate storage capacity, does nothing but store them. Newly joined Data Consumers request private keys from all of the authorities, and they do not know which attributes are controlled by which authorities. When the Data Consumers request their private keys from the authorities, authorities jointly create corresponding private key and send it to them. All Data Consumers are able to download any of the encrypted data files, but only those whose private keys satisfy the privilege tree Tp can execute the operation associated with privilege p. The server is delegated to execute an operation p if and only if the user's credentials are verified through the privilege tree Tp.

V. ACKNOWLEDGMENT

I would like to express my special thanks of gratitude to my guide Prof. Prof. S. V. Shinde sir, P.D.E.A. college of engineering, manjari who gave us golden opportunity to do this wonderful project on the topic of data Security.

REFERENCES

[1] Wei Li, Kaiping Xue, Yingjie Xue, 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.
[2] Jianan Hong, Kaiping Xue 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.
[3] 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.
[4] S. Kamara and K. Lauter, "Cryptographic cloud storage," in Proceedings of the 14th Financial Cryptography and Data Security. Springer, 2010, pp. 136-149.
[5] B. Wang, B. Li, and H. Li, "Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud," IEEE Transactions on Services Computing, vol. 8, no. 1,pp. 92-106, 2015.
[6] J. Yuan and S. Yu, "Public Integrity Auditing for Dynamic Data Sharing with Multiuser Modification," IEEE Transactions on Information Forensics and Security, vol. 10,no. 8, pp. 1717-1726, Aug. 2015.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)