iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** III **Month of publication:** March 2019

DOI: http://doi.org/10.22214/ijraset.2019.3049

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: 6.887
Volume 7 Issue III, Mar 2019- Available at www.ijraset.com

A Survey on Access Control in Semi-Trusted Cloud Environment

E. Karthik[1], D. Eswari[2], K. Archana[3], A. Devi Priya[4]
[1]*Professor, Computer Science and Engineering, S.A. Engineering College.*
[2, 3, 4]*Student, Computer Science and Engineering, S.A. Engineering College.*

Abstract: ***Cloud computing is a powerful technology that has a major significance in today's Business world. But it cannot be fully trusted due to various security concerns. One of which is lack of secure data access control. Various techniques have been proposed to achieve secure data access control in semi-trusted cloud environment. CP-ABE algorithm is widely used to provide access control for the outsourced data in the cloud through access policies. This algorithm helps to prevent EDOS attack that involves malicious attacker's consumption of cloud resources using challenge text as an access policy. Owner-centric cloud access control using CP-ABE algorithm has been proposed to allow data owners to have complete control over the outsourced data. But a single data owner cannot manage all the tedious work loads separately, as it results in single-point of performance bottleneck. Hence multiple data owner enforced access control techniques have been proposed that helps to manage tedious workloads effectively. Another scheme namely Multi-message Cipher-text Policy Attribute-Based Encryption (MCP-ABE) technique has been proposed in light for sharing scalable media. In P2P based systems, CP-ABE algorithm along with a proxy re-encryption scheme has been for access control in cloud storage.***

Keywords: Cipher text-policy Attribute-based Encryption (CP-ABE), data access control, EDOS attack, multiple data owner

I. INTRODUCTION

Cloud has many benefits, to ensure confidentiality, data owner outsource the data by encrypting the plain text. In past the cloud provider not granted to verify whether a downloader can decrypt due to this a malicious attacker can download many number of files due to this EDOS attack is taken place.

This problem is overcome by the paper [1] where we have resource consumption accountability to avoid EDOS attack and also have access policy of CP-ABE to increase security.

The existing system fails to provide shared access privileges among user and cloud user in flexible manner to overcome this the paper[2] given a solution where it uses cipher text policy attribute-based encryption this achieves flexible delegation and shared access privileges with scalability and fine-grained access control.P2P storage brings new challenges for data security and access control to overcome this, the paper[19] addressed the above issues by designing CP-ABE scheme and proxy re-encryption scheme which propose secure, efficient and fine grained data access control mechanism for P2P storage cloud named ACPC also provide access policy based on user attributes and integrate P2P reputation system. ACPC reduces computation overheads. Previously many malicious users can download the data which leads to EDOS attack this problem is addressed in [10] where we use MCP-ABE (Multi-message cipher-text policy attribute based encryption) technique is used where it allows a content provider to mention an access policy and encrypt multiple messages in one cipher text, So due to this the users whose attributes satisfies the given access policy can only decrypt the text.

Previously there is single point performance bottleneck which is addressed in the paper [4] where CA (Central Authority) is generated where we have secret keys for legitimacy verified users to enhance the security they proposed an auditing mechanism to detect in which AA(Attribute Authority) has wrongly performed legitimacy verification procedure also provide super performance improvement on key generation.

The current security solutions are based on perimeter security. Cloud storage enables cloud users to focus more on their core competencies by alleviating data owners' burden of local data storage and maintenance. However, data integrity becomes the biggest concern of cloud users because they lose physical control over their outsourced files. Ateniese et al. proposed the notion of provable data possession, or data auditing, to address this challenging problem. Considering many practical scenarios where all users sharing cloud data need to read and modify the data, very recently, Yuan and Yu proposed a novel and efficient integrity auditing scheme supporting multi-user modification, public auditing, high error detection probability and efficient user revocation.

II. PERFORMANCE ANALYSIS

TABLE 1: TYPES OF ABE ALGORITHMS

Algorithm	Encryption time (ms)	Decryption time (ms)	Communication time (ms)
ABE	8743	8351	4615
KP-ABE	7428	6843	4038
CP-ABE	7312	6713	3561

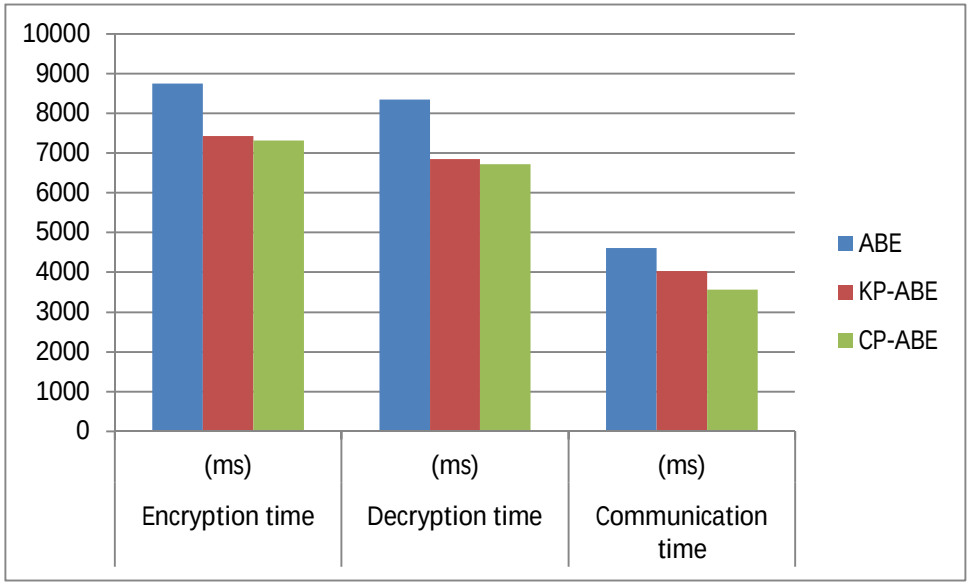


Fig: Performance analysis of ABE Algorithms

III.LITERATURE SURVEY

Some of the related works are discussed below:

In this paper [1], the authors have proposed a novel algorithm to deploy workflow applications on federated clouds along with an entropy-based method to quantify the workflow deployments. Then an extension of the Bell-LaPadula Multi-Level security mode is applied. In this paper [2], the authors have proposed a CP-ABE based cloud with white-box traceability and auditing namely crypt cloud. This scheme addresses the problem of credential misuse in semi-trusted cloud environment. In this paper [3], the author proposed that the data access control in public cloud storage systems was traditionally secured by a scheme called Cipher text-Policy Attribute-Based Encryption (CP-ABE). However in this scheme, there is a problem of single-point performance bottleneck which results in users getting stuck in a waiting queue for a long period of time to get their secret keys. Hence to overcome this problem, a more efficient heterogeneous framework scheme named RAAC is proposed for access control along with an auditing mechanism. In this paper [4], the authors have proposed a framework called Cloud Computing Adoption Framework (CCAF). CCAF multi-layered is used to provide security for real time data and three layers of security: 1) firewall and access control; 2) identity management and intrusion prevention and 3) convergent encryption). CCAF is more effective when combined with BPMN simulation to evaluate security process and testing results. In this paper [5] , the authors have proposed two assessment methods namely QPT and QHP and builds the security requirements specifications by exhibiting a flexible and straight forward framework that empowers User to perceive and address their specific security needs. In this paper [6], the authors have proposed a cloud architecture reference model along with a cloud security assessment model – Cloud-Trust, which helps in the quantization and estimation of the degree of confidentiality and integrity offered by the CCSs. The key functionality of Cloud-Trust is to assess the security levels of multi-tenant IaaS and to estimate the probability of CCS penetration levels by using the Bayesian network model of the CCS and the unique paths encountering APT attacks. In this paper [7], the authors have used CP-ABE scheme and a proxy re-encryption scheme to propose secure and efficient mechanism for P2P cloud storage namely ACPC. In this work most of the tedious work loads of data owners are delegated to cloud server and system peers. In this paper [8] , the authors have proposed a new scheme namely SAPIR which is a random combination of all data's that is stored across the network by using Random Linear

Fountain (RLF) codes. This proposed scheme provides adaptive and privacy against a significant number of colluding servers. To retrieve any requested content the servers within RG is collaborated with each other. The proposed solution is that the robust against a significant number of servers in the network. In this paper [9], the authors have proposed a new scheme that has four entities: the client, the cloud server, the auditor, and the key generation center (KGC) and six phases: Setup, Store, ChalGen, ProGen, VerPro, and CheckLog. In PDP model, when the client has updated their information to the cloud, he/she can delete the information in the local storage. If a client outsources a file with m blocks data and tags, the cloud server only store one block of them and passing the integrity auditing of the auditor. In this paper [10], the authors have proposed a two-factor data security protection mechanism with factor revocability for cloud storage system. Some naive approaches are used for enhancement of security protection for Double encryption (with an additional public key or serial number) and Split the secret key into two parts (The first part is stored in the computer while the second part is embedded into a security device).This scheme achieves two factors protection and security device revocability without requiring a great amount of additional complexity. In this paper [11], the authors have proposed ECSED, a novel semantic search scheme based concept hierarchy (the concepts at lower levels contain related meanings than those at higher levels) and the semantic relationship of encrypted datasets. ECSED uses two cloud servers (store the outsourced datasets and return results and compute the similarity scores. To improve this tree-based index structure is used. In this paper [12], the authors have proposed a scheme to deduplicate encrypted data stored in cloud based on data owner challenge and proxy re-encryption. This scheme can adjustably support on data update and sharing with deduplication even when the data owners are offline. It provides greater efficiency on big data deduplication in cloud storage. In this paper [13], the authors have proposed an identity-based (ID-based) RDIC protocol by making use of key-homomorphic cryptographic to lesser the complexity and the cost for publishing and managing the public key authentication framework in PKI-based RDIC schemes. It provides security against infected cloud server and third party verifier. In this paper [14], the authors have proposed a new system of novel server-side deduplication for encrypted data and allows cloud server to access to control the outsourced data encryption and this prevents the data leakage and guarantees data integrity against any tag inconsistency attack. This scheme has reduced computational overhead. In this paper [15], the authors have proposed an innovative and parallel trust computing scheme based on big data analysis for the trustworthy cloud service environment. It is used first to block and parallel computing mechanism, the speed of trust calculation is greatly which makes this trust computing scheme very suitable for a large-scale cloud computing environment.

IV. CONCLUSION

In this paper, we have presented a survey on access control in semi-trusted cloud environment. A comparison of existing techniques involving access control mechanisms is done. We have given an overview of methodologies of providing access control in semi-trusted cloud environment that provides security against EDOS attack. In the existing systems, data owners enforce the access control, which greatly reduces the complexity of key management and enhances the privacy requirements. These systems have provided a step towards trustworthy cloud computing environment.

V. FUTURE ENHANCEMENTS

Future research can include efficient resource consumption auditing with less overhead that should be practical and economically applicable in the semi-trusted cloud environment.

REFERENCES

[1] Zhenyu Wen ; Jacek Cala ; Paul Watson ; Alexander Romanovsky,“Cost Effective, Reliable and Secure Workflow Deployment over Federated Clouds”,IEEE Transactions on Services Computing ,2017(Volume: 10, Issue: 6), Page s: 929 – 941.

[2] Jianting Ning, Zhenfu Cao, Senior Member, IEEE, Xiaolei Dong, Kaitai Liang, Member, IEEE, Lifei Wei, and Kim-Kwang Raymond Choo, Senior Member, IEEE, “CryptCloud+: Secure and Expressive Data Access Control for Cloud Storage”, IEEE Transactions on Services Computing,2018,Page s: 1 – 1,Cited by: Papers (1)

[3] Kaiping Xue, Senior Member, IEEE, Yingjie Xue, Jianan Hong, Wei Li, Hao Yue, Member, IEEE,David S.L. Wei, Senior Member, IEEE, and Peilin Hong,“ RAAC: Robust and Auditable Access Control with MultipleAttribute Authorities for Public Cloud Storage”, 2017 , IEEE Transactions on Information Forensics and Security,(Volume: 12 , Issue: 4),Page s: 953 – 967,Cited by: Papers (16)

[4] Victor Chang, Muthu Ramachandran, Member, IEEE, “Towards achieving Data Security with the Cloud Computing Adoption Framework”,IEEE Transactions on Services Computing,2016,(Volume: 9 , Issue: 1),Page s: 138 – 151,Cited by: Papers (83).

[5] Jesus Luna, Ahmed Taha, Ruben Trapero, and Neeraj Sur, “Quantitative Reasoning About Cloud Security Using Service Level Agreements”,IEEE Transactions on Cloud Computing,2017 ,(Volume: 5 , Issue: 3),Page s: 457 – 471.

[6] Dan Gonzales, Member, IEEE, Jeremy Kaplan, Evan Saltzman, Zev Winkelman, Dulani Woods, “Cloud-Trust - a Security Assessment Model for Infrastructure as a Service (IaaS) Clouds”,IEEE Transactions on Cloud Computing,2017,(Volume: 5 , Issue: 3),Page s: 523 – 536,Cited by: Papers (11).

[7] Heng He, Ruixuan Li, Member, IEEE, Xinhua Dong and Zhao Zhang, Member, “Secure, Efficient and Fine-grained Data Access Control Mechanism for P2P Storage Cloud”,IEEE Transactions on Cloud Computing,2014 ,(Volume: 2 , Issue: 4),Page s: 471 – 484,Cited by: Papers (16).

[8] Mohsen KarimzadehKiskani and Hamid R. Sadjadpour, "Secure and Private Information Retrieval (SAPIR) in Cloud Storage Systems",IEEE Transactions on Vehicular Technology,2018,(Volume: 67 , Issue: 12),Page s: 12

[9] Feng Wang, Li Xu , Member, IEEE, and Wei Gao, "Comments on SCLPV: Secure Certificateless Public Verification for Cloud-Based Cyber-Physical-Social Systems Against Malicious Auditors",IEEE Transactions on Computational Social Systems,2018 ,(Volume: 5 , Issue: 3),Page s: 854 – 857

[10] Joseph K. Liu, Kaitai Liang, Willy Susilo, Jianghua Liu, and Yang Xiang, Senior Member, IEEE, "Two-Factor Data Security Protection Mechanism for Cloud Storage System",IEEE Transactions on Computers,,2016 ,(Volume: 65 , Issue: 6),Page s: 1992 – 2004

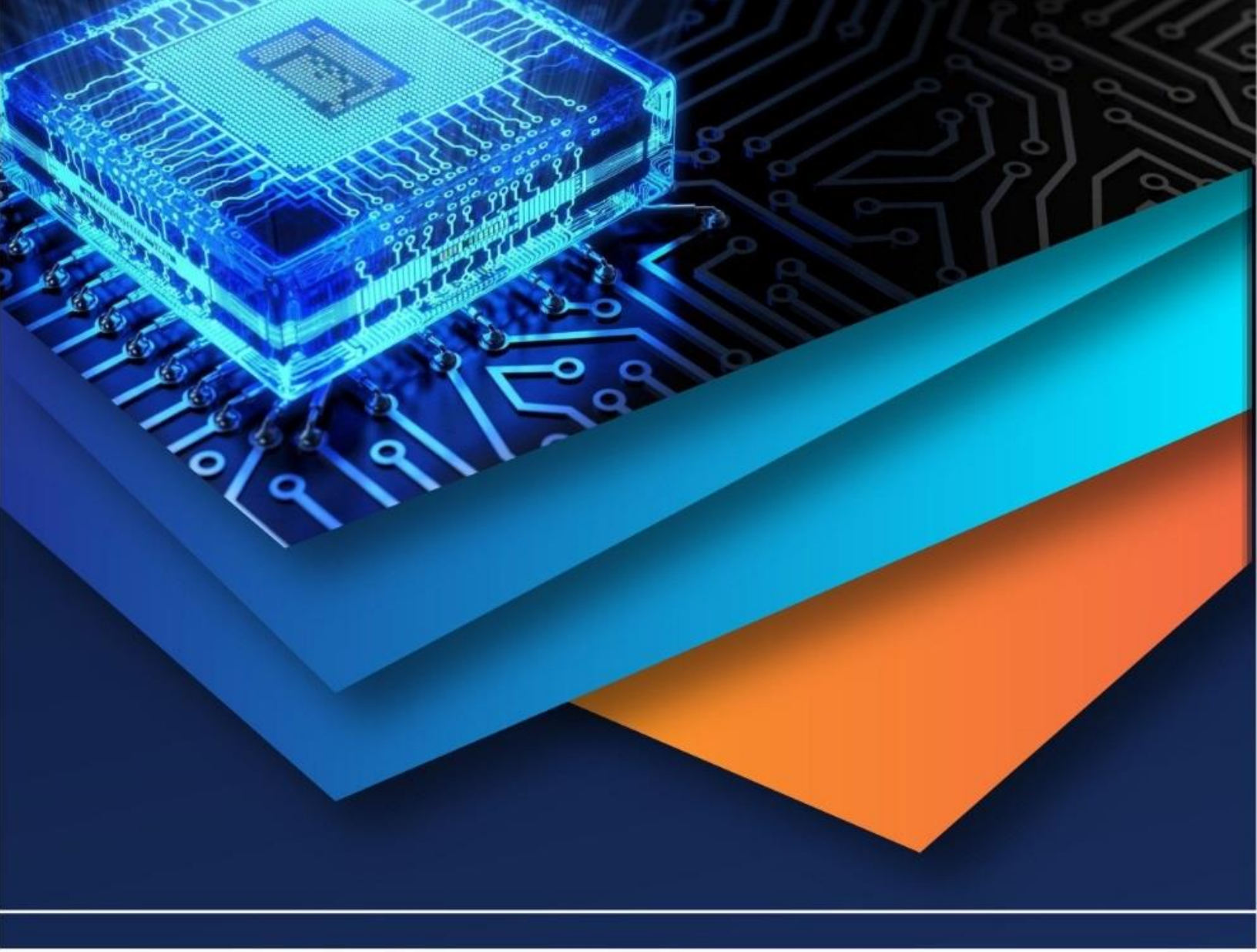
[11] Zhangjie Fu, Lili Xia, Xingming ,Sun Alex, X. Liu GuowuXie, "Semantic-aware Searching over Encrypted Data for Cloud Computing",IEEE Transactions on Information Forensics and Security,2018 ,(Volume: 13 , Issue: 9),Page s: 2359 – 2371.

[12] Zheng Yan, Senior Member, IEEE, Wenxiu Ding, Xixun Yu, Haiqi Zhu, and Robert H. Deng, Fellow, IEEE, "Deduplication on Encrypted Big Data in Cloud",IEEE Transactions on Big Data,2016 ,(Volume: 2 , Issue: 2),Page s: 138 – 150.

[13] Yong Yu, Man Ho Au, Member, IEEE, Giuseppe Ateniese, Xinyi Huang, Willy Susilo, Yuanshun Dai, and Geyong Min, ".Identity-Based Remote Data Integrity Checking With Perfect Data Privacy Preserving for Cloud Storage",IEEE Transactions on Information Forensics and Security,2017 ,(Volume: 12 , Issue: 4),Page s: 767 – 778.

[14] JunbeomHur, Dongyoung Koo, Youngjoo Shin, and Kyungtae Kang, "Secure Data Deduplication with Dynamic Ownership Management in Cloud Storage",IEEE Transactions on Knowledge and Data Engineering, 2016 ,(Volume: 28 , Issue: 11),Page s: 3113 – 3125

[15] XiaoyongLi , Member,,JieYuan,Member, IEEE, Huadong Ma, Senior Member, IEEE, and Wenbin Yao, "Fast and Parallel Trust Computing Scheme Based on Big Data Analysis For Collaboration Cloud Service", IEEE Transactions on Information Forensics and Security,2018,(Volume: 13 , Issue: 8),Page s: 1917 – 1931.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY