SECURE DATA GROUP SHARING AND CONDITIONAL DISSEMINATION WITH MULTI OWNER IN CLOUD COMPUTING

Vemuganti Shirisha , H.No: 21S41D5819,Mtech (Cse), Department Of Computer Science, Vaageswari College Of Engineering Thimmapur,Karimnagar, Telangana, India, Email-Id: vemugantishireesha@gmail.com.

Dr. Gulab Singh,Associate Professor, Department Of Computer Science, Vaageswari College Of Engineering Thimmapur,Karimnagar, Telangana, India,Email-Id: gulsinchu@gmail.com.

ABSTRACT

Cloud computing is being used to exchange enormous volumes of data due to its fast growth. While cloud computing has made use of cryptographic techniques to ensure data confidentiality, the mechanisms in place today are unable to enforce privacy concerns over cipher text that is associated with multiple owners. This means that co-owners are unable to effectively control whether or not data disseminators can actually distribute their data. This paper presents a conditional dissemination scheme with multi-owner in cloud computing that allows data owners to securely share private data with a group of users over the cloud. If the attributes in the data satisfy the access policies in the cipher text, the data disseminator can then share the data with a new group of users. Our next innovation is a multiparty access control system that allows the co-owners of the data to add new access rules to the cipher text based on their own privacy choices. Additionally, three solutions for policy aggregation—full permit, owner priority, and majority permit—are offered to address the issue of privacy conflicts resulting from disparate access regulations. Our approach is effective and feasible for safe data sharing with many owners in cloud computing, as shown by the security analysis and experimental outcomes.

Index Terms:- Data sharing, cloud computing, conditional proxy re-encryption, attribute-based encryption, privacy conflict.

I.INTRODUCTION

1.1 MOTIVATION:

Cloud computing has become popular due to its abundant storage capacity and rapid access. After combining computer infrastructure resources, it offers on-demand services over the Internet. Public cloud services are now offered by several well-known businesses, including Amazon, Google, and Alibaba. With the use of these services, both individual and business users may upload files (such as documents, movies, and images) to cloud service providers (CSPs) so they can access them from anywhere at any time and share them with others. Most cloud services implement access control by keeping an access control list (ACL) up to date in order to safeguard users' privacy. But consumers are worried about security breaches, mostly since the CSP stores the data in unencrypted form. The data owner no longer has control over the data after it has been submitted to the CSP. Regretfully, the CSP is often a semi-trusted server that complies with the established protocol but may gather user data and even utilise it for purposes other than those for which the users have given permission. However, a variety of data consumers may make excellent use of the data to understand user behaviour. These security concerns spur the development of practical solutions to safeguard data privacy. Adopting access control methods is crucial to achieving safe cloud computing data sharing.

1.2 PROBLEM DEFINITION:

As businesses and individuals increasingly rely on cloud service providers (CSPs) to store and manage their data, concerns about the control and access of this data have become paramount. Specifically, there are worries regarding security breaches, loss of control over data once it's entrusted to CSPs, and the potential for misuse of user data by semi-trusted servers.

One of the primary issues is the vulnerability of data shared via CSPs to unauthorized access or manipulation. Traditional cryptographic techniques may not adequately address these concerns, leading to the exploration of more advanced methods. Identity-based broadcast encryption (IBBE), attribute-based encryption (ABE), and remote attestation are among the cryptographic techniques discussed as potential solutions to enhance security and privacy in cloud computing.

However, while these techniques offer some level of protection, they also have

limitations, particularly concerning secure data distribution and fine-grained access control. This necessitates the exploration of more sophisticated approaches, such as conditional proxy re-encryption (CPRE), to address the evolving challenges of data security and privacy in cloud environments.

II.LITERATURE SURVEY

- Z. Yan, X. Li, M. Wang, and A. V. Vasilakos proposed a cloud computing offers a new way of services and has become a popular service platform. Storing user data at a cloud data center greatly releases storage burden of user devices and brings access convenience. Due to distrust in cloud service providers, users generally store their crucial data in an encrypted form. But in many cases, the data need to be accessed by other entities for fulfilling an expected service, e.g., an eHealth service. How to control personal data access at cloud is a critical issue. Various application scenarios request flexible control on cloud data access based on data owner policies and application demands. Either data owners or some trusted third parties or both should flexibly participate in this control. However, existing work hasn't yet investigated an effective and flexible solution to satisfy this demand. On the other hand, trust plays an important role in data sharing. It helps overcoming uncertainty and avoiding potential risks. But literature still lacks a practical solution to control cloud data access based on trust and reputation. In this paper, we propose a scheme to control data access in cloud computing based on trust evaluated by the data owner and/or reputations generated by a number of reputation centers in a flexible manner by applying Attribue-Based Encryption and Proxy Re-Encryption. We integrate the concept of context-aware trust and reputation evaluation into a cryptographic system in order to support various control scenarios and strategies. The security and performance of our scheme are evaluated and justified through extensive analysis, security proof, comparison and implementation. The results show the efficiency, flexibility and effectiveness of our scheme for data access control in cloud computing.

- B. Lang, J. Wang, and Y. Liu proposed for enterprise systems running on public clouds in which the servers are outside the control domain of the enterprise, access control that was traditionally executed by reference monitors deployed on the system

servers can no longer be trusted. Hence, a self-contained security scheme is regarded as an effective way for protecting outsourced data. However, building such a scheme that can implement the access control policy of the enterprise has become an important challenge. In this paper, we propose a self-contained data protection mechanism called RBAC-CPABE by integrating role-based access control (RBAC), which is widely employed in enterprise systems, with the ciphertext-policy attribute-based encryption (CP-ABE). First, we present a data-centric RBAC (DC-RBAC) model that supports the specification of fine-grained access policy for each data object to enhance RBAC's access control capabilities. Then, we fuse DC-RBAC and CP-ABE by expressing DC-RBAC policies with the CP-ABE access tree and encrypt data using CP-ABE. Because CP-ABE enforces both access control and decryption, access authorization can be achieved by the data itself. A security analysis and experimental results indicate that RBAC-CPABE maintains the security and efficiency properties of the CP-ABE scheme on which it is based, but substantially improves the access control capability. Finally, we present an implemented framework for RBAC-CPABE to protect privacy and enforce access control for data stored in the cloud.

- Q. Zhang, L. T. Yang, and Z. Chen proposed a survey **t**o improve the efficiency of big data feature learning, the paper proposes a privacy preserving deep computation model by offloading the expensive operations to the cloud. Privacy concerns become evident because there are a large number of private data by various applications in the smart city, such as sensitive data of governments or proprietary information of enterprises. To protect the private data, the proposed model uses the BGV encryption scheme to encrypt the private data and employs cloud servers to perform the high-order back-propagation algorithm on the encrypted data efficiently for deep computation model training. Furthermore, the proposed scheme approximates the Sigmoid function as a polynomial function to support the secure computation of the activation function with the BGV encryption. In our scheme, only the encryption operations and the decryption operations are performed by the client while all the computation tasks are performed on the cloud. Experimental

results show that our scheme is improved by approximately 2.5 times in the training efficiency compared to the conventional deep computation model without disclosing the private data using the cloud computing including ten nodes. More importantly, our scheme is highly scalable by employing more cloud servers, which is particularly suitable for big data.

- H. Cui, X. Yi, and S. Nepal presented a survey on the concept of Internet of Things (IoT) has raised in the cloud computing paradigm as it adds latency when migrating all pieces of data from the network edge to the data center for them to be approached. Edge computing has been introduced to extend the cloud computing architecture to the edge of the network, which analyzes most of the IoT data near the devices that produce and act on that data. Though edge computing solves the latency problem of data processing, it also brings issues to the data security and privacy preservation. One technique which is potential to provide scalable access control to support data security and privacy in edge computing is attribute-based encryption (ABE). In this paper, we propose a primitive named proxy-aided ciphertext-policy ABE (PA-CPABE), which outsources the majority of the decryption computations to edge devices. Compared to the existing ABE with outsourced decryption schemes, PA-CPABE has an advantage in which the key distribution does not require any secure channels. We present a generic construction of PA-CPABE and then formally prove its security. In addition, we implement an instantiation of the proposed PA-CPABE framework to evaluate its performance

- K. Xue, W. Chen, W. Li, J. Hong, and P. Hong proposed a people endorse the great power of cloud computing, but cannot fully trust the cloud providers to host privacy-sensitive data, due to the absence of user-to-cloud controllability. To ensure confidentiality, data owners outsource encrypted data instead of plaintexts. To share the encrypted files with other users, ciphertext-policy attribute-based encryption (CP-ABE) can be utilized to conduct fine-grained and owner-centric access control. But this does not sufficiently become secure against other attacks. Many previous schemes did not grant the cloud provider the capability to verify whether a downloader can decrypt. Therefore, these files should be available

to everyone accessible to the cloud storage. A malicious attacker can download thousands of files to launch economic denial of sustainability (EDoS) attacks, which will largely consume the cloud resource. The payer of the cloud service bears the expense. Besides, the cloud provider serves both as the accountant and the payee of resource consumption fee, lacking the transparency to data owners. These concerns should be resolved in real-world public cloud storage. In this paper, we propose a solution to secure encrypted cloud storages from EDoS attacks and provide resource consumption accountability. It uses CP-ABE schemes in a black-box manner and complies with arbitrary access policy of the CP-ABE. We present two protocols for different settings, followed by performance and security analysis.

III. EXISTING SYSTEM

An attribute-based CPRE approach was presented by Yang et al. via the implementation of an access policy inside a ciphertext produced using public-key encryption. The secret key linked to a collection of characteristics generates the re-encryption key, which the proxy may use to re-encrypt the ciphertext only in situations when these attributes meet the access policy requirements. In order to ensure receiver attribute authentication before to the re-encryption procedure, Wang et al. suggested a pre-authentication strategy for data sharing in the cloud.

DISADVANTAGES OF EXISTING SYSTEM:

Regrettably, this strategy disregards data confidentiality with regard to malevolent users and semi-trusted CSP, concentrating primarily on co-owners' access control over unencrypted data.

Because the requirements in previous CPRE schemes were limited to keywords, it would be more difficult to enforce complicated delegations in cloud computing.

IV PROPOSED SYSTEM:

In this research, we present a conditional dissemination strategy with multi-ownership in cloud computing and identity-based safe data group sharing. We provide a method to accomplish ciphertext group sharing across many users and capture the essential elements of multiparty authorization needs in order to lessen the issues with the current systems.

Using attribute-based CPRE, we accomplish fine-grained conditional distribution across the ciphertext in cloud computing. The data owner customises the first access policy before the ciphertext is initially delivered.

To address the issue of privacy conflicts, we provide three different approaches: majority permit, owner priority, and complete permit. In particular, the data disseminator must adhere to all access rules set out by the data owner and co-owners in the overall permission strategy. The majority permit approach allows the data owner to set a threshold value for the data co-owners first. The ciphertext may only be shared if and only if the data disseminator's characteristics satisfy the total number of access rules, which must be larger than or equal to this predetermined threshold.

ADVANTAGES OF PROPOSED SYSTEM:

In accordance with their privacy choices, the data co-owners may add new access rules to the ciphertext using our suggested multiparty access control technique. Therefore, the data disseminator may only re-encrypt the ciphertext if the characteristics meet sufficient access rules.

We conduct tests to assess the performance at each step in order to demonstrate the usefulness of our plan and verify that it is right.

V. SYSTEM DESIGN

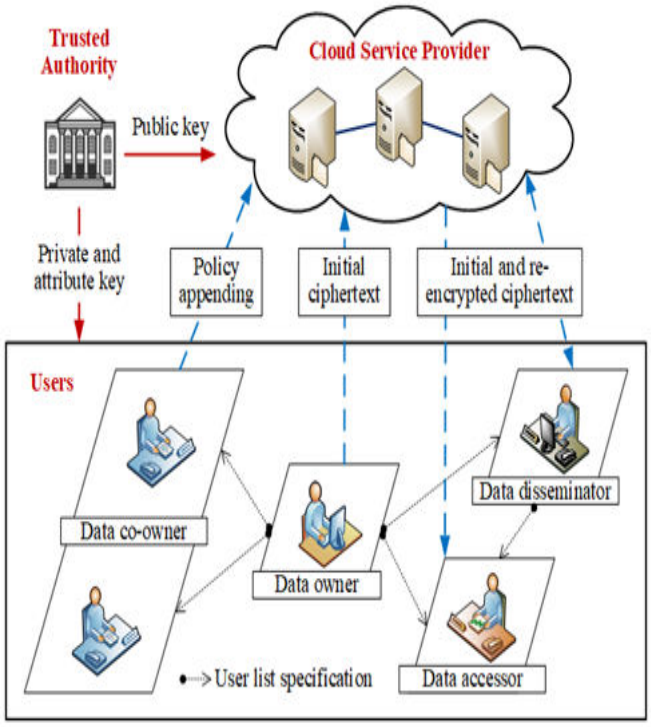


Fig1: Architecture of system.

VI.MODULE DESCRIPTION:

Trusted authority:

The trusted authority is a fully trusted part that initializes the system public key, and generates private keys as well as attribute keys for users. For example, it can be acted by the administrator of the organization or social security administration

CSP:

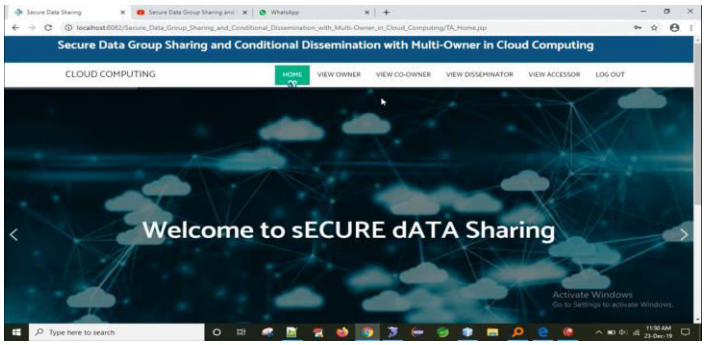
The CSP is a semi-trusted part that provides each user with a virtual space and convenient data storage service with the cloud infrastructure. It also appends access policies to the cipher texts for data co-owners and generates re-encrypted cipher texts for users.

Users:

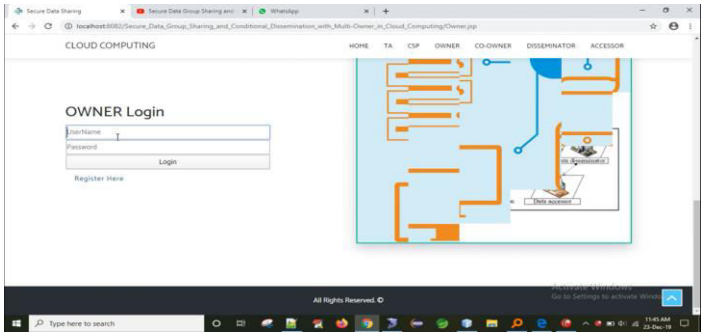
We divide the user role into the following categories: data owner, data co-owner, data disseminator and data accessor. The data owner can choose a policy aggregation strategy and define an access policy to enforce dissemination conditions. Then he encrypts data for a set of receivers, and outsources the cipher text to CSP for sharing and dissemination. The data co-owners tagged by data owner can append access policies to the encrypted data with CSP and generate the renewed cipher text. The data disseminator can access the data and also generate the re-encryption key to disseminate data owner's data to others if he satisfies enough access policies in the cipher text. The data accessor can decrypt the initial, renewed and re-encrypted cipher text with her or his private key.

VII. RESULT:

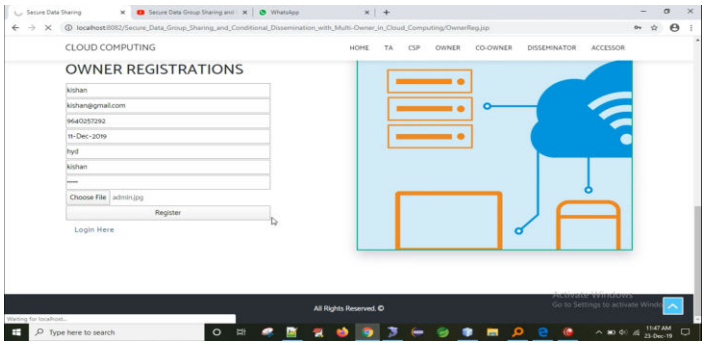
Home Page



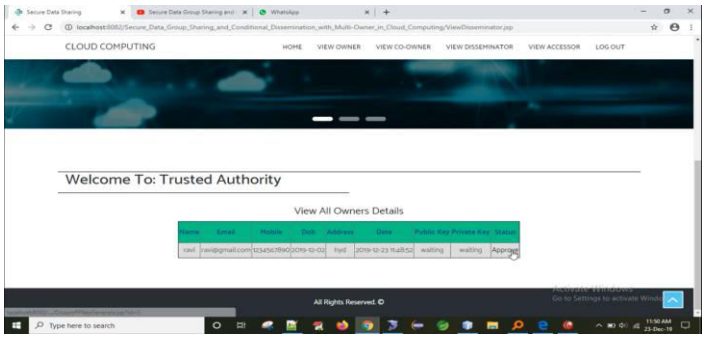
owner



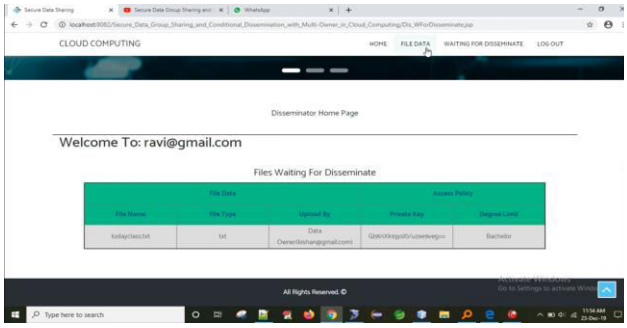
Owner registration



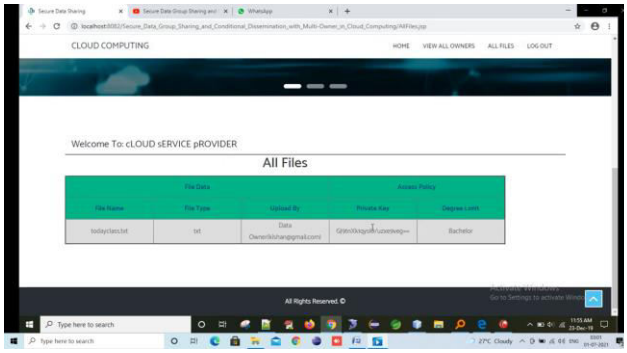
Trusted Authority



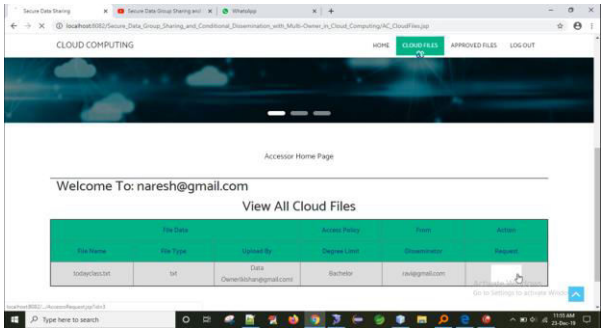
Disseminator



All Files



Accessor Home Page



VIII. CONCLUSION

When using cloud computing, customers are concerned about data security and privacy. Specifically, it becomes difficult to uphold the privacy concerns of many owners and maintain the anonymity of the data. In this research, we introduce a multi-owner conditional dissemination system and safe data group sharing in cloud computing. In our approach, the data owner might conveniently use the IBBE method to encrypt their private data and distribute it with several data accessors at once.Only data disseminators whose attributes fulfil the access policy in the ciphertext are allowed to re-encrypt the ciphertext, since the data owner may establish fine-grained access policies based on attribute-based CPREV. Additionally, we provide a multiparty access control method that enables co-owners of the data to add their own access rules to the ciphertext. In addition, we provide three policy aggregation mechanisms to address privacy conflicts: majority permit, owner priority, and complete permit.

IX. FUTURE ENHANCEMENT

We want to improve our system in the future by enabling keyword searches throughout the ciphertext.

X. REFERENCES

[1] Z. Yan, X. Li, M. Wang, and A. V. Vasilakos, “Flexible data accesscontrol based on trust and reputation in cloud computing,” IEEETransactions on Cloud Computing, vol. 5, no. 3, pp. 485-498, 2017.

[2] B. Lang, J. Wang, and Y. Liu, “Achieving flexible and self-containeddata

protection in cloud computing," IEEE Access, vol. 5, pp. 1510-1523, 2017.

[3] Q. Zhang, L. T. Yang, and Z. Chen, "Privacy preserving deep computationmodel on cloud for big data feature learning," IEEE Transactionson Computers, vol. 65, no. 5, pp. 1351-1362, 2016.

[4] H. Cui, X. Yi, and S. Nepal, "Achieving scalable access control overencrypted data for edge computing networks," IEEE Access, vol. 6, pp.30049–30059, 2018.

[5] K. Xue, W. Chen, W. Li, J. Hong, and P. Hong, "Combining dataowner-side and cloud-side access control for encrypted cloud storage,"IEEE Transactions on Information Forensics and Security, vol. 13, no. 8,pp. 2062–2074, 2018.

[6] C. Delerablée, "Identity-based broadcast encryption with constantsize ciphertexts and private keys," Proc. International Conf. on the Theoryand Application of Cryptology and Information Security (ASIACRYPT'2007), pp. 200-215, 2007.

[7] N. Paladi, C. Gehrmann, and A. Michalas, "Providing user securityguarantees in public infrastructure clouds," IEEE Transactions onCloud Computing, vol. 5, no. 3, pp. 405-419, 2017.

[8] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," Proc. IEEE Symposium on Security and Privacy (SP'07), pp. 321-334, 2007.

[9] L. Liu, Y. Zhang, and X. Li, "KeyD: secure key-deduplication withidentity-based broadcast encryption," IEEE Transactions on CloudComputing, 2018, https://ieeexplore.ieee.org/document/8458136.

[10] Q. Huang, Y. Yang, and J. Fu, "Secure data group sharing and disseminationwith attribute and time conditions in Public Clouds,"IEEE Transactions on Services Computing, 2018, https://ieeexplore.ieee.org/document/8395392.

[11] Box, "Understanding collaborator permission levels", https://community.box.com/t5/Collaborate-By-Inviting-Others/Understanding-Collaborator-Permission-Levels/ta-p/144.

[12] Microsoft OneDrive, "Document collaboration and co-authoring",https://support.office.com/en-us/article/document-collaborationand-co-authoring-ee1509b4-1f6e-401e-b04a-782d26f564a4.

[13] H. He, R. Li, X. Dong, and Z. Zhang, "Secure, efficient and finegraineddata access control mechanism for P2P storage cloud," IEEETransactions on Cloud Computing, vol. 2, no. 4, pp. 471-484, 2014.

[14] Z. Qin, H. Xiong, S. Wu, and J. Batamuliza, "A survey of proxy reencryptionfor secure data sharing in cloud computing," IEEE Transactionson Services Computing, 2018, https://ieeexplore.ieee.org/document/7448446.

[15] J. Son, D. Kim, R. Hussain, and H. Oh, "Conditional proxy reencryptionfor secure big data group sharing in cloud environment,"Proc. of 2014 IEEE Conference on Computer Communications Workshops(INFOCOM WKSHPS), pp. 541–546, 2014.