YIDDISH Vol 13 Issue 04,Oct 2023
ISSN NO: 0364-4308

SECURING DATA WITH BLOCK CHAIN AND AI

Sanjeevini S.H[1], T. Shreya Maadhury[2], P. Lahari[3], G. Tejaswini[4], G. Haripriya[5]

[1]Assistant Professor, Department of CSE(CS), MallaReddy Engineering College for Women, Hyderabad, TS, India.
Email: sanjeevinicsecs@gmail.com
[2,3,4,5]UG Students, Department of CSE(CS), MallaReddy Engineering College for Women, Hyderabad, TS, India.

ABSTRACT

Huge amounts of data are shared via cloud computing due to the quick development of cloud services. Although cryptographic techniques have been used to provide data confidentiality in cloud computing, current mechanisms are unable to enforce privacy concerns over ciphertext associated with multiple owners, making it impossible for co-owners to adequately control whether data disseminators can actually disseminate their data. In this research, we offer a multi-owner secure data group sharing and conditional dissemination strategy for cloud computing, where the data disseminator can distribute the data to a new group of users if the attributes comply with the access policies in the ciphertext. We also provide a multiparty access control system for the disseminated ciphertext, allowing the data co-owners to add new access restrictions in accordance with their personal privacy preferences. Three policy aggregation strategies—full permit, owner priority, and majority permit—are also offered to address the issue of privacy conflicts brought on by various access regulations. Our method is practicable and effective for secure data sharing with multiple owners in cloud computing, according to the security analysis and experimental findings.

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

INTRODUCTION

Rich storage resources and quick feedback are two characteristics that have made cloud computing a highly regarded technology. Additionally available are dispersed computer network resources and internet-delivered on-demand assistance. Public cloud services are now available thanks to a number of companies, including Google, Alibaba, and Amazon. Individual users and service users can upload data to the cloud service provider (CSP), which enables data sharing and is conveniently

available from anywhere at any time, with the assistance of these companies. Most cloud services maintain access control lists (ACLs) to implement access control and lessen client privacy concerns. Customers can choose to either authorise access requests for persons who have been pre-approved or decide to make their information available to anyone. Security risks between people rise since the CSP keeps the information in unencrypted. When the data is made available to the CSP, the information owner loses control. These defence and personal privacy considerations around data confidentiality serve as the driving force behind the compelling conclusions. CSP follows a prescribed protocol that qualifies it as a semitrusted web server, allowing it to use a customer's data for commercial purposes without that customer's consent. Other customers are quite interested in this data, and they would utilise it to learn more about the user's patterns of behaviour. In order to maintain secure information exchange, it is essential to apply accessibility control measures in cloud computing. Attribute-based security (ABE), remote attestation, and identity-based programme file encryption (IBBE) are now being employed as solutions to the safety and security challenges. ABE is one of the methods used in cloud computing for data exchange and protection. IBBE is a separate cloud computing option that enables information to be given to several receivers concurrently while taking into consideration each one's unique e-mail or ID. The encrypted data goes via access control by way of a system that ABE includes. IBBE makes it easier to assign information to specific people because it offers reasonably small policy sizes and cost-effective essential monitoring. These techniques make it possible for data owners to exchange information in a secure manner, which incentivizes more people to share their data via the cloud. These file encryption methods may prevent unauthorised parties from accessing the information, even though they do not help with data circulation in cloud computing. Additionally, after the data has been encrypted and delivered, the ciphertext that the data owner uploads cannot be changed. The proxy re-encoding strategy (PRE) entrusts the CSP with a re-encoding key connected to the new receivers in order to achieve secure data transfer in cloud computing. A reencryption secret cannot satisfy specific requirements since the day owner can only allow data disseminators

to distribute data that is similar to their own. The interpretation of conditional PRE (CPRE) thereby addresses this issue. a location where special ciphertext can be reencrypted. The conventional CPRE only supports basic key phrases, which makes it incapable of handling the dynamic situations that have actually developed in cloud computing. Using attribute-based CPRE can handle descriptive problems as opposed to search keywords, which would require ciphertext acquire access to control. The owner of the information will then construct the fine-grained distribution problem for the shared data in this manner. Cloud computing has become increasingly popular due to the advantages of wealthy people storing property as well as the future. This provides a summary of the computer system's characteristics and, in the end, offers benefits of on-demand over the Internet. Presently, a number of reputable companies, like Amazon, Google, and Alibaba, offer open cloud services. These systems enable both individual users and business users to upload data to a cloud service provider (CSP), access it from any location, and share it with others. The majority of cloud administrations maintain control by following the control list (ACL) in order to guarantee consumer security. We learn about a method for achieving multi-customer ciphertext team sharing and recognise the key components of multiparty authorization needs in order to overcome the aforementioned issues. The subsequent commitments under our Strategy:

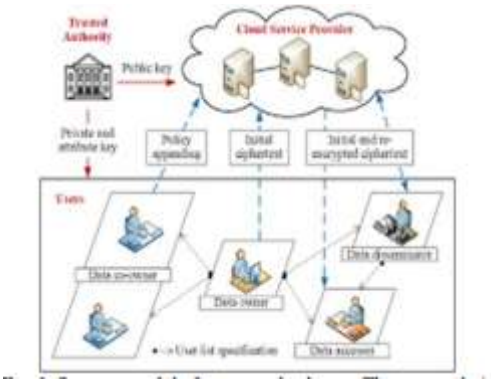
1. Using trait-based CPRE, we establish fine-grained, restricting distribution over the ciphertext in the cloud. Before the ciphertext is delivered, the information owner modifies the underlying accessibility arrangement. According to their security choices, the information co-owners can add extra accessible methods to ciphertext using our recommended multiparty reach control feature. If the features match ideal access approaches, the data disseminator will merely re-scramble the ciphertext moving ahead.

2. We offer three procedures—complete licencing, owner need, and also greater give—to address the problem of safety disputes. Except in exceptional circumstances, the data distributor must adhere to all access policies described in the data owner and co-owners fully licencing method. The data owner has the option to choose information co-owners at the outset of the dominant part grant procedure. The whole entryway

strategy carried out by the characteristics of the data disseminator must be more remarkable than or equal to this predetermined side in order for the ciphertext to be interacted. 3. We illustrate our strategy's accuracy and do tests to gauge how well it exhibits at each factor in order to develop its efficacy.

PROBLEM STATEMENT

IBBE uses compact consistent guideline sizes and also cost-effective critical control, which are more ideal for the secure transfer of data to different cloud recipients. When just one person decides to disclose this information with unauthorised people, there is a major and serious privacy risk. Multiparty access control for cloud computer data sharing, like cloud partnerships and cloud-based social networks, enables the shared information to be managed collaboratively with the specific authorization requirements of several connected customers as well as the requirement for problems with data dissemination.



Version for systems of the suggested strategy in Fig. 1. The following categories—data accessor, data coowner, information disseminator, and information owner—make up the user obligation.

The user function includes the roles of data accessor, co-owner, disseminator, and data owner.

Symbols	Description
MK, PK	The master secret key and system public key
SK	The private key of user
AK	The attribute key of user
M	The data
U	The set of data accessors' identities
W	The set of data co-owners' identities
DK	The symmetric key
CT_o	The initial ciphertext
T_o	The access tree of CT_o
CT_i	The newer ciphertext generated by policy appending
T_{co}	The access tree customized by data co-owner for CT_i
TK_i	The transformation key of data co-owner for CT_i
T_i	The access tree of CT_i
U'	The set of new accessors' identities
RK	The re-encryption key of data disseminator
CT_i'	The re-encrypted ciphertext

Table-1: Notations

EXISTING SYSTEM:

Yes, these file encryption solutions can prevent unauthorised parties from accessing the data, including malicious consumers and partially trustworthy CSPs, but they might not take cloud computing into consideration when considering data flow. In a cloud collaboration scenario like Box and also OneDrive, the

information disseminators (like the editor and also partner) may share the papers with additional people, including those outside the business. Once the data has been encrypted via the aforementioned methods, the ciphertext provided by the information owners cannot be changed. The proxy re-encryption (PRE) method is used to provide secure information circulation in cloud computing by giving the CSP access to a re-encryption crucial tied to the new receivers.

Although the data disseminator is permitted to disclose this re-encryption secret with others, doing so may not satisfy the functional requirement because the data proprietor may only allow for the sharing of a specific document. An additional novel idea known as conditional PRE (CPRE), which allows the data owner to implement re-encryption control over the initial ciphertexts and allows only the ciphertexts fulfilling specific requirements to be re-encrypted with the provided reencryption key, may be used to solve this problem.

Contrarily, traditional CPRE schemes can only support simple keyword conditions, making it difficult for them to be adapted to complex cloud computing scenarios.

SYSTEM SUGGESTED: The Peking University First Hospital's Health and Wellness Administration Facility is where we obtain our data (PUFH). To manage the data and set up a forecast plan, we use a data cleansing approach, dimensional reduction approaches, as well as other device detecting algorithms. The individual's case history and the results of the diagnostic tests are then converted into 0-1 attributes using word vector modelling. Second, we provide a dimensionality lowering method to solve the issue of high dimensionality and increasing processing complexity. Instead, we use artificial intelligence techniques to investigate the relationship between physical test data and potential carcinogens. These techniques are used by us to build our prediction network. Following a physical examination, the system offers an intuitive user interface for managers to confirm their health issues and for doctors to obtain intervention-set examinations. In actuality, the tool offers the doctor a way to improve projection accuracy through responses. These most recent pieces of tagged information will start the daily training process, which will naturally boost system performance. Co-owners of the information will undoubtedly refill the ciphertexts by

connecting their input methods as the spread issues, according to our goal. As shown in Fig., we have the procedures in place to comply with the requirements for multi-owner authorization.

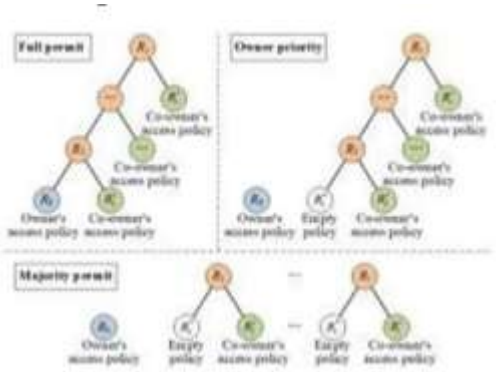


Fig. 2 displays three multiowner policy aggregation approaches.

1. Total permit: Each owner, including data owners and co-owners, has the opportunity to choose the data dispersion states. The data distributor will abide by any entry guidelines provided by specific owners.

The business owner needs: The data owner option has a big demand even though it gives co-owners. Only when the information disseminator complies with the entry arrangement of the data owner or the entry method of the data co-owners is information dissemination permitted.

3. Majority grant: All of the disseminator's access methods must be significantly more than or equal to the edge value that the information owner first chooses in order to spread the material.

SYSTEM REQUIREMENTS:

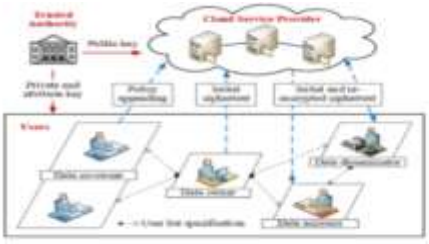
HARDWARE REQUIREMENTS:

- System : Pentium IV 2.4 GHz.
- Hard Disk : 40 GB.
- Ram : 2GB.

SOFTWARE REQUIREMENTS:

- Operating system : Windows .
- CodingLanguage : JAVA/J2EE
- Data Base : MYSQL
- IDE :Netbeans8.1

ARCHITECTURE DIAGRAM:



LITERATURE SURVEY:

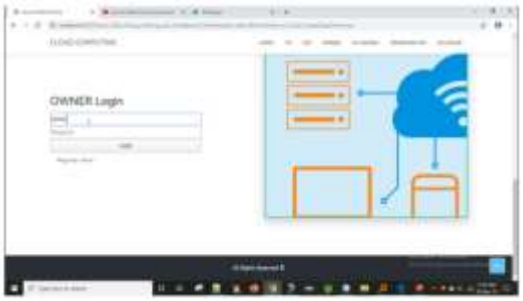
YEAR	TITLE	METHODOLGY	RESEARCH PROPOSAL	ALGORITHM
2018	Secure Data Group Sharing and Dissemination with Attribute and Time Conditions in Public Cloud	To achieve the capacity of bulk fine-grained access control and time-based exposing in cloud, a direct method is to handle time factor as an attribute.	In this scheme, only the users whose attributes satisfy the access structure and whose access rights are effective in the access time can recover corresponding data.	Setup(1k) KeyGen(PK, MK, S)
2019	Secure Data Group Sharing and Conditional Dissemination with Multi-Owner in Cloud Computing	In order to support expressive conditions rather than keywords, attribute-based CPRE is proposed, which deploys an access policy in the ciphertext.	provide three strategies including full permit, owner priority and majority permit to solve the privacy conflicts problem.	Enc(PK, M, T) Dec(PK, SK, CT)
2020	An Efficient Data Security System for Group Data Sharing in Cloud System Environment	To enable the strong security among the users, a new method is proposed cryptography storage system which diminishes the number of key exchange among the users.	System describes the details about group authorization, user approval, document upload, document view, document deletion and document access.	To provide more data security Advanced Encryption Standard algorithm is used to encrypt the document.

2021	A Privacy-Preserving and Verifiable Group Data Sharing Scheme in Cloud Computing	scheme can be divided into three parts, authentication phase, re-encryption phase between users and the proxy.	By leveraging proxy re-encryption and oblivious random access memory (ORAM), a privacy-preserving and untraceable scheme is proposed to support multiple users in sharing data in cloud computing.	attribute-based encryption (ABE), a proxy re-encryption and delayed re-encryption protocol

RESULTS:

OUTPUT SCREENSHOTS:

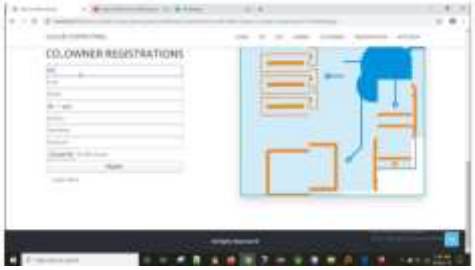
Owner Page:



Owner Registration:

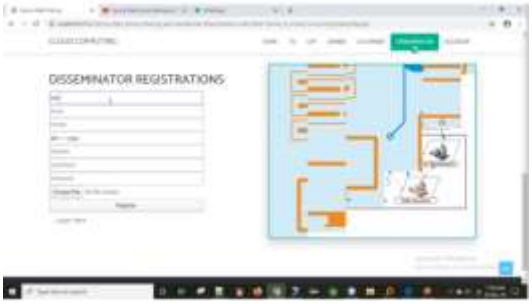
Regestration Completed:

Co-Owner Registration:

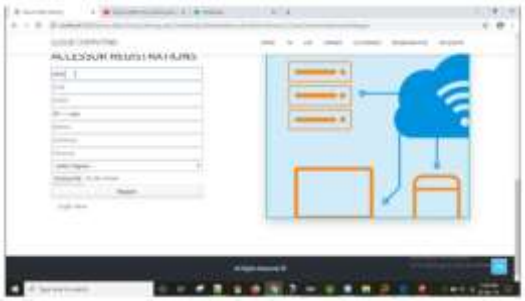


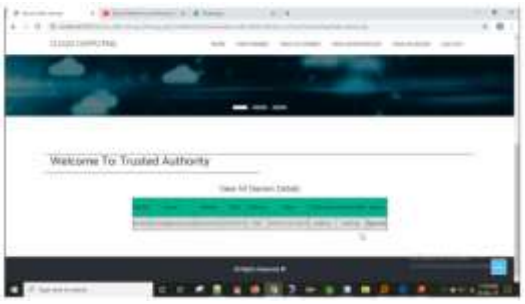
Regestration Completed:

Dissemnator Registration:



Upload Profile Pic:





CONCLUSION

Concerns regarding the security and privacy of user data are common among cloud computing users. Particularly, it becomes challenging to enforce privacy concerns of diverse owners and protect data confidentiality. In this study, we present a multi-owner safe data sharing strategy for cloud computing that uses conditional dissemination. With our proposal, the data owner could easily encrypt and transmit their confidential information to several data accessors at once using the IBBE technique. Because the data owner can give the ciphertext a fine-grained access policy based on attribute-based CPRE, the ciphertext can only be re-encrypted by data disseminators whose attributes satisfy the access policy in the ciphertext. We also provide a multiparty access control method where the co-owners of the data can add their access policies to the ciphertext. We also provide three policy aggregation solutions (full permit, owner priority, and majority permit) to solve the problem of privacy conflicts. Future versions of our method will be enhanced by the inclusion of keyword searches over the ciphertext.

REFERENCES

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

[2] B. Lang, J. Wang, and Y. Liu, “Achieving flexible and selfcontained data protection in cloud computing,” IEEE Access, vol. 5, pp. 1510- 1523, 2017.

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

[4] H. Cui, X. Yi, and S. Nepal, “Achieving scalable access control over encrypted 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 data owner-side and cloud-side access control for encrypted cloud storage,” IEEE Transactions on Information Forensics

Vol 13 Issue 04,Oct 2023
ISSN NO: 0364-4308

and Security, vol. 13, no. 8, pp. 2062–2074, 2018.

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