International Journal of Technology, Leadership and Sciences (IJTLS)
ISSN: 3107-9083 www.ijtls.com Paper ID: TLS-26/V2/I2-019
DOI: https://doi.org/10.5281/zenodo.19125595

SECURE AND PRIVACY-PRESERVING CLOUD DATA SHARING USING ATTRIBUTE-BASED ACCESS CONTROL

[#1]**SD. KHAJA PASHA,** ***Assistant Professor,***
[#2]**SOMA VAISHNAVI,** ***B.Tech Student,***
[#3]**KODURUPAKA AKSHITHA,** ***B.Tech Student,***
[#4]**DASARI PRIYANKA,** ***B.Tech Student,***
[#5]**MOHAMMAD SUFIAN HUSSAIN,** ***B.Tech Student,***
[#5]**GADDALA BHARGAV,** ***B.Tech Student,***
Department of AIML,
TRINITY COLLEGE OF ENGINEERING AND TECHNOLOGY, PEDDAPALLY, TG.

ABSTRACT: Cloud computing is an efficient and cost-effective way to transfer data. Data confidentiality is compromised when it is moved to approved cloud servers. Numerous strategies are put in place to enhance access control over shared data, preserving sensitive and important information in the process. It is possible to use ciphertext-policy attribute-based encryption (CP-ABE) to improve the security and effectiveness of these techniques. Although data confidentiality is the main focus of classic CP-ABE, user privacy has become a crucial concern. To protect user privacy and data confidentiality, CP-ABE uses an obscured access technique. However, the majority of current methods are inefficient in terms of processing and transmission costs. Furthermore, the majority of this research ignores privacy violations and authorization validation during the authority verification stage. This paper suggests a privacy-preserving CP-ABE system that incorporates effective authority verification as a remedy for the problems found. It guarantees that the size of its secret keys stays constant. Under decisional linear assumptions, the proposed approach offers particular security for the decisional n-BDHE problem. The computational findings validate the benefits of the suggested approach.

Index Terms*—Attribute-based encryption (ABE), authority verification, hidden access policy*

1. INTRODUCTION

The use of attribute-based encryption (ABE) to secure data in cloud computing access control is possible through ciphertext policy attribute-based encryption (CP-ABE) and key policy attribute-based encryption (KP-ABE). Secure information exchange in cloud contexts can be achieved with the help of CP-ABE, a cryptographic primitive.

The sole authority to set sharing access policies is the data owner. Data is safeguarded by CP-ABE using attribute-based access controls; a unique set of characteristics is associated with each user's secret key. In order to decipher the data, the user's credentials need to match the ciphertext's access criteria. In CP-ABE, users are required to procure their private keys from a trustworthy key authority. This is a major issue with the escrow process. Attributes with arbitrary states are not supported by most CPABE systems currently in operation. By introducing a weighted attribute data sharing system, this research aims to enhance attribute expression and solve the principal escrow problem. When implemented for processing and storage on the cloud, the suggested methodology shows improved functionality.

The cloud provider or key authority cannot obtain the user's private key in its entirety due to the two-party key issuing process. Weighted characteristics simplify access control and make it easier to generate more complicated binary values. Therefore, less space is needed to store ciphertext, and less time is required to encrypt data. When sending information to the cloud, users should not have unrealistic assumptions about how secure and private their data would be. However, conventional cryptographic primitives are unable to provide explicit data protection. Sharing data stored remotely across various system and security setups has recently attracted a lot of attention in privacy and security research.

The overarching goal of these actions is to achieve the necessary level of security while keeping the decryption process simple for consumers. Researchers have used hierarchical identity-based encryption (HIBE) and key-policy attribute-based encryption (KP-ABE) to protect sensitive data against unauthorized access and keep it confidential. Grants from the China National Key Basic research and Development Plan (Grant 2013AAOIA601), the China Doctoral Program of Higher Education (Grant 61170237), and the China National Natural Science Foundation (Grant 61170237) supported this research. However, certain information about how individual users access the cloud has leaked, and it isn't completely secure or good at preventing user privacy breaches. On the other hand, HIBE-based solutions generate a massive amount of keys, and each user ends up with a substantial number of them. They are also notoriously difficult to understand. To accomplish the goals of privacy and secure cloud data transmission, much work is still required.

The following requirements must be satisfied in order to create a cloud-based service that permits information exchange while protecting user privacy. Who can access a user's data stored in the cloud is mostly a decision for the data owner. Therefore, consumer privacy must be a top priority for cloud services. Shared data is now accessible from devices with lower processing capabilities, such smartphones and tablets. However, our understanding of these crucial aspects of cloud cooperation is still lacking. P2E secures data secrecy and privacy in the cloud without sacrificing usability or flexibility by integrating identity-based encryption (IBE) with cryptographic primitive ciphertext policy attribute-based encryption (CP-ABE). To guarantee privacy and prevent collusion, P2E makes use of a user's securely connected public and private keys. In contrast to systems based on HIBE, P2E does not generate additional user keys to address key management issues. P2E assigns relevant properties to each data file; users can access these attributes based on the data file types to which they have access. It is possible to generate a unique secret key for the same attribute by combining the public keys of all users. We create a pair of public and private keys for every feature to guarantee that all of the authorization mechanisms work.

Data files are encrypted using public key components and access matrices that are retrieved from the access structure. Since the configuration of users' private keys is dependent on their permissions, only those with the appropriate skills can decipher ciphertexts.

Here are the main points of this paper:

We demonstrate the security of P2E and its protection of access privilege confidentiality, backward secrecy, and granularity using cloud data sharing services. Additionally, we analyze performance and find that P2E has no effect on performance. Our privacy-preserving encryption method, P2E, prevents collusion, keeps data secret, and efficiently protects privacy. P2E is the lightest choice, according to the trial.

2. RELATED WORK

The key policy (KP) and ciphertext policy (CP) are integral components of both KP-ABE and CP-ABE, created through ABE protocols. The KP-ABE system produces the private key based on an access policy. The ciphertext is connected to a corresponding access policy in a CP-ABE framework. Users who contravene the policy's stipulations will permanently forfeit the restoration of their information. Currently, there is significant demand in obtaining ABE abilities. Nonetheless, the vast majority of these firms prioritize their own data security over that of their clients. Nishide devised the preliminary solution to protect customer privacy.

The access policy was only partially disclosed by this strategy, as it merely obscured the attribute name. The policy is obscured, preventing the adversary from acquiring user information. Nonetheless, their technique is fated to fail because to the exorbitant expense of computing it. In 2009, Waters proposed a CP-ABE system that utilized two separate encryption techniques. As a result, CP-ABE users were provided with an alternative data encryption technique. Lai subsequently employed this concept to build two HP-CP-ABE (hidden access policy CP-ABE) frameworks. It has been established that both provide the utmost level of security. The initial access structure is confined to the AND gate, whereas the subsequent one accommodates the more versatile linear secret sharing scheme (LSSS). Nonetheless, the confidential keys and ciphertext increase in accordance with the quantity of attributes. Rao subsequently unveiled an innovative and secure HP-CP-ABE approach. This technique is as secure as the preceding one, as it employs a composite-order group.

Nonetheless, it necessitates less time because the secret key and ciphertext are uniformly of identical size. This method is limited to the AND gate, which does not constitute an expression. Zhang leveraged Abdalla's technique to develop his hierarchical HP-CP-ABE strategy. It swiftly decodes information while maintaining a uniform key size for secure communication. Huang has demonstrated the HP-CP-ABE cryptosystem, which features stable key sizes and reduced computational expenses. It fails to comply with security standards, while it provides a degree of protection. Although the aforementioned technology can aid in protecting user privacy, a significant concern requires attention. When the access policy is obscured, the duration required to obtain communications from the server escalates, as users are compelled to decrypt the ciphertexts utilizing every possible combination of secret keys. It is essential to develop an effective method for decrypting ciphertexts. Zhang established an HP-CP-ABE system incorporating an authority verification phase to address this issue. Users can confirm their authorization at this point. The pairing process persists in eliciting privacy apprehensions.

Li subsequently developed an authority-verification technique to improve the HP-CP-ABE system. Consequently, users may abstain from undertaking superfluous computations. Nonetheless, the authority verification process allows us to assess the characteristics of the relevant access policy. Cui presented a revolutionary HP-CP-ABE technique. An increase in the number of features will lead to a rise in the quantity of secret keys and ciphertexts. Khan recommended the adoption of an LSSS-based access approach for HP-CPABE. Furthermore, support with authorization verification is accessible. Nonetheless, the exclusive component

that facilitated this was the adoption of concealed vector cryptography. It is inferior to other choices.

Zhang demonstrated an HP-CP-ABE system featuring an LSSS access policy and a variety of cosmological attributes. Prime order group-based schemes surpass composite order group-based schemes under identical conditions. Another approach of executing concealed access controls is inner-product predicate encryption (IPE). Nonetheless, this alteration will lead to a significant reduction in productivity. Phuong's IPE-inspired graphic illustrates that the length of the system's private keys and ciphertexts increases linearly with the number of features. Therefore, it is essential to enhance the CPU performance and augment the memory capacity.

3. SYSTEM DESIGN

To safeguard sensitive data in the cloud, we can employ security techniques include access control, attribute-based encryption (ABE), key policy attribute-based encryption (KPABE), and ciphertext-policy attribute-based encryption (CP-ABE). CP-ABE, a cryptographic primitive, has been proposed to enable secure information sharing in cloud environments.

The data proprietor exclusively dictates the access policies for sharing. CP-ABE protects data with access controls based on attributes, with each user's secret key linked to a specific set of attributes. The user's credentials must meet the access requirements of the ciphertext to decrypt the data. Users must obtain their private keys from a reliable key authority in CP-ABE. This poses a substantial escrow concern.

The majority of contemporary CP-ABE algorithms disallow the use of characteristics with random states. This work presents a weighted attribute-based data sharing method that improves attribute expressiveness and resolves the significant escrow issue. Therefore, the technique is more suitable for use in cloud-based applications. A two-party key issuance process prevents the cloud service provider or key authority from fully acquiring the user's private key. Weighted attributes streamline access controls, enhance the storage and decoding of ciphertext, and permit the binary characterization of an attribute.

SYSTEM ARCHITECTURE

Facial expression recognition allows this technology to preserve a major emotional category's expression. A conscientious firm may quickly build a strong reputation for facial traits, unlike the typical procedure that separates object extraction and detail sorting. Define a catastrophic threshold to solve the back-unfold problem. The probability estimates for each scenario are easily transferable.

International Journal of Technology, Leadership and Sciences (IJTLS)
ISSN: 3107-9083 www.ijtls.com Paper ID: TLS-26/V2/I2-019
DOI: https://doi.org/10.5281/zenodo.19125595

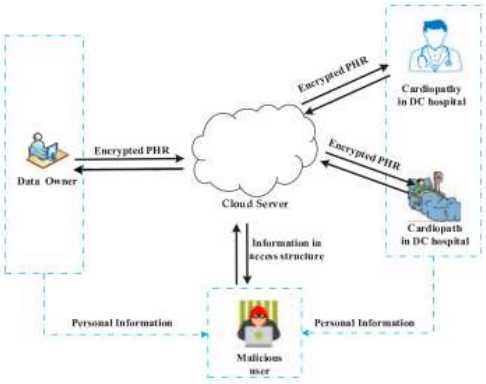

Fig 1: Architecture of face expression recognition system.

MODULES

Key Authority:

Tracking down everyone who had a hand in creating the CP-ABE covert and open regulations would be an enormous task. A user's property keys can be created, revoked, or amended by KA. Approved individuals who meet specific conditions are permitted access through the procedure outlined in it. The tone is captivating and sincere. Achieving fundamental competence in the management of sensitive data and the equitable execution of system duties are the aims. Unencrypted text, irrespective of its validity, must not have easy access to protected content.

CSP:

Provider of cloud computing services. The primary objective of the group is to enhance the effectiveness of data transfer. It provides people with vital information while ensuring that data storage is protected from unauthorized access. Together, the KA and the CSP—a semi-trusted key authority—offer thorough control over user access. We are able to achieve this by creating unique user keys and supervising the transfer of attribute group keys to authorized users. Act as though the CSP is trustworthy and exhibit qualities like honesty and inquisitiveness, much like the KA did in previous generations.

Data Owner :

Businesses may find that they can save money or have easier access with a cloud storage option. Data owners should encrypt their data and set up access restrictions based on attributes to make sure everyone is on the same page.

USER:

The ability to access data is fundamental to the operation of this organization. Encrypted data can only be accessed and decrypted by users who fulfill the requirements and are not banned

International Journal of Technology, Leadership and Sciences (IJTLS)
ISSN: 3107-9083 www.ijtls.com Paper ID: TLS-26/V2/I2-019
DOI: https://doi.org/10.5281/zenodo.19125595

from any sanctioned attribute groups. The KA and CSP are used to generate secret keys regardless of how decipherable the plaintext is. When it comes time to issue keys in the mathematical 2PC protocol, each participant must do it in their own unique way. Secured in their respective vaults are the master keys to this critical part. It is impossible for a single entity to produce all user secret keys since no entity has access to another entity's master secrets. The use of two processors allows this to be accomplished. The KA's refusal to provide assistance is conditional on the CSP's honesty.

4. RESULTS

Fig 2: Home page

Fig 3: View all users

International Journal of Technology, Leadership and Sciences (IJTLS)
ISSN: 3107-9083 www.ijtls.com Paper ID: TLS-26/V2/I2-019
DOI: https://doi.org/10.5281/zenodo.19125595

Fig 4: Send to the mail

5. CONCLUSION

The suggested attribute-based data sharing method makes use of the capabilities of the system as it is to guarantee appropriate management of data accessibility. A safe two-party calculation generates the private user keys.

The main concern with the escrow has been sufficiently resolved. When security standards are well-managed and Cloud Service Providers (CSPs) are kept out of the hands of malicious outside parties, cloud systems become more trustworthy. The weighted property would better define the feature. Streamlining authorization and enabling stateless functionality are both made possible by this feature. Data storage and encryption become less expensive as a result. By limiting who may access the system, the suggested changes will make the data exchange mechanism more secure.

The adaptable and configurable features of the data sharing system allow users to safely manage their data. Making experimental data graphs to compare the proposed system to the current one is the last stage. This means that less time and cloud storage for encryption will be required for the selected task.

The data shows that the proposed strategy works quite well and poses very little risk. Proxy re-encryption, searchable attribute-based encryption, and attribute-based data transit are all possible components of the proposed project. Research into possible data connectivity strategies is now being place on this platform.

REFERENCES

[1] A. Vouk and Mladel, "Cloud Computing: Issues, Research and Implementation," published in CIT Journal of Computing and Information Technology, vol. 16, no. 4, pp. 235–246, 2008.

[2] Uddin, Shahadat, et al., "Trend and efficiency analysis of co-authorship network," published in Scientometrics, vol. 90, no. 2, pp. 687–699, 2011.

[3] Ronghui Cao, Zhuo Tang, Chubo Liu, and Bharadwaj Veeravalli, "A Scalable Multicloud Storage Architecture for Cloud-Supported Medical Internet of Things," published in IEEE Internet of Things Journal, vol. 7, no. 3, March 2020.

[4] S. M. Metev and V. P. Veiko, "Laser Assisted Microtechnology," 2nd edition, edited by R. M. Osgood, Jr., Berlin, Germany: Springer-Verlag, 1998.

[5] A. Zhang, J. Chen, R. Q. Hu, and Y. Qian, "SeDS: Secure Data Sharing Strategy for D2D Communication in LTE-Advanced Networks," published in IEEE Transactions on Vehicular Technology, vol. 65, no. 4, pp. 2659–2672, 2016.

[6] Li, Z. Yang, and S. Xie, "Computing Resource Trading for Edge-Cloud-Assisted Internet of Things," published in IEEE Transactions on Industrial Informatics, 2019.

[7] W. Wang, P. Xu, and L. T. Yang, "Secure Data Collection, Storage and Access in Cloud-Assisted IoT," published in IEEE Cloud Computing, vol. 5, no. 4, pp. 77–88, 2018.

[8] T. Nishide, K. Yoneyama, and K. Ohta, "Attribute-Based Encryption with Partially Hidden Encryptor-Specified Access Structures," presented in the Proceedings of Applied Cryptography and Network Security, LNCS 5037, pp. 111–129, June 2008.

[9] J. Lai, X. Zhou, R. H. Deng, and Y. Li, "Fully Secure Ciphertext-Policy Hiding CP-ABE," presented in the Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, pp. 24–39, 2011.

[10] J. Lai, X. Zhou, R. H. Deng, Y. Li, and K. Chen, "Expressive CP-ABE with Partially Hidden Access Structures," presented in the Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security, pp. 18–19, May 2012.

[11] B. Waters, "Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization," presented in the Proceedings of the 14th International Conference on Practice and Theory in Public Key Cryptography , pp. 53–70, March 2011.