ATTRIBUTE-BASED CLOUD DATA SHARING FOR ENHANCED SECURITY AND PRIVACY

[#1]SARDAR INDRAJEETH KOUR, ***Department of MCA,***
[#2]Y.SUSHEELA, ***Assistant Professor,***
[#3]Dr.V.BAPUJI, ***Associate Professor& HOD,***
Department of Master of Computer Applications,
VAAGESWARI COLLEGE OF ENGINEERING, KARIMNAGAR,TELANGANA

ABSTRACT: Cloud computing provides a practical and competitively cost data sharing solution. Because the data is transported to some cloud servers, the privacy of the data contents is also affected. To protect sensitive and valuable information, many strategies are used to improve access control on shared data. Ciphertext-policy attribute-based encryption (CP-ABE) can make these methods more convenient and secure. Traditional CP-ABE just focuses on data confidentiality, however user privacy protection is now a critical problem. CP-ABE's disguised access policy ensures both data confidentiality and user privacy protection. However, the bulk of current approaches are inefficient in terms of communication and processing costs. Furthermore, the bulk of those studies fail to account for authority verification or the issue of privacy leaking during the authority verification step. To solve the concerns raised above, this paper proposes a privacy-preserving CP-ABE system with effective authority verification. It also achieves a consistent size for its secret keys. The proposed approach achieves selected security for the decisional n-BDHE problem with decisional linear assumption. The computational results back up the benefits of the recommended technique.

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

1. INTRODUCTION

Data security for cloud computing access control can be maintained via attribute-based encryption (ABE), including key policy attribute-based encryption (KP-ABE) and cipher text attribute-based encryption (CP-ABE). For secure cloud-based information sharing, CP-ABE has been proposed as a cryptographic primitive. Only the owner of the data can determine the access policies for sharing. To protect information, CP-ABE relies on access controls on attributes, with each user's secret key associated with a unique set of characteristics. The only way a user can decrypt ciphertext is if their credentials are in accordance with the ciphertext's access requirements. Users' private keys in CP-ABE must be issued to them by a reliable key authority. One major escrow issue is precipitated by this. Properties with arbitrary states are not supported by the vast majority of currently deployed CPABE systems. In this research, we develop a system for weighted attribute data sharing to improve attribute expression and address the key escrow problem. The proposed solution, then, is more compatible with cloud storage and processing. Neither the key authority nor the cloud service provider can steal the user's secret key in its entirety under a two-party key issuance system. Using weighted attributes allows for more nuanced binary value construction and simplified access control. The time it takes to encrypt data and the space it needs to store ciphertext are both reduced as a result. The sender of data to the cloud has a reasonable expectation of privacy and security for that data. On the other hand, common cryptographic primitives cannot be used to secure data directly. Sharing remotely stored data under different system and security settings has received a lot of interest in recent privacy and security research. To achieve the appropriate level of security without making the decryption procedure too difficult for consumers is a primary concern for these types of projects. In order to prevent unauthorized access and maintain the confidentiality of sensitive data, scientists have turned to hierarchical identity-based encryption (HIBE) and key-policy attribute-based encryption (KP-ABE). This research was supported financially by grants from the China

National Key Basic Study and Development Plan (Grant 2013AAOIA601), the China National Natural Science Foundation (Grant 61170237), and the China Doctoral Program of Higher Education. However, there is some information leakage regarding how some users connect to the cloud, and this information is neither fully collusion-proof nor able to safeguard user privacy. On the other side, HIBE-based approaches are difficult to keep up with and increase the amount of keys (each user has a high number of keys). Therefore, there is still a ways to go before we achieve the desired outcomes of good cloud data sharing and privacy protection. The following requirements must be completed to create a cloud-based service for exchanging information while protecting user privacy. The owner of the data should be the first to select who has access to a user's data stored in the cloud. Second, cloud services must respect users' right to confidentiality. Viewing shared data is now possible even on devices with less processing capability, such as smartphones and tablets. These fundamental aspects of collaboration in the cloud are currently poorly understood. P2E combines the identity-based encryption (IBE) technique with the cryptographic primitive ciphertext policy attribute-based encryption (CP-ABE) to safeguard privacy and maintain data secrecy in the cloud while maintaining usability and adaptability. In order to avoid collusion and maintain privacy, P2E uses a user's public key and a user's private key that are securely linked together. To solve the issue of key management, P2E does not generate additional user keys like HIBE-based systems do. P2E assigns pertinent characteristics that define each data file, and users can view these attributes depending on the data file types they have access to. When all users' public keys are combined, the resulting secret keys for the same attribute will be different for each user. To ensure the efficacy of these authorization methods, we generate a public and secret key pair for each attribute. Public key elements and access matrices derived from the access structure are used to encrypt data files. Users' secret keys are configured in accordance with their permissions, ensuring that only those with the necessary expertise can decrypt ciphertexts.

Specifically, the main contributions of this paper can be summarized as following:

We propose P2E, an efficient privacy-preserving encryption scheme that protects privacy, prevents collusion, and keeps data private when using cloud data sharing services; we demonstrate that P2E is secure, and that it protects fine-grainedness, backward secrecy, and access privilege confidentiality when using cloud data sharing; and we conduct a performance analysis that demonstrates P2E has a negligible impact on performance. The experiment demonstrated that P2E is as lightweight as it gets.

2. RELATED WORK

Both KP-ABE and CP-ABE consist of the key policy (KP) and ciphertext policy (CP) that are determined by ABE techniques. The KP-ABE system uses an access policy to generate the private key. The ciphertext is linked in a CP-ABE approach with the aid of an associated access policy. Users who don't adhere to the policy's requirements will never get their information back. The acquisition of ABE skills is currently trendy. However, the vast majority of these companies prioritize the security of their own data over that of their customers. Nishide pioneered the first method of protecting users' anonymity. By concealing merely the attribute name, this strategy only partially revealed the underlying access policy. Because the policy is obscured, the adversary is unable to obtain user information. Their proposal, however, is doomed to failure since it would be prohibitively expensive to calculate. Waters presented a CP-ABE strategy using two different encryption methods in 2009. Users of CP-ABE were thus provided with an additional means of data encryption. This technique was then utilized by Lai in the creation of two HP-CP-ABE (hidden access policy CP-ABE) strategies. Both have been proven to provide the highest level of safety. In contrast to the second access structure, which is compatible with the more versatile linear secret share scheme (LSSS), the first one can only be used with the AND gate. The ciphertext and the secret keys,

however, rise in size in proportion to the number of features. After that, Rao demonstrated an innovative and risk-free HP-CP-ABE technique. The use of a composite-order group makes this method just as secure as the previous one, but it is more time-efficient due to the constant size-match between the secret key and the ciphertext. However, this strategy is limited to the AND gate, which cannot be used in an expression. Zhang developed a hierarchical HP-CP-ABE strategy based on Abdalla's approach. It has fast decoding capabilities and maintains the same key size for private communication. Huang recently demonstrated the HP-CP-ABE, a cryptosystem with unchanged key sizes and reduced processing costs. It provides some safety, but not enough to be considered a security standard. Although the aforementioned technologies can help safeguard users' privacy, there is still one critical concern that must be addressed. If the access policy is concealed, the time it takes to get messages back from the server increases because users must try all possible combinations of the secret keys to decrypt the ciphertexts. An efficient method of decrypting ciphertexts should be developed. To alleviate this issue, Zhang developed an HP-CP-ABE system that includes an authority verification stage. This step allows users to verify their status as authorized users. The match phase still has privacy issues. Then, Li improved upon the HP-CP-ABE system by developing an authority checking mechanism. Users may reduce unnecessary computing as a result. However, the authority verification procedure also allows for examination of the access policy traits in question. Cui presented a novel HP-CP-ABE method. The number of secret keys and ciphertexts will increase proportionally with the number of attributes. Khan proposed an LSSS-based access method for HP-CPABE. There is also backing for confirming the authority. However, this was only possible because to the employment of hidden vector cryptography. It's not as effective as other solutions. Using an LSSS access policy and a sizable cosmological attribute set, Zhang demonstrated an HP-CP-ABE system. Prime order group based schemes perform better than composite order group based schemes in the same scenario. Inner-product predicate encryption (IPE) is another method that can be used to implement covert access constraints. However, this shift will significantly reduce productivity. Phuong's IPE-inspired figure reveals that the length of the system's ciphertexts and private keys scales linearly with the number of features. More memory and CPU speed are required as a result.

3. SYSTEM DESIGN

In order to keep sensitive information safe in the cloud, we can employ security measures like access control, attribute-based encryption (ABE), key policy attribute-based encryption (KPABE), and ciphertext-policy attribute-based encryption (CP-ABE). For secure cloud-based information sharing, CP-ABE has been proposed as a cryptographic primitive. Only the owner of the data can determine the access policies for sharing. To protect information, CP-ABE relies on access controls on attributes, with each user's secret key associated with a unique set of characteristics. The only way a user can decrypt ciphertext is if their credentials are in accordance with the ciphertext's access requirements. Users' private keys in CP-ABE must be issued to them by a reliable key authority. One major escrow issue is precipitated by this. The great majority of existing CP-ABE algorithms also forbid using characteristics with random states. This research demonstrates a mechanism for sharing data based on weighted attributes, which both eliminates the crucial escrow issue and increases the expressive power of attributes. Because of this, the final method is superior for use in cloud-based programs. Neither the key authority nor the cloud service provider can steal the user's secret key in its entirety under a two-party key issuance system. Weighted attributes allow you to characterize an attribute binary in any way you'd want, simplify the access policy, and lessen the burden of storing and decrypting ciphertext.

SYSTEM ARCHITECTURE

This device was built with facial expression recognition in mind, so it can remember the expression you want to use for one of the most significant emotion categories. A concerned company may immediately establish a solid

reputation for facial characteristics, in contrast to the typical procedure, which splits the object extraction and detail sorting processes. A catastrophic level is established to correct the back-unfold error. Probability estimates for each outcome can be readily forwarded at the conclusion.

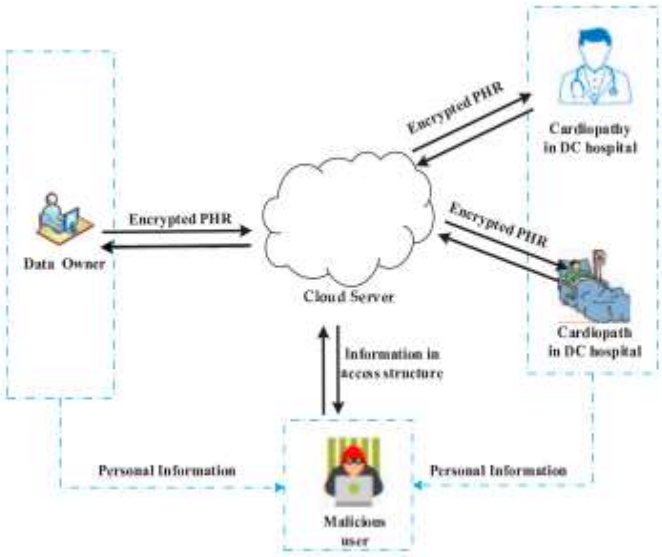

Fig 1: Architecture of face expression recognition system.

MODULES

Key Authority:

Key Authority (KA):The primary figure responsible for creating both the open and covert regulations for CP-ABE is only partly reliable. It is KA's responsibility to issue, revoke, and update a user's property keys. As an added bonus, it allows only approved individuals with specific characteristics to gain access. The tone is both sincere and intriguing. In other words, it intends to perform its duties inside the system equitably, but it also seeks to gain as much knowledge as possible about how sensitive data operates. The plaintext of protected data should not be easily accessible, regardless of the veracity of the information.

CSP:

Provider of cloud computing servicesIt's a company that facilitates the transfer of data. It is responsible for preventing unauthorized access to data storage while also providing relevant information to users. The CSP, as a semi-trusted key authority, generates unique user keys in tandem with the KA and distributes and revokes attribute group keys for each attribute to and from authorized users, thereby enabling fine-grained user access control. Assume that, like the KA in prior designs, the CSP is a semi-trusted (honest yet curious) party.

Data Owner :

It's a business with data that wants to make it more accessible or make financial savings by storing it with the CSP. Data owners are primarily responsible for encrypting their own data and establishing (attribute-based) access restrictions to ensure compliance.

USER:

It's an entity that requires data access. A user can decrypt the ciphertext and obtain the data if his or her set of attributes matches the access policy for the encrypted data and the user is not excluded from any of the valid attribute groups. Users should be able to receive secret keys from the KA and CSP, but neither should be able to read the plaintext of the information being sent. In the mathematical 2PC protocol's key issuance phase, each party distributes a unique key component to a user, protected by their own private master key. Since they can't learn each other's master secrets, no single person can generate all of the user secret keys. This is made possible by the 2PC system. If the KA is being honest, they will not cooperate with the CSP.

4. RESULT

Fig 2: Home page

Fig 3: View all users

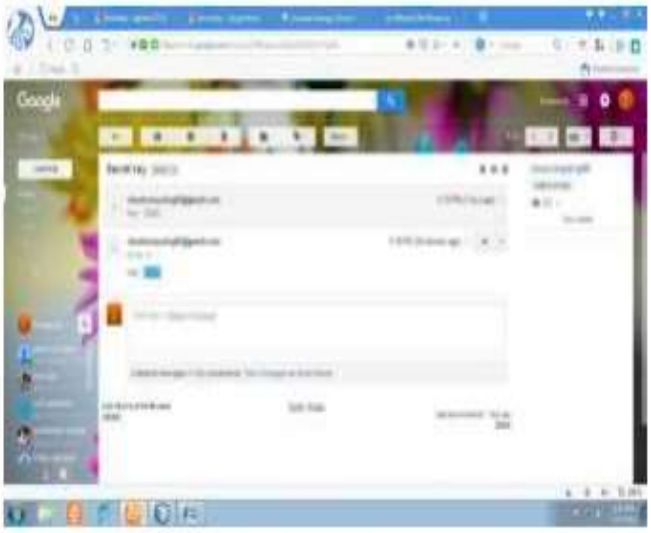

Fig: 4 Send to the mail

5. CONCLUSION

By taking advantage of the attributes of the system, the proposed attribute-based data sharing method provides granular control over data access. The private user keys are generated via a secure two-party calculation. The issue of key escrow is therefore resolved. By increasing protections against both the KA and CSP administration and malevolent outsiders, it helps make cloud systems semitrusted. It was also suggested that the weighted property be used in order to better explain the feature. You can utilize this feature to make stateless characteristics and streamline permissions. The price of encryption and data storage is reduced as a result. Therefore, the planned work secures the system for sharing data and regulates access to it. The data sharing system's secure user data control is also flexible and extensible. The final stage is to create graphs of the experiment findings that contrast the existing system with the proposed one. This means less time is needed to encrypt the specified task and less cloud storage is required. The findings demonstrate the efficacy and safety of the proposed action.Attribute-based data sharing, proxy re-encryption, and searchable attribute-based encryption may all be incorporated into improved versions of the proposed work in the future. Here is where research into potential data communication strategies is being conducted.

REFERENCES

[1].A Vouk, Mladel. “Cloud computingIssues, Research and Implementation”. CIT. Journal of Computing and Information technology 16.4(2008):235-246.

[2].Uddin, Shahadat, et al. "Trend and efficiency analysis of co-authorship network." Scientometrics 90.2 (2011): 687- 699.

[3].Ronghui Cao, Zhuo Tang, Chubo Liu, Bharadwaj Veeravalli. “A Scalable Multicloud Storage Architecture forCloudSupported Medical Internet of Things” IEEE Internet of Things Journal (Volume: 7, Issue: 3, March 2020)

[4].S. M. Metev and V. P. Veiko, “Laser Assisted Microtechnology”, 2nd ed., R. M. Osgood, Jr., Ed. Berlin, Germany: SpringerVerlag, 1998.

[5].A. Zhang, J.Chen, R. Q. Hu, and Y. Qian, “SeDS: Secure data sharing strategy for D2D communication in LTEdvanced networks,” IEEE Trans. Veh. Technol., 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,” IEEE Trans. Ind. Informatics, 2019.

[7].W. Wang, P. Xu, and L. T. Yang, “Secure data collection, storage and access in cloud-assisted IoT,” IEEE Cloud Comput., 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,” in Proc. Appl. Cryptogr. Netw. Security, Jun. 2008, vol. LNCS 5037, pp. 111–129.

[9] J. Lai, X. Zhou, R. H. Deng, and Y. Li, “Fully secure cipertext-policy hiding CP-ABE,” in Proc. 6th ACM Symp. Inf. Comput. Commun. Secur., 2011, pp. 24–39.

[10] J. Lai, X. Zhou, R. H. Deng, Y. Li, and K. Chen, “Expressive CP-ABE with partially hidden access structures,” in Proc. 7th ACM Symp. Inf. Comput. Commun. Secur., May 2012, pp. 18–19.

[11] B. Waters, “Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization,” in Proc. 14th Int. Conf. Practice Theory Public Key Cryptography Conf. Public Key Cryptography, Mar. 2011, pp 53–70.