Fuzzy Systems and Soft Computing
ISSN : 1819-4362

ENHANCING SECURITY AND PRIVACY IN CLOUD COMPUTING: ATTRIBUTE-BASED DATA SHARING

#1PERALA ANITHA,
#2POLUKONDA TEJASREE,
#3B.RAMESH, *Assistant Professor,*
Department of Computer Science and Engineering,
SREE CHAITANYA INSTITUTE OF TECHNOLOGICAL SCIENCES, KARIMNAGAR, TS.

ABSTRACT: Cloud-based data sharing is a low-cost and convenient conferencing feature. Because the data is transferred to multiple cloud sites, privacy and data issues arise. A variety of strategies are used to strengthen access control to shared data in order to safeguard new and valuable information. Ciphertext-policy attribute-based encryption (CP-ABE) can improve the security and usability of these approaches. At a time when user privacy is critical, standard CP-ABE is only concerned with keeping data secure.CP-ABE's disguised entrance approach protects your privacy and that of your data. It is worth noting, however, that most contemporary systems contain computational expenses and communication overhead that are not being used efficiently. Furthermore, the majority of these initiatives fail to address the issue of privacy leaks throughout the authority verification process. To address these issues, this paper presents a CP-ABE approach that protects privacy while ensuring that authority verification works properly.

KEYWORDS:*Improving, Security, Privacy, Attribute-Based, Data Sharing, Cloud Computing.*

1. INTRODUCTION

Organizing a conference with content shared via the cloud is straightforward and inexpensive. When individuals submit information to numerous cloud sites, they are concerned about data security and privacy. A range of procedures are implemented to strengthen access control over data sharing in order to protect sensitive and innovative information. Implementing ciphertext-policy attribute-based encryption (CP-ABE) can significantly improve the security and usability of these techniques. Standard CP-ABE is solely concerned with data security, even though user privacy is vital. The CP-ABE system for concealed entrances protects your data and personal information. It's also worth noting that most modern systems exhibit invisible transmission and processing lag. Furthermore, many of these projects fail to address the issue of privacy violations that occur throughout the authorization verification process. To address these difficulties, this study presents a CP-ABE method that ensures correct authority verification while also protecting privacy.

2. LITERATURESURVEY

Ciphertext-PolicyAttribute-BasedEncryption

Only users with particular encryption-related properties can decipher ciphertext. The majority of public key encryption algorithms in use today can protect data for a single user, but they struggle with increasingly complex encrypted access control mechanisms. A ciphertext-policy attribute-based encryption technique uses four core algorithms: setup, encryption, key generation, and decoding. We also include an optional fifth algorithm called Delegate. The Thesetup algorithm just takes into account the implicit security value.

Setup-The Thesetup method simply needs a constant security argument to work. It accepts public parameters (PK) and master keys (MK).

Encrypt -The message M, access structure A, and public factors all work with the encryption approach. By encrypting M and creating ciphertext CT, the technique assures that only users who meet the access structure's requirements can read the message.

Key Generation -A list of properties characterizing the key S is considered when establishing a key, in addition to the master key

MK. The acronym SK stands for the private key result.

Decrypt-The decryption technique requires a ciphertext CT carrying a policy A attain as well as a private key SK indicating a collection of characteristics. Must these

When the access structure is engaged, the algorithm decrypts the encrypted text and sends the message specified as M.

Secret Sharing –To ensure that everyone in the group receives a portion of the coded message, different people might divide and exchange secret information. We call this secret sharing or secret dividing. Individual shares are worthless on their own; several shares, presumably of various types, must be combined in order to replicate the secret.

3. OUTCOMEOFLITERATUREREVIEW

Cloud computing is gaining popularity as a solution to problems with high-performance computers and data storage in both the corporate and academic sectors. Because cloud storage makes it easier for end users to send data to the cloud via the Internet, it is an essential component of cloud computing. Cloud storage has many benefits, but it also has some serious downsides. One key issue that has arisen is the preservation of user privacy and security, especially in the context of public cloud storage. A completely trustworthy administrator usually monitors backup servers that store data for owners. In contrast, public cloud storage systems are frequently maintained and administered by an untrusted third party (the cloud provider).

Because attribute-based encryption, or ABE, gives users direct control over their data and allows for fine-grained access control, it is widely recognized as one of the best approaches for limiting who can access data in public clouds. Numerous ABE approaches have been proposed thus far. They can be classified into two types: ciphertext-policy attribute-based encryption (CP-ABE) and key-policy aspect-based encryption (KP-ABE).

KP-ABE systems associate access structures with decode keys, while ciphertexts are merely annotated with sets of features. Instead, by giving a unique access strategy based on user attributes to each file in CP-ABE systems, data owners can gain greater direct control over their information. For providing access control for public cloud storage, CP-ABE outperforms KP-ABE. The bulk of current CP-ABE systems are managed and keyed by a single authority.

When only one authority exists, there may be a single point of failure in terms of security and speed. It is also important to realize that if the single authority is compromised, the plan will not work as intended. As a result, access control in public cloud storage still seldom employs CP-ABE methods. In terms of security and performance, no matter how many multi-authority CP-ABE solutions exist, they cannot overcome the single point of failure problem. The complete set of attributes is separated into various groups utilizing these multi-authority CP-ABE approaches. Each collection of attributes is overseen by its own authority. Even if an opponent is unable to obtain the private keys for all governing groups, they will be granted greater rights if they successfully breach one or more of them. An adversary could also compromise one or more governance groups to gain the private keys associated with specific properties.

Furthermore, the current standard CP-ABE techniques still fail to address the speed issues caused by a single point of congestion. If there is an incident or failure at a clear authority, it will become increasingly difficult to produce and send private keys for each credit in the attribute subset over which the authority has control. Regardless, the overall system will continue to function regularly. To solve the performance and security challenges that the majority of current systems encounter due to a single point of failure, this paper introduces x, a robust and verifiable threshold multi-authority gain mechanism. When many authorities work together to manage the full set of traits, no single authority has complete control over any one of them. Our scheme's threshold secret sharing allows you to share the secret key with other authorities. This is owing to the fact that schemes require a private key to generate attribute private keys. In some CP-ABE schemes, the secret key replaces the master key. Threshold secret sharing ensures that no more than t authorities are compromised when one of them is unable to access the master key. It also ensures that the system will operate when all regulatory agencies are present. To the best of our knowledge, this is the first article to address the privacy and security concerns related with CP-ABE access techniques for single-point public cloud storage.

4.PROPOSEDSYSTEM

Access control can use attribite-based encryption (ABE) or text-policy attribute-based encryption (CP-ABE) in conjunction with Key Policy attribute-based encryption (KPABE) to protect cloud data privacy. The guidelines for data sharing are solely the responsibility of the data owner. CP-ABE is a simple cryptographic mechanism that can be used to transport sensitive data when using cloud computing. Each user's secret key in CP-ABE is linked to a set of access control attributes. Data is then encrypted using these attributes. For Auser to be able to decrypt the text, this sign must meet the ciphertext access requirements. Key bonding is more challenging in CP-ABE because users' secret keys must come from a recognized key authority. Unfortunately, the majority of CP-ABE systems in use today are incapable of managing features that can occur under any scenario. This study solves a critical bond problem and improves attribute expression to allow for more effective use of weighted-attribute data sharing in the cloud. The upgraded two-party key protocol prevents a key authority or cloud service provider from stealing a user's whole private key. The weighted-attribute method simplifies both the definition of the binary attribute and the establishment of access policies. This minimizes the time required to encrypt data and the costs associated with storing ciphertext.

ADVANTAGESOFPROPOSED SYSTEM

- The recommended PSE technique enables you to search for encrypted data using attributes as well as a secret acceptance policy based on keywords.
- The technique is applicable as long as there are many data owners and recipients.
- Each user in the system is assigned a separate set of attribute values. A third party verifies these values and gives the user a secret key.
- One amazing feature of the PSE system is that once the user obtains the secret key, he can use the private key, which comes in the form of a double door, to further expand the research subject.

5. SYSTEMARCHITECTURE

This device employs facial recognition to allow the user to focus on one of the main emotion categories. Organizations that display empathy can immediately develop a positive reputation, as opposed to typical systems in which the object extraction and detail classification stages function separately. To avoid the back-unfold error, the company's upper limit is methodically adjusted to a catastrophic level; at this point, the estimated likelihood of each incidence can be immediately passed forward. The central key authority (KA) is in charge of configuring both private and public CP-ABE setups. KA allows users to assign, remove, and alter attribute keys without having to do so manually. Furthermore, it offers access permissions to approved individuals based on their attributes. People are captivated and think it to be true. Simply put, its primary goal is to complete its assigned responsibilities within the system while also learning as much as possible about protected materials. Thus, even if you have good intentions, you should never attempt to decipher encrypted data. A cloud service provider (CSP) is a business that provides a platform for data sharing. Its role is to control who has access to external data storage and ensure that they receive reliable information. The CSP is a supplementary semi-trusted key authority that generates unique user keys from the KA and provides or revokes attribute group keys to allowed users based on each attribute. The keys listed above are then used to define specific user access limits. The CSP and KA, like the other approaches, are considered fairly dependable. The organization that wishes to submit data to the CSP in order to save money or time is the data owner. The data owner is largely responsible for creating an attribute-based access policy and encrypting their own data to ensure compliance with the policy before sharing it with others. This allows a company to control who gets access to what information. Because the KA and CSP can only be partially trusted, neither should be able to see the plaintext of the data that will be transferred. As long as the secret keys comply with the encryption data's access policy and are not revoked in any of the valid attribute groups, they should be permitted to distribute them to others.

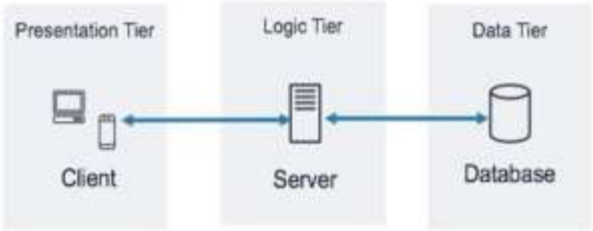

Fig1:SystemDiagram

One innovative feature is the ability to do complex mathematical operations on enormous amounts of data automatically, with each iteration going faster than the preceding one. AI models are iterative, which means that as more data is added, they must alter their predictions based on earlier estimates. It also ensures that evaluations and outcomes are consistent and reproducible. "While many AI methods have been accessible from now onward, indefinitely quite a while, the ability to apply them to a lot of information — over and over and quicker and quicker - is a new turn of events."

6.MODULES

Key Authority: The semitrusted key authority (KA) configures the public and private CP-ABE parameters. KA allows users to assign, remove, and alter attribute keys without having to do so manually. Furthermore, it offers access permissions to approved individuals based on their attributes. Realistic and curious all at same. Simply put, its primary goal is to complete its assigned responsibilities within the system while also learning as much as possible about protected materials. Thus, even if you have good intentions, you should never attempt to decipher encrypted data.

CSP:A cloud service provider is a business that enables data sharing. Its tasks include ensuring that external users have access to data storage and delivering relevant content offerings. Another semi-trusted key authority creates unique user keys and assigns and removes attribute group keys for each attribute to provide fine-grained user access control. This approach, like the others, should be classified as semi-trusted since, like the KA, it is honest and inquiring.

Data Owner : The organization that wishes to submit data to the CSP in order to save money or time is the data owner. Your primary job as a data owner is to set up and manage attribute-based access controls on your own data, which is encrypted before being shared with others.

USER: The "object" is the entity that the data is meant to reach. The user needs to process a collection of attributes that are in line with the access policy of the encrypted data and are not revoked in any of the allowed attribute categories in order to decode the encrypted text and retrieve the data. Both the and the semi-trusted key administrator centers should be able to grant private keys, regardless of whether they can view the cleartext of the data being sent.

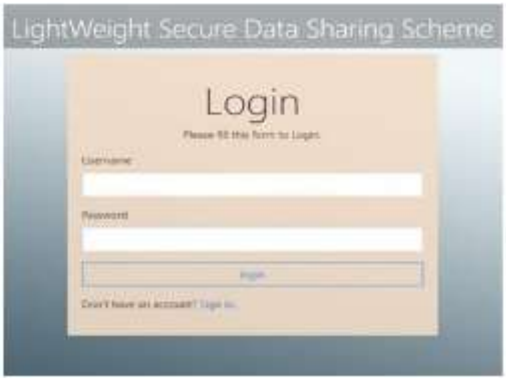
LightWeight Secure Data Sharing Scheme
Login
Please fill this form to Login.
Username
Password
login
Don't have an account? Sign in.

Fig2:LoginPagefor USER

7. RESULT

OUTPUT:-

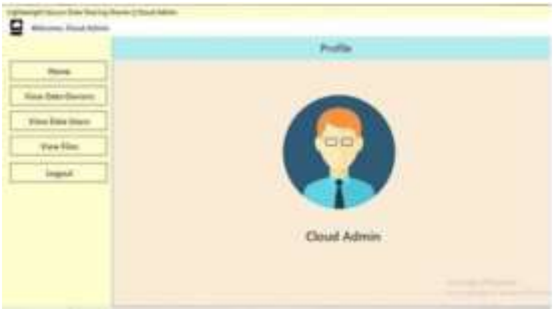

Fig3:CloudAdmin

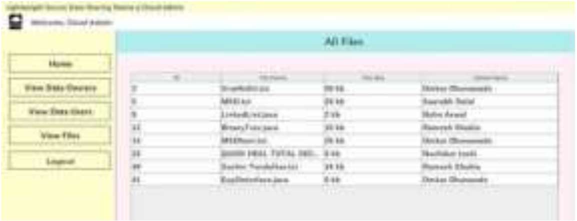

Fig4:AllFiles

8.CONCLUSION

The data sharing framework's capacity to provide granular control over data access is fully used by the attribute-based data sharing strategy that has been proposed. The adoption of a secure two-party computation to create private user keys eliminates the need for key escrow. It makes KA and CSP managers and other malicious users less trustworthy while also improving cloud security for data privacy. It was also suggested that the property's language may be enhanced by using the weighted feature. This function allows you to provide any type of state property, simplifies understanding of the access structure, lowers storage and security costs, and more. Consequently, the data sharing architecture benefits from the suggested method's efficient and secure control over data viewing. The data sharing system is capable of securely handling user data despite its dynamic nature and rapid growth rate. The experimental result graphs conclude with a comparison of the proposed method to the current system. Various data exchange systems are the focus of current research in these areas. Additional data will be gathered and car prices will be forecasted in future studies using advanced methods including genetic algorithms, fuzzy reasoning, and artificial neural networks. Our head of department is a shining example of a good citizen, and the Allfaith hand has acknowledged this. For their unwavering support, I am grateful to everyone—friends, family, and total strangers alike. Also acknowledged is Project, who is the head of the department.

REFERENCES

1. A Vouk, Mladel. “Cloud computing Issues, search 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 Different cloud Storage Architecture for Cloud Supported 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: Springer Verlag, 1998.
5. Zhang, J.Chen, R. Q. Hu, and Y. Qian, “SeDS: Secure data sharing strategy for D2D communicationinLTEadvanced.
6. Li,Z. Yang, and S. Xie, “Computing Resource Trading for Edge-Cloud-assistedInternet of Things,” IEEE Trans. Ind. Informatics, 2020.
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, 2021.