ASSESSMENT ON IMPROVED CLOUD COMPUTING SECURITY AND PRIVACY USING ATTRIBUTE-BASED DATA SHARING TECHNIQUE

[1]G. Vidya Sagar, [2]M. Kanchana, [3]Chegu. Rupa Kalpana, [4]E. Venkateswarlu
[1,2,3]Dept of Computer Science and Engineering, Sree Venkateswara College Of Engineering, Nellore (Dt), Andhra Pradesh, India.
[4]Dept of Electronics and Communication Engineering, Sree Venkateswara College Of Engineering, Nellore (Dt), Andhra Pradesh, India.

ABSTRACT

Cloud computing provides the practical and cost-effective service of data exchange. The privacy of the data contents is also a result when you consider that the information is outsourced to certain cloud servers. In order to safeguard the sensitive and irreplaceable data, many techniques are used to secure access to and control over the shared data. Cipher text-policy attribute-based encryption (CP-ABE) can improve the convenience and security of these methods. Conventional CP-ABE focuses solely on information confidentiality, however today; user privacy security is a major concern. CP-ABE with disguised access coverage guarantees record confidentiality and prevents user privacy from being disclosed as well. Nevertheless, most current systems are inefficient in terms of calculation cost and verbal interchange overhead furthermore, the majority of these efforts give little thought to authority verification or the problem of privacy leakage during the authority verification step. This work presents a privacy-maintaining CP-ABE system with efficient authority verification to address the issues mentioned above. The hidden keys of it also grow in size consistently. Under the decisional n-BDHE problem and decisional linear assumption, the suggested approach achieves selected safety. The results of the computations support the presented scheme's justification.

Keywords: Privacy preserving, ABE, authority verification

1. INTRODUCTION

Using statistics and scientific sources in the commercial company area is possible thanks to cloud technologies. The cloud offers a variety of scalable services that may be used instantly, including online databases, software interfaces, storage, and computer resources, among others. Offerings are available to users via PCs, laptops, and smartphones. Cloud storage offers services for managing and storing remote data. It is also helpful in computing and records analysis, which is simple since it can provide a number of services at once. In terms of information storage, the cloud offers several advantages, including reduced communication and preservation costs, resource savings, enabling remote access, and so on. However, humans may now not be inclined to keep their information in the cloud, even though it offers so many advantages due to the fact of the records confidentiality and privateness problems.The cloud server (cs) may also be trusted, or put another way, if data is uploaded to the cloud, the cloud service issuer may also get and disclose users' private information, and even gain access to and distribute the data unlawfully [1]. Humans have a tendency to encrypt data before uploading it to the cloud in order to guarantee its secrecy. But the statistical method becomes challenging due to the widely used encryption techniques. Abe is the ideal choice to get around this restriction.

Abe was initially put up in 2005 by sahai and waters [2], who guaranteed information secrecy and gave clients fine-grained access to control insurance policies. In cloud computing, it has been widely used as a fantastic method of encrypting the records that are outsourced. When the owner of the record (do) desires to share the contents of the record with other users, Abe increases effectiveness. It enables users to establish a file access policy for encrypted files, allowing users who have that policy to access submitted data.

Customers who do not complete the access form are unable to obtain any information on the contents of the data. For instance, we analyse the ability of a firm to access and change its records. If the CEO wants to distribute a labelled file to the managers of the revenue department, the planning department, and the research and development (r&d) department through the cloud. He or she can then employ an abe plan. He or she encrypts the file first and designates supervisor A as the shape with access rights (sales branch, planning branch, r&d). The encrypted file and entry right are then uploaded by the user into the cs.

Only the managers of the three departments mentioned above have access to the classified file, and even if they cooperate, neither the managers of other departments nor the regular workforce in the three departments mentioned above may do any in-depth analyses of the file. The majority of Abe's plans work flawlessly when exchanging impermeable facts. The do and the customers' right to privacy, however, is not acknowledged in these arrangements. The access coverage is typically sent with ciphertexts for ease of accessing superior data. In certain circumstances, the input form may also bring up sensitive user records. For instance, a patient may choose to share his or her personal health record (phr) with specific doctors and family members, but

Even if the malicious party cannot access the contents of the phr if the victim uses a standard abe scheme to encrypt it, he or she may still be able to obtain certain information about the users, as shown in fig. 1. The access policy mentions "cardiopathy" and "dc hospital," and the malevolent third party may also wager that the subject is experiencing a heart attack and receiving treatment at the dc hospital. Thus, a natural challenge is how to maintain the shared data's security while preserving their privacy.

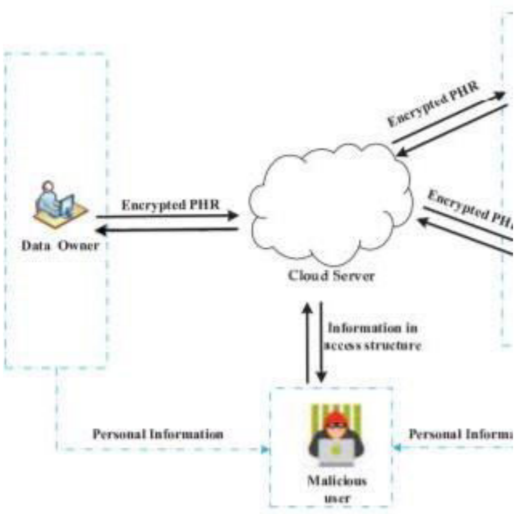


Fig1:Privacy Leakage Model

2. LITERATURE SURVEY

N. Fernando, S. W. Loke, and W. Rahayu are the authors.

Mobile computing is becoming more and more popular, but its inherent issues including resource scarcity, frequent disconnections, and mobility make it difficult to fully realise its promise. By running mobile apps on external resource providers to the mobile device, mobile cloud computing can solve these issues. In this article, we present a thorough overview of the research on mobile cloud computing while highlighting the relevant issues.

S. Abolfazli, Z. Sanaei, E. Ahmed, A. Gani, and R. Buyya are the authors.

Approaches for cloud-based mobile augmentation (CMA) have made significant progress recently in both academia and business. The most advanced mobile augmentation model, known as CMA, uses resource-rich clouds to expand, improve, and optimise mobile devices' computational capabilities in order to run resource-demanding mobile apps. The goal of augmented mobile devices is to store large amounts of data and execute complex calculations with the least amount of space and vulnerability. To address the diverse computing needs of mobile users, researchers make use of a variety of cloud-based computing resources (such as distant clouds and close mobile nodes).

S. Rajalakshmi and R. Kumar

Mobile devices and cloud computing ideas naturally complement one another to provide on-the-go benefits and functionality. One of the most significant subfields of cloud computing is emerging as mobile cloud computing, which is predicted to grow mobile ecosystems. Security concerns will undoubtedly increase as more mobile devices hit the market and develop. The vast increase in the number of devices linked to the Internet will also increase the demand for security.

2. PROPOSED SYSTEM

We offer a CP-ABE scheme with efficient authority verification, which is utilized to assist the user identify whether he or she is authorised or not, motivated by the aforementioned difficulties and based on [24]-[26]. The auxiliary information is utilised to produce the test parameters in Abdalla's verifiable random functions with the auxiliary information [14], which is where the test approach originates. The suggested method can resolve the ciphertexts verification without revealing the users' privacy.

It is suggested to employ a CP-ABE scheme structure with effective authority verification, which ensures data security and user privacy.

We provide an authority identification technique that may let the user confirm if he or she is an authorised one and successfully decrypts in order to save users from having to perform superfluous computations in the decryption procedure.

Constant private key size, regardless of the user's attribute number, is achieved by the suggested technique. It lowers the price of storage and transmission.

3. IMPLEMENTATION

This module requires the data owner to register with the authentication centre, which then verifies and approves the data owner login. Owner of the data may access, encrypt, and upload files using its Mac. Once the file has been uploaded, the authentication centre must provide storage access so that it may be stored in the cloud. After a file has been uploaded to the cloud, the data owner may also remove the file.

Verification Center

Authentication Centre verifies user & owner login in this module and approves registration. The authentication centre provides authorisation (Activate OR Deactivate) and lists all other sub-authentication centres. Every file submitted by the data owner is given access to cloud storage by the authentication centre.

AA1

The AA1 displays and creates all private key requests from users in this module. Additionally, it gives the data owner's uploaded file access to storage.

AA2

The AA2 displays and creates all of the users' requests for public keys in this module. Additionally, it gives the data owner's uploaded file access to storage.

Cloud Server

Obtain all files from the owner of the data and store all files and user information. After confirming the private key and secret key given by the authentication centre, provide files to the end user. Keep track of file transaction information and forward the user's request for a file download to the authentication centre.

End User (Receiver)

In order to download a file from a cloud server, the end user must first register, log in, and receive authorization from the authentication centre. They must then request the private key from AA1 and the secret key from AA2 from each of the two authentication authorities.

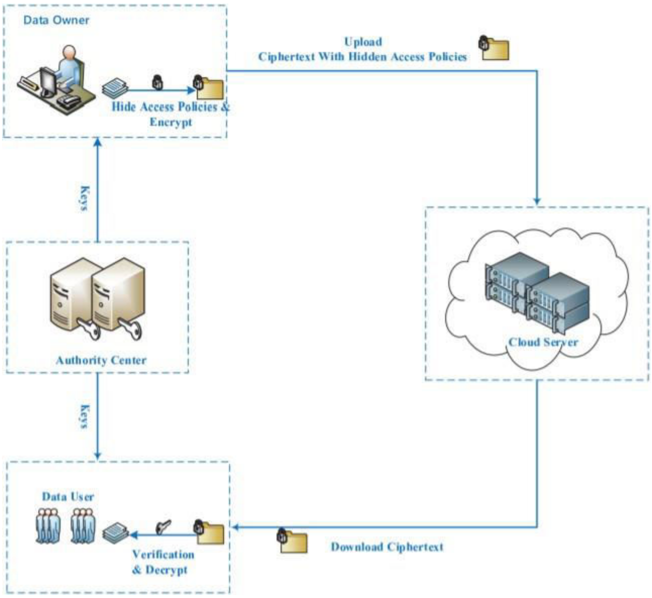
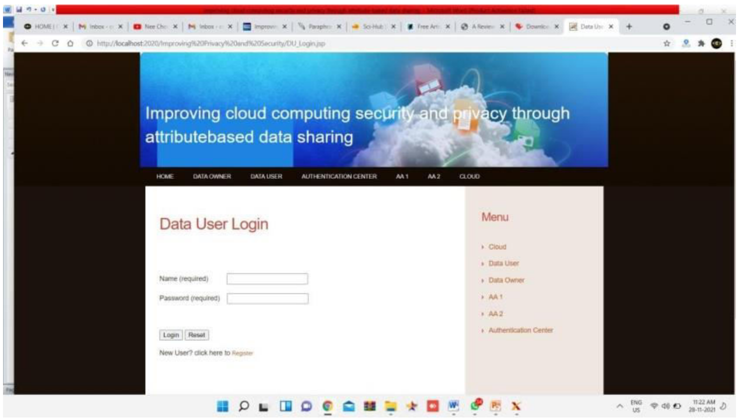


Fig2: System Model

4. RESULTS AND DISCUSION



Improving cloud computing security and privacy through attributebased data sharing

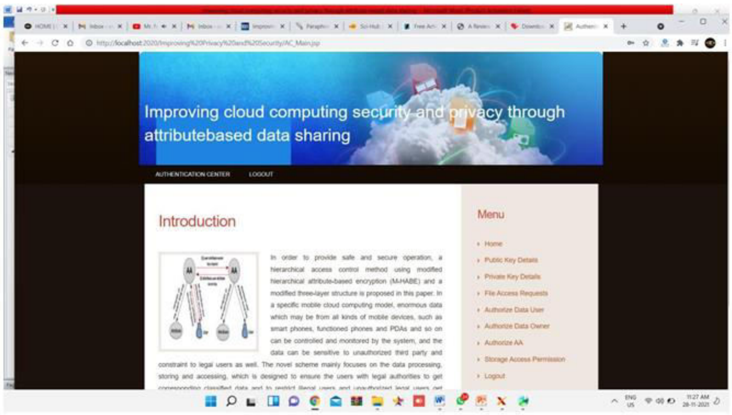
Data User Login

Name (required)

Password (required)

New User? click here to Register

Fig4.1Data userLogin form

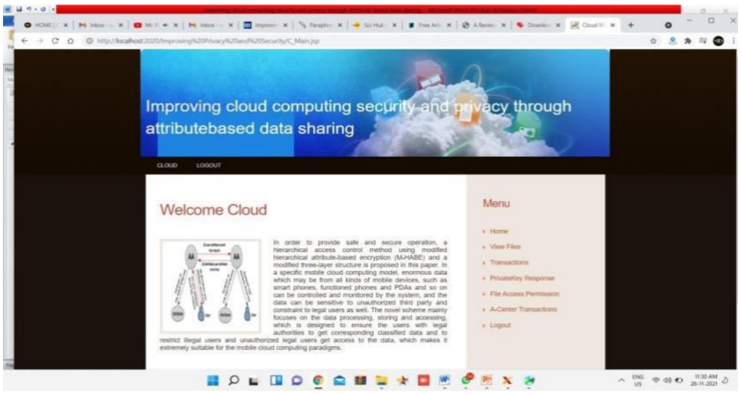


Improving cloud computing security and privacy through attributebased data sharing

Introduction

In order to provide safe and secure operation, a hierarchical access control method using modified hierarchical attribute-based encryption (M-HABE) and a modified three-layer structure is proposed in this paper. In a specific mobile cloud computing model, enormous data which may be from all kinds of mobile devices, such as smart phones, functioned phones and PDAs and so on can be controlled and monitored by the system, and the data can be sensitive to unauthorized third party and constraint to legal users as well. The novel scheme mainly focuses on the data processing, storing and accessing, which is designed to ensure the users with legal authorities to get corresponding classified data and to restrict illegal users and unauthorized legal users get

Fig 4.2 Authority Home Page



Improving cloud computing security and privacy through attributebased data sharing

Welcome Cloud

In order to provide safe and secure operation, a hierarchical access control method using modified hierarchical attribute-based encryption (M-HABE) and a modified three-layer structure is proposed in this paper. In a specific mobile cloud computing model, enormous data which may be from all kinds of mobile devices, such as smart phones, functioned phones and PDAs and so on can be controlled and monitored by the system, and the data can be sensitive to unauthorized third party and constraint to legal users as well. The novel scheme mainly focuses on the data processing, storing and accessing, which is designed to ensure the users with legal authorities to get corresponding classified data and to restrict illegal users and unauthorized legal users get access to the data, which makes it extremely suitable for the mobile cloud computing paradigms.

Fig 4.3 Cloud Main Page

CONCLUSION

In the popular model, we suggested a CP-ABE strategy for maintaining privacy. The newly proposed technique has numerous advantages over the existing ones, including stable dimension personal keys and succinct ciphertexts. Additionally, just 4 pairing calculations are required for decryption. In a top order group, the suggested approach ensures selected safety and anonymity. We show that the safety of the suggested scheme is reduced in the widely used model to the decisional n-BDHE and the DL assumptions. The proposed approach also aids in official verification while maintaining privacy. The additional technique, however, relies on a weak safety model and only supports "AND" coverage. The construction of a strong, impervious HP-CP-ABE scheme with wider flexible access coverage will be the subject of future activities.

REFERENCES

1. P.P.Kumar, P.S.Kumar, and P.J.Alphonse, “Attribute based encryption in cloud computing: Asurvey, gap analysis, and future directions,” J. Netw. Comput. Appl., vol.108, pp.37–52, 2018.
2. A.Sahai and B.Waters,“ Fuzzy identity- based encryption,” in Proc. 24th Annu. Int. Conf. Theory Applications Cryptographic Techn., May 2005, vol. LNCS 3494, 2015, pp. 457–473.
3. J. Li, H. Wang, Y. Zhang, and J. Shen, “Ciphertext-policy attribute-based encryption with hidden access policy and testing,” KSII Trans. Internet Inf. Syst., vol. 10, no. 7, pp. 3339–3352, Jul. 2016.
4. H. Cui, R. H. Deng, G. Wu, and J. Lai, “An efficient and expressive Ciphertext-policy attribute-based encryption scheme with partially hidden access structures,” in Proc. 10th Int. Conf. Prov. Secur., Nov. 2016, pp. 19–38.
5. F. Khan, H. Li, L. Zhang, and J. Shen, “An expressive hidden access policy CP-ABE,” in Proc. IEEE 2nd Int. Conf. Data Sci. Cyberspace, Jun. 2017, pp. 26–29.
6. Y. Zhang, Z. Dong, and R. H. Deng, “Security and privacy in smart health: Efficient policy-hiding attribute-based access control,” IEEE Int. Things J., vol. 5, no. 3, pp. 2130–2145, Jun. 2018.
7. 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.
8. B. Waters, “Ciphertext-policy attributebased 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.
9. Y. S. Rao and R. Dutta, “Recipient anonymous ciphertext-policy attribute based encryption,” in Proc. 9th Int. Conf. Inf. Sys. Secur., Dec. 2013, pp. 329–344.
10. L. Zhang, Q. Wu, Y. Mu, and J. Zhang, “Privacy-preserving and secure sharing of PHR in the cloud,” J. Med. Syst., vol. 40, pp. 1–13, 2016.
11. M. Abdalla, D. Catalano, and D. Fiore,“Verifiable random functions: Relations to identity-based key encapsulation and new constructions,” J. Cryptol., vol. 27, pp. 544–593, 2014.