An Effective Attribute Access Control Scheme for Mobile Cloud Computing using Double Key

Miss. B.J. Jawanjal
SGBAU, Amravati
India.

Dr. Prof. S.S.Sherekar
SGBAU, Amravati
India

Dr. V. M. Thakare
SGBAU, Amravati
India.

ABSTRACT

Access control is a key mechanism to secure outsourced data in mobile clouds. With the popularity of cloud computing, mobile devices can store or retrieve personal data from anywhere at any time.This paper focused on analysis of five different techniques Flexible Access Control With Outsourceable Revocation (FACOR),A lightweight data-sharing scheme (LDSS), Modified Hierarchical Attribute-Based Encryption (M-HABE),Constant-size Ciphertext Policy Comparative Attribute-Based Encryption (CCP-CABE), Cloudlets.These method contain some issue and drawbacks .To overcome these issue,this paper has proposed An Effective Attribute Access control Scheme for mobile Cloud Computing using Double Key.By security analysis and performance evaluation, the proposed scheme is proved to besecure as well as efficient in mobile cloud computing.

Keywords—FACOR, M-HABE, CCP-CABE.MCC.

I) INTRODUCTION

Cloud computing is a promising model to provide unlimited computation and storage capacity to its users, anytime from anywhere. Cloud computing systems benefit enterprises by providing scalable and durable resources [1]. In addition, it reduces the total cost of ownership by transforming the business from capital expenses to operational expenses model Cloud computing is an Internet-based computing pattern through which shared resources are provided to devices on demand [2]. It's an emerging but promising paradigm to integrating mobile devices into cloud computing, and the integration performs in the cloud based hierarchical multi-user data-shared environment [3]. With integrating into cloud computing, security issues such as data confidentiality and user authority may arise in the mobile cloud computing system. Cloud computing provides a scalable, location-independent and high-performance solution by delegating computation tasks and storage into the resource-rich clouds [4]. However, the computational overhead of encryption and decryption grow withthe complexity of the access policy. Thus, maintaining data security as well as efficiency of data processing in MCC are important and challenging issues[5].

This paper discuss five scheme for the data access in mobile cloud computing such as Flexible Access Control With Outsourceable Revocation (FACOR),A lightweight data-sharing scheme (LDSS), Modified Hierarchical Attribute-Based Encryption (M-HABE), Constant-size Ciphertext Policy Comparative Attribute-Based Encryption (CCP-CABE), Cloudlets.

But these method also have some problem so to overcome that An Effective Attribute Access control Scheme for mobile Cloud Computing using Double Key this scheme is proposed in this paper.

II) BACKGROUND

In the mobile cloud computing attribute access control schemes are used. The Flexible Access Control With Outsourceable Revocation (FACOR) scheme applies the attribute- based encryption to enable flexible access control on outsourced data, and allows mobile users to outsource the time-consuming encryption and decryption computations to proxies, with only

requiring attributes authorization to be fully trusted[1].Lightweight data sharing scheme (LDSS) for mobile cloud computing adopts CP-ABE, an access control technology used in normal cloud environment, but changes the structure of access control tree to make it suitable for mobile cloud environments. LDSS moves a large portion of the computational intensive access control tree transformation in CP-ABE from mobile devices to external proxy servers[2].To provide safe and secure operation, a hierarchical access control method using modified hierarchical attribute-based encryption (M-HABE) is used with modified three-layer structure [3].A new efficient framework named Constant-size Ciphertext Policy Comparative Attribute-Based Encryption (CCP-CABE) with the support of negative attributes and wildcards. It embeds the comparable attribute ranges of all the attributes into the user's key and incorporates the attribute constraints of all the attributes into one piece of ciphertext during the encryption process[4].In the cloudlets middle layer sitting between mobile devices and their cloud infrastructure. This middle layer is composed of cloudlets which are deployed by cloud services providers, such as wireless network access points (APs) to improve the performance of mobile cloud service stand be different from traditional mobile operator mode [5].

This paper introduces five data access scheme in MCCthese are Flexible Access Control with Outsourceable Revocation (FACOR),A lightweight data-sharing scheme (LDSS), Modified Hierarchical Attribute-Based Encryption (M-HABE), Constant-size Ciphertext Policy Comparative Attribute-Based Encryption (CCP-CABE), Cloudlets.

The paper is organised as follows:

Section I Introduction. **Section II** discusses Background. **Section III** discusses previous work. **Section IV** discusses existing methodologies. **Section V** discusses attributes and parameters and how these are affected on mobile cloud computing.**Section VI** proposed method and outcome result possible.

Section VIII Conclude this paper.

III) PREVIOUS WORK DONE

In research literature, many data access control models have been studied to improve the performance and efficientstore/retrieve of personal data.ZHOU

Shungan1 et al(2016) [1]has proposed flexible access control with outsourceable revocation (FACOR) for mobile clouds schemeto achieves data security against collusion attacks and unauthorized accesses from revoked users.

Ruixuan Li et al(2014)[2] has proposed methodologylightweight data sharing scheme (LDSS) for mobile cloud computing. LDSS can effectively reduce the overhead on the mobile device side when users are sharing data in mobile cloud environments.

Hong Wen et al (2014) [3] has proposedmodified hierarchical attribute-based encryption (M-HABE) This 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.

Zhijie Wanget al (2015) [4] has proposedConstant-size Ciphertext Policy Comparative Attribute-Based Encryption (CCP-CABE)achieves the efficiency because it generates constant-size keys and ciphertext regardless of the number of involved attributes, and it also keeps the computation cost constant on lightweight mobile devices.

TU Shanshanet al (2015) [5] has proposedcloudlets scheme which introduces a middle layer sitting between mobile devices and their cloud infrastructure. This middle layer is composed of cloudlets which are deployed by cloud services providers, such as wireless network access points (APs), to improve the performance of mobile cloud service.

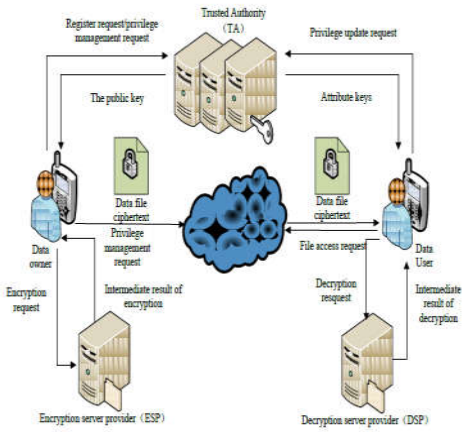
IV) EXISTING METHODOLOGIES

For secure data access in mobile cloud computing Flexible Access Control With Outsourceable Revocation (FACOR),A lightweight data-sharing scheme (LDSS), Modified Hierarchical Attribute-Based Encryption (M-HABE), Constant-size Cipher text Policy Comparative Attribute-Based Encryption (CCP-CABE), Cloudlets these scheme are used.

A] Flexible Access Control With Outsourceable Revocation (FACOR):

The FACOR schemeapplies the attribute based encryption to enable flexible access control on outsourced data, and allows mobile users to outsource the time-consuming encryption and decryption computations to proxies with only requiring attributes authorization to be fully trusted. The security analysis shows that FACOR scheme achieves data security against collusion attacks and unauthorized accesses from revoked users. Both theoretical and experimental results confirm that theproposed scheme greatly reliefs the mobile devices from heavy encryption and decryption computations as well as the complicated revocation of access rights in mobile clouds [1].

B] A lightweight data-sharing scheme (LDSS):



Figur

e1.LDSS framework

As shown in Fig. 1 a DO sends data to the cloud data has to be encrypted before it is uploaded. The DO defines access control policy in the form of access control tree on data files to assign which attributes a DU should obtain if wants to access a certain data file. In LDSS, data files are all encrypted with the symmetric encryption mechanism, and the symmetric key for data encryption is also encrypted using attribute based encryption (ABE).The access control policy is embedded in the ciphertext of the symmetric key. Only a DU who obtains attribute keys that satisfy the access control policy can decrypt the ciphertext and retrieve the symmetric key encryption service provider (ESP) and decryption service provider (DSP) are used. Both the ESP and DSP are also semi-trusted. Then it modify the traditional CP-ABE algorithm and design an LDSS-CP-ABE algorithm to ensure the data privacy when outsourcing computational tasks to ESP and DSP [2].

C]Modified Hierarchical Attribute-Based Encryption (M-HABE):

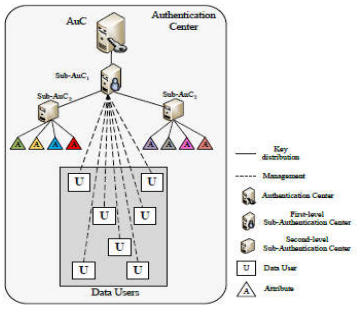


Figure 2.M-HABE model

Modified Hierarchical Attribute-Based Encryption (MHABE).As the Figure 2 shows, the proposal consists of an authentication centre (AuC), Sub-AuCs, and application users. The AuC is responsible for generating and publishing system parameter and the system master key; Sub-AuCs can be divided into first-level Sub-AuC(Sub-AuCi) and other Sub- AuCs, among which the AuC just need to be in charge of users and create their private keys, while other Sub-AuCs take charge of users attributes and create their secret identity keys and secret attribute keys for users. AuC, Sub- AuCs, and users attributes, especially, the ID of each user contains an integer for describing the

privilege level of the user. Additionally, data users also own a set of attributes while other internal parties[3].

D] Constant-size Cipher text Policy Comparative Attribute-Based Encryption (CCP-CABE):

Constant-size Ciphertext Policy Comparative Attribute-Based Encryption (CCP-CABE)The CCP-CABE framework, as shown in Figure 3 consists of a central trust authority (TA) a trusted encryption service provider (ESP), a cloud provider, data owners and data users. The Trust Authority issues public and private keys to data users through secure channelsand publishes global parameters. The trusted ESP has enormous computational power. If a data owner is constrainedby computational resource

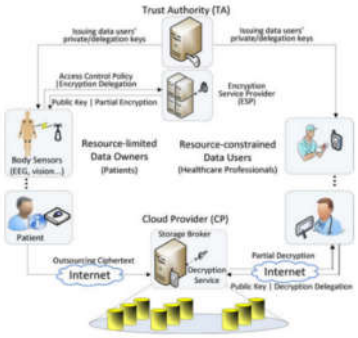


Figure3.The CCP-CABE framework

the ESP can perform part of data encryption for the data owner by generating the partiallyencrypted header e HP based on the data owner's access control policy regarding attribute constraints, such that thedata owner can perform further encryption requiring minimum computational power[4].

E] Cloudlets scheme:

Cloudletintroduces a middle layer sitting between mobile devices and their cloud infrastructure. This middle layer is composed of cloudlets which are deployed by cloud services providers, such as wireless network access points (APs), to improve the performance of mobile cloud service stand to be different from traditional mobile operator mode.Every mobile device has its assignedVMs in cloud for computing and storage purposes. VMs are able to communicate with other VMs as well as cloudlets. Access cloudlet is a kind of VMs that is hosted by a resourceful machine placed next to an access point or a cellular base station. And access cloudlet holds the ancillary service for accessing the cloud [5].

V) ANALYSIS AND DISCUSSION

The FACOR scheme provides an outsourceable revocation mechanism for mobile users to drastically reduce users' computations in revocation. FACOR can provide forward secrecy and collusion resistance. Since it is a more efficient,secure and flexible access control solution FACOR system can be suitable for MCC[1].

Traditional ABE is not suitable for mobile cloud because it is computationally intensive and mobile devices only have limited resourcesLDSS to address this issue. It introduces a novel LDSS-CP-ABE algorithm to migrate major computation overhead from mobile devices onto proxy servers, thus it can solve the secure data sharing problem in mobile cloud. LDSS can ensure data privacy in mobile cloud and reduce the overhead on users' side in mobile cloud[2].

TheM-HABE scheme can be more adaptive for mobile cloud computing environment to process, store and access the enormous data and files. The scheme not only accomplishes the hierarchical access control of mobile sensing data in the mobile cloud computing model but also protects the data from being obtained by an untrusted third party[3].

CCP-CABE kept the computational overhead constant for the data owners and data users regardless of the number of involved attributes by encrypting and decrypting over all attributes in a batch-processing manner. Moreover, it kept the communication overhead small and constant regardless of the number of attributes [4].

Cloudlets are deployed next to Wi-Fi APs and serve as a localized service point at a mobile

device's close proximity to improve the performance of mobile cloud access services in terms of response time [5].

Scheme	Advantages	Disadvantages
Flexible Access Control With Outsourceable Revocation (FACOR)	Efficient Correctness.	Decryption Proxy (DP) is most time most time-consuming operations
A lightweight data-sharing scheme (LDSS)	LDSS is provably secure, and is demonstrated to be more efficient and scalable	It has bring high revocation cost.
Modified Hierarchical Attribute-Based Encryption (M-HABE)	Adaptive scheme for mobile cloud computing	The information may be stolen by third parties.
Constant-size Ciphertext Policy Comparative Attribute-Based Encryption (CCP-CABE)	CCP-CABE achieves the efficiency because it generates constant-size keys.	Does not keep computation cost constant on high weight mobile devices
Cloudlets	Achieve fine-grained access control and attribute revocation for mobile cloud environment	The speed of mobile devices can be increase.

TABLE 1: Comparisons between different Schemes

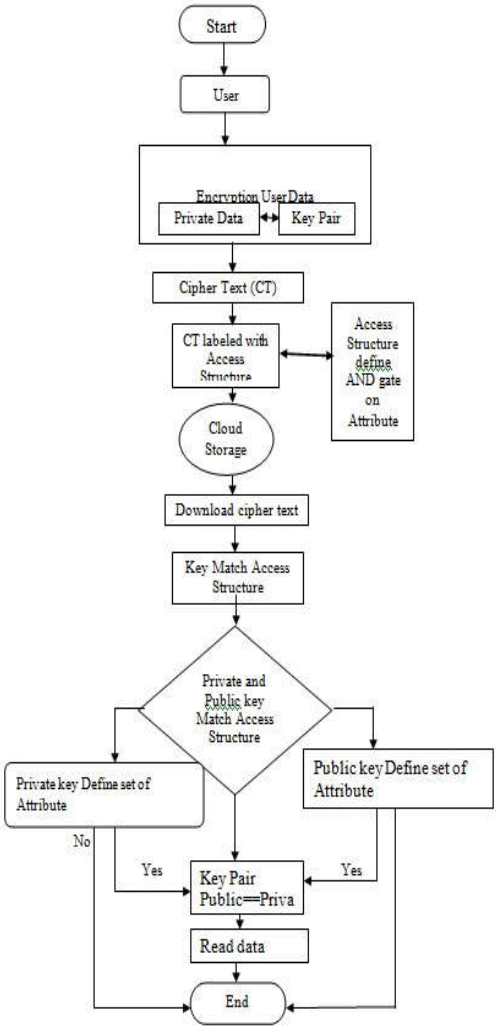
PROPOSED METHODOLOGY

An Effective Attribute Access control Scheme for mobile Cloud Computing using Double Key

This proposed scheme is an efficient and adoptive for the attribute access control in mobile cloud computing.

In the proposed method double key pairing is used. Public key and Private key is used. If the public and private key are match with each other equally then the users data is encrypted or decrypted. AND gate attribute access structure is used for attribute access.

Flowchart



VII) OUTCOME AND POSSIBLE RESULT

By security analysis and performance evaluation, the proposed scheme is proved to be secure as well as efficient for the access data in mobile cloud computing

VIII) CONCLUSION

This paper focused on the study of various such as scheme Flexible Access Control With Outsourceable Revocation (FACOR),A lightweight data-sharing scheme (LDSS), Modified Hierarchical Attribute-Based Encryption (M-HABE), Constant-size Ciphertext Policy Comparative Attribute-Based Encryption (CCP-CABE), Cloudlets. The proposed scheme is proved to be efficient for attribute access with double key for high end security.

IX) FUTURE SCOPE

From observation, the scope is planned to be studied in future work that proposed scheme can be used in any high end data access and security system.

REFERENCES

[1.] Cheng H, Rong C, Hwang K, et al. Secure big data storage and sharing scheme for cloud tenants [J]. China Communications, 2015, 12(6).

[2.] Adam Skillen and Mohammad Mannan. On Implementing Deniable Storage Encryption for Mobile Devices. the 20th Annual Network and Distributed System Security Symposium (NDSS), Feb. 2013 S. Abolfazli, Z. Sanaei, E. Ahmed, A. Gani, and R. Buyya, “Cloudbased

[3.] Y. Zhu, D.Ma, C.-J.Hu, and D. Huang, “How to use attribute-based encryption to implement role-based access control in the cloud,” in Proc. Int.Workshop Security Cloud Computer., 2013.

[4.] Prakash, M. Prateek, and I. Singh, ``Data encryption and decryption algorithms using key rotations for data security in cloud system," inProc. Int. Conf. Signal Propag. Computer. Technol. (ICSPCT), Jul. 2014.

[5] ZHOU Xuejun, GAO Wei, CAO Guohong, et al.An Incentive Framework for Cellular Traffic Offloading[J], IEEE Trans. Mobile Computing, 2014.