

Enhanced Versatile Secured Data Accesses Control for Cloud in Mobile Computing

Professor & Principal Dr.P.Chitti Babu, Assistant Professor, V.Nirmala, Ponna.jyothiswara

MCA Department & APGCCS, Rajampet, YSR Kadapa, India

drpcbbit@gmail.com, samramana44@gmail.com, rdjyothiswaraponna96@gmail.com

Abstract – In present days handling the data (storing and sharing) is most difficult. Providing the security is difficult task. So the data will be access by any one. Then the data owners are facing the many problems. And also the data owners and data users can be access and share the data is very difficult. Now a days the smart phones are used for all uses. So here they are used mobile cloud computing. By using this technology the data will be sharing and storing is simple. And also mobile networks are very faster and it will connect any ware and any time. There is no restriction on the network issues for mobile cloud. The mobile networks are available 4G network and it will be updated in day by day. So it is user friendly work, With explosive growth of mobile devices including smart phones, PDAs, and tablet computers and the applications installed in them, the mobile-Internet will maintain the development growth trend as 4G communication network is extensively promoted to our lives. It exists mobile cloud computing is provide the data is secure and safe. The flaws of data storing and data computing in mobile-Internet applications can be overcome by mobile cloud computing while the new paradigm can also accomplish cloud based multi-user data sharing, end geographical service limitation, and process real-time tasks efficiently at the same time.

Keywords – Encryption, Decryption, Priority.

I. INTRODUCTION

Security Issues for Cloud Computing

As long as the data is transmitted to cloud, it is utilizing cloud services like IaaS or DaaS, security challenges of which must be overcome since then. There are plenty of research results about cloud security, in conclusion, a secure cloud should at least satisfy 4 basic urges of consumers [12], say availability, confidentiality, data integrity, control.

1. Availability

Cloud providers should offer services that consumers could get and use at any places and any time. There are mainly two methods to enhance availability in cloud, which are virtualization and redundancy. Currently, cloud technology is mainly based virtual machine [13], since cloud providers can provide separated virtualized memory, virtualized storage, and virtualized CPU cycles, so that users can always get them.

Large cloud provider enterprises build data centers in multiple regions all over the world to protect files they store from failing in one particular region and spreading to other regions. For example, Google set three replications for each object stored in it [14], all these redundancy strategies are enhancing the availability for consumers to get whatever they want at any time and any place. Besides these concerns on availability, don't trust HTTP protocol too much as it is a stateless protocol for attackers, which

may cause unauthorized access to the management interface of cloud infrastructures [13].

2. Confidentiality

Confidentiality has been a huge barrier for cloud providers to popularize cloud to consumers since it comes out. It is understandable that consumers cannot trust the cloud services, after all, nobody knows what will happen to the files, especially important and confidential ones, once they are placed in cloud vendors' hosts.

There basically exist two common approaches in current cloud infrastructures, say physical isolation and encryption. Physical isolation specifically means virtual physical isolation as cloud services are transmitted via public networks. In this context, virtual physical isolation [15], [18] are using VPN and firewalls to secure database [12]. Encrypting vital and confidential data before placing it in cloud infrastructures is another method to enhance confidentiality of cloud. But do not count on that approach too much because novel methods of breaking cryptographic algorithms are discovered [13].

3. Data integrity

Data integrity ensures consumers that their storing data is not modified by others or collapsing owing to system failure. An easy method is making plenty of copies of consumers' files, which is a good but highly-cost way. Besides the method, a "cloud security capture application" [19] could be in use to show consumers when and where their data was modified or transmitted.

4. Control

It is a sophisticated work to control a cloud system, a controlling work mainly includes deciding what resource could be utilized in what occasions.

In order to own a secure control system, cloud vendors may need a specialized operating system. Virtualization based considered as the most popular definition of mobile cloud computing [4].

5. Security Challenges Descriptions

Availability Cloud providers are supposed to guarantee to consumers that they can get and use their data at any places and any time.

Confidentiality Consumers' data should be kept secret in cloud systems.

Data Integrity The data stored in cloud systems need a mechanism to ensure their data not lost or modified by unauthorized users. **Control** A secure control system distributes appropriate resources to be utilized in different occasions.

Table 1 Security Challenges

Security Challenges	Descriptions
Availability	Cloud providers are supposed to guarantee to consumers that they can get and use their data at any places and any time.
Confidentiality	Consumers' data should be kept secret in cloud systems.
Data Integrity	The data stored in cloud systems need a mechanism to ensure their data not lost or modified by unauthorized users.
Control	A secure control system distributes appropriate resources to be utilized in different occasions.

III. SYSTEM MODEL

A modified hierarchical attribute-based encryption (M-HABE) access control method applied in mobile cloud computing is proposed in this paper, which changes a proposed scheme called hierarchical attribute-based encryption HABE [8], M-HABE combines the hierarchical identity-based encryption [9] and the ciphertext-policy attribute-based encryption (CP-ABE) [10] to meet the conditions described above. Two major branches of ABE system are key-policy ABE (KP-ABE) [24] and ciphertext-policy ABE (CP-ABE) [10], the later one is utilized in many paradigms including this proposed paper. The access structure mentioned above in CP-ABE is placed in ciphertext, which means that the data sender can be so initiative that he/she can determine the receiver. Users are described by a set of attributes in CP-ABE, only when the attribute set satisfies the access structure can the user obtain the ciphertext

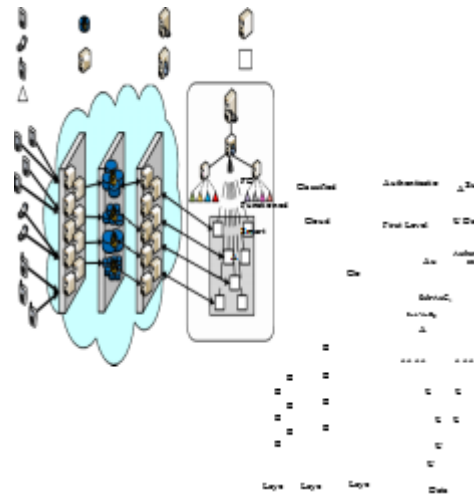


Fig. 3. General structure of M-HABE access control method for mobile cloud computing.

IV. RELATEDWORK

Access control issue deals with providing access to authorized users and preventing unauthorized users to access data. Attaching a list of authorized users to each data is the simplest solution to achieve access control. However, this solution is difficult in the scenario with a large number of users, such as the application mentioned above within the environment of cloud. Public cryptographic scheme is another solution, in which a public/secret key pair is given to each user and encrypt each message with public key of the authorized user, so that only the specific users are able to decrypt it. In the proposed scenario, users with different privilege levels have different rights to access the part of sensing data coming from the mobile devices. Therefore, one same data has to be encrypted into ciphertext once, which ought to be able to be decrypted multiple times by different authorized users.

1. Modified Hierarchical Attribute-Based Encryption (M-HABE)

We take a weather application on mobile devices as a scenario. As the mobile cloud computing defines [1] [22], there would be so much sensing data from the mobile devices inbursting into the cloud infrastructures to process and store the data. The sensing data belonging to a mobile cloud computing model can contain information of different hierarchies such as temperature and humanity numbers, the weather changing trend, information update frequency and so on. It is important that the users with lower privilege cannot get access to some information that the higher privilege user can get to, while the higher authority user can get access to all the data that is obtainable for users in lower hierarchical position since different users of the mobile cloud computing system

constitute a hierarchical authority system. At the same, all the information should be encrypted appropriately since the data is not supposed to be available for a third party which doesn't belong to the system. So a secure and hierarchical access control method should be proposed to apply in the mobile cloud computing system. An example of the access control list in such circumstance is shown in Table II. As the list suggests, the access structure should meet the following requirements:

- One encrypted data can be received by several users.
- Not only precise level descriptions, but users attributes are there in the access structure. For example, weather vertical comparison information can be attainable for users of level 4, some users with working numbers 290381, 209378, 98302, . . . , and users doing jobs such as meteorology researcher, journalist and so on, among which the users with specific numbers and users doing specific jobs are described as the attributes while the other one is described as an accurate privilege level.
- The structure of encryption keys should performs just as the hierarchical structure of the mobile cloud computing users. For instance, the way the authentication center within the mobile cloud computing application company distributes the keys to users should just be as how the users privileges show.

In order to accomplish these requirements, a proposed access control method should contain the following features:

- One ciphertext can be decrypted by several keys.
- Both precise level description and user attribute should be supported in the access structure of the method.
- The keys in the authentication center ought to have the same hierarchical structure just as the structure of users privilege levels.

Information Type	Access Structure
Temperature Value	All users
Weather Horizontal Comparison	Users of level 2, users in the cooperative company {××meteorology company, . . . }
Update Frequency	Users of level 3, users with titles {professor, doctor, major journalist, . . . }
Weather Vertical Comparison	Users of level 4, users with designated work numbers {290381, 209378, 98302, . . . }, users doing jobs of {meteorology researcher, journalist, . . . }
Location Accuracy	Users of level 5, users in specific locations

Table 2 List of The Access Structure in a Mobile Cloud Computing model

Information Type	Access Structure
Temperature Value	All users
Weather Horizontal Comparison	Users of level 2, users in the cooperative company {××meteorology company, . . . }
Update Frequency	Users of level 3, users with titles {professor, doctor, major journalist, . . . }
Weather Vertical Comparison	Users of level 4, users with designated work numbers {290381, 209378, 98302, . . . }, users doing jobs of {meteorology researcher, journalist, . . . }
Location Accuracy	Users of level 5, users in specific locations

Key Description

Public key encryption is utilized in the proposed system, the related keys are summarized in Table III.

Root key MK0 possessed by AuC is used to create MK* for Sub-AuC1.

Key Name Meaning

- MK0 Root key, owned by AuC
- MK* Master key, owned by Sub-AuC
- PK* Public key, owned by Sub-AuC1
- PKi Public key, owned by Sub-AuCs
- MKi Master key, owned by Sub-AuCs
- PKu Public key, owned by users
- SKu Secret key, owned by users
- SKi,u Secret identity key, owned by users
- SKi,u,a Secret attribute key, owned by users
- PKu Public key, owned by attributes

Table -III : List of Major Keys in Habe

Key Name	Meaning
MK ₀	Root key, owned by AuC
MK*	Master key, owned by Sub-AuC
PK*	Public key, owned by Sub-AuC1
PK _i	Public key, owned by Sub-AuCs
MK _i	Master key, owned by Sub-AuCs
PK _u	Public key, owned by users
SK _u	Secret key, owned by users
SK _{i,u}	Secret identity key, owned by users
SK _{i,u,a}	Secret attribute key, owned by users
PK _u	Public key, owned by attributes

2. Proposed Algorithms

Algorithm 1 Dual Algorithm

Input: {p†k : k ∈ B}

Output: {pLk : k ∈ B}

- 1: Initiate λ₀ = 0, -1 = -1, t = 0, {ptk : k ∈ B} = {p†k : k ∈ B}
- 2: while If ∃ i such that |λ_ti - λ_{t-1}i| > do
- 3: For all k = m, . . . , K - 1, update
 $\lambda_{t+1} k = \max \{ \lambda_{tk} + 1 \sqrt{t + 1} (ptk - ptk+1), 0 \}$. (26)
- 4: Calculate pt+1 = argmin_{0 ≤ p ≤ pmax} L(p, λ_{t+1}).
- 5: Set t = t + 1.

6: end while

7: Set $\lambda L = \lambda t, pL = pt$.

The dual algorithm fully takes advantage of the separable structure of the objective function in problem(20); it is easy to implement, since the optimal solution of the Lagrangian can be obtained easily; it provides an upperbound of problem (20); it is possible to return the global solution of problem (20) with a certificate (if the returned solution is feasible); if not, it returns a good approximate solution, which can be used as an initial point for local.

Algorithm 2 Dynamic Algorithm

Input: $\{pL_k: k \in B\}$

Output: $\{pD_k: k \in B\}$

1: Initiate $\{pD_k: k \in B\} = \{pL_k: k \in B\}$

2: while $\{pD_k: k \in B\}$ is infeasible do

3: Find the first and shortest infeasible sub-sequence $\{pD_i, pD_{i+1}, \dots, pD_j\}$ of $\{pD_k, k \in B\}$.

4: Set $pD_k = \arg \max_{0 \leq p \leq p_{maxj}} t = ift(p), \forall k = i, \dots, j$.

5: end while

2) Dynamic Algorithm: Now we deal with the case where $\{pL_k: k \in B\}$ is not feasible. We denote a subsequence of $\{p_k: k \in B\}$, say $\{p_i, p_{i+1}, \dots, p_j\}$, as an infeasible sub-sequence, if $p_i \geq p_{i+1} \geq \dots \geq p_j$ and $p_i > p_j$.

V. COMPARITIVE RESULTS



Name	Filename	Keyword	Description	Count	Ratio	Date
...
...
...

Fig.1 User Search Keys.



Name	Filename	Keyword	Description	Count	Ratio	Date
...
...
...
...

Fig.2 User Search History

REFERENCES

- [1]. N. Fernando, S. W. Loke, and W. Rahayu, "Mobile cloud computing: A survey," *Future Generation Computer Systems*, vol. 29, no. 1, pp. 84–106, 2013.
- [2]. S. Abolfazli, Z. Sanaei, E. Ahmed, A. Gani, and R. Buyya, "Cloudbased augmentation for mobile devices: motivation, taxonomies, and open challenges," *Communications Surveys & Tutorials*, IEEE, vol. 16, no. 1, pp. 337–368, 2014.
- [3]. R. Kumar and S. Rajalakshmi, "Mobile cloud computing: Standard approach to protecting and securing of mobile cloud ecosystems," in *Computer Sciences and Applications (CSA), 2013 International Conference on*. IEEE, 2013, pp. 663–669.
- [4]. J. Carolan, S. Gaede, J. Baty, G. Brunette, A. Licht, J. Rimmell, L. Tucker, and J. Weise, "Introduction to cloud computing architecture," White Paper, 1st edn. Sun Micro Systems Inc, 2009.
- [5]. E. E. Marinelli, "HyraX: cloud computing on mobile devices using mapreduce," *DTIC Document*, Tech. Rep., 2009.
- [6]. Q. Han, S. Liang, and H. Zhang, "Mobile cloud sensing, big data, and 5g networks make an intelligent and smart world," *Network*, IEEE, vol. 29, no. 2, pp. 40–45, 2015.
- [7]. Stojmenovic, "Access control in distributed systems: Merging theory with practice," in *Trust, Security and Privacy in Computing and Communications (TrustCom), 2011 IEEE 10th International Conference on*. IEEE, 2011, pp. 1–2.
- [8]. G. Wang, Q. Liu, and J. Wu, "Hierarchical attribute-based encryption for fine-grained access control in cloud storage services," in *Proceedings of the 17th ACM conference on Computer and communications security*. ACM, 2010, pp. 735–737.
- [9]. C. Gentry and A. Silverberg, "Hierarchical id-based cryptography," in *Advances in cryptology ASIACRYPT 2002*. Springer, 2002, pp. 548–566.
- [10]. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," in *Security and Privacy, 2007. SP'07. IEEE Symposium on*. IEEE, 2007, pp. 321–334.