A Modified Hierarchical Attribute-Based Encryption Access Control Method for Mobile Cloud Computing

Yuanpeng Xie, Hong Wen, Bin Wu, Yixin Jiang and Jiaxiao Meng

***Abstract*—Cloud computing is an Internet-based computing pattern through which shared resources are provided to devices on-demand. Its 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. With integrating into cloud computing, security issues such as data confidentiality and user authority may arise in the mobile cloud computing system, and it is concerned as the main constraints to the developments of mobile cloud computing. 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.**

***Index Terms*—Mobile cloud computing, M-HABE, access control.**

I. Introduction

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. What users of the mobile devices and applications need is that mobile-Internet can provide them with the service which is user-friendly, high-speed, and steady. In addition, the security issues of mobile terminals and the Internet access are attached importance to. And as a combination of cloud computing, mobile devices and wireless networks, mobile cloud computing is an emerging but very promising paradigm which brings rich computational resources to mobile users, network operators, as well as cloud computing providers [1] [2] [3]. 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.

There is no accurate definition of mobile cloud computing, several concepts were proposed, and two most popular schemes can be described as follows:

1) Mobile cloud computing is a kind of scheme which could run an application such as a weather monitor application on remote cloud servers as displayed in Figure 1, while the mobile devices just act like normal PCs except that the mobile devices connect to cloud servers via 3G or 4G while PCs through Internet. And this concept is considered as the most popular definition of mobile cloud computing [4].
2) Taking advantages of leisure resources such as CPU, memory, and storing disks, another model of mobile cloud computing exploits the mobile devices themselves as resources providers of cloud [5]. And the scheme supports user mobility, and recognizes the potential of mobile clouds to do collective sensing as well.

In this paper, we mainly use the first paradigm mentioned above, but the second one inspires us to assume that what if the mobile devices do not provide computing resources or storing resources but sensing data instead?

In fact, most mobile devices are capable to capture some data from the environment nowadays, for example, almost every smart phone are equipped with sensors of proximity, accelerometer, gyroscope, compass, barometer, camera, GPS, microphone [6], etc. Combining the concept of WSN, mobile devices can be regarded as mobile sensors that are able to provide other mobile devices who are users of the mobile cloud services with some sensing information including environment monitoring data, health monitoring data, and so on.

We take a weather monitor application as an example in this paper.

Assuming that a company develops a weather monitor application which aims to share real-time weather information such as temperature, humidity, pictures, and precise location information and so on to other users of the application. And the application utilizes the user-cloud-user model instead of peer-to-peer model so that the users can get classified and demanded information. Another feature of the application is that the users are divided into different hierarchies, depending on which users can get different sensing data, and users with higher privilege level can, of course, get access to more specific and more frequently updated information.

In order to meet what the application requires, security issues of the whole system should not be ignored, among all security issues the most important two security issues in such model can be divided into two parts: authority of application

Yuanpeng Xie and Hong Wen is with the National Key Laboratory of Science and Technology on Communications, University of Electronic Science and Technology, Chengdu 610054, China. E-mail: pengye91@hotmail.com and sunlike@uestc.edu.cn.

Bin Wu is with the School of Computer Science and Technology, Tianjin University, Tianjin, P. R. China. E-mail: binwu.tju@gmail.com

Yixin Jiang and Jiaxiao Meng are with the EPRI, China Southern Power Grid Co. Ltd., Guangzhou, China.

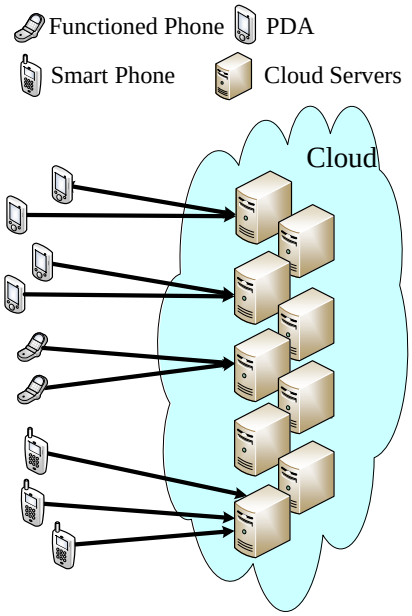


Fig. 1. A mobile cloud computing model

users and the confidentiality of sensing data. Those issues can be solved by providing methods of access control [7]. Attribute Based Encryption (ABE) is a recent cryptographic primitive which has been used for access control [8]–[11]. 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.

Based on such application demands, the concept of attribute based encryption is introduced [11]. Senders encrypt message with certain attributes of the authorized receivers. The ABE based access control method uses several tags to mark the attributes that a specific authorized user needs to possess. The users with certain tag sets can get access to the specific encrypted data and decrypt it. Lots of paper [12]–[15] introduced the scheme about the attribute based encryption access control method in the cloud computing. In the mobile loud computing environment, there are tremendous data which needs to be processed and marked with attributions for the convenient attributing access before storing. At the same time, the hierarchical structure of the application users need an authentication center entity to control their attributes.

In this paper, a hierarchical access control method using a modified hierarchical attribute-based encryption (M-HABE) and a modified three-layer structure [16] is proposed. Differing from the existing paradigms such as the HABE algorithm and the original three-layer structure, the novel scheme mainly focuses on the data processing, storing and accessing, which is designed to ensure the application users with legal access authorities to get corresponding sensing data and to restrict illegal users and unauthorized legal users get access to the data, the proposed promising paradigm makes it extremely suitable for the mobile cloud computing based paradigm. What should be emphasized is that the most important highlight of all in the proposed paper can be described as that the modified three-layer structure is designed for solving the security issues illustrated above.

The rest of the paper can be organized as follows. Section 2 points out the security issues in mobile cloud computing paradigm, which can be divided into 2 portions including security issues of cloud computing and security issues of mobile cloud computing. The proposed modified hierarchical attribute based encryption access control method is described in section 3. Section 4 demonstrates how the proposed access control method based on M-HABE applies in a weather application scenario specifically. Conclusions are given in section 5.

II. Mobile Cloud Computing Security Issues

More and more users are starting to use mobile cloud computing services such as iCloud and OneDrive services because of the poor storage and computation capability of current mobile devices. However, these kind of mobile cloud services are considered to be vulnerable in security and users may lose their stored files or messages such as pictures, documents, contacts, and calendars, whats worse, those information may be stolen by third parties. In September, 2014, Apple admitted that iCloud was compromised by hackers and many pictures of celebrities leaked out [17].

Such leakage event alarmed us that the security issues of mobile cloud should be taken seriously. For solving such security challenges, data authority and data confidentiality should be paid more attention.

Authority of data users: Different authority-level system to get access to sensing data for application users should be established since the paradigm is applied in the hierarchical multi-user shared environment, which also means that the users with higher authority level should get all the data that the users with lower privilege level could get access to, while the lower privilege users cant get the data beyond his/her authority.

Confidentiality of data: Although the cloud services utilized in the scenario are provided by private cloud which is supposed to be secure, it is still necessary to ensure the sensing data protected from malicious third parties that do not belong to the mobile cloud system. Therefore it is important for the system to bring in a secure and efficient encryption scheme.

In this section, we mainly discuss the general cloud computing security issues and mobile cloud computing issues.

A. 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 cloud services make it difficult to overcome defects in security control because of the insufficient control mechanisms that virtualized networks offer. And poor key management procedures of virtualized based cloud services make it worse [13]. Because virtual machines don't have a fixed hardware infrastructure and cloud-based content is often geographically distributed, it is a very tough task to ensure a secure control in cloud.

We conclude the discussion in Table I.

TABLE I
SECURITY ISSUES FOR CLOUD COMPUTING

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.

B. Security Issues for Mobile Cloud Computing

Mobile cloud computing model in this paper means that mobile device users run applications on remote cloud servers instead of mobile devices themselves, the paradigm performs almost the same as normal cloud computing with computers except that mobile cloud model connects mobile devices and cloud servers through 3G or 4G while cloud computing paradigm via Internet, therefore, mobile cloud computing inherits the security threats of traditional cloud computing. Whats more, the security issues that are specific to mobile devices such as battery exhaustion attacks [20] mobile bonnets and targeted attacks [21] should be concerned as well [1] .

III. 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 doesnt

TABLE II
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

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:

a) One encrypted data can be received by several users.
b) 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.
c) 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:

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

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.

A. Related Work

1) Hierarchical identity-based encryption

The concept of Identity Based Encryption (IBE) was proposed by Shamir [11] first in 1984, differing from traditional symmetrical encryption system, IBE took arbitrary character strings that can represent the identities of users, such as ID numbers, e-mail addresses, as public keys to encrypt data. One advantage of IBE is that the sender didnt have to search the public keys information on certificate authority (CA) online, which solved the problem of poor CA performance. The shortage of IBE system was that all users keys were generated by the private key generation (PKG), which would become the bottleneck in the system.

Horwitz [23] proposed the idea of hierarchical IBE (HIBE) in 2002, a user in the higher hierarchical position of the system could create private keys for lower position users with his/her private keys. Which mean that only the first level users private keys need be created by PKG, while lower-level users private keys could be generated and managed by their ancestors. This improved system relieved PKG of great burden and enhanced the system efficiency by authenticating identities and transporting keys within locality area instead of global area.

The public key of a user is described by a set of IDs composed of the public key of father node and the users own ID in the method of G-HIBE [9], the most important feature of the proposal is that the users public key could reflect precise position of the user in the hierarchical structure.

2) Ciphertext-policy attribute-based encryption

Attribute based encryption (ABE) [24] is regarded as the IBE method with an access structure bringing into the ciphertext or private key, the access structure determines what ciphertext can be obtained by which users.

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 obtains the ciphertext.

The core of the proposed scheme is called modified hierarchical attribute-based encryption (M-HABE), which is different from the HABE scheme.

HABE was proposed based on G-HIBE [9] and CP-ABE [10] by Wang [8] in 2010, it was designed mainly for the usage within an enterprise. We modified the proposal to adapt the scenarios of mobile cloud computing system, which could be illustrated as figure 2, with the aim of making it accommodate to the system based on mobile cloud computing.

As the Figure 2 shows, the proposal consists of an authentication center (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-AuC$_i$) and other Sub-AuCs, among which the AuC just need to be in charge of

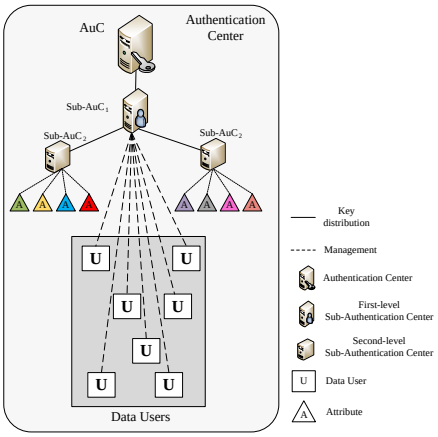


Fig. 2. M-HABE model

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-AuC$_1$
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

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.

Each data user shown in the figure possesses a unique ID which is a character string designed to describe the features of internal parties within the system, and so do 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 do not.

B. Key Description

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

a) Root key MK_0 possessed by AuC is used to create MK_* for Sub-AuC$_1$.

b) Each Sub-AuC owns a public key PK_i and a master key MK_i, among which PK_i is composed as (PK_{i-1}, ID_i) where PK_{i-1} is the public key of the Sub-AuC's father node, and MK_i is also created by the father node. PK_* is the public key of Sub-AuC$_1$, which can be demonstrated as ID_* meaning that it is composed by its own IDs. Unlike HABE proposed by Wang [8], Sub-AuC$_1$ in this paper only needs to take charge of users, and create their secret keys SK_u for them. And other Sub-AuCs have a set of attributes to manage, while they also create users' secret identity keys $SK_{i,u}$ and data users' secret attribute keys $SK_{i,u,a}$ at the same time.

c) Each data consumer is described by one precise ID denoted as ID_u, and a set of data users' attributes represented as $\{a\}$. Besides these, each user also owns a user public key PK_u denoted as $\{PK_*, ID_u\}$ and a consumer secret key SK_u, a set of user secret identity key $\{SK_{i,u}\}$ and a set of consumer secret attribute key $\{SK_{i,u,a}\}$.

d) Each attribute a is described by a precise ID denoted as ID_a. And even an attribute owns a public key in the form of (PK_{i-1}, ID_i) where PK_i is the public key of Sub-AuC that takes charge of the attribute.

C. M-HABE Definition

The M-HABE is composed by the following algorithms:

Setup: Given a security parameter K that is huge enough, AUC will generate a system parameter params and a root master key MK_0.

CreateMK: Using system parameter $params$ and their own master keys, AUC or Sub-AuCs can create master keys for lower-level Sub-AuCs.

CreateSK: With its own master key MK_* and system parameter $params$, Sub-AuC$_1$ creates secret key SK_u for each consumer if it is sure that the public key of the user is PK_u, or there would be no secret key for the user.

CreateUser: Sub-AuCs will create users' secret identity keys $SK_{i,u}$ and secret attribute keys $SK_{i,u,a}$ for them if the Aub-AuC makes sure that the attribute a is in charge of it and the user u satisfies a. And if not there would be no secret identity keys or secret attribute keys.

Encrypt: With $\boldsymbol{R}$ denoting a set of users' IDs, $\boldsymbol{A}$ representing the attribute-based access structure, the pubic keys of all the users that are in $\boldsymbol{R}$, and the public keys of all the attributes that are in $\boldsymbol{A}$, the data provider, which is also a data user of the cloud computing in this case, can encrypt the sensing data D into ciphertext C.

RDcrypt: Given the ciphertext C, a data user possessing the precise ID that is in $\boldsymbol{R}$ can decrypt the ciphertext C into plaintext D with $params$ and the user's secret key SK_u.

ADcrypt: Given the ciphertext C, a data user possessing an attribute set $\{a\}$ that satisfies $\boldsymbol{A}$, which means that the consumer owns at least an attribute key $SK_{i,u,a}$, can also decrypt the ciphertext C into plaintext D with system parameter $params$, the user's secret identity key $SK_{i,u}$, and the secret attribute key $SK_{i,u,a}$.

D. M-HABE Construction

Assuming that IG is a BDH parameter generator, the M-HABE scheme based on bilinear map [9] is constructed by following algorithms:

Step 1. $Setup(K) \rightarrow (params, MK_0)$: The AUC firstly chooses the root master key $mk_0 \in Z_q^*$, and then outputs the system parameter $params = \langle q, G_1, G_2, \hat{e}, n, P_0, Q_0, H_1, H_2 \rangle$, among which

$(q, G_1, G_2, \hat{e})$ is the output of IG, n is a positive integer, P_0 is a random generator of G_1, $H_1 : \{0,1\}^* \rightarrow G_1$ and $H_2 : G_2 \rightarrow \{0,1\}^n$ are two random oracles. In this step, the system parameter is able to be obtained publicly while the master key MK_0 is kept secret.

Step 2. $CreateMK(params, MK_i, PK_{i+1}) \rightarrow (MK_{i+1})$: Assuming that Sub-AuC$_i$ is the father node of Sub-AuC$_{i+1}$. And the master key of Sub-AuC$_{i+1}$ which is created by Sub-AuC$_i$ is in form of $MK_{i+1}=(mk_{i+1}, SK_{i+1}, Q\text{-}tuple_{i+1}, H_A)$, among which

- mk_{i+1} is a random element belonging to Z_q^*.
- $SK_{i+1}=SK_i+mk_iP_{i+1} \in G_1$, where mk_i is part of MK_i, $P_{i+1}=H_1(PK_{i+1}) \in G_1$. Especially, SK_0 is the generator of G_1 if the father node is AUC, which means that $i=0$.
- $Q\text{-}tuple_{i+1}=(Q\text{-}tuple_i, Q_{i+1})$, where $Q_{i+1}=mk_{i+1}P_0 \in G_1$.
- $H_A : \{0,1\}^* \rightarrow Z_q^*$ is a random oracle.

Step 3. $CreateSK(params, MK_*) \rightarrow (SK_u)$: System parameter $params$ and master key MK_* are used by AuC to create managers secret key $SK_u=(Q\text{-}tuple_*, SK_*+mk_*P_u)$, where $P_u=H_1(PK_u) \in G_1$.

Step 4. $CretaeUser(params, MK_i, PK_u, PK_a) \rightarrow (SK_{i,u}, SK_{i,u,a})$: Suppose a user u asks for the attribute key about attribute a, what the Sub-AuC does firstly is to check if the attribute a is in its charge, and outputs $SK_{i,u}=(Q\text{-}tuple_{i-1}, mk_imk_uP_0)$, $SK_{i,u,a}=SK_i+mk_imk_uP_a$ if it is, where $mk_u=H_A(PK_m) \in Z_q^*$, $P_a=H_1(PK_a) \in G_1$, or the algorithm will output 'null'.

Step 5. $Encrypt(params, R, A, PK_a, PK_u, D) \rightarrow CT$: Given a set of ID $R=\{ID_{u_1}, \ldots, ID_{u_m}\}$ and a DNF access control structure $A=\vee_{i=1}^{N}(CC_i)=\vee_{i=1}^{N}(\wedge_{j=1}^{n_i}a_{ij})$, where N is the number of conjunctive clause in A, n_i is the number of attribute in the i-th conjunctive clause CC_i, and a_{ij} is the j-th attribute in CC_i. Assume that all the attributes in CC_i are managed by the t_i-th level Sub-AuC denoted as Sub-AuC$_{it_i}$ whose public key is $(ID_{it_1}, \ldots, ID_{it_i})$, where ID_{ik}, for $1 \leq k \leq t_i$, is the ID of Sub-AuC$_{it_i}$'s ancestor, and ID_{i1} is the ID of AuC, which is ID_*. The following steps demonstrate how to encrypt sensing data D by senders:

- Compute $P_*=H_1(PK_*) \in G_1$.
- For $1 \leq i \leq m$, compute $P_{u_i}=H_1(PK_{u_1}) \in G_1$.
- For $1 \leq j \leq t_i$, compute $P_{ij}=H_1(ID_{i1}, \ldots, ID_{ij}) \in G_1$.
- For $1 \leq i \leq N$ and $1 \leq j \leq n_i$, compute $P_{a_{ij}}=H_1(ID_{i1}, \ldots, ID_{it_1}, ID_{a_{ij}}) \in G_1$.
- Choose a random number $r \in Z_q^*$, assume that n_A is the lowest common multiple (LCM) of $n_1, \ldots, n_N$, and compute formula (1)-(7):

$$U_0=rP_0; \tag{1}$$

$$U_{u_1}=rP_{u_1}, \ldots, M_{u_m}=rP_{u_m}; \tag{2}$$

$$U_{12}=rP_{12}, \ldots, U_{1t_1}=rP_{1t_1}; \tag{3}$$

$$U_1=r\sum_{j=1}^{n_1}P_{a_{1j}}; \ldots; \tag{4}$$

$$U_{N2}=rP_{N2}, \ldots, U_{Nt_N}=rP_{Nt_N}; \tag{5}$$

$$U_N=r\sum_{j=1}^{n_N}P_{a_{Nj}}; \tag{6}$$

$$V=D \oplus H_2(\hat{e}(Q_0, rn_AP_*)) \tag{7}$$

- Let $C_D = [U_0, U_{u_1}, \ldots, U_{u_m}, U_{12}, \ldots, U_{1t_1}, U_1, \ldots, U_{N2}, \ldots, U_{Nt_N}, U_N, V]$, and the ciphertext $CT = [R, A, C_D]$

Step 6. $RDcrypt(params, ID_u, SK_u, CT) \rightarrow D$: The user u_i can get access to the ciphertext and decrypts it into the plaintext D if the ID of u_i is in R, the verification is shown in Eq.(8):

$$\begin{aligned}
&V \oplus H_2\left(\frac{\hat{e}(n_AM_0, SK_*+mk_*P_{u_i})}{\hat{e}(n_AQ_*, M_{u_i})}\right) \\
&= V \oplus H_2\left(\frac{\hat{e}(rn_AP_0, mk_0P_*+mk_*P_{u_i})}{\hat{e}(n_AQ_*, rP_{u_i})}\right) \\
&= V \oplus H_2\left(\frac{\hat{e}(rn_AP_0, mk_0P_*)\hat{e}(rn_AP_0, mk_*P_{u_i})}{\hat{e}(n_AQ_*, rP_{u_i})}\right) \\
&= V \oplus H_2\left(\frac{\hat{e}(mk_0P_0, rn_AP_*)\hat{e}(n_Amk_*P_0, rP_{u_i})}{\hat{e}(n_AQ_*, rP_{u_i})}\right) \\
&= V \oplus H_2\left(\frac{\hat{e}(mk_0P_0, rn_AP_*)\hat{e}(n_AQ_*, rP_{u_i})}{\hat{e}(n_AQ_*, rP_{u_i})}\right) \\
&= V \oplus H_2(\hat{e}(Q_0, rn_AP_{u_i})) \\
&= D
\end{aligned} \tag{8}$$

Step 7. $ADcrypt(params, SK_{i,u}, SK_{i,u,a}, CT) \rightarrow D$: Given the ciphertext C, a user possessing an attribute set $\{a\}$ that satisfies $\mathbf{A}$, which means that the user owns at least an attribute key $SK_{i,u,a}$, can also decrypts the ciphertext C into plaintext D with $params$, the user's secret identity key $SK_{i,u}$, and the secret attribute key $SK_{i,u,a}$, the verification is shown in Eq.(9):

$$V \oplus H_2 \left(\frac{\hat{e}\left(U_0, \frac{n_A}{n_i}\sum_{j=1}^{n_i}SK_{(it_i,u,a_{ij})}\right)}{\hat{e}\left(mk_umk_{it_1}, \frac{n_A}{n_i}U_i\right)\prod_{j=2}^{t_i}\hat{e}(M_{ij}, n_AQ_{i(j-1)})}\right)$$

$$
\begin{aligned}
&= V \oplus H_2 \\
&\left(\frac{\hat{e}(U_0, n_A SK_{i1})}{\hat{e}\left(SK_{it_i,u}, \frac{n_A}{n_i} U_i\right) \prod_{j=2}^{t_i} \hat{e}(U_{ij}, n_A Q_{i(j-1)})} \times \right. \\
&\left. \hat{e}\left(U_0, n_A \sum_{k=2}^{t_i} mk_{i(k-1)} P_{ik} + \frac{n_A}{n_i} mk_{it_j} mk_u \sum_{j=1}^{n_i} P_{a_{ij}}\right)\right) \\
&= V \oplus H_2 \\
&\left(\frac{\hat{e}(M_0, n_A r P_{i1}) \hat{e}\left(SK_{it_i,u}, \frac{n_A}{n_i} U_i\right)}{\hat{e}\left(SK_{it_i,u}, \frac{n_A}{n_i} U_i\right) \prod_{j=2}^{t_i} \hat{e}(U_{ij}, n_A Qi(j-1))} \times \right. \\
&\left. \prod_{k=2}^{t_i} \hat{e}(Q_{i(k-1)}, n_A U_{ik}) \right) \\
&= V \oplus H_2(\hat{e}(Q_0, n_A r P_*)) \\
&= D
\end{aligned} \tag{9}
$$

Note 1: In order to improve the performance of the whole scheme, data user can send $Q\text{-}tuple_{i(t_i-1)}$ to cloud to explicit the great computation ability with the aim of helping to compute $\prod_{j=2}^{t_i} \hat{e}(M_{ij}, n_A Q_{i(j-1)})$, so that the data user can decrypt the ciphertext with computing bilinear maps only constant times when running the ***ADcrypt*** algorithm.

Note 2: The public key of data consumer u (ID_*, ID_u) can be combined with the public key of attributes $(ID_*, \ldots, ID_i, ID_a)$ in form of a character string as the input of H_1 and H_A.

IV. M-HABE Access Control Method Applied in Cloud-based Smart Grid

Applying M-HABE, the proposed scheme is illustrated in Figure 3. The whole system works as following steps:

- All kinds of mobile devices which are installed with the mobile cloud computing based weather application are distributed into different locations all over the country with users. The applications can exploit the sensors installed in the mobile devices to capture the weather data that the applications need, including temperature value, humidity information, atmospheric pressure and so on.
- The sensing weather data is transported to the layer1 which is a kind of IaaS cloud service provided by the cloud provider [25].
- Before sent to layer 2, the sensing weather data is classified by its data model [16] in layer 1 with its excellent ability of computing and storing, the step can be illustrated by figure 4. The data model we present is inspired by the data model proposed in [26], based on which our data model is composed by format, device ID, size, time, value and period. Therefore, a raw data can be expressed as a vector $Data$ $\langle format; mobiledeviceID; sizeltimelvalue; period \rangle$. $Format$ stands for the basic format of the raw weather data that a specific mobile device produces, there are different kinds of formats depended on different kinds of mobile devices, for example, JPEG, WMA, TXT,PNG,WMV,etc. $MobiledeviceID$ is the only sign of the source mobile device where raw weather data comes from. The $size$ of sensing weather data is defined by the raw weather data itself, which indicates the size of one specific weather data. As for $time$, as long as a mobile device captures data from the environment where it is in, the time that the sending action occurs will be regarded as the $time$ attribute of the raw sensing data. A $value$ sign represents the most important characteristic of sensing data, the meaning it stands for differs from format to format, and different kinds of mobile devices have different meanings. For example, for a temperature sensor, the value means specific numbers of the temperature, while the humidity sensors can only produce the data with the $value$ attributes that indicate the specific numbers of humidity. A $period$ identification is a time cycle of the sensing data, it is utilized to describe the life period of one specific sensing raw data, and the data will be destroyed once the storing time in cloud of it is beyond the $period$ time.
- The sensing weather data is encrypted into ciphertext in layer 2 by M-HABE encryption algorithm using the key in form of $(R, A, PK_a | a \in A, ID_u \in R)$,Ł and the cyphertext is sent to layer 3 which is also a kind of IaaS cloud service in cloud. The encryption step can be demonstrated as Figure 5.
- The data users of the scheme are in charge of just like Figure 2 indicates. The users can get access to the ciphertexts only if he/she satisfies the requirements of ***RDcrypt*** algorithm or ***ADcrypt*** algorithm that are described in part III. The decryption procedure is shown in Figure 6.

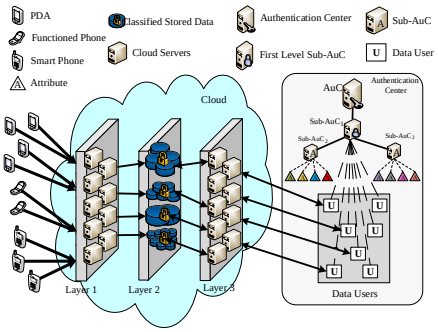


Fig. 3. General structure of M-HABE access control method for mobile cloud computing

V. Conclusion

The paper proposed a modified HABE scheme by taking advantages of attributes based encryption (ABE) and hierarchical identity based encryption (HIBE) access control processing. The proposed access control method using M-HABE is designed to be utilized within a hierarchical multi-user data-shared environment, which is extremely suitable for a mobile cloud computing model to protect the data privacy and defend unauthorized access. Compared with the original

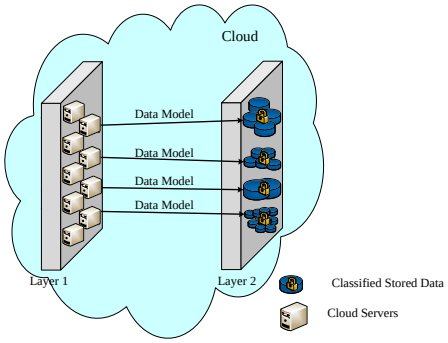


Fig. 4. Data model

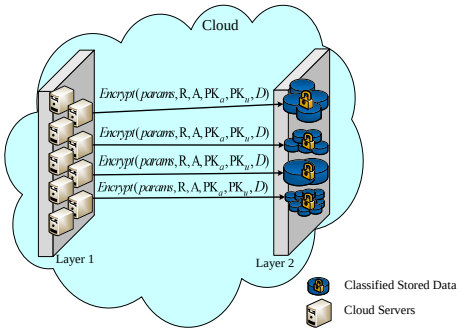


Fig. 5. Encryption procedure

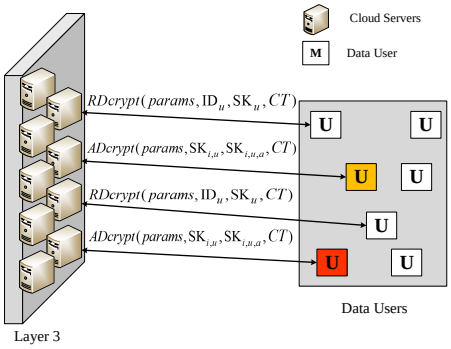


Fig. 6. Decryption procedure

HABE scheme, the novel scheme can be more adaptive for mobile cloud computing environment to process, store and access the enormous data and files while the novel system can let different privilege entities access their permitted data and files. The scheme not only accomplishes the hierarchical access control of mobile sensing data in the mobile cloud computing model, but protects the data from being obtained by an untrusted third party.

ACKNOWLEDGMENT

The work is sponsored by EPRI, CSG research founding, NSFC (No. 61271172, 61572114), 863 High Technology Plan (Grant No. 2015AA01A707), NSFC A3 Program (No.61140320) and RFDP (Grant No. 20120185110030, 20130185130002).

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, "Cloud-based 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. Remmell, 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] I. 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 cryptologyASIACRYPT 2002*. Springer, 2002, pp. 548–566.

[10] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Security and Privacy, 2007. SP'07. IEEE Symposium on*. IEEE, 2007, pp. 321–334.

[11] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in cryptology*. Springer, 1985, pp. 47–53.

[12] M. Zhou, R. Zhang, W. Xie, W. Qian, and A. Zhou, "Security and privacy in cloud computing: A survey," in *Semantics Knowledge and Grid (SKG), 2010 Sixth International Conference on*. IEEE, 2010, pp. 105–112.

[13] B. Grobauer, T. Walloschek, and E. Stöcker, "Understanding cloud computing vulnerabilities," *Security & privacy, IEEE*, vol. 9, no. 2, pp. 50–57, 2011.

[14] S. Ghemawat, H. Gobioff, and S.-T. Leung, "The google file system," in *ACM SIGOPS operating systems review*, vol. 37, no. 5. ACM, 2003, pp. 29–43.

[15] M. Zhou, R. Zhang, W. Xie, W. Qian, and A. Zhou, "Security and privacy in cloud computing: A survey," in *Semantics Knowledge and Grid (SKG), 2010 Sixth International Conference on*. IEEE, 2010, pp. 105–112.

[16] Y. Xie, J. Zhang, G. Fu, H. Wen, Q. Han, X. Zhu, Y. Jiang, and X. Guo, "The security issue of wsns based on cloud computing," in *Communications and Network Security (CNS), 2013 IEEE Conference on*. IEEE, 2013, pp. 383–384.

[17] R. Walters, "Cyber attacks on us companies in 2014," *Heritage Foundation Issue Brief*, no. 4289, 2014.

[18] A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, and I. Stoica, "Above the clouds: A berkeley view of cloud computing," *Dept. Electrical Eng. and Comput. Sciences, University of California, Berkeley, Rep. UCB/EECS*, vol. 28, p. 13, 2009.

[19] L. Sumter, "Cloud computing: security risk," in *Proceedings of the 48th Annual Southeast Regional Conference*. ACM, 2010, p. 112.

[20] B. R. Moyers, J. P. Dunning, R. C. Marchany, and J. G. Tront, "Effects of wi-fi and bluetooth battery exhaustion attacks on mobile devices," in *System Sciences (HICSS), 2010 43rd Hawaii International Conference on*. IEEE, 2010, pp. 1–9.

[21] J. Oberheide and F. Jahanian, "When mobile is harder than fixed (and vice versa): demystifying security challenges in mobile environments," in *Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications*. ACM, 2010, pp. 43–48.

[22] W. Zhang, Y. Wen, and H.-H. Chen, "Toward transcoding as a service: energy-efficient offloading policy for green mobile cloud," *Network, IEEE*, vol. 28, no. 6, pp. 67–73, 2014.

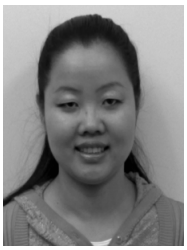
[23] J. Horwitz and B. Lynn, "Toward hierarchical identity-based encryption," in *Advances in CryptologyEUROCRYPT 2002*. Springer, 2002, pp. 466–481.

[24] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proceedings of the 13th ACM conference on Computer and communications security*. Acm, 2006, pp. 89–98.

[25] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica *et al.*, "A view of cloud computing," *Communications of the ACM*, vol. 53, no. 4, pp. 50–58, 2010.

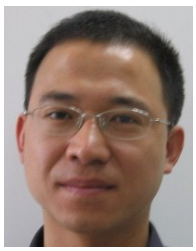
[26] T.-D. Nguyen and E.-N. Huh, "An efficient key management for secure multicast in sensor-cloud," in *Computers, Networks, Systems and Industrial Engineering (CNSI), 2011 First ACIS/JNU International Conference on*. IEEE, 2011, pp. 3–9.

Yuanpeng Xie received the bachelor degree in communication engineering from the University of Electronic Science and Technology of China in July 2013. He is currently studying for his master degree in communication and information system in National Key Laboratory in Communication at University of Electronic Science and Technology of China. His research interests include the security issues in cloud computing, the integration of WSNs and cloud computing, and security issues in smart grid.



Hong Wen received the M.Sc. degree in Electrical Engineering from Sichuan University, P. R. China, in 1997. She pursued her Ph.D. degree in Communication and Computer Engineering Dept. at the Southwest Jiaotong University (Chengdu, P. R. China). Then she worked as an associate professor in the National Key Laboratory of Science and Technology on Communications at UESTC, P. R. China. From Jan. 2008 to Sept. 2009, she was a visiting scholar and postdoctoral fellow in the ECE Dept. at University of Waterloo. Now she holds the professor position at UESTC, P. R. China. Her major interests focus on wireless communication system and security.

Bin Wu received his Ph.D. degree in Electrical and Electronic Engineering from The University of Hong Kong (Pokfulam, Hong Kong) in 2007. He worked as a postdoctoral research fellow from 2007-2012 in the ECE Dept. at University of Waterloo (Waterloo, Canada). He is now a professor in the School of Computer Science and Technology at Tianjin University (Tianjin, P. R. China). His research interests include computer systems and networking as well as cloud computing.



Yixin Jiang received the Ph.D. degree in Computer Science from Tsinghua University in 2006. From 2011, he was a senior researcher of EPRI, China Southern Grid. His research interests include smart grid, security and performance evaluation in wireless communication and mobile computing. He has published more than 80 papers in research journals and IEEE conference proceedings in these areas.

Jiaxiao Meng received the B.S. degree in Traffic and Transportation from Central South University of Forestry and Technology, Changsha, Chian, in 2004. He is currently pursuing the M.D. degree in Telecommunications engineering at Beijing University of Posts and Telecommunications. From 2012 to 2015, he was a Research Assistant with Electric Power Research Institute,CSG, Guangzhou, China. His research interest includes the Network Security and Cloud Computing.