ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Hierarchical Attribute-Based Encryption Handling Control Method by Mobile Cloud Computing

Villuri Divya
Department of Computer Science and Engineering,
SIMS College,
Guntur, Andhra Pradesh 522001, India.

B Mounika Chowdary
Department of Computer Science and Engineering,
SIMS College,
Guntur, Andhra Pradesh 522001, India.

ABSTRACT

Cloud computing is an Internet-based computing pattern through which shared resources are provided to devices ondemand. 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.

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, highspeed, 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 isconsidered as the most popular definition of mobile cloud computing [4]. 2) Taking advantages of leisure resources such as CPU,

Cite this article as: Villuri Divya & B Mounika Chowdary, "Hierarchical Attribute-Based Encryption Handling Control Method by Mobile Cloud Computing", International Journal & Magazine of Engineering, Technology, Management and Research, Volume 6 Issue 7, 2019, Page 33-37.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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 provideothermobiledeviceswhoareusersofthemobileclou d 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 informationandsoontootherusersoftheapplication.Andthe application utilizes the user-cloud-user model instead of peer-to peer-models othattheuserscangetclassified anddemanded 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.

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 user scant 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.

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

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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.

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.

- Key Description Public key encryption is utilized in the proposed system, the related keys are summarized in Table III. a) Root key MK0 possessed by AuC is used to create MK∗ for Sub-AuC1. b) Each Sub-AuC owns a public key PKi and a master key MKi, among which PKi is composed as (PKi−1,IDi) where PKi−1 is the public key of the Sub-AuC's father node, and MKi is also created by the father node. PK∗ is the public key of Sub-AuC1, which can be demonstrated as ID∗ meaning that it is composed by its own IDs. Unlike HABE proposed by Wang [8], Sub-AuC1 in this paper only needs to take charge of users, and create their secret keys SKu for them.

M-HABE Definition The M-HABE is composed by the following algorithm

s: Setup: Given a security parameter K that is huge enough, AUC will generate a system parameter params and a root master key MK0. 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-AuC1 creates secret key SKu for each consumer if it is sure that the public key of the user is PKu, or there would be no secret key for the user. CreateUser: Sub-AuCs will create users' secret identity keys SKi,u and secret attribute keys SKi,u,a for them if the AubAuC 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 R denoting a set of users' IDs, A representing the attribute-based access structure, the pubic keys of all the users that are in R, and the public keys of all the attributes that are in 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.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

RDcrypt: Given the ciphertext C, a data user possessing the precise ID that is in R can decrypt the ciphertext C into plaintext D with params and the user's secret key SKu. ADcrypt: Given the ciphertext C, a data user possessing an attribute set {a} that satisfies A, which means that the consumer owns at least an attribute key SKi,u,a, can also decrypt the ciphertext C into plaintext D with system parameter params, the user's secret identity key SKi,u, and the secret attribute key SKi,u,a.

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 hformat;mobiledeviceID;sizeltimelvalue;periodi.

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 MHABE is designed to be utilized within a hierarchical multiuser 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 originalHABE 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

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. 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

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

(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 attributebased 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. St¨ocker, "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.

Author Details

Villuri Divya
MCA Student,
Reg No: 316233620011
SIMS College.

B Mounika Chowdary
M.Tech (CST),
Assistant Professor,
SIMS College.