Available online at www.sciencedirect.com

SciVerse ScienceDirect

AASRI Procedia 2 (2012) 262 – 267

AASRI Procedia

www.elsevier.com/locate/procedia

2012 AASRI Conference on Power and Energy Systems

User Authentication using Profiling in Mobile Cloud Computing

Hoon Jeong, Euiin Choi*

Department of Computer Engineering, Hannam University, Ojung-Dong 133, Daeduk-Gu, Daejeon, KOREA

Abstract

As Cloud Computing has been spreading widely, users and service providers enables to use resource or service cheaply and easily without owning all the resource needed. However, cloud computing, virtualization technology, large distributed processing technologies, service availability, high-traffic processing will occur due to various problems. In recent years, among many of these problems in application security, access control, authentication, and password and a lot of it has been studied. User authentication in a mobile environment, especially the more important to them and high level of security certification is required. In this paper, in a mobile environment for high level security authentication using profiling techniques for access control and user authentication is proposed.

Key-words: Mobile Cloud Computing; Profiling; Security; Access Control; User Authentication;

1. Introduction

The market of mobile recently has been evolving rapidly and cloud computing is spreading into mobile as well. That is why mobile cloud computing is becoming a new issue today. Cloud computing is the computing that provides virtualized IT resources as a service by using Internet technology. In cloud computing, a user lends IT resources(software, storage, server, network) as needed, uses them, get a support of real-time scalability according to service load, and pays as he/she goes[1].

* Corresponding author. Tel.: +82-10-3709-1107; fax: +82-42-629-8120.
E-mail address: eichoi@hnu.kr.

 doi:10.1016/j.aasri.2012.09.044

Mobile cloud computing creates a new chance for IT industry because it allows the superiority and economic of cloud computing to meet the mobility and convenience of mobile and draws a synergy effect for both. Also mobile cloud computing refers to an infrastructure that data storage and data processing is done outside mobile device by using cloud computing in the regardless of kinds of mobile devices.

Authentication and data security among Cloud Computing technologies are dealt with in this section. Lim described it into 8 of categories in his paper[2] and Traian Andrei[3] also mentioned the same referring to Gartner's[4]. So as to secure data of individuals or enterprises, authentication technology shall be offered basically. Especially, in Cloud Computing, the availability of entire system can be falling when security a large volume of data, so an appropriate cipher should be used for the situation. Also when something happens to the key-stored server, it is not possible for a lot of users to access to data, there should be a study on a key management. It is very important to study on fault tolerance and data recovery technologies when there is an incident in order to prevent a service discontinuance or data loss. Examples of Cloud service discontinuance and data loss are the examples of what problems can be caused when these mechanisms not work properly. He also described some security guidelines for Cloud Computing using what Gartner says [4]. They are privileged user access, regulatory compliance, data location, data segregation, recovery, investigative support, and long-term viability.

So, profiling technique has been studied to provide a suitable service for user and personal profile information in mobile environment. In this system, a formal model has to be provided to offer information needed by application. However, there are some technical constraints for this model to overcome because it itself cannot be applied to mobile platform due to limited device resources, so the study on intelligent mobile service in mobile platform is still insufficient. Recent interest related to mobile cloud is personal smartphone.

Therefore, in this paper designs a profile based model on mobile cloud platform and develops in order to guarantee data security through user authentication.

2. Related Works

The object of awareness in this mobile cloud computing which differ from previous computing environment is not human, but device[5]. This means that information is to be personalized. They actively have to provide various service and information to aware human's behavior and thought. For this problem solving on mobile cloud computing, it was inferred situation which was able to understand human's behavior which collected from various sensors. And they are provided service and information to user through the inferred context. Generally, situation which arose around human was able to collect from sensor, but personal inclination and thought was not. Therefore, they used the method of personal information storage for analyzing inclination, such as personal profile, history, diary[6, 7]. As mentioned above, user of mobile cloud computing was provided various services without human's recognization by mobile devices in anywhere and anytime. So, we have to infer context for provide the services to users correctly. Therefore, there are studying about technique of context inference to use personal inclination and information. As it demanded personal inclination and information in context inference, using the user's profile for storing it, research about technique of profile was as follow:

UbiData project was suggested data process and synchronization and addresses these three challenges using an architecture and sophisticated hoarding, synchronization, and transcoding algorithms to enable continuous availability of data regardless of user mobility and disconnection, and regardless of the mobile device and its data viewing/processing applications[8, 9]. Manuele Kirsch-Pinheiro proposed a context-based filtering process, aimed at adapting awareness information delivered to mobile users by collaborative web systems. This filtering process relied on a model of context which integrates both physical and organizational dimensions, and allows representation of the user's current context as well as general profiles. These profiles

are descriptions of potential user contexts and express awareness information filtering rules to apply when the user's current context matches one of these rules. Given a context, these rules reflect user preferences. They describe how the filtering process performs in two steps, the first for identifying the general profiles that apply, and the second for selecting awareness information[10].

However, these profile techniques not sufficient on mobile cloud computing. Therefore, this paper proposes profile in order to manage resources more effectively by using personal information and do modeling information in mobile platform and reason.

2.1 Definition of Cloud Computing and the Appearance Background

Gartner defines cloud computing as "a style of computing where scalable and elastic IT-related capabilities are provided 'as a service' to external customers using Internet technologies"[11, 12]. Cloud Computing is a kind of on-demand computing method that lets users use IT resources such as network, server, storage, service, application, and so on via Internet when needing them rather than owning them[13]. Cloud Computing can be considered as a sum of SaaS(Software as a Service) and utility computing and Figure 1 shows the roles of users or providers in the Cloud Computing under the concept[11]. The first appearance of the concept of Cloud Computing is from what John McCarthy said that computation might someday be organized as o public utility in 1960s[14, 15]. The term of "Cloud" was originated from the telecommunication world in 1990s, when providers started using virtual private network(VPN) for data communication[16]. Since then, Cloud Computing has been developing rapidly because of IT infrastructure such as the spread of wired/wireless communication network and the high speed, a variety of tool sets, the spread of free software, and so on[17].

2.2 Security Technology in the Cloud Computing Environment

There are no concrete security technologies in Cloud Computing, however, if we regard Cloud Computing as an extension of the existing IT technologies, it is possible to divide some of them by each component of Cloud Computing and apply to[18]. Access control and user authentication are representative as security technologies used for platforms. Access control is the technology that controls a process in the operating system not to approach the area of another process. There are DAC (Discretionary Access Control), MAC (Media Access Control), and RBAC(Role-Based Access Control). DAC helps a user establish the access authority to the resources that he/she owns as he/she pleases. MAC establishes the vertical/horizontal access rules in the system at the standard of security level and area for the resources and uses them. RBAC gives an access authority to a user group based on the role the user group plays in the organization, not to a user. RBAC is widely used because it is fit for the commercial organizations. Technologies used to authenticate a user are Id/password, Public Key Infrastructure, multi-factor authentication, SSO(Single Sign On), MTM (Mobile Trusted Module), and i-Pin[18].

3. User Authentication in the Cloud Computing

The representative user authentication security technologies described above have some weaknesses. This section looks at user authentication security technologies and their weaknesses briefly[12, 18]. Id/password: the representative user authentication method. It is simple and easy to use, but it has to have a certain level of complication and regular renewal to keep the security.PKI(Public Key Infrastructure): an authentication means using a public-key cryptography. It enables to authenticate the other party based on the certificate without shared secret information. In PKI structure, it is impossible to manage and inspect the process of client side.

Multi-factor: a method to heighten the security intensity by combining a few means of authentication. Id, password, biometrics like fingerprint and iris, certificate, OTP(One Tome Pad), etc. are used. OTP information as well as Id/password can be disclosed to an attacker. SSO(Single Sign On): a kind of passport if it gets authentication from a site, then it can go through to other sites with assertion and has no authentication process. The representative standard of assertion is SAML.MTM(Mobile Trusted Module): a hardware-based security module. It is a proposed standard by TCG(Trusted Computing Group) which Nokia, Samsung, France Telecom, Ericson, etc. take part in. It is mainly applied to authenticate terminals from telecommunications, however, it is being considered as a Cloud Computing authentication method with SIM(Subscriber Identity Module) because of generalization of smartphone[19]. i-Pin: a technique to use to confirm a user's identification when the user uses Internet in Korea now. It operates in a way that the organization which itself performed the identification of the user issues the assertion. Among the security technologies mentioned above, Id/password and OTP may have a key logging attack or SSL strip attack and can be disclosed to the attacker.

Authentication service provides to authorization service that is user's ID after authentication through various context-aware information of attempted user about information access. Authorization service performs not only supervise for requirements about information access of user's but also decision of context information for all constraints by role. And then that provide context-knowledge model repository for location of resources that is accessible of user. User&Role repository is storing role about user's ID and authority policy repository is describing security policy. Context knowledge model is the map of knowledge that provides locations of all information resources which is accessible according to role and context information. This method is limited by resources access along the surrounding environment in case of accessible user request to approach. Figure 1 below shows the platform for authentication service.

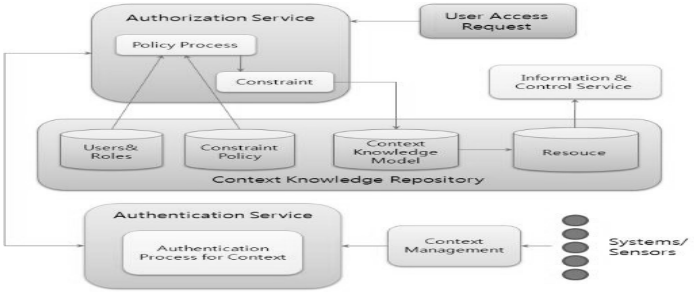

Fig 1 Platform for Authentication service

4. Profile Structure

A user's profile specifies information of interest for an end user. So in this paper, the profile was consisted of user information part and service information part. User information part stored user's information such as user's name, inclination, hobby and Service information part stored services that they were used such as service name, service provider etc.

Structure of user profile was follow:

- User Information: User name, User ID, Personal inclination, hobby, etc
- Service Information: Service Name, Service Provider, Service context, Service frequency value, etc

Because profile stored how much the service information used, stored not only used service, but also information when, how, where used. Also, there are stored the information about what context used.

DTD of profile which we were suggested follow.

```
<?xml version='1.0' encoding='UTF-8' ?>
<!ELEMENT ups_profiles (upsp)>
<!ELEMENT upsp(user_info, service_list?, device_info)>
<!ELEMENT user_info (username , password, hobby)>
<!ATTLIST user_info userID ID #REQUIRED >
<!ELEMENT username (firstname , lastname)>
<!ELEMENT firstname (#PCDATA)>
<!ELEMENT lastname (#PCDATA)>
<!ELEMENT password (#PCDATA)>
<!ELEMENT hobby (#PCDATA)>
<!ELEMENT service_list (service*)>
<!ELEMENT service (service_name, service_provider, service_time, service_frequency*) >
<!ELEMENT service_name(#PCDATA)>
<!ELEMENT service_provider(#PCDATA)>
<!ELEMENT service_time(#PCDATA)>
<!ELEMENT service_frequency(week_info, access_time, location)>
<!ATTLIST service_frequency value CDATA #REQUIRED >
<!ELEMENT week_info (#PCDATA)>
<!ELEMENT access_time (#PCDATA)>
<!ELEMENT location (#PCDATA)>
```

5. Conclusions

This paper had a close look at access control and user authentication which are security technologies used in the platform in the Cloud Computing environment. In the Cloud Computing environment, misuse of access authority to resources and leak of personal information which should be used to authenticate a user could affect faster and more powerful compared to mono-system. For the effective user authentication in the Cloud Computing environment, the authentication technologies described above should be used by combining them suitably or a secure user authentication method for the right purpose of Cloud Computing should be developed. As a further research, a proper user authentication service model and protocol for Cloud Computing should be designed and developed.

Acknowledgements

This work was supported by the Security Engineering Research Center, granted by the Korea Ministry of Knowledge Economy.

References

[1] Gartner Says Cloud Computing Will Be As Influential As E-business, http://www.gartner.com/it/page.jsp?id=707508 (June, 2008)
[2] Lim, C.: Cloud Computing Security Technology. In Review of KIISC, V.19, n.3, pp. 14-17,

ISSN:1598=3978 (2009)
[3] Andrei, T.: Cloud Computing Challenges and Related Security Issues, http://www.cs.wustl.edu/~jain/cse571-09/ftp/cloud.pdf (May, 2009)
[4] Gartner, Assessing the Security Risks of Cloud Computing, http://www.gartner.com/Display Document?id=685308 (June, 2008)
[5] M. Weiser. : Hot topics-ubiquitous computing, In: IEEE Computer, Vol. 26, No. 10(1993).
[6] Barkhuus, L., Dey, A. :Is Context-Aware Computing Taking Control away from the User Three Levels of Interactivity Examined. In: Proceedings of the 5th International Conference on Ubiquitous Computing (UbiComp'03)(2003).
[7] Elfeky, M.G., Aref, W.G., Elmagarmid, A.K. : Using Convolution to Mine Obscure Periodic Patterns in One Pass, In: Proceedings of the 9th International Conference on Extending Database Technology (EDBT)(2004).
[8] G. M. Sur, J. Hammer, : Management of user profile information in UbiData, In: Technical Report TR03-001, Dept. of CISE, University of Florida, Gainesville(2003).
[9] J. Zhang, A. S. Helal, J. Hammer. : Ubidata: Ubiquitous mobile file service, In: Eighteenth ACM Symposium on Applied Computing(2003)
[10] Manuele.Kirsch-Pinheiro, Marlene Villanova- Oliver, Jerome Gensel, Herve Martin, : Context-Aware Filtering for Collaborative Web Systems: Adapting the Awareness Information to the User's Context, In : ACM Symposium on Applied Computing(2005).
[11] Armbust, M., et al.: Above the Clouds: A Berkeley View of Cloud Computing. In: Technical Report. http://www.eeec.berkeley.edu/Pubs/TechRpts/2009/EEEC-2009-28.html (2009).
[12] Gartner Says Cloud Computing Will Be As Influential As E-business. http://www.gartner.com/it/page.jsp?id=707508 (2008).
[13] Kim, J., Kim, H.: Cloud Computing Industry Trend and Introduction Effect. In: IT Insight, National IT Industry promotion Agency (2010).
[14] http://en.wikipedia.org/wiki/Cloud_computing#History.
[15] Dikaiakos, M.D., et al.: Cloud Computing Distributed Internet Computing for IT and Scientific Research. In: IEEEInternet Computing, pp. 10-13, September/October (2009).
[16] Harauz, J., et al.: Data Security in the World of Cloud Computing. In: IEEE Security & Privacy, pp. 61-64 (2009).
[17] Lee, J.: Cloud Compting, Changes IT Industry Paradigm. In: LG Business Insight, pp. 40-46 (2009).
[18] Un, S., et al.: Cloud Computing Security Technology. In: ETRI, vol. 24, no. 4, pp. 79-88 (2009).
[19] TCG: http://www.trustedcomputinggroup.org.