World of Computer Science and Information Technology Journal (WCSIT)
ISSN: 2221-0741
Vol. 5, No. 2, 23-27, 2015

Secure Mobile Cloud Computing Based-On Fingerprint

Alaa Hussein Al-Hamami, Jalal Yousef AL-Juneidi
Department of Computer Sciences and Informatics
Amman Arab University
Amman, Jordan

Abstract—Cloud computing is a new paradigm shift of computing offers managed, scalable and secured and high available computation resources and software as a service that enables the users to access to cloud services from anywhere and anytime. Mobile Cloud Computing (MCC) refers to the availability of Cloud Computing (CC) services in a mobile environment and it is the combination of the heterogeneous fields like mobile phone device, cloud computing & wireless networks. Nowadays the term of MCC is become the buzzword and a major discussion thread in the IT world. In this paper we have designed a new effective model to solve the identification problem in MCC. The proposed solution which we have provided is based mainly on the fingerprints to prove the users identity to determine if this user is authorized or not. We combine each fingerprint with a password to form a multiple passwords scheme. The password consists from the finger sequence in the hand (left or right) plus a fixed password; this will make the passwords to be easy to remember. The results showed that this scheme is very strong and difficult to break it.

Keywords- Cloud Computing; Mobile Cloud Computing; Smart Phone Device; Fingerprint Recognition.

I. INTRODUCTION

Cloud is a new paradigm shift of computing for enabling convenient, on-demand network access to a share pool of configurable computing resources (e.g. network, service, storage, application, and service); that can be rapidly provisioned and released with minimal management effort or service provider interaction [1]. The term cloud also used often as a metaphor for the internet, and currently is further used as an abstraction of complexities .Cloud computing builds on established trends for driving the cost out of the delivery of services while increasing the speed and agility with which services are deployed. It shortens the time from sketching out application architecture to actual deployment. Cloud computing incorporates virtualization, on-demand deployment, Internet delivery of services, and open source software. Because cloud computing is available to everyone, they need to authenticate in order to ensure the entry is authorized to use cloud computing services. The term cloud also used often as a metaphor for the internet, and currently is further used as an abstraction of complexities .Cloud computing builds on established trends for driving the cost out of the delivery of services while increasing the speed and agility with which services are deployed. It shortens the time from sketching out application architecture to actual deployment. Cloud computing incorporates virtualization, on-demand deployment, Internet delivery of services, and open source software. Because cloud computing is available to everyone, they need to authenticate in order to ensure the entry is authorized to use cloud computing services.

Mobile phone devices were rare things in the early new century, but now it is very rare to find a house where there is no mobile phone, it has become a mobile device in the time of technological tools which almost never leaves its user, day or night. According to Portio Research the number of mobile phone users that will reach 7.5 billion users by the end of 2014, which means more than three quarters of the world, the mobile phone device is considered one of the most common devices in the history of technology. The mobile phone device in our time has become a key point of contact between people, as well as a key point of contact between businesses and consumers. Mobile phone devices have changed the way of communication between human beings, not only that, but also it contributed to the creation of new businesses. Because the mobile phone device has enormous capabilities in this device that is small in size, light in weight, it is not a device that sends and receives calls only, but also it has a number of amazing advantages, it is a variety of devices in a single small lightweight device.

II. CLOUD COMPUTING DEPLOYMENT

Cloud computing is classified into four basic types of cloud deployment models. They are public, private, hybrid, and community of clouds; Figure 1 shows the types of cloud computing.

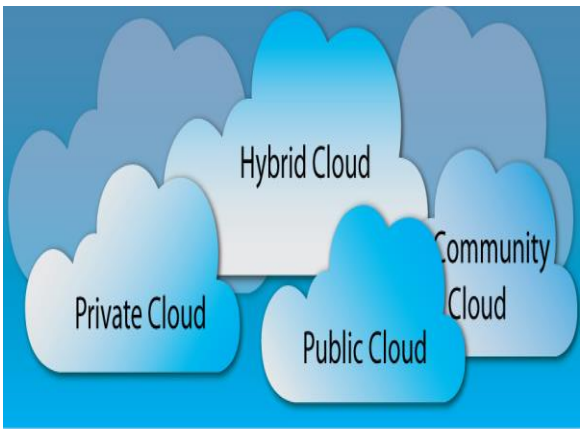

Figure 1. Types of Cloud Computing [2].

A. Public Cloud

Provide a pool of shared computing resources, applications, and storage to the customer as a single virtualized service. They generally allow you to grow or shrink these resources as needed and oftentimes provide built-in failover and redundancy. But, they are delivered (as the name suggests) publicly and in a defined fashion, so you are unable to secure your services with a private firewall or access them privately over your Wide Area Network (WAN) [3].

B. Private Cloud

Provide a dedicated instance of these services for your exclusive use and, as a result, can be secured and accessed privately. While they are housed in provider's data center, they do not leverage the pool of shared resources, so they cannot grow and shrink and do not include failover and redundancy. Private Clouds most of the times utilize the same technology (hardware, virtualization, and security) as an on-premise deployment, but they are outsourced to a service provider for hosting and care and feeding of the environment [3].

C. Hybrid Cloud

The cloud infrastructure is a combine of two or more distinct cloud infrastructure like public, private and community. That remains unique entities, but is bound together by standardized or proprietary technology that enables data and application portability. Application with less stringent security, legal, compliance and service level requirements can be outsourced to the public cloud, while keeping business-critical services and data in a secured and controlled private cloud [3].

D. Community Cloud

The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations) [3].

III. Characteristics of Cloud Computing

Cloud computing is a paradigm of computing, a new way of thinking about IT industry and it has five essential characteristics of cloud computing.

A. Scalability & Elasticity

Clients should be able to dynamically increase or decrease the amount of infrastructure resources in need, large amount of resources provisioning and deployment should be done in short time, and system behavior should remain identical in small scale or large one [1].

B. Availability & Reliability

Clients should be able to access computation resources without considering the possibility of hardware failure, Data stored in IaaS cloud should be able to be retrieved when needed without considering any natural disaster damage, and Communication capability and capacity should be maintained without considering any physical equipment shortage [1].

C. Manageability & Interoperability

Clients should be able to fully control the virtualized infrastructure resources which allocated to them, Virtualized resources can be allocated by means of system control automation process with pre-configured policy, States of all virtualized resource should be fully under monitoring, and Usage of infrastructure resources will be recorded and then billing system will convert this information to user payment [1].

D. Performance & Optimization

Physical resources should be highly utilized among different clients, Physical resources should form a large resource pool which provides high computing power through parallel processing, and Virtual infrastructure resources will be dynamically configured to an optimized deployment among physical resources [1].

E. Accessibility & Portability

Clients should be able to control, manage and access infrastructure resources in an easy way, such as the web-browser, without additional local software or hardware installation, and provided infrastructure resources should be able to be reallocated or duplicated easily [1].

IV. Mobile Cloud Computing

Mobile Cloud Computing (MCC) refers to the availability of Cloud Computing (CC) services in a mobile environment; Figure 2 shows mobile cloud computing Architecture. It incorporates the elements of mobile networks and cloud computing, thereby providing optimal services for mobile users. In MCC, mobile devices do not need a powerful configuration (e.g., CPU speed and memory capacity) since all the data and complicated computing modules can be processed in the cloud [4].

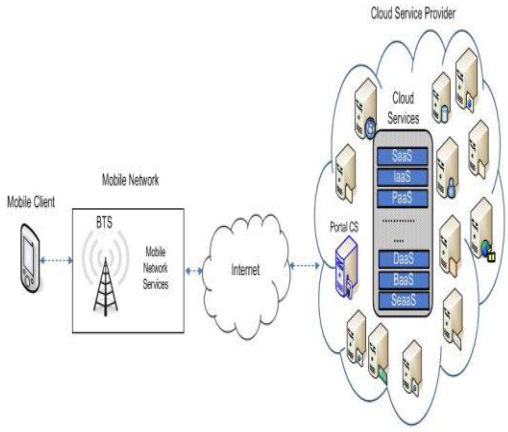

Figure 2. Mobile Cloud Computing Architecture [3].

In MCC the users can get all the CC services in his or her mobile devices through internet. Mobile cloud merged the elements of mobile networks and cloud computing, thereby providing the optimal services for mobile users. Mobile cloud computing which combines mobile computing and cloud computing, has become one of the industry buzz words and a major discussion thread in the IT world. And according to ABI Research [6], "By 2015, more than 240 million business customers will be leveraging cloud computing services through mobile devices, driving revenues of $5.2 billion". It must be noted that there were only 42.8 million MCC subscribers in 2008 [6]. This underlines the end mobile device user will eventually be the benefactor of the MCC. Company users can share resources and applications without a high level of capital expenditure on hardware and software resources. Nature of cloud applications also is advantageous for users since they do not need to have very technical hardware to run applications as these computing operations are run within the cloud. This reduces the price of mobile computing to the end users. They could see a huge number of new features enhancing their phones due to MCC. At the same time the developers also have real advantages from mobile cloud computing. The largest benefit of cloud computing for developers is access to a broader audience of a wide range of mobile subscribers. Since cloud computing applications go through a browser, the end user's mobile operating system does not have any impact on the application. Along with the plethora of benefits, there are a large number of issues to be addressed and unsolved problems to be solved. Several challenges such as the dependency on continuous network connections, data sharing applications and collaboration, and security another key challenge for MCC is network availability and intermittency. Also MCC concepts rely on an always-on connectivity and will need to provide a scalable and high quality mobile access.

V. MOBILE CLOUD COMPUTING SECURITY

Provide secure use for mobile cloud computing user's consider one of the key issues most cloud providers are given attention. Since mobile cloud computing is a combination of mobile networks and cloud computing, the security related issues are then divided into two categories: Mobile network user's security; and cloud security. Because of the large number of cloud computing users and because of the abundance of information on cloud it must control the process of access to the cloud computing to prevent any illegal access to the cloud.

VI. RELATED WORKS

A. *Akhil Kaushik & et al*

Have proposed three different methods to safely and easily login to a cloud service using one time password with the user's mobile phone as an authentication device. Furthermore, three different suggestions that are secure and easy to use for registering new users to the cloud service have been made. The best encryption algorithm to use in cloud services with respect to security and speed has been evaluated. The Suggestion ended up in a working solution that uses one time password authentication in a mobile for the login procedure, a very safe registration system and with all traffic transmissions encrypted with RC4 [7].

B. *Thamba Meshach & et al*

Have proposed authenticated key exchange scheme, namely Mobile Cloud Key Exchange (MCKE), which aimed at efficient security-aware scheduling of scientific applications? The scheme has been designed based on the commonly-used Internet Key Exchange (IKE) scheme and randomness-reuse strategy, both theoretical analyses and simulation results have demonstrated that. Compared with the IKE scheme, the MCKE scheme has significantly improved the efficiency by dramatically reducing time consumption and computation load with the same level of security [8].

VII. THE PROPOSED SYSTEM

In this paper we have designed a new efficient model, this model scans all the user's fingerprints with their password which is considered a new and good idea because it will provide more security to the mobile cloud computing. In this model the user can choose any fingerprint and its password he wants in order to authenticate himself on the mobile cloud computing where the suggested solution goes by saving the fingerprints for the authorized users with a password for each fingerprint, and in this case we need ten passwords, where each password represents the location of the finger in the hand, and in our system the fingerprints are read beginning with the left hand from the pinky finger whose location is " 1" to the thumb whose location is " 5", after that we begin with the thumb in the right hand, so that the location of the thumb is "6", and so on until we reach the last finger in the right hand whose location is "10"; Figure3 shows the password fingerprint .

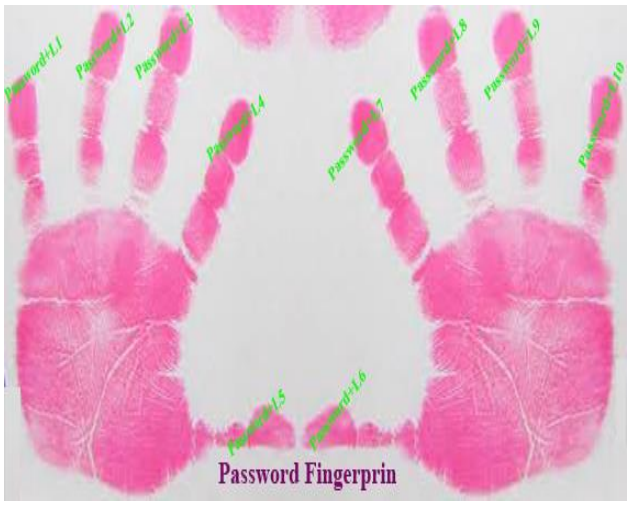

Figure 3. Fingerprint Password.

The problem of remembering the passwords is solved through putting one password accompanied with the location of the finger so that they will be remembered easily. This way is considered to be effective because it provides us with multiple passwords that are easily remembered by the authorized user and difficult to remember by the unauthorized one. For example: if the user's original password is (Jalaljuneidi), then the fingerprint's password will be (JalaljuneidiL1) where L refers to the left hand and number 1 refers to the finger's order in the left hand. Then, the scan fingerprint along with its password are sent and stored in the database in the cloud computing server, where the matching process is performed later between the stored fingerprint and the fingerprint that will be used by the user who wants to access the account on the cloud computing through a mobile phone device. When the user wants to access the account, he/she must enter the defined password of the proposed model, and then the fingerprint will be entered with its password. If the password of the read fingerprint is valid, the application will match it with the previously stored one in the database. If both fingerprints are matched, the user will be authorized to access the cloud computing and can get benefit from the cloud computing utilities; Figure 4 shows the proposed solution. In this paper, we will use the basic fingerprint algorithms, one for fingerprint orientation, another is for the fingerprint feature extraction and the last is for the matching process. Our system consist of two stages the first one is store the fingerprints in the cloud server's database and the second stage matching the fingerprints with the fingerprints that were previously stored in the cloud server's database.

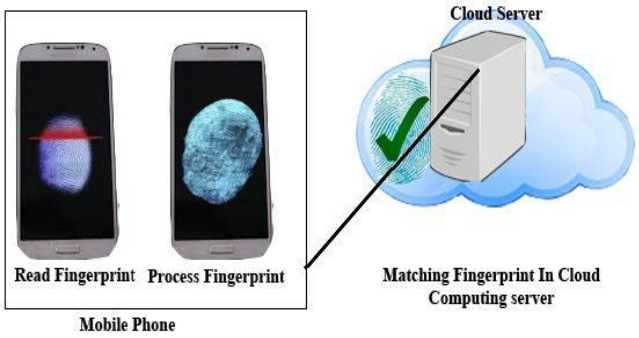

Figure 4. Fingerprint Authentication Model.

A. Store the fingerprints in the cloud server's database

In this stage the user will be registered by entering username and password, then the user must scan all the fingerprints with password for each fingerprint (fingerprint password is the original password plus the location of the finger in the user's hand). After that the fingerprint features with its passwords will be send to the database to store it for the next stage, then the system set sign as registered user to distinguish later between the new user and registered user.

B. Matching the fingerprints with the fingerprints that were previously stored in the cloud server's database

In this stage the user must enter the password to open the mobile device, then must enter the username and fingerprint password, then in the second level the user must enter the fingerprint password and if it is valid the user will go to the next level and if it is wrong the user will be rejected because the user is un authorized. If the user entered valid fingerprint password, then he/she must send fingerprint by special sensor that is located on mobile phone devise. After the user fingerprint has been read and send to the date base, the system will match it with the fingerprint that was previously stored in the cloud server's data base and if the matching is ok, the user will be considered as authorized and any process can be done on the cloud account. User at this stage can be either authorized or unauthorized.

Authorized User

The user in this stage can choose any fingerprint he wants of his ten finger prints so that he can verify his identity on the mobile cloud computing, and he should also put the password for the fingerprint that e chooses, after that the entered user's fingerprint is matched with his ten previously saved fingerprints. And if it is matched successfully, the user will be able to access the mobile cloud computing services.

unauthorized User

The unauthorized user is a person who doesn't know the system at all, and if he succeeds in entering the password correctly, he will still have to enter his fingerprint. The system

will match the user's entered fingerprint with the previously saved fingerprints of the user. Then the system will prevent him from accessing the mobile cloud computing because of the lack of matching between the entered fingerprint and the saved ones.

VIII. CONCLUSION

In this paper we have explained the concepts of mobile cloud computing, and we have presented the benefits, services, deployment, properties and characteristics of cloud computing and security issue related to it. Furthermore, we have clarified the concepts of mobile phone device, phone service, benefits and mobile security of mobile phone device. On the other hand, we have explained the concept of authentication and the methods of authentication. Also, we have cleared the concepts of fingerprint authentications and Fingerprint image preprocessing. And we have designed a new efficient model for mobile cloud computing based on fingerprint, the implemented model works on storage all the user's fingerprints with their password on cloud server, when them want to access the cloud computing through mobile phone device they most scan any one of their fingerprints and its password.

IX. FUTURE WORKS

Mobile cloud computing is considered a new technology, and as previously known, a new technology brings new threats and because perfect security does not exist, we suggest a group of ideas for future works on mobile cloud computing.

Use eye iris recognition to identify the authorized user, because this method is more rigid.

Improve the detection process for fingerprint through raising the ability to read the low resolution fingerprints.

Enhance the detection process through recognize the cuts, paints, or any obstacle for recognition.

Make the completion of the process of matching fingerprints inside Mobile phone device instead of cloud computing server.

ACKNOWLEDGMENT

I want to thank ALLAH for his blessings that help me achieve this paper. I would like to thank Prof. Dr. Alaa H Al-Hamami who supported and helped me to complete this paper and because he was always available when I needed his assistance. I would like to thank my brother in-low Mohammed Saleh AL-Juneidi for his assistance.

REFERENCE

[1] NIST (National Institute of Standards and Technology). http://csrc.nist.gov/groups/SNS/cloud-computing, Retrieved on 14/11/2014.

[2] http://www.atomrain.com/it/technology/cloud-deployment-models, Retrieved on 21/4/2014.

[3] k. Soeung and W. K. Sung, " Mobile Cloud Computing Security Considerations,"journal of security engineering, January 2012.

[4] D. C. Ronnie and L. Sunguk," Security Considerations for Public Mobile Cloud Computing," International Journal of Advanced Science and Technology Vol. 44, July, 2012.

[5] W. Minjuan, C. Yong and J. K. Muhammad, " Mobile Cloud Learning for Higher Education: A Case Study of Moodle in the Cloud," the international review of research in open and distance learning, vol 15 no 2, April 2012.

[6] ABI Research. http://www.abiresearch.com, Retrieved on 15/4/2014.

[7] K .Akhil, O. A. Hari, G. Kirtika and G. Sakshi, " Secure Authentication with Encryption Technique for Mobile on Cloud Computing," International Journal of Scientific Research Engineering & Technology (IJSRET), Volume 1 Issue 5 pp 028-033, August 2012.

[8] M. W. Thamba and B. K. Suresh, " Secured and Efficient Authentication Scheme for Mobile Cloud," International Journal of Innovations in Engineering and Technology (IJIET), Vol. 2 Issue, February, 2013.

AUTHOR PROFILES

Prof. Dr. Alaa Hussein Al-Hamami

Dean of Computer Sciences and Informatics College

Amman Arab University

http://profalaa.weebly.com

Alaa Al-Hamami is presently Professor of Database Security and Dean of Computer Sciences and Informatics College, Amman Arab University, Jordan. He is a reviewer for several national and international journals and a keynote speaker for many conferences. He is supervising a lot of PhD, Msc, and Diploma thesis. His research is focused on Distributed Databases, Data warehouse, Data Mining, Cryptography, Steganography, and Network Security. Dr. Al-Hamami published fourteen Books in Computer Philosophy and other Computer topics in addition to several chapters in IGI and Springer publications. He is Chief Editor and Editor for several Magazines in addition to his participation in project research evaluations.

Mr. Jalal AL-Juneidi

Mr. Jalal AL-Juneidi has a Diploma in Information Technology , Al-Balqa Applied University /Al-husson University College, 2004. BSc. in Computer Science, 2005, College of Science, University of jerash, Jordanand his MSc. in Computer Science from College of Computer Sciences and Informatics, 2014, Amman Arab University, Jordan. Mr AL-Juneidi joined the ministry of education as an IT experter for from 2005 till now and as a lecturer.