Cloud Computing Security Enhancement by Using Mobile PIN Code

Basim Alhadidi[1]*, Zahraa Arabeyat[1], Fesal Alzyoud[1], Ali Alkhwaldeh[2]

[1] Al-Balqa' Applied University, Prince Abullah Bin Ghazi Faculty of Information Technology, Salt, Jordan.
[2] Philadelphia University, Faculty of Engineering, Amman, Jordan.

* Corresponding author. Tel.:+962-77-5432241; email: hadidi72@hotmail.com
Manuscript submitted February 10, 2015; accepted May 8, 2015.
doi: 10.17706/jcp.11.3.225-231

Abstract: The proliferation of internet users is increasing rapidly as a result of network growth in technology (wired and wireless) in recent years, cloud computing services has gained attention in the scientific and industrial communities. Cloud computing provides a flexible and cost effective services for consumers and companies through offering services, resources and infrastructure for providers. Cloud computing is a sub-domain of computer network so security issues are a challenge for cloud computing spread, there are many security issues and concerns appear while using cloud services. Protecting data from threats and attacks is the most challenging tasks nowadays, since people and companies stores confidential data in the cloud. The purpose of this paper is focus on granting and authenticating data, while these data are transferred over cloud to gain the trust from the provider.

Key words: Cloud computing, PIN code, security, mobile computing.

1. Introduction

Cloud computing is an internet techniques that uses central remote servers to keep, stores data and applications. Cloud computing enables consumers and firms' employees to use applications without the needs to install special software's, this technology allows more efficient computing by centralizing storage, memory, processing and bandwidth [1]. Cloud computing allows delivering hosted services over the Internet by using software that is installed on computer based on client-side. Cloud computing can be summarized by three segments: applications, storages, and connectivity, Cloud computing is independent computing as it is totally different from grid and utility computing, an example of cloud computing is Google Apps, it enables to access services via the browser and deployed on millions of machines over the Internet [2]. The architecture of cloud computing can be classified to three types of models' services, namely Infrastructure as a service (IaaS), Software as a Service (SaaS) and Patform as A Service (PaaS) [3]-[5].

1.1. Cloud Services Models

Cloud Computing includes software and hardware, the system software refers to the applications which are delivered over the Internet, while the hardware include all the physical components in client and server sides [6]. Cloud computing can be categorized to three types with respect to the service model: Infrastructure-as-a-Service (IaaS), Platformas-a-Service (PaaS) and Software-as-a-Service (SaaS)[9].

1.1.1. Infrastructure-as-a-Service (IaaS)

It is base layer of the cloud stack and serves as a foundation for the other two layers. This type of services distributes a full computer infrastructure via the web or Internet. Most popular provider of IaaS like Amazon Web Services, it offers virtual server instances with unique IP addresses and block of storage on demand. [3], this service minimizes the initial investment in computing hardware such as servers, networking devices and processing power.

1.1.2. Platform-as-a-Service (PaaS)

It is defined as a set of product development tools and software that is hosted on the provider infrastructure; this service helps the consumer to deploy his own applications without installing any platform or tools on their machines [10].

1.1.3. Software-as-a-Service (SaaS)

In this model, the vendor supplies the software product, the hardware infrastructure and interacts with the user through front end portal; the applications are accessed through s thin client interface such as web-based email.

Cloud computing technology uses large pools of resources that are connected through private or public networks. Cloud computing provides its services according to the previous mentioned models as described in Fig. 1. This technology simplifies infrastructure planning and provides dynamically scalable infrastructure for cloud based applications, data, and file storage. Businesses can choose to deploy applications on Public, Private, Hybrid clouds or the newer Community Cloud [7].

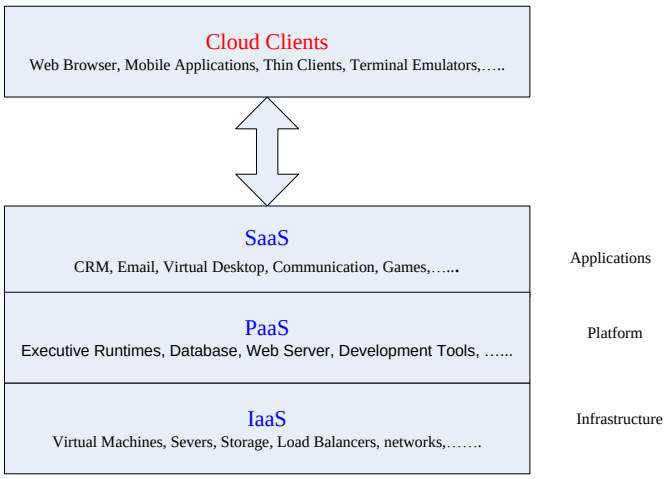

Fig. 1. Cloud computing layers [8].

1.2. Cloud Computing Types

Cloud computing can be categorized according to the subscribe user depending on his needs. As a home user or small business owner, home user will most likely use public cloud services.

1.2.1. Public cloud

It is based on the standard cloud computing model, where a service provider makes resources (such as applications) available to all general public over the Internet. Public cloud may be free or offered on a pay-per-usage model. A public cloud can be accessed by any subscriber with an internet connection and access to the cloud space. Public cloud service has the following benefits:

1) Inexpensive and easy setup because of hardware.
2) Scalability to meet needs.
3) You pay for what you use, so there no wasted resources.

1.2.2. Private cloud

It consists of virtual machines or application in a company that own set of hosts. They provide benefits of shared hardware costs, the ability to recover from failure and the ability of scaling up or down depending upon demand. It provides hosted services to a limit number of people behind a firewall. A private cloud is established for a specific group or organization and limits access to just that group.

1.2.3. Community cloud

It is shared among two or more organizations that have similar cloud requirements. This will help in limiting the capital costs for its establishment as the costs are shared among the organizations. The operation may be in house or with a third party on the premises.

1.2.4. Hybrid cloud

It is multiple cloud systems that connected in a way to allows programs and data to be a moved easily from one deployment system to another. It's also can be defined as a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together. A hybrid cloud is essentially a combination of at least two clouds, where the clouds included are a mixture of public, private, or community. Hybrid clouds are useful for archiving, allowing local data to be replicated to a public cloud.

2. Challenges of Cloud Computing

Converting the IT infrastructure for enterprises and firms into cloud computing is a cheap solution, but unfortunately Small to Medium Enterprises (SMEs) and the large enterprises face potential problems that delay the adoption of cloud computing [11].

2.1. Privacy and Security of Data

Cloud computing uses data and resources that are distributed among different clients, so privacy and security of data face sever threats and vulnerability. Threat can be defined as a potential attach that may lead to a misuse of information and resources, while vulnerability refers to the flaws in a system that allows an attack to be successful [12]. In SaaS, data of organizations is often processed and stored as a plaintext in the cloud, but this will produce security issues [13]. PaaS security composites of platform security and customer's deployed applications [14], PaaS inherits smashups security such as data network security. In IaaS, the cloud users have better control and security than other models as there is no vacation in virtual machines, they control all the security policies correctly [15].

2.2. Costing and Continuously Evolving

The main cost of cloud computing depends on in information security management which includes: the costs of migrating, implementing, integrating, training, and redesigning. Also it includes the cost of training supporting people in the new processes [16]. Cloud consumers consider the tradeoffs amongst integration, computation and communication. The customer needs saving money on buying hardware and staffing to maintain it. User requirements are continuously evolving, as are the requirements for networking, storage and interfaces. This means that public cloud does not remain static and is also continuously evolving.

3. Security Issues and Solutions in Cloud Computing

Adapting cloud computing in organizations produces different risks than traditional IT solutions. Unfortunately, integrating security into these solutions make them more rigid [17]. In this section we will concentrate on the Security challenge and suggest an enhancement for more secure cloud computing. Since the consumers and providers need to send data and services over cloud with a high security concerns, they need to do that in safe data transmission. Also they need to give a very secure authentication method to guarantee the safety of data. All sectors are migrating to cloud computing because IT costs can be cut, it reduces capital expenses, and is a viable option to modernize legacy systems.

3.1. Authentication

Trust in a cloud computing relies on the selected deployment model, as the governance of data and applications is outsourced and delegated out of the owner's strict control. In traditional architectures, trust was enforced by an efficient security policy and flow among participants. In a cloud deployment, this perception is totally obscured.

Cloud service providers request customers to store their account information in the cloud, cloud service providers have the access to this information. This presents a privacy issue to the customer's privacy information. When a customer decide to use multiple cloud service, the customer will have to store his/her password in multiple cloud, the more cloud service the customer is subscript to, the more copy of the user's information. this will lead to multiple authentication processes. For every cloud service, the customer needs to exchange his/her authentication information. These redundant actions may lead to an exploit of the authentication mechanism. Cloud service providers use different authentication technologies for authenticating users, this may have less impact on SaaS than PaaS and IaaS, but it is present a challenge to the customers. Authentication is the act of creating or validating something (or someone) as authentic and claims made about the topic are true.

Many different ways are used in cloud services to gain authentication for users. One of the most common ways is to login at the cloud provider's web page through a web browser to gain access to privileges and services associated with that user. Login process in usual contains two information username and password [18].

The main authentication used is Two Factor Authentication, in this type of authentication user has to provide two main terms to get authentication to him. For example, when a user login to webpage he share his password and a series of random numbers generated from authentication device.

3.2. Static Passwords

A static password is the usual way that users authenticate when login to a service is needed. The password is usually a secret word picked by the user and it may contain letters, numbers or special characters. Many weaknesses are existed in static passwords, if the password is too simple it will be exposed by different types of threats such as Trojans, social engineering. When user choose hard password it will be very hard to remember, this lead to writing it on a piece of paper, which will be a big security risk. Passwords remain the most familiar and commonly-used form of user authentication in organizational settings, in spite the growing number of graphical and biometric authentication mechanisms [19].

Passwords are used by almost all business applications for authentication. However static passwords have many drawbacks e.g. passwords can get hacked. It is recommended to move to dynamic password scheme like One Time Passwords or OTP [20]. OTP give more secure environment than static passwords as there are no chances to forget or reuse passwords. Each time a new password is generated for each login session. Authentication by one time passwords are more reliable and user friendly as well. OTP generation can be done by various OTP generation algorithms for generating strings of passwords, OTP offering a strong authentication by using two-factors: user name and a device name [21].

4. Proposed Solution for Static Password over Cloud Computing

Authentication solution must be strong, simple to integrate with the existing infrastructure and easy to deploy and manage. In this paper a proposed solution which is based on authentication over mobile by using One Time Password (OTP) concept will be proposed, the proposed solution will be described in this section; mobile device will be used as authentication device, user have to enter the PIN code to generate a One Time password that can be used for login process.

1) A user needs to login to his/her personal account through a web browser.
2) The user starts an application on a mobile phone then enters a PIN code.
3) After that an One Time Password is generated and displayed on the phone.
4) The user enters his/her username and the One Time Password at the login page, and sends the information to the authentication server.
5) A permission access will be given to the user or the access will be denied.

This solution offers more security on cloud services since it's only send the username and one time password , and it save the cost by making the mobile device as same as authentication device. Fig. 2 shows Authentication System Using One Time Password.

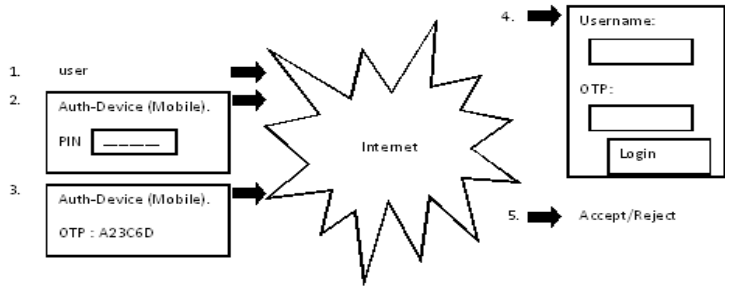

Fig. 2. Authentication using one time password.

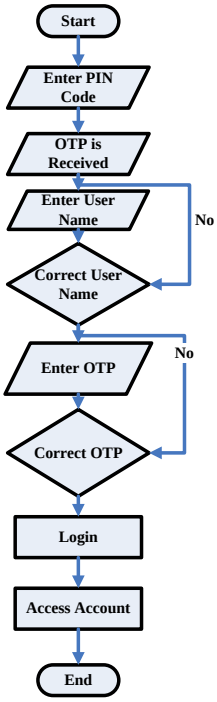

Fig. 3. Flowchart for authentication using one time password.

The proposed solution depends on using one time password to overcome the drawbacks of key security consideration. The authentication process starts by entering the pin code which is unique, and then the user has to enter his user name if it is correct the system will ask him to enter his OTP, if user name and OTP are correct the user can enter his account as described in the authentication flowchart depicted in Fig. 3.

5. Conclusion

Cloud computing is a promising technology with profound implications not only for Internet services but also for the IT sector as a whole. Unfortunate, several obstacles issues are exist; particularly these issues are related to service-level agreements (SLA), security and privacy, and power efficiency. This paper tested the

current security over cloud services. Modify technique have been proposed for more secure authentication regarding cloud services, the proposed solution is based on time password through using the mobile PIN code and username. The traditional way used static passwords to let user get access to their accounts. In this paper One Time Passport is proposed as a new technique to get authentication over cloud services, this solution is more secure and easy to deploy.

Acknowledgment

Authors would like to thank to the Scientific Research Deanship at Abalqa' Applied University and Philadelphia University for encouragement of research and researchers at both the universities.

References

[1] Karwasra, N., & Sharma, M. (2012) Cloud computing: security risks and its future. *International Journal of Computer Science and Computer Engineering*, *Special Issues on Emerging Trends in Engineering*, 5-9.

[2] Shaikh, F. B., & Haider, S., (2011, December 11-14) Security threats in cloud computing. *Proceedings of 6th International Conference on Internet Technology and Security Transaction* (pp. 214-219). Abu Dhabi, United Arab Emirates (UAE).

[3] Subashini, S., & Kavitha, V., (2011) A Survey on security issues in service delivery models of cloud computing. *J Netw Comput. Appl., 34(1)*, 1-11.

[4] Mell, P., & Grance, T., (2011) The NIST dewfinition of cloud computing. NIST. *Special Publication 800-145*, Gaithersburg, MD.

[5] Zhang, Q., Cheng, L., & Boutaba, R., (2010) Cloud computing: State-of-the-art and research challenges. *Journal of Internet Services Applications, 1(1)*, 7-18.

[6] Armburst, M., Rabkin, A., Zaharia, M., *et al*. (2009) Above the clouds: A berkeley view of cloud computing. UC Berkeley Reliable Adaptive Distributed Systems Laboratory.

[7] Cattteddu, D., & Hogben, G., (2009) Cloud computing: Benefits, risks and recommendations for information security. From http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment

[8] Voorsluys, W., Broberg, J., & Buyya, R. (February 2011). Introduction to cloud computing. In R. Buyya, J. Broberg, A. Goscinski (Eds.), *Cloud Computing: Principles and Paradigms* (pp. 1–44). New York, USA: Wiley Press.

[9] Catteddu, D. Cloud computing: Benefits, risks and recommendations for information security. *Communications in Computer and Information Science*, *72*, 17.

[10] Islam, M. M., Morshed, S., & Goswam, P. (July 2013). Cloud computing: a survey on its limitations and potential solutions. *IJCSI International Journal of Computer Science Issues*, *10(2)*, 159-163.

[11] Durkee, D. (2010). Why cloud computing will never be free. *Communications of the ACM*, *53(5)*, 62-69.

[12] Hashizume, K., Rosado, G. D., Fernandez-Medina, E., & Ferandez, B. E. (2013). An analysis of security issues for cloud computing. *Journal of Internet Services and Applications*, *a SpringerOpen Journal*, *4(5)*, 1-13.

[13] Ju, J., Wang, Y., Fu, J., Wu, J., & Lin, Z., (2010) Research on key technology in SaaS. *Proceedings of International Conference on Intelligent Computing and Cognitive Informatics* (pp. 384-387). Hangzhou, China, IEEE Computer Society, Washington, DC, USA.

[14] Mather, T., Kumaraswany, S., & Latif, S. (2009). *Cloud Security and Privacy*. O'Reilly Media, Inc, Sebastopol, CA.

[15] Jaeger T, & Schiffman, J. (2010). Outlook: Cloudy with a chance of security challenges and improvements. *IEEE Security Privacy, 8(1)*, 77-80.

[16] Anthony, B., & Syed, M. R. (January 2011). An overview of the security concerns in enterprise cloud computing. *International Journal of Network Security & Its Applications (IJNSA)*, *3(1)*, 30-45.

[17] Cloud Security Alliance. (2011). Security guidance for critical areas of focus in cloud computing, V3.0. From https://cloudsecurityalliance.org/guidanc/csaguide.v3.0.pdf

[18] National Institute of Science and Technology NIST Special Publication 800-118: Guide to Enterprise Password Management (Draft): Recommendations of the National Institute of Standards and Technology. (2009). From: http://csrc.nist.gov/publications/drafts/800-118/draftsp800-118.pdf.

[19] Philip, G. I., & Sasse, M. A. (2010). The true cost of unusable password policies: password use in the wild. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 383-392).

[20] Hsieh, W. B., & Leu, J. S., (2011). Design of a time and location based one time password authentication scheme. *Proceedings of 7th IEEE International Conference*.

[21] Chowdhary, R., & Rawat, S., (2013). One time password for multi-cloud environment. *International Journal of Advanced Research in Computer Science and Software Engineering*, *3(3)*, 595-597.

Basim Alhadidi Was born in Jordan in June 1972. He earned his Ph.D in 2000, in engineering science (computers, systems and networks). He received his M.Sc in 1996 in engineering science (computer and intellectual systems and networks). He is presently a professor at the Computer information Systems Department at Al-Balqa' Applied University, Jordan. Prof. Alhadidi published many research papers in many topics such as computer networks, image processing, and artificial intelligence. He is a reviewer for several journals and conferences. He was appointed in many conferences as keynote speaker, reviewer, track chair and track co-chair.

Zahraa Arabeyat earned her M.Sc in 2014 in computer science from Al-Balqa' Applied University. She is presently a lecturer at the Computer Science Department at Al-Balqa' Applied University, Jordan.

Faisal Y. Alzyoud received his Ph.D with honority in computer networks from Universiti Sains Malaysia in June 2011 with the thesis entitled "XCAST based routing protocol for push-to-talk applications in MANETs". He received his B.Sc from Jordan University in engineering and M.Sc in information system from The Arab Academy for Banking and Financial Sciences in 2004. Faisal's research interests are in the field of wireless networks, ad hoc networks, multicast and multicast for small group, QoS and real time applications. Dr. Alzyoud works as a lecturer at Al-Balqa Applied University and as a part time lecturer in other universities, he is a fluent speaker of Arabic, English and Malay languages.

Ali Alkhwaldeh received his Ph.D with a excellent degree in computer networks engineering from University of HTYY "KPI", Ukraine in 2006, he received his B.Sc and M.Sc degrees in computer engineering from the same university in 1998 and 1999 respectively. Dr. Al-Khawaldeh research interests are in the field of wireless networks, embedded system design, and programming algorithmic design. Dr. Al-Khawaldeh works as a staff member at the Computer Engineering Department, Faculty of engineering, Philadelphia University; he is a fluent speaker of Arabic, English and Russian languages.