Journal of Basic and Applied Engineering Research
p-ISSN: 2350-0077; e-ISSN: 2350-0255; Volume 2, Issue 23; October-December, 2015, pp. 1994-1996

http://www.krishisanskriti.org/Publication.html

Mobile and Cloud Data Security Issues, Challenges and Preventive Measures

Mayank Jain[1] and Aquil Ahmad Khan[2]

[1,2]ICERT, New Delhi
E-mail: [1]engineermayankjain@gmail.com, [2]akhan2786@gmail.com

Abstract—*The fast pace of modern life, accelerated business processes and decision making, have all created the need for fast and reliable access to data and information. Mobile devices, which have become ubiquitous, offer easy connections to the world of information. The Cloud Computing is from one of the most widely and popularly technologies that are used today. Mobile and Cloud Computing is in the favour of a new system in the field of mobile world. Now we have data moving across a multiplicity of devices, including tablets, smartphones and even wearable devices as people use their smart watches to notify them of company phone calls, SMSs and so forth. Cloud Computing is from one of the most widely and popularly technologies that are used today. Mobile and Cloud Computing is in favour of a new system in the field of the mobile world. The uses of the computational resources on pay per use models a lot of business is growing. The Data security issues and challenges focusing on the computing and service delivery types are shown in this paper and also present the various ways of preventing the Data security issues.*

Keywords: *Mobile and Cloud data; Cloud Computing; Private, Public & Hybrid Cloud; Data Security.*

1. INTRODUCTION

Cloud Computing means much more data flowing from devices to servers, servers to devices, sensors to devices and devices to devices. A good deal of that data will be business-generated information and needs to be kept confidential or have restricted access. Mobile devices generally connect over wireless networks rather than wired Ethernet, which requires additional security and exposure. Mobile applications are highly connected to web services and this broadens the possible vectors for data exfiltration. And above all this, there's cloud.

More and more companies, however, are moving their data as well as their applications to cloud services providers. In these type of cases, you may not know exactly what security measures are being implemented to protect that data and what is the physical location of the data is. From security point of view, it makes sense for the cloud services providers to keep that information under wraps. Making the move to the cloud requires placing our data in the hands of the cloud services providers, which means it involves trusting that the cloud services providers will protect it.

2. BASICS OF CLOUD COMPUTING

Cloud computing is an easy way of storing and accessing data and programs over the Internet without using up your own device internal data. Cloud is just for enhancing the usability of the Internet. It is a process of delivering/enabling scalable, expandable and almost perfectly elastic software services to an organization's computers and devices through the Internet technologies.

3. PROTECTING MOBILE AND CLOUDE DATA

There are many ways to protecting data that has "gone mobile" or is stored in the cloud is same as protecting data in on-premises data centre.

Encryption

Encrypting the data adds another level of protection and is the best way to protect data. Mobile data needs to be protected while at rest on the device and while in transit across the Internet. Web-based data traffic is usually encrypted using Transport Layer Security (TLS), which is the newer iteration of Secure Sockets Layer (SSL). Non-web data can be encrypted using VPN protocols such as IP sec or SSH tunnelling. Email can be encrypted using S/MIME or PGP.

Authentication

The first step in protecting data is to verify the identity of the person who is attempting to access it. With sensitive mobile data, traditional username and password authentication isn't enough. Multi-factor authentication provides stronger protection and today's mobile devices support many forms of authentication; including fingerprint scanners, pattern recognition etc.

Containerized applications

Containerization is a big trend these days and goes hand-in-hand with cloud computing. Containerized applications can create a private corporate workspace on a user's personally owned device so they get access to the corporate data and apps with enterprise-grade security without any requirements of dependencies'.

Authorization and access controls

Once identity has been established, the system must be able to determine which data files that user is allowed to open and what level of access he/she can have (read only, modify, delete, etc.). This is done by making some alterations in permissions, privileges and user rights.

Virtual private networks

VPN protocols such as SSL or IPsec encrypt the transmission of data between the remote user and the corporate network, and most companies support VPN connections.

Mobile Device Management (MDM) and Mobile Application Management (MAM)

A MDM system allows you to create and apply policy-based security to all of the mobile devices that access your company network, manage certificates and keys, monitoring device health and security status, track usage and access, control access to data, and even lock or remote wiping a device if it's lost or stolen. MAM helps you keep mobile apps updated and configured correctly for best security which makes the data they generate and store more secure.

User education

Ensure that mobile users are aware of your best security practices and understood how to apply them. One of the most important aspects of training is encouraging them to not jailbreak devices. Jail breaking lets users override devices application protections to download non-approved, non-supported apps, which can make devices more vulnerable to malware and other attacks.

Educate yourself

When selecting a cloud services provider, be sure to read the user agreement regarding the storage of data and ask questions of you have concerns. Ensure that your Cloud Service Provider encrypts stored data.

Data classification

Such classification allows you to evaluate whether some of your data may not be appropriate for cloud storage because of its sensitivity or regulatory requirements.

Back it up

Ensure that data can be restored after a device is damaged, wiped or lost, by taking advantage of data backup capabilities supported by each mobile OS. Best practices include passcode-protecting access to backup files and cloud storage, encrypting those backups wherever possible and preventing business data from being backed up to personal storage areas.

4. CONCLUSION

Mobile cloud computing contains two factors by the combination of mobile network and cloud computing. Using the mobile network, all the data or computation is being transferred to the cloud and cloud stores that data in its storage and if any computation task arrives which smartphones is not capable of executing due to lack of battery power and resources in mobile phones then it is transferred to resourceful cloud which does the execution. Mobile cloud computing is platform having largest scope in the future because it combines the advantages of both Mobile Cloud and Cloud Computing, thereby providing optimal services for mobile users.

In the field of computing, Mobile Cloud Computing has brought a new dimension to Networking Service. The main moto of this service is to interconnect Mobile Cloud where application providers and enterprises will be able to access valuable network and billing capabilities across multiple networks, making it easy for them to enrich their services whether these applications run on a mobile device, in the web, in a SaaS Cloud, on the desktop or an enterprise server.

In this article an overview on mobile cloud computing in which its definitions, architecture, and advantages have been presented. This paper contains the security issues and preventive measures concerning mobile cloud computing, which help us to study and analyse various security issues and their preventive measures in mobile cloud computing.

REFERENCES

[1] A. Liu, Y. Yuan, A Stavrou, “SQLProb: A Proxy based Architecture towards Preventing SQL Injection Attacks”, SAC March 8-12, 2009,Honolulu, Hawaii, U.S.A.

[2] Mell Peter, Grance Timothy “The NIST Definition of Cloud Computing” NIST Special Publication 800-145 in September 2011.

[3] Gupta Pragya, Gupta Sudha” Mobile Cloud Computing: The Future of Cloud” International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering Vol. 1, Issue 3, September 2012, pp. 134145.

[4] Hoang T. Dinh, Chonho Lee, Dusit Niyato* and Ping Wang,” A survey of mobile cloud computing: architecture, applications, and approaches”,Wiley Online Library (wileyonlinelibrary.com), 11 October 2011, DOI: 10.1002/wcm.1203.

[5] Seny Kamara, Kristin Lauter, “Cryptographic cloud storage”, Lecture Notes in Computer Science, Financial Cryptography and Data Security, pp. 136-149, vol. 60 54, 2010.

[6] Mohamed Al Morsy, John Grundy and Ingo Müller,” An Analysis of The Cloud Computing Security Problem”, Proceedings of APSEC 2010 Cloud Workshop, Sydney, Australia, 30th Nov 2010.

[7] Cloud security alliance: Security guidance for critical areas of focus in cloud computing v2.1, Dec 2009.
[8] E. Nurmi, R. Wolski, C. Grzegorczyk, G. Obertelli, S. Soman, L. Youseff, and D. Zagorodnov, "The Eucalyptus Open-Source CloudComputing System," Cluster Computing and the Grid, IEEE International Symposium on, vol. 0, pp. 124–131, 2009.
[9] T. Garfinkel and M. Rosenblum, "When virtual is harder than real:security challenges in virtual machine based computing environments," Proceedings of the 10th conference on Hot Topics in Operating Systems –Volume 10, 2005.
[10] YanivBalmas"Mobile Network Security Availability risks in mobile networks" , ERT Lab Security Researcher November 2013.
[11] White Paper. Mobile Cloud Computing Solution Brief. AEPONA, 2010.
[12] BhavyaSareen, Sugandha Sharma and MayankArora Department of CSE CGC, Gharuan Chandigarh, India "Mobile Cloud Computing Security as a Service using Android".
[13] D. Gollmann, "Securing Web Applications",Information Security Technical Report, vol. 13, issue. 1, 2008, Elsevier Advanced Technology Publications Oxford, UK.