Cloud Computing on Mobile Devices: Security Issues

Hardayal Singh Shekhawat
Associate Professor (IT), Govt. Engineering College, Bikaner, (India)
Research Scholar: Suresh Gyan Vihar University, Jaipur, (India)
shekhawat.hardayal@gmail.com

***Abstract*— In This paper we have discussed major security issues of cloud computing on mobile devices. Today's modern mobile devices like smart phones, PDA, Tablet PCs etc are progressing to approach the capabilities and extensibility of standard desktop personal computers. These mobile devices operate independently of each other, using only local computing, sensing, networking, and storage capabilities and functions provided by remote Internet services. It is generally difficult or expensive for one mobile device to share data and computing resources with another. Data is shared through centralized services, requiring expensive uploads and downloads that strain wireless data networks. Cloud computing is clearly one of today's most enticing technology areas due, at least in part, to its cost-efficiency and flexibility. However, despite the surge in activity and interest, there are significant, persistent concerns about cloud computing that are impeding momentum and will eventually compromise the vision of cloud computing as a new IT procurement model. With continued research advances in trusted computing and computation-supporting encryption, life in the cloud can be advantageous from a business intelligence standpoint over the isolated alternative that is more common today.**

***Keywords*— Cloud computing, Mobile devices, security, Authentication, Authorization, Service level agreement.**

I. INTRODUCTION

Most of today's mobile devices applications are geared towards an individual user and only use the resources of a single phone. There is an opportunity to harness the collective sensing, storage, and computational capabilities of multiple networked phones to create a distributed infrastructure that can support a wealth of new applications. These computational resources and data are largely underutilized in today's mobile applications. Using these resources, applications could conveniently use the combined data and computational abilities of an entire network of mobile devices to generate useful results for clients both outside and within the mobile network. This interface and the underlying hardware would create a mobile-cloud upon which compute jobs could be performed. We define mobile-cloud computing to be an extension of cloud computing in which the foundational hardware consists at least partially of mobile devices.

II. MOBILE DEVICES

New developments in mobile device hardware and software have allowed users to perform various tasks that were possible on personal computers only and specialized devices like digital cameras and GPS personal navigation systems. Using mobile devices like the Apple iPhone, Android phones, and the BlackBerry, mobile users can now make full use of the Internet and communication technology, capture and manage photos and videos, play music and movies, and play complex games. Users can also transfer videos, photos, text messages and files from one device to another using internet. Users have access to the Internet via 3G services, WiFi, and peer-to-peer networking and can switch from one network to another automatically. So mobile devices are used to store, generate, and share multimedia and general text data. Mobile devices can also be used to download video and audio files using internet. These devices has inbuilt non volatile memory so they can store several gigabytes of multimedia data in that memory.

Sensors provide many interesting applications on mobile devices. They gives information about the location, movement, and orientation of the mobile phone and the environment's temperature and lighting. Various mobile phones contain digital compass, GPS system, map application which tells current location and provides customized directions. Applications in these devices contain local sensor data to customize and enhance the user's experience. These devices also support various games which use motion data and input to give real effects. Mobile devices are also used to

Now mobile devices are widely used around the world for all above discussed purposes. There are currently more then 4 billion mobile subscriptions in the world [1]. Among the devices used by these subscribers, mobile devices are becoming increasingly common, accounting for a larger percentage of the mobile phone market and replacing less capable mobile phones. Mobile devices accounted for more than 14% of all mobile device shipped in 2008 and 17% of all mobile devices in 2009[2]. Mobile devices are also used for online purchasing. According to *Newmedia Trendwatch* In 2012 14% of the travellers purchased their travel plans using mobile devices and by 2014 mobile revenue will be 18% of the online market and 8% of the total travel market [3].

III. CLOUD COMPUTING

Cloud computing provides technology like IT Infrastructure, IT platform and IT products as a set of services in a scalable mode so customer can use the services they want to use and pay for used services only. A more formal definition of cloud computing as per Gartner is: "a style of computing where massively scalable IT-enabled capabilities are delivered as a service to external customers using internet technologies" [4].

Cloud computing system makes computing functionality to be used as a service in a multi-tenant manner. The cloud enabling technology includes virtualization and grid technology, enabled application platform (SEAP). These service are exposed as industry standard interfaces like web services using Service Oriented Architecture (SOA) or Representational State Transfer (REST) services or any proprietary services. Cloud computing services are provided by the cloud vendors and used by clients on pay per use basis.

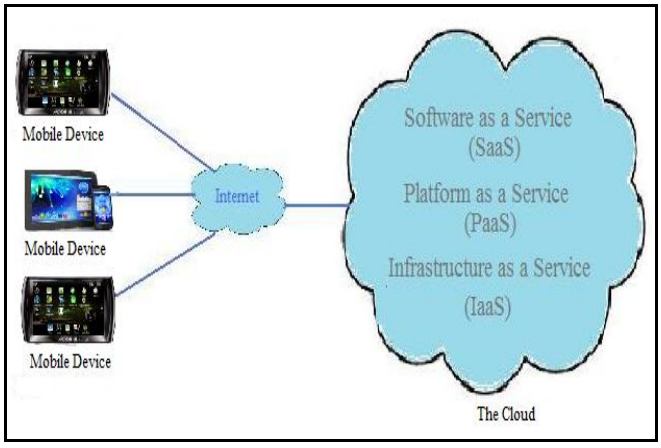

Fig1. Mobile Cloud Computing

The types of services provided by cloud computing providers are broadly classified as follows:

Software as a service (SaaS): - Software as a service provides applications on demand to the loud customers. A single instance of an application runs on the cloud and serves various clients together. Applications like customer relationship management (CRM), e-mail, instant messaging, and office productivity applications are provided as a service by the cloud service providers. For example salesforce.com services (5) or google office productivity application (6), or Microsoft exchange online (7) etc.

Platform as a service (PaaS): - Platform as a service provides development environment as a service. PaaS delivers a platform by integrating an OS, middleware, application software and deployment environment to the clients. For example, someone developing a PaaS offering might base it on a set of Sun™ xVM hypervisor (8) virtual machines that include a NetBeans™ integrated development environment, a Sun GlassFish™ Web stack and support for additional programming languages such as Perl or Ruby, Google app engine(9), salesforce.com (10) etc.

Infrastructure as a service (IaaS): - Infrastructure as a service provides basic storage and compute capabilities as a service to the clients over the network. Computer hardware, servers, storage devices, networking devices and other systems are provided o handle workload of the computing application. Example Amazone EC2(11), Amazone Simple DB(12), Amazone S3(13).

IV. SECURITY ISSUES

Security is very important when accessing cloud computing resources using mobile devices. Following security issues should be considered when using mobile device to access cloud computing.

A. Access Control

Access Control is most common and most important security objective of any mobile information system management. It has two objectives authentication and authorization. Authentication in the context of mobile information security is the binding of a real-world identity to an equivalent electronic one.

1) Authentication

Mechanisms for mobile cloud computing can be divided into three categories [14]:

• *Something you know*: - This is the most common category for mobile cloud computing security where a principle is authenticated according to something user knows such as a PIN, a password, her mother's maiden name, and suchlike.

• *Something you have*: - Principal is authentication according to something a user carries. User will need to present something he/she carries in order to be authenticated. A typical example is the use of a smart card which stores a password or other form of identifier.

• *Something you are:* - This method refers to biometrics where a principle is authenticated by providing a sample found on user's body, which uniquely identifies user among other people. The sample may derive from his fingerprint, voice or iris and is compared for matching with an already stored sample of the same person.

2) Authorization

For mobile devices is not who someone really is (i.e. authentication), but what user is allowed to perform on a given system. The requirements of authorization usually

derive directly from the hierarchy, organization, and specifics of the environment in which is deployed. It is common for companies with more than few employees to categorize them according to the roles they possess. One of the first authorization models which is still widely used is the Role-Based Access Control (RBAC) [15]–[17] and it is based in exactly this observation. In RBAC, each user is assigned to one or more roles and each role is associated with a set of permissions (and maybe a set of restrictions). As mentioned though persons that may possess the same roles may be needed to have permissions on different resources. Although some RBAC implementations support this, it is obvious that the complexity of management increases.

B. Confidentiality

Protection of unauthorized access to the exchanged data is very importance from the data security point of view. Due to the nature of networks, eavesdropping may not be detectable so the aim is to prevent any unauthorized adversary from getting a meaningful context out of the captured data, rather than preventing her from capturing them at all. The objective of preserving this quality is known to the information security field as confidentiality. The technology to meet this objective is cryptography. The information should be encrypted before transmitting and decrypted at the receiving end. The encryption and decryption should be done by using cryptographic keys, which are known by sender and receiver only.

Two important factors for selecting a good encryption algorithm are the length of the key used, in bits, and the amount of testing it had survived. The US standard for encryption is currently a variation of the Rijndael algorithm, mostly known as the Advanced Encryption Standard (AES).Certainly there exist other good candidates such as Blowfish, RSA, IDEA, SEAL, PGP, and many others [18]. The state of the art in encryption is based on the use of quantum mechanics in order to perform quantum cryptography [19].

V. CONCLUSION

To address the growing concern of cloud computing on mobile device threats, we have mentioned two approaches to secure cloud data while accessing using mobile device. By Access control system of any mobile information system management we can protect cloud data from unauthorized and unauthenticated user. By confidentiality we encrypt data before transferring between cloud and mobile device and we will decrypt it back using key at the destination.

REFERENCES

[1]. International Telecommunication Union, (2009) Measuring the Information Society -The ICT Development Index. http://www.itu.int/ITU-D/ict/publications/idi/2009/material/IDI2009_w5.pdf.
[2]. Matt Hamblen, (200), Smart phones lead market growth. http://www.pcworld.com/article/158697/smart_phone_sales.html
[3]. Newmedia Trendwatch, (2013), Mobile Devices. http://www.newmediatrendwatch.com/markets-by-country/17-usa/855-mobile- devices
[4]. Stamford, (2009), Gartner Highlights Five Attributes of Cloud Computing. http://www.gartner.com/newsroom/id/1035013
[5]. Salesforce Products, (2013), Sales force Product Overview http://www.salesforce.com/products/.
[6]. Google, (2013), Apps for Business. http://www.google.com/apps
[7]. Microsoft, (2013), Exchange Online. http://office.microsoft.com/en-us/exchange/microsoft-exchange-online-email-for- business-FX103739072.aspx
[8]. Sun, (2009), Cloud computing architecter. www.sun.com/featured-articles/CloudComputing.pdf
[9]. Google, (2009), App Engine. http://code.google.com/appengine/
[10]. Salesforce.com, http://www.salesforce.com/appexchange/
[11]. Amazone Elastic Compute Cloud (EC2). http://www.salesforce.com/appexchange/
[12]. Amazone SimpleDB. http://amazone.com/simpledb/
[13]. Amazone Simple Storage Service. http://aws.amazone.com/simpledb/
[14]. R. Anderson, (2008). Security Engineering: A Guide to Building Dependable Distributed Systems, 2nd edition, John Wiley & Sons, Inc., New York, NY, USA.
[15]. R.S. Sandhu, (1996), E.J. Coynek, H.L. Feinsteink, C.E. Youmank. "Role-Based Access Control Models", IEEE Computer, 29 (2), pp 38-47, IEEE Press.
[16]. D. Ferraiolo, D. Kuhn, (1992), "Role-based access control". In Proceedings of NIST-NSA National Computer Security Conference, pp 554-563, NSA.
[17]. D. Ferraiolo, D. Kuhn, R. Chandramouli, (2003), Role-Based Access Control. Artech House.
[18]. B. Schneier, (1996), Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd edition, John Wiley & Sons, Inc., New York, NY, USA.
[19]. D. Bruss, G. Erd´elyi, T. Meyer, T. Riege, J. Rothe, (2007) "Quantum Cryptography: A Survey", ACM Computing Surveys, 39 (2).