Authentication in Mobile Environment: Threats and Security Measures to Enhance Recitation of Mobile Users

Parthiban[#1], D. Premanand[#2], K. Kuzhandaivelu[#3]

#1 Final year M. Tech (CSE), Christ College of Engineering and Technology, Pondicherry, India.

#2 Final year M. Tech (CSE), Christ College of Engineering and Technology, Pondicherry, India.

#3 Final year M. Tech (CSE), Christ College of Engineering and Technology, Pondicherry, India.

ABSTRACT

Today information technology world are fully occupied by Smart phones, tablets, laptop computers, USB memory cards and many more which enable the mobile users to store and access data from where ever they are in the world. Mobile computing devices of this type can store large amount of complex data with the help cloud computing. Usually, at this point of view there is heavy risk in handling data and accessing it in a secured manner. They are easy to steal or lose, and unless precautions are taken, an unauthorized person can gain access to the information stored on them or accessed through them. This paper deals with the variety of threats that are often faced by the mobile community and its users and proposes security measures to successfully handle them [2].

Key words: Smart Phone, Tablets, Online Services, USB Memory Cards.

I. INTRODUCTION

Advanced mobile devices, known as Smartphone, are a class of devices built at their core around ease of connectivity and always-on accessibility of online services. This kind of devices are often undergoes security threaten. As the cost of these smart devices gets decreased, the usability and accessibility get increased. Not only the corporate people, but even normal mobile users are also making use of these smart devices for their day to day activities such as reservation of tickets, online money transfer, online registration, e-payment for several official activities and so on. This means, the PC World are now turn around to smart world. Remote connectivity is being used for all major classes of enterprise applications smart devices are been employing for inventory management, sales, client record management, email and voice communications. As a mobile technology grows and develop, automatically mobile services tend to continuously grow and diversify. There is also a need to develop and deploy security measures and a service for mobile environment is indispensable. The secure provision of

mobile computing and telecommunication services is rapidly increasing in importance as both demand and applications for such services continue to grow. This paper will examine Smartphone platforms in general, making reference to specific examples as necessary to illustrate categories of vulnerabilities. Some of the major threats for mobile users are Mobile malware, Eavesdropping, Unlicensed and unmanaged applications, theft or loss of smart devices and unauthorized access to data [2].

Figure 1: Mobile Users with Various Mobile Operators

The vast development of mobile environment is possible only with help of recent computing trend, most probably, the cloud computing. Only with the presence and availability of cloud, it is possible to have data from any part of the world, in an on-demand fashion. Another issue is the movement of data from one location to another. Data is initially stored at an appropriate location decide by the Cloud provider. However, it is often moved from one place to another. Cloud providers have contracts with each other and they use each other's' resources. Cloud Computing offers a high degree of data mobility. Consumers do not always know the location of their data. Cloud computing (CC) has been widely recognized as the next generation's computing infrastructure. CC offers some advantages by allowing users to use infrastructure (e.g., servers, networks, and storages), platforms (e.g., middleware services and operating systems), and soft ware's (e.g., application programs) provided by cloud providers (e.g., Google, Amazon, and Sales force) at low cost.

Increased IP network connectivity in itself brings a familiar raft of security challenges, well known in the desktop environment, but new to the relatively immature mobile operating systems. A number of existing technologies enable security professionals to ensure some degree of security in the implementation of these mobile platforms (encryption, VPN, firewalls, anti-malware scanners). These tools are familiar to all security experts, but the method in which they are applied to mobile devices differ significantly from the desktop and portable (laptop) computing environment[6].The large variety of mobile platforms, with disparate operating systems installed on dozens of different hardware platforms, imposes an extremely broad and challenging surface to defend. Since a serious concentration is needed to this areas so as to improve the integrity in the mobile environment. This paper is organized as-section 2 describes the need of security in mobile environment, section 3 explains threats for

mobile community, section 4 states security measures for mobile users and section 5 concludes the whole paper.

II. THE NEED OF SECURITY IN MOBILE ENVIRONMENT

Today every single piece of information is transferred only through the means of mobile hand held devices. Thus the arises a strong need in providing security of such data that are transferred. At this point the job of cloud provider starts, the cloud provides high range of secure transmission of data in a wireless medium. The following figure will explain the main components that are available in cloud environment to provide maximum integrity and authenticity to its mobile users who are all active in the present cloud [2].

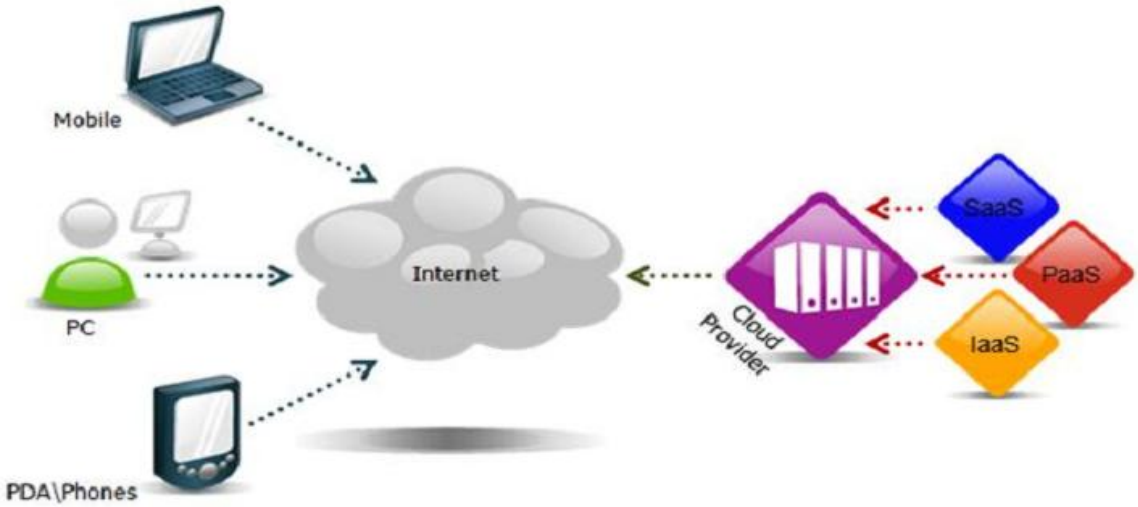

Figure 2: Need for Mobile Security

- SaaS is the short form of software as a service, is a model of software deployment whereby the provider licenses an application to the customers for use as a service on demand. This facility greatly reduces of buying new software or to create software that raises higher cost and time to the mobile users [1].

- IaaS stands for infrastructure as a service, that is the delivery of computer infrastructure (typically a platform virtualization environment) as a service. Usually the user spends more on building the infrastructure for his/her concern. This can be completely solved with this layer of cloud.

- PaaS stands for platform as a service is the delivery of computing platform and solution stack as a service. Here the user can choose his/her desired platform in any programming language. In simple terms the user is free in selecting the programming domain of the concern [1].

III. THREATS FOR MOBILE COMMUNITY: CYBER ATTACK

Mobile devices face a number of threats that pose a significant risk to corporate data. Like desktops, Smartphone and tablet PCs are susceptible to digital attacks, but they are also highly vulnerable to physical attacks given their portability. Here is an overview of the various mobile device security threats and the risks they pose to corporate assets [3].

Mobile malware - Smartphone and tablets are susceptible to worms, viruses, Trojans and spyware similarly to desktops. Mobile malware can steal sensitive data, rack up long distance phone charges and collect user data. High-profile mobile malware infections are few, but that is likely to change. In addition, attackers can use mobile malware to carry out targeted attacks against mobile device users.

Eavesdropping carrier-based wireless networks have good link-level security but lack end-to-end upper-layer security. Data sent from the client to an enterprise server is often unencrypted, allowing intruders to eavesdrop on users' sensitive communications.

Unauthorized access - Users often store login credentials for applications on their mobile devices, making access to corporate resources only a click or tap away. In this manner unauthorized users can easily access corporate email accounts and applications, social media networks and more [3].

Theft and loss -Couple mobile devices' small form factor with PC-grade processing power and storage, and you have a high risk for data loss. Users store a significant amount of sensitive corporate data–such as business email, customer databases, corporate presentations and business plans–on their mobile devices. It only takes one hurried user to leave their iPhone in a taxicab for a significant data loss incident to occur.

Unlicensed applications- can cost your company in legal costs. But whether or not applications are licensed, they must be updated regularly to fix vulnerabilities that could be exploited to gain unauthorized access or steal data. Without visibility into end users' mobile devices, there is no guarantee that they are being updated.

Together with an explosive growth of the mobile applications and emerging of cloud computing concept, mobile services are rapidly expanding. Security and integrity are the core concepts to be taken into account in this era. Installing and running security software are the simplest ways to detect security threats. Mobile devices are resource constrained, protecting them from the threats is more difficult than that for resourceful devices. Mobile devices are exposed to numerous security threats like malicious codes and their vulnerability. Typically, a cloud environment provides the flexibility to have the applications and data available to the end-user from wherever they are. In a mobile environment, users are physically in different locations such as the office or at home, or they are travelling; they will try to access their portal from any network, including non-corporate networks (such as public Wi-Fi) and public LANs. They'll use any device -- a corporate PC/laptop, personal PC, corporate-issued Smartphone (such as a BlackBerry) or a personal Smartphone (such as an iPhone) [3].

IV. SECURITY MEASURES FOR MOBILE USERS: WAR AGAINST CYBER ATTACK

Data Loss Prevention (DLP) is another emerging technology that shows promise in addressing some of the issues raised by mobile platforms. Vendors use several terms to refer to DLP technology: Information Leak Detection and Prevention (ILDP), Information Leak Prevention (ILP), Content Monitoring and Filtering (CMF), Information Protection and Control (IPC) or Extrusion Prevention System. Whatever the name, DLP is concerned with actively monitoring and protecting information at rest and in transit on a network. DLP can also allow an organization to maintain a positive inventory of each copy of protected data and manage the information's lifecycle as it is created, transmitted and securely deleted[4].

Securing Data on Clouds: Although both mobile users and application developers benefit from storing a large amount of data/applications on a cloud, they should be careful of dealing with the data/applications in terms of their integrity, authentication, and digital rights.

Authentication: This security measure presents works using cloud computing to secure the data access suitable for mobile environments. The scheme used for authentication here is TrustCube and implicit authentication, to authenticate the mobile clients [5] TrustCube is a policy-based cloud authentication platform using the open standards, and it supports the integration of various authentication methods. The authors build an implicit authentication system using mobile data (e.g., calling logs, SMS messages, website accesses, and location) for existing mobile environment. The system requires input constraints that make it difficult for mobile users to use complex passwords. As a result, this often leads to the use of simple and short passwords or PINs. Fig. 4 shows the system architecture and how the system secures mobile users' access.

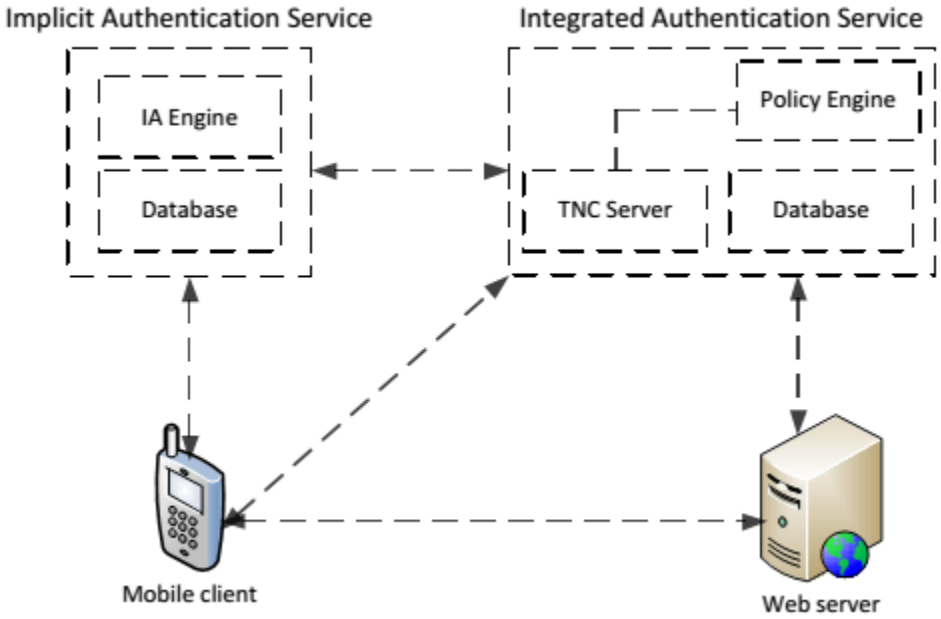

Figure 4: System Architecture Using Trustcube Authentication

When a web server receives a request from a mobile client, the web server redirects the request to the Integrated Authenticated (IA) Service along with the details of the request. The IA Service retrieves the policy for the access request, extracts the information that needs to be collected, and sends an inquiry to the IA Server through the trusted network connect (TNC) protocol. The IA Server receives the inquiry, generates a report, and sends Accepted in Wireless Communications. After that, the IA Service applies the authentication rule in the policy and determines the authentication result (whether or not the mobile client is authenticated successfully for the access request) and sends the authentication result back to the web server. Based on the authentication result, the web server either provides the service or denies the request.

V. CONCLUSION

Security is the major concern for any mobile user in the mobile environment. This situation can be successfully managed with the help of cloud computing. This paves the way for the establishment of new latest trend which is known as mobile cloud computing (MCC). This paper also concludes the need for providing security in mobile environment. Here in this paper we have clearly stated what all the threats that the mobile user faces are and how to handle them in the successful way. Experts in the IT field suggest data loss prevention method, security used with the help of cloud and authentication using Trust cube.

VI. REFERENCE

[1] Jasleen, "Security Issues In Mobile Cloud Computing", IJCSET, July 2012.

[2] Wiley http://onlinelibrary.wiley.com/doi/10.1002/wcm.1203/abstract

[3] http://en.wikipedia.org/wiki/Mobile_cloud_computing

[4] Z. Song, J. Molina, S. Lee, S. Kotani, and R. Masuoka. "TrustCube: An Infrastructure that Builds Trust in Client," in Proceedings of the 1st International Conference on Future of Trust in Computing, 2009.

[5] M. Jakobsson, E. Shi, P. Golle, and R.Chow, "Implicit Authentication for Mobile Devices," in Processing of the 4th USENIX Workshop on Hot Topics in Security (HotSec), August 2009

[6] Erik Couture ,"Mobile Security: Current threats and emerging protective measures", SANS Institute, December 3, 2010.