Security Analysis of Smartphone and Cloud Computing Authentication Frameworks and Protocols

ABSTRACT

We live in a digital world where every detail of our information is being transferred from one smart device to another via cross-platform, third-party cloud services. Smart technologies, such as, Smart phones are playing dynamic roles in order to successfully complete our daily routines and official tasks that require access to all types of critical data. Before the advent of these smart technologies, securing critical information was quite a challenge. However, after the advent and global adoption of such technologies, information security has become one of the primary and most fundamental task for security professionals. The integration of social media has made this task even more challenging to undertake successfully. To this day, there are plentiful studies in which numerous authentication and security techniques were proposed and developed for Smartphone and cloud computing technologies. These studies have successfully addressed multiple authentication threats and other related issues in existing Smartphone and cloud computing technologies. However, to the best of our understanding and knowledge, these studies lack many aspects in terms of authentication attacks, logical authentication analysis and the absence of authentication implementation scenarios. Due to these authentication anomalies and ambiguities, such studies cannot be fully considered for successful implementation. Therefore, in this paper, we have performed a comprehensive security analysis and review of various Smartphone and cloud computing authentication frameworks and protocols to outline up-to-date authentication threats and issues in the literature. These authentication challenges are further summarized and presented in the form of

different graphs to illustrate where the research is currently heading. Finally, based on those outcomes, we identify the latest and existing authentication uncertainties, threats and other related issues to address future directions and open research issues in the domain of Smartphone- and cloud-computing authentication.

**EXISTING SYSTEM**

* Firstly, mobile CC with a biometrics scheme is proposed in Rassan, I. A. L. and AlShaher, H., “Securing Mobile Cloud Computing Using Biometric Authentication (SMCBA)”. Computational Science and Computational Intelligence (CSCI), 2014 International Conference, 10-13 March 2014. pp. 157-161. This study provided a generalized overview, but failed to present details of the authentication computations. Absence of a secure mechanism has made this study vulnerable to parallel processing attacks. Secondly, an NFC-based CC proposal was discussed in next paper called Urien, P. and Piramuthu, S., “Securing NFC Mobile Services with Cloud of Secure Elements (CoSE)”. In Memmi, G. and Blanke, U. (Ed.) Mobile Computing, Applications, and Services. (322-331). Springer International Publishing, 2014.
* The proposal has outlined number of authentication attacks, however, the authors failed to explain how their work is sustainable to those attacks. Next, an advanced mobile based credential protocol is presented in Khan, A., Mat Kiah, M. L., Madani, S., Khan, A. and Ali, M., “Enhanced dynamic credential generation scheme for protection of user identity in mobile cloud computing”. The Journal of Supercomputing 66(3), 1687-1706, 2013. [92] Al-Hasan, M., Deb, K. and Rahman, M. O., “User-authentication approach for data security between smart phone and cloud”. Strategic Technology (IFOST), 2013 8th International Forum on, June 28 2013-July 1 2013. 2-6, 2013. The session variables, t1and t2, used in this protocol are not secured, which makes it vulnerable to parallel session attacks.

**Disadvantages**

* + There is no corresponding Authentication Framework and Protocols.
  + There is no any Smartphone or Sensor Addition devices Used.

**PROPOSED SYSTEM**

* The system is proposed a new concept of Cloud Secure Element (CoSE) for a Near Field Communication (NFC) based application in Smartphones for mobile payments. The proposed mechanism consists of four components, namely; service kiosk, Smartphone, grid or cloud of secure elements and an administration console. The authors further explained the complete workings of those components.
* The authors of this article claimed that their study has prevailed a number of security attacks including; relay attacks, DoS attacks and message modification attacks. However, they failed to provide any level of authentication attack analysis supported by any standardized technique. Therefore, this concept is insufficient to be considered for adoption

**Advantages**

* The system is uses Smartphone Security Service on Clouds which is effective and Secure.
* The system is more efficient due to Privacy-Aware Mobile Cloud Computing Authentication.

**SYSTEM REQUIREMENTS**

➢ **H/W System Configuration:-**

➢ Processor - Pentium –IV

➢ RAM - 4 GB (min)

➢ Hard Disk - 20 GB

➢ Key Board - Standard Windows Keyboard

➢ Mouse - Two or Three Button Mouse

➢ Monitor - SVGA

**Software Requirements:**

* Operating System - Windows XP
* Coding Language - Java/J2EE(JSP,Servlet)
* Front End - J2EE
* Back End - MySQL