Chapter 27
Mobile Cloud Computing Security Frameworks: A Review

Anita Dashti
Foolad Institute of Technology, Iran

ABSTRACT

Mobile Cloud Computing (MCC) is a rich technology of mobile that offers cloud resources and network technology features like unlimited storage at any time via Ethernet or internet based on Pay-Per-Use method. In MCC all processes will be done in cloud servers and data is stored there too, thus mobile devices are just a tool for presenting events. MCC technology is completely different from previous traditional network technologies, so nowadays most impossible ways are becoming possible. MCC is a combination of cloud computing and mobile network. Being online and internet network brings some problems for users. One of the most popular challenges in this technology is building a secure architecture in mobile internet platform. Different security frameworks in different contexts of security challenges in MCC are recommended and compared in some common parameters to have better understanding of which one is the best for user's needs.

INTRODUCTION

Mobile cloud computing is a technology that refers to accessing the resources in network whenever and wherever wanted (Gupta, 2012). The popularity of internet network and cloud computing is getting clear to all. Everything is going to be computerized and the popularity of cloud computing helps to have another architecture that inherits from previous technologies. The number of mobile devices are growing every day, thus the needs for mobile applications increases (Gupta, 2012). As well as having advantages using this technology, some significant issues can rise and cause concerns for users who want to migrate to cloud servers. These issues are privacy, accessibility, security, reliability and some other related ones (Reza, 2016). Mobile devices are becoming important as a part of human life which plays an important role that effects the life and makes it more convenient. Cloud computing has helped users to take their

DOI: 10.4018/978-1-5225-5634-3.ch027

information with them everywhere, also helped to access them whenever wanted (Hoang, 2011). Mobile phones were not invented in the last century, but now is rare to find a house without some mobile phone device. Smart phones have become popular in the last 5 years and in 10 people 6 has a smart phone and the rest has a mobile phone device. Technology never leaves its users alone and is coming up fast according to their needs. According to Portio Research the number of mobile phone users will reach 7.5 till the end of 2014 (Al-Hammami, 2015). It means more 3 quarter of the world will choose mobile device to help them during the day, because it's small, light, can make/receive a call, processes data and all the user needs can be done using it. Mobile phone device is considered one of the most common thing in the history of the technology (Al-Hammami, 2015). Today the mobile phone device has become a key point to contact between people, businesses and consumers. Mobile phone devices have changed the way of communication between human beings, also it contributed to the creation of new businesses (Al-Hammami, 2015). After popularity of MCC and increasing growth of mobile devices, limitations of mobile devices caused a kind of migration for mobile users to cloud. This way, it's clear that mobile internet can fix in cloud computing architecture and because MCC is fixed on cloud computing architecture, so it inherits all security issues plus mobile device limitations. Portable devices need less CPU processing ability, storage capacity, battery, bandwidth, smaller monitor and keyboard than a PC. These are called limitations in MCC technology. Too many works have been done for improving security in cloud computing, but because of mobile device limitations all frameworks can't be used in mobile devices (Chaubey, 2016). Mobile device limitations and security issues on the way of using MCC has drew attentions to itself. Many researches have been done to improve security and privacy that causes concerns for all users. Some solutions can run in mobile devices, some run in cloud-side and some can handle both. Because of mobile device limitations cloud-side frameworks are welcomed more than others. In this chapter the main purpose is to introduce different best security frameworks that are focused on data security and third party misuse. Then by comparison of these frameworks all features can be revealed clearly.

Background: Cloud and Mobile Cloud Computing

Cloud computing delivers different kinds of services over the internet by computing resources that are provided dynamically (Gupta, 2012). This technology is popular because it eliminates the limitations. These limitations include computing overhead, different service requirements and other related problems. According to (Mell, Sep. 2011), released in its "Special Publication 800-145", the National Institute of Standards and Technology (NIST) defines cloud computing as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction". NIST believes that characteristics of cloud computing are as stated bellow.

- **On-Demand Self-Service:** Users can change cloud services online (add, delete or change storage network and software).
- **Broad Network Access:** The user can access cloud services using smart and portable devices wherever connected to the access point.
- **Resource Pooling:** The user can use required cloud resources anytime and anywhere.
- **Elasticity:** The user can add or remove other users and resources according to the user's needs.