Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 94 (2016) 418 – 423

Procedia Computer Science

The 3rd International Symposium on Emerging Inter-networks, Communication and Mobility (EICM-2016)

Data Management in Mobile Enterprise Applications

Marwah Hemdi[a*], Ralph Deters[b]

1. [a] *University of Saskatchewan, Saskatoon, SK, Canada*
2. [b] *University of Saskatchewan, Saskatoon, SK, Canada*

Abstract

Nowadays, businesses provide applications to their employees that allow these employees to use their own smart devices to work more efficiently. The popularity of so-called Bring Your Own Device (BYOD) programs, which allow the employees in an enterprise to use their personal devices to carry out their job duties, has been increasing significantly. Unfortunately, some of the enterprises that have BOYD applications do not provide significant security to minimize loss in the event of a device's loss or theft. The problem studied here concerns the protection of an enterprise's mobile-application data from unauthorized access. To solve this problem, we are evaluating some of the context of the users. Finally, we built a prototype to test the proposed solution.

Peer-review under responsibility of the Conference Program Chairs

Keywords: Mobile Cloud Computing; Bring Your Own Device; Data Management;

1. Introduction

The introduction of cellphones attracted customers all over the world; as time went by, feature phones became smartphones, which have operating systems. These more powerful devices became more popular, and more people obtained them. The number of smartphones' users had been growing rapidly in the recent years.

* Corresponding author.
E-mail address: mah411@mail.usask.ca

Peer-review under responsibility of the Conference Program Chairs
doi:10.1016/j.procs.2016.08.064

Wang et al[1] stated that the number of mobile devices including tablets and smartphones were sold in 2012 was 821 million devices, and in 2013 the number of devices were sold are more by 46%[1].

Furthermore, the term mobile cloud computing (MCC) is introduced to make people attach more with their smartphones. One outcome of this new technology was that businesses could furnish their employees with applications to help them do their jobs better. Many enterprises have supported Bring Your Own Device (BYOD) programs, which allow employees to use their personal devices for professional duties. Morrow[2] indicated that personal electronic devices were used in industrial aspects by employees 80% of the time[2]. Unfortunately, some of the enterprises supplying BOYD applications to their employees have not developed commensurate security in case the devices are lost or stolen. "Millions of cell phones and smartphones are lost or stolen every year. It is thought that approximately 22% of the total number of mobile devices produced will be lost or stolen during their lifetime, and over 50% of these will never be recovered[3]." An enormous challenge, then, is to protect data from unauthorized access. We address in this paper the problem of data security in enterprises' mobile applications. To that end, we have evaluated and applied some policies regarding some of the users' contexts, specifically username, password, and accessed time. To evaluate the proposed solution, we tested it by building a mobile application to serve as a client-side, creating a server-side via cloud computing, and connecting the two sides via a Web service.

2. Problem Definition

Protecting a smart-device (phone or tablet) application is essential, since most of the devices' owners use them to do online operations that require sensitive information. The prevalence of MCC solves problems posed by massive amounts of data—the cloud provides unlimited capacity. Web services like HTTP methods with RESTful services have made sending and retrieving data easier. These factors and others are what gave rise to the idea that mobile-device users could use their smartphones or tablets to carry out their everyday tasks. Enterprises naturally want to use available technologies for their own benefit; one result has been the concept BYOD. If a worker uses his or her own device in a professional capacity, he or she reduces many costs to the business. For example, money otherwise spent to purchase PCs and space, or to monitor and fix company-issued devices, is saved. Likewise, employees, as they often prefer to do, can manage their own time to accomplish their work anytime and anywhere.

Because of improved technologies like smartphones and the use of the cloud computing to store data and information, threats such as malicious software are very different than they were in the past: these threats are invisible and thus more dangerous in their potential to cause damage.

Storing very sensitive information (bank account information or personal information like homes' addresses) on a smart device is considered risky because the device could be lost or stolen any time. Though virtually any application requires one layer of authentication—a combination of username and password—for example, a single layer is not secure enough, because there are many software programs capable of cracking passwords. Consequently, enterprises must apply some policies to help protect employees' information when they allow BYOD[4].

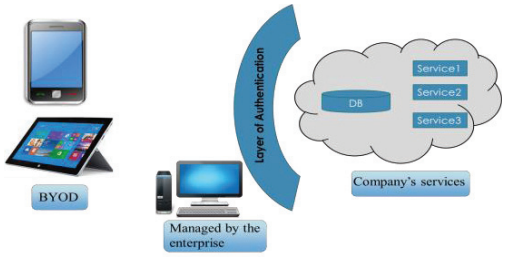

Fig. 1. Problem Definition