Data Management in Mobile Enterprise Applications

Marwah Hemdia*, Ralph Detersb

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.

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: mab411@mail.usask.ca
Wang et al. 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 BYOD 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
3. Related works

3.1. Mobile Cloud Computing

Mobile Cloud Computing (MCC) is the term that used to describe mobile devices connected by the Cloud Computing (CC) via Internet. Fernando definition of MCC\(^5\) stated that the term of MCC means one’s ability to use a mobile device to access a remote cloud server through the Internet, e.g., using a smartphone to access Google’s applications, which are stored in Google’s cloud. According to Dinh et al\(^6\) connectivity between mobile devices via CC enables users to get all the benefits of CC. Bahar et al\(^7\) mentioned some of the services provided by cloud computing that aid in its growth. First, Software as a Service (SaaS) allows customers to use diverse applications running on the cloud infrastructure using a client interface; but those customers do not have any control over the underlying cloud infrastructure. The second service is Platform as a Service (PaaS), which gives consumers a platform and allows them to create applications using programming languages; however, the users cannot control or change the underlying cloud infrastructure. The third service gives customers full control over the computer infrastructure: Infrastructure as a Service (IaaS). Nowadays, many developers create applications using MCC so they can save money, effort, and storage, and they give users a lot of useful services.

3.2. Bring Your Own Device (BYOD)

BYOD is a concept that has been used widely in the business world in recent years; it means that an enterprise allows its employees to use their personal devices (smartphones, tablets, and laptops) for work tasks. Kulkarni et al\(^4\) have identified the advantages of mobile computing (MC) that have made mobile devices so attractive to workers. For instance, mobile devices are small and compact, so they are portable; smart devices have high levels of connectivity; and mobile devices decrease power consumption. Furthermore, workers do not want to be limited in performing their work; they want the ability to complete tasks anytime and anywhere. Additionally, BYOD benefits the enterprise by reducing costs, as the company need not pay for a big space or for devices and their maintenance. Although BYOD has a lot of advantages, it needs a large number of policies to control and secure company data. Yu\(^8\) said that “whether for work or play, users want to use their own devices and their own applications.” Further, some statistics gathered from real studies’ results, which prove that large numbers of workers allowed to use their own devices for work are not very careful with those devices’ data. In one study, 60% of workers in businesses allowing BYOD were found to be users of at least one free file-sharing application, and 55% of those did not tell their IT departments about such use\(^8\).

3.3. Web services

The Web is a universal ecosystem that can accommodate all kinds of operations on applications and services; it makes us able to search, transfer, cache, replicate, and much more. One of the biggest factors that made the Web essential is people: “Webber et al\(^9\) wrote ‘human users are the direct consumers of the services offered by the majority of today’s web applications.’” Applications, including those developed via mobile cloud computing, are a type of distributed system, because they have the ability to connect numerous devices in a network. According to Dospinescu and Perca\(^10\) “Web services are a solution for the integration of distributed information systems, autonomous, heterogeneous and self-adaptable to the context.” There are various types of web services; each has strengths and weaknesses. Representational State Transfer (REST) is one of the most popular Web services today. Christensen indicates that RESTful on smart mobile devices which were connected to a cloud computing platform, and he concludes that REST improves created applications by surpassing the abilities of old-style smart devices\(^11\). This leads to a new generation of mobile applications with remarkable potential.
4. The Proposed Solution

The proposed solution is to add onto an existing or new infrastructure a layer of security which can evaluates whether the user trying to access the enterprise cloud is an employee of the enterprise or not.

Fig. 2. The Proposed idea on the problem definition

The creation of the proposed solution consists of two essential steps. The first step is to create the client-side, which is the mobile application. The second step is to build the server side of the system. We will connect the two sides via HTTP and RESTful Web services.

4.1. Client Side (Mobile Application)

The client side is the mobile application prototype for the Android platform; we created it using Xamarin, which is used across platforms to create mobile applications. The application has an interface that contains two text fields, for username and password, and a button. When a user writes her or his name and password and then clicks the button, those contexts should be sent to the database we created on the server side in the cloud platform.

Fig. 3. The Interface of the Application

4.2. Server Side (Cloud Computing)

In our design, we created the server using Google Cloud Platform. Cloud Platform is a PaaS: developers use it to host their Web applications. There are two parts to the server

1. Google App Engine (GAE) is the local side of the server; on this side, we wrote the Python code to connect the client-side with the database in the cloud. This part acts as middleware between the client and the database; here, we created the Uniform Resource Locators (URLs) to transfer the user context (username and password). The Python code for this research contains a “get” function to retrieve the data that is stored in the database and a “post” function to take the user context from the client side and save it to the database. In the POST method, we wrote the username and password authentication step.

2. The cloud SQL is the part where we created a ‘project’ and an ‘instance’ inside that ‘project’ in the Google cloud. Moreover, the data evaluation happens in this database using SQL commands to build a trigger: every time a certain user signs in, the system will get the username, password, and server time (because the server time is unalterable). The trigger will check the entered contexts and apply some comparison to evaluate them.
4.3. Web service

After creating the server and client sides, we used HTTP and RESTful web services to connect the client with the server so they could share the data. We chose RESTful for the tremendous qualities which makes it easier to be used with mobile platforms\(^{10}\). Some of them are mentioned below:

- The ability to reduce the effect of network instability because REST is stateless.
- REST is easy to invoke because it is URL based.
- Use HTTP methods.
- Returns Extensible Markup Language (XML) and/or JavaScript Object Notation (JSON).

Our project is URLs-based, so it was suitable to apply HTTP operations. Each method (POST and GET) had its own URL. “PUT” and “DELETE” were not applied here because we did not want to destroy or modify any user data.

5. Evaluation Plan

To evaluate this research, we simulated the proposed solution by building a prototype application and implementing it on a mobile device as a client. We used a Google Nexus 7, an Android device. We observed the connection between the client side and the server side using Advanced Rest Client, a Google-provided app. It is an online debugger that helps developers run and monitor their applications and detect errors. We applied the POST and GET methods for the proposed solution for one user only; we found out the following:

1. **Time**: in the POST method sending the data took 5131 milliseconds. However, the GET method took 5645 milliseconds.
2. **Bandwidth usage**: The size of the message sent from the mobile device to the cloud computing server is significant. In Advanced Rest Client in the POST and the GET methods the content length was 653 in octets (8-bit bytes).

6. Conclusion and Future Work

The present technology continues to improve rapidly, especially in the industry world. The increase in the number of mobile devices, the popularity of mobile cloud computing, and the advent of BYOD policies bear this out. A resulting problem, as we see it, is how best to secure the data in an enterprise’s mobile application. Our motivation is to prevent losses for the enterprise and threats to the safety of the enterprise’s employees and clients. Our proposed solution is an analysis approach applied to the users’ contexts to authenticate users’ identities in an enterprise application. To evaluate the proposed solution, we built a prototype consisting of two sides—a client side, which is a mobile application tested on a smart device, and a server side, created in a privately-owned cloud—and connected those using HTTP and RESTful Web services.

The next step will be focusing more on

1. evaluating more users to send different numbers of requests and thus discover the overhead performance, including the response time and the latency; and
2. choosing another type of user context, such as location, the media access control address (MAC address), or the IP address of the mobile device.
References

1. Y. Wang, J. Wei, and K. Vangurry, “Bring your own device security issues and challenges,” in Consumer Communications and Networking Conference (CCNC), 2014 IEEE 11th, 2014, pp. 80–85.
2. B. Morrow, “BYOD security challenges: control and protect your most sensitive data,” Netw. Secur., vol. 2012, no. 12, pp. 5–8, Dec. 2012.
3. “Bring your own device: Security and risk considerations for your mobile device program,” EY Build. Better Work. World, pp. 1–16, Sep. 2013.
4. G. Kulkarni, R. Shelke, R. Palwe, V. Solanke, S. Belsare, and S. Mohite, “Mobile Cloud Computing - Bring Your Own Device,” in 2014 Fourth International Conference on Communication Systems and Network Technologies (CSNT), 2014, pp. 565–568.
5. N. Fernando, S. W. Loke, and W. Rahayu, “Mobile cloud computing: A survey,” Future Gener. Comput. Syst., vol. 29, no. 1, pp. 84–106, Jan. 2013.
6. H. T. Dinh, C. Lee, D. Niyato, and P. Wang, “A survey of mobile cloud computing: architecture, applications, and approaches,” Wirel. Commun. Mob. Comput., vol. 13, no. 18, pp. 1587–1611, Dec. 2013.
7. A. N. BAHAR, M. A. HABIB, and M. M. ISLAM, “Security architecture for mobile cloud computing,” Int. J., vol. 3, no. 3, pp. 2305–1493, 2013.
8. W. YU, “BYOD Security Considerations of Full Mobility and Third-party Cloud Computing,” Inf. Syst. Control J., pp. 39–42, 2013.
9. J. Webber, S. Parastatidis, and I. Robinson, REST in Practice: Hypermedia and Systems Architecture. O’Reilly Media, Inc., 2010.
10. O. DOSPINESCU and M. PERCA, “Web Services in Mobile Applications,” Inform. Econ., vol. 17, no. 2, pp. 17–26, 2013.
11. J. H. Christensen, “Using RESTful Web-services and Cloud Computing to Create Next Generation Mobile Applications,” in Proceedings of the 24th ACM SIGPLAN Conference Companion on Object Oriented Programming Systems Languages and Applications, New York, NY, USA, 2009, pp. 627–634.
12. R. G. Lennon, “Changing user attitudes to security in bring your own device (BYOD) amp; the cloud,” in Tier 2 Federation Grid, Cloud High Performance Computing Science (RO-LCG), 2012 5th Romania, 2012, pp. 49–52.
13. Y. Lin, C. Huang, M. Wright, and G. Kambourakis, “Mobile Application Security,” Computer, vol. 47, no. 6, pp. 21–23, 2014.
14. “Total annualized cost of cyber crime targeting U.S. companies in 2014 and 2015 (in million U.S. dollars),” Statista, 2016.
15. L. G. Dobranski, “FACTORS THAT INFLUENCE THE OVERALL INFORMATION SECURITY RISK IN THE ENTERPRISE THAT ARE ATTRIBUTABLE TO THE USE OF PERSONAL MOBILE DEVICES – BYOD,” University of Fairfax, 2014.