International Journal of Information Management 34 (2014) 329–335

Contents lists available at ScienceDirect

International Journal of Information Management

journal homepage: www.elsevier.com/locate/ijinfomgt

A framework of cloud-based virtual phones for secure intelligent information management

Jiun-Hung Ding [a], Roger Chien [b], Shih-Hao Hung [b,*], Yi-Lan Lin [a], Che-Yang Kuo [a], Ching-Hsien Hsu [c], Yeh-Ching Chung [a]

[a] Department of Computer Science, National Tsing Hua University, Taiwan
[b] Department of Computer Science and Engineering, National Taiwan University, Taiwan
[c] Department of Computer Science and Information Engineering, Chung Hua University, Taiwan

ARTICLE INFO

Article history:
Available online 30 December 2013

Keywords:
BYOD
Mobile cloud computing
Mobile security
Information management

ABSTRACT

As mobile networks and devices being rapidly innovated, many new Internet services and applications have been deployed. However, the current implementation faces security, management, and performance issues, which are critical to the use in business environments. Migrating sensitive information, management facilities, and intensive computation to security hardened virtualized environment in the cloud provides effective solutions. This paper proposes an innovative Internet service and business model to provide a secure and consolidated environment for enterprise mobile information management based on the infrastructure of cloud-based virtual phones (CVP). Our proposed solution enables the users to execute Android and web applications in the cloud and connect to other users of CVP with enhanced performance and protected privacy. The organization of CVP can be mixed with centralized control and distributed protocols, which emulates the behavior of human societies. This minimizes the need to handle sensitive data in mobile devices, eases the management of data, and reduces the overhead of mobile application deployment.

1. Introduction

Nowadays, mobile devices, such as *smartphones* and *tablets*, have become increasingly popular, and its shipping volume already exceeds the volume of personal computers (PC's). Mobile devices are being integrated into our personal lives, business activities, government services, and even military operations. *Enterprises* must carefully use such rapid-evolving mobile technologies in daily operations to meet high security and management requirements.

For information management in an enterprise environment, it is critical to evaluate the potential risks and issues as mobile technologies being integrated into its infrastructure. Valuable, sensitive and private contents can be leaked and cause great damages when a mobile device is compromised (Li & Clark, 2013). For instance, as unofficial mobile applications are downloaded, many of them may be *malwares* created by repackaging existing applications and injecting malicious code (Zhou & Jiang, 2012). A malware can steal the credentials of a mobile user and gain access to data and recourses of an enterprise via the user's mobile device. After analyzing more than 1.85 million mobile apps, Juniper Networks recently reported that the total amount of mobile malware increased by 614% between March 2012 and March 2013 to a total of 276,259 malicious mobile applications (Protalinski, 2013).

Facing the increased number of security threats for mobile devices, it is important to find proper solutions to strengthen today's mobile environments. In this paper, we hope to address the following issues for the information security and management in an enterprise IT infrastructure:

- *Operating environments*: There are diversified operating environments for mobile devices. While Android and iOS dominate mobile market today, new technology evolves so fast that there are multiple versions of operating environments being used by vendors, which has created a fragmentation problem which makes deployment of applications and management of mobile devices difficult for enterprises (Han et al., 2012).
- *Security and isolation*: While modern mobile operating environments use sandbox to isolate the execution of applications and provide a seemingly more secure execution environment, mobile devices are still subjective to many types of malware attacks (Zhou & Jiang, 2012). Unfortunately, due to resource limitations, such as CPU speed and battery time, mobile devices are not protected as well as PC's are, in terms of antivirus/anti-malware schemes, application management facilities, network traffic monitoring mechanisms, and virtualization technologies. Furthermore, a *rooted* Android device or a *jailbroken* iOS device

* Corresponding author. Tel.: +886 919695141.
E-mail address: hungsh@ntu.edu.tw (S.-H. Hung).

0268-4012/$ – see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.ijinfomgt.2013.11.006

allows applications to execute in the superuser mode and even gain the highest privilege to break the sandbox isolation protection (Li & Clark, 2013).

- *Sensory applications*: Different from PC's, each mobile device usually contains a rich set of sensors. There are sensory applications which may take advantage of the sensors to identify the user's location and position with a GPS and a gyroscope, record audio with a microphone, and connect to a payment system via the near-field communication (NFC) protocol. These features may not be aware by traditional enterprise management software.
- *Consumerization of IT:* It has become a trend that enterprise employees prefer to carry their own devices, use their own applications and connect to the corporate network with their own device, with or without the approval from the organizations. The term BYOD (Bring your own device) refers to such mobile workers who bring their own mobile devices into their workplace. Embracing the consumeration of IT will not only save money but also improve employee productivity (Webopedia, 2013). However, this poses security threats to the organization as it introduces untrusted devices and unsecure network connections to the work environment.

To help enterprises solve these problems in terms of manageability and security, we propose a framework called *cloud-based virtual phone* (CVP) technology for mobile devices based on our previous works on virtualized execution environment for smartphones (Hung, Shih, Shieh, Lee, & Huang, 2012). The concept of CVP is inspired by the behavior of the *human societies* and the idea of *federalism*, which describes the progress of federation that divides sovereign into federal government and states (Bednar, Eskridge, & Ferejohn, 1999). The proposed framework enables critical business applications to be executed in a controlled virtualized environment on enterprise server farm, while the client-side software can be quickly deployed to almost any mobile devices to interact with the business applications. Unlike traditional *Virtual Desktop Infrastructure* (VDI) technology (Baratto, Potter, Su, & Nieh, 2004), our framework is designed to support local execution of non-critical mobile applications with data synchronization protocols. Overall, our framework contains an *HTML5 Web-based front end* (Kanaka, 2013) to provide different modes of operations, a *KVM-based virtual phone system* (KVM, 2013) to execute mobile applications efficiently, and a set of *security/management modules* to ensure the confidentiality of data and to mitigate the complexity of policy enforcement. The framework also provides a set of APIs is also provided for enterprise to develop their own applications that can be deeply integrated into this framework.

The rest of this paper is organized as the following. Section 2 further describes the weaknesses in the current solutions and the related works. Section 3 describes the models and the proposed framework. Section 4 presents the case studies and discusses experimental results. Finally, Section 5 concludes this paper and discusses future research directions.

2. Background and related works

Mobile technologies brought anytime, anywhere access to information resources and caused significant impacts to the IT organization (IBM, 2012). There are a variety of wireless mobile networks available today, such as WiFi, 3G/4G, Bluetooth, NFC, etc. for connecting a mobile device to the Internet Service Providers (ISP's) or surrounding devices. Unlike a PC which is connected to a fixed network router, it is possible for the user to send out messages via one of those wireless communication channels without being monitored by the enterprise.

BYOD has become a new trend for the enterprise. According to the reports from Unisys and IDC, there are about 40% of information workers who use their own mobile devices to access business applications. This trend has increased 10% compared with 2010 (Burt, 2011; IDC, 2011). While BYOD can bring several benefits to the enterprise, such as making the enterprise to be agile and more competitive (Tomson, 2012), BYOD also represent the security and management challenges to the IT management. It is obvious that security is not easy to control (Miller, Voas, & Hurlburt, 2012; Tomson, 2012). When employee lost their devices, it may cause enterprise's internal information to be stolen. When employee quit their job, the enterprise data stored in their own devices would be a threat if they sell enterprise data to enterprise's competitor (Assing & Calé, 2013; Miller et al., 2012).

IDC has reported that IT managers need to realize that even if they do not allow employees to use their own devices, they will find workarounds and BYOD will still seep into the enterprise (Sacchi, 2012). Therefore, IT departments must find the right balance between flexibility and potential security risks. The existing solutions, such as MDM and VDI (discussed below), to incorporate mobile devices into an enterprise environment still have some weaknesses.

MDM (mobile device management) is inherited from device management or endpoint management in PC era. A client software needs to be installed on client mobile device, and it regularly reads the status of the device, checks if any policies is violated and reports to central management system. It may also create the secure storage for specified applications. However, to deploy MDM to various mobile OSes and device configurations has a portable issue. In addition, MDM client software will detect threats through granting more privileges, but application sandboxing in mobile platform may limit the functions of MDM. Furthermore, if a MDM is exploited, mobile devices and the data they contain will be compromised (Rhee, Won, Jang, Chae, & Park, 2013). Compared with MDM, our CVP (Cloud-based virtual phone) will use the virtual machine technology to isolate business domain from mobile devices. Security threats are detected in a centralized virtualization environment with a better portability and fewer privilege issues.

VDI (Virtualization Desktop Infrastructure) allows the user to access to the user's desktop environment hosted by a remote enterprise server via a remote display protocol. This enables the IT department to control and manage the user's environment. Since VDI is designed to deliver server-hosted virtual desktops to a range of devices, it can be easier for IT to perform cross-platform management and security checks (Oracle, 2013). However, there are two problems for using VDI on mobile device: (1) the mobile device must be connected to the network all the time, and (2) VDI does not support sensory mobile applications. In comparison, our CVP offers both on-line and offline execution models as well as sensor-aware interfaces.

3. The proposed framework

In this section, we describe our proposed framework in details. Section 3.1 gives an overview on the framework. Section 3.2 describes the information management facilities in this framework. This section focuses on the concept and organization of the CVP framework.

3.1. Overview of the framework

Bednar et al. (1999) describes the progress of federation that divides sovereign into federal government and states as *federalism*. Three features in federalism are referred as follows. The first