Secure Managed Application and Execution Platform Technology for Smart Devices

● Hidenobu Ito ● Kazuaki Nimura

With the rapid spread of smart devices such as smartphones and tablets, corporate IT systems are increasingly shifting away from PCs and towards such devices. In order for businesses to take full advantage of smart device capabilities, new security features are needed that are different from those conventionally designed for PCs. Accordingly, Fujitsu Laboratories Ltd. has developed platform technology for application management and execution that provides for flexible and secure use of business applications without sacrificing usability. In this paper, we introduce the concept and technical mechanism along with use cases. This technology provides the secure environment necessary for corporate use by distributing the applications associated with the users' contexts to their devices and properly protecting and controlling the execution of those distributed applications which include confidential information.

1. Introduction

In the recent consumer market, the spread of smart devices such as smartphones and tablets has made it possible for users to easily download the necessary applications from application stores and quickly utilize various services.

This model, which has been established in the consumer world, is permeating into the business world and there has been an ongoing shift of devices used in corporate IT systems from mainly PCs to mainly smart devices. In order for businesses to take full advantage of the capabilities of smart devices, a service platform is required that provides corporate users with various business applications equipped with management and security features at levels different from those conventionally designed for PCs.

In addition, a sea change is occurring in the area of applications for smart devices. Up to now, application developers have used the development environment provided by device OS vendors to develop applications for the respective OSes, and the applications have been distributed via application stores provided by the device OS vendors. However, corporate use involves various types of devices including PCs, and creating separate applications for the respective OSes causes the management cost to increase. For that reason, it is often the case that, for business systems, Web applications written in HTML are built on the server side and used with device browsers.

With this situation in the background, packaged Web applications[1)] are now beginning to attract attention. In this concept, Web applications, which are generally deployed on a server, are distributed in the form of packages and made resident on devices in the same way as ordinary applications. They can also be used on devices even in an offline state without connection to the server. Furthermore, they have features that compare favorably with those of ordinary applications and they can be developed, distributed and executed without having to depend on the development environments or application stores of device OS vendors. This raises expectations for applications to be disseminated further in the future, mainly for business use. By building a system based on packaged Web applications, a system can be realized that is usable offline and capable of centrally distributing, executing and managing business applications regardless of the device types.

2. Issues with and requirements for business use of smart devices

Smart devices are being introduced into business

although they raise concerns in terms of security including lack of established antivirus measures similar to those for PCs and a higher risk of loss due to their portable nature.

For example, even if company-provided devices exclusively for business purposes are prepared for employees to use, the system operation is rendered inefficient if the workers are not permitted to use convenient applications that are generally distributed, for security reasons. Employees need to use their personal smartphones if they want to use applications to check the train operation status or search for a route to a destination while moving from the office to the customer's site.

In these circumstances, the "bring your own device" (BYOD) movement, which promotes the use of personally owned devices for business operations in enterprises, has appeared and come to be widely known by corporate IT departments as well. However, while many enterprises are considering introducing BYOD, its implementation rate still remains low at 14.4%.[2)]

As a method that allows for secure business use of personally owned devices, one conventional idea has been to make use of remote desktop technology or desktop virtualization technology[3)] to create a sharp distinction between private and business environments on smartphones. With these technologies, security can be achieved but there are problems: remote desktop technology is not able to be used in an offline state and desktop virtualization technology poses a heavier processing burden on smartphones, which have a lower processing capacity than PCs, due to the need to run multiple OSes. This may cause stress to users and impair the benefits of introducing smart devices in terms of convenience.

Meanwhile, even if the environments can be completely separated, the security of the applications themselves that run on them must not be compromised. Packaged Web applications can resolve the issue of offline use and can be installed and executed without intervention of the OS for ready use, and thus they may help to improve convenience. On the other hand, there is the problem of insufficient protection of resources in applications. For example, there is a risk that information of a certain application may be accessed by another application that can easily acquire its content.

Accordingly, the following are required in order to put smart devices to business use without sacrificing their convenience.

1) Isolated execution environment of business application
2) Protected application resources
3) Achievement of 1) and 2) above with a low processing burden

Putting in place a scheme that satisfies these requirements raises expectations for a higher implementation rate of BYOD.

3. Developed technology

To meet the requirements described in the previous section, we have developed a secure application management and execution platform technology that realizes secure operation, preventing users from inadvertently interfering with the business environment by managing applications from the cloud. Secure application management and secure application execution satisfy requirements 1) and 2) respectively, and requirement 3) is satisfied by implementing them without depending on the OS. An overall picture of this technology is shown in **Figure 1**.

The business application store is placed in the cloud, where business applications are packaged for deployment.

The application server defines various places and contexts in the real world, such as companies and conferences, as logical places (virtual places) and associates them with groups of applications required in those places from the business application store. It is also equipped with a function to push applications from the server to devices.

A smart device acquires information from various sensors in the device and, based on that information, the location manager identifies a context including the location of the device. The context information is delivered to the application server through the location manager as appropriate. The application server decides on an appropriate context based on the information delivered and also presents a required group of applications to the user by switching the Context Desktop of the device according to the virtual place. It is also possible to push the applications from the application server as required.

This technology is characterized by what may

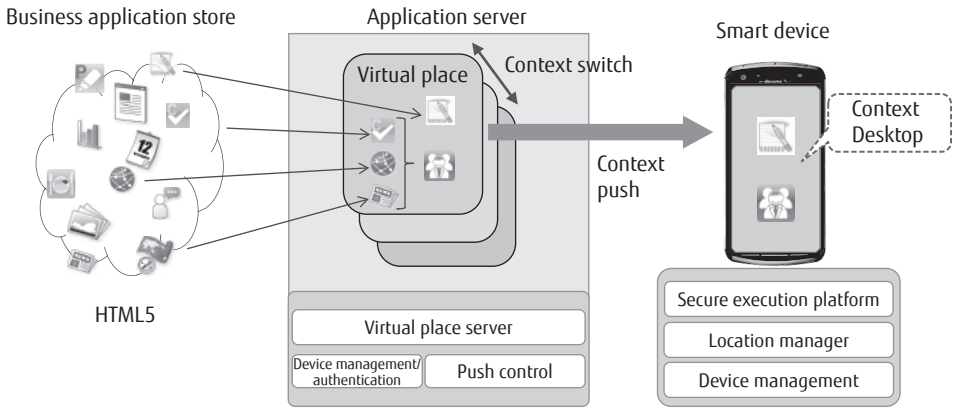

Figure 1
Overall configuration of secure application management and execution platform.

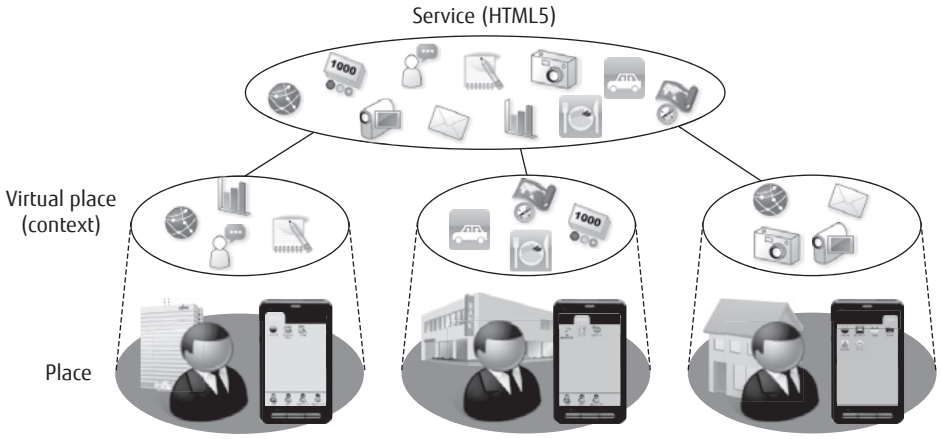

Figure 2
Context Desktop.

be called "systematization for one context," where applications are associated with a particular context for narrowing down the application operation environment, and application use is restricted outside this context. This is one means of securing applications, and a technique of switching applications according to the condition of operability by grouping applications for respective conditions is called Context Desktop.[4),5)] It is used for managing application groups for corporate use. The function to appropriately control the application operation while protecting applications is called "secure execution platform." [6)–8)]

The following outlines the respective technologies.

3.1 Context Desktop

Context Desktop is a technology for switching screens and managing applications to be delivered according to the situation (**Figure 2**). For example, when a person with a smartphone is detected as being in the office, the technology switches the smartphone screen to one appropriate for work and narrows down the choice of applications to be used, thereby improving user convenience. Applications are delivered from the cloud to the smartphone on an as-needed basis and erased when no longer needed. Managing applications from the cloud in this way allows for a secure operation that does not permit users to inadvertently interfere with the business environment.

Context Desktop makes it possible to come up

with various scenes of use that are different from the existing ones.

The applications used here are packaged Web applications written in HTML5. This system saves users the trouble of installing the applications and allows applications to be freely delivered and executed without troubling the users.

3.2 Secure execution platform

Secure execution platform is a platform technology for controlling isolation and secure execution of applications based on packaged Web applications (**Figure 3**).

To reduce the burden on the devices, applications and data are encrypted in the cloud in advance and packaged, and then delivered to smart devices. By encrypting them in advance for individual devices, they are made inoperable with other devices. They are kept in an encrypted state in smartphones until the applications are used, when the applications are executed as the applications and data are dynamically decrypted in the execution memory. It means that no decrypted information remains except that in the execution memory, and this allows for secure execution of the applications and prevents interference from other applications.

As control for application execution, unnecessary operation can be prevented by restricting use against cameras and networks as required. For example, even if an application contains an embedded malicious code that reads data stored in a device's memory card and uploads it to a Website, Websites other than the predefined one can be made unusable, thereby preventing the malicious code from running.

This technology does not require complicated control such as running of multiple OSes as with the desktop virtualization technology and operation generally does not impose much burden on the CPU or memory although there is some overhead due to decryption. By using the ordinary environment provided by the device OS for private applications and the Web application environment running on the secure execution platform for work to separate the two environments, it is possible to achieve BYOD that is adequate for corporate use and fast as well.

4. Operation example

Figure 4 shows an operation example of Context Desktop.

The screen on the left is the home screen usually used by the user. When the user enters the company premises, the SSID of an in-house wireless LAN access point is detected, and the system automatically delivers business applications and switches the home screen to one exclusively for work (screen on the right). When the user exits the company premises and goes out of the access range of the in-house wireless LAN, the original home screen comes back. In this example, the screen switching is triggered by the detection of a wireless LAN access point but there are other triggers

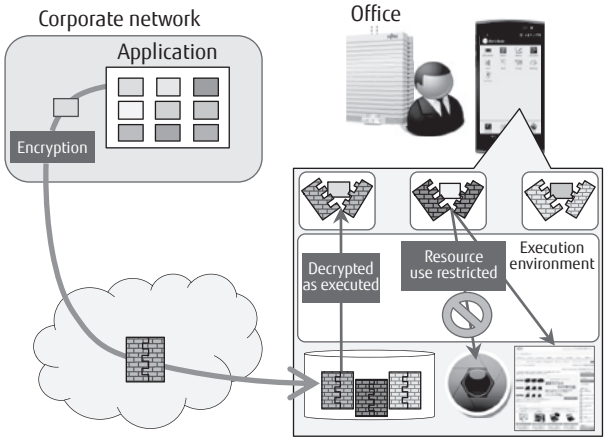

Figure 3
Secure execution platform.

Home screen Business screen

Figure 4
Operation example of Context Desktop.

possible. For example, the switching can be linked with an entry control system that uses cards such as near field communication (NFC) or with a scheduler.

Execution of an application on the screen shown on the right is protected by secure execution as shown in **Figure 5**. The screen on the left shows ordinary application execution without the present technology applied, and the screen on the right shows application execution on the secure execution platform. With an ordinary unencrypted application, the content of the application can be easily acquired by creating an application that accesses information of the unencrypted application. On the other hand, an application that runs on the secure execution platform can be encrypted, and be made decryptable only in the execution environment so as to block access from other applications. This eliminates the concern of unauthorized acquisition of application information.

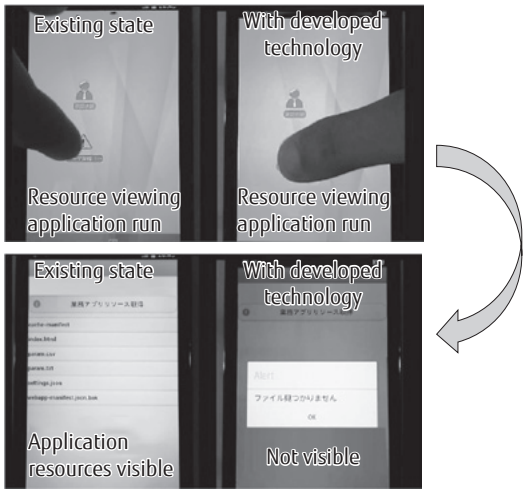

Figure 5
Operation example of secure application execution.

5. Use cases

Specific use cases of the present technology described up to now are shown in **Figure 6**.

Possible use cases can be roughly divided into those where smart devices are used in facilities such as stores and schools and where sales representatives and maintenance personnel carry smart devices to make use of them.

In the former, applications that are optimally suited for individual stores or individual places in a store can be automatically configured to deal with customers. Other examples include automatic distribution of education materials to students who have entered a classroom and provision of services that are only available in particular places. In addition, restriction of use outside the facilities prevents the information from being unnecessarily taken out.

For the latter, information about specific customers or equipment to be maintained that differs for each

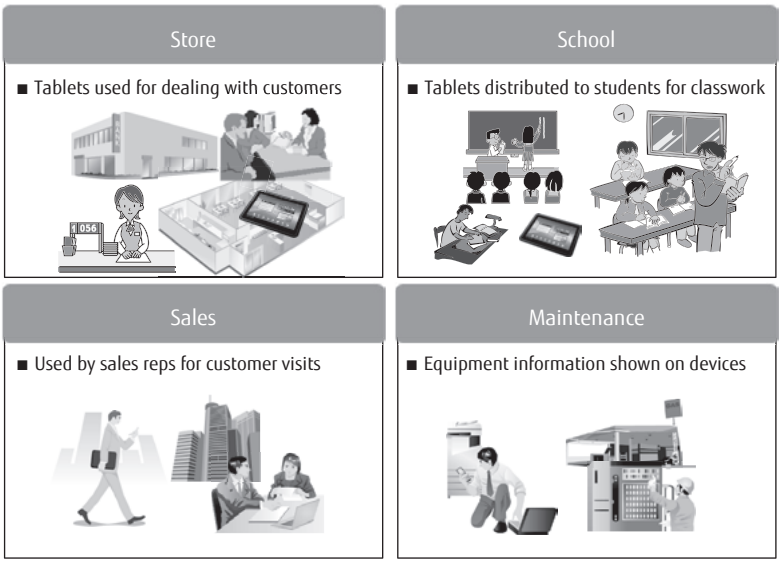

Figure 6
Use cases of present technology.

destination to visit can be shown on the devices. In this way, information can be isolated for each customer and only the information required in each particular location can be used in a given place.

The two technologies are capable of protecting these types of use.

6. Conclusion

This paper has described platform technology for realizing secure application management and execution integrating smart devices and cloud services, and its application to business use.

The technology is characterized by the fact that it creates an isolated work space in a personally owned device in order to enable and disable that work space according to changes in the user's situation. Technologies used for that purpose are Context Desktop, which groups applications by the condition of operability and switches applications according to the condition, and secure execution platform technology capable of appropriately controlling operation while protecting applications. In this way, managed security can be ensured and applications securely executed without sacrificing the convenience of smart devices.

We plan to apply this technology to cloud service products so that the services described by the use cases can be realized.

References

1) Packaged Web Apps (Widgets). *http://www.w3.org/TR/widgets/*
2) Focusing on BYOD Solutions. *Nikkei Communications* May issue, pp. 70–73 (2013) (in Japanese).
3) Fujitsu Fsas: Desktop Virtualization Service (in Japanese). *http://jp.fujitsu.com/group/fsas/services/infra/virtualization/desktop/*
4) T. Matsumoto et al.: Context Desktop Technology, *Fujitsu Sci. & Tech. J.* Vol. 49, No. 2, pp. 178–183 (2013).
5) H. Ito et al.: Application Push & Play – Proposal on Dynamic Execution Environment Combined with Personal Devices and Cloud Computing. *International Journal of Informatics Society (IJIS)*, Vol. 4, No. 3, pp. 135–142, December 2012.
6) Fujitsu: Fujitsu Develops Platform Technology for Secure Application Execution on Smartphones for Business Use. *http://www.fujitsu.com/global/news/pr/archives/month/2012/20120831-02.html*
7) K. Nimura et al.: A Secure Use of Mobile Application with Cloud Service. SmartApp (International Workshop on Smart Mobile Application), June 2012.
8) Fujitsu: Fujitsu Introduces FUJITSU Mobile Initiative to Provide Structure for Mobile Products and Services Lineups. *http://www.fujitsu.com/global/news/pr/archives/month/2013/20130827-01.html*

Hidenobu Ito
Fujitsu Laboratories Ltd.
Mr. Ito is currently engaged in research and development of mobile application execution platform technology.

Kazuaki Nimura
Fujitsu Laboratories Ltd.
Mr. Nimura is currently engaged in research and development of mobile application execution platform technology.