A Secure and Reliable e-Wallet using a Smart SSD

Im Y. Jung, Gil-Jin Jang

School of Electronics Engineering, Kyungpook National University, Republic of Korea
iyjung@ee.knu.ac.kr, gjang@knu.ac.kr

Abstract: An Electronic Wallet (e-Wallet) application requires a secure and reliable transaction against attacks and failures. Internet of Things (IoT) is a more vulnerable environment to e-Wallet attacks because both data and the computing environment can move along with the users. This paper proposes a secure and reliable e-Wallet application using a Smart Solid State Drive (SSD). The proposed scheme copes with the security problems inherent to a changing society, pursuing ubiquitous computing using a high-tech Smart SSD.
[Jung I, Jang GJ. A **Secure and Reliable e-Wallet using a Smart SSD**. *Life Sci J* 2014;11(7s):117-121] (ISSN:1097-8135). http://www.lifesciencesite.com. 21

Keywords: Electronic Wallet; Internet of Things; Security; Reliability; Smart SSD

1. Introduction

Hardware is developing toward increased levels of integration. Although a high degree of integration reduces the size of electronic devices, the performance and functions of the devices should either remain unchanged or be improved. Small-sized devices satisfy user convenience and aesthetic demands. For example, smartphones, which evolved from the traditional telephone, are also used as small computer devices. Current Solid State Drives (SSDs), which are smaller and have a larger storage capacity than ever before, are set to replace magnetic hard disks owing to their fast data access ability and cheaper price. These days, processors and RAM, which were previously separate from storage, are being embedded into SSDs.

Taking advantage of the mobility of small-sized user devices, Internet of Things (IoT) lets users enjoy a sense of freedom through a ubiquitous computing environment. More than ever, users want to avail of services on the go. However, there are technical issues to be addressed for freer user movement: the secure management of data and a reliable computing environment for sensitive applications such as e-health care, e-banking, and e-payments.

An Electronic Wallet (e-Wallet) application provides a means of maintaining important data such as secret codes including passwords, credit card information, and e-money just like in a real wallet. Today, many different services allow electronic payments. Examples include mobile credit cards [15] and (mobile) T-money [8]. Mobile credit cards are also a type of application installed in a Universal Subscriber Identity Module (USIM) [17-18] chip or other type of smart card[1], and can be used as a general credit card. However, users should keep a secret code to submit when using a mobile credit card. When T-money, a rechargeable transportation card, is implemented as a smart card, it can be used to store e-money. People cannot look in the smart card. They can pay or check the balance of the e-money in the smart card only by the smart card reader.

Because e-money has the same value as cash, an e-Wallet, which is used to manage and make payments with e-money, should meet a certain level of security and reliability. Basically, an e-Wallet should support secure data management, reliable recharging, and fault-tolerant transaction management. In an IoT environment, an e-Wallet should allow user mobility. Because user-requested services can move along with users and can be provided at any location using IoT, issues of security and reliability have emerged. Therefore, the security and reliability of an e-Wallet in an IoT environment are difficult problems to resolve.

This paper proposes a secure and reliable e-Wallet application using a Smart SSD. In particular, the proposed scheme provides an e-Wallet on a Self-organizing Software platform (SoSp) which is one type of IoT platform with the security and reliability maintained by the Smart SSD.

The remainder of this paper is organized as follows. A Smart SSD is introduced in Section 2. In Section 3, an e-Wallet applied in IoT is described, particularly in a SoSp network. The security and reliability of an e-Wallet using a Smart SSD is discussed in detail in Section 4. Section 5 describes previous work related to this issue. Finally, some concluding remarks are provided in Section 6.

[1] A smart card, chip card, or integrated circuit card (ICC) is any pocket-sized card with embedded integrated circuits [9].

2. Smart SSD

An SSD is a large storage drive that uses NAND Flash Memory. Modern SSDs provide high performance for concurrent random writes, and have powerful processors, memory, and multiple I/O channels for flash memory, enabling In-Storage Processing (ISP) with almost no hardware changes. Figure 1 shows a modern SSD where ISP can be utilized.

A Smart SSD, which includes powerful CPUs and RAM, has been proposed as an advanced storage drive upon which downloaded programs can be directly executed [1]. A Smart SSD furthers energy conservation by reducing the number of data transfers and through efficient data processing using ISP.

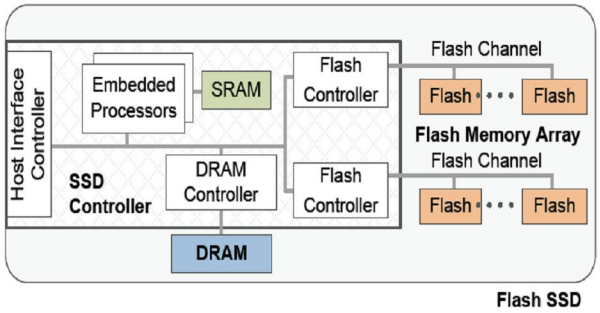

Figure 1. Modern SSD equipped with processors and RAM (adopted from [1])

3. e-Wallet in Internet of Things

3.1 SoSp Network as an IoT

A Self-organizing Software platform (SoSp) [7] is one type of IoT framework. Various services connected through welfare devices such as electrocardiogram-measuring and medicine-administrating devices can be provided using an SoSp. The well-being services including such health services can follow users because SoSp supports ubiquitous computing; users can use their services at any location where an SoSp is implemented.

Because the well-being services are very important for elderly, sick, and disabled users, it is important to develop an easy-to-use interface for such users. Electronic transactions can expand offline businesses and help develop a nation's economy. On one hand, people can enjoy the convenience of online transactions. On the other hand, they also risk exposure to hackers and other security threats. To strengthen security, important data can be stored on a secure device such as a smart card. Alternatively, people can carry an item such as a credit card issued by a payment company. For online transactions using such cards, users should maintain a secret code such as a password. However, it may be a burden for the disabled, patients, or the elderly to have to memorize their secret codes or carry different cards issued by different companies.

An SoSp network has a strong point for elderly, sick, or disabled users because it can implement IoT, which enables computing environments or services to follow users who are unable to move about freely. However, the security issues inherent to ubiquitous computing are obstacles to well-being services provided by an SoSp. This paper addresses the security issue of an e-Wallet in an SoSp network and proposes a secure e-Wallet application using a Smart SSD.

3.2 e-Wallet Application in SoSp Network

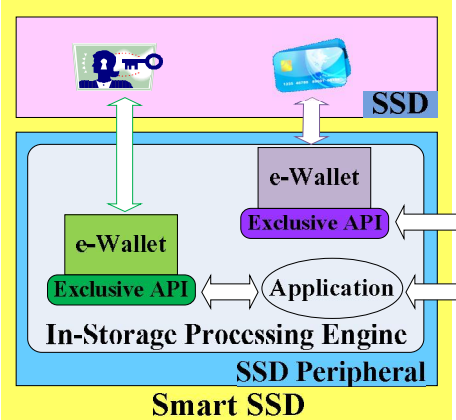

Figure 2. e-Wallet in Smart SSD

Figure 2 shows e-Wallets installed on a Smart SSD. An e-Wallet, which contains passwords, personal information, mobile credit cards, and e-money, can be used for personal identification and payment.

Because an e-Wallet is an application, an instance of the e-Wallet can be downloaded and processed. An e-Wallet application is generally intended to be securely downloaded and processed on a smart card. However, users should carry the card or device in which the card is embedded. These days, however, users carry various types of cards: credit cards, debit cards, point cards, mileage cards, T-money, and so on. To reduce the number of cards in a user's wallet, mobile credit cards have been proposed. A mobile card, which can be used like a credit card, is an application downloaded and installed on the USIM chip of a smart phone; as a type of smart card, a USIM chip generally maintains the user's identity information for accounting purposes. Owing to the limitations in chip size and power supply, a smart card cannot store large amounts of data. In addition, it cannot support heavy and lengthy processing [11]. An e-Wallet can be downloaded and installed on any secure device. A smart SSD is a secure device with a

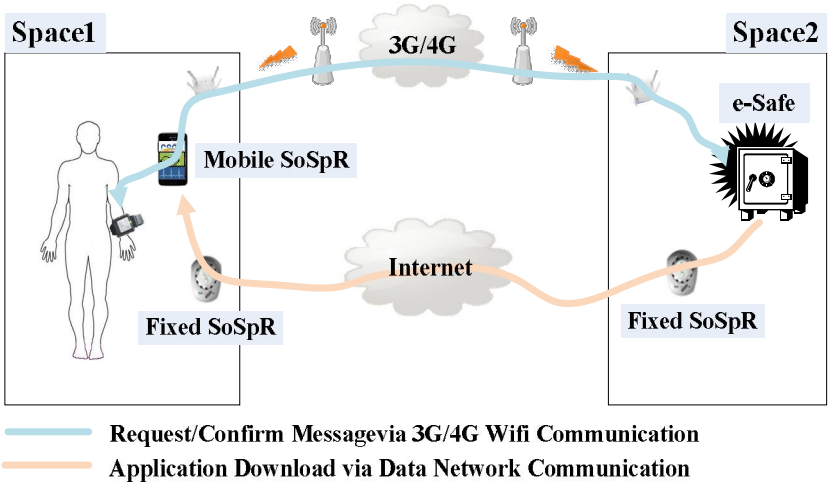

Figure 3. SoSp Domain for e-Wallet

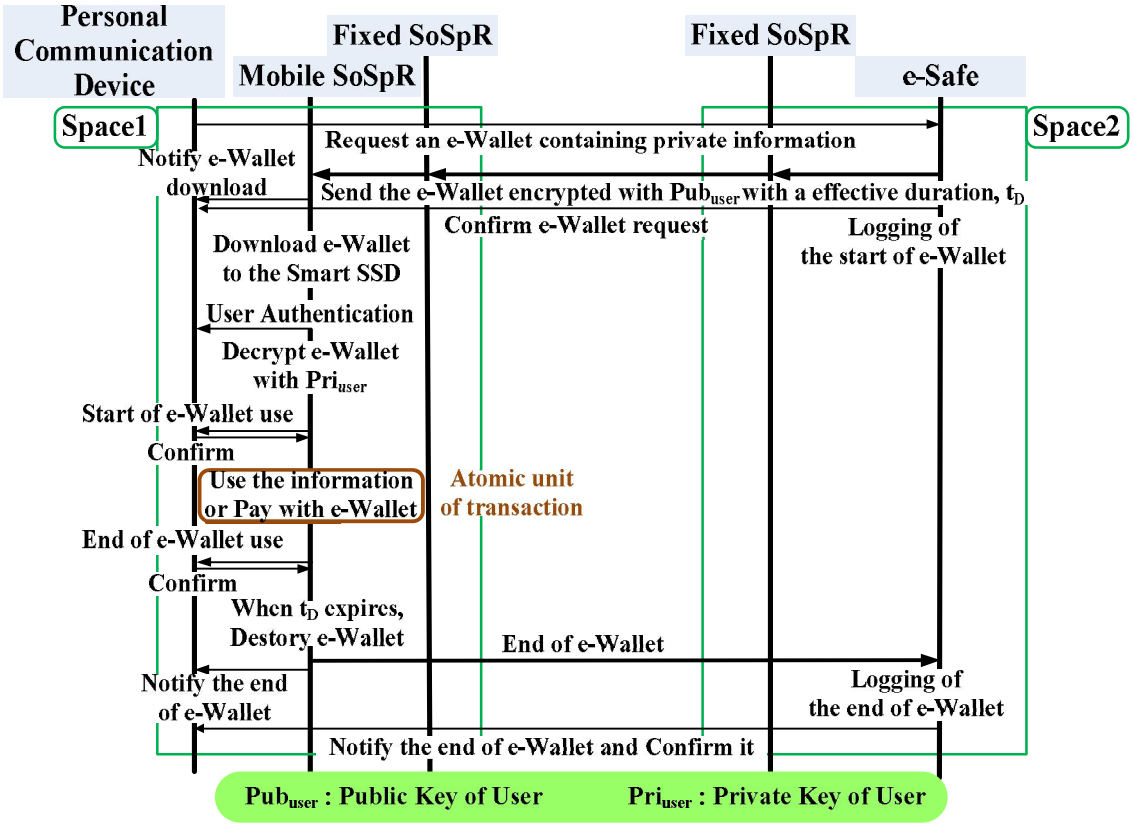

Figure 4. A Secure and Reliable e-Wallet in a SoSp Network

larger amount of storage and more powerful processing units than a smart card.

4. A Secure and Reliable e-Wallet using a Smart SSD

As shown in figure 2, an e-Wallet application is downloaded and installed on a Smart SSD. Just as a real wallet is used to keep important personal information, an e-Wallet can be replenished with additional e-money. An e-Wallet pays for items and services using e-money, which it manages using the ISP of the Smart SSD. The only way an e-Wallet installed on a Smart SSD can communicate with the outside world is through exclusive e-Wallet APIs. Accessing the important data and e-money stored in an e-Wallet directly is prohibited. Because there are no gaps exposed to an attack between the SSD and peripheral ISP components, an e-Wallet is secure in a smart SSD. In addition, reliable transaction management is possible because all e-money processing is done on the Smart SSD.

The following section describes how a vulnerability caused by the service mobility of IoT can be addressed using a Smart SSD in detail.

Figures 3 and 4 show a secure e-Wallet scheme in an SoSp network. There are two communication channels, one for notification messages for the downloading and completion of e-Wallet transactions between personal communication devices such as PAAR watch and e-Safe, and the other for the downloads of e-Wallet and add-ons.

There are two types of core devices in an SoSp, mobile SoSpR and fixed SoSpR. SoSpR indicates an SoSp-Router. As an identifiable node, an SoSpR can communicate other SoSpRs and provide many ubiquitous services. A fixed SoSpR attached to the ceiling or wall of a unit space, communicates with the devices in the unit space. It communicates with other fixed SoSpRs through a wired data network. However, it interacts with mobile SoSpRs installed on mobile devices such as smartphones or other mobile devices using one-hop wireless communication; one-hop communication simplifies the routing issue caused by multi-hop communication. The two types of SoSpRs can both use a smart SSD because such drives currently include their own processors, memory, storage, and communication devices [16].

When the user brings up their e-Wallet by touching the app button on their personal communication device such as a PAAR watch [7], the request is delivered to his/her e-Safe by the smartphone through a 3G/4G network. An e-Wallet is downloaded from e-Safe, which keeps critical private information and issues the instances of e-Wallet containing this information. The e-Safe contains many e-Wallets of the user, and encrypts e-Wallets containing information requested by the user as well as the effective period, $t_{D,}$ using the user's public key, Pub_{user}. In addition, it sends an encrypted e-Wallet to the location the user wants through fixed SoSpRs on the data network. The location notifies the personal device of the e-Wallet download. The location can be a mobile SoSpR such as the user's smartphone with an installed smart SSD. To use the e-Wallet, the user should decrypt it using his/her private key, Pri_{user}. Before decryption, the user should be authenticated to use Pri_{user} in the smart SSD of the mobile SoSpR. Such authentication should provide an easy interface and be exact. Biometric authentication can be a good choice. After decryption using Pri_{user}, the user can access their private information such as passwords, e-money, and mobile cards provided by the e-Wallet. The critical information is passed to the applications that need it directly on the same smart SSD through the exclusive APIs of the e-Wallet. The use of e-money and private information is controlled by an internal timer. The user can use the information provided by the e-Wallet during a predefined period of time after authentication. After the time period expires, the user should be authenticated again before using the information. The timer plays the role of an e-Wallet lock. In addition, after t_D expires, the e-Wallet is destroyed. If the user wants to use the e-Wallet again, they should download a new one.

The entire process of an application requesting information in an e-Wallet is considered as a transaction unit. A connection failure during the e-Wallet processing rolls the application back to the state before the e-Wallet was called. The e-Wallet does not approve the transaction and related payment until it receives a successful reply from the application requesting the information.

Security vulnerabilities from gaps and exposed communication between components related to the processing can therefore be avoided. Because there is no external intervention during the processing in a smart SSD, it is easy to control the failure states and ensure processing consistency. An easy-to-use interface is very important for disabled, elderly, and sick users because they may be mentally and/or physically hindered. The proposed scheme does not require users to memorize any passwords or carry any additional items. The only interface required is a touch screen. The user can call up the e-Wallet they want and be authenticated through a biometric authentication process such fingerprint verification using only a touch screen. No critical information is revealed during all the processing.

5. Related Works

IoT and ubiquitous computing are important research subjects [19][23-24]. IoT frameworks have been proposed and implemented to realize ubiquitous computing. SoSp is one such framework. Services for IoT frameworks have also been suggested and their trial versions have been implemented.

It is important to check whether IoT services have real-life practicality in terms of performance, fault tolerance, and security. Because existing models of reliability and security for legacy computing environments cannot be adopted by IoT without modification, new models should be developed for IoT [20-22]. Currently, there are no security models for SoSp services.

A smart SSD is about to be released, and services utilizing a smart SSD are being studied [2][25].

This paper addressed the issues of security and reliability of a critical IoT service, i.e., an e-Wallet using a smart SSD.

6. Conclusion and Future Works

This paper proposed a secure and reliable e-Wallet application using a Smart SSD. The proposed scheme allows an e-Wallet application to be provided on an SoSp network, which is a type of IoT, with security and reliability achieved using a Smart SSD. An e-Wallet is an application allowing users to freely make payments and identify themselves in an Internet-based e-World environment because it maintains identity information or secret codes used for mobile credit cards or e-money. SoSp can provide improved well-being services for disabled, elderly, and sick users by supporting critical features such as payment and identification capabilities using a Smart SSD.

As future work, we plan to study secure Smart SSD APIs for the proposed e-Wallet application and secure authentication in IoT.

Acknowledgements:

This work was supported by the IT R&D program of MSIP/KEIT. [10041145, Self-Organizing Software platform (SoSp) for Welfare Devices]

Corresponding Author:
Prof. Gil-Jin Jang
School of Electronics Engineering
Kyungpook National University
Republic of Korea
E-mail: gjang@knu.ac.kr

References

1. Do J. et al. Query Processing on Smart SSDs: Opportunities and Challenges. SIGMOD 2013.
2. Kang Y. et al. Enabling Cost-effective Data Processing with Smart SSD. IEEE Symposium on Massive Storage Systems and Technologies (MSST) 2013.
3. Smart Card Alliance. Security of Proximity Mobile Payments. White paper 2009; www.smartcardalliance.org
4. Arkko J., et al. Weak Authentication: How to Authenticate Unknown Principals without Trusted Parties. Lecture Notes in Computer Science 2003.
5. Vincent K., Cull T. Cell phones, electronic delivery systems and social cash transfers: Recent evidence and experiences from Africa. International Social Security Review 2011; 64.
6. Sander T., Ta-Shma A. On Anonymous Electronic Cash and Crime. ISW 1999; LNCS 1729: 202-206.
7. Kim H.Y. et al. Self-Organizing Middleware Platform Based on Overlay Network for Real-Time Transmission of Mobile Patients Vital Signal Stream. The Journal Of Korea Information And Communications Society (J-KICS) 2013; 38C(7):630-642.
8. T-money, http://en.wikipedia.org/wiki/T-money
9. Smart Card, http://en.wikipedia.org/wiki/Smart_card
10. Mobile T-money, http://www.t-money.co.kr/
11. Shanghai Fudan Microelectronics Co., LTD. FM1216 Series CPUCard Chip: Datasheet. 2013; http://www.fmsh.com
12. Yelopay. https://www.yelopay.com
13. PayPal. https://www.paypal.com
14. WIKIPEDIA, http://en.wikipedia.org/wiki/Escrow
15. http://www.looppay.com/product/fob/
16. Kim T.H. et al. A Middleware Architecture for Dynamic Reconfiguration of Agent Collaboration Spaces in Indoor Location-aware Applications. International Journal of Distributed Sensor Networks 2014.
17. http://en.wikipedia.org/wiki/USIM
18. http://en.wikipedia.org/wiki/Universal_Subscriber_Identity_Module#USIM
19. Murphy A.L., Picco G.P., Roman G.C. LIME: a middleware for physical and logical mobility. International Conference on Distributed Computing Systems 2001; 524–533.
20. Stajano F. Security Issues in Ubiquitous Computing. Handbook of Ambient Intelligence and Smart Environments 2009.
21. Weber R.H. Internet of Things – New security and privacy challenges. Computer Law & Security Review 2010; 26:23-30.
22. Heer T. et al. Security Challenges in the IP-based Internet of Things. Wireless Personal Communications 2011; 61(3):527-542.
23. Conti M., Kumar M. Opportunities in Opportunistic Computing. Computer 2010; 43(1):42-50.
24. Zhu F., Mutka M., Ni L. Service Discovery in Pervasive Computing Environments. IEEE Pervasive Computing 2005; 4(4): 81-90.
25. Kim S. et al. Fast, energy efficient scan inside flash memory SSDs. International Workshop on Accelerating Data Management Systems (ADMS) 2011.

4/28/2014