Singapore Management University

Institutional Knowledge at Singapore Management University

4-2009

The Digital Wallet: Opportunities and Prototypes

Rajesh Krishna BALAN
Singapore Management University, rajesh@smu.edu.sg

Narayanasamy RAMASUBBU
Singapore Management University, nramasub@smu.edu.sg

Follow this and additional works at: https://ink.library.smu.edu.sg/sis_research
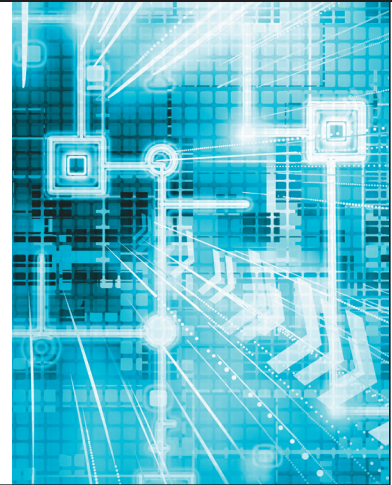
Part of the Software Engineering Commons

Citation

The Digital Wallet: Opportunities and Prototypes

Rajesh Krishna Balan and Narayan Ramasubbu
Singapore Management University

Example digital wallet applications support secure P2P mobile cash transactions and alleviate point-of-sale confusion for consumers using multiple payment, discount, and loyalty cards.

Physical wallets present numerous problems. If you're standing in a checkout line, retrieving the right amount of cash or the appropriate combination of payment, discount, and loyalty cards can be time consuming. Worse, if you lose your wallet or it's stolen, you have to remember which cards you had in it and manually cancel each one, as well as order new cards or identification documents—driver's license, health and auto insurance cards, and so on.

One solution to these problems is to replace the physical wallet with a digital wallet integrated into an existing mobile device like a cell phone. This would let users manage multiple monetary and ID instruments and quickly search them by name, type, or other keywords. In addition, a digital wallet would enhance security as all data would be encrypted and backup options would make recovering from loss or theft easier.

The idea of a digital wallet isn't new. Consumers in Japan and South Korea can already use their cell phones to pay for groceries, order drinks from a vending machine, and even identify themselves at airline ticket counters. Companies in other countries, includ-ing the US and Sweden, are planning to roll out digital wallet applications within the next two years.

We have developed two novel digital wallet solutions for use in Singapore: mFerio, a secure peer-to-peer (P2P) mobile cash payment system; and pFerio, a point-of-sale information system for highlighting the best deals to consumers using multiple payment, discount, and loyalty cards.

THE SINGAPORE FACTOR

The convergence of four trends has made Singapore a ready market for digital wallets.

First, the population is very tech-savvy—almost everyone carries a cell phone. Singaporeans are thus more likely to use digital wallet applications integrated with their cell phones, as in South Korea and Japan.

Second, cell phone technology is now mature enough—in terms of computational capability, battery lifetime, memory, input mecha-nisms, and graphical user interfaces (GUIs)—to support digital wallet solu-tions. Newer cell phones incorporate near field communication (NFC) technology such as Sony's FeliCa chip, which provides highly secure, very-short-range, very-low-power, easy-to-set point-to-point contactless communication between devices.

Third, every major bank in Singa-pore offers Internet banking services. These banks are constantly looking for ways to increase the number of online financial transactions, which are cheaper for them to process. A digital wallet achieves this and also lets the banks leverage their existing Internet infrastructure to support more products and introduce new services that could help differentiate them from their competitors.

Finally, Singapore's regulatory bodies are actively seeking to inte-grate as many financial services as possible. As the Japanese and South Korean experiences have shown, government participation is crucial to successful deployment of the tech-nology. Our preliminary discussions with some of these stakeholders sug-gest that they are keen to provide a digital-wallet-like solution that inte-grates all current payment schemes and can serve as the vehicle for new payment models.

SECURE P2P MOBILE CASH PAYMENTS

Most current mobile payment solu-tions require infrastructure support. At least one of the parties involved

in a transaction must be connected to some back-end payment server via either the short message service (SMS) or Global System for Mobile Communications (GSM)/code division multiple access (CDMA)-based technology.

Consider the following scenario: Bob is attending a conference and takes a taxi from the airport to the downtown hotel hosting the conference. Due to the building layout, the taxi can only let Bob out at an underground lobby. Bob reaches his destination and tries to pay the taxi driver using his cell phone. However, neither can get a signal on their wireless equipment (cell phone and radio receiver, respectively). Bob has to dig cash out of his wallet to pay the driver as well as keep track of the receipt to be reimbursed later.

To support secure P2P mobile cash transactions, mFerio combines a digital cash system with an authentication system. No additional connectivity or infrastructure beyond that of standard cell phones is required. We developed mFerio as a Java ME application on Nokia 6131 phones with built-in NFC capability.

Figure 1 illustrates a P2P transaction using mFerio. After clicking on the application, the user performs six steps.

The user first authenticates herself by typing in her PIN (Figure 1a). She then selects a payment task from the main menu (Figure 1b). She can initiate a transaction to either pay someone or request payment. She can also receive payment requests on this screen. After selecting a task, the user enters the reason for payment from a predefined list of pull-down options, types in the amount to be paid, and clicks okay to proceed.

In the transaction's second step, the user holds her phone next to that of the recipient, which must also be running the mFerio application
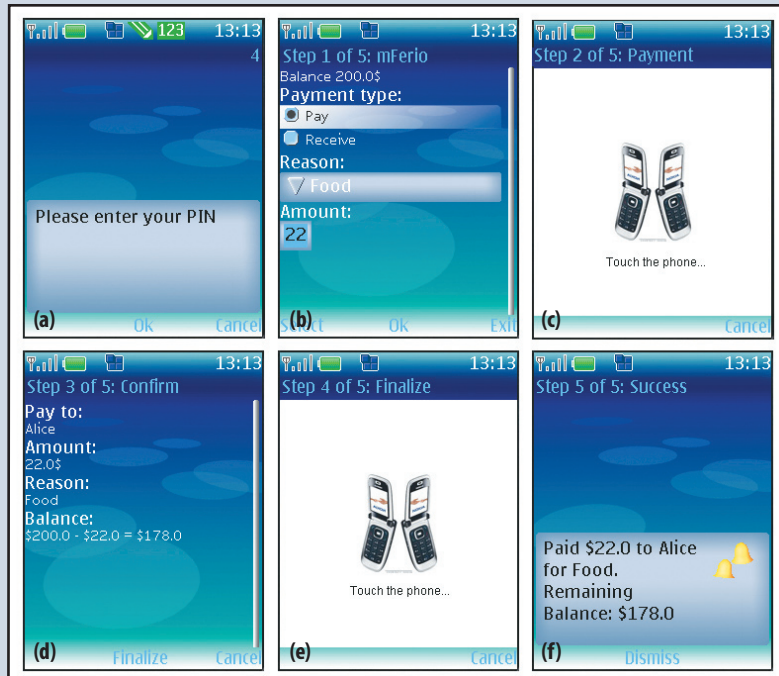

Figure 1. mFerio peer-to-peer payment system screenshots. To make a P2P transaction, the user (a) authenticates, (b) enters payment details, (c) exchanges initial payment information and establishes a secure connection, (d) confirms payment details, (e) finalizes payment, and (f) confirms payment.

(Figure 1c). During this first connection, mFerio creates a private session key for both the initiator and recipient using the Diffie-Hellman cryptographic protocol. It then encrypts and exchanges basic information with its peer using an adapted Even-Goldreich-Yacobi protocol.

The system displays this basic information about each party along with the transaction details. For example, as Figure 1d shows, the user sees the recipient's name, the payment amount and reason for payment, and the values of her stored cash before and after the transaction. The recipient sees something similar. Both parties must agree to the payment to proceed to the final step; otherwise mFerio cancels the transaction.

The user "touches phones" with the recipient once more to complete the transaction and exchange the agreed-upon payment tokens, again using the Even-Goldreich-Yacobi pro-

tocol (Figure 1e). Finally, as Figure 1f shows, mFerio displays a "success" summary page and stores this page as an automatically signed receipt.

In an evaluation of mFerio using a total of 104 participants, mostly undergraduate students, we found that the application outperformed regular cash transactions in terms of speed, accuracy, ease of use, and cognitive load in all but the most basic situations—where a single note or coin was being exchanged.

ALLEVIATING POINT-OF-SALE CONFUSION

Consider another scenario: Jill is at the grocery store checkout counter with a cart full of items. While the cashier is ringing these up, Jill thinks about how to pay for her purchases. Should she use the Visa card with a cash-back bonus or the AMEX card with frequent-flyer points? Which card will give her the best deal? Jill also remembers that

she can get additional discounts if she pairs particular payment cards with the store loyalty card. However, she can't remember which cards the store accepts for this extra discount. Unfortunately, the cashier only knows about two cards, neither of which Jill possesses.

This scenario, in various forms, is commonplace in retail locations. It also reflects a typical pervasive computing problem—namely, users possess large amounts of information of which they're only vaguely aware, and they have no idea what is useful in different contexts. For example, the choice Jill makes in one grocery store may not be applicable in another that offers separate discounts.

The complexity in this scenario arises from the fact that users typically have many payment, discount, and loyalty cards while retailers have their own preferred payment cards and discount, loyalty, and reward schemes that are time, store, product, and even usage dependent. Even with a complete list of retailer options, finding the optimal set of cards for a particular situation can be cognitively demanding for users.

Providing users with such information is nontrivial, as many combinations can provide similar overall deals but in different ways—for example, one may provide cash rebates and another frequent-flyer miles. Users need to be able to quickly find the cards that give them the deals they want.

To address this problem, we have developed a cell phone application, pFerio, that consists of three components: XML schemas for describing user and retailer card details, mechanisms to find the best deal, and a GUI that displays the results in an understandable form.

The system first uses XML schemas to describe the cards currently in a user's physical wallet. pFerio then transfers these descriptions into the secure storage area of the user's NFC-
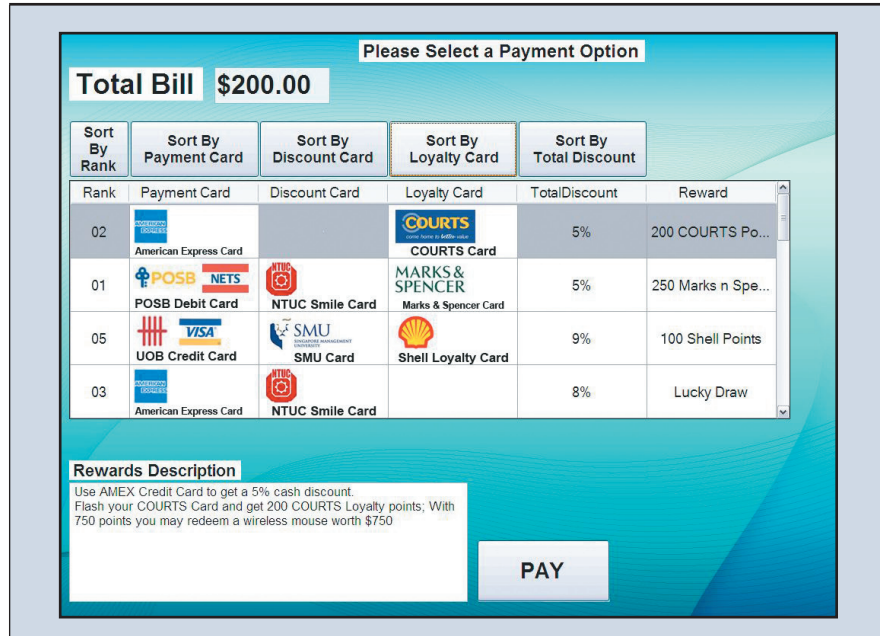

Figure 2. pFerio retailer checkout interface. Users can select their preferred deal using multiple ranking criteria. (All company logo images are owned by the respective companies.)

enabled phone—that is, the digital wallet.

At checkout time, users click on pFerio, authenticate themselves, and start the point-of-sale application. They place their phone on a reader provided at the checkout counter. The system reads the XML schemas and runs various algorithms to find the best matches. From that point, users interact with the system using the LCD checkout screens provided by the retailer, as shown in Figure 2. They select the cards that give the deal they want and make the payment, completing the checkout procedure.

Usability tests of pFerio using 35 participants, again mostly undergraduate students, showed that pFerio was much easier to use than traditional methods such as asking the cashier about the deals or remembering them yourself.

We're currently designing and developing additional digital wallet implementations for use in Singapore. We're also planning to deploy mFerio and pFerio in real-world set-

tings and conduct more and larger usability studies. **C**

Rajesh Krishna Balan is an assistant professor in the School of Information Systems at Singapore Management University. Contact him at rajesh@ smu.edu.sg.

Narayan Ramasubbu is an assistant professor in the School of Information Systems at Singapore Management University. Contact him at nramasub@smu.edu.sg.

Editor: Bill N. Schilit, Google; bill.schilit@computer.org