Selection of the Appropriate Wireless Payment Technology in Mobile Banking

A. Sanayei
Faculty of Administrative Sciences & Economics
email: Info@Drsanayei.com

A. Ansari
PhD. Candidate, Faculty of Administrative Sciences Economics
University of Isfahan
email: Noosh.azar@gmail.com

Abstract
As mobile technologies are becoming more advanced and mobile devices are making a big impact on daily life, a new type of payment system named mobile payment (m-payment) has emerged, enabling users to pay from their wireless devices especially mobile phones. This paper analyzes currently available Wireless-payment systems and finds the stored-value card to be the best overall payment scheme for mobile banking. A good payment protocol should balance the requirements of security and convenience. WAP (Wireless Application Protocol) is one of the prevalent wireless technologies is being embraced by the banking sector. This leads us to suggest that multiple usages can be added to m-payment systems with higher security merit so that they can gain a critical customer base. This study is trying to compare the way of WAP, with other payment technologies and wants to show that by using Analytic Hierarchy Process (AHP) method in mobile banking can provide the goals of the users properly.

Keywords: Wireless Payment, Mobile Banking, Analytic Hierarchy Process, WAP.

Introduction
Mobile payment is gaining momentum, but as soon as discussions start on mobile payment solutions, concerns are raised on the security of these concepts. The most prominent challenge arising from these innovations relates to the concept of security. Mobile payment means wireless based on electronic payment for M-commerce to support point-of-sale/point-of-service (POS) payment transactions using mobile devices such as cellular phones, smart phones and personal digital assistants (PDAs), or mobile terminals. In general, M-payment systems is widely used by merchant to make wireless based payment, content vendors, information and service providers to process and support m-payment transactions based on wireless commerce applications.

Organizations are developing wireless based online payment applications to expand their business globally, it increases the growing need of regulatory requirements for the
Selection of the Appropriate Wireless Payment Technology in Mobile Banking

... protection of confidential data, and especially in internet based financial areas. Existing internet based authentication systems often use either the Web or the Mobile channel individually to confirm the claimed identity of the remote user (Antovski & Gusev, 2003).

The existing m-payment systems can be classified as:

*Account-based payment systems

There are three subdivisions of account-based M-payment systems:

1. The payment system based on mobile phone: which facilitates the customer to do commerce and make payment over mobile phones. This system is unable to make peer-to-peer payments.

2. The Smart Card Payment systems: The smart card exemplifies the real-time payment method and is the only payment scheme capable of converting stored value back to real currency. The SIM cards used within the GSM phone are smart cards as well. Their size and compatibility with the magnetic stripe card theoretically makes the smart card an ideal carrier for personal information, such as secret keys, passwords, customization profiles and medical emergency information.

3. Credit-Card: The credit card is the most popular payment method for online shopping today, despite its vulnerability to security breaches when used online (Turban et al., 2000).

*POS payment systems

1. Automated POS payments.
2. Attended POS payments.

*Mobile wallets: Mobile money allows for any mobile phone subscriber – whether banked or unbanked – to deposit value into their mobile account, send value via a simple handset to another mobile subscriber, and allow the recipient to turn that value back into cash easily and cheaply (GSMA, 2009). Customers can do multi-home with several debit or credit payment instruments in a single wallet. Several implementations of wallets that are company-specific are in use globally.

Mobile Banking

Mobile Banking, as has been demonstrated, gained non-negligible relevance for banks today. Developments in the banking sector, e.g. increased competition on account of technological developments coupled with the process of globalization have produced new challenges for banks. Mobile Banking presents an opportunity for banks to retain their existing, technology-savvy customer base by offering value-added, innovative services. It might even help attracting new customers (Krueger, 2001). Further, Mobile Banking presents a chance to generate additional revenues. An effective approach to security involves a delicate trade-off between security and customer convenience. Often customers can perceive security requirements as an inconvenience (Ondrus & Pigneur, 2004).
Therefore, wireless technology has made many of the components of its mobile security approach optional. This allows banks and credit unions that select wireless payment technology solution to determine the best blend of security and convenience for their customers. The majority of security approaches today work along two lines: first, make it more difficult for an attacker to obtain customer credentials; second, make it more difficult for an attacker to use those credentials to execute a fraudulent transaction. Customer education is an important step in the first approach. A knowledgeable customer is less likely to be ensnared by phishing attempts. Similarly, a bank or credit union may eschew the use of a channel that may be used in phishing.

**Wireless Payment Transactions**

The use of a new generation of embedded computer devices is extending the potential of solutions form-business. The goal is to achieve reliable, scalable and secure e-business solutions by connecting any device with any data through any network. Since the capabilities of the devices and networks are evolving quickly – enhancing the richness and usability of applications – this adds to the complexity of the Wireless Payments challenge (Das, Saxena, & Gulati, 2005).

There are three main groups of actors on the wireless commerce stage. Network Service Providers, Financial Institutions and Retailers (or Merchants). The differing requirements of these groups leads to a natural tension, but for wireless commerce to become a reality, they have to work with each other. There is a large supporting cast who are set to benefit from wireless commerce. ISPs, Web hosting firms, smart card suppliers and the device manufacturers all have an important role to play, but it is the Network Service Providers and Financial Institutions and Retailers who must take the lead (Shon & Swatman, 1998). With Mobile Web, he/she uses his/her mobile phone’s web browser to access Online Banking account information. The applications include the same functionality as Mobile Web plus convenient one-touch access to the sign-in page. Mobile payment protocols must offer robust security because the financial data are sending over wireless networks. In this sense, customers and merchants require mutual authentication, payment authorization, confidentiality, integrity and non-repudiation (Heijden, 2002).

**Wireless Payment System**

Banks understand risk management, and they have the regulatory approval to take care of customers’ money. They also have a trusted brand and this is a major asset in lowering the consumer’s perception of financial risk in a new product area. Wireless processing via cell phone is probably one of more cost effective ways to process cards on the road. Not only does a service like this work with cell phones, but also any phone for that matter.

The organization offers its merchants multiple point-of-sale (POS) and networking
The wireless payment system is composed of initialization process and transaction process. Initialization process is to download program of payment system, formal authentication certificate and personal credit information to mobile device, to save them into non-volatile memory, while another one is executed every time of transaction through mutual exchange between connection server and mobile device. The wireless payment system has two methods for payment, which is based on card (hardware type) or not on card (software type). The method based on card is equipped with a smart card having various financial Payment system refers to a service to pay the charges using credit card, debit card or mileage when we purchase service and product on and off lines. The processing procedure of the payment system is generally divided into customer security, payment at POS, imposition and request of payment and liquidation between payment service provider and consumer. Most of the payment systems take similar procedure regardless of its technical method.

End-to-end security between the customer and the customer’s Bank cannot be built only based on WTLS(Wireless Transport Layer Security). A WAP (Wireless Application Protocol) gateway must be used as a bridge between the different protocols.

The organization needed to find a dependable wireless payment gateway provider that could provide a secure and reliable network and also work with them to activate their POS terminals for transaction processing. The security of the system also depends on the security of the messages sent by SMS and WAP. The user will get a SMS with the required details which are essential to identify and recognize the users initiated transaction (Schwiderski & Knospe, 2002).

Wireless Payment is the ability to initiate or confirm a payment transaction from a wireless device. The payment can be either:
- An immediate transfer of value from buyer to seller in exchange for goods or service.
- A promise to transfer value from buyer to seller in exchange for goods or service.

Wireless Payment is a complex solution that requires the integration of a number of industry players. Like any growth area there are many ingenious technologies offered by a range of innovators. There are many industry standards groups, each of which have a slightly different take on the needs of the market (Zheng & Chen, 2003).

**Mobile Payment Technologies**

The mobile technology landscape provides various possibilities for implementing m-payments. Mobile phone may send or receive information through channels like SMS, USSD or WAP/GPRS. The choice of the channel influences the way m-payment schemes are implemented. Secondly, the m-payment client application may reside on the phone or else it may reside in the subscriber identity module (SIM) (Lee, 2004). The detail about
customer’s bank account/credit/debit card is stored inside the phone/SIM. When customer wants to transfer the money to a merchant he accesses the application and enters phone/account number. The application running on his mobile encrypts the details of account-number/credit/debit-card including the amount to be transferred to the bank and on the contrary. Mobile payment is enabled by a variety of emerging technologies, many of which are still maturing. The key technologies are (Kim, 2004):
- WAP, including WAP Identity module (WIM) for additional security (Pradhan, Lawrence & Zmijewska, 2005).
- Bluetooth.
- Network, including GSM, GPRS, 3G.
- Mobile payment software.
- Smart card and SIMs.

At this time, developing countries banks provide mobile banking through three channels: through the WAP (Wireless Application Protocol), GPRS (General Packet Radio Service) and SMS (Short Message Service) using the WIG (Wireless Internet Gateway).

**Short Message Service (SMS)**

one of the most successful m-payment procedures relying on 2G networks, uses SMS technology to both send a customer a message with payment details, and to receive their PIN as authorization. SMS is a store and forward service that is inherently insecure because the messages are transmitted in the clear and stored in the clear at an SMS Centre before being forwarded to their intended recipients. SMS often suffers from latency problems. Time critical transactions should not rely on SMS channel. The ease of use of such systems is affected by the requirement to register on the internet beforehand. Use of SMS in the banking sector can be exceptionally varied and multifunctional, offering a whole new world of opportunities.

Managing customer relationships via mobile channels is proving to be a revenue-generating asset leading to new customers and business growth. As an interactive channel for personalized communication with customers in real-time, SMS is also a cost-effective solution with a positive impact on brand positioning.

**General Packet Radio Service (GPRS)**

GPRS is a packet-switched data service available to GSM users. This protocol has been designed to take care of the core banking security requirements. The protocol ensures both client and server trust and authenticate each other prior to sharing sensitive information. In addition to higher data rates, GPRS provides users with all time connectivity while only charged for the data viewed or received with a minimal on-line charge. GPRS [19] only uses its radio resources when users are actually sending or receiving data, therefore the
available radio resource can be concurrently shared between several mobile data users, rather than dedicating a radio channel to a single user for a fixed period of time. This efficient use of scarce radio resources means that large numbers of GPRS users can potentially share the same bandwidth and be served from a single cell (Dahlberg & et al, 2007).

**Wireless Application Protocol (WAP)**

WAP is an open international standard for applications that uses wireless communication. Its principal application is to enable access to the internet from a mobile phone or PDA. WAP allows people to conduct their business transactions through their mobile phone. As consumers have become more trusting of electronic payment systems, it is likely that this will positively influence consumer's choice to use WAP banking (Ratten, 2008).

Both WAP and SMS are capable of providing the authentication channels to support asymmetric signature operations. This is done by translating internet information into a format which can be displayed within the constraints of a mobile device. To obtain Internet access on a mobile device, the device should be WAP-enabled and the website information should be described in WML (Wireless Markup Language) format. Thus these cases have many difficulties with the launch of WAP, especially in Middle East, due to the slow speed and high charges when using WAP on GSM technology. The increase use of GPRS will see an increase popularity of WAP usage.

**Description of Research Approach**

As Analytic Hierarchy Process (AHP) is the widely used decision support tool in business and industry. Hierarchical analysis sub-divides a complex decision making problem into easily understandable hierarchy elements and makes decisions based on the elements. The method satisfies theorems such as reciprocal, homogeneity, dependency and expectation, and alternatives are extracted through four steps.

AHP has a number of advantages in the best selection of mobile payment. First, it can efficiently translate intricate problems into an orderly hierarchy, because of its strong capacity for solving multi-criteria decision problems (Azis, 2007). Secondly, the AHP approach is able to quantify the decision maker’s experiential judgments, particularly when the objectives lacked quantifiable data. Key factors affecting the best selection are identified and divided into different hierarchies corresponding to different evaluation levels. Experts are questioned to evaluate relative importance of each factor in a lower hierarchy relative to the corresponding factor in an upper hierarchy. Weights corresponding to the relative importance of all factors in each hierarchy can then be calculated. In addition, the factor appraising values have obtained by the questionnaire investigation, and then the appropriate
Wireless Payment Technology has calculated. An ordinal ranking based on the total value gained by each payment scheme determines their relative performance. Based on this analysis of the results, is suggested appropriate alternatives.

Criteria for Selecting Appropriate Factors

The alternatives of system quality include Security, Cost for Customer, Transmission Speed, Transmission Speed, Compatibility and Usability. With the aim of analyzing and comparing the diverse services, it is necessary to define a criterion (Hort, Gross & Fleisch, 2002). This is composed by:

- Security: Each permission is assessed according to the risk of being used by certain code or persons, as well as according to the consequences of possible misuse. Security contains such as: Privacy, anonymity, trustworthiness, regulatory framework, regulation and consumer protection (Karnouskos, Hondroudaki, Vilmos & Csik, 2004).

- Cost for Customer: There are two kinds of costs in adopting m-payment systems: fixed and transaction costs. Fixed costs refer to those of installing payment equipment and payment software.

- Cost for Bank Server: Depends on the amount of data required to be sent (Mobile payment forum, 2002).

- Transmission Speed: The ability to transmit across the network rich content – including voice, video, multimedia and text. The transmission speed of all the mobile banking depends on numerous factors. It depends on the strength of the signal received by the user’s mobile phone. Therefore it depends on the location of the user, the traffic of the network, the number of base towers in the area around the user’s mobile and etc. All these factors can influence the speed of transmission, thus no actual experiment can be conducted.

- Connection type and Reliability: Delivering time-sensitive information. The ability to connect to the service instantly

- Compatibility: Using subscriber data to personalize the user interface with the application and to customize the end-user experience

- Usability: Everybody can understand the policy used, as the value charged for the permission correlates to the real costs and the estimated risk. As for most of the mobile services, usability is a determining factor.

Alternative Evaluation Using AHP

Decision makers calculate the success factor and alternative elements of wireless payment through pairwise comparison matrix using AHP. The top hierarchy sets the goal of problem, the middle hierarchy sets criteria for defining alternatives, and lastly, alternative elements are extracted.
Selection of the Appropriate Wireless Payment Technology in Mobile Banking

Data Collection

An expert poll is considered as the best source for the sample data used in AHP method. Most of consumers still lack experience in using m-payment systems, therefore are used the expert poll to avoid sampling errors (Economides & Himmelberg, 1995). This study is conducted a survey of Internet IT engineers and scholars in Iran regarding their assessment of the three m-payment technology alternatives. Among the 64 interviewees, 30 were from technological and 20 from business research fields. In the survey, is asked the interviewees to measure the degree to which each payment system technology corresponds to the factors on a nine-level ordinal scale. The total value for each payment alternative is then derived by multiplying the data collected from the expert poll by the associated priority weights of all the factors (Salmeron & Herrero, 2004).

Table 1

<table>
<thead>
<tr>
<th>Value</th>
<th>Definition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Equal</td>
<td>Two activities contribute equally to the objective</td>
</tr>
<tr>
<td>3</td>
<td>Moderate preferred</td>
<td>Experience and judgment slightly favor one activity over another</td>
</tr>
<tr>
<td>5</td>
<td>Strongly preferred</td>
<td>Experience and judgment strongly favor one activity over another</td>
</tr>
<tr>
<td>7</td>
<td>Very strongly preferred</td>
<td>An activity is strongly favored over another and its dominance demonstrated in practice</td>
</tr>
<tr>
<td>9</td>
<td>Extremely strongly preferred</td>
<td>The evidence favoring one activity over another is of the highest degree possible of affirmation</td>
</tr>
<tr>
<td>2,4,6,8</td>
<td>Medium</td>
<td>Used to represent compromise between the preferences listed above</td>
</tr>
</tbody>
</table>

Figure 1 illustrates the process used to conduct an AHP evaluation. First Step, is constructed the hierarchical structure by which the causalities between the factors and alternatives are established. Second step, is calculated the priority weights among the factors through the pairwise comparison matrix. Third step, is calculated the total value for each payment alternative based on the priority weights multiplying the data from the expert poll.
Results

The results in Table-2 corroborate that Security factor more forcefully determine the performance of m-payment systems than other factors. Table 3 lists the scores for the three payment technology alternatives. The scores are obtained by multiplying the K-values assigned to the ordinal data collected from the expert poll by the associated priority weights of the factors. The findings reported in Table-3 are robust because AHP analyses using different value assignment methods produce consistent results. Table 3 shows that the WAP technology scores 166.68 points in total, the SMS technology 151.56 points and the GPRS technology 162.45 points. Therefore is conclude that the WAP technology is a superior m-payment instrument, and the SMS technology is the least desirable vehicle. The WAP technology earns the best score because it performs satisfactorily in all aspects. In particular, the WAP technology functions best in the security, Cost for Bank Server and Compatibility, scoring 36.25, 21.83 and 29.4 points, respectively.

In contrast, the SMS technology performs worst in the wireless payment technologies, gaining a Compatibility score of only 13.02 because it is the most deficient in convenience and merchant acceptance. Although the SMS technology has the first largest payment network (i.e., 29.4 points), the low levels of its other factors compromise its likelihood of being extensively accepted.

Table 2

<table>
<thead>
<tr>
<th>Factors</th>
<th>Percentage weight between the factors</th>
<th>Ranking</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>0.22</td>
<td>1</td>
</tr>
<tr>
<td>Cost for Customer</td>
<td>0.14</td>
<td>4</td>
</tr>
<tr>
<td>Cost for Bank Server</td>
<td>0.08</td>
<td>7</td>
</tr>
</tbody>
</table>

Figure 1. The AHP decision tree.
Selection of the Appropriate Wireless Payment Technology in Mobile Banking

<table>
<thead>
<tr>
<th>Factors</th>
<th>Percentage weight between the factors</th>
<th>Ranking</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transmission Speed</td>
<td>0.12</td>
<td>5</td>
</tr>
<tr>
<td>Connection type and Reliability</td>
<td>0.18</td>
<td>2</td>
</tr>
<tr>
<td>Compatibility</td>
<td>0.10</td>
<td>6</td>
</tr>
<tr>
<td>Usability</td>
<td>0.16</td>
<td>3</td>
</tr>
</tbody>
</table>

Table 3

Comparison of the mobile payment Technology alternatives

<table>
<thead>
<tr>
<th>Factors</th>
<th>SMS</th>
<th>WAP</th>
<th>GPRS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>30.56</td>
<td>36.25</td>
<td>34.26</td>
</tr>
<tr>
<td>Cost for Customer</td>
<td>23.57</td>
<td>26.2</td>
<td>27.25</td>
</tr>
<tr>
<td>Cost for Bank Server</td>
<td>17.63</td>
<td>21.83</td>
<td>17.3</td>
</tr>
<tr>
<td>Transmission Speed</td>
<td>16.8</td>
<td>18.6</td>
<td>19.3</td>
</tr>
<tr>
<td>Connection type and Reliability</td>
<td>20.4</td>
<td>22.1</td>
<td>26.79</td>
</tr>
<tr>
<td>Compatibility</td>
<td>13.2</td>
<td>29.4</td>
<td>20.3</td>
</tr>
<tr>
<td>Usability</td>
<td>29.4</td>
<td>12.3</td>
<td>17.25</td>
</tr>
<tr>
<td><strong>total</strong></td>
<td>151.56</td>
<td>166.68</td>
<td>162.45</td>
</tr>
</tbody>
</table>

Consistency rate is calculated based on the consistency index to test the validity. If the consistency rate is below 10%, the corresponding pair-wise comparison matrix is considered consistent. In this study, passes the consistency test since its calculated CI is 0.067.

Consistency rate = 0.067

Conclusion

In this paper, is proposed that the success of a m-payment technology depends on Security, Cost for Customer, Cost for Bank Server, Transmission Speed, Connection type and Reliability, Compatibility, and Usability factors. An AHP analysis was used to evaluate the performance of three m-payment technologies. The results of this analysis yielded several insights that confirm previous findings and shed light on the future of mobile payment schemes. First of all, this study corroborates that security factor dominates over other considerations in experts’ adoption of m-payment technologies. Secondly, among other factors, the Connection type and Reliability by and large determines the comparative advantages of m-payment technologies. Finally, the WAP technology is found to be the superior payment technology choice among the three technologies because it has
the best performances (WAP Forum, 2005). In addition, the GPRS technology could be a likely choice providing that its Cost for Customer can be formed. It is imperative to note that the present results cannot be perfectly applied to the business environment over the mobile Internet. Even though is found that the SMS technology is the least favorable choice among the three technologies considered, is predicted that its capability will be much deployed over mobile broadband services. In this sense, telecommunication operators acting as the access provider are better positioned than content providers or banks to command the m-payment scheme they prefer. Because the SIM card is preinstalled in almost every handset, the telecommunication operator can easily trace transaction records. Moreover, the wireless payment technology is capable of handling a large number of small transactions. The benefit for customers in adopting the wireless payment technology is that there would be no extra installment costs if it were to become the de facto payment instrument over the mobile payment. The wireless payment technology should become a far more popular payment instrument providing mobile commerce develops to a large extent (Standage, 2001). Nevertheless, SMS technology may still compromise its competitiveness. In addition, the most important alternative is security in technology quality between mobile payment operators and contents users, and the understandability of contents is also important for users to understand and use contents without difficulty. In addition, transaction in usability and the lateness of contents in contents quality are important, and privacy supported by network and flexibility of system integration in system quality are also important factors.

The evaluating SMS technology does not necessarily limit to be use for mobile banking solution. This technology can be altered to adapt to support secure SMS messaging solutions for peer-to-peer communication. There is no mobile application authentication in the developed J2ME application; this makes the Secure SMS/GPRS protocol susceptible to phishing. In short, the related of Future Mobile payment Technology, is based on Biometrics and will further increase security, but the authentication method can be a security risk. They increased location-based services actually add to security as well as marketing and usability. Back-end security will be more of a “honeypot”, and more IP data means more opportunities for sniffing, caching, archiving, and hacking. Payment fraud will be an issue via false entry/data copying, but more serious problem will be identity impersonation and large-scale disclosures.

References


Mobile payment forum white paper, (2002), enabling secure, interoperable and user-friendly mobile payments. Mobile payment forum USA, pp. 30-42.


