BIOMETRIC AUTHENTICATED SECURITY SOLUTION TO ONLINE FINANCIAL TRANSACTIONS

Dr. P. S. Aithal*.
**Srinivas Institute of Management Studies, Pandeshwar, Mangalore - 575 001, INDIA, psaithal@srinivasgroup.com*

ABSTRACT

The dramatic increase in the use of mobile phones has been closely followed by the increase in mobile fraud. Although eager to use mobile financial services, many subscribers are concerned about the security aspect when carrying out financial transactions over the mobile network. In fact, lack of security is seen as the biggest deterrent in the widespread adoption of mobile financial services. Hence, fraud prevention has become an essential ingredient in the success of online financial transactions. To enhance the security for financial transaction a biometric authentication system is proposed.

Keywords: Online financial transaction, biometric authentication, ubiquitous banking, mobile business.

Introduction:

Ubiquitous banking using mobile devices (mobile banking) is an effective and convenient way of providing electronic banking facility to costumers from anywhere and at any time. The advent of mobile communication technology and globalization are increasingly driving the banking financial services to become ubiquitous, personalized, convenience, disseminative and secured. Realizing the advantages to be gained from mobile banking, financial institutions have begun to offer mobile banking options for their customers in addition to the internet banking they already provide. Most of the literature uses the term "mobile banking" in the sense of traditional retail banking activities such as transferring money, paying bills, checking an account balance, and perhaps even checking on the status of the mortgage. This relatively limited definition may be a reflection of the natural bias many have about banking, simply because their relationship with them is primarily characterized by retail banking activities. In addition, many individuals have an interest in the stock market, whether through ownership in derivatives like mutual funds or directly in individual equities. These individuals may have an interest or a need to check the status of their investments or actively manage those investments. Thus, the products and services of the modern financial services institution include banking, brokering, and payment services. Each is a different, although complementary aspect of financial and business activities. Mobile technologies extend across many of the banks product lines and well beyond the retail framework. The reason Why the ubiquitous banking using mobile devices is expected to take over the Internet based online banking services is due to lack of security and a high level of fraud is seen as a major obstacle to the customers for financial transactions. For example, the web browsers and servers are enabled to use public key infrastructures for cryptographic key distribution and to use cryptographic protocols such as SSL for communication security [Dierks T. and Allen C., (1999)]. For financial transactions using internet, the security at both the client and the server end must be taken care. On the client side, the poor platform integrity, the multitude of default CA (Code Authentication) certificates and the arcane user interface pose severe security threats. The high level of vulnerability on the server side is best illustrated by the fact that almost all reported hacker attacks are targeted against servers. The most important types of system attacks which pose severe threat on internet financial transactions are : Password cracking, screen emulators, data diddling, social engineering, malicious code, distributed denial of service, physical perimeter penetration, and wireless intercepts [John H. N. and Mahesh S. R.,(2002)]. Other attacks that typically require more sophistication are: cryptanalysis, man in the middle attacks, fast factoring, registry or directory reengineering, EMI/RFI intercepts, IP hijacking, IP spoofing, anonymous IP addressing, and steganography etc. System security can be addressed by installing firewalls and intrusion detection systems, by monitoring security alerts and prompt implementation of security patches. However, this requires skilled system

administrator[1]s to continuously look after systems, which is relatively labour intensive compared to communication security and may not possible in small size mobile communication devices at client.

Security Issues in Ubiquitous Banking:

Mobile personal devices, usually with a built-in display and keyboard, are well-positioned to provide a technical solution for reducing fraud and allowing the fair allocation of responsibility for damages from fraud. Some amount of security is already part of the authentication mechanism of existing mobile phones as a way to prevent call theft. Moreover, it is relatively easy and inexpensive for device manufacturers to incorporate additional mechanisms to ensure secure transaction authorization. These mechanisms help prevent most fraud and allocate responsibility fairly for any remaining fraud. For users, their value far outweighs their relatively modest cost. Secure transactions using mobile phones consist of four independent processes :

1. Identification process :The device identifies the user through physical possession (as with regular mobile phones), passwords, or biometrics (such as voice recognition).

2. Authentication process :The mobile banking service provider authenticates the transaction request from the device via either subscriber identification (as with existing phones) or cryptographic mechanisms such as digital signatures or secure protocols, like the Wireless Transport Layer Security Specification.

3. Secure performance :The financial transaction is performed by the mobile banking service provider, possibly with the help of the merchant and/or other transaction provider(s) for bill payments and may involve secure payment protocols (such as Internet Keyed Payments/Secure Electronic Transactions, or iKP/SET) [Bellare, M. et. al. (2000) and MacGregor, R., et. al. (1997)].

4. Confirmation : A confirmation of the completed transaction is delivered to the user.

Mobile phone devices should incorporate mechanisms to securely authenticate transaction requests that can be used by multiple transactions and scenarios. To allocate responsibility, transaction requests should be digitally signed by the device using a private key (not known to the providers) kept in the device. The user does not have to obtain a public-key certificate from a trusted certificate authority; it suffices that the agreement between the user and the provider states the public key and the algorithm. To reduce hardware costs, designers may prefer public-key signature algorithms (such as the Digital Signature Algorithm, or DSA [Digital Signature Standard (DSS) (1994)], so most of the computations are done offline, and online signing is efficient. The device displays the transaction details to the user and asks his or her consent for

each transaction request. The device should ensure the user is aware of the entire request, possibly by limiting the request format. For example, payment transactions may display the amount and other transaction details related to that particular financial service. The security of this design depends on the secure operation of the mobile personal device, including its user identification. Some current mobile devices, including phones, use only simple, preprogrammed processors, and therefore can be trusted to operate securely. However, some devices support downloaded, general-purpose applications and like computers, may be vulnerable, as with viruses.

Secure transaction authorization may, therefore, involve a secure coprocessor, used only to authorize transactions and possibly to view confidential data. There should be visible indication when the display and keyboard are controlled by the secure co-processor, allowing the user to securely identify (such as by password) and authorize transactions. The co-processor is invoked by the main processor to authorize transactions, providing the raw request in shared memory. If authorized, the co-processor returns the signed transaction request in the shared memory. The simplest secure transaction architecture involves only the user, the device, and a single transactions provider (such as a bank, brokerage, or insurance company). The user identifies to the mobile device, possibly through secure identification mechanisms (such as a PIN, voice identification, or fingerprint); the device then authorizes a transaction to the provider (such as money transfers and investments). Authorization is preferably through some secure public-key signature process, allowing precise allocation of responsibility for fraud (disputed transactions). However, less secure forms of authorization (such as relying on subscriber identification and/or encrypted passwords) may suffice for some applications, as in e-banking and mobile commerce solutions. More complex payment transactions such as mobile purchasing typically involve at least one additional party, the merchant. In the simplest case, the merchant receives payment from external payment/transaction provider (such as a bank or credit card company); the mobile transaction provider authorizes the transaction. Wireless communication capability supports mobility for end users in mobile banking systems. Wireless LAN and WAN are major components used to provide radio communication channels so that mobile service is possible. In the WLAN category, the Wi-Fi standard with 11 Mbps throughput dominates the current market. It is expected that standards with much higher transmission speeds, such as IEEE 802.11a and 802.11g, will replace Wi-Fi in the near future. Cellular networking technologies are advancing at a tremendous pace and each represents a solution for a certain phase, such as 1G, 2G, and 3G, in a particular geographical area, such as the United States, Europe, or Japan. Compared to WLANs, cellular systems can provide longer transmission distances and greater radio coverage, but suffer from the drawback of much lower bandwidth (less than 1 Mbps). In the latest trend for cellular systems, 3G standards supporting wireless multimedia and high-bandwidth services are beginning to be deployed. WCDMA and CDMA2000 are likely to dominate the market in the future.

Secured Transaction Model for Ubiquitous Banking:

The business models for mobile banking may be based on Consolidation, Location based services, Immediate product payment, Bill payment, Systematic interoperability, and Non-credit card users [Marche S and Watters C, (2004)]. These models are based on specific applications. In consolidation model, the applications that provide consolidated financial views across institutions have value for those people who have banking relationships with more than one financial institution. Such an application would be able to consolidate all assets and liabilities in one view. Visual confirmation of such transactions is one of the attractive features of mobile banking and trading, as the user sees the complete transaction all at once. The restricted screen size of mobile devices is a challenge for this type of visibility, certainly in the near future. In Location-based services model the mobile technology is adopted for identifying and using the actual physical location of the user. This provides an opportunity to customize both data and services by taking into account personal factors and location-related factors [Hightower, J., &Borriello, G. (2001)]. Currently, providing and using location-specific information is possible with a wireless device. The costs and benefits of this functionality to all of the parties involved and the risk that users may be reluctant to have their movements recorded in this way. In Immediate product/service payment model, mobile devices afford the opportunity for consumers to purchase goods or services and draw the payment directly from their bank accounts in a manner similar to the debit card. Bill payment model allows payment bills online. One of the arguments that favour the use of a wireless device in many situations is to satisfy the need for urgency. A cell phone is often invaluable in the case of emergency, which is by definition urgent and time sensitive. Generally, there is not much urgency or time sensitivity to bill payment transactions or most other bank transactions, with the possible exception of the minority of investors who are active traders [Kiesnoski, K. (2000)]. Consumers always look for uninterrupted service with an uncomplicated interface between the customer, the device, the wireless service, the network, the merchant, and the bank. This systemic interoperability is a key user consideration in systematic interoperability model. M-banking does offer the potential for a portable payment/banking system that provides systemic interoperability. Presently in most of the countries, the payment mechanism of choice for medium-sized payments is the credit card. Under Non-credit card users model, Mobile banking and mobile payment schemes would have value for those people who do not have a credit card, such as the teenagers, children, or poor credit risks.

Regardless of the bright future of mobile banking, its prosperity and popularity will be brought to a higher level only if information can be securely and safely exchanged among end systems (mobile users and banking service providers). Online banking through mobile service providers is more secure than online banking through internet because of the usage of private network of the service provider (PNSP) and the users' personal mobile device. The existing electronic

authorizations for mobile payment security are based on account - holder authentication by the payment system. The use of secure and convenient mobile personal devices through PNSP could revolutionize the payment, banking and investment industries worldwide. In consumer oriented model proposed by Varambally K. V. M. and Aithal P. S., (2009) the mobile banking services are provided through mobile network service provider PNSP, either by collaboration or by strategic alliance. A consumer can use any private mobile network to access a particular real or virtual bank. The consumers and businesses in emerging markets are likely to find mobile financial services more attractive than do their counterparts in developed markets, because they have fewer alternatives. For many remote or low-income consumers, mobilehandsets and the mobileInternet could for the first time provide access to financial services such as basic banking and electronic payments; otherwise financial-services providers find such segments impossible to serve cost-effectively. Mobile networks are cheaper to build than fixed-line networks, and mobile services are generally cheaper to roll out than their precursors. A mobile-payments network, for example, can cost less to create and operate than an electronic point-of-sale (POS) merchant network. This means that some countries will be able to leapfrog over intermediate technologies and move directly from a paper-based payments system to a mobile one, without ever having to build an extensive wired POS or automated-teller-machine network.

To avoid lack of security and a high level of fraud which is a major obstacle to people embracing the possibilities and advantages of using internet based online banking services, in this model, it is proposed to use the secured network provided by mobile network service providers. The integration of present mobile communication technology with banks is an ideal solution to increase the potential customers trust towards ubiquitous financial transactions using mobile devices. This model supports the user identification through physical possession of mobile device, passwords, or biometrics and authenticates the transaction request from the device by mobile banking service provider through mobile network service provider via either subscriber identification or secure protocols, like the Wireless Transport Layer Security Specification. The secured financial transaction is performed by the mobile banking service provider, with the help of the network service provider(s) for financial transactions as well as for bill payments. The transaction process is completed by delivering a confirmation of transaction to the user. Such consumer oriented model changes the attitude of customers towards using m-banking services due to the advantages of convenience, low cost, anywhere, anytime banking and increases trust on online financial transaction.

How much value a mobile-financial-services business can create depends largely on its relevance to a given market. But in any market, abusiness can create value in two ways: directly, by enhancing benefits to customers or reducing costs for participants, or indirectly, by increasing cross-selling, cutting the cost of acquiring customers, or reducing customer churn. Indirect benefits are available only to the provider that comes first to market with a given service or that

has assets or capabilities distinctive enough to retain share once competitors have entered the market. The low-cost mobile banking can bring into the fold a considerable group of consumers who formerly could be served only at too high a cost. It replaces the most costly elements of a basic banking service (ATMs and tellers) with a deposit and withdrawal process that relies on much cheaper mobilecommunications and "franchised" (merchant-based) tellers. But the mixing of brand names, distribution networks, and financial services is leading to complex ownership and alliance structures, and extensive vertical integration could undermine competition. Links can lead to fewer benefits for consumers when they exploit reputation or involve sunk-cost investment to reduce competition on price. Mixed conglomerate structures can also challenge a basic principle of competition policy, the separation of content and carriage. Some mixed conglomerates-such as a telecom company merged with a financial service provider-will be able to control content and carriage and can limit access to networks by buyers of services, or to suppliers that wish to access potential customers. Lack of competition may not result in higher prices for financial services, but it could reduce product and process innovation. To ensure competition and innovation, restrictions may be called for on such vertical or horizontal links. In considering such restrictions, authorities will have to balance many issues, including the potential risk diversification benefits of mixed conglomerates and the benefits for competition of entry by non-financial entities in the financial service sector. At present, banks, for the most part, are watching from the sidelines while their primary role as the premier financial intermediary is being diminished by online brokers and other financial service providers. As recently as two years ago, many leading banks were preoccupied with merger and acquisition aimed at expanding networks of brick-and-mortar branches rather than creating or pursuing virtual branches in cyberspace. In truth, bankers' main motive to implement Internet banking was, and still is, to prevent the defection of their customers to other electronic banks or other financial service providers. Such consumer oriented model changes the attitude of customers towards using m-banking services due to the advantages of convenience, low cost, anywhere, anytime banking and increases trust on online financial transaction.

Biometrics Authentication and Enhanced Transaction Security:

There may also be a significant role for technology in improving mobile transaction security, as the following report makes clear. There has been a lot of work on biometric identity systems in recent years. The report surveys that work and assesses its relevance for mobile banking. In particular, it identifies a biometric technology approach that has already been incorporated in some mobile handsets—a sophisticated, but low-cost, fingerprint sensor. Use of this approach for mobile banking would work something like this: When a customer initiated a mobile banking transaction, the handset would request that the user register his or her fingerprint on the sensor, and the handset would compare the fingerprint to the one already stored in the phone (and, as a backup, also stored on the bank mobile transaction server). The handset would then send the

transaction request and the result of the fingerprint comparison—in effect, a biometric ID authentication—to the bank server for approval and execution of the transaction. That would replace the device-based security safeguard (the SIM card) with something much more robust and harder to defeat. As the report makes clear, the technology to implement such a system is available now. Biometrics is one approach to the authentication of an individual claimed identity. Recognizing individuals through observation of particular physical characteristics is known as biometrics. A biometrics authentication is a two-stage process. During the first stage, some sort of capture device is used to take a measurement of particular physiological or behavioral characteristics and in the second stage; the measurement is compared to a stored value. Based on the comparison result the system makes an authentication decision. Biometric technologies do not actually compare the physical traits that they are designed to use as a unique identifier, rather, they create templates for comparison. This enrollment process may require the individual to provide multiple instances of the biometric trait. The initial comparison templates are created during an enrollment process [Arumugaperumal S., (2006)].

One way to increase the strength of an authentication mechanism is to use multiple factors of authentication. In the case of biometrics, this could involve requiring the user to input a password or PIN (Personal Identification Number) or to produce some sort of authentication token such as smart card that contains both the PIN and any one of the biometric systems with 1:1 matching. The advantage of such is that many are designed to operate with biometric systems and have sufficient space for storage of biometric templates with them. However, assessing the extent to which an additional authentication factor can increase the overall strength of the authentication services. When passwords are used for authentication, the decision is made relatively straightforward- if correct password is supplied the result is positive authentication, otherwise the individual is rejected. A biometric authentication is conceptually different, in that the decision is based on a probability. Any organization considering the use of biometrics needs to understand the impact of this when reaching a trust decision. Biometrics is a measurable physical characteristics or personal behavioral trait used to recognize the identity or verify the claimed identity of an enrollee. Examples of physiological characteristics that are used in biometric device include fingerprints, the geometry of the face or hand and patterns within the iris or retina or in the layout of veins. Behavioral characteristics include voice pattern, gait and the dynamics of handwriting or keystrokes. For the authentication process the chosen characteristics must be unique to each individual. Also it is possible to measure the characteristics with the reasonable degree of accuracy. Once the measurement has been taken the data is converted into a biometric template. A template is a representation of the measurement that retains all the relevant information but takes up far less space than the original. It is this template that is compared to a template generated in the same manner during the initial enrolment procedure and based on the similarity of the two, a decision is made whether the user should be granted access.

There are various biometric products like a plethora of fingerprint scanners, voice and facial recognition system, retina/iris scanners, hand geometry devices and signature verification systems available in the market. While fingerprints have proven to be highly reliable and accurate over the years, particularly now using RF imaging, they're not completely infallible. They can be affected over time by such things as years of manual labor or physical injury, so there would probably be a desire to update the reference templates as and when necessary for commercial and financial applications. Other factors that can cause failure in a fingerprint scan are cold and humidity (particularly in the older types of fingerprinting), and location, angle and pressure of placement on the sensor (known as a platen). Other issues to consider are that the use of fingerprints requires physical contact, which can be a problem in some cultures, and the fact that finger printing's long association with criminal justice lends itself to some privacy resistance, although this will probably ameliorate over time with increased use of biometrics and updated privacy laws. Fingerprint capture technology is easily accommodated on a cell-phone, with sensor sizes ranging from 12 mm x 5 mm to about 1.5 cm x 1.5 cm, and low power and processing requirements. The fingerprint template itself ranges in size from about 256 bytes to 500 bytes.

Conclusion:

We have investigated the security threats in mobile banking implementations using the GSM network. The discussions support to build applications for portable devices that ensure users can securely send their banking information via the GSM network. The mobile banking solutions developed provide platforms for users to bank using SMS and GPRS. In order to enhance the security, biometric finger print detection can be used in mobile device. The possibility of using bio-metric finger print security to enhance user authentication are discussed.

REFERENCES

1. Arumugaperumal S., (2006), Effective Method of Security Measures in Virtual Banking, *Journal of Internet Banking and Commerce,* vol. 11, no.1.
2. Bellare, M., Garay, J., Hauser, R., Herzberg, A., Krawczyk, H., Steiner, M., Van Herrenweghen, E., and Waidner, M., (2000), Design, implementation, and deployment of the iKP Secure Electronic Payment System. *J. Select. Areas Commun. 18,* 4, pp. 611–627.
3. Dierks T. and Allen C., (1999), "The TLS Protocol Version 1.0. IETF Request for Comments", *RFC* 2246, January 1999.
4. Digital Signature Standard (DSS), (1994), National Institute of Standards and Technology (NIST). Federal Information Processing Standards Publication FIPS 186. U.S. Department of Commerce, Washington, DC, May 1994.

5. Hightower, J., &Borriello, G. (2001). Location systems for ubiquitous computing.*IEEE Computer*, *34*(8), pp. 57-66.
6. John H. Nugent and Mahesh S. Raisinghani, (2002), The information technology and telecommunications Security imperative: important issues and drivers, *Journal of electronic commerce research*, vol. 3, no. 1.
7. Kiesnoski, K. (2000). Wireless banking.*Bank Systems and Technology*, *37*(2), 40-43.
8. MacGregor, R., Ezvan, C, and Liquori, L., (1997), Eds. *Secure Electronic Transactions: Credit Card Payment on the Web in Theory and Practice.* SG24- 4978-00 Redbook, IBM, International Technical Support Organization, Raleigh, NC, July 2, 1997; see www.redbooks.ibm.com/.
9. Marche S and Watters C, (2004), *Mobile Commerce Applications*, Shi &Nansi, Publication.
10. Varambally K. V. M. and Aithal P. S., (2009), Mobile Business Technology and Business Proliferation of Banks - A Futuristic Approach, Amity Business Review, vol. 10, No. 1, pp. 9 -25.