Mobile Commerce: A Model to Address New Financial Transaction Security Concerns

Raj Gururajan[1], Chaiyaporn Chirathamjaree[2]

[1] Murdoch University, School of Information Technology (r.gururajan@murdoch.edu.au)
[2] Edith Cowan University, School of Computer & Information Science
(c.chirathamjaree@cowan.edu.au)

Abstract

Security of transactions in Mobile Commerce is moving away from an IT concern to a Business concern because of potential loss of revenue to businesses due to lack of privacy, integrity or confidentiality, system slowdown or downtime. While most of the various security procedures are limited to corporate IT infrastructure, in mobile commerce, issues concerned with transaction security appear to have extended beyond the corporate network to embrace the complete business process. Any lapse in procedures that maintain confidentiality of data, or violation of privacy could affect corporate image and hence would impact customer relationships. Any adverse effect on customer relationship would negatively impact business revenue. In addition to existing security problems in a wired commerce environment, the emergence of mobile devices has renewed calls for addressing security threats to financial transactions. These problems are discussed in this paper as key issues in terms of organisation's architectural and procedural approaches to security, reliability and availability of business transactions.

Keywords:

Mobile commerce, security threats, IT security, risks, business transactions.

1. Introduction

In the past, majority of the computer security officers had difficulty in convincing management to allocate financial resources for IT security. However, with the emergence of electronic commerce and various legislations, organisations appear to have understood the necessity for computer security, especially data security [1]. The current trend in most organisations appears to be security officers focussing on IT security – namely – focussing on hardware security, software security and access security [1]. The access security involves both physical access and logical access. What appears to be missing from these security procedures is proper integration of business transactions. Ghosh [2] states that while various security measures have dealt independently from business transactions, electronic commerce and the emerging mobile commerce have changed the perception that independent IT infrastructure security alone can protect an organisation in terms of its business needs. To support Ghosh's statement, Deise [3] has identified a shift in the focus of IT security in organisations, resulting in new security policies to focus on reliable, available and trusted business transactions of organisations.

In this paper, new security threats arising from mobile commerce is initially highlighted. These threats are then linked to financial transactions in order to highlight the potential loss or damage to organisations' revenue. The organisations' IT requirements are assessed with a view to provide support to financial transactions in a mobile commerce environment. Organisational support is then formed into an 'architecture' and the architecture is discussed in terms of IT in an organisation, how does IT support an organisation and what does IT do to support the business processes of financial transactions. This architecture is subsequently elaborated in terms of action items so that transaction security in an organisation can be guaranteed. It is hoped that these action items would enable organisations to tighten their security measures.

2. Security Threats Arising from Mobile Commerce

Security threats in mobile commerce can range from passively eavesdropping into others' messages to actively stealing users' data [4]. In a radio frequency operated mobile commerce, with minimum difficulty it is possible to listen to one's conversation. This has an impact for consumers because they are concerned about their data and voice messages from unauthorised access. On the other end of the problem is the inherent security risk involved in transferring information over the networks. This problem consists of two components: *identification integrity*, and *message integrity*. The identification integrity refers to the signature elements found in the messages in order to establish where the message is originating. The message integrity refers to details to establish that the message is received as sent and no third party has attempted to open, modify or alter the contents. According to Zhang & Lee [5], these two items appear to cause a lot of concern to both the sender and the receiver. While the sender risks theft or misuse of his/her personnel information such as account and bank details, the receiver (usually a merchant) risks repudiation of the transaction and resultant non-payment.

In addition to the above two, additional security concerns in mobile commerce arise due to the new development in technology itself [5]. The mobile technology is envisaged in such a way that the services offered will eventually warrant payment for the type of services offered. This is already emerging in the domain of mobile telephones. For instance, when mobile telephone users access other network carriers, a special charge is levied on the users. Therefore, it is safe to assume that there will not be any "free services" in the future. The technology is developing in such a way that the payment for such services will be through some form of "smart cards". The details stored in the smart cards need to be transmitted via the networks for validation and verification in order to determine service levels. If these networks are not fully secure, there are possibilities for security breaches to happen.

One major security breach that can happen in mobile commerce is when the user details are transformed from one mobile network to another [6]. When this transformation occurs, any encrypted data needs to be decrypted for transparency. In mobile commerce, when mobile devices make requests to web pages of a network server, a four-stage process is followed. First, the requests arise from the originating Wireless Transport Security Layer (WTSL) protocol. Second, the requests are translated at the originating Wireless Application Protocol (WAP) gateway. Third, they are sent to the standard Session Security Layer (SSL) protocol of the destination network. Fourth, the translated information reaches the Hyper Text Transfer Protocol (HTTP) modules in the new network in order for the requests to be processed. In the process of translating one protocol to another, the data is decrypted and then re-encrypted. This process is commonly known as the "WAP Gap". If an attacker is able to have access to the mobile network at this point, then simply capturing the data when it is decrypted can compromise the security of the session.

Data in the Mobile Commerce environment is secured using encryption technology. According to Ghosh, [2], it has already been proven that the technology is vulnerable to attacks. Hackers have broken some of the existing algorithms for encryption. So, there is nothing like a complete security. Further, there is no international regulatory framework available to enforce certain security related problems. For example, in the current climate, no individual organisation or government can guarantee security to consumers. When the security breach appears in an international transaction, no one country will be able to assume responsibility to prosecute the vandals. While these problems have been recognised and solutions are being proposed, organisations tend to lose consumer confidence. This will potentially impact organisations' revenue.

Trust is central to any commercial transaction and more so in the case of mobile commerce [7]. Trust is normally generated through relationships between transacting parties, familiarity with procedures, or redress mechanisms. In the case of mobile commerce, the need for creating the trust in the consumer assumes extreme importance because of its virtual nature. It hinges on assuring consumers and businesses that their use of network services is secure and reliable, that their transactions are safe, that they will be able to verify important information about transactions and transacting parties such as origin, receipt and integrity of information, and identification of parties dealt with. Therefore the challenge is not to make mobile Commerce fool proof but to make the system reliable enough so that the value greatly exceeds the risk.

Any new development in technology in today's consumer minds creates both curiosity as well as reluctance. The informality and lack of overall control creates the perception that the Internet is inherently insecure [8]. This inherent perception can trigger business risks and technological risks [9]. Business risks involve products and services, inadequate legal provisions, reliability of trading partners, behaviour of staff and demise of Internet service providers. Technological risks involve hacker attacks, computer viruses, data interception and misrepresentation. To achieve

satisfactory levels of trust, organisations have to think about managing both business and technological risks. Currently Mobile Commerce relies mostly on knowledge-based trust that is useful for Business-to-Business (B2B) commerce [7]. However, there is a big surge in the identification-based trust to satisfy consumer concerns about their transaction details. In addition, current architectures for mobile communications do not provide full security measures in terms of transaction integrity. Some of the models envisaged for mobile commerce are based on smart cards oriented approach and hence the issue of financial transaction security needs greater examination in mobile commerce.

3. Security Threats that Can Impact Financial Transactions

Security risks in a mobile commerce environment associated with financial transactions can be categorised into traditional risks and non-traditional risks [10]. Traditional risks usually involve loss or damage to tangible physical assets and resulting economic loss. For example, loss of computer hardware may have an impact on incomplete transaction. Alternatively, a data disk, which is not fully protected from theft can place an organisation into some form of risk. Treatment of traditional risks is usually addressed in risk management policies. Protecting tangible assets from traditional perils, even when those assets are devoted to mobile commerce, does not involve new and different techniques. These security treats are beyond the scope of this paper.

Non-traditional risks involve the sustaining damage to organisations' computer systems and electronic data [11]. These risks can fall under the category of stolen information, damages to web sites by hackers, hijack of web sites and viruses. An attack may be perpetrated for any of a number of reasons including financial gain involving credit card fraud, curiosity with no specific intent of harm, espionage by domestic or foreign competitors, or by foreign governments, revenge by a terminated employee intent on wiping out files, disclosure of personal data to unauthorised institutions as in health related cases, thrill seeking, disruption to stop critical activities, and extortion for financial or political reasons. Any attack, internal or external, on a computer system is at minimum disruptive and forces the administrator to shut down the system realising in revenue loss.

Non-traditional security breaches also include any unauthorized access or use of a company's computer system and data by an outsider or insider [3]. For example, a hacker could break into a company's computer system and steal or destroy data. Widespread use of mobile commerce enhances the possibility of an outsider invading an organisation's computer system. Due to businesses reliance on computers for their daily operations, breaches of a company's computer or information security system are a risk to almost all functional components of businesses. Use of software to encrypt and, thus, safeguard communications provides some protection, but also adds a risk that a virus or other bug could damage equipment or data. Further, according to Dang [12], theft of information such as critical electronic files that include financial data, customer information, marketing and new product data, trade secrets, and personnel data may provide competitors with a strategic advantage, criminals with the means to commit fraud, and others the opportunity to disparage the company. Dornan [13] states that the use of misappropriated information may harm third parties such as customers, employees, and business partners. The theft of information may undermine an acquisition or cause a public relations problem and hence potential loss to revenue.

Security breaches may be very costly to an organization [14]. When an unauthorized access to the computer is gained for the purposes of committing a crime or fraud, reputation is also at stake. Other security issues include the prohibition against the use of high-level encryption technology by domestic or foreign governments so that agencies can break the codes if necessary for defence or law enforcement, changes in international standards, and loss of encryption key recovery.

4. A Closer Look at Fraud and Crime Risks in Mobile Commerce

The scope of computer fraud and crime is immense in mobile commerce. Among the most common crimes are malicious mischief, such as the insertion of viruses or Trojan horses into one or more computer systems; the fraudulent transfer of money to personal accounts; the use of forged electronic signatures; the theft of credit card information and credit card fraud; Medicare and Medicaid fraud; the theft of intellectual property; illegal use of software; stock and commodity market manipulations; and similar illegal activities. Most losses are insurable, but premiums will be relatively exorbitant if security measures are not appropriately enacted [6].

A hacker may use a number of methods such as the insertion of viruses, spamming and web snatching to access computer systems and data and cause resulting damage. Damage may occur at data centers or to transmission networks, routers, and power sources. Virus attacks may also come from innocent parties who pass on an infection

without knowledge that the system is contaminated, usually by e-mail.

Using another technique called a *distributed denial of service*, hackers attacked some of the most well-known and highly secured web sites in the world, including Yahoo.com, eBay.com, and Amazon.com. This technique hijacks numerous computers on the Internet and instructs each one to flood a target site with phony data. The target site trying to accommodate the phony data becomes overworked and soon begins to lose memory. The result is effectively slowing or shutting down the entire site to real customers.

Web snatching is a practice in which one party plants a virus in another party's Web site that automatically moves the viewer from the selected site to a site run by the web snatcher. This is done without the permission of the selected Web site owner or the site visitor. In many instances, the viewer is unable to get out of the unwanted site, short of turning off the computer, and is held hostage to the new site. The diverted-from and diverted-to sites usually have nothing in common with each other.

Financial institutions and companies that have inadequate electronic security protection are more likely than not to suffer losses of money, information, or other corporate assets. Surveys have shown that most companies and institutions have incurred losses, and a substantial number have no idea whether they have come under electronic attack or not. Insiders or former insiders have committed most of the electronic crime and fraud, but there are many examples of third-party fraud and theft.

Mobile commerce can only be conducted if all parties believe there is adequate security. The majority of those who use the Internet, on which current mobile commerce technologies are built, are very concerned about security [2]. Some 40 percent of Internet consumers give false information when they use the Web because they do not trust the Internet's security [15]. Other users refuse to register at sites that require what the consumer believes to be personal information [16]. Many persons want the government to legislate security on the Internet, as they are not confident businesses will do the job on their own [17]. Therefore, it is critical that businesses enhance both their security and their security image to combat fraud and crime on the Internet as well as to increase customer confidence and participation to realise secured transactions.

5. Security Risks in Mobile Commerce Emerging from Reliance on Third Parties

Today, most organisations rely on computers for their daily operations. Traditional risks and non-traditional security risks can interrupt a business or literally shut it down. For example, a security breach by a hacker can severely disrupt a business and those that depend on it. Most businesses in mobile commerce are dependent in several ways on the continued reliability and operation of computer controlled systems not within their control such as the telephone network managed and controlled by computers. Businesses are dependent on their financial institutions that are also managed and controlled by computers. In mobile commerce, to accommodate home users, organisations are dependent on their Internet service providers. Suppliers and customers depend on each other's electronic data systems and on mutual systems, such as a third-party commodity exchange. When one system fails, it may cause the other systems to fail as well. Failure may be a slowdown in the dependent system, also called the ‘brownout’ or a total denial of service, also called the ‘blackout’ [2].

The above said risks can result in many different types of losses [13] [18] [19]. The losses that arise from reliance on third party can generally be grouped into: (1) loss or damage to property, both tangible and intangible, (2) business interruption, and (3) extra expense. Property losses occur when loss or damage is suffered to a firm's own tangible property or to property for which the firm is responsible. Traditionally, this means damage to a building or other business property, including computer equipment. In the mobile commerce world, the focus is on damage to computer networks and, more importantly, data. An important issue is whether data is considered tangible property under a typical property insurance policy. It appears that insurers will begin to address the issue of what is defined as covered property under these policies. More likely, courts will have to decide this issue.

Property losses can also occur when an organisation's intangible or intellectual property is infringed or violated. Copyrighted materials can be copied without permission, trademarks can be infringed upon or diluted, and patented property or ideas can be stolen. Today, a firm's intellectual property may be its most valuable asset [3]. Organisations need to protect their intellectual property from hackers, crackers, competitors, and others, as well as make sure they do not infringe on the intellectual property rights of third parties. This could potentially expose a firm to third-party liability.

Time element losses typically include business interruption (BI) losses and service interruption losses. BI loss is the

economic loss resulting from the interruption of business activities. Business interruption losses may result from the inability to access data, the theft of data, or a threat to the integrity of the database. For example, a security breach of a credit card database may cause the database owner to curtail activity on the system until a damage assessment is completed and the system integrity is re-established. Not only is there a disruption of the database operations, there is also a consequential effect on all third-party users of the system.

Service interruption losses include economic losses associated with the interruption of utilities. A service interruption incident can occur from an "off-site" exposure or event. There have been many incidents of communication cables inadvertently being cut. Long-distance telecommunication companies have experienced software problems in data routing that effectively crippled their networks for several days.

In addition to the business losses and service losses, mobile commerce gives rise to new implications about doing business and being protected from interruptions in doing business [20]. Businesses suffering losses related to server outages face the risk of losing customers for extended periods of time. In mobile commerce, the increased reliance on suppliers is also exposing businesses to new risks for financial losses. These range from suppliers of goods (such as raw materials) to suppliers of services (such as server usage, delivery services, electricity, and telephones).

Business interruption may have several consequences - e.g., loss of income; extra expenses to recover; loss of customer, partner, and shareholder confidence; and, ultimately, reduced market capitalization. Third parties harmed by the denial of service may sue, adding liability losses to first-party damages. In some cases, business interruption may constitute a breach of contract.

According to Lee [21], service denial may cause a customer business interruption, network suspension, or a disruption in or delay of services. Service denials may result in damage claims or lawsuits for breach of contract.

6. Expense Incurred by Organizations Due to Business Interruptions

In the event of an interruption, a business may incur extraordinary expenses to resume operations as quickly as possible. Extra expense coverage is for those costs incurred by the policyholder in excess of the normal costs that would have been incurred to conduct business during the same period had no loss or damage occurred. An example of extra expense might be increased freight charges incurred to meet a customer's demand for an order due to delays in the production process associated with a loss event.

In the mobile commerce area, there are new types of costs that may need to be considered in the context of risk and insurance, including additional costs of operating Web sites from alternative servers, costs of operating Web sites through alternative providers, costs to repair Web sites damaged by hackers or equipment failures, and costs of rebuilding other lost information [22]. Thus, various security risks arising from a combination of issues warrants a closer scrutiny for assessment of an organisation’s IT requirements in order to facilitate a secured financial transaction.

7. Nature of Financial Transactions in An Organization

When a financial transaction is facilitated in a mobile commerce environment, usually the consumer accesses the organisation’s computer to search for appropriate details. Once the consumer is satisfied with his/her order, an order is placed. The consumer places an order using the infrastructure provided by the Internet storefront and using his or her payment method of choice. Once the order reaches the organisation, the transaction is processed. A number of security issues such as verifying the credentials of the consumer arise at this point. Provision for real-time security and connectivity to authorise payment via the Internet or wireless medium forms an integral component of the transaction. The organisation involved in the transaction channels the transaction through various financial networks such as banks, ensuring that customers are authorized to make their purchase.

While security issues are applied onto a transaction, usually the client/server architecture for performing transaction processing is used. The client is installed on the organisation’s merchant site by the third-party providing user authentication for financial details and this client is integrated with mobile commerce application. The client is usually pre-integrated with store management systems including for management reporting purposes.

For the purposes of transaction authorization, the client software establishes a secure link with the processing server over the Internet using an SSL connection, and transmits the encrypted transaction request. The server, which is a multi-threaded processing environment, receives the request and transmits it over a private network to the appropriate financial processing network.

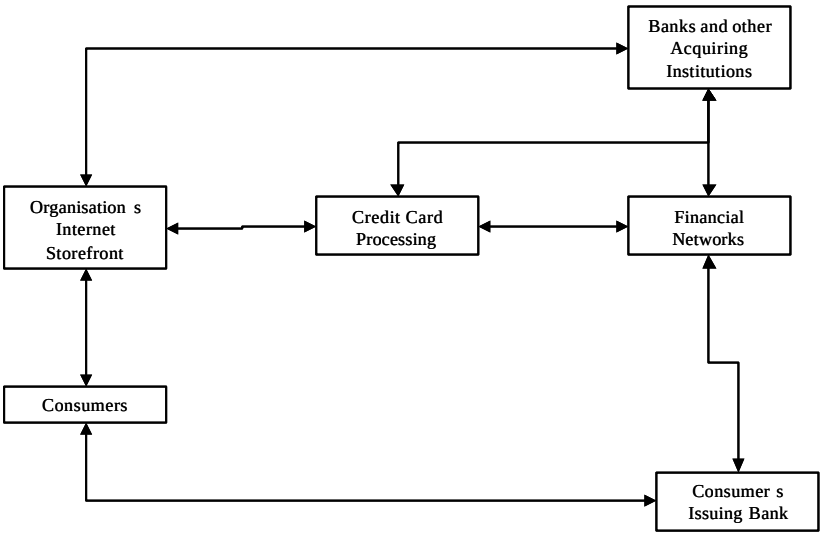
Depending upon the consumer’s financial status, the transaction is approved or denied. When the authorization

response is received from the financial network, the response is returned via the same session to the client on the consumer's site. The client completes the transaction session by transparently sending a transaction receipt acknowledgment to the server before disconnecting the session.

The whole transaction is accomplished in few seconds, including confirmation back to the customer and the organisation. If the transaction is approved, funds will be transferred to the organisation's account. Once the transaction is confirmed, the transaction will be securely routed and processed. As proof of a securely processed transaction, both the customer and the organisation will receive a transaction confirmation number.

This can be shown using the following figure (Figure 1):

Fig. 1 Transaction Processing Cycle



In order to guarantee secured transactions at an organisation level, there is a compelling need to describe an architecture to support almost all the elements of the transaction that can be conducted in the organisation. The security aspects not only involve the organisational IT infrastructure but also third-party security levels in order to approve a financial transaction. It should be remembered that consumers expect the organisation to facilitate a reliable and secure transaction and it is in the interest of the organisation that third parties involved in the transaction are reliable and capable of providing necessary security to consumer's transactional details.

While the above diagram portrays a complete financial transaction system, the following diagram portrays the component that needs to be supported by an organisation. The conceptual architectural elements cover components such as office systems, databases, and other Business Logic Components. This is shown in Figure 2 below.

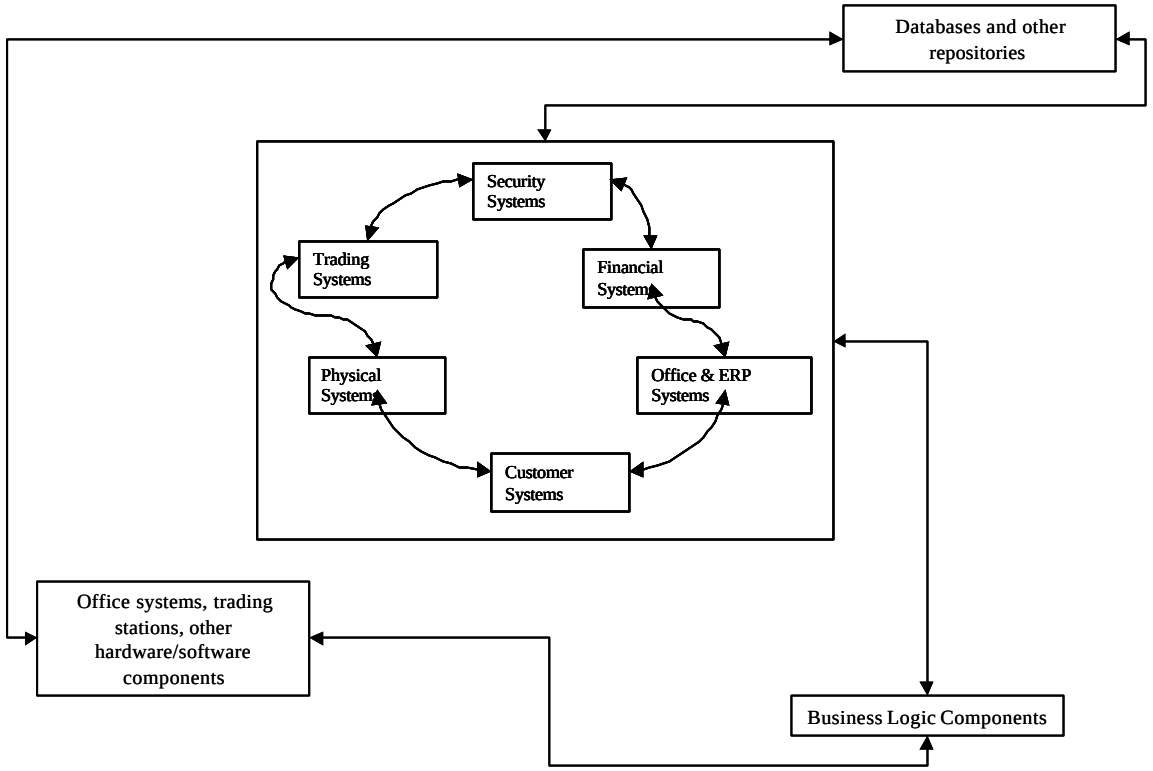


Fig. 2 Business Processing Facilitating Mobile Commerce Transaction

8. Assessment of Organization's IT Requirements

In order to guarantee security of transactions in mobile commerce, initial assessment of an organisation's IT requirement is essential for a number of reasons [23]. These include the ever-changing customer requirements, changing hardware and software platforms, dynamically changing user needs and user experiences gained from the innovative IT products. Therefore, such an assessment involves four key components of mobile commerce. They are (1) Embedded computers in many everyday objects [24]; (2) Next generation wireless networks [14]; (3) Interfacing technologies for bi-directional communications [1]; and (4) Design of applications that satisfy user needs [12].

The first key component arises from the need that there are going to be more wireless devices by 2005 and the prediction is that by 2005, mobile devices will outnumber wired devices [25]. These mobile devices would consist of some form of embedded systems in them and hence the allocation of priority. The next component follows from the first one which highlights the need for networks to go wireless in order to support the concept of mobility and hence mobile devices. Users communicate via a number of different mobile devices and hence the bi-directional communication aspect is essential for an organisation to ensure transactions are reliable and secure. Finally, to accommodate diversity of user needs, applications assume a key component role in mobile commerce.

With these four key components in mind, when organisations' IT requirements are assessed, importance should also be given to 'user experiences'. In mobile commerce environment, these user experiences typically involve cameras, music and other emerging innovative technologies such as positioning systems and hence organisations should find a way to accommodate these ever changing user experiences. Organisations would then be tempted to add additional hardware and software resources to their existing infrastructure but this will increase the financial burden of an organisation. One emerging suggestion appears to be the consideration of 'interface' facilities to enable sharing other third-party resources. This requires address and connectivity mechanisms that do not exist today. While recent newspaper articles forecast such capabilities are emerging, the bigger challenge for organisations is to create applications that truly have this multi-modal, multi-channel character because it is believed that the immediacy of wireless technology is great.

With this scope in mind, if we analyse an organisations' IT infrastructure, then we would be able to bundle business needs to support secure transactions into four main groups. They are:

1. Technical infrastructure that can identify what IT is made up of in an organisation;

2. Physical components of IT that can identify how these components support various workflow requirements in an organisation;
3. Logical components that can identify how IT components support various business processes; and
4. Real time measurement and control of security and service levels in real time.

While the first three points provide essential components of an application architecture in an organisation, the fourth point provides the control and maintenance components of the application architecture. This real time control is essential in mobile commerce because of the difficulty in describing complete security architecture to ensure security of transactions.

9. Conclusion

The concept presented in this paper is an initial attempt to address various new security concerns in the emerging mobile commerce. The conceptual model is derived in order to accommodate various business processes as an integral component and security management encompassing these business processes. It is believed that this model will assist in avoiding issues such as loss of transaction authenticity because the business process is integrated with the security procedures in the model. Further, the business processes are kept in the centre of the model to enable transaction confidentiality and integrity from an organisational point of view. Further, the interdependence of various systems with in the architecture is expected to provide much needed real-time reaction to any causes of transaction unvailability in mobile commerce.

While the model is only a conception, the inclusion of business process along with IT security is expected to provide tight controls to management in terms of financial transactions. This is rapidly becoming essential in the competitve world of mobile commerce where the volume of transactions ensure healthy revenue to organisations. Therefore, the focus was set on transaction security and the model was conceived. It is hoped that this model helps organisations to get a head start to review their security procedures and establish a better control on financial transactions.

References

[1] Dang, A. V. (2000a). *E-Business raises transaction security concerns* (Research Note): Gartner Advisory.

[2] Ghosh, A. K. (2001). *Security and Privacy for E-Business*. New York: Wiley

[3] G Deise, M. V., Nowikow, C., King, P., & Wright, A. (2000). *Executive's Guide to e-Business: From Tactics to Strategy*. New York: John Wiley & Sons, Inc..

[4] Loney, M. (2000). M-Commerce safety fears. *IT Week, 3*, 6.

[5] Zhang, Y., & Lee, W. (2000). *Intursion detection in wireless ad-hoc networks.* Paper presented at the ACM/IEEE MobiCom.

[6] Hulme, G. (2000). Services Seeks to Bring e-Business to Small Businesses. *Informationweek.com, August 2000*, 21.

[7] Fink, D. (2000). Developing trust for Electronic Commerce. In L. Janczewski (Ed.), *Internet and Intranet: Security and Management: Risks and Solutions* (pp. 44-86): Idea Group Publishing.

[8] Schiller, J. (2000). *Mobile Communications.* New York: Addison-Wesley.

[9] Shroeder, S. (1999). Wired for business. *Risk Management*(March), 12-22.

[10] Judge, P. (1998). Little guys still say NO to the net. Business Week, 134.

[11] Young, D. (2000). Handicapping M-Commerce: Getting ready for wireless e-commerce. *Wireless*

Review(August), 24-30.

[12] Dang, A. V. (2000b). *Four action items for E-Business: Transaction Security* (Research Note): Gartner Advisory.

[13] Dornan, R. (2001). *The essential guide to wireless communication applications.* Upper Saddle River, NJ: Prentice Hall PTR.

[14] Gerrard, M. (2000). *Organising for E-Business: Getting it right* (Commentary): Gartner Advisory.

[15] Craig, J., & Julta, D. (2001). *e-Business Readyiness: A Customer Focused Framework*. Boston: Addison Wesley

[16] Anonymous. (2000a, 15 August 2000). E-Commerce is growing. *The Australian*.

[17] Stowe, B. (2000). Wireless networking looks attractive, but what about cost of keeping it secure? *Infoworld* (May).

[18] Anonymous. (2000b). E-Commerce is growing. *The Australian*.

[19] Smith, D., & Andrews, W. (2001). *Exploring Instant Messaging*: Gartner Research and Advisory Services.

[20] Arena, A. (2000). Asian Internet start-ups invests heavily in dot.coms. *Australian Communications* (February), 15-18.

[21] Lee, A. (2000). Small firms must take Internet plunge or risk being sidelined. *The Engineer*, 10 November 2000, 10.

[22] Lewis, T. (1999). Ubinet: The ubiquitous Internet will be wireless. *IEEE Computer*, 32, 10.

[23] Langley, N. (2000). Get moving on m-commerce. *Computer Weekly*, 68.

[24] Hayward, S., Dulaney, K., Egan, B., Plummer, D., Deighton, N., & Reynolds, M. (2000). *Beyond the Internet: The Supranet* (Commentary) : Gartner Advisory.

[25] Koller, L. (2000). Banks flirting with wireless billing. *Bank Technology News*, 13, 25.