CYBER TIMES®
INTERNATIONAL JOURNAL OF TECHNOLOGY AND MANAGEMENT

ISSN: 2278-7518

Vol. 5, Issue 2, April 2012 - September 2012

CYBER TIMES®
(Leader in Innovative Tech-World)

Cyber Times International Journal of Technology & Management

Vol. 5, Issue 2, April 2012 – September 2012
ISSN: 2278-7518

EDITOR-IN-CHIEF

Dr. Anup Girdhar

EDITORIAL ADVISORY BOARD

Dr. Sushila Madan
Dr. A.K. Saini
Mr. Mukul Girdhar

EXECUTIVE EDITORS

Ms. Kanika Trehan
Mr. Rakesh Laxman Patil

"*Cyber Times International Journal of Technology & Management*". All rights reserved. No part of this journal may be reproduced, republished, stored, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior permission of the publisher in writing. Any person who does any unauthorized act in relation to this journal publication may be liable to criminal prosecution and civil claims for damages.

Editorial Office & Administrative Address:

The Editor,
310 Suneja Tower-II,
District Centre, Janak Puri,
New Delhi-110058.

ISSN: 2278-7518

Phone: 011-25595729, +91-9312903095

Website: http://journal.cybertimes.in

Email: editor@cybertimes.in

Disclaimer: Views and information expressed in the Research Papers or Articles are those of the respective authors. "*Cyber Times International Journal of Technology & Management"*, its Editorial Board, Editor and Publisher (Cyber Times) disclaim the Responsibility and Liability for any statement of fact or option made by the contributors. The content of the papers are written by their respective authors. The originality and authenticity of the papers and the explanation of information and views expressed therein are the sole responsibility of the authors. However, effort is made to acknowledge source material relied upon or referred to, however; "*Cyber Times International Journal of Technology & Management*" does not accept any responsibility for any unintentional mistakes & errors.

Cyber Times International Journal of Technology & Management, Bi-Annually, Vol.5, Issue 2, has been Published, Printed and Edited by Dr. Anup Girdhar, on behalf of Cyber Times, at 310 Suneja Tower-II, District Centre, Janak Puri, New Delhi-110058.

From the Editor's Desk

At the outset, I take this opportunity to thank all the contributors and readers for making ***"Cyber Times – International Journal of Technology & Management"*** an outstanding success.

The response that we have received from the Researchers, Authors, Academicians, Law-Enforcement Agencies and Industry Professionals for sending their Research Papers/ Articles for publication is duly acknowledged across the globe.

We are pleased to present the Volume 5, Issue 2, of *"**Cyber Times International Journal of Technology & Management**"* which include three major categories and sub-categories under Technology, Management, and Research Articles which are as follows:

Technology

Cloud Computing, Artificial Intelligence, Wireless Networks, Cyber Security and Network Attacks, Penetration Testing, Cyber Laws, Cyber Crime Investigation, Data Mining, Databases, Mobile Commerce, Software Testing, etc.

Management

Management Strategies, Human Resources, Business Intelligence, Global Retail Industry, Business Process Outsourcing, Indian Economy, Performance Management, Risk Management, International Business.

Research Articles

Atomic Power and Open Source Software.

I am sure that this issue will generate immense interest of Readers in different aspects of Technology & Management.

We look forward to receive your valuable and future contributions to make this journal a joint endeavor.

With Warm Regards,

Editor-in-Chief

General Information

- "*Cyber Times International Journal of Technology & Management*" is published bi-annually. All editorial and administrative correspondence for publication should be addressed to The Editor, Cyber Times.

- The Abstracts received for the final publication are screened by the Evaluation Committee for approval and only the selected Papers/ Abstracts will be published in each edition. Further information is available in the "Guidelines for paper Submission" section.

- Annual Subscription details for obtaining the journal are provided separately and the interested persons may avail the same accordingly after filling the Annual subscription form.

- This journal is meant for education, reference and learning purposes. The author(s) of this of the book has/have taken all reasonable care to ensure that the contents of the book do not violate any existing copyright or other intellectual property rights of any person/ company/ institution in any manner whatsoever. In the event the author(s) has/have been unable to track any source and if any copyright has been inadvertently infringed, please notify the publisher in writing for the corrective action.

- Copyright © "*Cyber Times International Journal of Technology & Management*". All rights reserved. No part of this journal may be reproduced, republished, stored, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior permission of the publisher in writing. Any person who does any unauthorized act in relation to this journal publication may be liable to criminal prosecution and civil claims for damages.

- Other Publications:
  - Cyber Times Newspaper (English) – RNI No: DELENG/2008/25470
  - Cyber Times Newspaper (Hindi) – RNI No. DELHIN/1999/00462

- Printed & Published by: Cyber Times
  310 Suneja Tower-II, District Centre,
  Janak Puri, New Delhi-110058

CONTENTS

SECTION-I
TECHNOLOGY

SECTION-II
MANAGEMENT

SECTION-III
RESEARCH ARTICLES

SECTION-IV
CASE STUDY

A COMPARATIVE STUDY ON TECHNOLOGIES FOR SECURE TRANSACTION IN MOBILE COMMERCE

By

Jyoti Batra Arora
Assistant Professor, Jagannath International Management School, Delhi
Email: jybatra@gmail.com

Dr. Sushila Madan
Associate Professor, Lady Shri Ram College, University of Delhi
Email: sushila_lsr@yahoo.com

ABSTRACT

M-Commerce is any financial transaction made through mobile devices. The mobile devices are categorized in three generation and each generation uses different technologies such as SDR, RFID, and WAP. The security has more significant importance in M-Commerce than E-Commerce. It involves data, network and memory protection through different methods during transaction through mobile devices. M-Commerce uses J2ME, WAP and i-mode as programmable display standard and involves technical or direct and non-Technical or indirect risk in security. WAP is an industry initiated standard has emerged as a common communication technology and delivering wireless services on mobile. The attacker attacks the weakest link to make a loophole in security. Java with XML makes a powerful combination of portable code and data. The customer shares very sensitive information with merchant which can be major cause of security loophole during transaction. WAP allows a relatively easy and unproblematic integration of mobile applications into existing Internet services. WAP devices uses SSL between web server and gateways a potential security breach. JAVA based applications has cross platform compatibility to enhance scalability and performance of server.

M-Commerce can improve the efficiency and effectiveness of business activities by distributing information to the workforce remote and by offering new ways in which to interact with customers. Our research work discusses these three major technologies and their usage in security of transaction. It explains the significance of security with these techniques in mobile transaction.

Keywords: i-mode, J2ME, SSL, WAP

INTRODUCTION

M-Commerce or Mobile-Commerce is a commercial transaction carried through mobile phones. It can be a process, systems or procedure that includes checking account balance, depositing a change, buying or selling any product, all this doing on mobiles. MasterCard (2000) defined M-commerce as a term to online financial transaction shopping or the transfer of funds using mobile commerce. Green in 2000 explained high conjunction of mobile devices has prompted the idea of M-commerce which is actually an E-commerce. Peter keen and Ron Mackintosh in 2001 defined M-commerce as the extension of E-commerce from wired to wireless computers and telecommunications and from fixed location to anytime, anywhere and anyone device. Veijalainen (2003) referred M-commerce to E-commerce activities performed by people while on the move. Woo and Jang (2008) defined M-commerce as e-Business with mobile device with in its fundamental concept and architecture.

Schiller categorized mobile technology into three generations. The first generation of mobile communication was analogue. The second generation used digital encoding for voice. The third generation which is in developing stage will support multimedia capabilities and circuit switched low speed data services. M-commerce uses the different technology in all generation. These technologies are **RFID**, **SDR, AMC**, **Digital Signal Compression**, **Biometric**, **WAP IPV6**, and **Turbo Codes**. **RFID** is used in packing of products on store shelve, to pay for tolls and access fees, to purchase at vending machines. **SDR** overcomes the design problems of mobile devices. **Digital signal compression or Source coding** is employed to reduce bit rate requirement with lossless compression technique like the Lempel Ziv and Huffman code. **Biometric** control includes finger imaging, palm printing, hand geometry, iris and retina vascular pattern, stroke dynamics, voice recognition and speech pattern to authenticate user to access certain place and to monitor assets. **WAP** is an industry initiated standard, has emerged as a common communication technology and delivering wireless services on mobile. The feasibility of combining these technologies for use in a specific setting will be dependent upon security protocol. Hu etal. had shown that lack of security provision created a barrier against the adoption of M-commerce. The handheld devices have equivalent computing power to the desktop. While driving more and more functionality into mobile device, the security risks such as theft, loss of data is also driving.

Some other risks are like identity theft and credit card frauds. Gururajan (2006) said that security in the case of mobile commerce has more significant importance than a traditional E-commerce as it is ease to eavesdrop into other's message with minimum difficulty in mobile environment. He categorized security risks in M-commerce as technical or direct risk and Non-technical or indirect risk (Figure-1.)

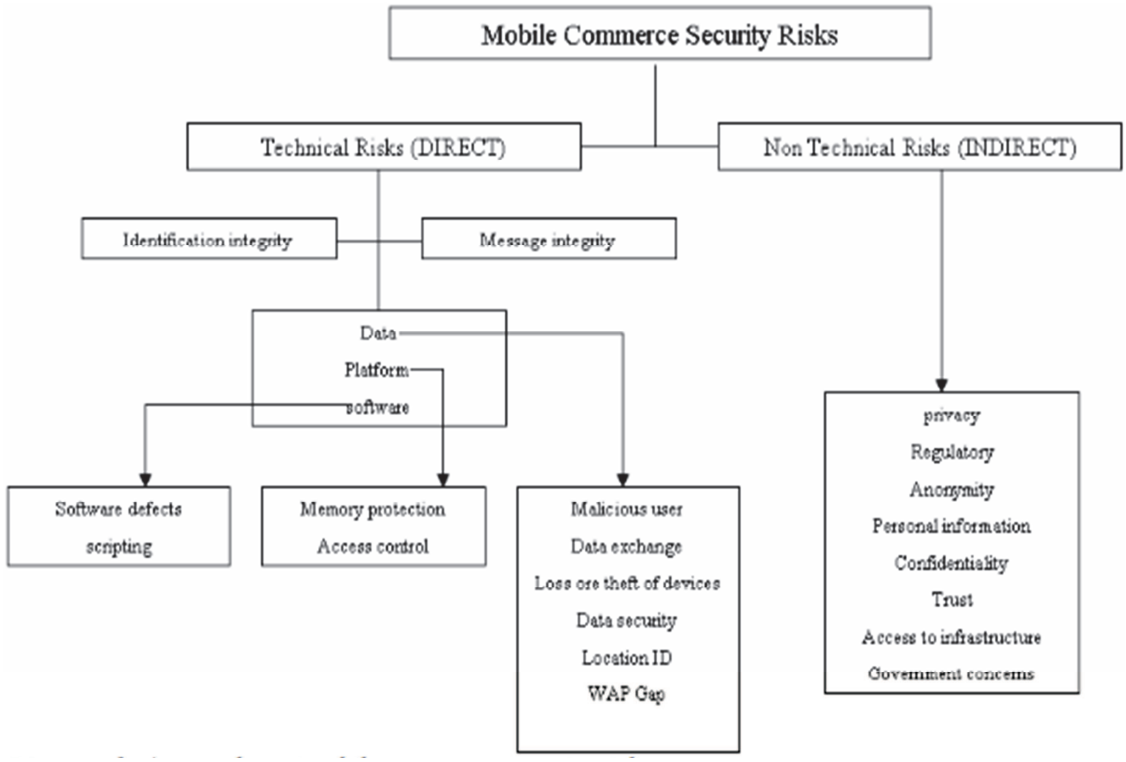

Figure-1: Security Risk in mobile commerce (Raj Gurarajan 2006)

The identification integrity refers to the signature element found in message to infer from where the message is originating the message integrity points to detail to establish that no third party opened, modify or alter the content. The technical risks have more concern of sender and service. The risk of theft or misuses of personal information and repudiation of transaction are major issues for both. Data in M-commerce is secured by using encryption technology which is vulnerable to attack. Therefore, the word complete security is obsolete the technical security risks can also be seen into impact data in a mobile commerce transaction platform to facilitate data communication and necessary protocol and software for this communication. Dorman (2001) poised that vary nature of wireless computing is the generation of adhoc network for communication. Wireless connection can be easily broken-down without adhoc network. This can be done at transport layer of network. Zhang and Lee (2000) showed that mobile user move through many different cells and adhoc network and communication is handed off from domain to domain. During this communication a single malicious domain can facilitate malicious download of data or program. Data is exchanged between mobile user and network during the realization of different services.

This is the point where information can be altered or stolen. Schiller (2000) poised that transaction in wireless communication is interrupted and reinstated without proper authentication procedure which is strictly followed by wired network. He has given the reason that WTSL does not follow rigorous authentication procedure and do not perform standard check after the establishment of connection. It helps the attacker to redirect transaction request without the knowledge of user. Most websites are not configured to deal with intermittent service failure, which becomes an advantage to attacker.

The data security is the major issue in security of M-commerce. Langley in 2000 proved that user's data can be easily revealed when he establishes a connection using protocol supporting mobile communication. In March 2000, AT&T wireless and sprint PC's sent user's phone number to the website which they accessed from their web enable wireless phone. These websites could track users and can used for offline direct telemarketing. The weak state of privacy protection is evident in the business setting too (Lee 2000).

Ghosh (2001) stressed on memory protection. He stated that most PDA devices do not provide memory application for its application which causes serious threats for each application own security and privacy attacker can steal the decrypted key in the signing application's memory. Apart from technical issues in security Shortliffe and Barnett (2001) gave a concern regarding the privacy of information. In August 2001 in West Australia the local councils parted with ratepayer information to certain building contractor. This discloses the personal information to other parties. Yampel and Eskenazi (2001) said that due to nature of transmission of M-commerce details of customers can be easily captured and analyzed. Sausser (2003) in his research has shown that data collection firm can track user's online web usage by means of software program. Clarke (2003) has identified WAP gap as another major security risk. The wireless request to a web page is translated at a WAP gateway from WTSL protocol to the SSL protocol. During this process of translation the data is encrypted and decrypted. If an attacker can access mobile network then they can easily make compromise the security. These attackers tend to attack the weakest link like server and client because of strength of the perceived security elements of data encryption. The research also states that achieving secure application is difficult without the infrastructure which fully supports security for computing application on the device. The other loophole in security of M-commerce is access control for objects to prevent unauthorized user and program from accessing confidential data in database or private keys.

Stuart and Bawany (2001) defined different software flaws in mobile transaction security. The first flaw is in the logic of a program and its implementation. The second flaw is use of low-level language for the development of application for mobile device. Thirdly, the physical limitations of these devices like limited power bandwidth and processing cycles may impose security and performance trade off. Finally security features available in advanced language like JAVA is ignored by vendors due to developmental time constraints. In M-commerce cookies are replaced with locator devices and these devices facilitate the tracking and monitoring the individual's activities. The location information can be captured even when device is merely on and not handling any call. Flink (2001) stated three major issues for necessity of trust.

They are diverse nature, the intensive use of supply chain, the empowerment of workers and self-directed team work. One has to manage technological and business risks to get a satisfactory level of trust. Simpson (2003) in his research showed that there are many incidents where personal information is disclosed without proper consent. Trust is the center of security risk in the case of mobile transaction. Green (2004) in his report said that consumers are more worried about their privacy and potential intrusion in M-commerce environment.

To grow and develop M-commerce in a country National IT infrastructure, education and awareness of citizen has important role to play. In short, future trends clearly indicate that the device manufacturers as well as service and infrastructure providers will keep adopting the WAP standard.

The major issues related to use of infrastructure are skills availability of radio frequency, technology and service cost. A minimum standard availability can hinder development. Government is concerned with regulatory framework in development of M-commerce. M-commerce uses application layer technologies like WAP/ WML, i-mode, DoCoMo, XHTML. On client side it uses J2ME and WML on open wave on like layer it has authentication key management and encryption CDMA and CDPD along with symmetric encryption and RSA is a link layer. Varshney and Vetter (2000) argue that each of the levels in the framework encompasses (I) Wireless (Network) Infrastructure (II) Mobile Middleware (III) Wireless User Infrastructure and (IV) Mobile Commerce Applications play a critical role in M-commerce success and deployment. J2ME uses 3-tier structure. Mobile middleware use MOM for communication and XML for presentation. WAP design accommodates the entire wireless network such as CDD, OMA, GSM, PDC, PHS, TDH, MOBTTEC, USSD, IS-136. It uses WCMP, WDR, WTLS and WHL protocols. Lei etal (2004) poised WAP gateway as an interpreter between the mobile device and a web server to decode and encode the information, so that the server and the mobile device can communicate with each other.

M-commerce not only includes consumer but also enterprise solutions that enable companies to operate more efficiently. M-commerce technology is expanding into enterprise market. As per Indian telecommunication report as on Jan31, 2011 the total growth in wireless sector is 771.18 million, whereas the total growth in telecommunication sector is 806.13 million.
Consumers use services like SMS for e-mail notification, SMS chat and downloading the ringing tone offered in market. Many organizations have launched M-commerce like Alliance SpintCompuwave, Mobile telephony and Yankee group (Stoica 2003). The present state of M-commerce is not stable or matured. There are some bewildering problems like lack of coherence and stability in standard and protocols in the mobile world, bottle neck in network cascade of hardware and software options.

Service and support is more important in M-commerce than traditional business. The strength of M-commerce is based on four factors: the anticipated ubiquity of devices, online access for a large portion of the world's population, location sensitivity of the devices and authentication and authorization capabilities (John etal. 2008). Different generations of mobile (1G, 2G, and 3G) play an important role in development and expansion of M-commerce. These generations varies with their speed of data transmission. Research is going on to make a seamless gaming between 2.5G, 3G and WLAN so that mobile device will detect the network with higher bandwidth and switched to it.

The handover will occur without interrupting existing connections, and then WLAN can be used as complementary technology of M-commerce [eito]. Different mobile devices use three programmable display standards- J2ME, WAP and i-mode. J2ME is java technology customized for embedded devices with limited processor, memory display and input capabilities. Java with XML creates a powerful combination of portable code and portable data. J2ME has built in consistency across products in terms of running anywhere, anytime and over any device. Java technology in mobile devices has two advantages: security and disconnected transaction with wireless synchronization. XML increases the size of parsing. Hence, operating of J2ME on cell phone becomes tough. The other technology is WAP and i-mode. If there is any security issues that disturb the M-commerce will actually affect the customer and organization. The goal of this paper is to make a comparison among three basic techniques used for making transaction through mobile.

WAP

This global standard has been developed in 1998 as WAP1.0 by WAP forum. WAP Forum is also known as open middle alliance- a consortium of leading mobile phone manufacturers including Motorola, Nokia and Ericsson. The main purpose of WAP forum is to develop an application to operate mobile telecommunication and transmit internet contents on different mobiles independent of transmission technology. WAP applications are written in WML (Wireless Markup Language) that work with all constraint of mobiles like small display, limited user input facilities, limited disk and memory resources. WAP can work with complicated graphics and images with the introduction of GPRS and higher data transfer rate. The conversion of content into WML increases the cost of WAP. The major limitation of WAP 1.0 was that the information WAP gateway decrypts the data before transmit it to web server which leads to misuse of information. In July 2001 WAP 2.0 was introduced which does not store the data in decrypted form. It use XHTMLMP (Extensible hypertext Markup Language Mobile Profile) to support the standard of WAP and i-mode.

TRANSACTION USING WAP

The mobile service provider (MSP) or mobile telephony company uses a WAP gateway to establish a connection between the wired and wireless Internet. A customer places an order using WAP enabled mobile phone to the merchant (WAP forum 2001). The merchants' website is connected to the fixed internet. The very sensitive information is shared among customer and merchant such as credit card number and address. The WAP gateway in WAP 1.2 version, the data is transmitted in original unencrypted form causes end to end security problem. The WAP gateway is software and act as a point between the customer and merchant. WAP runs on a computer under the control of the mobile service provider. The loop hole in security is that the data exchanged can be available to people with privileged access to the WAP gateway like system administrator of PC where WAP gateway is running on.

Therefore, the privacy of data depends on the internal security policy of the mobile service provider (what are the policy used by different service provider). This loop hole in security of WAP gateway is recognized by many researcher Niel christstian and Niel Jorgensen (2001) suggests not using gateway, rather using internet protocols end to end.

WTLS

The communication between WAP gateway and mobile phone has to be secured. Due to the constraint of mobile phones, SSL/TLS protocols cannot be used for this purpose. The implementation of WTLS is similar to the Internet implementation of TLS and used for transmission between mobile phone and WAP gateway. The difference between the two is that WTLS was designed so that it can cope with long round-trip times, low bandwidth connections, low processing power, small memory capacities and cryptography exportation regulations. It is these differences that pose the serious security problems. WTLS uses Elliptic Curve Cryptography (ECC) by default with advantages that it uses keys with much smaller size of 170-180 bits to achieve 1024 bit RSA level of security. WTLS also work on datagram based communication layer instead of connection based communication layer. WTLS has its own certificate format optimized for size and limited bandwidth and also support X.509 certificate.

THE WTLS PROBLEM

WTLS and TLS are not compatible. To best illustrate why this is such a large security concern, an example will be given. A wireless user is purchasing an item off a web site using TLS. They fill out the form and submit their credit card information. The wireless device creates a WTLS connection to the WAP gateway. The WAP Gateway recognizes that a secure channel is desired and attempts to use TLS to connect to the web site. A problem occurs during this process. The WAP Gateway cannot simply pass the WTLS connection along to the web server because the server only understands TLS. The WAP Gateway only has one possible way of making the connections work. It must decrypt WTLS and then re-encrypt it under TLS; this means that the WAP gateway has a point where the data that the user is trying to keep secret is available un-encrypted. This should definitely be a cause for alarm for anyone that values the secrecy of his or her personal information. It can be argued that this is not a large security hole because the conversion occurs in the memory of a trusted gateway computer. The rebuttal to this point is to talk about the history of TCP/IP. When that protocol suite was in its infancy, there were parts where trust was assumed between two parties but as the technology grew, users became aware that they could take advantage of this trust and exploit systems. An example of this type of behavior can be found in the method that TCP used to simply create a connection every time that one was requested, but look at what happens today. A user could flood a server with millions upon millions of connection requests and eventually cause a denial of service error. This is just an example of misplacing trust, especially early in the life cycle of a protocol suite. In the WAP problem, if the gateway were ever compromised, then that hacker could have access to all the confidential information by dumping the contents of memory into a log and then searching for known patterns that contain credit card numbers.

WAP allows a relatively easy and unproblematic integration of mobile applications into existing Internet services. Web servers can be modified with the help of suitable software to offer WAP functionality. Only a WAP gateway is required as hardware the content must be made WML compatible so that it can be read by mobile devices.
Translating all relevant content into WML increases the cost of WAP. WAP works only on special programming language XHTMLMP. WAP devices uses SSL between web server and gateways a potential security breach. But if SSL is striped out and data is placed into another security format, the data would be potentially exposed on the carrier's network. Java technology uses java application can run on a mobile even when it is disconnected or out of coverage area.

J2ME

Unlike WAP, we can run and interact with most of the application in standalone mode and can be synchronized with backend infrastructure later. Java helps in dynamically download of new application. Java based application has cross platform compatibility which increases the scalability and performance for server and reduces demand for network bandwidth. Another major drawback of WAP is that contents must be compatible with WML only. The mobile technologies are the most successful technologies that have emerged into society as its relative short time to perform any task that desktop computer can perform. The other advantage is using the mobile devices that allow us to send and receive data with an ease from different location. To provide secure solution for storing and accessing data J2ME includes security and trust services API (SATSA).

This is flexible to run with different protocols and cryptographic algorithm on CDC and CLDC configuration. All packages require a smart card except SATA crypto package which provide classes for implementing data security architecture based on message digest, digital signature, symmetric and asymmetric encryption/decryption algorithm. The other solutions like bouncy castle crypto apis provide a light weight cryptography, API for implementing security architecture in a mobile application. There are different storage location to store the data in mobile device.1) Active memory 2) Small database 3) Persistent Memory:J2ME uses RMS(Record Management System) –a simple record based persistent storage mechanism to store the binary data within a record store which allow mobile application to add, remove or update data. RMS cannot manage large sized resources like multimedia application; therefore extension of external memory of device by using memory cards can be solution to these problems. The user input data is compared with data in the device persistent memory. The MIDlet application can also store persistent data with RMS system. Each application has a unique id to utilize the RMS space. The data location within device memory is dependent on the RMS id and is not exposed to an inquiring MIDlet, the data is secured.

This scenario offers a relative data security and vulnerable to reverse engineering and brute force attacks on device memory. The implemented techniques are used to hide clear data behind a cipher value to increase the level of security, which can be obtained by computing a message digest value.

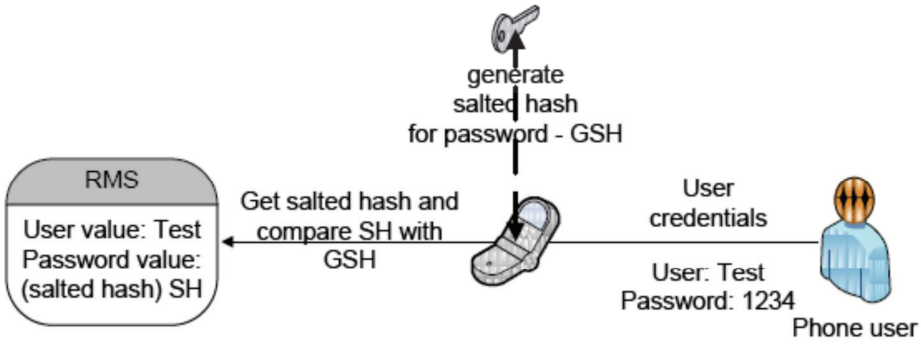

Figure-2: Storing Password Salted hash within RMS.

The clear data can store the short sensitive values using message digest values using a message digest algorithm and the result is stored in RMS. A hash value is given to each value using algorithm. The function is one-way and not possible to obtain the sensitive value from its hash value. This function does not provide a perfect security solution as it is very prone to collision. A brute force or dictionary attack can be used to attack is used to guess password. The sensitive data is salted before completing the hash value to protect the hash value being used to obtain the input value. The salt is an additional value added to clear password to modify the message digest. The next sequence generates a SHAI 160bits, 20 bytes, hash value which is the salted form of the password. The **J2ME** also support MD5 message digest which generate 128 bits hash value. The encryption algorithm is the alternate to message digest solution, which generate a cipher text from a clear text and decrypting of the cipher is used to get the clear data. The cipher can be stored using either RMS or the file system. The major disadvantage of encryption is that it affects the application performance and battery life.

I-MODE

NTT DoCoMo – a Japanese network carrier introduced i-mode in 1999. It is based on iHTML i.e. i-mode compatible HTML. It works on packet switched technology hence compatible with GPRS and UMTS and makes use of push and pull services (Teltarif 2004). User can access the internet services and charged according to volume of data transmitted. The i-mode compatible sites can be categorized as following:

CONTENT PROVIDED BY OFFICIAL PROVIDER

The contents are integrated in i-mode menu and can be accessed directly by clicking the menu. These official partners have an agreement with NTT and charged 9% commission for collecting the bills and approving the contents.

CONTENT PROVIDED BY UNOFFICIAL PROVIDER

These sites can be viewed like other Internet sites i.e. by typing the address in browser. The providers of these sites have their own mechanism to collect charges for their services. The content providers need not to pay fees for i-mode compatible content. The actual profit of NTT is by transferring data on account of network usages. The other network carrier requires a license to offer i-mode services. It is very successful in Japan and has shown a little success outside Japan. There are only fourteen countries that have i-mode enabled services. These are Taiwan (2002), Germany (2002), Holland(2002), Belgium (2002), France(2002), Spain(2003), Italy(2003), Greece(2004), Australia(2004), Israel(2005), Russia(2005), United Kingdom(2005), Ireland(2005) and Singapore(2005). In Germany, over a million E-plus and O2 users are using i-mode services. The service is named as MMO2 owing to legal complication with E-Plus.

M-COMMERCE IN BUSINESS

The Internet is a platform for what is to come, a business platform, a technological platform and a platform for managerial experience. On this basis, it is possible to have pervasive wireless network in faster pace than the Internet did because companies can leverage the lessons of the past. The Jupiter consumer survey showed that 33 percent of mobile users are not using M-commerce because they feel that their credit card or payment information is not secured. It also states that in December 2000, hackers broke into the commerce site of Egghead.com and were suspected of stealing more than 3 million credit card account numbers. Through this study industry sector can gain substantial benefits in manufacturing, marketing and retailing. Gartner Group report (2001) showed that manufacturing firms utilizing M-commerce have increased worker productivity. Juniper report (2010) has shown that more than 76% of consumers surveyed use their smart phones to access personal or business information, including 51% to enter or modify passwords, 43% to access banking and credit card statement, 30% to access utility bills, 20% to share financial information, 18% to access employer's proprietary information, 17% to access medical records, 16% to share security numbers.

M-commerce require ISO 9001:27001 as its security certificate. Bharti Airtel got award in 2009 from ISO for standardization. It also uses ISO/IEC 27001:2005 for security techniques and information security management.

The futures of M-commerce would not only be low costs user friendly high speed connection and high level of security, but also be automatic language translator pre-installed so that everyone would understand each other irrespective of their language. This technology would develop faster than everyone could imagine. Leung and Antypas (2001) showed that M-commerce could improve the efficiency and effectiveness of business activities by distributing information to the workforce remote and by offering new ways in which to interact with customers. Nadesan (2001) poised that investing in effective mobile technology is likely to increase mobile workers productivity 30%. The US advocated that Internet commerce should be a tax free zone.

LITERATURE REVIEW OF THESE TECHNOLOGIES

Bergstrom (2001) had given trust, user friendliness, business models and regulatory aspects as other security issues. Tarasewich etal. (2002) had shown three technological issues: mobile clients, communications infrastructure and other technology. M-commerce firms require the security control like firewalls, anti-virus protection user identification: authentication and secure device management to protect company network and web applications.
Standardization, privacy and security solutions and electronic cash format reap a competitive advantage. The literature is also available on different technologies used in M-commerce for security measurement.

Baldi and Thaung's (2002) described i-mode and its impact as security measure in M-commerce. They have also explained its adoption process from cultural prospective. Okazaki (2004) conducted an empirical study of pull-type advertising platform on i-mode. His proposed model was based on users and gratifications theory and on Dacoffe's (1996) Internet advertising value model. His finding suggests information, entertainment and irritation are the three primary factors that influence consumer's intention to click text banner ads in mobile platform. Varshney (2005) in his study has shown that WAP, i-mode and J2ME are major security services used in M-commerce. He has explained the effectiveness of J2ME over WAP.

In the study Mourad etal. in 2006 described J2ME CLDC security model. They designed the set of attack scenario and execute them. Yaun and Lung (2006) in their study proposed that applications in J2ME offer more in terms of features and security than WAP. They have also explained that for high level mobile security code one should look no further than J2ME applications. The research paper given by sun micro system in 2006 supported the same, but it also lack to explain how XML format can be lighter for limited wireless bandwidth.

In the study in year 2007, different encryption methods for the security of transaction in M-commerce were given. This study showed that quasi group encryption is rather a new encryption method that has not been studied very much by the cryptographic community. There is still a lot to do in security analysis of this cipher. It is based on table lookup, and implements white box cryptography which would be more straightforward than with block cipher, such as DES or AES.

Presently research is going on i-mode and J2ME. WAP forum is used in most mobile devices. Researchers have given many papers in development and growth of WAP. In i-mode, digital radio packets are sent between handset and radio towers are encoded via a proprietary DoCoMo scheme.

This information about this scheme is not available. Java platform make users to develop portable code that can run on multiple platform. It has been designed to strike a balance between portability and usability. In the study given by Kanvalwir (2009), it has been shown that strong use of transplanted J2ME technology development process and its short development life cycle made it so popular. He has also shown that use of J2ME technology is increased because of increased use of mobile devices. The J2ME CDLC security model developed in above work do not project permission and protection domain in M-commerce. Though the cryptographic techniques are available but on mobile networks they are easily hackable.

The study on different security techniques could not able to explain any model for adoption of mobile for daily transaction. The gap in the literature is due to the fact that all aforesaid studies include a specific technology with specific type of mobile system. The above studies could not explain the security techniques which can be used on any mobile and addition of a new factor which affects the security is difficult. Also the tools to measures the risk in security are not explained by these studies. Moreover, the security protocol using J2ME during mobile payment practically could not develop a prototype for stimulated environment and delays and error in sending the messages for payment.

Also mobile CMS were not compatible with technology as web application which is gap in aforesaid studies that is updating of application on mobile devices through GPRS. The absence of proper management can have negative effect in the performance of business and lead to failure of mobile computing.

CONCLUSION

Since research is going on the different areas of M-commerce, but still there are lacking in some fields of research like operating system. Most mobile devices have simplified operating systems. M-commerce is a new innovation in the market therefore, there is not much research regarding its impacts. Many researchers poised on general aspect of M-commerce. Other researchers have focused on different areas like issue and challenges of M-commerce, a framework for its applications, mobile clients and communication infrastructure and fourth generation wireless network. The issues and challenges of M-commerce vary from market to market like in U.S. it is involved in potential growth whereas in Europe it is focused on a socio-economic analysis of new market evolution. There are basically three challenges in M-commerce: technical challenges, business and security issues.

The prime concern is that M-Commerce has to deal with the new problem of finding location dependent data which is also given as a future scenario by most of the studies. Most of the studies describe about the security techniques in M-commerce and few of them also focus on adoption of mobile technology.

This paper discusses the three major technologies and their usage in security of transaction in Mobile commerce. It can be concluded from the aforesaid study that though Mobile commerce is emerging area of business but still more research is required to make it secure from any device. The i-mode has many advantages over WAP. Firstly, the content providers need not to install their own payment mechanism and being charged at low rate. Secondly, iHTML is the subset of HTML, so Internet contents can be transferred with fewer problems.

WAP uses XHTMLMP which is compatible to WAP and i-mode; but i-mode still require special i-mode compatible device. The research work explains J2ME usage with XML in mobile devices and security in mobile transaction. However, the study could not explain the standardization of these security services in M-commerce and limitation of different types of mobiles using these technologies.

REFERENCES

[1] Abhijit Chaudhary, Jeam-Pierre kuilboer (2002), "*E-business and E-commerce"*

[2] *Infrastructure: Technologies supporting*", the e-Business Initiative, United states, Mcleraw – Hill Iswin

[3] Alka gupta and Mayank Srivastva, 2002"*Integrated Java Technology for End to End M-Commerce"*

[4] Baldi, S. and P.P. Thaung 2002, "The entertaining way to M-commerce: Japan's approach to the mobile Internet – A model for Europe?" Electronic Markets, Vol. 12, No. 1: 6-13.

[5] Brittos Ramesh Kumari, Rabara Alberts 2010,"An architectural Design for secure Mobile Remote Macro payments", Journal of next generation Information Technology, Vol 1, No 2.

[6] European information Technology observatory 2004' edition 15, October 2004, Brussels

[7] Fahy M, J feller, P. Finnegan and C-Murphy 2002,"Measuring and Managing intangibles in mobile commerce: The potential of mediation standards", PRISM case 9.1.1.Ist project 2000– 29665 RESUE European case clearing house (reference no 302 -162-1)

[8] Fatahi Somayeh 2010,"ARMrayan multimedia Mobile CMS", IJCSIS, vol. 8, no 5, August 2010.

[9] Green, P., 4 June, 2004."Eastern Europe's Foray into M-commerce", The New York Times p.3.8

[10] Gururajan Raj, 2006 "A Discussion on security Risk in Mobile Commerce", e-Business Review, 7(2), ISSN 1229-6546

[11] Hope-Rose. D. (2001)," Successful E-Business Deployment: Beyond Software" (No.COM 14-5080): Gartner

[12] http://www.mastercardintl.com/newtechnology/mcommerce/whats/

[13] http://www.micsymposium.org/mics_2006/papers/HuKaoYangYeh.pdf

[14] http://www.cstechnion.ac.i//~biham/publications.html (2007)

[15] Hu, P.J.Chau, P.Y.K., and LiuSheng.O.R. (2002), "Adoption of telemedicine technology by health care organizations: An exploratory study", Journal of organizational computing and electronic commerce, 12(3).197-222.

[16] Infotech (N.D.), Answers to your queries, http://www.salahkarindia.com/queries/infoechanswerseries.html.

[17] John Garofalakis, Flora Oikonomou, Vasilios Stefanis, 2008,"System's Design and Implementation for Easy Creation of Mobile Commerce Systems," iciw, pp.115-120, 2008 Third International Conference on Internet and Web Applications and Services

[18] Kannan PK, A chang and A.B. whinstone 2001,"Wireless Commerce: Marketing Issues and Possibilities", Sprague RH Jr (Ed.), Proceedings of 34th Hawaii International Conference on System sciences, Pis cataway, New Jersey, IEEE

[19] Keen, P., Mackintosh, R., 2001."The Freedom Economy: Gaining the m-commerce Edge in the Era of the Wireless Internet", McGraw- Hills.

[20] KrodaT, Wihofiezki.O, "MMO2 bietet handy Portal I-MODE", Financial Times Deutschland No. 235/49 P551.

[21] Lee. A. (2000),"Small firms must take Internet plunge or risk being side-lined". The Engineer,10 (November 2000), 10

[22] Lei P.W, Chalwin CR, Young RCD, Tong SH, "Opportunities and limitations in M-Commerce", Shi, Nan Si (Eds :) wireless communications and mobile commerce, Hesschey 2004, Pg 80-104.

[23] Leung k and J Antypas (2001), "Improving Returns on M-commerce investments", Journal Business strategy 22:12-13

[24] Maffeis, S. 2000. "M-Commerce Needs Middleware!"

[25] Maginnis F, R White and C Mckenna (2000),"Customer on move: M-commerce demands a business object broker approach to EAI" .EAI Journal, NOV /DEC

[26] Mourad Debbai, Mohamad Saleh, Chmseddine Tali and Sami Zhioua 2006,"Security Evolution of J2ME CLDC Embedded Java Platform", Journal of Object Technology Vol 5 No 2 March-April 2006, Pg 128-154.

[27] Mayer, R.C., Davis J.H., and Schoorman, F.D. (1995),"An integrative model of organisation trusts". Academy of Management Review, 20(3), 709-734.

[28] Okazaki, S.2004, "How do Japanese consumers perceive wireless ads? A multivariate analysis," International Journal of Advertising, Vol. 23, No 4: 429-454.

[29] Powell, M (1997), "Electronic Commerce: An overview of the legal and regulatory issues", International Trade Law and Regulation, 3(3), 83-93 Ross (2000) CBS, Broadcasting and Cable (February), 38

[30] Scniller. J. (2000) "Mobile Communications" New York: Addison-WesleyStuart, D., and Bawany, K. (2001), "Wireless Service: United Kingdom (operational Management Report No.DPRO-90741): Gartner"

[31] Sharma Rajiv, Sharma Rupak, Raj Shailendra 2011,"confronts and issues in m-commerce [a business on mobile and net approach]", International journal of information technology and knowledge management, vol 4, no1, pp51-55.

[32] Sawma V and R Probert 2003, “Specializing the NIST security service model for electronic commerce systems”, Federal information systems security education association (FISSEA) 2003 annual conference, March 4-6 silver spring MD

[33] Tarasewich P, R.C Nickerson and M Warkentin 2002, “Issues in mobile e-commerce”, Common Assoc Inform sys 8:41-64

[34] Varshney U & R Vetter 2000,”Emerging Mobile and Wireless Network”, Communications of the ACH, 43:73 – 81

[35] Varshney Upkar, Alshaali saif 2005,”On the usability of mobile commerce”, International journal of mobile communications, Vol. 3 Issue 1

[36] Veijalainen, J, Weske, M, 2003 “Modelling Static Aspects of Mobile Electronic Commerce Environments”. Chapter 7 in Advances in Mobile Commerce Technologies, Lim Ee Peng,Keng Siau(eds.)IDEA Group publishing,137-170.

[37] Woo Jongwook, Jang Minseok 2008,”The Comparison of WML, cHTML and XHTML-MP in M-commerce”, Journal of Software, Vol 3, No. 7.

[38] www.mobilecommercdaily.com/2011/01/06/mobilesecurity-the elephant in the room.html

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

[40] Wireless Review (August).24-30

[41] Zhao, P.C., 2003, “Limitation of Mobile Commerce”, http://pczhao.netfirms.com/elimit.html

CATEGORIES COVERED

The categories covered in this Issue are as follows:

Technology

Cloud Computing, Artificial Intelligence, Wireless Networks, Cyber Security and Network Attacks, Penetration Testing, Cyber Laws, Cyber Crime Investigation, Data Mining, Databases, Mobile Commerce, Software Testing, Ecommerce etc.

Management

Management Strategies, Human Resources, Business Intelligence, Global Retail Industry, Business Process Outsourcing, Indian Economy, Performance Management, Risk Management, International Business.

Research Articles

Atomic Power and Open Source Software.

PRICE: 850

H. O.: 310, Suneja Tower-II, District Centre, Janak Puri, New Delhi-110058.
Ph: +91-9312903095, **Email:** editor@cybertimes.in
B. O.: 519, Dattawadi, Near P. M. C. School, Sinhgad Road, Pune - 411030.
Ph: +91-9860201117, Email: editorpune@cybertimes.in