The International Journal Of Engineering And Science (IJES)
|| Volume || 5 || Issue || 6 || Pages || PP -70-75 || 2016 ||
ISSN (e): 2319 – 1813 ISSN (p): 2319 – 1805

A Survey on Mobile Commerce Security Issues and Applications

K Sridhar[1] Dr.D.Suresh Babu [2] and Dr.T.Venugopal[3]
[1] *Research Scholar, JNTU Hyderabad, Telangana*
[2] *Dr.D.Suresh Babu, Head, Dept CS, Kaktiya Government College Hanmakonda, Telangana*
[3] *Dr.T.Venugopal, Associate Professor, JNTU Sultanapoor, Telangana*

----------**ABSTRACT**----------
Electronic saving money and Mobile managing an account are seen as one of the best business-to-buyer applications in electronic trade and versatile business. The utilization of e-saving money and m- managing an account particularly in created nations has become quickly. Low charges, time investment funds and opportunity from time and spot have been observed to be generally imperative components of e-managing an account and m-saving money. These administrations are simple to utilize helpful and good with way of life , pace of administration conveyance is quick. There are two sorts of administrations offered in e-keeping money and m-keeping money, i.e. A) Notifications and alarms and B) Data, in which the bank sends messages containing data or notice required by the client. In this paper shows another system for using so as to enhance security of these messages steganography and cryptography system together.
Keywords: *Steganography, m-management, e-saving,wireless secuit.*

Date of Submission: 17 May 2016 Date of Accepted: 27 June 2016

I. INTRODUCTION

Electronic keeping money altogether changed the route in which numerous clients' Original copy got May 9, 2012; reexamined June 13, 2012. Creators are with the Department of Computer Engineering, Government School of Engineering & Research, Awasari, Pune, India (email: patu_pawar@yahoo.co.in; shgawande@yahoo.co.in). Gotten to their ledger. Banks incredibly bolster this not just on the grounds that they could address their client's issue for accommodation additionally on the grounds that of the gigantic financial effects in supplanting a high-cost channel (bank representatives) through an ease channel (a focal web server) for straightforward exchanges, with the extra advantage of killing the need for a media change. Since clients considered their cellular telephone as an individual trusted gadget making it to a basic piece of their lives and the greater part of these gadgets got to be Internet-empowered, the normal conclusion was the change of saving money applications to cell phones as the following stride of electronic saving money advancement. For portable saving money, the favorable circumstances even go much further than for electronic keeping money: The high entrance of portable telephones achieves every single social level, versatile applications disband the impediments of electronic keeping money as they take into account an utilization at whatever time anyplace and the subjective and target security of the gadget is higher than that of a PC . There are two sorts of administrations offered in e-keeping money and m-keeping money, i.e. A) Notifications and alarms and B) Data, in which the bank sends messages containing data or notice required by the client. In spite of the fact that the conventions in the system have expanded the security of these messages and counteract revelation of this data as far as could be expected under the circumstances, this paper shows another system for using so as to enhance security of these messages steganography and cryptography system together.

Steganography is a craft of concealing data. The objective of steganography is to have undetectable correspondence in totally imperceptible way while the objective of cryptography is to secure correspondence from a busybody. Pictures are perfect for data concealing as a result of the extensive measure of space is made in the putting away of pictures. Steganography comprises of routines for transmitting mystery messages. These mystery messages are exchanged through obscure spread bearers. In this system before concealing message into a spread picture; message is scrambled first by utilizing AES calculation and afterward this scrambled message is handled to cover up into a picture so that steno-picture contains shrouded message which is not in plaintext structure. Another essential point is that we are stowing away encoded message into a picture utilizing "Arbitrary LSB Steganography" that is installing information in non-consecutive LSB insertion design with the goal that it is indiscernible and inconsistent to identify.

II. APPLICATIONS OF M-COMMERCE

Keen Cards with an implanted coordinated microchip can be utilized as prepaid telephone cards, ATM cards, or open transportation cards. They can be biometrically upgraded to incorporate voice acknowledgment, iris and face outputs, and unique mark confirmation. In France, approximately 35 million Keen cards are available for use and consistently they handle more than three billion exchanges [4]. Remote saving money alludes to acquiring over Web empowered HWDs like remote application convention (WAP) telephones or PDAs. Intuitive television is improved television where extra substance is added to a current telecast arrange that the viewer can inquiry, demand or even communicate live with the system. It has held channels and transfer speed for information applications, for example, climate, news, diversions, or business. It additionally offers administrations like Feature on Interest (VOD) or Individual Feature Recording (PVR). Organizations are giving offices to track stocks on HWDs. Aspiro, a Swedish organization, permit its clients to check stock costs or take a gander at their portfolios and even exchange utilizing WAP telephones or PDAs. Getting to data utilizing WAP cell telephones and PDAs is fundamentally getting to be well known for business-to-business (B2B) and business-to-customer (B2C) applications. Versatile and remote advances have been a vital piece of barrier and military since the time that these advances were accessible. In light of developing concern with cyberterrorism, security has without a doubt turned into the absolute most vital issue on the grounds that numerous U.S. insight administrations use versatile advances and remote systems for correspondence and business.

III. M-COMMERECE SECURITY CONCERN

M-Business is uniting two advancements, remote correspondence and customary E-Trade, with a background marked by security issues. Combined with the joining of voice and information interchanges, between association with outside information systems and issues encompassing the exchanges themselves, the potential dangers are high [7]. There are three fundamental security segments in M-Trade: (an) Exchange: providing so as to ensure the exchange parties and their information a worthy level of security, (b) Data: securing important and delicate data about clients, and (c) Foundation: shielding the system framework from assault.

Portable 3D is Visa Worldwide's new worldwide secure particular that is relied upon to guarantee the security of Web installments made over cell phones [14]. It was created in conjunction with somewhere in the range of 15 businesses, including Ericsson, Motorola, and Prophet Portable, and was propelled in September 2001. It expands installment authentication activities into M-Business, empowering the Visa card backers to accept the character of their cardholders progressively, guarantees that installment information sent over open.

systems is not traded off and permits shoppers to effectively shield their Visa accounts from unapproved utilize, and backings worldwide interoperability, empowering customers to have a predictable and consistent experience paying little heed to the strategy or gadget being utilized to get to the Web. Various Visa M-Trade projects are presently in progress worldwide to test the legitimacy of M-Business installment arrangements and raise shopper's mindfulness. In Asia, Visa has joined forces with Hutchison Information transfers and Dao Heng Bank to add to a portable installment administration utilizing versatile 3D Safe. In Europe, Visa has made a vital partnership with Omnitel Vodafone, while in the US, Visa and Sprint are cooperating to help encourage secure portable installments.

An acceptable level of security is needed for the effective arrangement of HWDs. To a certain degree, it appears to be sensible to use arrangements utilized for the wired environment as a part of the instance of the remote environment. In any case, this methodology is not generally attainable in light of the contrasts between the wired and remote environ-ments. For instance, in light of the equipment restrictions of the HWDs, no huge directing tables can be kept up on these gadgets, in this way expanding the danger of a refusal of-administration assault. Moreover, remote correspondences make physical listening in verging on imperceptible [10]. Like wired correspondence, remote correspondence additionally needs three fundamental security necessities: (i) confiden-tiality-data is unveiled just to honest to goodness substances or procedures, (ii) honesty unapproved alteration of data is counteracted, and (iii) accessibility approved elements can get to an administration gave they have appro-priate benefits. The components suitable to the HWD are talked about here. M-Trade needs a few layers of security: (i) gadget security, (ii) dialect security, (iii) remote security, and (iv) cryptographic security.

3.1 Device Security

Inside of the configuration of cell phones, there are various amazing security highlights. The most essential of these are: (i) an implicit watchword mechanism which will bolt after a few mistyped endeavors and (ii) an industry affirmed, sealed savvy card, known as Endorser Recognizable proof Module (SIM) card.

The SIM card and the cell phone are constantly put away together and the gadget is a consistently utility question that is effectively lost or stolen. Time-out and key-locks are regularly not utilized on telephones. This implies that the length of the telephone stays turned on the solid secret word framework will be skirted. All WAP information, in some well-known handsets, is put away in the telephone's memory, not in the SIM; this will incorporate login and secret key data. These components positively reduce the security of the cellular

telephone. The SIM card utilized as a part of cell phones are accepted smaller scale processor and they can be utilized to encourage versatile business. Gemplus SIM cards include an advanced signature and open key encryption [11] and the innovation is implanted in the card. In May 1999, Motorola, mutually with Identix, the biometrics organization, created unique mark filtering gadgets, called the DFR 300 that is 4.5 milli-meters thick. This filtering gadget can now be incorporate into the HWDs.

3.2 Dialect Security

On the off chance that extraordinary reason M-Business programming, for example, a stock exchanging application, is to be sent on cell phones, then Java is the prescribed dialect to be utilized as the sending dialect on the HWDs. By utilizing Java, the measure of programming that should be changed with a specific end goal to embrace the application to different portable stages is minimized. Doable Java execution situations are accessible for PDAs, Advanced cells, Communicators, (for example, Symbian), portable workstations, and different stages. Maffeis [6] likewise prescribed utilizing server side Java innovation, for example, the Jave-2 Venture Version (J2EE) stage, in the server farm. This considers shorter time-to-market and maintains a strategic distance from merchant lock-in.

3.3 Wireless Security

3.3.1Wireless Application Protocol (WAP)

WAP is "an open, worldwide detail that engages portable clients with remote gadgets to effectively get to and interface with data and administrations in a split second." WAP is as of now the main freely accessible answer for remote correspondence and empowers M-Trade where Web information moves to and from remote gadgets. WAP-empowered telephones can get to intuitive administrations, for example, data, area based administrations, corporate data and between dynamic amusements. WAP is focused at different sorts of HWD and Bluetooth empowered cell telephones.

3.3.2 WAP Security

WAP 1.x security utilizes the Remote Transport Layer Security (WTLS) convention. This convention is what might as well be called Secure Attachment Layer (SSL) and it gives confirmation, encryption and honesty administrations. WTLS has three levels, all have security and respectability: (i) Class-1 has no confirmation (mysterious), (ii) Class-II has server validation just, and (iii) Class-III has both customer and server verification. WTLS bolsters some well-knownalgorithms like Diffe-Hellman, RC5, SHA-1, and Thought. It likewise bolsters some trusted systems like DES and 3DES, yet it doesn't bolster Blowfish and PGP.

Since Web-and WAP-based conventions are not specifically interoperable, a segment knows as the WAP portal is required keeping in mind the end goal to make an interpretation of Electronic conventions to and from WAP-based conventions. The WAP entryway is programming which keeps running on the PC of the Portable Administration Supplier (MSP). In this way delicate data is deciphered into unique decoded structure at the WAP portal [5]. This issue is known as WAP crevice.

Open key cryptography (PKC) is utilized to trade a symmetric or private key utilizing authentication and afterward all transmission is encoded. A short key size of 40 bits is utilized due to power restriction. A sealed component, known as WIM (Remote Personality Module) is outlined as a component of the WAP structural planning to store private information, for example, key matches, testaments, and PIN numbers inside of the cell phone. By and by, a WIM is implemented utilizing a keen card. Remote Markup Dialect (WML) is utilized as a part of WAP 1.x innovation. Figure 1 shows WAP hole model.

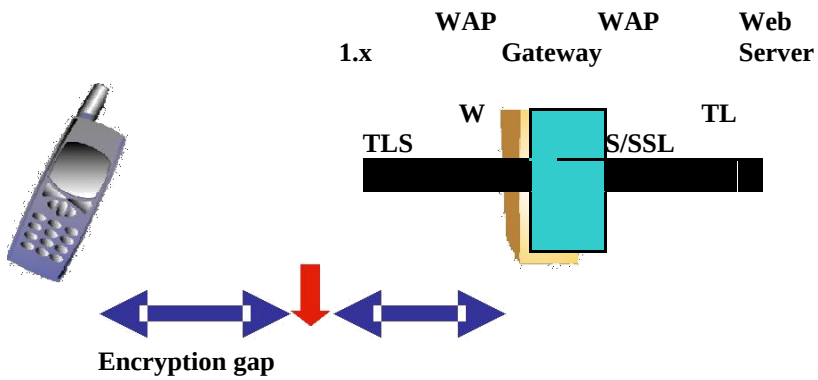

Figure 3.1 WAP Gap Model (not a full end-to-end security)

WAP 2.0 security uses TLS (Transportation Layer Security) instead of WTLS due to requiring end-to-end security with all IP based technology in order to overcome the WAP gateway security breaches. It is a Public Key Infrastructure (PKI) enabling protocol that provides the services such as authentication by using digital signatures and public key certificates, confidentiality by encrypting data, etc. This protocol uses RSA, RC4, 3DES, and SHA-1 algorithms for encryption. Wireless PKI (WPKI) is released for the first time. Figure 2 shows the WAP proxy model.

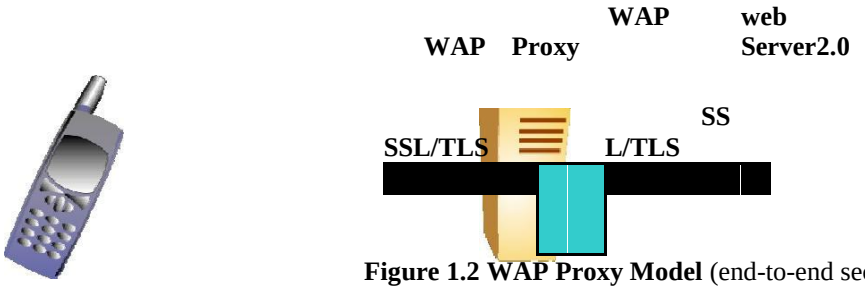

Figure 1.2 WAP Proxy Model (end-to-end security)

3.3.3. PKI/WPKI

PKI frameworks and WTLS are at the heart of today's versatile security innovation. In a WAP situation WTLS must be deciphered at the WAP passage into SSL, the Web standard. A PKI is an arrangement of approaches, processors, programming, equipment, and advances that utilization PKC and authentication administration to secure correspondence [18]. PKI's trusted administrations empower the protected exchange of data and backings a wide mixed bag of M-Trade applications. PKI must guarantee the accompanying: (i) privacy, accomplished by Cryptography, (ii) verification, accomplished by computerized certificates, (iii) respectability, accomplished by advanced marks, and (iv) non-disavowal, accomplished by computerized marks and endorsements.

PKI comprises of the accompanying segments: (i) Testament Power (CA)- in charge of issuing and repudiating authentications, (ii) Enrollment Power (RA)- tying between open key and the characters of their holders, (iii) Endorsement Holders-individuals, machine or delicate product specialists that have been issued with declarations and can utilize them to sign advanced reports, (iv) Confirmation Power (VA, Customers)- approve computerized marks and their testaments from a known open key of a trusted CA, and (v) Storehouses stores that make accessible authentications.

WPKI is an improved expansion of customary PKI for the remote environment. "WPKI includes the necessary cryptographic innovation and an arrangement of security administration principles that are generally perceived and acknowledged for meeting the security needs of M-Business" [18]. WPKI applications need to work in a domain with less capable CPUs, less memory, confined force utilization, and littler showcases. WPKI arrangements are prone to utilize "system specialists" that deal with some of these errands. The HWD must in any event have the capacity to perform a computerized mark capacity to allow the foundation of a WPKI. System operators can perform all other WPKI-related assignments, for example, approval, and documenting or declaration conveyance. Figure 3 demonstrates a schematic outline of WPKI.

Figure 1.3 Wirelesses PKI

The private keys are put away in WIM or SWIM. Two primary segments of WPKI are the PKC and the key affirmation administration. Keeping in mind the end goal to perform comprehensively, overall PKI enactment is needed. Various organizations, including Endow, Certicom, RSA Security, VeriSign, and Baltimore, have declared arrangements empowering the utilization of PKI programming in a remote domain. The greatest test in executing a PKI answer for remote arrangement lies in the gadgets them-selves. With constrained transfer speed and low power, a little screen and no console, the normal cell phone introduces various exceptional issues. Certicom developed Circular Bend Cryptography (ECC) that lessened the key size from RSA's 1024 bits to as

few as 56 bits and made taking care of endorsements a great deal simpler for low-data transmission and low-control gadgets [2]. This method can transform an advanced mark in a brief moment contrasted with the RSA procedure, which takes just about 15 seconds to process a computerized mark on a Palm gadget. Both Nokia and Ericsson have been supporting server declarations since the center of 2000.

IV. WIRELESS LAN SECURITY

4.1 IEEE 802.11B

The WLAN standard IEEE 802.11b gives a system to verification and encryption. It gives a greatest of 11 Mbps remote Ethernet associations utilizing the band at 2.4 GHz. 802.11b security components comprises of security system called Wired Proportionate Protection (WEP) . WEP is in light of RC4, a symmetric stream figure. It has a pseudo-irregular number generator, whose yield is XORed to the information. WEP can utilize 40 or 128 bits key size. In any case, utilizing a 128 bits key size, 802.11b throughput drops much because of substantial figuring. In August 2001, RC4 was declared to be softened and can be laughed to the point of tears not as much as thirty minutes. Thus, WEP can be broken. WEP with 40 bits key size can be softened up constant.

4.2 Bluetooth

Bluetooth innovation, created by Ericsson in 1998, is utilized to join distinctive HWDs and gives a system to confirming gadgets. Gadget validation is given utilizing a mutual mystery between the two gadgets. The normal shared mystery is known as a connection key, produced from PIN. This connection key is set up in a unique communication session called matching. Every single matched gadget share a typical connection key. There are two sorts of connection keys: (i) unit keys and (ii) mix keys [17]. The connection key is a 128-bit arbitrary number. A gadget utilizing a unit key uses the same mystery for the greater part of its associations. Unit keys are proper for gadgets with restricted memory or a constrained client interface. Amid the matching methodology the unit key is scrambled and exchanged to the next unit. Stand out of the two matched units is permitted to utilize a unit key. Mix keys are connection keys that are one of a kind to a specific pair of gadgets and they are just used to secure the correspondence between these two gadgets. Unmistakably a gadget that uses a unit key is not as secure as a gadget that uses a blend key. Since a unit key is basic to all gadgets with which the gadget has been matched, every such gadget has information of the unit key. Subsequently they find themselves able to listen stealthily on any movement in light of this key.In each Bluetooth gadget, there are four elements utilized for keeping up the security at the connection level: (i) the Bluetooth gadget has an IEEE characterized 48-bit exceptional location, (ii) a private confirmation key which is a 128-bit arbitrary number, (iii) a 8-128 bit long private encryption key, and (iv) an irregular number, which is often an evolving 128-bit number that is made by the Bluetooth gadget itself [12]. The security calculations of Bluetooth are viewed as solid. Bluetooth standard does not utilize the RC4 figure; rather it utilizes the E1, a changed square figure SAFER+. No down to earth direct assault has been accounted for.

V. CONCLUSION

M-Trade security is an exceptionally vital issue that needs further research to present productive and viable arrangements. In this article, different security concerns were explained. ECC positively seems to give a suitable distinct option for RSA. There are potential preferences, particularly when utilized as a part of gadgets with constrained preparing ability and memory. Run of the mill applications incorporate M-Business utilizing handheld remote gadgets. There are, in any case, a few issues and issues that are restraining the across the board appropriation of EEC. These incorporate (i) the genuine security of such frameworks is still not surely knew, (ii) trouble of producing suitable bends, and (iii) moderately moderate mark confirmation. Time will tell its future.

ACKNOWLEDGMENT

We would like to thank to all the faculty members of department of computer science and my friends for their good wishes, their helping hand and constructive criticism which led the successful completion of this paper.
We thank all those who directly and indirectly helped us in this regard.

REFERENCES

[1]. A. Fouratiet al [2002]: A SET Based Approach to Secure the Payment in Mobile Commerce. In Proceedings of 27th Annual IEEE Conference on Local Computer Networks (LCN'02), Tampa, Florida
[2]. Anurag Kumar jain et al. [2012]: Addressing Security and Privacy Risks Mobile applications. IEEE Computer society.
[3]. ArunKumar Gangula et al. [2013]: Survey on Mobile Computing Security. IEEE Computer Society.
[4]. Ashok K Talukder ET AL. [2005]: Mobile Computing. TaTa McGraw Hill Education, January.
[5]. B. S. Yee [1994]: Using Secure Coprocessor, PhD thesis, Carnegie Mellon University.
[6]. Bernaard menezes [2015]: Network security and cryptography. CENGAGE Learning,second edition.
[7]. C. Boyd et al. [2001]: Curve Based Password Authenticated Key Exchange Protocols. LNCS Vol. 2119, pp. 487-501.
[8]. C. Boyd et al. [2001]: Elliptic Curve Based Password Authenticated Key Exchange Protocols. LNCS Vol. 2119, pp. 487-501.

[9]. CUI Jian-qi et al.[2007]: New secure mobile Electronic commerce solution based on WA. Application Research of Computers Vol.24
[10]. Dharma prakash agrawal et al. [2015]: Introduction to Wireless and Mobile Systems. Third Edition, Cengage Learning USA.
[11]. Feng Tian et al. [2009]: Application and Research of Mobile E-commerce security based on WPKI. IEEE International Conference on Information Assurance and Security.