E-ISSN: 2278–179X

JECET; June-August, 2012; Vol.1.No.2, 101-117

Journal of Environmental Science, Computer Science and Engineering & Technology

Available online at www.jecet.org

Computer Science

Research Article

Future Trends in Mobile Commerce: Service Offerings, Technological Advances and Security Challenges

Dr. Manish Shrimali

Department of Computer Science & Information Technology,
Janardan Rai Nagar Rajasthan Vidyapeeth (Deemed) University, Udaipur (Raj) India

Received: 21 May 2012**; Revised:** 9 June 2012**; Accepted:** 14 June 2012

Abstract: Driven by the ubiquitous deployment of mobile systems, the widespread use of the Internet, the rapid advances in wireless technologies, the insatiable demand for high-speed interactive multimedia services, and the growing need for secure wireless machine-to-machine communications, mobile commerce is rapidly approaching the business forefront. In this paper, future trends in major aspects of mobile commerce are discussed. In light of the fact that the highly-personalized, context-aware, location-sensitive, time-critical, pin-point information presentation forms the basis upon which promising applications can be built, mobile commerce services are presented. In order to provide a multitude of attractive applications and ensure their success in future, a plethora of enabling technology is identified. Finally, privacy concerns, rust issues, and security challenges in wireless arena are discussed.

KEYWORDS: Mobile commerce, m-commerce services, privacy, security, trust, wireless technologies, mcommerce.

INTRODUCTION

Mobile commerce - the conduct of business transactions over the Internet-enabled wireless devices - is slowly becoming a dominant force in business and society. The push for advancing technology and the pull of public demand for low-cost, high-speed communications and ubiquitous access to information anytime anywhere have revolutionized the telecommunications industry over the past two decades. More recently, Internet access and high computing power in wireless devices began to pave the way for the introduction of broadband interactive multimedia applications. Nevertheless, the wireless Web market is

still in its infancy, and mobile commerce (m-commerce) is expected to evolve significantly in the future, especially in view of the current implementation of 3G systems and the future deployment of 4G systems, inter-connecting a multitude of diverse wireless networks, such as WBAN, WPAN, WLAN, and WMAN.

As wireless evolves from a secondary means of communication to a principal means of communication, it leads to the grayling of lines between personal interactions and business transactions. Although the growth and pervasiveness of this continuing wireless revolution appears to be inevitable, the path and speed of growth of this technology are not so predictable. It is clear that different generations of mobile communication systems have evolved to satisfy the demands of high data rate, high mobility, wide area coverage, diverse applications, high spectral efficiency, high flexibility of mobile devices and networks, and low costs. In view of this backdrop, it is anticipated that mcommerce will become widely popular and ubiquitously available. In this paper, future trends in m-commerce services and technologies, as well as privacy concerns and security challenges will be highlighted.

2. WIRELESS USER EQUIPMENT AND SYSTEMS

Today's communication-centric and computing-centric devices are becoming a single intelligent wireless device. The future user wireless devices, dubbed as universal wireless handheld devices, will have numerous functionalities, all aiming to establish communications, enhance education, furnish entertainment, provide information, and conduct
Transactions for mobile users. To this end, engineering design trade-offs will be required to form the right balance between device's capabilities and their constraints, With low-power requirements and long-lasting batteries, the universal wireless handheld devices will be small, low-cost, light-weight, easy-to-use, and IC-card-reader equipped. They will all have high-speed, always-on, packet-switched bandwidth-on-demand access capabilities to the Internet another networks, as well as to other wireless devices and equipment, anytime anywhere.

While connected, they will function as virtual keys, secure ID cards, digital cash, tagreaders, remote control devices, pagers, locating devices, and phones, and will also get e-books, e-newspapers, e-mails, voice-mails, and video-mails. Although use of data, and, in general, multimedia continue to accelerate exponentially, voice will remain a dominant mode of communications while the user is on the move, for talking or listening provides hands-free and eye-free operations and is also several times faster than typing or reading text messages. However, to convey the same information, a number of I/O enabling technologies will have to be incorporated in the wireless devices.

These technologies may include:

(I). **Speech recognition** (converting spoken words to text),

(II). **Speech synthesis** (converting e-mails to intelligible speech),

(III).**Voice activation** (bringing voice-control to navigate the Web sites and to replace a long series of sequential inputs in an automated voice-menu-driven phone system), and

(IV). **Optical character recognition** (converting hand-written text to typed-written format).

To achieve such, the user's device should be multi-band, multi-mode, multi-functional, and multi-standard to accommodate in transparent fashion all types of wireless systems. These wireless systems may include analogy cellular systems (1G:AMPS), digital cellular systems (2G: IS-54/-136, IS-95,GSM, DCS-1800, PDC; 2.5G: HSCSD, GPRS, CDMA2000-1X; 3G: EDGE, CDMA2000-1XV, WCDMA, TD-CDMA),digital cordless phones (DECT, Home RF), wireless PBXs, wireless LANs (IEEE 802.11 family, European Hiper LAN),WPANs (Bluetooth, Infrared, Ultra-Wideband), WMANs(WiMax, LMDS, MMDS, FSO), and mobile (L-band/S-band)satellite and GPS systems. Accordingly, diverse radio interfaces are required, which may be met by the implementation of radio-defined software technologies.

3G systems, which are now being deployed, need smaller cells, resulting in more base stations and higher systems costs. These characteristics are primarily due to their operating frequency, modulation and power management requirements. It may, therefore, not be very economical to install 3G systems in large rural areas. Thus, 2G systems and even 1G analogy system will continue to exist, especially in remote and isolated regions. The primary contributions to 3Gdevice's higher costs are flash memory, RAM, miscellaneous communications-related functionalities, as well as radiofrequency and baseband chips. 3G systems promise transmission speeds of up to 2 Mbps in stationary applications, 384 Kbps for slow-moving users, and 128 Kbps for users in fast-moving vehicles.

Unlike for 2G systems, for3G systems, authentication is mutual (i.e., the wireless device also authenticates the network), and the encryption is mandatory-unless the device and network both agree on anunciphered connection .In the future, 4G systems will focus on seamlessly integrating all wireless networks, and they will be the platform for mobile systems. This focus contrasts with 3Gsystems, which merely focus on developing new standards and hardware. 4G systems will be all IP-based multimedia services in heterogeneous networks that allow users to use any system at anytime anywhere. The new challenge facing the mobile industry is to minimize the fragmentation of the market and to enable seamless interoperability so as to simulate the growth of mobile services. 4G devices should be multi-band, multi-functional, and multi-mode capable and be able to handle various contents.

The primary 4G systems objectives over 3G systems objectives:

(i).Higher transmission rate (by two orders of magnitude),

(ii).Larger capacity (by one order of magnitude),

(iii).Higher frequency band (beyond 3 GHz),

(iv).Single-device (ubiquitous, multi-functional, multi-service, multi-band),

(v).Increased coverage (global roaming),

(vi).Simple billing (one bill with reduced total access cost),

(vii).High quality of service (accommodating varying transmission rates, channel characteristics, bandwidth allocation, fault-tolerance levels, and different hand-off support), and

(viii).Lower system costs (one order of magnitude).

will directly play pivotal roles in all aspects of the next generation of m-commerce.

3. M-COMMERCE SERVICES, PAYMENT, AND VALUE CHAIN

There appears to be no m-commerce application that cans be qualified as a "killer" application. However, the key advantage of m-commerce is its ability to support a wide variety of attractive and innovative applications, and that will be the "killer" characteristic of m-commerce. It is worth highlighting that the highly-personalized, context-aware, location-sensitive, time-critical applications, conducted in aver secure environment are the most promising commerce applications. There are indications that the next generation of wireless communications services based on 4Gsystems will not be limited to human but rather to anything that very small wireless chips can be attached to (i.e., machine-to-machine communications). However, the cellular phone market, when measured in terms of the number of wireless devices, is becoming saturated at a rather rapid pace. In short, there cane no significant increase in traffic merely through voice telephony. In view of this limitation, there appear to be two viable strategies to achieve growth in mobile communications:

(i) ***Implementation of new mobile services with an array of diverse multimedia applications***, and

(ii) ***The introduction of new wireless devices with enhanced features, including direct device-to-device communications capabilities.***

The ubiquitous wireless devices with various radio interfaces possess capabilities to connect to a multitude of heterogeneous networks, including the Internet, PSTN, ISDN, and WLAN. They can also allow communications directly with other wireless devices, such as tether less machine-to-machine communications. Both of these developments can lead to a great increase in the volume of user traffic, thus increasing the average revenue per user, a key metric for measuring the profitability of mobile-based businesses. Future mobile systems will introduce various quality-of-service (QoS) levels in order to provide various types of best effort multimedia services corresponding to user's demand. QoS may include priority, reliability, bit error rate, security, and delay, jitter, and throughput measures. The conversational services, with their real-time voice/video, connection or tented applications, are

characterized by a low fixed delay of about 20 - 30 milliseconds, a modest bit error rate of about1E-03 to 1E-05, and a low-blocking probability for network access.

On the other hand, transactional, retrieval, messaging, and distribution (e.g., multicasting) services, with their non real-time connectionless applications, are characterized by varying delay of 150 milliseconds or more, a low bit error rate of 1E-05 to 1E-07 to aim high data integrity, and a lowdelayprobability for network access . It is worth noting that the effective user transmission rate (i.e., throughput) which can characterize, to a large extent, the set of commerce applications available to the user is a function of the cell size and the speed of the mobile user. Every generation of mobile services (e.g., 2G, 3G, and 4G) brings about more efficient spectrum utilization; that is, more users per unit spectrum per unit area (bits

per second per Hzper square kilometres). Spectral efficiency measures the ability of a wireless system to deliver information or billable services. There are many factors which can contribute to the3spectral efficiency of a system, including modulation format, channel coding technique, air interface overhead, multiple access method, and acceptable interference level, to name a few. There are many factors shaping mobile billing, in general, and m-commerce payment, in particular.

A major determining factor for the success of m-commerce is service affordability-such as low access, subscription, and usage fees. Also, mobile payments, which are virtual payments, can be divided intomacro-payments, typically a payment of $10 or more-and micro-payments typically a payment of $10 or less. For a macro-payment, authentication through a trusted financial institution is required, which must be carried out over the public wireless access and wired-line backbone net works, while invoking all possible security measures. On the other hand, a micro-payment may use the operator's infra structure or involve a cash card (in addition to the ID card which stores the confidential information, such as the user's secret authentication key) and proximity payments through short distances by using Bluetooth, Infra-Red, RFID, and UWB technologies. In the selection phase, the customer indicates what goods and services are desired, and he/she negotiates the price of the goods and services and the terms of conditions. The transaction details highlight the description of goods or services, the customer's name, and other required details. The customer then responds with transaction credentials (which may contain the payment credentials), the transaction details, and some authentication of the customer.

Upon authentication, the payment is approved, the funds are transferred, and the goods will be delivered, or services will be provided. In mobile payment, although confidentiality (making sure information is not visible to eavesdroppers), integrity (finding out the content has not been tampered with), and no repudiation (proving the transaction has taken place) are primary concerns, authentication (ensuring communicating parties are certain of each other's identity) is of paramount importance. As a result, public key cryptography, which is slower but more powerful than symmetric key cryptography, will be used for authentication and the exchange of symmetric session keys. In order to prevent a false (cracker's) public key as a legitimate public key, a certificate authority issues a public key certificate that would contain the name, the public key, and the expiration date. In view of the fact that the emerging wireless devices will have more throughputs, processing power, and memory, more complex encryption techniques-such as longer keys and/or more sophisticated multi-level algorithms-will be employed to enhance mobile payment security .

Although encryption can be the most effective tool for privacy and security, it is generally used only as a security measure when mcommercetransactions are conducted and not when essential data are generally stored in databases. The development environment for m-commerce insignificantly more complex than e-commerce, thus requiring broader base of expertise. In m-commerce, it is virtually impossible to achieve all technical and business requirements simultaneously, for some are clearly in conflict with others. Moreover, there are constraints associated with business and regulatory environments that can influence some of these requirements, such as service coverage, location determination, backward compatibility, and privacy concerns, to name a few.

The m-commerce applications can be successfully provided to mobile users only when a number of enterprises, called them-commerce value chain, are complementarily involved in the creation and delivery of these services, with the goal of sharing revenue. In order to drive interoperability of mobile data services, the world's mobile operators, device and network suppliers, information and communication technology companies, application developers and content providers have joined forces to ensure seamless mobile services for end-users anywhere. This outcome will be achieved by defining industry-wide requirements, architectural frameworks, and industry specifications for enabling technologies and end-to-end interoperability, all based on open specifications of standards, protocols, and interfaces. The federal government also plays a pivotal role, not only in terms of setting policies and ensuring that regulatory issues are fully respected, but in terms of auctioning spectrum (instead of comparative bidding and lottery as licensing methods). This role, in turn, can lead to huge investment requirements, which need to be met by some major players. M-commerce services with compelling contents are provided by tight business and strategic partnership arrangements and by involving a large number of companies, with each influencing other parties in the value chain.

4. M-COMMERCE ENABLING TECHNOLOGIES

Providing mobile users with wireless communications functions for their communications, information, education, entertainment, and business needs, as well as giving wireless communications functions to stationary places for access and security and to moving objects for asset and logistic purposes form the cornerstones of mobile commerce. To achieve these

Goals, significant technological advances in a number of enabling technology are anticipated.

- ***Radio frequency identification (RFID)*** is a generic term for technologies that use radio waves to automatically identify individual items or some of their attributes. RFID possesses several benefits over bar codes:

  First, it does not need to meet line-of-sight requirements as long as the RFID tags are within the range of a reader.

  Second, quite much number of RFID tags can be read simultaneously.

  Third, every unique item can have its own RFID tags.

  The mobile consumer will use RFID readers in their mobile phones to scan RFID tags, say in the packaging of products on store shelves, to pay for tolls and access fees, to purchase at vending

machines and points of sales, to access secure rooms, buildings, and other partitioned areas, and to control home and office appliances. With RFID, a scanner can read the encoded information even when the tag is concealed. For example, it may be embedded in a product's casing, or sewn into an item of clothing, or sandwiched between a banknote's layered papers. The stealthy nature of RFID technology has raised concerns among privacy advocates that RFID tags could be tracked beyond their intended use. For example, security agencies might use them to covertly monitor individuals or their belongings. Lower frequencies (LF and MF) usually are cheaper, use less power, are better able to penetrate non-metallic substances, and are ideal for scanning objects with high-water content. On the other hand, higher frequencies (HF and UHF) typically offer a better range and can transfer data faster; they tend to be more directed and, thus, require a clearer path. Active tags can have a farther read range than passive tags, but passive tags are less expensive and require no maintenance.

- ***Location determination***s seen to be an indispensable feature for mobile commerce. Network-based positioning is carried out by terrestrial systems through various techniques, such as cell of origin, time of arrival, angle of arrival, and enhanced observed time difference. The device-based positioning is carried out by satellite systems typically using three or four MEO satellites, also known as GPS. However, a hybrid approach delivering the accuracy of device-centric option, while avoiding a line-of-sight requirement as well as increased cost, size, and power consumption, is also used. Though FCC does not require the mobile network operators to use a specific technology, it has indicated specific performance metrics for location-enabled technology. For network-based technology, location information accuracy is required to be within 100 meters 67% of the time and within300 meters 95% of the time. But for the device-centric technology, these distances must be halved. In view of possible launches of LEO satellites and the significant increase in the processing capabilities of the wireless devices, as well as the fact that the cell sizes are shrinking from macro to micro to pico, the location-based technologies are expected to become more accurate and less costly in the future.

- ***Software defined radio (SDR)*** enables reconfigurable system architectures for wireless networks and user devices. To provide users with m-commerce services under an array of heterogeneous networks, certain design problems (such as limitations in device size, cost, power consumption, and backward compatibilities to systems) must all be overcome. The most viable way of implementing these types of wireless devices is to adopt a software radio approach. The received analogy signal is processed by a reprogrammable baseband digital signal processor in accordance with the wireless environment. However, certain problems then need to bead dressed-such as an analogy radio interface with multiple antennas and amplifiers and very fast high-speed analogy-to-digital conversions and DSP functions-which can all, intern, add to the circuit complexity and high-power consumption and dissipation. SDR can provide the user with a single piece of scalable hardware that is at once compatible at a global scale.

- ***Adaptive modulation and coding (AMC)***is one of the most viable and effective means to dynamically combat wireless channel degradation and meet performance requirements. In AMC,

for the same symbol rate (i.e., occupied bandwidth),the signal power, the modulation technique, the information rate, and the channel-coding rate, can all be adjusted in accordance with instantaneous variations in channel conditions (such as multi-path and proximity to the base station) and quality of service requirements. Forward-error-correcting(FEC) codes (whose rates may range from 1/2 to5/6) and digital modulation techniques (ranging from QPSK to 64 QAM) will be dynamically adapted for every single5individual, giving rise to up to a six-fold spectral efficiency(bits per second per Hz).

- ***Digital signal compression*, also known as source coding**, is employed to reduce the bit rate requirements (bandwidth demands). It is widely applied to all sources of modality. Both proprietary and standard techniques are widely available and are constantly being improved upon. Texts, software, and faxes generally employ lossless compression techniques, such as the Lempel-Ziv and Huffman codes. On the other hand, MPEG video, JPEG image, and MP3 audio coding standards employ lossy compression, where known limitations of the human visual and audio systems are exploited to introduce losses but in a controlled manner. With advances in compression, a wider array of feature-rich m-commerce applications and/or lower service costs can be provided.

- ***Biometrics*** as an essential security measure will play an imperative role in the next-generation m-commerce services. Traditionally, most security systems authenticate the user based on something that he/she knows, such as a password. However, where security really matters, it makes sense to adda second layer, which could be something that he/she has (e.g., a smartcard). Also, as a third option, and probably the most authentic method, could be something that he/she is, something that, at least theoretically, would be virtually impossible to forge. Biometric control measuring physical characteristics and behavioural patterns will be widely employed to allow the user to access his/her own wireless device, to enable the user to access certain places, and to allow the user to monitor assets. Of course, depending on their effectiveness, cost, intrusiveness, and accuracy, more than one biometric controls may be simultaneously employed. Biometric control may include finger imaging, palm print, hand geometry, iris and retina vascular pattern, facial recognition and thermograph, signature and handwriting, key stroke dynamics, and voice recognition and speech patterns.

- ***WAP (*Wireless Application Protocols)** appears to be the key to future IP-based m-commerce applications. WAP, an industry-initiated world standard, has emerged as a common communications technology and uniform interface standard for presenting and delivering wireless services on wireless devices. WAP specifications include a micro-browser, access functions, and layered communication specifications for sessions, transport, and security. The WAP gateway is used to translate the WAP protocols (protocols that have been optimized for low bandwidth, low power consumption, limited screen size, and low storage) into the traditional Internet protocols (TCP/IP). These specifications enable bearer-independent and interoperable applications. In short, future trends clearly indicate that the device manufacturers, as well as service and infrastructure providers, will keep adopting the WAP standard.

- ***IPv6,* the Internet Protocol version 6,** is a permanent solution to the address shortage and uses a 128-bit address, split into 16 bytes, vis-à-vis IPv4's 32-bit address. WithIPv6, there will always be enough IP addresses for all mobile devices and moving tags. IPv6 is a feature-rich standard, including built-in-security by supporting IPSec to promote interoperability between different IPv6 implementations.IPv6 also allows for better support for quality of service through traffic identification. Mobile IPv6 is a standardize dip-based mobility protocol for IPv6 wireless systems. In this design, each device has an IPv6 home address. Whenever the device moves outside the local network, the home address becomes invalid; therefore, the device obtains a new IPv6address (called a care-of-address) in the visited network. This hand-off process causes an increase in the system load, high handover latency, and packet losses. Because 3G systems work with IPv6, it is anticipated that 4G systems will work with IPv6 as well.

- ***Mobile ad hoc networks,*** vis-à-vis fixed topology wireless networks, may be characterized by wireless nodes, the lack of fixed infrastructure support, dynamic topologies, band width constrained variable-capacity links, energy-constrained operations, and limited physical security. In such peer-to-peer networks, end-user wireless handsets also act as secure wireless routers that are part of the overall network infrastructure. Upstream and downstream transmissions hop through subscriber handsets and fixed wireless routers to reach the destination. Routing for the best path is defined for the least power. Mobile ad hoc networks will help a community of subscribers to increase dramatically spectrum reuse and reduce overall power consumption. Mobile adjacent works bring about a host of challenges and opportunities, but due to emerging wireless device-to-device connectivity requirements, mobile ad hoc networks will prove to be anever-essential component.

- ***MIMO,* multiple-input multiple-output**, can significantly increase system capacity, range, and reliability. The wireless broadband channel is a non-line-of-sight channel and includes impairments, such as time-selective and frequency-selective fading. To circumvent these problems, MIMO exploits propagation environment characteristics by employing multiple antennas at the transmitter and receiver to create spatial channels, for it is not very likely that all the channels will fade simultaneously. The space diversity, enabled by smart antennas using phased array and digital beam forming techniques, combines multiple antenna elements with digital signal processing to optimize the irradiation/reception pattern. It is anticipated that MIMO, in combination with other advanced techniques such as OFDM and CDMA will be heavily utilized for 4G systems to enhance the system capacity and performance.

- ***OFDM,* orthogonal frequency division multiplexing,** is selected over a single-carrier solution due to lower6complexity of equalizers for high data rates. Multiple narrowband carriers (tones), which are orthogonal to one another, are more robust to multipath. With proper coding and interleaving across frequencies, multipath turns into an OFDM system advantage by yielding frequency diversity. In addition to MIMO's space diversity and OFDM's frequency diversity, site diversity for base stations and time diversity forenoon-time-sensitive applications will also be employed to improve the system capacity and performance.

- ***CDMA*, code division multiple access,** is the access scheme for 3G systems, and it will almost certainly be for future 4Gsystems, for it can significantly enhance capacity through effective use of orthogonal codes. The primary advantage of CDMA is its ability to reject interference whether it is the unintentional interference by another user simultaneously attempting to transmit through the
- channel or the intentional interference by a hostile transmitter attempting to jam the transmission. CDMA, as opposed to FDMA and TDMA, can allow an increase in system capacity at the expense of a modest and gradual degradation in performance. It is worth noting that combining multi-carrier OFDM transmissions with CDMA gives rise to exploiting the wideband channel's inherent frequency diversity by spreading each symbol across multiple subcarriers.
- ***Turbo codes*-** demonstrated experimentally and by simulation but not yet proven theoretically-are capable of approaching the Shannon theoretical limit of channel capacity in a computationally feasible manner. This capability is in contrast to the traditional FEC codes where to significantly improve the FEC performance, its code-word length of linear block code or the constraint length of a convolutionalcode must be increased significantly, which in turn, causes the computational complexity of a maximum likelihood decoder to increase exponentially. The error performance of the Turbo code decoder significantly improves with the number of iterations of the soft-input-soft-output decoding algorithm, but at the expense of additional computational complexity and decoding delay. Turbo code's performances can be impacted by interleaving type and length, number of iterations, code rate, type (block or convolution) and structure (series or parallel). Even a small reduction in the link threshold can improve the system capacity and/or enhance the link performance significantly.
- ***Data encryption*** is the best approach to handle security in the wireless and m-commerce arena. The primary goals are to provide an easy and inexpensive means of encryption to all authorized users possessing the appropriate key and to ensure the cracker's task of producing an estimate of the plaintext without the benefit of the key is made difficult and expensive.

Depending on the wireless device's constraints (such as limited processing power, memory and power) and mcommerce applications requirements in terms of delay and burstiness, secret key cryptography (symmetric key) based onmulti-layer algorithms, or public (asymmetric) key cryptography based on elliptic curve techniques, or a hybrid of both will have to be employed. In the absence of effective encryption, there can be no m-commerce applications.

5. PRIVACY, SECURITY, AND TRUST IN M-COMMERCE

The growth of the Internet and e-commerce has dramatically increased the amount of personal information that can be potentially collected about individuals by corporations and governments. Such data collections, along with usage tracking (click stream data) and the sharing of information with third parties are always invoking issues of privacy, especially in view of the fact that they can be easily done through high-speed links and high-capacity storage devices in a very accurate fashion, and most often without the consumer's or citizen's expressed knowledge or consent . This valuable information, often collected by hidden tools such as cookies and Web bugs can be shared with third parties for marketing

purposes and surveillance operations, and its perceived value has been occasionally behind the stock-market valuations of some companies. In fact, this detailed information can be combined with other off-line data such as demographic and psychographic data to predict a user's interests, needs, and possible future purchases.

To deal with the problem of profiling, trust seals and government regulations appear to be two forces pushing for more and better privacy disclosures on the Web. The former tend to promote privacy in the form of self-regulation, where they may eventually become more of a privacy advocate for corporations rather than for consumers. The latter can advance privacy through legislation but can also potentially create privacy worries for citizens by monitoring their telecommunications traffic. For instance, the FBI's powerfulDCS1000 Carnivore program is a computer-automated snooping tool that is capable of intercepting and sorting out millions of text messages, such as telephone conversations and e-mails passing through ISPs by monitoring incoming and outgoing messages to specific IP addresses. It is clear that governments' regulations and legislation can be as likely to thwart privacy as to enforce it. Even though wireless communications possess numerous merits, privacy is not one of them. M-commerce possesses, in addition to all privacy issues related to e-commerce, another major privacy threat: the sharing of knowledge about a user's location with others.

There are basically three solutions to this positioning problem:

(i). *The network-based solution*, where the calculations are carried out by the cellular network and the positioning information may then be passed to the user;

(ii). *The device-based solution*, where the wireless device computes its own position; and

(iii). *A hybrid solution*.

The pitfall associated with the network-based positioning is that the information about the user's whereabouts can be collected but not necessarily passed to the user. Instead, the information may be exploited by other entities, all without the user's knowledge, let alone his/her consent. Also, there are some privacy implications about the requirement that wireless devices need to be embedded with a location tracking technology to provide location-based services, For instance, if location records were kept over time, an in-depth profile could be compiled for other, perhaps unwarranted, purposes.

Many countries, such as Canada and those in the European Union, strictly regulate the collection and use of personal data by business corporations and government agencies. They

Have opted for regulated self-regulation. For instance, the privacy provisions of Canada's PIPEDA set out rules for the protection of personal information collected, used, or disclosed in all sectors of the economy, so as to strike pragmatic balance between privacy and economy. For instance, PIPEDA warrants all mobile service providers in Canada to take steps to ensure that:

(i).they is responsible for personal information under their control,

(ii).they obtain expressed consent before using or disclosing customers' location

Information,

(iii).they limit to the purpose identified for the collection of information, and

(iv).They protect with the necessary security to safeguard the personal information.

In contrast, the United States has chosen self-regulation as their basic strategy, based on the model of the well-informed, the rational and the self-protecting consumer. In this model, privacy may be considered to be a barrier for mcommerce, and accordingly a minimum level of protection into be desired. In any event, even if there were method to absolutely ensure privacy, service providers and customers may not embrace the technology quite as readily, because it may be inexpensive in practice and offer a lower quality of service. Since every cellular telephone is physical-locating device even when the user is not in a call, and there is no known way to avoid revealing the caller's location when a cell phone is in use, privacy about the mobile user's location can always be potentially compromised. With the apparent omnipresent availability of wireless devices, m-commerce services have a very promising prospect. However, the success of m-commerce depends much on the security of the underlying mobile technologies.

Wireless technology, by its nature, violates fundamental security principles. In short, wireless communications rely on open and public transmission media (i.e., over the air) that raise further security vulnerabilities, in addition to the security threats generally found in wired networks. For instance, the chargeback rate for credit card transactions on the Internet (that is for e-commerce) is about fifteen times more than that for point-of-sale credit card transactions; this, in turn, points to the fact that security will always be an indispensable factor in the success of m-commerce.

The mcommerce security challenges relate to the user's mobile device, the wireless access network, the wired-line backbone network, and m-commerce applications. Security threats in m-commerce may be passive (such as information monitoring and release for fraudulent purposes) or active (such as the modification of information through denial-of-service and unauthorized access). Unlike the wire-line networks, the unique characteristics of wireless networks pose a number of non-trivial challenges to security design, such as vulnerability of the air interface, an open peer-to-peer network architecture (in mobile ad hoc networks), a shared wireless medium, the limited computing power of mobile devices, a highly dynamic network topology, and the low data rates and frequent "disconnects" of wireless communications.

There are basically two approaches to the challenges to wireless security: being proactive and being reactive. The proactive approach attempts *a priori* to prevent a cracker from launching attacks in the first place, typically through various cryptographic techniques. In contrast, the reactive approach seeks to detect security threats *a posterior* and to react accordingly. Due to the absence of a clear line of defence, a complete security solution should integrate both approaches. Because security is a chain, it is only as secure as the weakest link. A failed link may significantly degrade the strength of the overall security solutions. Enhanced security features require additional overhead (increased bandwidth), increased complexity (additional cost), and processing delay (degraded performance), which, in turn, can adversely impact network performance.

Mobile services are prone to two types of fraud risks: subscription fraud and device theft. Subscription fraud (also known as identity theft) is the same problem that issuer's of credit cards have when someone pretends to be another subscriber. As with other forms of credit-related identity theft, the imposter fails to pay the bills and the service is eventually cut off. Although the customer wills not be responsible for paying the imposter's bills, as he/she may have to take steps to clear his/her credit report. Device theft has become more attractive to thieves as the wireless devices become smaller and more powerful. The charges incurred by the thief appear on the legitimate consumer's monthly bill, and it's not certain that the service provider will remove these charges from the customer's account. Almost as soon as the stolen device is reported, the location technology can be employed to help track down the thief. Also, to combat theft, in addition to the usage of password, a device could be tailored to its owner, using effective, yet inexpensive, biometric control technologies. But it appears that most of the device manufacturers are not very keen to include these biometric technologies, for a more palatable option is to have their products stolen so their customers will have to replace them frequently. Significant portions of the land area do not have access to digital services, and will almost always be covered by analogy systems. Standard radio scanners can monitor analogy signals, but cannot decipher digital ones, unless law enforcement-grade scanners are employed.

The cloning (also known as service theft) of a cellular phone occurs when the electronic serial number(ESN) and the mobile identification number (MIN) of cellular phone are stolen by radio scanners sniffing the cellular frequency bands and reprogrammed into another cellular phone without the knowledge of the carrier or subscriber through the use of electronic scanning devices. After this process is completed, both phones (the legitimate and the cloned) are billed to the original, legitimate account. That problem has been reduced by almost two orders of magnitude through the application of digital technology, including advanced access schemes and compression techniques.

Means to detect cloned phones on the analogsystems are as follows:

(i).Duplicate detection (the network sees the same phone being used in two places at the Sometime and reacts by shutting them both off),

(ii).Velocity trap (the network notices that the phone seems to be moving at impossible or Most unlikely speeds),

(iii).Radio-frequency fingerprinting (the network spots the clones with the same identity But different RF fingerprints),

(iv).Usage profiling (customers' phone usage patterns are kept, and when discrepancies Are noticed, the customer is contacted),

(v).Call counting (both the phone and the network keep track of calls made with the Phone, and should they differ, service is denied), and

(vi).PIN codes (a user enters a PIN code to unlock and lock a cell phone).

There are wireless threats that are significantly more likely to occur in WLANs than in cellular networks, such as interception (passive eavesdropping), man-in-the-middle attack (active eavesdropping), and denial-of-service (jamming). Interception occurs when the signal is transmitted over a radio path (which is an open, uncontrolled medium) and compatible receivers, equipped with mobile scanners, can listen to the message. The sender and the intended receiver of the message may not even be aware of the intrusion. Interception is used to gather information on the network under attack, such as who uses the network, what is accessible, and what the coverage area is.

A man-in-the middle attack aims to subvert the confidentiality and integrity of the session. Here, attacker impersonates a network resource to sniff the traffic of another wireless client by sending unsolicited signals to target stations. The target stations will send all traffic to the attacker instead of the intended destination, and the attacker is now in a position to modify communications. In the default mode, WLANs do not provide any security.

In order to provide a certain level of security, the IEEE-defined Wired Equivalent Privacy (WEP) was designed to provide security. However, it is now clear that WEP authentication is completely insecure; an attacker can intercept an authentication exchange without knowing the secret keys. In fact, if many frames are intercepted, the WEP keys can be recovered using statistical analysis. There is another limitation. Due to the fact that all participants must have the same key, public portals (e.g., hotels, airport) provide no security. In response to the deficiencies in WEP standards, the emerging IEEE 802.11istandards have been introduced to improve the WLAN security problems and to turn wireless networking into at rusted medium for all wireless users.

Denial-of-services is caused when the entire network is jammed. The jamming attack could be against the client's wireless device or against the network's access point. The reliability and security of the technology is an essential trust-related characteristic of online interaction, where certain vulnerabilities are unknown, even to the most knowledgeable consumers. It is obvious that wireless communications, in general, cannot be as reliable as wired communications. Thus, the occurrence of a technical or technological failure is more likely for m-commerce as for e-commerce, and that can, in turn, further diminish the level of trust.

For instance, dropped calls (a carrier fails to hand off a call in progress),busy signals (too many customers in a cell call at the sometime), and dead spots (an area where the signal between the handset and the cell tower is blocked) can all impact the wireless service performance, thus potentially adversely impacting on the level of trust in m-commerce. The emerging advances in m-commerce-whether they be through telecommunications technologies to help realize higher rates, wider coverage, and higher quality of service, or through business frameworks to cultivate measures such as informed consent, minimum-risk insurance, Website quality, information clarity, company competence and integrity, and public and private policies-will all help build trust in mcommerce. The mass adoption of m-commerce will be realized after wireless users (potential customers) trust mobile services. The level of energy emitted by WLAN and WPAN devices is much less than the electromagnetic energy emitted by mobile phones. The

scientific consensus is that the radiation from mobile phones is harmful, but the dosage is so low at any given time that most people will suffer no apparent medical problems. However, the impact of their use for very many years is not known at the present time, and their long-term effects could remain unknown for a generation. In m-commerce, as opposed to mere wireless voice communications, the device is generally in front of the user (i.e., the device is not next to the user's ear).Noting that the signal power is attenuated by the square of distance, health hazard for m-commerce applications, where they are generally more visually-based than audio-based, will be even less serious than mobile phone calls. In fact, for mobile phone calls, well-designed hands-free headsets could prove to be quite safe, especially if a very low-power wireless technology, such as Bluetooth, is employed to provide a link between the device and headset. The issue of health and safety in wireless devices either as legally imposed by the governments' regulations or as apparently complied by the manufacturer's raises the issue of trust. In principle, the strong majority of people accept the safety guidelines, health recommendations, and regulatory standards issued by governments and what the manufacturers claim to respect.

6. CONCLUSION

The major limitations of m-commerce, as viewed today, are small screens on wireless devices, limited processing power, modest memory, restricted power consumption, poor voice quality, low-speed data transmission, non-ubiquitous coverage, unproven security, scarce bandwidth, and possible health hazards. In view of the fact that mobile computing is accelerating at a rate faster than Moore's law, and according to Edom's law of bandwidth , wireless transmission rates also follow Moore's law, many of these limitations are expected to diminish, if not being eliminated, over time. In light of the fact that m-commerce is just at its inception, the real potential has yet to be visualized, let alone tapped. Noting that the highly-personalized, context-aware, location sensitive, time-critical applications are the most promising applications in m-commerce, there are many m-commerce applications envisaged to become very widely popular. They include: i) digital cash (to enable mobile users to settle transactions requiring micro-payments), ii) human-to-machine communications (to facilitate mobile users to communicate to stationary locations for access and security and to moving objects for asset and logistic purposes using FID technologies), iii) telemetry (to activate remote recording devices for sensing and measurement information), and iv) broadband-interactive multimedia communications and messaging anytime, anywhere.

4G systems with more security, higher speeds, higher capacity, lower costs, and more intelligent infrastructures and devices will help realize m-commerce applications. With improved wireless security and privacy through data encryption and user education, on the one hand, and with the wide deployment of 4G systems, on the other hand, it is anticipated that m-commerce will, inescapably, become the most dominant method of conducting business transactions.

7. APPENDIX: LIST OF SELECT ACRONYMS

CDMA: Code Division Multiple Access;

FCC: Federal Communications Commission;

GPS: Global Positioning System;

GSM: Global Systems for Mobile communications;

ISDN: Integrated Services Digital Network;

ISP: Internet Service Provider;

ITU: International telecommunications Union;

MIMO: Multiple Input Multiple Output;

MMS: Multimedia Messaging Services;

OFDM: Orthogonal Frequency Division Multiplexing;

PIPEDA: Personal Information Protection &Electronics Document Act;

PSTN: Packet-Switched Telephone Network;

RFID: Radio Frequency Identification;

SDR: Software Define Radio;

SMS: Short Messaging Services;

UWB: Ultra Wide-Band;

WAP: Wireless Application Protocols;

WBAN: Wireless Body Area Network;

WEP: Wired Equivalent Privacy;

WLAN: Wireless Local Area Network;

WPAN: Wireless Personal Area Network;

WMAN: Wireless Metropolitan Network

WRC: World Radio Conference

8. REFERENCES

[1]. ITU, *World Telecommunications Development Report*, 2003

[2]. Merrill Lynch, *Wireless Matrix*, 3Q03.

[3]. A. Mehrotra, *Cellular Radio: Analog and Digital Systems*, Artech House, 1994.

[4]. www.umts-forum.org

[5]. www.docomo.com

[6]. N. J. Muller, *Wireless A to Z*, McGraw-Hill, 2003.

[7]. B. G. Evans and K. Baughan, "Visions of 4G,"*Electronics and Communication Engineering Journal*,2000,pp. 293-303,.

*__Correspondence Author: Dr. Manish Shrimali ;(Associate Professor);__ Department of Computer Science & Information Technology; Janardan Rai Nagar Rajasthan Vidyapeeth (Deemed) University; *Udaipur (Rajasthan – 313001), INDIA;* E-mail: manishshrimali2009@gmail.com,