(IJISE) 2016, Vol. No. 4, Jul-Dec **e-ISSN: 2454-6402, p-ISSN: 2454-812X**

SECURITY ISSUES AND CHALLENGES IN MOBILE COMPUTING AND M-COMMERCE

Kamatchi K[1], Dr. Anu Bharti[2]

[1] *Research Scholar, Department of Computer Science & Engineering, Sunrise University, Alwar*

[2] *Asso. Prof., Dept of Computer Science & Engineering, Sunrise University, Alwar*

ABSTRACT

Mobile computing and Mobile Commerce is most popular now a days because of the service offered during the mobility. Mobile computing has become the reality today rather than the luxury. Mobile wireless market is increasing by leaps and bounds. The quality and speeds available in the mobile environment must match the fixed networks if the convergence of the mobile wireless and fixed communication network is to happen in the real sense. The challenge for mobile network lies in providing very large footprint of mobile services with high speed and security. Online transactions using mobile devices must ensure high security for user credentials and it should not be possible for misuse. M-Commerce is the electronic commerce performed using mobile devices. Since user credentials to be kept secret, a high level of security should be ensured.

KEYWORDS: *PKI, WPKI, Certificates, M-Commerce.*

1. INTRODUCTION

Mobile computing provides flexibility of computing environment over physical mobility. The user of a mobile computing environment will be able to access to data, information or other logical objects from any device in any network while on the move. To make the mobile computing environment ubiquitous, it is necessary that the communication bearer is spread over both wired and wireless media.

The emerging mobile industry expected to be characterized by increasingly personalized and location based services. The availability of user preferred information despite of location made mobile computing successful. The advancement of mobile technology has revolutionized the way people use mobile devices in their day to day activity [1].

Mobile computing offers a computing environment over physical mobility. The user of a mobile computing environment will be able to access to data, information or other logical objects from any device in any network while on the move. To make the mobile computing

environment ubiquitous, it is necessary that the communication bearer is spread over both wired and wireless media [2].

Mobile System Infrastructure

The mobile system infrastructure provides the necessary services needed for the proper functioning of the entities involved in a mobile system, architecture. One of the most widely deployed cellular infrastructures is GSMor2G and its designers had several goals. Better quality for voice, higher speeds for data, international roaming, protection against charge fraud and eaves dropping. The UMTS or 3G promised advanced services such as mobile internet, multimedia messaging, video conferencing etc. UMTS standards were defined by an international consortium called 3GPP (Third generation partnership project) [3].

1.1.2 Fundamentals of a cellular system

The generic block diagram of a cellular system is shown in the Fig 1 below.

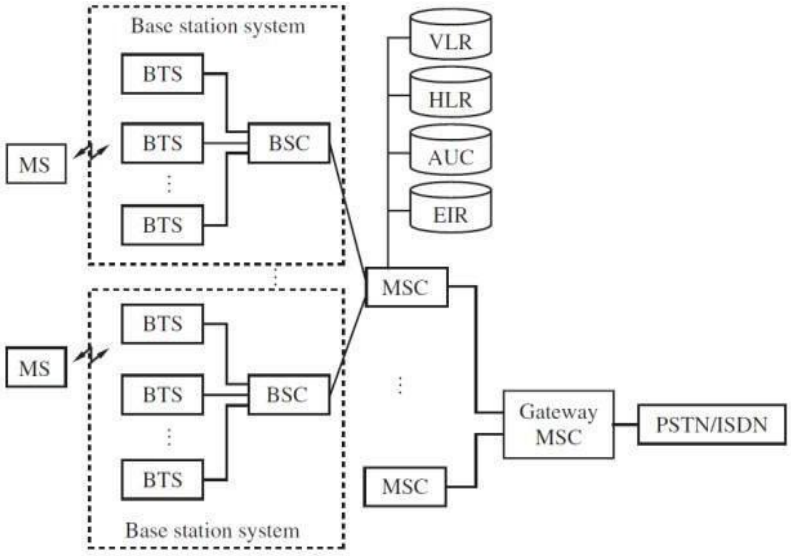

Fig 1: Cellular System

The basic geographical unit of a cellular system is called a cell is the geographical area covered by a transmitter. At the lowest level, a cell phone is connected to a base station (or base transceiver station) by a radio link. Multiple base stations are connected to and controlled by a

base station controller. The connection between a base station and its controllers could be a microwave link, optical link in general any radio link. Multiple base station controllers and upstream are connected to Mobile switching centre. The Mobile Switching Centre (MSC) forwards an incoming call to the destination MSC. The MSC also keeps track of accounting and billing information. MSC are connected each other through wired networks such as Public Switched Telephone Network (PSTN).

The user has a subscription to some networks called as his home network. A one to one association between MSC and a network is maintained. An MSC has a database, called the Home Location Register (HLR) having information of all its subscribers. The data base contains the information of subscriber's mobile number, the services availed and a secret key stored in the mobile known only to the HLR. HLR also maintains the dynamic information of its roaming customers for charging. It includes the current location of a user and the cellular network used by the user [4].

A subscriber may avail the services of other networks (called as foreign networks) that have an agreement for roaming with subscriber's home network. Each cellular network also maintains a database called as Visitor Location register (VLR) of users currently visiting that network with the list of services the subscriber entitled to 2G technology introduced Subscriber Identity Module (SIM) card which stores three secrets used for cryptographic operations[5]. The secrets are:

1. IMSI (International Mobile Subscriber Identity): A unique 15 digit subscriber identification number used to identify each registered users uniquely. It is stored in the SIM and has following three parts.

a. Mobile Country Code (MCC):Ithas3decimalplaces.

b. Mobile Network Code (MNC): It has 2 decimal places. These two fields uniquely identify a country and the operator.

c. Mobile Subscriber Identification Number (MSIN): It has a maximum of 10 decimal places and identifies the user in the home network.

2. A 128 bit subscriber authentication key known only to the SIM and HLR of the subscriber's home network.

3. A PIN known to the phones owner and used to unlock the SIM. It is used to prevent the misusing of the stolen phones.

2. SECURITY IN POPULAR MOBILE NETWORKS

Security in GSM

The two principal tasks involved for providing GSM Network security are:

a) Entity authentication and Key agreement
b) Message protection.

Entity Authentication and Key Agreement

Fig 2 illustrates authentication procedure involved in GSM. It has following steps.

1. Authorization request from Cell Phone:

During authorization request step, the cell phone sends the encryption algorithm can support to the base station and IMSI/TMSI number to the MSC. If the cell phone is away from its home network, the IMSI will be received by the MSC of the visited network. The latter communicates the IMSI to the MSC/HLR of the cell phones home network with a request to provide a challenge that will be used to authenticate by a cell phone.

2. Creation and transmission of authentication vectors:

The IMSI obtained by the MSC is used to index the home location registers to obtain a shared key, Ki known only to the SIM and HLR of the home network. The MSC/HLR generates 128 bit random number, RAND, which functions as a challenge in the challenge-response authentication protocol. The two quantities XRES and Kcare computed as below.

XRES=A3 (RAND, Ki) Kc=A8 (RAND, Ki)

Where, A3 and A8 are two keyed hash functions. XRES is the expected response in the challenge response authentication protocol. Kc is the encryption key. The HLR creates five authentication triplets, each seeded by freshly chosen random numbers. Each triplet is of the form-

<RAND, XRES, Kc>

The triplets are sent to the MSC of the home network by the HLR. If the cell phone is visiting a foreign network, the MSC forwards the triplets to the MSC of the visited network. Five triplets are sent so that four subsequent authentications may be performed without the need to repeatedly involve MSC/HLR of the home network.

The MSC sends the challenge (RAND) from the first triplet to the base station and it is forwarded to SIM on the cell phone.

3. Cell Phone response:

Once the SIM has received RAND, it computes SRES (Signed Response) similar to XRES. It can be computed by an entity with the knowledge of Ki, key shared between the SIM and HLR. The cell phone sends SRES to the base station and it is forwarded to MSC. The MSC compares if SRES is equal to XRES and if they are same MSC concludes that SIM knows Ki and identifies it as a genuine subscriber.

4. Computation/Receipt of encryption key:

The SIM computes Kc and MSC extracts Kc from its authentication triplet and communicates it to the base station. Further all communications between cell phone and base station are encrypted using Kc.

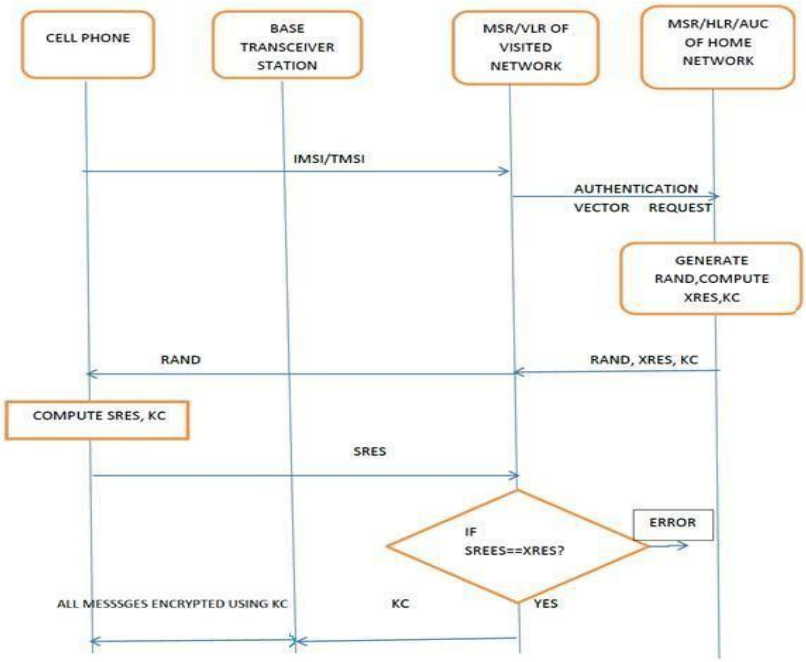

Fig 2: Authentication steps in GSM

Message Protection

Stream cipher technique is used to encrypt the message transmission between cell phone and base station. The key stream generator for this is denoted as A5. The key stream is a function of the 64 bit encryption key, Kc, and 22 bit frame number.
KEYSTREAM= A5 (Kc, FRAME_NUMBER)

For each frame transmitted, the frame number is incremented which changes the key stream for each frame sent during a call. Usually cipher text is generated by X-ORing the plain text and the key stream.

Computation of the key stream and encryption do not require any static information stored in the SIM. Computation of XRES and Kc requires the subscriber authentication key, Ki. Hence the functions A3 and A8 must be supported by the SIM and A5 typically not.

Problems and drawbacks

There are some security shortcomings identified in GSM. The first flaw is related to authentication of the subscriber as illustrated in the following Fig 3 .The system uses temporary identifier, Temporary Mobile Subscriber Identity (TMSI) to prevent the identity. If the VLR could not recognize or TMSI is lost, the IMSI is transmitted in plain text. There is no possibility of encrypting IMSI with A5, RAND is transmitted only after the successful authentication of the system is happened. This flaw may be exploited by using forged BTS and BSC. Unless the IMSI is transmitted in plain text subscriber is rejected. This type of attack is not common in principle in GSM networks and could be fought by a mutual subscriber-BSS authentication.

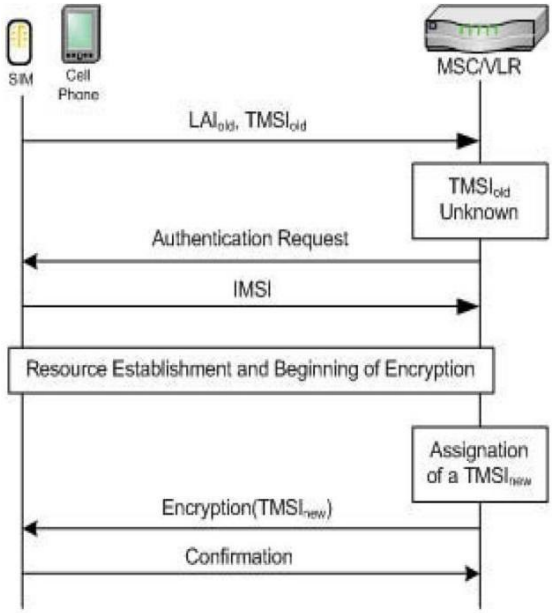

Fig 3: Unknown TMSI and plaintext IMSI transmission

In GSM, the SIM is authenticated to the network, but authentication of network is not carried out as a part of GSM protocol. This could result in false base station problem.

Another flaw comes from SIM card cloning. If an attacker succeeds in cloning a SIM card and then turns a Mobile Network (MN) on, the network will detect two mobile devices with same identifiers at same time and will close the subscription and thus impeding identity thefts.

Security in General Packet Radio Service (GPRS)

GPRS technology lies between 2G and 3G, promises higher data throughput for sporadic traffic illustrated in Fig 4. 2.5G extends GSM by adding best effort packet switched communication for low latency data transmission.

GPRS Architecture

Unlike GSM, GPRS is able to provide packet based IP connectivity to a MN and also proposes a higher through put by allocating radio resources as a volume of information to be transmitted. The GPRS has following two entities.

a) Serving GPRS Support Node (SGSN): It manages the attachments of MN in the service zone and acts as an interface for packets on the way to GGSN. The links between these two entities are based on IP, but use traffic is protected by encapsulating in a proprietary protocol called as GTP (GPRS Tunneling protocol).SGGN is the in charge of security providing integrity, authentication, and authorization as BSC in a 2G.

b) Gateway GPRS Support Node (GGSN):It provides the connectivity between operator's packet oriented network and IP network. It collects traffic statistics and manages billing, session and routing information. It also provides IP address to a MN and sustains for entire duration of attachment.

Fig4 illustrates various elements of a GPRS network and their interconnections. There are mainly three interfaces in GPRS network. They are:

1. Gp: Interface between internal SGSN and external GGSN.
2. Gi: Interface between mobile operator and network.
3. Gn: Interface between GGSN and SGSNs of the same operator.

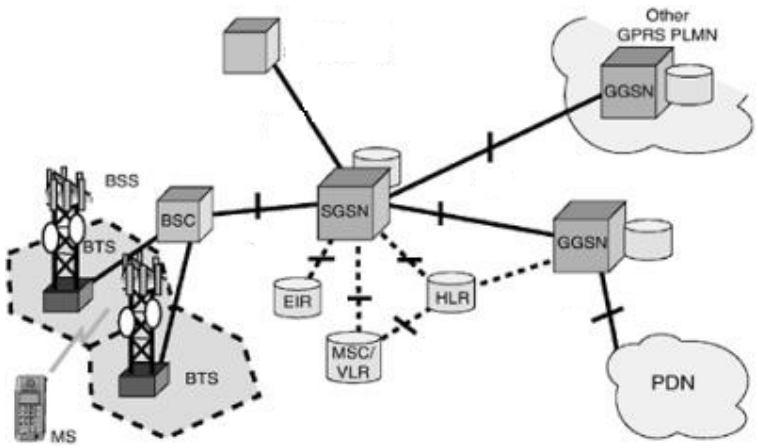

Fig 4: GPRS network and inter connections

GPRS Subscriber authentication and GPRS data encryption

This process is similar to the authentication of GSM. The authentication is performed by SGSN and uses an independent random number GPRS-RAND. The GPRS network provides a distinct challenge reply (GPRS-SRES) and GPRS encryption key (GPRS-Kc) from the GSM network.

GPRS data encryption is performed using GPRS encryption algorithm (GEA). It differs from GSM in such a way that, here encryption is performed up to SGSN and not between MN and BTS.GPRS- Kc key is separately stored from GSM Kc key.

Security flaws in GPRS

The weak points of GPRS network are as follows.

1. The mobile terminal or SIM card:
   Authentication algorithms are similar to those of GSM and similar kind of attacks may be initiated.
2. The GPRS radio link:
   The encryption of radio link is based on KASUMI cipher it is deliberately simplified to perform well in resource limited devices.

3. The GPRS Application security:
   The application security protocol proposed for GPRS is Wireless Application Protocol (WAP) maintained by WAP forum. The WAP gap is a serious security flaw.

2.3 Security enhancements in UMTS

The UMTS uses larger frequency band and its objective is to provide high data and voice rate. Since it has larger frequency band, a higher number of calls may be simultaneously serviced. The throughput for data communication has been increased significantly. Following Fig 5 illustrates UMTS infrastructure and its connecting elements.

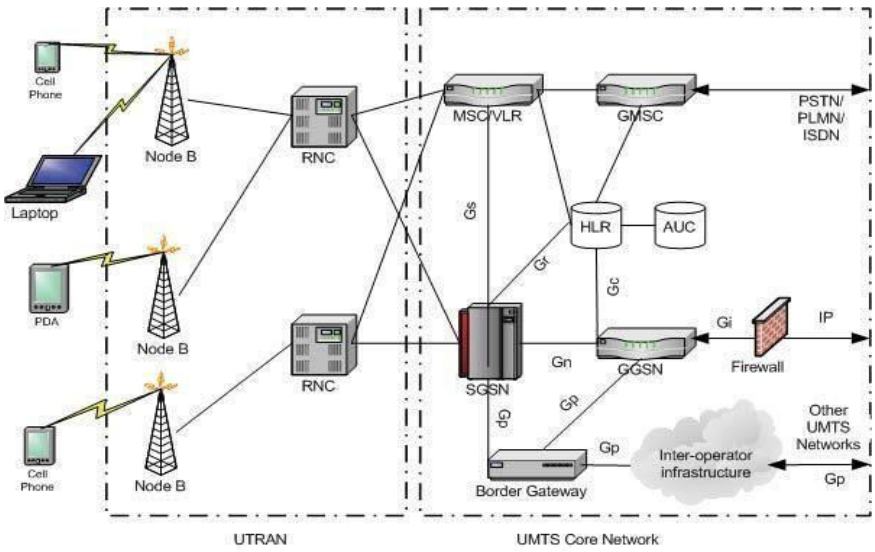

Fig 5: The UMTS Infrastructure

The UMTS network supports interoperability with GSM/GPRS network. The infrastructure includes GSM/GPRS specific and UMTS specific functionalities. The UMTS reuses GSM/GPRS functionalities for voice calls or data transmissions. It differs in the protocol layer for each interface with respect to radio technology [6]. The following two nodes replace those of GSM/GPRS.

a) Node B replaces BTS
b) RNC (Radio Network Controller) replaces BSC

The 3G Security system define a higher security management for UMTS networks. New security provisions have been added such that detection of rogue base stations, network mutual authentication, strict control over the transmission of secret keys, longer encryption keys etc.

GSM SIM card is replaced with more powerful chip called as USIM (Universal Subscriber IdentityModule).FollowingfeaturesarebuiltintoUMTStoovercometheshortcomingsofGSM.

1. False base station problem is impossible in UMTS, since each signaling message is individually authenticated and integrity protected.
2. GSM does not support mutual authentication of network and cellphone. In UMTS, as a part of mutual authentication protocol, the SIM card and the network agree on an encryption key and also a key for integrity protection of messages. To prevent replay attacks, the sequence numbers and nonce are used.
3. Data and signaling messages are encrypted. Both integrity protection and encryption are based on KASUMI-a 128 bit block cipher.
4. Messages on all wireless links are encrypted, not the link between cell phone and the base station. The algorithms for encryption and integrity can be negotiated between the SIM and the network.

The Fig 6 and Fig 7 illustrate the authentication procedure in a UMTS network.

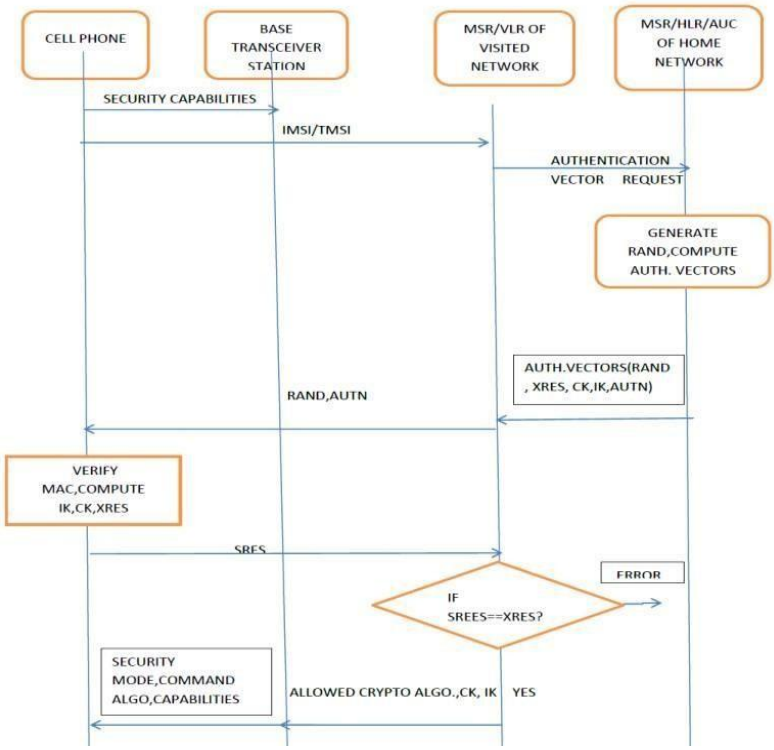

Fig 6: Authentication Protocol

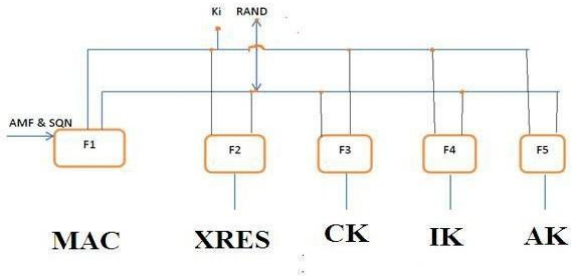

Fig 7: Authentication vector computation

2.2.4 Integrity Protection and Encryption

Message origin authentication and integrity protection are provided using a MAC. In UMTS the MAC computation and Encryption are performed as shown in Fig 8.

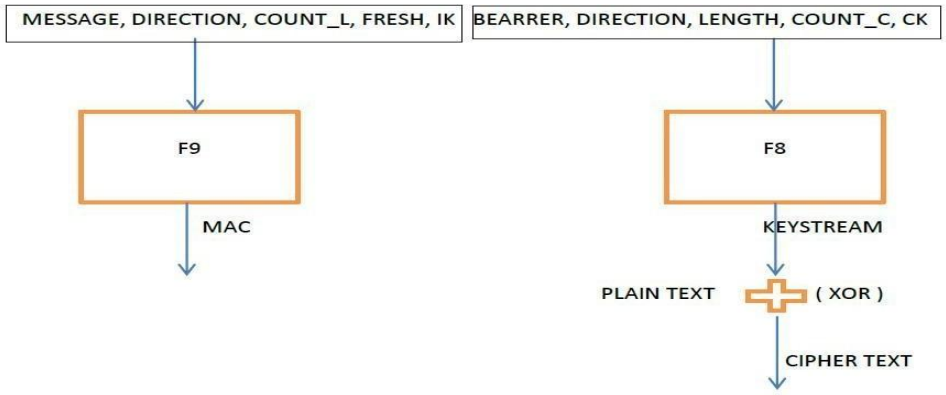

Fig 8 : MAC computation and Encryption in UMTS

The per- message MAC is computed as follows.

Per –message MAC= F9 (IK, COUNTi, FRESH, Direction, message)
The Integrity key IK is computed during authentication and key agreement phase, is used during the generation and verification of MAC. Two variables COUNTi (sequence number derived from the frame number) and FRESH (a random number) are used to prevent replay attacks. At connection set up, COUNTi is initialized by the cell phone while FRESH is generated by the BSC. The Direction indicates from where the message is originated (BSCorCellphone).

In UMTS, integrity check is performed only on signalling data, encryption is performed on both signalling and user data. A stream cipher is used and the key stream is a function of the cipher key CK, a frame count, COUNTc, the radio channel indication (bearer), and the direction indication.

KEYSTREAM= F8 (CK, COUNTc, BEARER, DIRECTION, LENGTH)
The functions F8 and F9 are based on KASUMI, an 8 round fiestel cipher with 64 bit block

size and 128 bit key. For MAC generation, KASUMI in CBC (Cipher Block Chaining) mode used and key stream generation uses OFB (output feedback).

The reason for choosing KASUMI based on an excellent combination of security, performance and implementation characteristics.

3. NEXT GENERATION MOBILE NETWORKS

The next generation networks are also called as 4G by International Telecommunication Unit (ITU) currently under development. It is aiming to provide a maximum throughput of 100 mb/s. The 3G networks supported transparent interconnection of IP, PSTN etc., 4G networks will support full heterogeneity in the radio subsystem and supporting multiple radio technologies. For example WLAN and cell phones are transparently connected without any communication or compromise with quality of service.

The 4G network Architecture

Fig 8 illustrates the 4G architecture with its components.

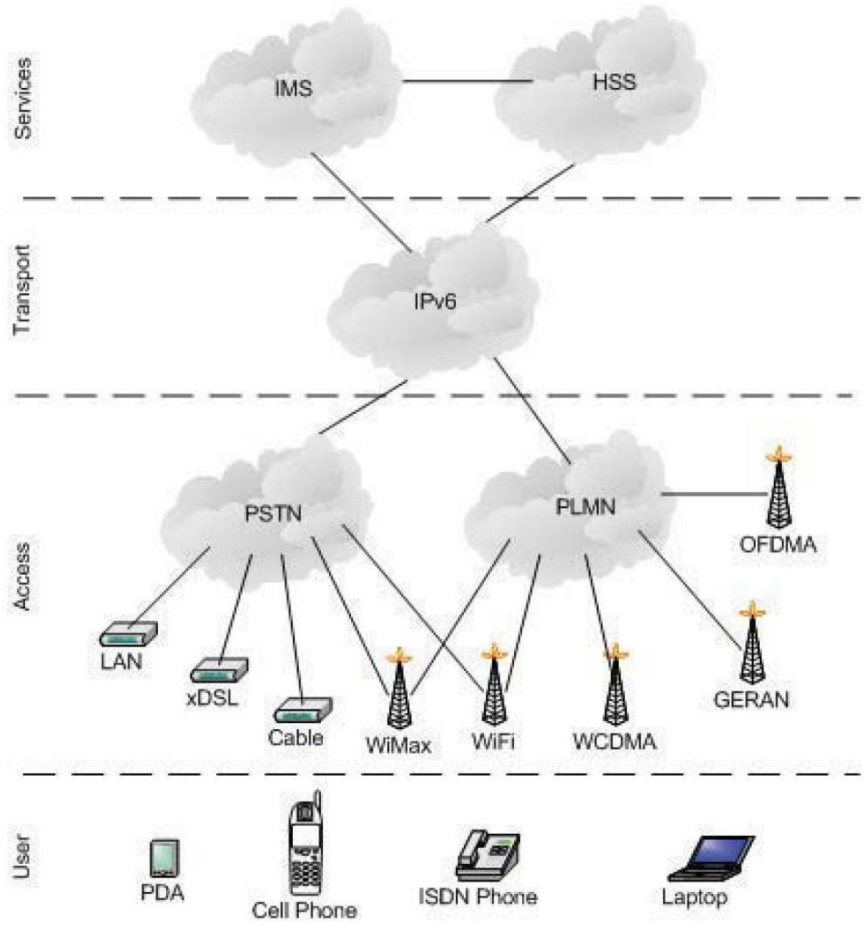

Fig 8: 4G network Architecture

The4G technologyisdesignedtofacilitateimprovedperformanceoverprevioustechnologies.It is intended to support voice, video/multimedia applications with broadband support. The 4G network mainly composed of four layers namely user, access, transport, service. Each layer communicates each other using total transparent and communication technologies. The 4G technology is developed by keeping following points in mind [7].

1. High data rate (1GBPS peak rate for low mobility and 100 MBPS peak rate for high mobility)
2. High capacity
3. Low cost per bit

4. Low latency
5. Good quality of service
6. Good coverage
7. Mobility support at high speed rates

The next generation mobile communication technology universally identified as 4G technology and more importance is given to increased security and reliable communication. The 4G is Internet Protocol based technology and works based on TCP/IP [8]. At present LTE (Long Term Evolution) and Wi MAX (World Wide Interoperability for Microwave Access) are the two key identified technologies for achieving 4G performance objectives [9]. The following paragraphs briefly discuss the above two key technologies.

WiMAX

The Fig 9 illustrates a cellular Wi MAX architecture components and technologies. ASN (Access Service Network) and CSN (Connectivity Service Network) are the two key components in this architecture. The elements in the ASN are base station and ASN gateways connected over IP infrastructure. The ASN gateway maintains accounting information and security policies with mobility support for mobile stations. The Mobile IP home agent in the CSN provides global mobility. The key elements involved in this architecture are as below.

1. AAA (Authentication, Authorization and Accounting): It is located in CSN network, authenticates mobile station against the credentials stored in AAA database. After successful authentication the Mobile Station (MS) profile is handed over to ASN gateway with associated quality of service parameters.
2. Home agent (HA): It processes control signals from ASN gateway and assigns mobile IP address to MS and manages data traffic through HA server.
3. IP Multimedia System (IMS) Server: It processes VoIP call. If the call is outside the Wi MAX network for a telephone number, the IMS selects appropriate Media Controller gateway or Media Gateway to the PSTN. Various mobility scenarios are supported including inter ASN gateway, intra ASN gateway and when a MS moves from one BS to other served by same ASN-GW calls are switched seamlessly using signaling.

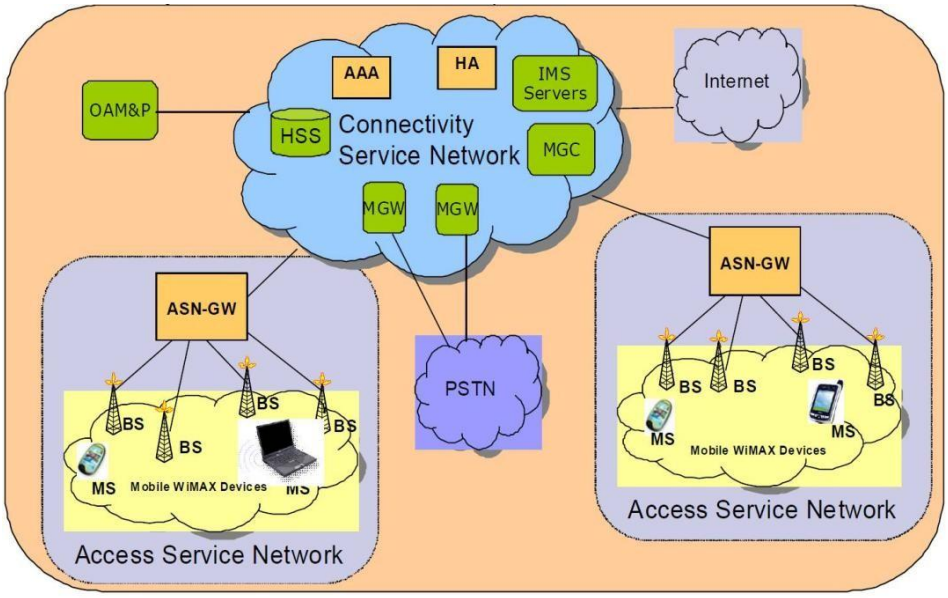

Fig 9: WiMAX Architecture

LTE

The LTE architecture is demonstrated in Fig 10 below.

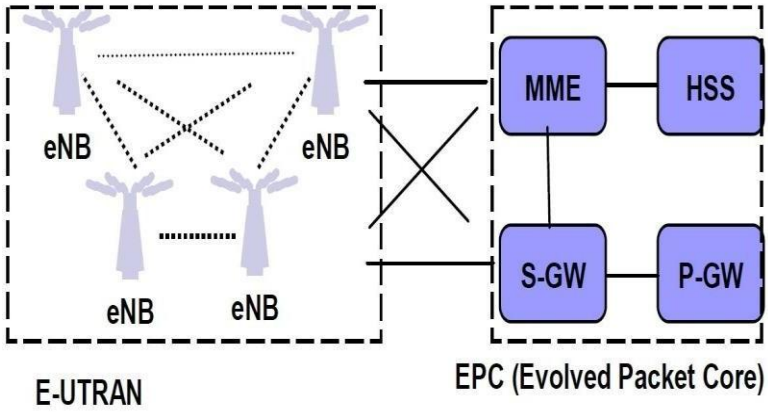

Fig 10: The LTE Architecture

The user equipment connected to wireless network through eNB (enodeB) with in E-UTRAN (Evolved UMTS Terrestrial Radio Access network). The providers network is connected through an IP based Evolved Packet Core (EPC). An LTE network has two types of Network Elements.

1. aneNB (enode B), which is an enhanced base station
2. The access gateway (AGW), performs all functions required for EPC.

An LTE utilizes flata llIP based architecture, where traffic generated at user device is represented in native IP format. These packets are then processed by enodeB and AGW. The AGW contains several modules including HSS (Home Subscriber Server), P-GW (Packet Data Network gateway), S-GW (Serving Gateway) and MME (Mobility Management Entity).
The MME is an important entity in LTE architecture. It identifies UE and handles security and authentication test with interacting HSS. It tracks UE in idle mode and handles roaming. It chooses an S-GW during initial connection and at intra LTE handover.

The S-GW terminates interface towards E-UTRAN and handles routing and forwarding of data packets.

The P-GW terminates interface towards packet data network (service provider wire line network). It also performs policy enforcement, per user packet filtering, billing and charging and IP address allocation for UE.

The per user accounting information is maintained by HSS. It also holds subscription related information for handling sessions. It generates authentication data and handles to MME. A challenge response authentication mechanism and key agreement procedure is used between UE and MME.

Vulnerabilities in LTE/SAE

The vulnerabilities in LTE/SAE is classified under the following categories [9].

1. Threats against user identity and privacy
2. Threats of USIM/UE tracking
3. Threat related to handovers and base stations

4. Threats related to denial of service
5. Threats of unauthorised access to the network
6. Compromise of eNB credentials and physical attack on eNB
7. Attacks on core networks, including eNB location based attack

4. M- COMMERCE: RISKS, SECURITY AND PAYMENT METHODS

The unprecedented development in wireless and mobile communication has brought forward incredible opportunities for M-Commerce. Mobile wireless has exploded in popularity because of its simplicity and revolution in communication. Mobile wireless market is increasing by leaps and bounds. The success of mobile communication lies in the ability to provide instant connectivity anytime and anywhere to provide high speed data services to the mobile user. The quality and speeds available in the mobile environment must match the fixed networks if the convergence of the mobile wireless and fixed communication network is to happen in the real sense. The challenge for mobile network lie in providing very large footprint of mobile services with high speed and security.

A Mobile Payment is defined as a payment for product or services between two parties for which a mobile device plays a key role in the realization of payment. In an M-Payment activity a mobile phone is used by the payer in one or more steps during banking or financial transactions. The ubiquity of cell phones together with the convenience it offers suggests that mobile payments will constitute an increasing proportion of electronic payments.

Mobile applications can be either be mobile web or native. Security issues in mobile web applications closely resemble those of traditional web applications because of homogeneity in underlying development technologies and protocols [6]

Features of M-Commerce

Following are some unique features of M-commerce.

a. Ubiquity: Here services are offered irrespective of users geographic location.
b. Immediacy: This feature is closely related to ubiquity where real time availment of services is offered for genuine user. eg: stock market data.
c. Localisation: Positioning technologies such as GPS offers goods and services specific to

customer location.

d. Instant Connectivity: Constant online facility connected with the network avoiding dial up or boot up procedure.

e. Proactive functionality: This feature ensures that the right information(relevant) at right time andplace.Serviceslikeoptinadvertisingenablestheuserchoicesandpreferencesfrequently.

M- Commerce Architecture

The M-Commerce architecture is 3 tier architecture and mainly consists of following components as indicated in Fig 11.

1. Frontend (client): The mobile device or the piece of software running on the mobile device.
2. Middleware (server): It is the software server running business logic of the system.
3. Backend (database): The back end mainly comprised of database servers.

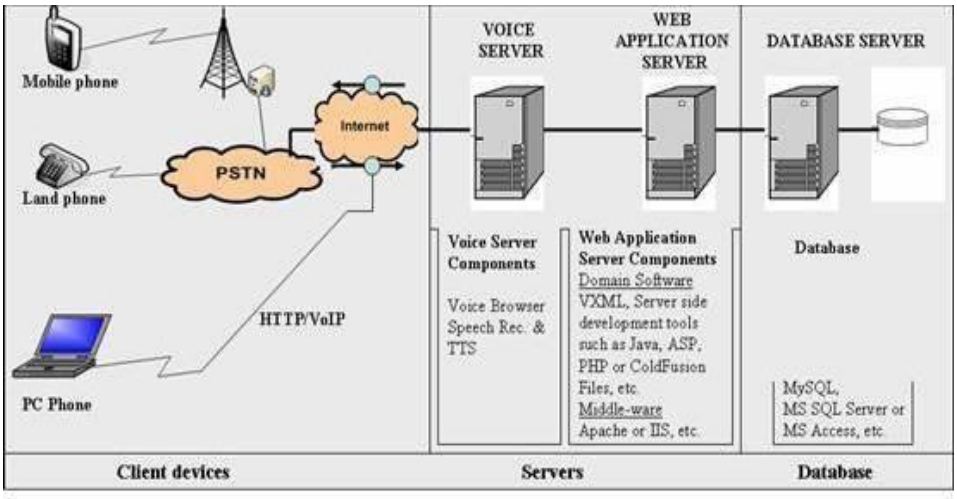

Fig 11: The M-Commerce Architecture

The M-Commerce architecture depicts different entities involved in 3 tiers and their functionalities. The cell phones are the client devices and used to access different services to the users. It provides the interface for the customers and serves as the front end for interaction. The base stations will route and forward the signal to intended destination. The SMS Gateway/WAP gateway supports either text or internet based communication.

The Middle ware constitutes Web server keeps the business logic of the M-Commerce system. After successful authentication of user, the intended server will provide service requested by the client after proper charging. At the back end there exists a database or set of data bases.

M-Payment Life cycle

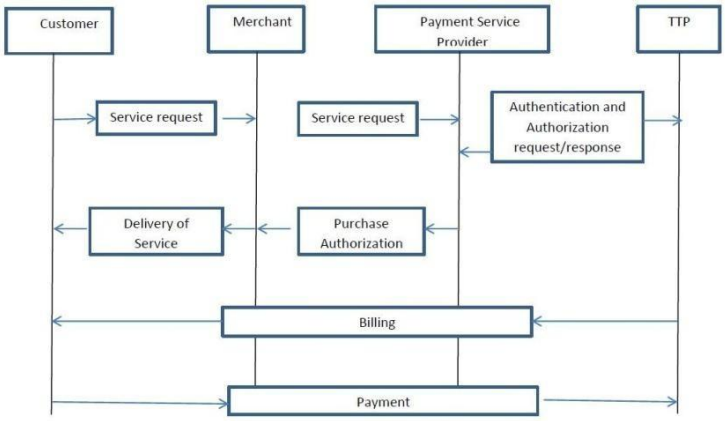

Fig 11: M-Payment life Cycle

Payment transaction in a mobile environment is very similar to a typical payment card transactions shown in Fig 11. It differs in the transport of payment detail involved i.e. wireless device using WAP/HTML based browser.

Mobile payment lifecycle has the following main steps.

1. Registration: Customer opens an account with payment service provider for payment service through a particular payment method.
2. Transaction: Transaction mainly comprised of following four important steps.
   a) The desire of a customer is generated using a SMS or pressing a mobile phone button.
   b) The content provider forwards the request to the payment service provider.
   c) Payment service provider then requests a trusted third party to authenticate and authorize the customer.
   d) Payment service provider informs content provider about the status of the authentication

and authorization. If successful authentication of the customer is performed, content provider will deliver the requested goods.

3. Payment settlement: This operation can take place during real time, prepaid or post-paid mode. A real time payment involves the exchange of some form of electronic currency, for example payment settlement directly through a bank account. In prepaid type of settlement customers pay in advance using smartcards or electronic wallets. In post pay mode the payment service provider sends billing information to the trusted third party, which sends the bills to customers, receives money back, and then sends the revenue to payment service provider.

5. WIRELESS PUBLIC KEY INFRASTRUCTURE (WPKI) BASED M-COMMERCE SECURITY SYSTEM

Public key cryptography technique is used as backbone for the WPKI to provide security in m- commerce. The entire certificate management life cycle activities starting from certification creation, generation, storing, distribution and revocation of public key certificate is supported by an WPKI architecture. Fig 7 below illustrates various components existing in an integrated WPKI system[8].

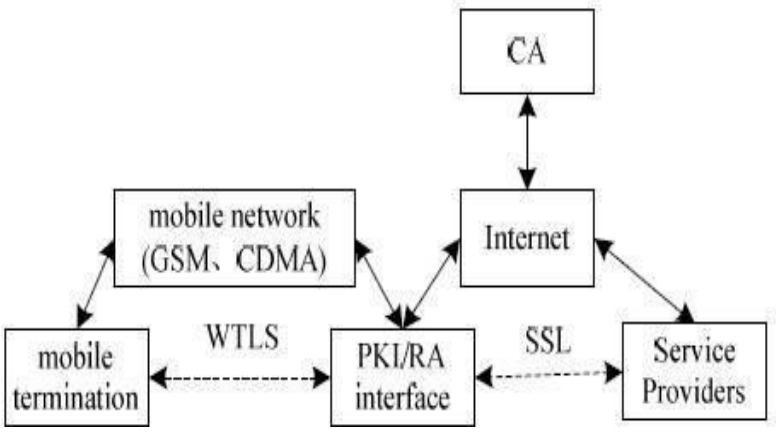

Fig 7: Components of M-Commerce security architecture

WAP is the key entity in a wireless environment for connecting the internet. WTLS is the lighter version of TLS and it is suitable for wireless environment. For the secure connection and communication between service providers SSL is used. For high efficiency the system

adopts enhanced certificate verification method which reduces the load of resource constrained devices.

6. SCOPE, ADVANTAGES AND LIMITATIONS

The wide spread use of mobile devices now a day generates huge amount of revenues by reducing time and money needed for multiple purposes. The rapid development in mobile computing technology not only creates several opportunities for the business and also opens the door for doing disasters using misuse of technology. The information residing in the mobiles and integrity of the information, security of the information during its journey over the air security of the information within the wireless network has to be given much importance.

Because of Mobile Computing or Mobile networks, M-Commerce has become reality today. The support of large number of cellular network service providers with competing speed made user to use his mobile device as a transacting module rather than simply using it for making calls. Following are some of the merits and demerits of M-commerce.

Advantages of M-Commerce

1. Convenience: Just a few clicks on the device serve user purpose.
2. Flexible accessibility: User can be accessible through mobile devices and through various messengers.
3. Easy connectivity: As long as network is available the device can be in action.
4. Personalization: Since the device belongs to a specific user, it provides personalization to its user.
5. Time efficient: Critical transaction can be possible to execute within a very short span of time.

Disadvantages of M-Commerce

1. Technological constraints of mobile devices may limit file size to be processed.
2. User interface may not be friendly to operate.
3. Limitation over the number of characters to be used on SMS.

7. CONCLUSION

The mobile devices have captured the place of personal computers for the day by day activity. The wide spread use of mobile devices now a day generates huge amount of revenues by reducing time and money needed for multiple purposes. The rapid development in mobile computing technology not only creates several opportunities for the business and also opens the door for doing disasters using misuse of technology. The information residing in the mobiles, integrity of the information and security of the information during its journey over the air security of the information within the wireless network has to be given much importance. Because of Mobile Computing or Mobile networks, M-Commerce has become reality today. The support of large number of cellular network service providers with competing speed made user to use his mobile device as a transacting module rather than simply using it for making calls.

REFERENCES

[1] Mahmoud Elkhodr, Seyed Shahrestani and Kaled Kourouche," A Proposal to improve the security of mobile banking applications", IEEE International conference on ICT and Knowledge Engineering, 2012

[2] Ashok K Talukder and Roopa R Yavagal, "Mobile Computing", TaTa McGraw Hill Education, January 2005

[3] Hua Ye, "Design and Implementation of M-Commerce system applied to 3G Network platforms based on J2ME",IEEE International conference on Electrical and Control Engineering,2010

[4] Dharma Prakash Agrawal and Qing An Zeng, "Introduction to Wireless and Mobile Systems", Third Edition, Cengage Learning USA

[5] Hakima Chaouchi and Maryline Laurent maknavicius, "Wireless and Mobile Network Security", Second Edition, Wiley Publishers

[6] Anurag Kumar Jain and Devendra Shanbhaug, "Addressing Security and Privacy Risks Mobile applications", IEEE Computer society, 2012

[7] Bernaard menezes, " Network security and cryptography", CENGAGE Learning, second edition

[8] Feng Tian et al., " Application and Research of Mobile E-commerce security based on WPKI", IEEE International Conference on Information Assurance and Security, 2009.