Journal of Advances and Scholarly Researches in Allied Education
Vol. 16, Issue No. 2, February-2019, ISSN 2230-7540

Security Challenges Related to Mobile Commerce and Computing

Sumeer Kumar*

Research Scholar

Abstract – Mobile wireless market is expanding significantly. Mobile computing and Mobile Commerce is most well known now days as a result of the administration offered during the portability. Mobile registering has become the truth today instead of the extravagance. The quality and paces accessible in the Mobile condition must match the fixed organizations if the combination of the Mobile wireless and fixed correspondence network is to occur in the genuine sense. The test for Mobile organization lies in giving huge impression of Mobile network with rapid and security. Mobile Commerce utilizing Mobile phones must guarantee high security for client qualifications and it ought not be workable for abuse. M-Commerce is the electronic trade performed utilizing Mobile phones. Since client certifications to be left well enough alone, a significant level of security ought to be guaranteed.

Key Words – Mobile Wireless, Mobile Computing, Mobile Commerce, Mobile Network, Online Transactions, Security.

----------X----------

1. INTRODUCTION

Mobile computing gives adaptability of figuring condition over physical portability. The client of a Mobile figuring condition will have the option to admittance to information, data or other consistent items from any gadget in any organization while progressing. To make the Mobile registering condition omnipresent, it is fundamental that the correspondence carrier is spread over both wired and remote media.

The rising mobile industry expected to be described by progressively customized and area based administrations. The accessibility of client favored data in spite of area made versatile registering fruitful. The headway of Mobile innovation has changed the manner in which individuals utilize cell phones in their everyday action [1].

Mobile computing offers a registering situation over physical versatility. The client of a Mobile registering condition will have the option to admittance to information, data or other intelligent items from any gadget in any organization while progressing. To make the Mobile processing condition pervasive, it is fundamental that the correspondence carrier is spread over both wired and remote media [2].

Mobile System Infrastructure

The mobile framework foundation offers the vital types of assistance required for the correct working of the substances engaged with a versatile framework, engineering. One of the most generally conveyed cell frameworks is GSM or 2G and its creators had a few objectives. Better quality for voice, higher paces for information, worldwide meandering, security against charge extortion and listening in. The UMTS or 3G guaranteed progressed administrations, for example, Mobile web, sight and sound informing, video conferencing and so forth. UMTS principles were characterized by a global consortium called 3GPP (Third era organization venture) [3].

1.1.2 Fundamentals of a Mobile framework

The conventional square chart of a cell framework is appeared in the Fig 1 beneath

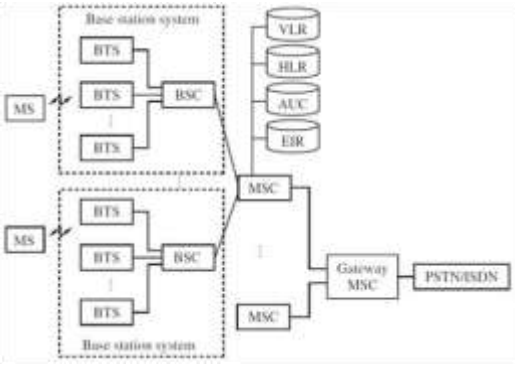

Fig 1: Cellular System

The essential topographical unit of a phone framework is known as a cell is the geological territory secured by a transmitter. At the most minimal level, a mobile phone is associated with a base station (or base handset station) by a radio connection. Various base stations are associated with and constrained by a base station regulator. Different base station regulators and upstream are associated with Mobile exchanging focus. The Mobile Switching Center (MSC) advances an approaching call to the objective MSC. “The MSC additionally monitors bookkeeping and charging data.

The client has a membership to certain organizations called as his home organization. A coordinated relationship among MSC and an organization is kept up. A MSC has an information base, called the Home Location Register (HLR) having data of every one of its supporters. The information base contains the data of endorser's versatile number, the administrations benefited and a mystery key put away in the Mobile known uniquely to the HLR. HLR additionally keeps up the dynamic data of its wandering clients for charging. It incorporates the current area of a client and the cell network utilized by the client [4].

A supporter may benefit the administrations of different organizations (called as unfamiliar organizations) that have an arrangement for meandering with endorser's home organization. Each phone network additionally keeps up an information base called as Visitor Location register (VLR) of clients presently visiting that network with the rundown of administrations the supporter entitled to.2G innovation presented Subscriber Identity Module (SIM) card which stores three privileged insights utilized for cryptographic tasks [5].

2. SECURITY IN POPULAR MOBILE NETWORKS

Security in GSM

The two chief errands required for giving GSM Network security are:

a) Entity confirmation and Key arrangement

b) Message insurance.

Substance Authentication and Key Agreement

Fig 2 shows confirmation technique associated with GSM. It has following advances.

1. Authorization solicitation from Cell Phone:

During approval demand step, the mobile phone sends the encryption calculation it can support to the base station and IMSI/TMSI number to the MSC. In the event that the PDA is away from its home organization, the IMSI will be gotten by the MSC of the visited network. The last conveys the IMSI to the MSC/HLR of the PDAs home organization with a solicitation to give a test that will be utilized to confirm by a phone.

2. Creation and transmission of confirmation vectors:

The IMSI acquired by the MSC is utilized to list the home area registers to get a mutual key, Ki known distinctly to the SIM and HLR of the home organization. The MSC/HLR produces 128 bit irregular number, RAND, which capacities as a test in the test reaction verification convention. The two amounts XRES and Kc are registered as underneath.

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

Where, A3 and A8 are two keyed hash capacities. XRES is the normal reaction in the test reaction validation convention. Kc is the encryption key. The HLR makes five confirmation trios, each cultivated by newly picked arbitrary numbers. Every trio is of the structure

<RAND, XRES, Kc>

The trios are sent to the MSC of the home organization by the HLR. In the event that the mobile phone is visiting an unfamiliar organization, the MSC advances the trios to the MSC of the visited network. Five trios are sent so four resulting confirmations might be performed without the need to consistently include MSC/HLR of the home organization.

The MSC sends the test (RAND) from the primary trio to the base station and it is sent to SIM on the mobile phone.

3. Cell Phone reaction:

When the SIM has gotten RAND, it registers SRES (Signed Response) like XRES. It very well may be registered by a substance with the information on Ki, key shared between the SIM and HLR. The mobile phone sends SRES to the base station and it is sent to MSC. The MSC analyzes if SRES is equivalent to XRES and in the event that they are same MSC presumes that SIM knows Ki and recognizes it as an authentic endorser.

4. Computation/Receipt of encryption key:

The SIM processes Kc and MSC removes Kc from its confirmation trio and conveys it to the base station. Further all interchanges between wireless and base station are scrambled utilizing Kc.

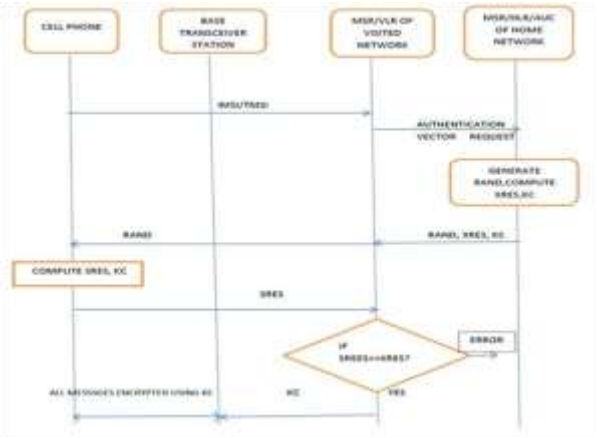

Fig 2: Authentication steps in GSM

Message Protection

Stream figure strategy is utilized to scramble the message transmission between wireless and base station. The key stream generator for this is meant as A5. The key stream is a component of the 64 cycle encryption key, Kc, and 22 piece outline number.

KEYSTREAM= A5 (Kc, FRAME_NUMBER)

For each edge communicated, the edge number is increased which changes the key stream for each edge sent during a call. Typically figure text is produced by X-OR ing the plain content and the key stream.

Calculation of the key stream and encryption don't need any static data put away in the SIM. Calculation of XRES and Kc requires the supporter validation key, Ki. Subsequently the capacities A3 and A8 must be upheld by the SIM and A5 regularly not.

Issues and disadvantages

There are some security deficiencies distinguished in GSM. The primary defect is identified with confirmation of the endorser as represented in the accompanying Fig 3 .The framework utilizes brief identifier, Temporary Mobile Subscriber Identity (TMSI) to forestall the personality. On the off chance that the VLR couldn't perceive or TMSI is lost, the IMSI is communicated in plain content. There is no chance of encoding IMSI with A5, RAND is communicated simply after the effective verification of the framework is occurred. This blemish might be abused by utilizing produced BTS and BSC. Except if the IMSI is communicated in plain content supporter is dismissed. This sort of assault isn't regular on a fundamental level in GSM organizations and could be battled by a common endorser BSS validation.

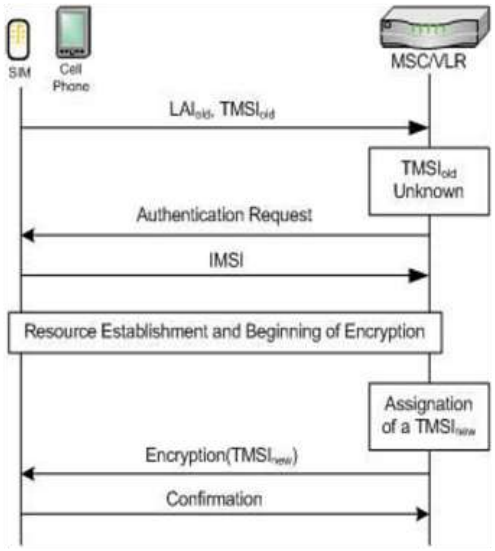

Fig 3: Unknown TMSI and plaintext IMSI transmission

In GSM, the SIM is confirmed to the organization, however validation of organization isn't done as a piece of GSM convention. This could bring about bogus base station issue. Another imperfection originates from SIM card cloning. In the event that an aggressor prevails with regards to cloning a SIM card and, at that point turns a Mobile Network (MN) on, the organization will identify two cell phones with same identifiers at same time and will close the membership and in this way blocking personality robberies.

Security in General Packet Radio Service (GPRS)

GPRS innovation lies somewhere in the range of 2G and 3G, guarantees higher information throughput for inconsistent traffic outlined in Fig 4. 2.5G expands GSM by including best exertion bundle exchanged correspondence for low inertness information transmission.

GPRS Architecture

Not at all like GSM, GPRS can give bundle based IP availability to a MN and furthermore proposes a higher throughput by allotting radio assets as a volume of data to be communicated. The GPRS has following two elements.

a) Serving GPRS Support Node (SGSN): It deals with the connections of MN in the administration zone and goes about as an interface for bundles while in transit to GGSN. The connection between these two entities depend on IP, however client traffic is secured by typifying in an exclusive protocol called as GTP (GPRS burrowing convention). SGGN is the accountable for security providing

respectability, validation, and approval as BSC in a 2G.

b) Gateway GPRS Support Node (GGSN): It gives the availability between administrators packet arranged organization and IP organization. It gathers traffic measurements and oversees charging, session and directing data. It additionally gives IP address to a MN and supports for whole duration of connection.

Fig 4 represents different components of a GPRS organization and their bury associations. There are for the most part three interfaces in GPRS organization. They are:

1. Gp: Interface between inside SGSN and outside GGSN.

2. Gi: Interface between versatile administrator and organization.

3. Gn: Interface among GGSN and SGSNs of a similar administrator.

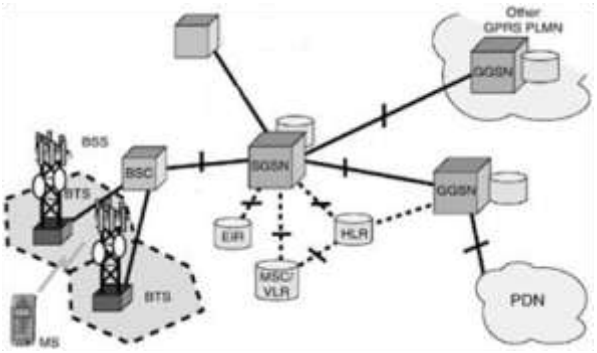

Fig 4: GPRS network and inter connections

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 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.

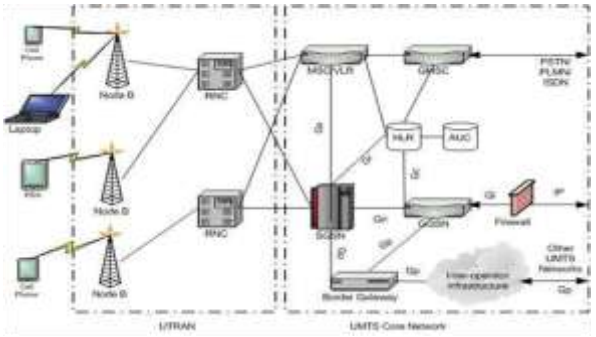

Fig 5: The UMTS Infrastructure

The UMTS network underpins interoperability with GSM/GPRS organization. The foundation incorporates GSM/GPRS explicit and UMTS explicit functionalities. The UMTS reuses GSM/GPRS functionalities for voice calls or information transmissions. It varies in the convention layer for every interface concerning radio innovation [6]. The accompanying two hubs supplant those of GSM/GPRS.

a) Node B replaces BTS

b) RNC (Radio Network Controller) replaces BSC

The 3G Security framework characterize a higher security the executives for UMTS organizations. New security arrangements have been included with the end goal that location of rebel base stations, network shared verification, exacting command over the transmission of mystery keys, longer encryption keys and so forth. GSM SIM card is supplanted with all the more impressive chip called as USIM (Universal Subscriber Identity Module). Following highlights are incorporated with UMTS to defeat the deficiencies of GSM.

1. False base station issue is incomprehensible in UMTS, since each flagging message is individually validated and honesty secured.

2. GSM doesn't uphold common verification of organization and PDA. 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 signalling messages are encrypted. Both trustworthiness security and encryption are based on KASUMI-a 128 digit block figure.

4. Messages on all remote connections are scrambled, not the connection between phone and the base station. The calculations for encryption and honesty can be haggled between the SIM and the organization.

The Fig 6 and Fig 7 represent the verification methodology in an UMTS organization.

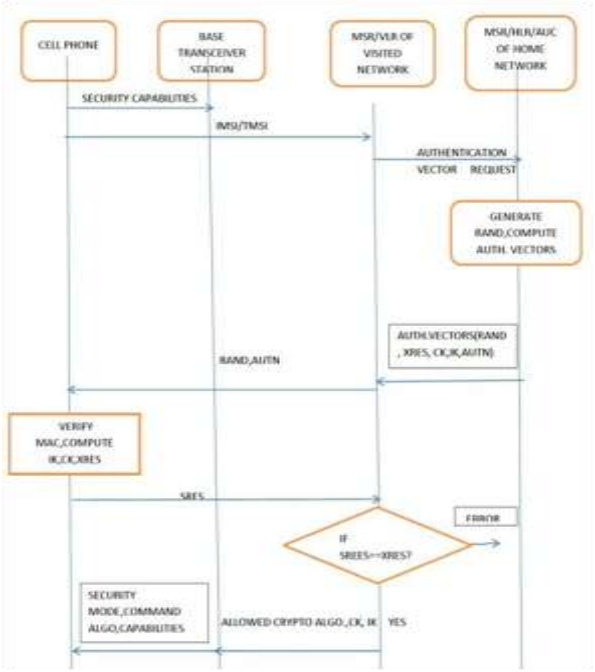

Fig 6: Authentication Protocol

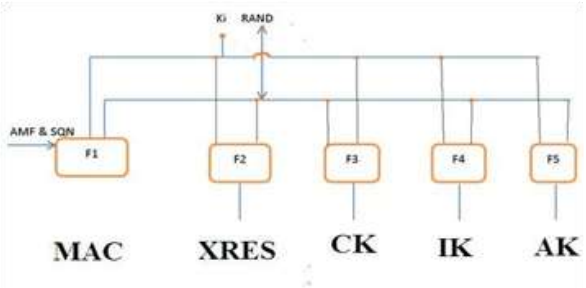

Fig 7: Authentication vector computation

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.

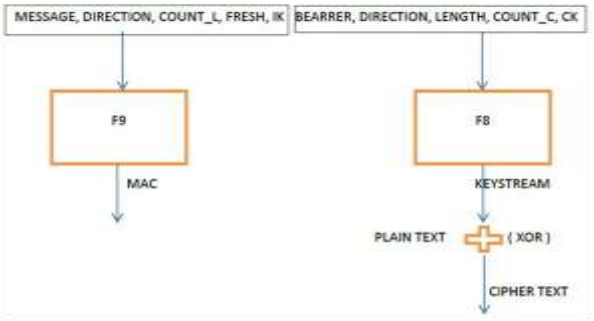

Fig 8 : MAC computation and Encryption in UMTS

The per-message MAC is processed as follows.

Per – message MAC= F9 (IK, COUNTi, FRESH, Direction, message)

The Integrity key IK is processed during validation and key understanding stage, is utilized during the age and check of MAC. Two factors COUNTi(grouping number got from the edge number) and FRESH (an arbitrary number) are utilized to forestall replay assaults.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 (BSC or Cell phone).

In UMTS, trustworthiness check is performed uniquely on flagging information, encryption is performed on both flagging and client information. A stream figure is utilized and the key stream is an element of the code key CK, an edge check, COUNTc, the radio channel sign (carrier), and the course sign.

KEYSTREAM= F8 (CK, COUNTc, BEARER, DIRECTION, LENGTH)

The capacities F8 and F9 depend on KASUMI, a 8 round fiestel figure 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 likewise called as 4G by International Telecommunication Unit (ITU) right now a work in progress. It is meaning to give a most extreme throughput of 100 mb/s. The 3G networks upheld straightforward interconnection of IP, PSTN and so forth., 4G organizations will uphold full heterogeneity in the radio subsystem and supporting different radio

advancements. For instance WLAN and PDAs are straightforwardly associated with no correspondence or bargain with nature of administration.

The 4G network Architecture

Fig 8 delineates the 4G engineering with its parts.

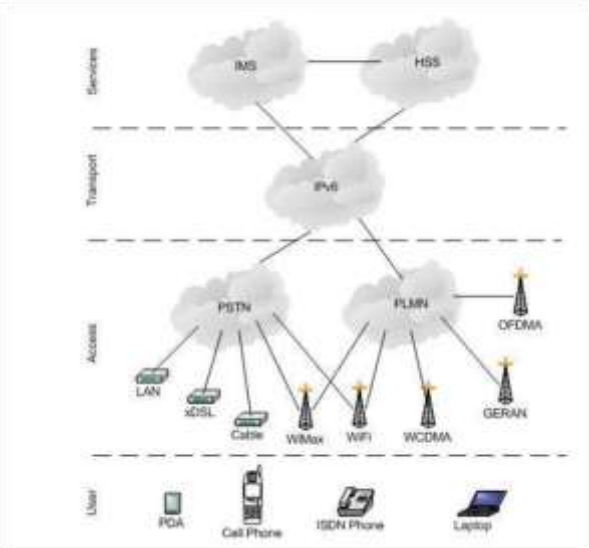

Fig 8: 4 Gnetwork Architecture

The 4G technology is intended to encourage improved execution over past advancements. It is planned to help voice, video/mixed media applications with broadband help. The 4G network mostly made out of four layers to be specific client, access, transport, administration. Each layer imparts each other utilizing all out straightforward and correspondence innovations. The 4G innovation is created by remembering following focuses [7].

1. High information rate (1 GBPS top rate for low versatility and 100 MBPS top rate for high mobility)
2. High limit
3. Low expense per bit
4. Low inertness
5. Good nature of administration
6. Good inclusion
7. Mobility help at fast rates

The cutting edge versatile correspondence innovation all around distinguished as 4G innovation and more significance is given to expanded security and solid correspondence. The 4G is Internet Protocol put together innovation and works based with respect to TCP/IP [8]. At present LTE (Long Term Evolution) and WiMAX (World Wide Interoperability for Microwave Access) are the two key recognized advances for accomplishing 4G execution targets [9]. The accompanying sections quickly examine the over two key innovations.

WiMAX

The Fig 9 outlines a cell WiMAX design parts and advances. ASN (Access Service Network) and CSN (Connectivity Service Network) are the two key segments in this design. The components in the ASN are base station and ASN doors associated over IP foundation. The ASN passage keeps up accountibg data and security strategies with portability uphold for versatile stations. The Mobile IP home specialist in the CSN gives worldwide versatility. The key components associated with this design are as underneath.

1. AAA (Authentication, Authorization and Accounting): It is situated in CSN organization, authenticates versatile station against the qualifications put away in AAA information base. After successful confirmation the Mobile Station (MS) profile is given over to ASN entryway with related nature of administration boundaries.
2. Home specialist (HA): It measures control signals from ASN entryway and doles out versatile IP address to MS and oversees information traffic through HA worker.
3. IP Multimedia System (IMS) Server : It measures VoIP call. On the off chance that the call is outside the WiMAX network for a phone number, the IMS chooses fitting Media Controller gateway or Media Gateway to the PSTN. Different versatility situations are upheld including bury ASN entryway, intra ASN door and when a MS moves from one BS to other served by same ASN-GW calls are exchanged consistently utilizing flagging.

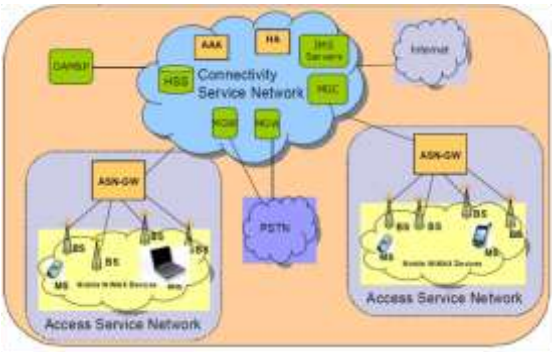

Fig 9: WiMAX Architecture

LTE

The LTE architecture is demonstrated in Fig 10 below.

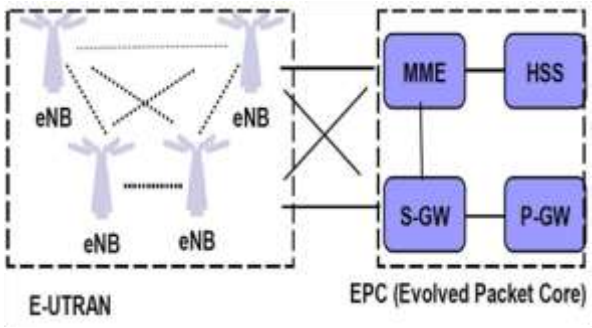

Fig 10: The LTE Architecture

The client gear associated with remote organization through eNB (enodeB) with in E-UTRAN (Evolved UMTS Terrestrial Radio Access organization). The suppliers network is associated through an IP based Evolved Packet Core (EPC). A LTE network has two kinds of Network Elements.

1. aneNB (enodeB) , which is an improved base station

2. The access passage (AGW), plays out all capacities required for EPC.

A LTE uses level all IP based design, where traffic created at client gadget is spoken to in local IP design. These parcels are then handled by enodeB and AGW. The AGW contains a few modules including HSS (Home Subscriber Server), P-GW (Packet Data Network door), S-GW (Serving Gateway) and MME (Mobility Management Entity).

The MME is a significant element in LTE design. It distinguishes UE and handles security and confirmation test with interfacing HSS. It tracks UE out of gear mode and handles meandering. It picks a S-GW during introductory association and at intra LTE handover.

The S-GW ends interface towards E-UTRAN and handles directing and sending of information bundles. The P-GW ends interface towards parcel information organization (specialist co-op wireline network). It additionally performs strategy implementation, per client parcel separating, charging and charging and IP address assignment for UE.

The per client bookkeeping data is kept up by HSS. It additionally holds membership related data for dealing with meetings. It produces verification information and handles to MME. A test reaction validation instrument and key arrangement strategy is utilized among UE and MME.

Weaknesses in LTE/SAE

The weaknesses in LTE/SAE is grouped under the accompanying classes [9].

1. Threats against client character and protection

2. Threats of USIM/UE following

3. Threat identified with handovers and base stations

4. Threats identified with refusal of administration

5. Threats of unapproved admittance to the organization

6. Compromise of eNB accreditations and physical assault on eNB

7. Attacks on center organizations, including eNB area based assault.

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

The remarkable advancement in remote and versatile correspondence has presented inconceivable open doors for M-Commerce. Portable remote has detonated in prominence on account of its effortlessness and transformation in correspondence. Portable remote market is expanding significantly. The accomplishment of portable correspondence lies in the capacity to give moment availability whenever and anyplace to give rapid information administrations to the versatile client. The quality and velocities accessible in the versatile climate must match the fixed organizations if the intermingling of the portable remote and fixed correspondence network is to occur in the genuine sense. The test for versatile organization lie in giving huge impression of portable administrations with fast and security.

A Mobile Payment is characterized as an installment for item or administrations between two gatherings for which a cell phone assumes a key part in the acknowledgment of installment. In a M-Payment action a cell phone is utilized by the payer in at least one stages during banking or money related exchanges. The omnipresence of phones along with the accommodation it offers recommends that versatile installments will establish an expanding extent of electronic installments. Portable applications can be either be versatile web or local. Security issues in portable web applications intently take after those of conventional web applications on account of homogeneity in basic advancement innovations and conventions [6]

Highlights of Mobile-Commerce

Following are some novel highlights of M-business.

a. Ubiquity: Here administrations are offered regardless of clients geographic area.

b. Immediacy: This element is firmly identified with pervasiveness where on-going availment of services is offered for authentic user.eg: securities exchange information.

c. Localisation: Positioning advances, for example, GPS offers products and ventures explicit to customer area.

d. Instant Connectivity: Constant online office associated with the organization staying away from dial up or boot up strategy.

e. proactive usefulness: This component guarantees that the privilege information(relevant) at right time and spot. Administrations like pick in promoting empowers the client decisions and inclinations frequently.

Portable Commerce Architecture

The M-Commerce design is 3 level engineering and fundamentally comprises of following parts as demonstrated in Fig 11.

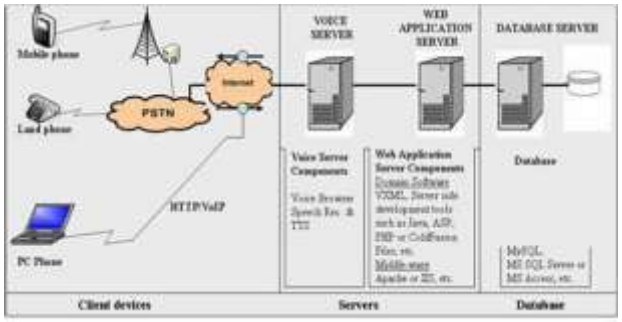

Fig 11: The M-Commerce Architecture

1. Front end (customer): The cell phone or the bit of programming running on the portable device.

2. Middleware (worker): It is the product worker running business rationale of the framework.

3. Back end (information base): The back end fundamentally included information base workers.

The M-Commerce design portrays various elements engaged with 3 levels and their functionalities. The mobile phones are the customer gadgets and used to get to various administrations to the clients. It gives the interface to the clients and fills in as the front end for collaboration. The base stations will course and forward the sign to expected objective. The SMS Gateway/WAP door underpins either text or web based correspondence.

The Middle product establishes Webserver keeps the business rationale of the M-Commerce framework. After effective verification of client, the planned worker will offer support mentioned by the customer after appropriate charging. At the back end there exists an information base or set of information bases.

Portable Payment Life cycle

Installment exchange in a portable climate is fundamentally the same as a run of the mill installment card exchanges appeared in Fig 11. It varies in the vehicle of installment detail included for example remote gadget utilizing WAP/HTML based program.

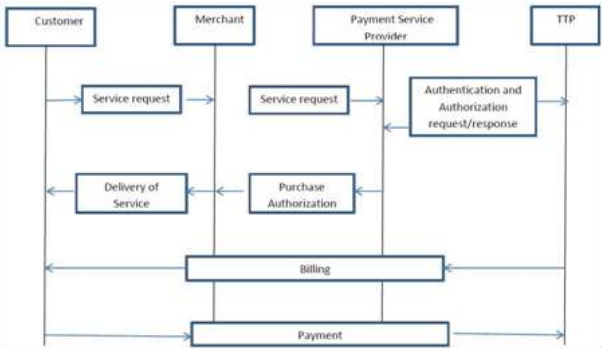

Fig 11: M-Payment life Cycle

Mobile payment lifecycle has the accompanying primary advances.

1. Registration: Customer opens a record with installment specialist organization for installment service through a specific installment strategy.

2. Transaction: Transaction principally involved after four significant advances.

   a) The want of a client is produced utilizing a SMS or squeezing a cell phone button.

   b) The content supplier advances the solicitation to the installment specialist co-op.

   c) Payment specialist co-op then demands a confided in outsider to confirm and approve the client.

   d) Payment specialist co-op educates content supplier about the status regarding the validation and approval. In the event that fruitful verification of the client is

performed, content provider will convey the mentioned merchandise.

3. Payment settlement: This activity can happen during ongoing, paid ahead of time or post-paid mode. A constant installment includes the trading of some type of electronic money, for example installment repayment legitimately through a ledger. Inprepaid sort of settlement customers pay ahead of time utilizing brilliant cards or electronic wallets. In post pay mode the payment specialist co-op sends charging data to the confided in outsider, which sends the bills to clients, gets cash back, and afterward sends the income to installment administration provider.

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

Public key cryptography procedure is utilized as spine for the WPKI to give security in m-business. The whole testament the board life cycle exercises beginning from accreditation creation, age, putting away, dispersion and renouncement of public key declaration is upheld by a WPKI design. Fig 12 beneath outlines different parts existing in a coordinated WPKI framework [8].

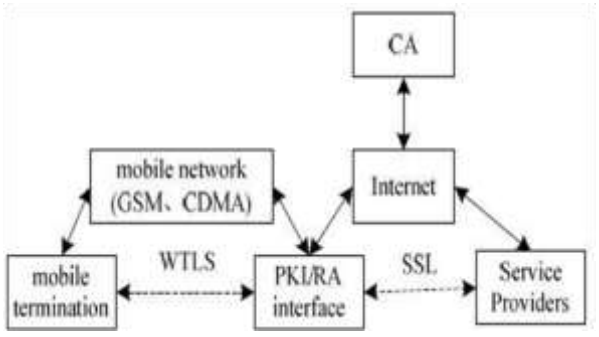

Fig 12 : Components of M-Commerce security architecture

WAP is the key substance in a remote climate for interfacing the web. WTLS is the lighter rendition of TLS and it is reasonable for remote climate. For the protected association and correspondence between specialist co-ops SSL is utilized. For high proficiency the framework embraces upgraded declaration check strategy which diminishes the heap of asset compelled gadgets.

6. SCOPE, ADVANTAGES AND LIMITATIONS

The broad utilization of cell phones now daily creates gigantic measure of incomes by diminishing time and cash required for different purposes. The fast advancement in portable processing innovation not just makes a few open doors for the business and furthermore opens the entryway for doing fiascos utilizing abuse of innovation. The data dwelling in the mobiles and uprightness of the data, security of the data during its excursion over the air security of the data with in the remote organization must be given a lot of significance.

Due to Mobile Computing or Mobile organizations, M-Commerce has become reality today. The help of enormous number of cell network specialist organizations with contending speed made client to utilize his cell phone as an executing module instead of essentially utilizing it for settling on decisions. Following are a portion of the benefits and faults of M-business.

Favorable circumstances of M-Commerce

1. Convenience: Just a couple of snaps on the gadget fill client need.

2. Flexible openness: User can be available through cell phones and through different couriers.

3. Easy availability: insofar as organization is accessible the gadget can be in real life.

4. Personalization: Since the gadget has a place with a particular client, it gives personalization to its client.

5. Time effective: Critical exchange can be conceivable to execute with in an exceptionally limited ability to focus time.

Dis Advantages of M-Commerce

1. Technological limitations of cell phones may restrict record size to be prepared.

2. User interface may not be cordial to work.

3. Limitation over the quantity of characters to be utilized on SMS.

7. CONCLUSION

The PDAs have gotten the spot of PCs for the bit by bit development. The certain usage of PDAs now every day makes colossal proportion of salaries by lessening time and money required for different purposes. The quick improvement in versatile figuring innovation not simply makes a couple of open entryways for the business and besides opens the portal for doing calamities using maltreatment of development.The data living in the mobiles, honesty of the data and security of the data during its excursion over the air security of the data with in the wireless network must be given a lot of significance. Due to Mobile Computing or Mobile networks, M-Commerce has become reality today. The help of huge number of

cell network specialist co-ops with contending speed made client to utilize his cell phone as an executing module instead of just utilizing it for settling on decisions.

REFERENCES

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

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

[3] Ashok K Talukder and Roopa R. Yavagal (2005). “Mobile Computing”, TaTa McGraw Hill Education.

[4] Hakima Chaouchi and Maryline Laurent Maknavicius: “Wireless and Mobile Network Security”, Second Edition, Wiley Publishers

[5] Dharma prakashagrawal and Qing an Zeng, “Introduction to Wireless and Mobile Systems”, Third Edition, Cengage Learning USA

[6] Anurag Kumarjain and Devendra Shanbhaug (2012). “Addressing Security and Privacy Risks Mobile applications”, IEEE Computer society.

[7] Feng Tian et. al. (2009). “Application and Research of Mobile E-commerce security based on WPKI”, IEEE International Conference on Information Assurance and Security.

[8] Bernaardmenezes, “Network security and cryptography”, CENGAGE Learning, econd edition.

Corresponding Author

Sumeer Kumar*

Research Scholar

sameernandal30@gmail.com