International Journal of Future Generation Communication and Networking
Vol. 14, No. 1, (2021), pp. 872–882

An Enhanced Authentication Protocol in Tripartite Signcryption for Mobile Communication dependent

A Reuga Devi[1], Dr. K. Krishnaveni[2]

[1] *Madurai Kamaraj University College, Madurai, Tamil Nadu, India*

[2] *Sri S. Ramasamy Naidu Memorial College, Sattur, Tamil Nadu, India*

Abstract

This paper presents a new authentication convention utilizing the tripartite signcryption plot without bilinear pairings that gives classification and validation between three elements. Versatile correspondence appears to be extremely alluring to clients just as administrators and specialist co-ops. Be that as it may, notwithstanding of its various points of interest, versatile correspondence has been confronting numerous security issues. In this paper, it is exhibited how the proposed three sided signcryption plan can be utilized to give validation and to ensure secure correspondence. The utilization of the proposed three sided signcryption plot decreases the flagging overhead contrasted with the plan in [1].

KEYWORDS: Signcryption, Tripartite, Mobile Communication, Mobile Security

INTRODUCTION

Remote and portable correspondance Framework are popular among the clients also the administrators and specialist organizations. In contrast to wired organizations, the remote organizations give anyplace and whenever admittance to clients. The Global System for Mobile Communications (GSM) possesses practically 70% of the remote market and is utilized by a huge number of endorsers on the planet [2]. In remote administrations, secure and mystery correspondence is attractive. It is the enthusiasm of both the clients and the specialist organizations. These gatherings could never need their assets and administrations to be utilized by unapproved clients. The administrations like web based banking, e-installment, and e/m-business are now utilizing the Internet. The money related foundations like banks and different associations might want their clients to utilize online administrations through cell phones keeping the remote exchange as secure as conceivable from the security dangers. Shrewd cards (for example SIM card) have been proposed for applications like secure admittance to administrations in GSM, to confirm

ISSN: 2233-7857IJFGCN

clients and secure installment utilizing Visa cards and MasterCard [3]. Remote exchanges are confronting a few security challenges. Information sent through air face nearly similar security dangers as the information over wired organizations and significantly more. Be that as it may, the impediments in remote data transmission, battery, computational force and memory of remote gadgets force further limitations to the security instruments execution [4]. The utilization of portable correspondence in e/m-business has expanded the significance of security. A proficient remote correspondence foundation is needed in each association for secure voice/information correspondence and clients validation. Among the fundamental destinations of a proficient framework is to diminish the flagging overhead and to decrease the quantity of HLR/AuC (Home-Location Register/Authentication Center) refreshes as the Mobile Station (MS) changes its area often [4].

Tripartite security instruments are of specific significance as they are valuable in giving basic security in a few indispensable applications, for example, in web based business where the three elements engaged with the convention are the trader, the client and the bank. Other intriguing applications incorporate an outsider being added to seat or official a discussion with the end goal of impromptu examining, information recuperation or escrow purposes [5].

Signcryption joins the functionalities of encryption and advanced marking in a solitary intelligent advance. It gives different security administrations including secrecy, respectability, message root genuineness and non-renouncement. Y. Abouelseoud proposed a three sided Signcryption plot from bilinearpairings in [6]. This three sided signcryption plot is utilized to lessen the flagging overhead in the safe electronic exchange (SET) convention.

This paper presents a productive three sided signcryption plot without bilinear pairings. It tends to be used to give classification and confirmation in portable correspondence networks in an effective path as it empowers diminishing the flagging overhead. The rest of the paper is composed as follows. In the following area, the alluring security includes that a signcryption plan ought to give are summed up. In Section 3, the proposed three sided signcryption conspire is portrayed and the security properties of the plan are examined in Section 4. A diagram of the engineering of GSM is given in Section 5 and in the area that follows the utilization of public key cryptography in versatile correspondence conventions is surveyed. The utilization of the proposed three sided signcryption plan to give confirmation in versatile correspondences is inspected in Section 7. At long last, Section8 closes the paper.

ISSN: 2233-7857IJFGCN

2. SECURITY REQUIREMENTS FOR ANY SIGNCRYPTION SCHEME

Here, the security prerequisites for any signcryption conspire are given [7,8,9]:

2.1 Confidentiality

It implies that solitary the planned beneficiary of a signcrypted message ought to have the option to peruse its substance. That is, after observing a signcrypted message, an assailant ought to pick up nothing about the first message, other than maybe its length

2.2 Unforgeability

It alludes to the powerlessness of any substance to create a substantial message-signature pair aside from the assigned endorser.

2.3 Public Verifiability

It implies that any outsider or judge can confirm that the signcrypted text is legitimate or not, with no requirement for the private key of the sender or the recipient.

2.4 Non-Repudiation

The sender of a message can't later deny having sent the message. That is, the beneficiary of a message can demonstrate to an outsider that the sender in reality sent the message.

2.5 Integrity

This implies that the beneficiary ought to have the option to check that the got message is the first one that was sent by the sender and it has not been altered during transmission.

2.6 Authentication

It includes affirming the character of a framework client. Validation frequently includes checking the legitimacy of in any event one type of recognizable proof. Additionally, it permits the real beneficiary alone to be persuaded that the ciphertext and the marked message it contains were made by a similar entity.

2.7 Forward Secrecy

It alludes to the failure of an aggressor to peruse signcrypted messages, even with admittance to the sender’s private key. That is, the secrecy of signcrypted messages is ensured, regardless of whether the sender’s private key is undermined

ISSN: 2233-7857IJFGCN

3. THE TRIPARTITE SIGNCRYPTION SCHEME

In this part, the four modules of the three sided signcryption conspire in [13].This plot used to decrease the motioning over head in the validation convention in GSM.

3.1 Setup

Given security boundary *k*(usually 160), the CA (endorsement authority) picks *q a* enormous prime number with $q>2^k$, *(a, b)* is a couple of numbers which are more modest than q and fulfill $(4a^3+27b^2)$ *mod* $q\neq\neq 0$. E is the chose elliptic bend over the limited field F_q : $y2=(x3+ax+b) \bmod q$. R is the base point or generator of a gathering of focuses on E, meant as G. Likewise, O is the point at vastness and n is the request for the point R, with n being a prime number, $n.R=O$ and $n>2^k$. The CA chooses a cryptographic one way hash work H : {0,1}*□ Z_q. The CA distributes the framework boundaries:{*k,a,b,E,R,H*}. Moreover, a safe symmetric key encryption component ought to be settled upon between the conveying parties.

3.2 Key Generation

The private/public key sets for the three imparting parties are produced as follows. Every part picks an arbitrary number d and then processes the relating public key as $Q=dR$. The key sets for elements A, B and C are given as $Q_a=d_aR$, $Q_b=d_bR$ and $Q_c=d_cR$ respectively. The signcryption and unsigncryption periods of the proposed conspire are appeared in Figure1.

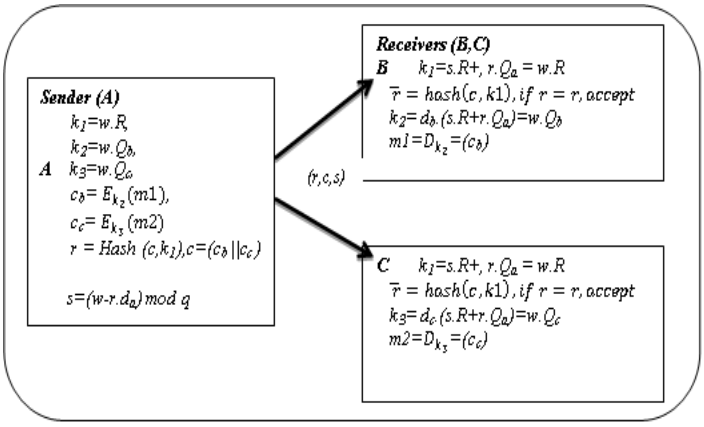


Fig 1: The tripartite signcryption scheme configuration

3.3 Signcryption

ISSN: 2233-7857IJFGCN

Phase A needs to communicate something specific m_1 to B and a message m_2 to C. A signcrypts the messages as follows:

The sender A produces an arbitrary number $w \in [1, n-1] \in [1, n-1]$ and computes:

- $k_1 = w.R$, $k_2 = w.Q_b$, *and* $k_3 = w.Q_c$, he key utilized is essential for the x-organize estimation of the focuses k_1, k_2, k_3
- $c_b = E_{k_2}(m1)E_{k_2}(m1)$, *and* $c_c = E_{k_3}(m2)E_{k_3}(m2)$
- $r = Hash\ (c,k_1), c=(c_b \| c_c)$
- $s=(w-r.d_a)\ mod$
- *(r,c,s) has been send by A to B and C*

3.4 Unsigncryption

- The recipient B utilizes his/her mystery key d_b to recoup the encryption key $k_2; k_2=d_b(s.R+r.Q_a)=w.Q_b$
- B recuperates k_1 without utilizing any mystery keys and this help the public certainty in the proposed conspire where $k_1=s.R+r.Q_a=w.R$
- B computes $r = Hash\ (c,k_1)$, *at the point if* $\bar{r} = r\bar{r} = r$, B acknowledges the signcrypted-text and in any case prematurely ends the protocol.
- B figures $m_1=D_{k_2}\bar{c_b}D_{k_2}\bar{c_b}$

The receiver C does likewise ventures as B:

- The recipient C utilizes his/her mystery key to recoup the encryption $k_3; k_3=d_c(s.R+r.Q_a)=w.Q_c$.
- C recoups k_1 without utilizing any mystery keys by processing $k_1=s.R+r.Q_a=w.R$. At that point, substance C. computes $r = Hash\ (c,k_1)$, *at the point if* $\bar{r} = r\bar{r} = r$, C acknowledges the signcrypted-text.
- At last, C recuperates the message $m_2=.D_{k_3}\bar{c_c}D_{k_3}\bar{c_c}$

3.5 Public verifiability

Any outsider can recoup k_1 without utilizing any mystery keys supporting public obviousness in the proposed plot, where $k_1= s.R+r.Q_a=w.R$. At that point, the outsider figures, $\bar{r}\bar{r}$= *Hash* (c,k_1), *at the point if* $\bar{r} = r\bar{r} = r$, it acknowledges the signcrypted-text.

4. GSM OVERVIEW

GSM (Group Special Mobile) initially was a gathering framed by the European Conference of Post and Telecommunication Administrations (CEPT) in 1982 to create cell frameworks for substitution of effectively contrary cell frameworks in Europe. Later in 1991, when the GSM began administrations, its importance was changed to Global System for Mobile Communications (GSM) [2].

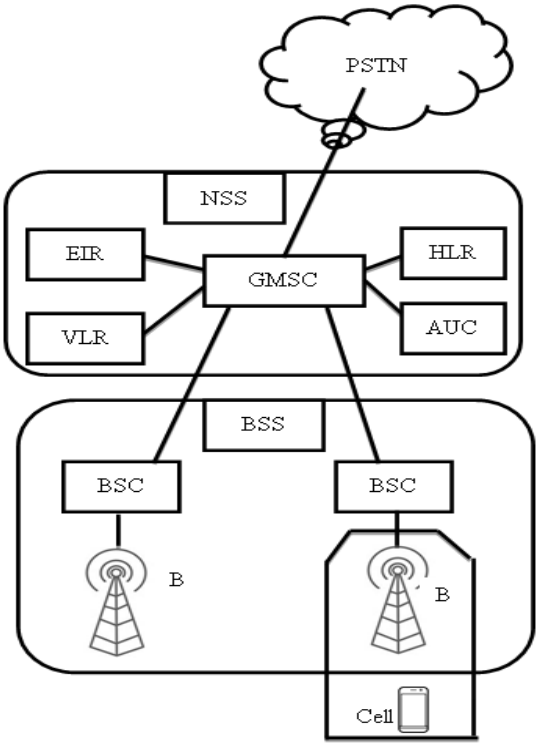
ISSN: 2233-7857IJFGCN

The whole design of the GSM is partitioned into three subsystems: Mobile Station (MS), Base Station Subsystem (BSS) and Network Subsystem (NSS) as appeared in Figure 2.

1.The MS consists of a Mobile Equipment (ME) (for example cell phone) and Subscriber Identity Module (SIM) card which stores mystery data like International Mobile Subscriber Identity (IMSI), mystery key (Ki) for confirmation and other client related data.

2. The BSS, the radio organization, controls the radio connection and gives a radio interface to the remainder of the organization. It comprises of two kinds of hubs: Base Station Controller (BSC) and Base Station (BS). The BS covers a particular topographical zone (hexagon) which is known as a cell. Every cell contains numerous versatile stations. A BSC controls a few base stations by dealing with their radio assets.
3. The BSCis associated with a Mobile administrations Switching Center (MSC) in the third aspect of the organization NSS, Subscribers confirmation data individually [2, 11].

Fig.2 Components of GSM



additionally called the Core Network (CN). Notwithstanding MSC, the NSS comprises of a few different information bases like Visitor Location Register (VLR), Home Location Register (HLR) and Gateway MSC (GMSC) which interfaces the GSM organization to Public Switched Telephone Network (PSTN). The MSC, in participation with the HLR and the VLR, gives various capacities including enlistment, verification, area refreshing, handovers and call routing.

ISSN: 2233-7857IJFGCN

The HLR holds regulatory data of endorsers enlisted in the GSM organization. Likewise, the VLR contains just the required managerial data of supporters right now found/moved to its zone. The Equipment Identity Register (EIR) and Authentication Center (AuC) contain a rundown of substantial portable supplies

5.Related Work: Authentication and Encryption In GSM GPRS and UMTS using Public Key Cryptography

This segment audits the confirmation convention in [2].The three principle elements, MS, VLR and HLR, are utilizing four sets of public/private key matches as follows:

- *V_H_{PrK} : VLR-HLR link;s private key V_H_{PuK} : VLR-HLR link;s public key*
- *M_V_{PrK} : MS-VLR link's private key*
- *M_V_{PuK} : MS-VLR link's public key*
- *H_{PrK} : HLR private key*
- *H_{PuK} : HLR public key*
- *M_{PrK} : Mobile private key*

These three elements trade four messages with one another as appeared in fig 3

$$Y_{it} = \alpha_1 + \alpha_2 D_{2i} + \alpha_{3i} D_{3i} + \beta_{1it} CPI_{1it} + \mu_{it} \quad 1.$$

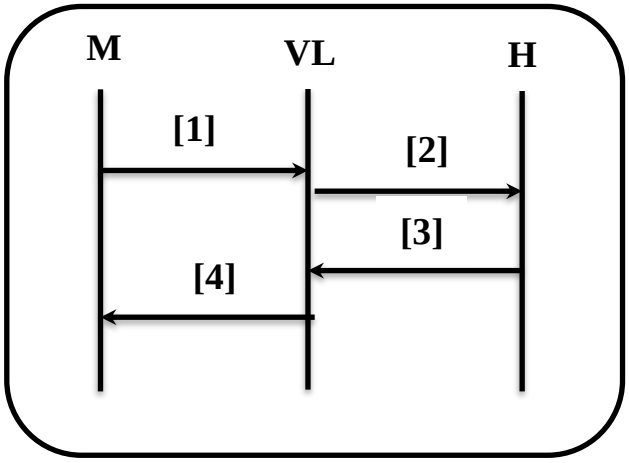


Figure 3. The detail of the components in everyone

ISSN: 2233-7857IJFGCN

- *Message* = $E_{M\_V\,PuK}$ *(IK || SK || RAND ||* $E_{H_{PuK}} E_{H_{PuK}}$ *(IMSI || K_i)*
- *Authentication information* = $E_{H_{PuK}} E_{H_{PuK}}$ *(IMSI || K_i)*
- *Acknowledge* = M_{PUK}
- *Forward Acknowledge* $= E_{m_{PuK}}(RAND) = E_{m_{PuK}}(RAND)$

The image "||" speaks to the connection of two components. The MS makes mystery keys SK, IK and an irregular test RAND. It begins the verification trade by sending an Identity Message to the visited VLR. This message comprises of the link of RAND, SK and IK scrambled utilizing the public key M_V_{PuK}. The IMSI and K_i encrypted utilizing the public key H_{PuK} is additionally part of the Identity message.
The VLR utilizes the comparing private key M_V_{PrK} to unscramble its aspect of the message and concentrate the required data RAND, SK andIK. The VLR advances the remainder of message ($E_{H_{PuK}}$ $E_{H_{PuK}}$ *(IMSI || K_i)*) unchanged as an Authentication Information message to the HLR. The keys SK and IK are utilized later for classification and uprightness of both the information and signs, individually.
The HLR decodes the Authentication Information message with its private key H_{PrK} and gets the IMSI and K_i sent from MS. The mystery key K_i is utilized as an arbitrary test for client/MS confirmation. The MS and the HLR have a similar mystery key Ki. The HLR thinks about the got K_i with its own K_i. In the event that they coordinate, the client is verified.
Utilizing the IMSI, the HLR finds the comparing user's public key M_{PuK} and is shipped off VLR in the Authentication Acknowledge message. This message goes about as a sign to the VLR that the client has been validated by the HLR. The VLR utilizes the public key M_{PuK} to scramble the RAND challenge got from MS in the Identity Message. The MS unscrambles it with its own private key. The outcome is contrasted and the RAND put away at the MS. In the event that they are equivalent, the VLR is verified as it guarantees the MS that the VLR is the main substance having the MS-VLR link's private key M_V_{PrK}. The issue with this convention is that a disavowal of-administration assault might be conceivable if the aggressor changes the flagging substance dependent on which the client and organization verify one another. For instance, if the encoded substance of RAND challenge is adjusted or if IMSI or K_i is changed during transmission, the organization and client confirmation will bomb regardless of whether the client and organization are real. To adapt to this issue, an advanced mark can be utilized. The start to finish honesty of the verification boundaries ought to be guaranteed on the grounds that the end elements, the VLR/HLR and the MS, settle on the choice of confirmation. In addition, the protocol includes four traded messages and this causes flagging overhead. The proposed convention dependent on the three sided signcryption is more proficient than encryption then signature[12].
Besides, the quantity of traded messages becomes three instead of four messages. The following area talks about the proposed improvement in details.

6. The Proposed Authentication Protocol Based On The Tripartite Signcryption Scheme

Using signcryption accomplishes both secrecy of message substance and confirmation. Signcryption will tackle the disavowal of administration assault in [1]. Additionally, utilizing a three sided conspire lessens the quantity of traded signals between the substances. Figure 4 shows the traded messages in the proposed verification protocol.

ISSN: 2233-7857IJFGCN

[1] identity message and authentication information = [signcrypt (m_1=IK||SK||RAND), (m_2=IMSI||K_i)], MS will send message to VLR and HLR
[2] Authentication Acknowledge = Q_{MS}
[3] forward Authentication Acknowledge = Signcrypt(RAND)
The signcryption set up is done as in Section 3.2 The private/public key sets for the three imparting parties are created as follows: every part picks an arbitrary number dand then processes the relating public key as $Q=dR$. The key sets for substances MS, VLR and HLR are given as Q_{MS} =d_{MS}.R, Q_{VLR} =d_{VLR}.R and Q_{HLR} =d_{HLR}.R respectively.
The MS creates mystery keys SK, IK and an irregular test RAND. It begins the validation cycle by sending an Identity Message to the visited VLR. This message incorporates two sections. The initial segment (signified as m_1) is utilized by MS and VLR, which is the connection of RAND, SK and IK. The subsequent part (meant as m_2), which is the connection of IMSI and K_i. Both m_1 and m_2 are signcrypted by the three sided plot in Section 3 utilizing the public keys of VLR and HLR and the private key of MS.MS VLR HLR[1][2][3][4]

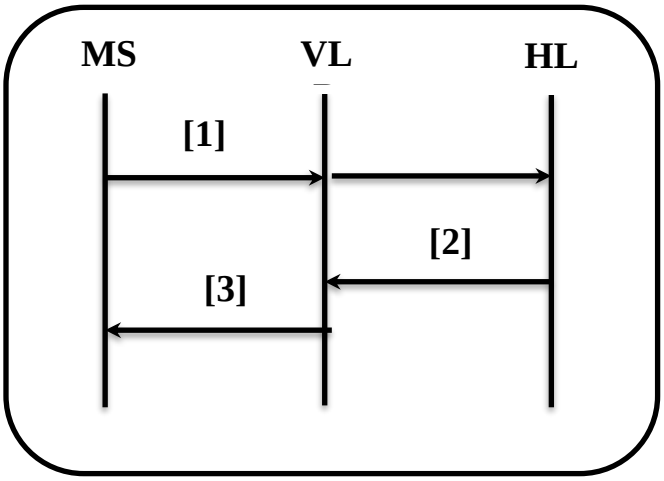


Fig.4 The traded messages in the proposed protocol

The figures are
$c_{VLR}=E_{k_s}E_{k_s}$(RAND)||SK||IK)
$c_{HLR}=E_{k_s}E_{k_s}$(IMSI||K_i)
MS processes the signcrypted figure c=(c_{VLR} || c_{HLR}), and the mark r=Hash(k_1,c) and s=(w-r.d_{MS}) mod q then sends them to both VLRand HLR. The HLR uses the relating private key d_{HLR} with Q_{MS} and gets the IMSI and K_i sent from MS. The mystery key K_i is utilized as an arbitrary test for client/MS authentication. The MS and the HLR have a similar mystery key K_i. The HLR compares the got K_i with its own K_i. On the off chance that they coordinate, the client is confirmed. It is hard for an outsider to change this mystery without being distinguished by HLR.
The HLR can effectively recognize it utilizing IMSI of the mentioning client sent in the Identity message and the mark confirmation fizzles. Utilizing the IMSI, the HLR finds the comparing user's public key Q_{MS}

ISSN: 2233-7857IJFGCN

and is shipped off VLR in the Authentication Acknowledge message. This message goes about as a sign to the VLR that the client has been verified by the HLR. The VLR uses the public key Q_{MS} with its private key d_{VLR} to unsigncrypt its aspect of the message and concentrate the required data RAND, SK and IK. The keys SK and IK are again utilized for secrecy and honesty of both the information and signs, separately. It additionally utilizes the public key Q_{MS} to signcrypt the RAND challenge got from MS in the Identity message. The MS decrypts it with its own private key d_{MS} and the VLR public key Q_{VLR}. The outcome is contrasted and the RANDstored at MS. In the event that they are equivalent, the VLRis confirmed as it guarantees the MSthat the VLRis the main substance having a similar mystery key.This approach beats the disavowal of administration assault utilizing the signcryption crude as examined in the security examination of the proposed three sided plot under the unforgeability property. The methodology in [1] experiences the forswearing of administration assault and the creator recommended including an advanced mark after encryption however it burns-through time and includes an enormous number of calculations. In this manner, utilizing signcryption is more proficient than sign-then-scramble crude [12]. In addition, this whole cycle includes three as opposed to four flagging messages contrasted with [1], accordingly flagging overhead is diminished.

7. CONCLUSION

In this paper, a new communication protocol used in GSM using tripartite signcryption scheme without using bilinear pairings that proposed in [13]. The proposed scheme is used to reduce the signaling overhead in the authentication step in mobile communication systems and combats the denial of service attack. The proposed protocol implemented by three steps to achieve the authentication between the three parties MS, HLR and VLR and this reduces the signaling overhead when compared with the protocol in [1] that implemented using four steps to achieve the authentication between the three parties MS, HLR and VLR

REFERENCES

1) D. Boneh and M. Franklin, Identity-Based Encryption From The Weil Pairing, In: Advances In Cryptology-CRYPTO 2001, In: Vol. LNCS, 2139, Springer-Verlag, 2001, pp. 213–229.
2) R. Borgohain et al., " TSET: Token Based Secure Electronic Transaction"; International Journal of Computer Applications, May 2012, ISBN: 978-93-80866-55-8, DOI: 10.5120/5056-7374.
3) Eman F. Abu Elkhair, “An Improvement to the SET Protocol Based On Signcryption”, International Journal on Cryptography and Information Security (IJCIS), Vol.3, No. 2, June 2013, pp 1-13.
4) Fagen Li and Tsuyoshi Takagi, “Secure identity-based signcryption in the standard model”, Mathematical and Computer Modelling, Volume 57, 2013, pp. 2685–2694

ISSN: 2233-7857IJFGCN

5) H.Gupta and V. K. Sharma," Role of Multiple Encryption in Secure Electronic Transaction", International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6, November 2011.
6) Hassan M. Elkamchouchi et al., "An Improved Authentication Protocol for Mobile Communication based on Tripartite Signcryption", International Journal of Computer Applications, ISSN 0975 – 8887, Volume 92 – No.14, April 2014, pp. 13-18.
7) Z. Jin et al., An Improved Semantically-Secure Identity-Based Signcryption Scheme In The Standard Model, Computers & Electrical Engineering, 36 (3), 2010, pp. 545–552.
8) Krishna Prakash and Balachandra, "Security Issues and Challenges in Mobile Computing and M-Commerce", International Journal of Computer Science & Engineering Survey (IJCSES) Vol.6, No.2, April 2015, pp 29-45.
9) F. Li et al., Analysis Of An Identity-Based Signcryption Scheme In The Standard Model, IEICE Transactions On Fundamentals Of Electronics, Communications And Computer Sciences E94-A (1), 2011, pp. 268–269.
10) B. Libert and J.J. Quisquater, "A New Identity Based Signcryption Schemes", In: 2003 IEEE Information Theory Workshop, Paris, France, 2003, pp. 155–158.
11) Mahmoud Elkhodr Et Al., "A Proposal To Improve The Security Of Mobile Banking Applications", IEEE International Conference On ICT And Knowledge Engineering, 2012.
12) Sumit Chakraborty, "Mobile Commerce: Secure Multi-party Computation & Financial Cryptography", Technical Report / MCSMCFC/ V1.0 15082015, 2015, pp. 1-13.
13) P.Subhasri and Dr.A.Padmapriya., "Enhancing the Security Of Dicom Content Using Modified Vigenere Cipher", International Journal of Applied Engineering Research, Volume: 10(55), January 2015, pp. 1951-1956.
14) B. Zhang, "Cryptanalysis of an Identity Based Signcryption Scheme without Random Oracles", Journal of Computational Information Systems 6 (6), 2010, pp. 1923–1931.

ISSN: 2233-7857IJFGCN