American Journal of Engineering Research (AJER) 2015
American Journal of Engineering Research (AJER)
e-ISSN: 2320-0847 p-ISSN : 2320-0936
Volume-4, Issue-11, pp-143-149
www.ajer.org
Research Paper Open Access

Secure SMS Mobile Transaction with Peer to Peer Authentication Design for Mobile Government

Mohammad Khalaf Rahim Al-juaifari
Mohammad.aljuaifari@uokufa.edu.iq
University Of Kufa-Iraq

Abstract: *Currently, many researches in Mobile government secure transmission of plaintext with universal availability in all GSM networks had been proposed. The most important characteristic of this research is a new system that contains all the capabilities and plugging security holes in the algorithms and methods used in previous systems design. The main reason of the intensification of efforts for the purpose of security in a mobile government is the real threat that accompanies the movement of transaction from the sender to the recipient. Moreover, mobile government used in improving convenience is one the clearest manifestations of the development of society and solving various problems using other method related to availability, speed, financial, in addition to the administrative issues related to the fight against corruption side a side with E-government. In this paper, illustrating how a mobile phone can provide citizens and Non-government organizations with mobile government services relevant to the design and implementation of security mechanisms coinciding with the birth of the third generation technology in Iraq so as to ensure the highest level of security transaction provided by UMTS security is also built upon GSM network.*

Keywords: *SMS* (Short Message Service), *Mobile Government (M-government), Electronic Government (e-Government), Global System for Mobile (GSM), third-generation (3G), Universal Mobile Telecommunications System (UMTS), 3GPP (Third Generation Partnership Project), OTP (One Time Password), GSM (Global System for Mobile Communications),SHA (Secure Hashing Algorithm), Elliptic Curve Digital Signature Algorithm (ECDSA), message digest (MD).*

I- INTRODUCTION

The entry of mobile phones in the online world, the opportunity that mobile phones offer has pulled more people into the wireless world, and citizen-mobile related services such as voice communication, but is also used in governance, Mobile Democracy and many more. M-Government combines both terms 'mobility' and 'e-Government' and Offers a lot of potential like: availability (more people is on), speed, better administration, saving cost & time …etc. Generally, text, voice, sound or image message sent over a public communications network is called (SMS), which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient. There is no such scheme that support complete SMSs security, Lack of security still the main issue in mobile government although a lot of numbers of SMS-based mobile protocols have been proposed. For instance, SMS based transactional services available in UK, Europe, and many cities across North America after the telecom industry de-regulation and adoption of UMTS is a so-called "third-generation (3G)," broadband, packet -based transmission of text, digitized voice, video, and multimedia at data rates up to and possibly higher than 2 megabits.

In [1] describes the wide using of SMS day by day as in figure 1 shows the increasing use of SMS from 2006 to 2016. 2014, 2015 and 2016 is forecasted.

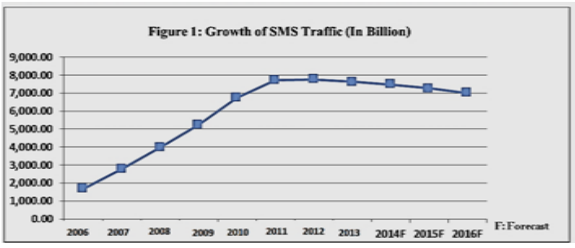


Fig. 1: Growth of SMS Traffic

Increasing may happened because more organizations used communication with their client and others, Mobile phones now have 5G,4G, LAN and WLAN connectivity not only 3G, use 3G in proposed system that including simulates the reality of the current communication technology in Iraq.

Biometric protection considered as costly way in case they are used in the security system of government mobile and other internet applications, especially when designing an authentication for customers, so in the system OTP algorithm using which allows executing password once by preventing trying to predicate password using irreversible and random sequence.

The main objective of this paper is to show how mobile phone can serve citizens and firms in mobile government. Hence, it provides different services to citizens. It is developed as a new technique to deliver service and the government transfer make citizens easy to access public services. The changes in the Internet and World Wide Web technologies and services lead to new developments in the way e-government efforts provide services to citizens and businesses, and in the way governments handles their internal operations. Frontline SMS project1 aims to Frontline SMS allows data exchange between remote entities (PCs, Laptop, etc.) based on SMS messages. Another example one of the revolutionary developments comes from adoption of wireless mobile technologies in government related activities: m-government to present technological drivers of m-government and present cases where these technologies are being used. Finally, concludes with discussions of mainly security challenges for m-government implementations currently and in the future.

II- RELATED WORKS:

By default SMS does not guarantee confidentiality and integrity to the message content. Therefore SMS is not totally secure and reliable [2]. In [3] Mobile Government: 2010 and Beyond has been finalized with the contribution and effort of several supporters of m-government.

Although modern smart phones provide users a variety of different communication capabilities, SMS technology is still favored all over the world (MBAONLINE, 2011). The popularity of SMS technology has led to a plethora of SMS based services. Also the public sector tries to make use of SMS technology's popularity. SMS based m-Government services can already be found in various countries around the world. Comprehensive overviews of existing SMS based projects and initiatives are given in (Mobile Solutions Ltd, 2010) and (Zefferer, 2011). SMS has played an essential role in developing countries for many years. Especially in rural areas, reliable fixed-line communication networks are often not available. Contrary, mobile communication networks are often well evolved even in underdeveloped regions. Yet, they are limited to GSM technology most of the time. The consequent restriction to telephony and text messaging improve communication capabilities in regions with underdeveloped infrastructures. For instance, an SMS based service is Kenya's Blood Bank-SMS project2. Due to missing reliable fixed-line communication networks, statuses of blood banks are exchanged via an SMS based service between different hospitals. A lot of trying to develop new system easier to manage, independent of SMS gateway, and less expensive such as in [4].

There are various other SMS based services from the health sector available in developing countries. In South Africa, citizens can request location information on HIV testing centers via SMS. Text to Change3 is a health education initiative that aims to inform people in developing countries about diseases such as malaria or AIDS using text messaging technologies. In developed countries, reliable fixed-line communication networks are usually well evolved. Mobile communication networks are thus just one out of multiple communication and information alternatives and mainly used to satisfy demands of the typical western always-on society. Hence, SMS based services in developed regions differ from those of developing countries in various aspects. In fact, most existing SMS based services aim to improve convenience. For instance, in various European cities parking fees can be paid via text messages4. In Norway, also tax declarations can be done with the help of SMS messages5, which has significantly eased the entire tax declaration process for citizens. Various countries in both developing and developed regions make use of SMS to broadcast relevant information to their citizens. For instance, in Venice, Italy, citizens are supplied with flood warnings per SMS6. In London, UK, the Metropolitan police forward bomb alerts and similar security warnings to registered citizens via SMS7.
Nowadays, the (3GPP) is responsible for the development and has led to the development of various useful SMS based services. In [5] SMS is a popular medium for many Services such as mobile banking, news alerts etc...

In such scenarios, SMS based transactional services can be useful, The approach introduced in this paper implements transactional services on SMS basis and incorporates electronic signatures to meet security requirements of such services. In addition, it is also possible to use a SIM card to perform certain cryptographic

operations, while executing the remaining part of the application through the ME, like in the mobile payment scheme presented by Hassinen et al. [6].

With Internet rapidly developing, SMS with e-commerce plays an important role in business transactions and is conducting business communications and solutions over the networks and through computers and mobiles [7] to give limitations of SMS technology, most SMS based services are rather informational than transactional. This is reasonable since transactional services can have higher security requirements that are difficult to meet with SMS based approaches. Therefore, transactional services are traditionally provided through web based approaches, which allow an easier integration of cryptographic methods such as electronic signatures. Unfortunately, there are scenarios in which web access is not available and web based services cannot be accessed. The term SMS refers Short Message Service SMS stands for Short Message Service. It is a technology that enables the sending and receiving of messages between mobile phones. SMS first appeared in Europe in 1992. Later it was ported to wireless technologies like CDMA and TDMA.GSM and SMS standards were originally developed by ETSI. ETSI is the abbreviation for European Telecommunications Standards Institute. maintenance of the GSM and SMS standards has been done by [7]. (GSM) is the most popular standard for mobile telephony systems in the world [8].

There is a need to provide an additional encryption on the transmitted messages and Global Service for Mobile communications with the greatest worldwide number of users. As suggested by the name SMS, data that can be held by an SMS message is very limited. One SMS message can contain at most 140 bytes (1120 bits) of data, so it can contain up to [9].

III- Proposed Solution:

The system implied OTP with digital signature for user authentication, OTP support to work with Applet running on a mobile phone or PDA. OTP via SMS text message, OTP is generated at a center and sent as a text message to the server side by using RADIUS protocol for validating the OTP values validating Active Directory, Lightweight Directory Access Protocol and internal database. The OTP value is passed as a standard RADIUS request to the vendor-specific OTP authentication server.

A signature generates with user's signing key in case of matching password authentication and the OTP authentication. After applying Ciphering on SMS, electronic signatures applied to meet the requirements for integrity of digital data and non-repudiation of origin then transmitted signed encrypted SMS.
Proposed security mechanism should satisfy secure, easy to implement no storage of secret cryptographic keys,

3.1. The M-GOV Infrastructure:

M-GOV Infrastructure designed to achieve trust and confidence, authentication, integrity, confidentiality and non-repudiation. Storage of documents so as to ensure the security and integrity preservation in addition to the possibility of data retrieval and update ... Fig. 2 describes the M-government conceptual infrastructure, whose components are described in short in the following.

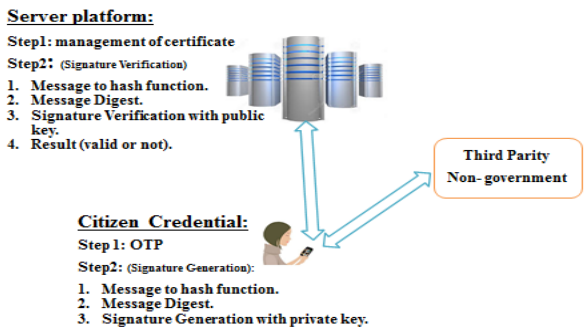


Fig. 2: M-government infrastructure

By providing appropriate credentials, Citizens and M-Government can be securely mutually authenticated and communicate using digital signatures and certificates. Public Key Infrastructure can be considered as public authorities, third party and notarization services entities. Notarization services contain time stamping, digital signing and secure storage to be available for third parity. In [10] supports authentication and confidentiality

implemented through the RSA, DSA and ECDSA signature schemes. Main aspects of proposed system consist of three modules these are achieving entity authentication, and achieve key exchange.
First is Initialization: Installing the application software on the user's mobile phone, PDA, tablet etc. registering the user details into the system, generating the user name and password for Citizens. **Second is OTP:** It is a password that is valid for only one login session or transaction.
OTP in [11] security supported by preventing stealing password then hacker should control phone in addition to user name and password. OTP Programs run on mobile device to provide a PIN with token that change with time and implement the confidentiality by encrypting the message using a symmetric secret one-time password. The one-time password is only shared between the citizen and the server. The strength of the confidentiality depends on the security strength of the passwords generation algorithm. It is assumed that only the authorized users will know his passwords.

Third is Secure Message is protocol used to implement the integrity of the message digest, the hashed value of the message content calculated server application and the mobile phone application. If the content is altered during transmission, the hashing algorithm will generate a different digest value at the receiver side. If the digests mismatch, the receiver will know that the integrity of the message has been compromised.

III- Secure Message method:

3.1 Proposed System Design:

A new system shown in figure 3 has been proposed starts from sender side (message handler) and installing the application in mobile phone then register the user by The following points represent the procedures that used to design proposed system:

- UTMS networks media that proposed in the system.
- The security and efficiency of this protocol is analyzed.
- Hashing algorithm applied on the message before transaction operation.
- The MD is then inputted into a Digital Signature Algorithm (DSA) which generates/verifies the signature for the message.

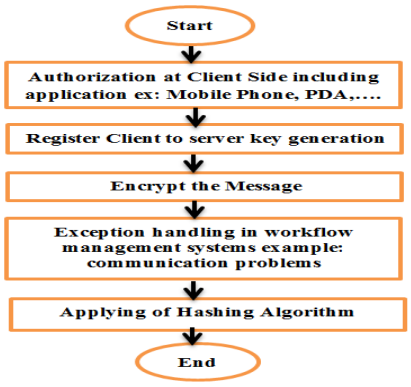


Fig. 3: Proposed Procedure Diagram

Figure 4 shows that SMS is comprised of the header and the payload (which is the content of the message). The header provides four bytes to specify metadata and the size of the payload. The maximum length of the payload is usually 160 characters at 8-bit per character.

User Data Header (instructions)	Sequence Number (instruction)	Data Length (instruction)	Payload . . padding	Variable bit MAC

Fig. 4: SMS message structure

3.2 SHA-1 Algorithm: used for applying user name and password after that encrypting the message operation.

3.2.1 SHA-1 features:

In this part of proposed system is SHA-1 which have the properties of: its outputs a 160 bits digest of any sized file or input, uses a 512 bit block size and has a maximum message size of 264 -1 bits, word size 32 bits, 80 rounds, and internal state | output size is 160 bits without having conditions on the chaining variables.

Other SHA-1 characteristics are:

- Different messages that produce the same MD.
- Any changes made to the messages will result in a different MD.
- Signing the MD makes the message more efficient since the MD is a smaller size then the message.
- The same hash function is needed to verify the message.
- SHA-1 is computationally infeasible to find a message that corresponds to a given MD.

A secure Hash Algorithm (SHA) is necessary to ensure the security of the Digital Signature Algorithm (DSA).

Each round uses a different K and different nonlinear mixing function f in figure below:

3.2.2 SHA-1 Algorithm Framework:

Step 1: Append Padding with and 0's Bits makes message length to 64 bits less than an even multiple of 512.

Step 2: 64 bits are append Length to the end of the padded message.

Step 3: Prepare 80 processing functions

Step 4: Prepare 80 processing constant words

Step 5: buffers of words (32 bits)

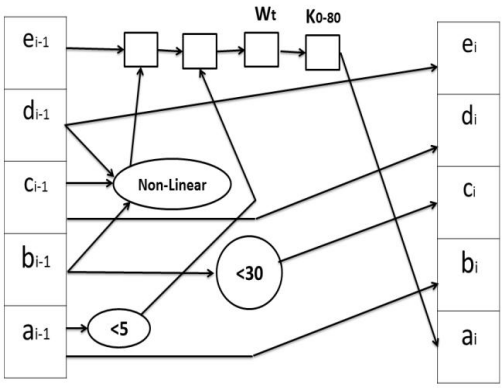


Fig. 5: SHA-1 block diagram

As shown in figure 5 above the description of following are:

X1 (output) = M1 (512 bits) +x0 input (160 bits); where m1 expand from 512 to 2560 bits.

Initialization is 4 rounds of (20 iterations each) repeat algorithm on the procedure until compressing whole messages in to single 160 bit vector.

Initialize four rounds of 20 iterations each distributed from k0 to k80.

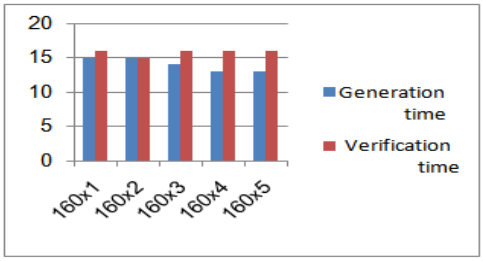


Fig. 6: ECDSA with SHA-1 Digital

IV- Implementation:

Programming Platform can be implemented by using Java Micro Edition (J2ME).net framework and others with corresponding data base connectivity.

Fig. 7: Client side Registration to M-Government

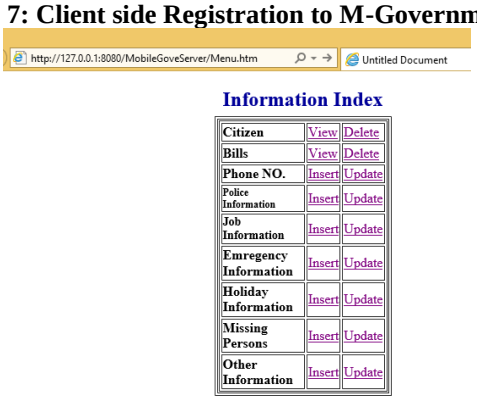
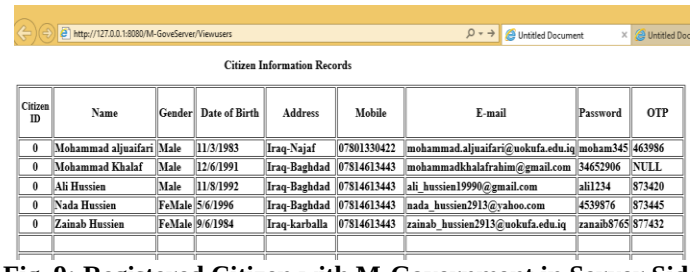


Fig. 8: Citizen Information (Editing Page Server Side)



Citizen ID	Name	Gender	Date of Birth	Address	Mobile	E-mail	Password	OTP
0	Mohammad aljuaifari	Male	11/3/1983	Iraq-Najaf	07801330422	mohammad.aljuaifari@uokufa.edu.iq	moham345	463986
0	Mohammad Khalaf	Male	12/6/1991	Iraq-Baghdad	07814613443	mohammadkhalafrahim@gmail.com	34652906	NULL
0	Ali Hussien	Male	11/8/1992	Iraq-Baghdad	07814613443	ali_hussien19990@gmail.com	ali1234	873420
0	Nada Hussien	FeMale	5/6/1996	Iraq-Baghdad	07814613443	nada_hussien2913@yahoo.com	4539876	873445
0	Zainab Hussien	FeMale	9/6/1984	Iraq-karballa	07814613443	zainab_hussien2913@uokufa.edu.iq	zanaib8765	877432

Fig. 9: Registered Citizen with M-Government in Server Side

Hash function is needed to verify the message. The MD is then inputted into a Digital Signature Algorithm signature generation and verification

Based on [9] develops digital Signature algorithm based on ECDSA and results shows that signature generation and verification using of ECDSA is better than DES, AES RSA, ElGamal, and Blowfish due to low computational power since it provides high security than the default cryptography in use on the web with smaller key size.

By applying one time password algorithm with message digest in proposed system as shown in figure below:

Fig. 10: Message Digest Implementation

MD5 for encrypting and decrypting message: user name and password: The SHA-1 for text mohammadkhalaf is: 2c29979418c4daebd7d31b53350ded2ecff450ea
(DSA) Which generates/verifies the signature for the message. Runs in 80 rounds.

REFERENCES

[1] Growth History of SMS Source: PortioResearchLtd. http://www.portioresearch.com/en/blog/2013/the-15-trillion-$-dollar-story-of-sms.aspx

[2] "A Security M'echanism for Secure SMS Communication" HULISANI RATSHINANGA, JOHNNY LO AND JUDITH BISHOP.

[3] Computer Science Department, University of Pretoria, South Africa hratshin, jlo, jbishop @cs.up.ac.za Mobile Government: 2010 and Beyond white paper,2010.

[4] Salman Firdaus bin Haji Sidek, "The Development of the Short Messaging Service (SMS) Application for the School Usage", 978-1- 4244-6716-7/10/$26.00, 2010@ IEEE, pp 1382-1386

[5] C.Narendiran, S.Albert Rabara, N.Rajendran,"Performance Evaluation on End-to-EndSecurity Architecture for Mobile Banking System", 2008@IEEE.

[6] M. Hassinen, K. Hypponen, and K. Haataja, "An Open, PKI-Based ¨ Mobile Payment System," in ETRICS, 2006, pp. 86–100.

[7] M. Toorani and A. BeheshtiShirazi, "SSMS - A secure SMS messaging protocol for the m-payment systems", in Computers and Communications, IEEE Symposium on, July 2008@IEEE, pp 700–705.

[8] Nassim Khozooyi, Maryam Tahajod, Peymankhozooyi, "Security in Mobile Governmental Transactions", 2009 Second International Conference on Computer andElectrical Engineering, 978-0-7695-3925-6/09 $26.00 © 2009 IEEE, pp 168-172.

[9] Alfredo De Santis, Aniello Castiglione and Umberto Ferraro Petrillo "An Extensible Framework for Efficient Secure SMS" International Conference on Complex, Intelligent and Software Intensive Systems, 2010@IEEE, pp 843-850.

[10] Neetesh Saxena and Narendra S. Chaudhari "Secure Encryption with Digital Signature Approach *for Short Message Service" , 2012 World Congress on Information and Communication Technologies Stefan Certic "The Future Of Mobile Security"*

[11] *CS Network Solutions Limited http://www.cs-networks.net*

[12] *Neetesh Saxena , Narendra S. Chaudhari " Secure Encryption with Digital Signature Approach for Short Message Service", 2012 World Congress on Information and Communication Technologies.*