International Journal of Wireless Communications and Mobile Computing
2016; 4(4): 62-67
http://www.sciencepublishinggroup.com/j/wcmc
doi: 10.11648/j.wcmc.20160404.11
ISSN: 2330-1007 (Print); ISSN: 2330-1015 (Online)

Security of VAS-SMS Services in 3G, for TV & Radio Programs

Saad Abdalratha Makki, Hasan Kadhim Alsuwaiedi

Department of Computer Science, College of Education, Almustansiriah University, Baghdad, Iraq

Email address:
drsaadamakki@yahoo.com (S. A. Makki), alsawedi@yahoo.com (H. K. Alsuwaiedi)

To cite this article:
Saad Abdalratha Makki, Hasan Kadhim Alsuwaiedi. Security of VAS-SMS Services in 3G, for TV & Radio Services. *International Journal of Wireless Communications and Mobile Computing.* Vol. 4, No. 4, 2016, pp. 62-67. doi: 10.11648/j.wcmc.20160404.11

Received: July 29, 2016; **Accepted**: August 5, 2016; **Published**: August 21, 2016

Abstract: The modern telecommunication is spread in every day live especially after 3G technologies and beyond. The traditional mass media (TV & Radio) stations has also influenced and get dramatic changes by the new information technologies. So the partnership between the carriers and the traditional media was Inevitable. Also contribution of the third party which called Mobile Value Added Service (MVAS) companies that works between the carriers and the traditional media as a joint support station, for both main parties. Value added services (VAS) in telecom is considered as a new financial source to the cellular companies beside its classical work (e.g. phone calls or fax). This type of services found its way to TV & Radio stations through the benefits from the huge audience or followers they got. One of the main VAS services is the SMS service, in which all the previous three parties try to get their share from the revenue. The security of SMS information is an important issue, to prevent the fabrication or changing the information flows between parties. This paper suggest and provide digital signature security method as a new mechanism that guaranties the security services concerned with SMS flows between all companions. Providing the SMS with the needed authentication and integrity to the weakest point in the flow scheme, which are the TV stations. The target is to overcoming the security threats for all partners, taking 3G component under consideration as the main new technology implemented in Iraq and Iraqia-TV station is taken as example.

Keywords: SMS Security, VAS in TV & Radio Programs, VAS Companies, Content Providers

1. Introduction

SMS is an umbrella for many applications e.g. MMS and WAP [1]. SMS considered as one of the top services that has been provided by mobile phone companies. Where it is viewed as the primary data services introduced in 2G and beyond generation [2]. It has been used in many applications such as mobile banking, healthcare monitoring, salary payment [3] and registration in election [4] etc. Value Added Services (VAS) in telecommunications are considered as a new services beside its classical work (e.g. phone calls or fax) and as new profit source to the mobile operator companies. The cellular companies do their VAS services (e.g. ringtone music, caller-ID, Voice-SMS...…etc.) and other services are done by an independent Mobile VAS (MVAS) companies (e.g. SMS news broadcasting, advertising SMS or bulk SMS, Games….etc.) [5]. MVAS company considered as a third party sometimes can handle the content provider like Reuters, the international news agency, or Iraqia broadcast network, which has been used in our study as a case study.

Figure 1. Shows the current relationship between the three parties. The audience plays a major part when they watching TV shows and participating in this TV shows, by sending a short message SMS, to the short-code number that they see in the screen, which represent one of the carriers.

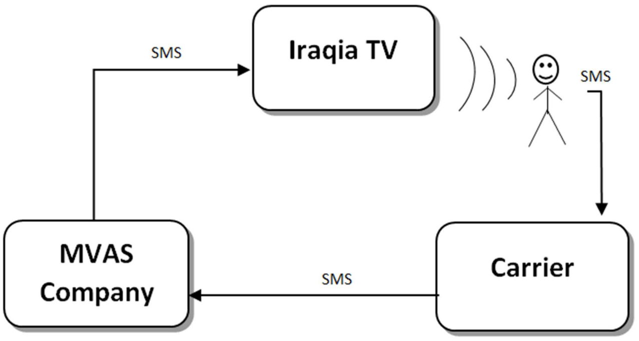


Figure 1. *The current SMS flows of the three parties.*

Inside the carrier the messages are aggregated in a database of the SMS Serving Center (SC) [6]. Which in turn, redirected the SMS to ESME (External Short Message Entity) which is:-

1. A mobile station signed within the same network or another one.
2. A computer server connected directly to SC working as the incoming port of SMS services, it could be owned by Mobile Value Added Services companies or owned by the operator itself.
3. A computer connected to the internet, allowed to send/receive short message [7].

In our situation it has been dealt with stat two above. Where the gathered short messages directed to MVAS company, which in turn, either do a manipulation on SMS messages or directed them directly to Iraqia-TV station to do the necessary processing, according to the TV show (wither it is a lottery show or else). Then, showed the final result to the audience. All that flow of SMS data happened without any security mechanism, in any part of the three parties.

The possible threat in this situation:-

a). Minimize the number of the total SMS messages by the carrier company.

b). Minimize the number of the total SMS messages by the MVAS Company.

c). Forge or tamper in the content of some SMS messages by the carrier Company.

d). Forge or tamper in the content of some SMS messages by the VAS Company.

Obviously all the above threats may happened for financial reason, to increase the profit of one party from another. The main security services her, are the Integrity “the SMS cannot be tampered by the intruders, the system should be able to find out such alteration”. And the Authentication “each party has the ability to authenticate the other party” [8]. Other security services (secrecy or Non-repudiation) are not an issues her because the SMS data are a commercial data and not high military data or else.

The main objective of this paper is to show a new security proposal that can a sure the integrity and the authentication of the SMS flows between the cellular company and the MVAS company and the Iraqia-TV station, by using the digital signature mechanism inside MySQL database server.

2. Related Works

In our proposal it have been used the security of SMS inside MySQL database server. So it’ll be explained a combination of the related works for the two fields, the SMS security and the MySQL security.

In 2011, Nanda and Awasthi analyzed Joint Channel Coding and Cryptography and Soft Input Decryption and proposed two algorithms to be used in SMS security. NTRUSign [9] and XTR – NR Signature [10].

In 2012, Saxena and Chaudhari performed research [11] in securing SMS with a variant of ECDSA. Also, Saxena, Chaudhari, and Prajapati [12] proposed an encryption approach that used a password-based key exchange protocol based on Diffie-Hellman and generated a shared secret-key which could be used in message encryption as well as in MAC functions.

In 2013Geovandro C.C.F. Pereira [13] submit a SMSCrypto encloses a tailored selection of lightweight cryptographic algorithms and protocols, providing encryption, authentication and signature services.

In 2014, Saxena and Chaudhari [4] proposed a protocol called EasySMS which provides end-to-end security during the SMS transmission. This solution puts key management on the control of Mobile Network Operator. In 2014 Fahrianto, Masruroh, and Ando [14] Saied that a combination of two ciphers Caesar and Vinegére was good enough to protect the secrecy of SMS. Also in 2014, Patil, Sahu, and Jain [15] studied SMS compression in order to minimize the overhead of payload due to encryption, and proposed a method for compression of SMSs after encryption using Elliptic Curve.

In 2015, Alexandre and Romulo [16] submitted an “Implementation Issues in the Construction of an Application Framework for Secure SMS Messages on Android Smartphones” which Constructed of the application framework called “CryptoSMS” for SMS security that provides encryption, integrity, authentication, and non-repudiation for SMS messages. By using an asymmetric algorithm, such as RSA-OAEP or ECIES.

In 2015, Mohammad Khalaf [17] proposed a Secure SMS Mobile Transaction with Peer to Peer Authentication Design for Mobile Government. By applying Ciphering on SMS, electronic signatures applied to meet the requirements for integrity and transmitted signed encrypted SMS by using SHA-1 Algorithm& digital Signature algorithm based on the Elliptic Curve Digital Signature Algorithm (ECDSA), between client-server systems which provide services to citizens in mobile government as mobile application.

3. Proposed Solution

The proposed solution is to provide security to the SMS messages that’s flows between the three main components/parties (Carrier or Mobile Phone Network, MVAS Company, Iraqi-TV station). The security are especially concerned in the Authentication and Integrity of SMS’s. The authentication is made basically by using the username and password of everyone has the authority to enter to the server system. Also there is another username and password for the authorized persons, who enter the main DataBase (schema) that stored all SMS information in the SMS Center of the carriers.

Either about integrity it have been used the Hash function (SHA 512) and also used the Advanced Encryption Standard AES, which both combine the Digital Signature, to encrypt the SMS schema that hold by the system server in SMS Center.

The security was done in this mechanisms to prevent any dishonest party from doing manipulation to the SMS data. Causing of, reducing the revenue earned to Iraqia-TV or other parties.

This manipulation may reduce the total amount of SMSs or changing its content, to get advantage of the races that happened in TV shows of Iraqia-TV. Either about the secrecy (confidentiality) of the SMS contain it is not a matter of issue in our proposed security server system, because it have been dealing with a commercial SMS, concerned in TV show programs. Not in high military secret information or else. So the digital signature (Hash plus AES encryption) will be done, in the sending side, and be decrypted in the receiving side, to provide the needed security mechanisms.

Also it is important to know that the link between the three parties depend on public internet lines. To protect SMS flows during transmission we depend on the internet protocols security.

To build a security program that can provide, the security mechanisms to the SMS, this system has to work side by side with the standard infrastructure wither inside the carriers (especially in the SMS Center) or outside. It will name the new proposed program as Signature SMS System (SigSms Sys. As short). Therefore the system, supposed to work, either inside the carrier telecommunication company see Figure 2. As a first idea, and will receive its SMS messages data from the database that reside in the SMS Center. Without any process inside Iraqia-TV, just a web-page as interface for viewing the SMS data.

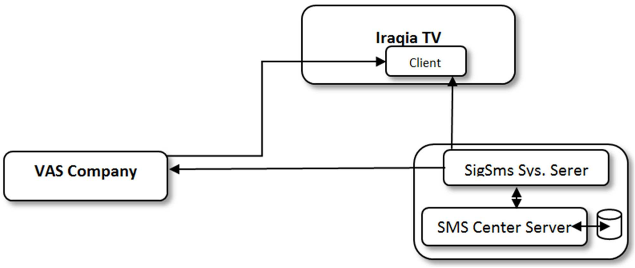


Figure 2. *The first idea of SMS security flows.*

The second idea is that the SigSms Sys. Will reside only in the Iraqia-TV station and will receives its SMS message data from the database that reside in the SMS Center, side by side with the MVAS Company, in this situation the digital signature are meaningless. As showed in Figure 3.

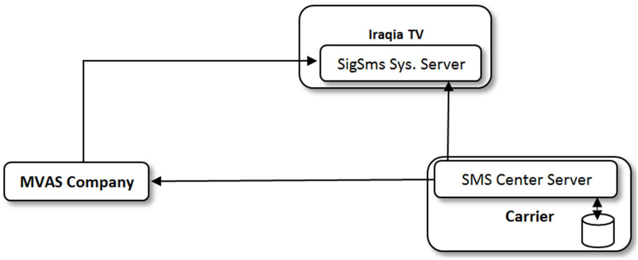


Figure 3. *The second idea of SMS security flows.*

If it is taken the cons and pros of first idea, it’s difficult to get the agreement of Carriers Companies to put outside server program, inside their company SMS Center, Of course for security rezones. Although it’s better to make a digital signature to the SMS data before send it to the MVAS Company, to avoid their manipulation on SMS data before sending them to Iraqia-TV, Also its better to send the SMS data to Iraqia-TV with a digital signature to avoid internet threats.

For the second idea, when both Iraqia-TV & MVAS Company receive the SMS data from the same table in the specified schema. And avoid the security sensitivity of Carriers companies. But the public internet lines security are still matter of issue in this idea, without a digital signature to the SMS data.

So it is better to combine between the previous two ideas, and producing a final proposal, providing the requirements for all the three parties, by making a partnership agreement with the carrier company to remove their security sensitivity. Making the SigSms System Server in both sides in the carrier company side, and in the Iraqia-TV side. As showed in Figure 4.

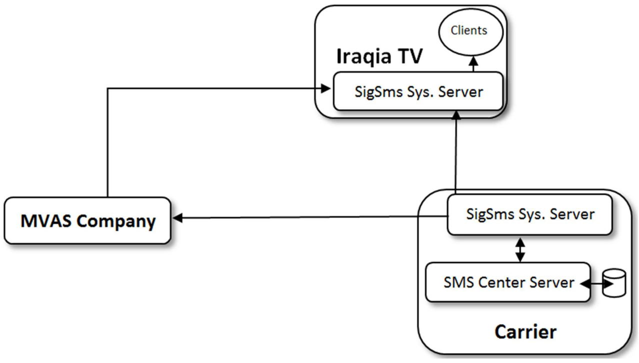
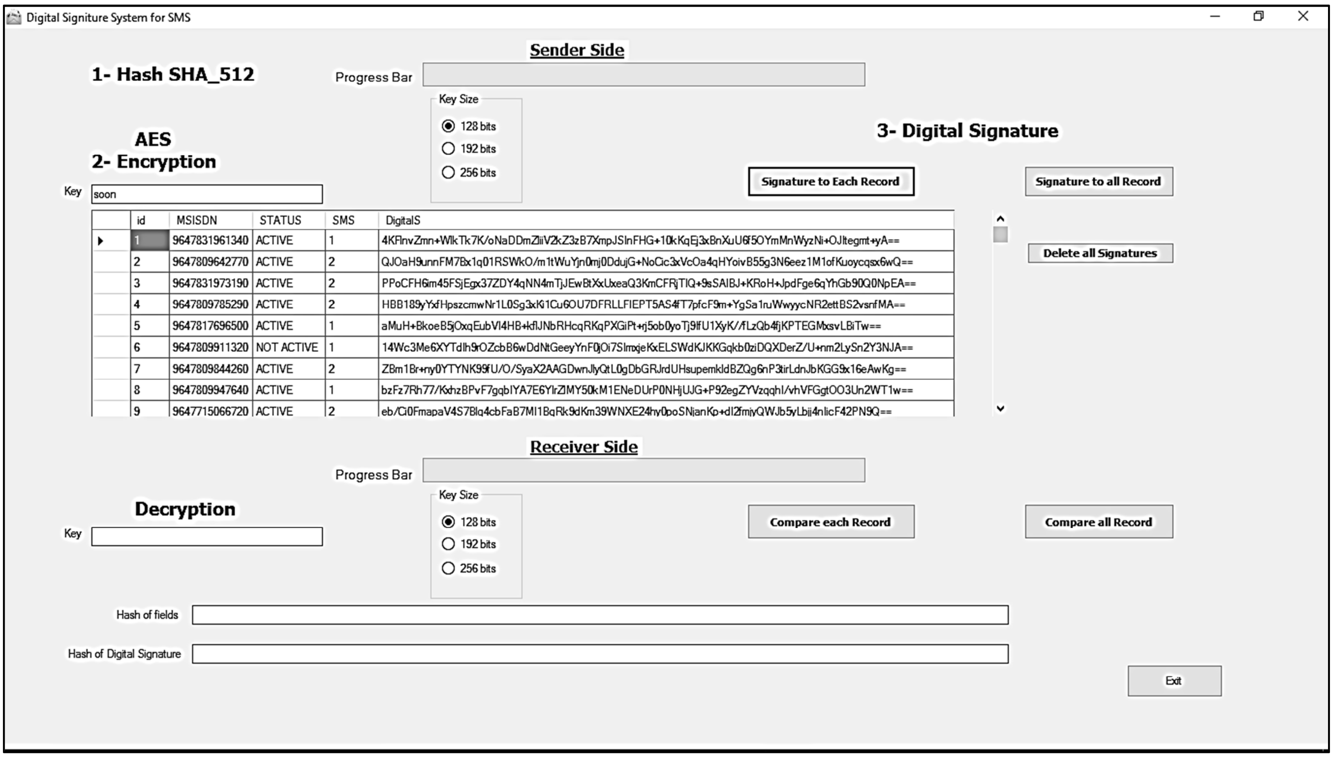


Figure 4. *The new proposed system of SMS security flows.*

4. Practical Implimentation

After building the SigSms System Server, by using the Visual C++ inside the Visual Studio 15 environment, it can be seen the main interface window as in Figure 5. With a sample of database. Showed that each record has got its own digital signature. Separating the main program window into two sides, sending and receiving sides, to simulate the real work between the Carrier and Iraqia-TV. Also it can see the fields of the record that have been created (Id, MSISDN, STATUS, SMS, DigitalS) which represent the needed information to transmitted SMS.

- Id: represent the primary key for the record.
- MSISDN: the phone number.
- STATUS: the condition of the number was verified as ACTIVE or not
- SMS: sms content
- DigitalS: the digital signature of the fields in the same record



Key: soon

Key Size: ● 128 bits ○ 192 bits ○ 256 bits

	id	MSISDN	STATUS	SMS	DigitalS
▶	1	9647831961340	ACTIVE	1	4KFlnvZmn+WlkTk7K/oNaDDmZliiV2kZ3zB7XmpJSlnFHG+10kKqEj3xBnXuU6f5OYmMnWyzNi+OJltegmt+yA==
	2	9647809642770	ACTIVE	2	QJOaH9unnFM7Bx1q01RSWkO/m1tWuYjn0mj0DdujG+NoCic3xVcOa4qHYoivB55g3N6eez1M1ofKuoycqsx6wQ==
	3	9647831973190	ACTIVE	2	PPoCFH6im45FSjEgx37ZDY4qNN4mTjJEwBtXxUxeaQ3KmCFRjTlQ+9sSAIBJ+KRoH+JpdFge6qYhGb90Q0NpEA==
	4	9647809785290	ACTIVE	2	HBB189yYxfHpszcmwNr1L0Sg3xKi1Cu6OU7DFRLLFIEPT5AS4fT7pfcF9m+YgSa1ruWwyycNR2ettBS2vsnfMA==
	5	9647817696500	ACTIVE	1	aMuH+BkoeB5jOxqEubVl4HB+kflJNbRHcqRKqPXGiPt+rj5ob0yoTj9lfU1XyK//fLzQb4fjKPTEGMxsvLBiTw==
	6	9647809911320	NOT ACTIVE	1	14Wc3Me6XYTdlh9rOZcbB6wDdNtGeeyYnF0jOi7SlmxjeKxELSWdKJKKGqkb0ziDQXDerZ/U+nm2LySn2Y3NJA==
	7	9647809844260	ACTIVE	2	ZBm1Br+ny0YTYNK99fU/O/SyaX2AAGDwnJlyQtL0gDbGRJrdUHsupemkldBZQg6nP3tirLdnJbKGG9x16eAwKg==
	8	9647809947640	ACTIVE	1	bzFz7Rh77/KxhzBPvF7gqbIYA7E6YlrZlMY50kM1ENeDUrP0NHjUJG+P92egZYVzqqhl/vhVFGgtOO3Un2WT1w==
	9	9647715066720	ACTIVE	2	eb/Ci0FmapaV4S7Blq4cbFaB7Ml1BqRk9dKm39WNXE24hy0poSNjanKp+dl2fmiyQWJb5yLbjj4nlicF42PN9Q==

Key:

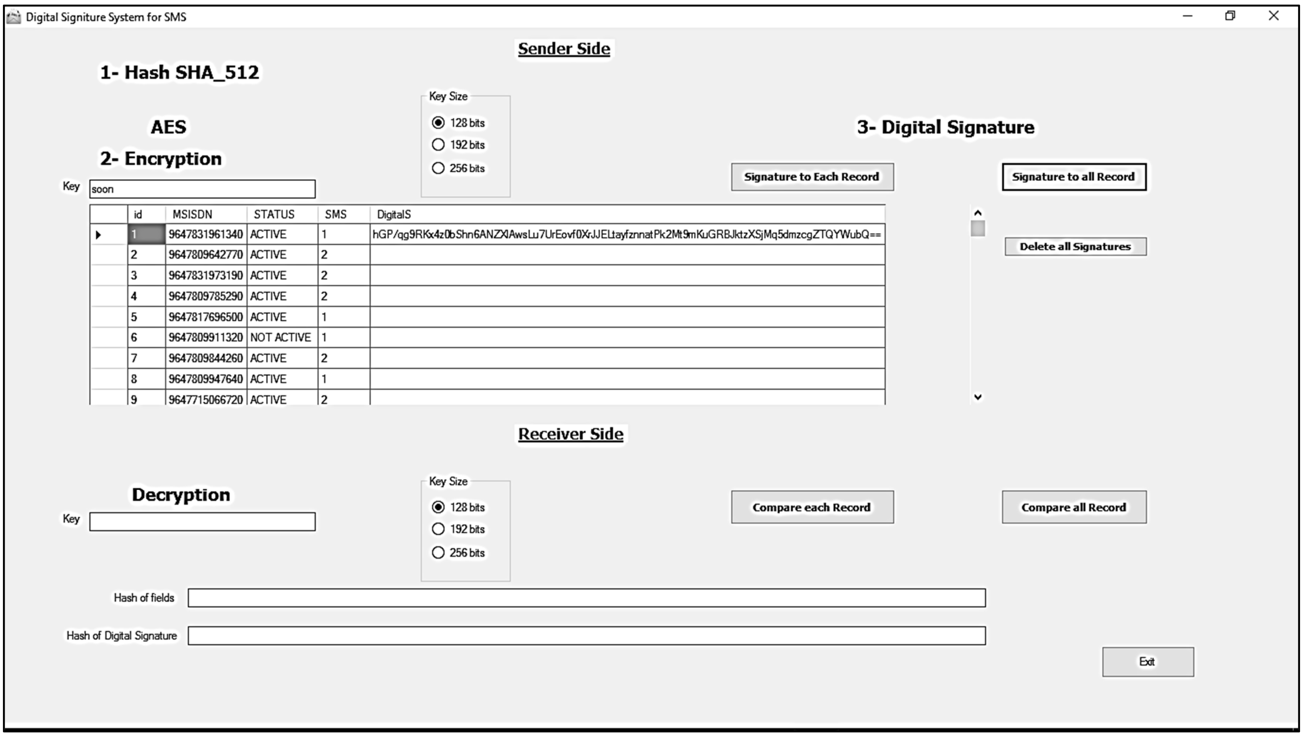
Key Size: ● 128 bits ○ 192 bits ○ 256 bits

Hash of fields:

Hash of Digital Signature:

Figure 5. *The main interface window of the SigSms System Server.*

Furthermore adding another function button to make a one digital signature to all the records in the database. Adding the comparison function buttons for each type of the previous digital signature. See Figure 6.



Key: soon

Key Size: ● 128 bits ○ 192 bits ○ 256 bits

	id	MSISDN	STATUS	SMS	DigitalS
▶	1	9647831961340	ACTIVE	1	hGP/qg9RKx4z0bShn6ANZXlAwsLu7UrEovf0XrJJELtayfznnatPk2Mt9mKuGRBJktzXSjMq5dmzcgZTQYWubQ==
	2	9647809642770	ACTIVE	2	
	3	9647831973190	ACTIVE	2	
	4	9647809785290	ACTIVE	2	
	5	9647817696500	ACTIVE	1	
	6	9647809911320	NOT ACTIVE	1	
	7	9647809844260	ACTIVE	2	
	8	9647809947640	ACTIVE	1	
	9	9647715066720	ACTIVE	2	

Key:

Key Size: ● 128 bits ○ 192 bits ○ 256 bits

Hash of fields:

Hash of Digital Signature:

Figure 6. *One digital signature for all records inside database.*

5. Performance Evaluation

During the testing and evaluation it has been used two type of database-table, a prepared information one, with hundred records. And another one, used an original information that have been got it from an Independent MVAS Company, about two thousands records concerned with one of the races in Iraqia-TV shows.

It has been used the most common structured query language (SQL) data manipulation statements (INSERT, UPDATE, DELETE and SELECT). In the code of database processing, that prove its efficiency in all common database.

The speed of processing proved its efficiency in handling all the records of database. Especially it haven't used any security-software, represent the Hash function or the AES algorithm. But it has been built both the Hash SHA512 and the AES algorithm from scratch.

The system have been built on a computer device that had an Intel Core duo 2.00GHz processor speed, with 3GB RAM, was working fine with hundred records. But with the increasing of the database amount it shows some delay. So it have been used alternative fast computer have a processor of Intel Core i5 2.50 GHZ and 4GB Ram. Which showed a better performance and fast result of digital signature for all database.

6. Concluation and Future Work

- Conclusion with regard to the SMS security has been specified as the following:-

a). It has been design and implement the SMS security system server (SigSms System Server) as a new proposal between the SMS-Center inside 3G network, and the External Short Message Entity (ESME) (which is a server connected to internet). Because of, that this part of SMS data flows security, wasn't covered before and all the last works concentrated on End-mobile user to End-mobile user security, or called End-to-End security.

b). All the SMS data that has been signatures, are taking from the SMS Serving Center (SC) Server database that belong to the Mobile Network company, receiving the SMS of the all mobile users, all that happened in real-time, which prevent the forgery and denial by the Mobile Network company, to the transmitted SMSs data.

c). It has been used the Secure Hashing Algorithm SHA512 bits and the Advanced Encryption Standard AES algorithm, which both improved their capabilities and strongest, in commercial application. Preventing any security threats.

d). It has been used the Client-Server MYSQL database rather than, using just a normal local database. To simulate the situation between SMS-Center and the External Short Message Entity (ESME).

e). It has been used, a user authentication to the SigSms System Server to prevent unauthorized users from login the system.

- Future work suggestions can specified as the following:-

a). It could be exclude the role of the MVAS Company, by built-in a separated technical department inside Iraqia-TV station by using the SigSms System Server, and working directly with the cellular company. Without the need to a third party, which reflect on increasing the financial side, and more technical flexibility on work between two partners, better than three. As found in the Middle-east Broadcasting Channels (MBC) TV network, who doesn't deal with any MVAS company.

b). It is better to use asymmetric key distribution techniques better than the symmetric key that have been used in SigSms System Server, to provide more security and avoiding the disadvantages of sessions-key.

c). It is better that SigSms System, to work with a more powerful computers, specialist in heavy processing, to get a fast-result in real time.

d). SigSms System Server can be developed to work with Multimedia Message Services (e.g. MMS) and cover all the VAS services.

References

[1] Minoru Etoh, Next Generation Mobile Systems 3G and Beyond, DoCoMo Communications Laboratories USA, John Wiley & Sons Ltd, 2005.

[2] Erik Dahlman, 4G LTE/LTE-Advanced for Mobile Broadband, Elsevier books, 2011.

[3] Santhi Mol P., A Survey on Different Protocols for Secure Transmission of SMS, International Journal of Engineering Research and General Science, July-August, 2015.

[4] Neetesh Saxena, EasySMS: A Protocol for End-to-End Secure Transmission of SMS, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, JULY 2014.

[5] Narayanan Anandpadmanabhan, VALUE ADDED SERVICES IN INDIA, Master Thesis Report, Royal Institute of Technology.

[6] G. Gomez and R. Sanchez, End-to-End Quality of Service over Cellular Networks Data Services Performance and Optimization in 2G/3G, John Wiley & Sons Ltd, 2005.

[7] Krzysztof Wesolowski, Mobile Communication Systems, JOHN WILEY & SONS, LTD, 2002.

[8] Neetesh Saxena, Enhancing Security System of Short Message Service for M-Commerce in GSM, International Journal of Computer Science & Engineering Technology (IJCSET).

[9] A. K. Nanda and L. K. Awasthi, "Encryption based channel coding algorithm for secure SMS," The World Congress on Information and Communication Technologies, 2011.

[10] A. K. Nanda and L. K. Awasthi, "Joint Channel Coding and Cryptography for SMS" The Int'l Siberian Conference on Control and Communications, 2011.

[11] Neetesh Saxena and N. S. Chaudhari, "Secure encryption with digital signature approach for Short Message Service," The World Congress on Information and Communication Technologies, 2012.

[12] Neetesh Saxena, N. S. Chaudhari, and G. L. Prajapati, “An extended approach for SMS security using authentication Functions”, 2012.

[13] G. C. C. F. Pereira, “SMSCrypto: A lightweight cryptographic framework for secure SMS transmission”, Journal of Systems and Software, 2013.

[14] Fahrianto, Masruroh, and Ando, “Encrypted SMS application on Android with combination of Caesar cipher and vigenere algorithm” The international Conference on Cyber and IT Service Management, 2014.

[15] M. Patil, V. Sahu, and A. Jain, “SMS text Compression and Encryption on Android O. S”, The Int’l Conf. on Computer Comm. and Informatics, 2014.

[16] Alexandre and Romulo, “Implementation Issues in the Construction of an Application Framework for SecureSMS Messages on Android Smartphones”, The Ninth International Conference on Emerging Security Information, Systems and Technologies, 2015.

[17] Mohammad Khalaf, “Secure SMS Mobile Transaction with Peer to Peer Authentication Design for Mobile Government”, American Journal of Engineering Research (AJER), 2015.