A new Simplified Security Proposal for VAS-SMS Services, between TV, Radio Stations and 3G Mobile Phone Networks.

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), Alsuwaiedi@gmail.com (H. K. Alsuwaiedi)

Abstract— Value Added Services VAS in Mobile-Phone-Networks, found its way to TV & Radio stations through the benefits from the huge audience or followers they got. Also the traditional media decides to get advantages of VAS services and consider it as a new revenue source. The traditional TV & Radio stations and the mobile phone network based on 3G technologies and beyond, both get dramatic changes by the new information technologies. So the partnership between the mobile-phone-networks and the traditional-media was unavoidable. The contribution of the third party which called MVAS (mobile value added service providers) companies that works between the mobile-phone-networks and the traditional media as a linkage ring station, for both main partners. The previous three parties try to get there share from the revenue of the VAS-SMS service. This paper suggest a new proposal based on excluding the role of MVAS companies by designing and implementing a New-SMS-Signature System, as a new Message Authentication Code MAC mechanism, that guaranties the Authentication & the Integrity criteria concerned with SMS flows between the traditional TV & Radio stations and the mobile phone network company. The target is to overcoming the security threats between the main two partners, without the need for a third part as MVAS companies, taking the Iraqi Media Network (IMN) as a case study.

Index Terms— Keywords: 3G Mobile Phone Networks SMS, VAS in TV & Radio Programs, VAS Companies.

1 INTRODUCTION

THE Short Message Service (SMS), consider as a basic service in the Global System for Mobile Communications (GSM) network, which enables to send a text message from one mobile-user to another, within the same network or another [1]. SMS is considered as one of the top services in 2G and beyond generation [2]. The SMS used for booking travel on trains and requests for delivery of goods, and in the protection systems for buildings and cars from thefts or fires. Recently have been used to authenticate the new users, of social media network web-site, such as, Facebook, Tweeter [3]. SMS also is used in many other application in everyday life [4]. Value added services (VAS) in telecommunications is considered as a new profit source to the mobile operator companies beside its classical work (e.g. phone calls or fax). The cellular companies do their VAS services (e.g. ringtone music, commercial voice-message...…etc.). Some other services are done by Mobile VAS (MVAS) companies (e.g. SMS news broadcasting, advertising SMS or bulk SMS, Games….etc.) because that mobile operator companies need to spread its VAS services and do not depend on its staff only [5]. The third party was the content-provider like CNN-TV channel, or Iraqi Media Network (IMN), which has been used in our paper as a case study.

Figure 1. Shows the current work and relationship between the three parties. The audience plays a major role, by sending a short message SMS, to the short-code number which they watching TV-shows or listening to Radio stations, sending SMS to a short-code number represent one of the mobile-phone company, as participating in this programs.

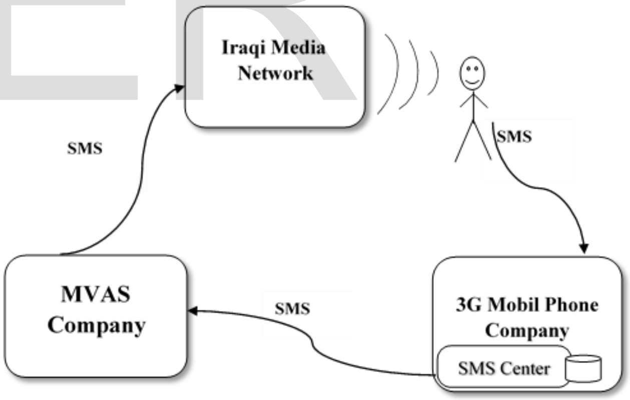


Figure 1. The SMS flows between the three partners

In the mobile phone network the messages are aggregated in the SMS Serving-Center (SC) inside a database server [6].which in turn, redirected the SMS to External Short Message Entity (ESME), which is one of these parts:-

1. A mobile-Phone 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 MVAS companies or owned by the operator itself.
3. A Personal computer (with a built-in SIM card) connected with the internet, allowed to Send/Received an SMS [7].

In our situation it has been deal with the above, point two.

Where the gathered SMS short messages directed to MVAS company, which in turn, either do a manipulation on SMS messages or directed them directly to IMN to do the necessary processing, according to the TV-show(wither it is a lottery show or else). Then showed the result to the participant audience.

Till now all that flow of SMS data happened without any type of security mechanism, in any part of the three parties. Where the possibility threats in this situation will be:-

- Minimize the number of the total SMS messages by the Mobil Phone Company and by the MVAS Company.
- Forge or tamper in the content of some SMS messages by the Mobil Phone Company and by the MVAS Company.

Obviously all the above threats may happened for financial reason, to increase the profit of one part than another. The first security services are the Integrity "the SMS cannot be tampered by the intruders, the system should be able to find out such alteration". The second is Authentication "each party has the ability to authenticate the other party" [8]. The third is Non-Repudiation "prevent the denial of contribution in communication process by one of the participant" [18]. Other security services (i.e. confidentiality) 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 based on excluding the role of MVAS companies from the whole process, and a sure the Non-repudiation, integrity and the authentication of the SMS flows between the mobile phone network and the IMN by using the SMS-Signature mechanism inside MySQL database server of the SC.

2 Related Works

It will be review the security of SMS from End-to-End user of mobile phone, which considered as the closest to the submitted proposal of this thesis. 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 the Non-Repudiation, Integrity and the Authentication to the SMS messages flows between the two components (3G Mobil Phone Network, IMN) and excluding the currently role of MVAS companies from the whole process. For the proposed system server it will call as SMS Signature System (SMS-Sig-Sys. As short). Authentication was made on the interface window of the SMS-Sig-Sys. By implementing the user authentication by demanding, the username and password of authorized users, who have the ability to enter the proposed system server. Also there is another type of authentication, which called database authentication, by demanding the username and password for the authorized users, who enter the main DataBase (schema) that stored all SMS information in the SMS- Serving-Center of 3G network.

The main authentication and integrity that have been used to the SMS flows during transmition between two parties, is implemented by using the Cryptographic Hash function (SHA2- 512bit) and also used the Advanced Encryption Standard AES, which both combine the SMS-Signature, which applied on the databases of SMS, inside the SMS Serving Center SC of 3G mobile network.

By using AES encryption it has been used a Secret Session-key between the transmition parties (3G Mobil Phone Network and the IMN). The Secret Session-key provide the authentication because just the sender and the receiver, knows that key.

For a best design environment, it have to take in consideration the location of the SMS-Sig-Sys server, that can provide the needed security service to the SMS flow, as it know that system have to work side by side with the standard infrastructure wither inside the 3G mobile network (inside the SMS Center) or outside the mobile network. As a first idea the proposed system, supposed to work, inside the 3G Mobile Network Company such as the figure 2, and will receive its SMS message data from the database that reside inside the 3G SMS-Center, without any process inside the Iraqi Media Network, worked just as interface to viewing data.

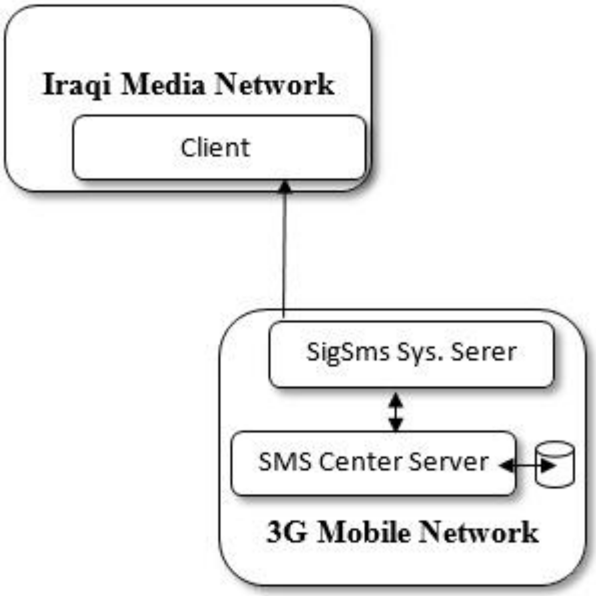


Figure 2. The first idea of System location

The idea of second location, the SMS-Sig-Sys. will reside only in the Iraqi Media Network and will receive its SMS message data from the database that reside in the SMS-Center As showed in the figure 3, in this situation the SMS-Signature considered a meaningless.

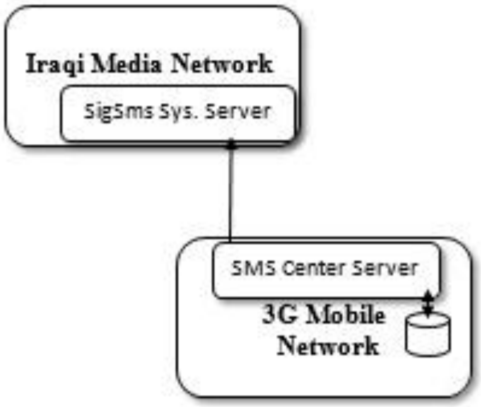


Figure 3. The second idea of System location

The Cons and Pros of first location, it is difficult to get the approval agreement of Mobile Phone Companies to put an outside system server inside their Companies SMS Center mostly that was for their security rezones. Although it is better to make the SMS-Signature to the SMS data before send it to Iraqi Media Network, to avoid internet threats on SMS data.

The Cons and Pros of the second location, when both IMN receive the SMS data from the database of SMS Center, by dealing with the security sensitivity of mobile phone companies. The SMS-Signature for the SMS data must be done in the sending-side, not in the receiving-side. Therefore it is better to combine between the previous two "location ideas" and produce a hybrid one, that can provide the suitable requirements for the two parties. By making a Partnership agreement with the 3G mobile phone company to remove their security sensitivity. Making the SMS-Sig-Sys Server in both sides, in the 3G mobile phone-side and in the Iraqi Media Network-side. As shown in figure 4

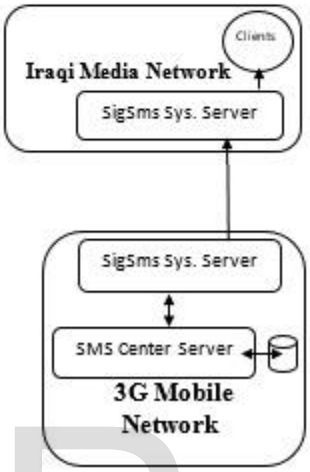
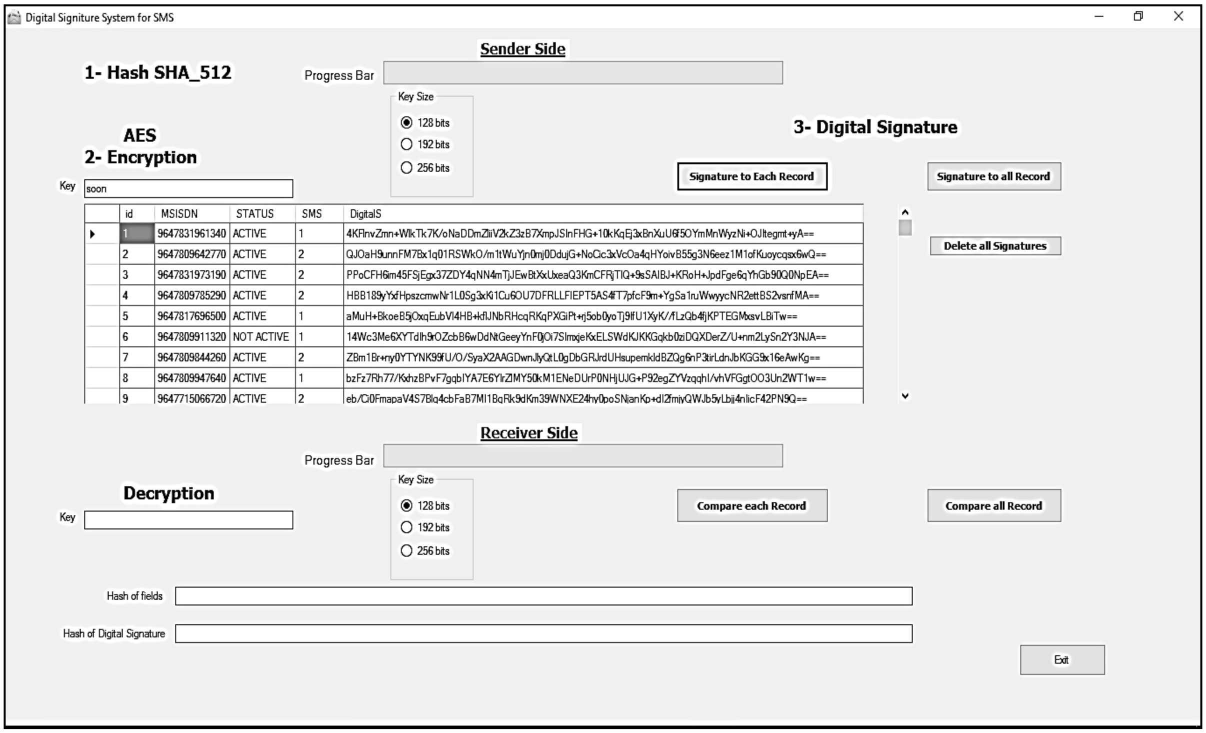


Figure 4. The best location of the proposed System

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 **signature**. Separating the main program window into two sides, sending and receiving sides, to simulate the real work between the 3G mobile phone network and Iraqi Media Network. It can be seen the fields of the records that have been created (Id, MSISDN, STATUS, SMS, and Signature) 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
- **Signature**: 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/oNaDDmZliV2kZ3zB7XmpJSlnFHG+10kKqEj3xBnXuU6f5OYmMnWyzNi+OJltegmt+yA==
	2	9647809642770	ACTIVE	2	QJOaH9unnFM7Bx1q01RSWkO/m1tWuYjn0mj0DdujG+NoCic3xVcOa4qHYoivB55g3N6eez1M1ofKuoycqsx6wQ==
	3	9647831973190	ACTIVE	2	PPoCFH6im45FSjEgx37ZDY4qNN4mTjJEwBtXxUxeaQ3KmCFRjTIQ+9sSAIBJ+KRoH+JpdFge6qYhGb90Q0NpEA==
	4	9647809785290	ACTIVE	2	HBB189yYxfHpszcmwNr1L0Sg3xKi1Cu6OU7DFRLLFIEPT5AS4fT7pfcF9m+YgSa1ruWwyycNR2ettBS2vsnfMA==
	5	9647817696500	ACTIVE	1	aMuH+BkoeB5jOxqEubVI4HB+kflJNbRHcqRKqPXGiPt+rj5ob0yoTj9lfU1XyK//fLzQb4fjKPTEGMxsvLBiTw==
	6	9647809911320	NOT ACTIVE	1	14Wc3Me6XYTdlh9rOZcbB6wDdNtGeeyYnF0jOi7SImxjeKxELSWdKJKKGqkb0ziDQXDerZ/U+nm2LySn2Y3NJA==
	7	9647809844260	ACTIVE	2	ZBm1Br+ny0YTYNK99fU/O/SyaX2AAGDwnJlyQtL0gDbGRJrdUHsupemkldBZQg6nP3tirLdnJbKGG9x16eAwKg==
	8	9647809947640	ACTIVE	1	bzFz7Rh77/KxhzBPvF7gqbIYA7E6YlrZIMY50kM1ENeDUrP0NHjUJG+P92egZYVzqqhI/vhVFGgtOO3Un2WT1w==
	9	9647715066720	ACTIVE	2	eb/Ci0FmapaV4S7Blq4cbFaB7Ml1BqRk9dKm39WNXE24hy0poSNjanKp+dI2fmjyQWJb5yLbjj4nlicF42PN9Q==

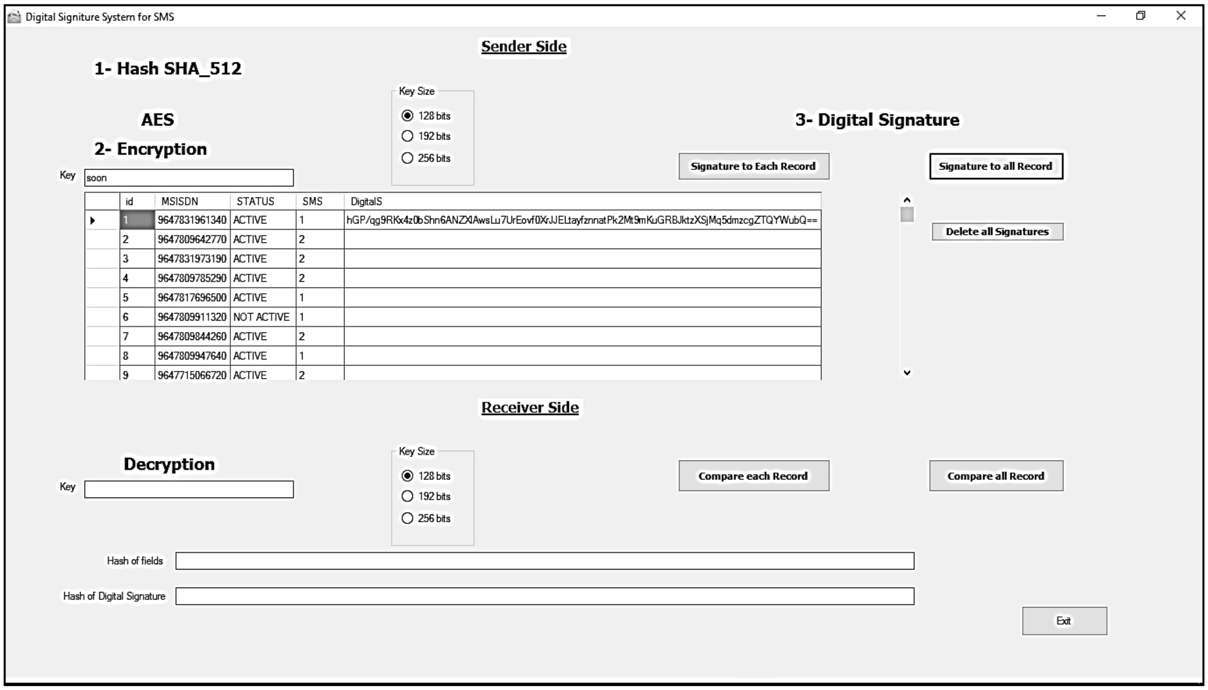
Key Size
● 128 bits
○ 192 bits
○ 256 bits

Figure 5. The Main Interface of the SigSms System

For the inside design of the SMS-Sig-Sys. Server, it has been implemented two Solutions techniques concerned with the SMS-Signature:-

A) Signature-To-Each-SMS-Record: by which each record in the database has its own Signature as in the Figure 5.

B) Signature-To-All- Records: by which all records of the database has just one Signature as in the Figure 6



Key Size
● 128 bits
○ 192 bits
○ 256 bits

Key: soon

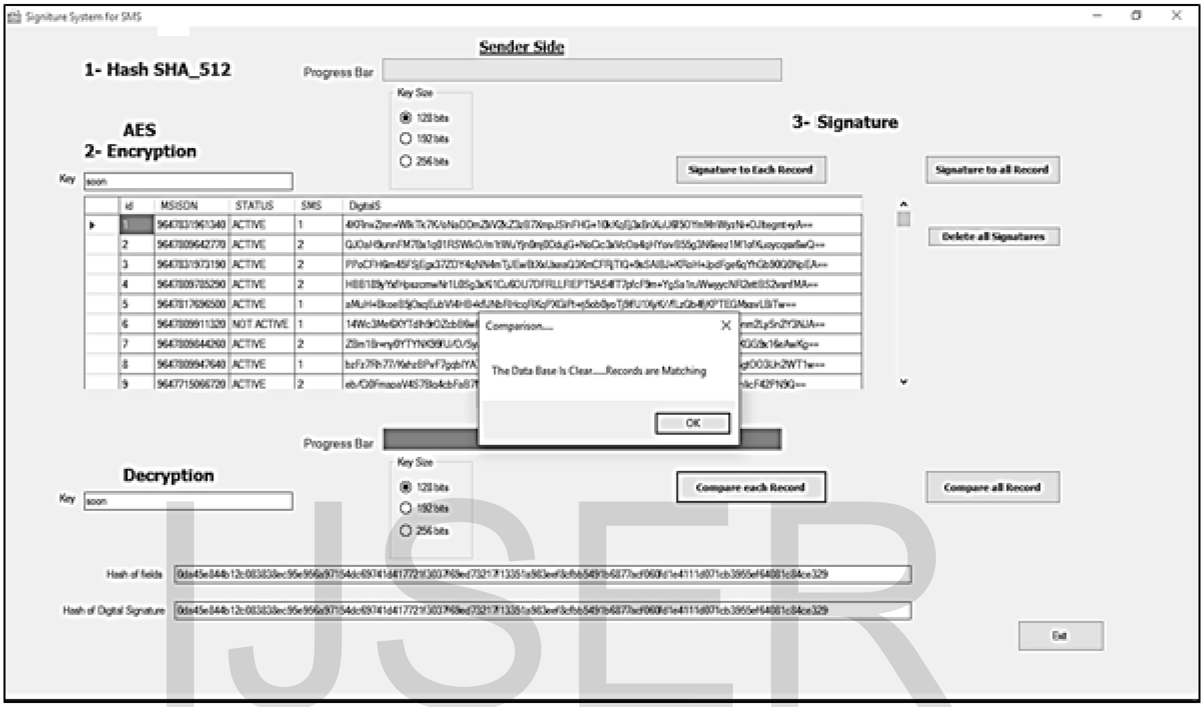
	id	MSISDN	STATUS	SMS	DigitalS
▶	1	9647831961340	ACTIVE	1	hGP/qg9RKx4z0bShn6ANZXlAwsLu7UrEovf0XrJJELtayfznnatPk2Mt9mKuGRBJktzXSjMq5dmzcgZTQYWubQ==
	2	9647809642770	ACTIVE	2	
	3	9647831973190	ACTIVE	2	
	4	9647809785290	ACTIVE	2	
	5	9647817696500	ACTIVE	1	
	6	9647809911320	NOT ACTIVE	1	
	7	9647809844260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

Key Size
● 128 bits
○ 192 bits
○ 256 bits

Figure 6. One Signature for All Records

For the Signature-To-Each-SMS-Record technique, in the sender side (mobile phone network), the Hashing function is done internally inside the code of the system. The user have to specify the Session-key then selecting the key-size which programmed as a radio-button, then have to press the button the "Signature to-each- Record". See figure 5 which will take the Signature of the each record, putting it in the adjacent "DigitalS" field.

In the receiver side, (the IMN Side) it will be checked each record. The receiver have to specify the decryption key first then specify the key-size, press "Compare each Record" button. Which will compare the hash of each field in the database and the hash of the received-Signature after decryption. See figure 7. For the second technique Signature-To-All- Records it has been implementing, the same mechanisms with a different buttons in the main interface window as in previous figure 5.



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

Key soon

	id	MSISDN	STATUS	SMS	DigitalS
▸	1	9647831961340	ACTIVE	1	4KFnwZnn+WlkTk7K/oNaDOmZbV2kZ3z87XmpJSnFHG+10kKqf|3x8n0LU8507YmMrWyzNi+OJtegmtvyA==
	2	9647809642770	ACTIVE	2	GJOaH8unnFM7Ba1q01RSWkO/m1tWuYjn8mj0DduG+NoCic3aVcOs4pHYov855g3N6eez1M1ofKuoycqpa6eQ==
	3	9647831973190	ACTIVE	2	PPoCFHGm45FS|Egx37ZDY4qNN4mTjJEw8XxUaxaQ3KmCFR|TiQ+9eSA8U+KRoH+JpdFge6qYhCb90Q0NpEA==
	4	9647809785290	ACTIVE	2	HBB18ByYxFHpazomeNr1L05g3eK61Cu6OU7DFRLLFIEPT5A54fT7pfcF9m+Yg5a1nJWwyycNFQet852varfMA==
	5	9647817696500	ACTIVE	1	aMuH+8koe85jOxqEubV4HB+e5JNbF0Hcq/IKq/PXGPt+q5ob8poTj9FU16yK//FLzQb4|KPTEGMsavLBiTw==
	6	9647809911320	NOT ACTIVE	1	14Wc3Me6KYTdh9rOZcb06e [illegible] nm2LySn2Y3NJA==
	7	9647809644260	ACTIVE	2	Z8m1Brwy0YTYNK98U/O/Sy [illegible] KGGk16eAwKg==
	8	9647809947640	ACTIVE	1	bzFz7Rh77/KehzBPvF7gqbIYA [illegible] gtOO3UnZWT1w==
	9	9647715066720	ACTIVE	2	eb/Q0FmapaV4S7BoAcbFa87 [illegible] nlcF42PN9G==

Comparison....

The Data Base Is Clear.....Records are Matching

OK

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

Key soon

Hash of fields 0da45e844b12c083838ec95e956a97154dc69741d41772130376 9ed73217f13351a983eef8cfbb5491b6877acf060fd1e4111d871cb3955ef64081c84ce329

Hash of Digital Signature 0da45e844b12c083838ec95e956a97154dc69741d41772130376 9ed73217f13351a983eef8cfbb5491b6877acf060fd1e4111d871cb3955ef64081c84ce329

Figure 7. The comparison for each record

5. PERFORMANCE EVALUATION

During the testing it has been used a prepared information table. Also used a real information database that have been got from a Lebanese MVAS Company, where the number records about two thousands, concerned with one of the races in IMN shows, containing a real participants number.

The evaluation based on the comparison between the used, two SMS-Signature solutions techniques:

- **Signature-To-Each-SMS-Record**
- **Signature-To-All-SMS-Records**

During the execution with the Signature-To-Each-SMS-Record technique it was noticed that it take more processing time wherever the data-table of the database became bigger. Even the comparison in the receiver side between the Signatures take more time when the SMS data records became bigger. Because the SMS-Signature has been done to each record sequentially which need more time.

Either about the execution of the SMS-Signature-System server based on the Signature-To-All-SMS-Records technique it was noticed that it take less processing time for the same data-table of the database became that has been used for the first technique. Even the comparison in the receiver-side between the Signatures take less time, for the same SMS data records. That was because, that the Signature has been done to all records of the data-table for one time only. This technique based on, one SMS-Signature to all SMS data records. Therefore the processing time was so little in the Signature-To-All-SMS-Records.

It have 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. Even when the programming of Hash function or the AES algorithm, it has not used any ready-security-templates or tools, but it has been built it from scratch for the proposal solution.

The system have been built on a computer device that had an Intel Core duo 2.00GHz processor speed, with 3GB Ram. But with the increasing of the database amount it take some time. So it has 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 Signature between the two SMS-Signature solutions techniques

6. CONCLUTION AND FUTURE WORK

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

a). It has been exclude the role of the MVAS Company, by built-in a separated technical department inside IMN depending on the use of the SigSms System Server, and working directly with the Mobile Network 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.

b). 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.

c). 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.

d). 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.

e). 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).

f). 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 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.

b). 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.

c). 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 Systems3G 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.

[18] Lein Harn; "On the Security of Wireless Network Access with Enhancements"; University of Missouri - Kansas City; September 2003