A Secured Automatic Notification System Based on Short Message Service

Emmy Mugisha[1,2], Bob Alex Ogwang[2,3], Victor Ongoma[2,4], Gongxuan Zhang[1]
[1]Nanjing University of Science and Technology (NJUST), Nanjing, P.R China
[2]Nanjing University of Information Science and Technology, Nanjing, P.R. China
[3]Uganda National Meteorological Authority, Uganda
[4]South Eastern Kenya University, Kenya

Abstract

In this paper, a framework has been implemented for applying a secured automatic notification system. A secured module, containing Rijndael Encryption Algorithm has been proved. The system can: send and receive data using Global System for Mobile communications (GSM) Modem; SIEMEN Modem, store sent and received data into database; Structured Query Language (MySQL) for future auditing and sent data to be forwarded along Internet domain automatically under Simple Mail Transfer Protocol (SMTP) with two data suggested security model. The performance of implemented communication secured system is related to Short Message Service (SMS) communication density, its reliability and robustness along transmission medium suggests. The coupling level of parallel SMS/SMTP communication is defined to represent the communication density; it is proved to be significant in communication since a higher coupling level generates more message forwarding from terminals on GSM network. The technology is useful in the field of computer engineering in terms of communicating securely through GSM network and beyond.

1. Introduction

A communication system necessitates transfer of messages from one party to another/others. Short Message Service (SMS) is a communication protocol that creates room for exchange of short messages between mobile telephone gadgets [1, 2]. The application is used in various practical world applications [3 - 6]. For instance, in a study conducted in Beijing on information dissemination analysis of different media towards the application for disaster pre-warning, showed that out of the six media considered, SMS is the most effective based on its high speed. The Cell phones are preferred because they can disseminate more detailed information since verbal communication allows better clarification of complex statements [7].

The confidentiality of the message(s) vary, most users desire more secure and private communication over cellular networks in their daily data usage from remote terminals. This is especially important in communications of secret nature such as in military operations, health institutes, transportation companies and government organs. In some cases, very confidential information such as password and bank details is exchanged through SMS without information security. This exposes SMS usage to security threats such as disclosure of the message and replay attack [8, 9]. Therefore, securing communication through popularly used means; text/code messages are of great importance.

In SMS communication trend, under Global System for Mobile communications (GSM) network, communications for remote terminals can receive/send short messages without any hindrance due to its accuracy in data transmission along cellular channels [10, 11]. In terms of security, for further engineering on information cycle, different organizations and running institutions have remote equipments that require timely monitoring. The automatic functions of the machines/devices include turning off/on, reporting captured data, notifying hazardous events, secret information exchange, among others. This paper provides a parallel secured automatic SMS notification application using GSM network or other, connecting remote terminals to monitor or control over, hence forwarding secured notification contents to Internet domains using Simple Mail Transfer Protocol (SMPT).

Datta et al. [12], pointed out that electrical equipments including alternator, transformer, circuit breakers, among others, installed in different locations in a power system need to be monitored and controlled for healthy operation and smooth running of the system. The convergence of wireless communication technology and embedded controller technology with different transducers makes these supervisory systems more reliable, flexible, and much efficient as well as cost effective than wire line deployment. In this scheme, a state-of-the-art stand-alone Dedicated Hardware Unit (DHU) was developed using microcontroller for monitoring system's parameters like instantaneous voltage, current, temperature, frequency and speed of alternator and transformer in a power plant. Equipment is interfaced with one DHU. The DHU is also interfaced with GSM modem for GSM based wireless access. Each DHU compares the measured value with a pre-set or limiting values of the above mentioned parameters and if any abnormalities are detected an SMS is generated and is sent to the pre-located mobile or central station. The receiver may then send a return SMS requesting the details of the abnormalities. Upon receiving this request, the details of the fault are then sent through another SMS by the DHU and it will take the appropriate action as per content of the return message.

A study on an automatic medical emergency telephone communications device indicated that when an individual who is under stress of emergency response such as a fire, dials 91 1 or another dedicated number to request an ambulance or other response, unless the 91 1 system has sophisticated enhanced (E91 1) capabilities, there may be no way to respond to the emergency in time [13].The study suggested the designing inexpensive system to provide address and other pertinent data to a central monitoring point without caller intervention when activated by an external signal. The system should also recognize the need of insuring the security of the transmitted information so that an outside party cannot access it with an incoming call. Long distance appliance control using mobile short messaging service and Internet in parallel illustrates a secure and reliable system for remotely controlling electrical appliances by SMS and/or Internet [14 - 16]. It requires serial interfacing of two micro-controllers with SIEMENS AX75 cell phone and a personal computer respectively. In their implemented hardware scheme, a low cost mobile was used instead of the relatively expensive GSM modem used by Nikolova et al. [17]. SMS based control, any electronic appliance can be turned on or off by sending SMS from a pre-registered mobile number. Literally, any device (one or more at a time) can be controlled by a single SMS, as long as the coverage of a mobile network goes. The same appliances can also be controlled over Internet. The whole process requires a webpage where a list of all the appliances that can be controlled is available and the appliances can be turned on or off by mouse-clicks. Combinations and working together of mentioned components can be seen in an architectural view in Figure 1.

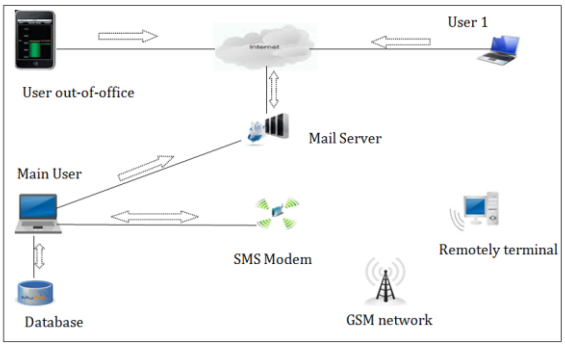


Figure 1. Application Architecture

The content of the data to be sent or received is under two categories, first; is data received from Remote Surveillance Devices (RSD). The device is connected to a GSM network or others that enables it to generate a message with specific data according to its function. The SMS modem is responsible of receiving this message and forward it along Internet domain as well as stored in application's database for future usage.

The second category involved data transfer from the SMS modem to remote devices for information or communication aspects regarding for reporting timely and immediate response for emergency ack. These entire data to be forwarded must be encrypted first before for security issues.

The implemented work in this work follows the design-science manner; the goal is to apply automatic secured SMS notification within Internet domains and parallel to remote terminals on GSM network or otherwise.

2. Materials and Methodology

The methodology that has been used for the implementation is under: a) Related work: to determine the corner point of concentrated potential challenges is located and to place this into the philosophy of the existing body of knowledge in SMS communication scenarios; b) Prototyping: to develop a theoretical prototype of an automatic SMS communication environment that handles insufficiencies within the current body of communication; c) Test and Finesse: testing the application using several scenarios which in turn result finesse of its structural and operation; d) Evaluation: to assess the functionality and performance of the output.

A framework is designed and presented, fulfilling requirements of a secured automatic SMS notification communication based on SMS/SMTP services. It contains all features that an SMS communication needs, and has been realized in a GSM network and Internet environment. The framework incorporates three fundamental parts which includes security (Advanced Encryption Standard) model; an automatic SMTP service along Internet medium; GSM connected terminals for SMS along cellular networks. The security model determines the concept of forwarding secured information on Internet transmission environment. It introduces cryptographic algorithm for sharing authenticated and confidential information exchange along Internet trend.

In this paper, implementation of Advanced Encryption Standards (AES) was used and surveyed from different relevant present work as an advanced tool in terms of information security is concerned. Rijndael is the algorithm that has been selected by the U.S National Institute of Standards and

Technology (NIST) as the candidate for AES designed by Vincent Rijmen and Joan Daemen from Belgium. It uses symmetric – key algorithm. This work involves aforementioned skills in encrypting forwarded contents to Internet medium, and the same applied to the receiving end point when getting back to the original contents under decryption process. Two passphrase and saltvalue keys are generated randomly each time random key function generator is triggered, passing them into encryption and decryption functions to act accordingly.

3. Results and Discussion

Fixing key in cipher text is a technical trick to fix key chars into ciphers. It is fixed according to the length of a key string, at the first char of the ciphertext, a key char is placed after a certain number of chars from the beginning of ciphers to the end. Here, the length of a key is limited to nine byte and this makes it possible to sink into ciphertext string with no key's char reminder.

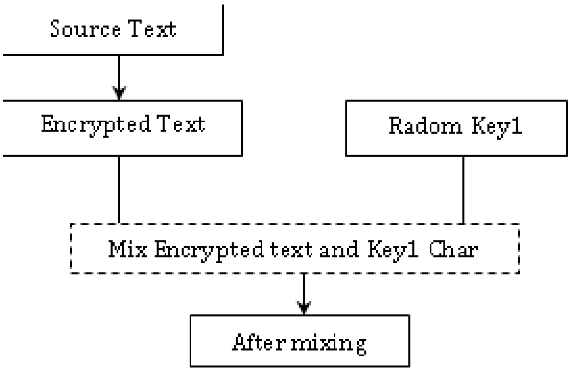


Figure 2. Fixing key bit structure

Result preview

C1	K1	C2	K2	C3	K3	C4	K4	--------	K11	Attached C

Where **C1** is the first char of the cipher string, and **K1** is the key char of the key string which is fixed after stepping 1 length of the cipher, starting from the first cipher byte/char. K11 is the 11th key byte/char and Attached C is the remained cipher after fixing.

Embedding Key bits in ciphertexts: the style of transferring key together with ciphertext demonstrates embedding key into encrypted information from the sending point and extraction of key on the other receiving point for decryption. Both cipher and key are converted into bits, key bits are added to cipher's 7th (Most Significant bit) bit making it 8bit representation for one byte.

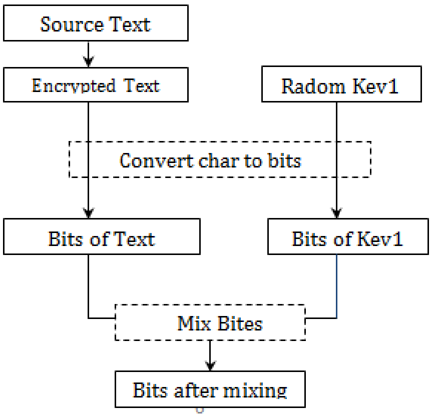


Figure 3. Embedding key bits structure

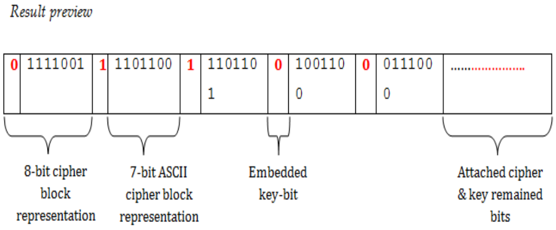
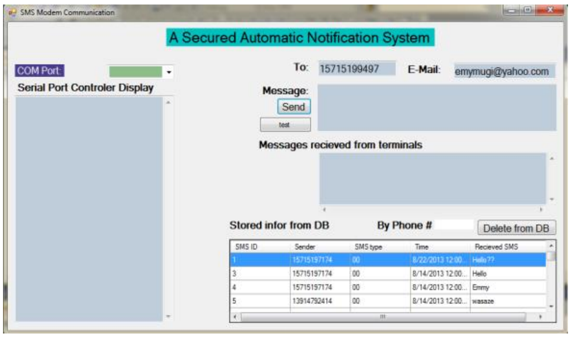

Result preview
0
1111001
1
1101100
1
110110
1
0
100110
0
0
011100
0
....
8-bit cipher block representation
7-bit ASCII cipher block representation
Embedded key-bit
Attached cipher & key remained bits

Figure 4. Result preview

Keys Extraction for decryption process; under fixed or embedded key technique, the extraction process undergoes the same process of fixing or embedding algorithm, but instead of fixing its extracting. Online webpage was developed for decryption at the receiving side. It is designed to specifically extract or separate a key from cipher contents.

The SMTP server is an Internet standard for e-mail (electronic-email) transmission a cross Internet protocol (IP) networks. It is an application layer protocol in OSI reference model. SMTP uses TCP port 25. A number of one-to-one electronic messaging was used in the 1960s [18]. Communication with one another using systems developed for specific mainframe computers. Computers were interconnected especially in the U.S Government's ARPANET standards developed to allow users of different systems to e-mail one another. We configured basic SMPT server parameters to support mail forwarding along Internet medium. As known on SMTP functionalities, MUA defined by i.e. sender user address (e-mail) for example 'senderAddress = **"emymugi@126.com";**' and its password; ' pwd = **"xxxxxx123";**', the receiving user likewise; 'receiverAddr = **emmy@yahoo.com**;' together with message title; 'title = **"System Mail message";**' as well as message body; 'content =**Message.Text'**. The MX (Mail Exchange) which SMTP server that is dedicated to forward in-coming message (email) to desired destination 'smtpServer = **"smtp.126.com"**; with a server listen port; serverport = **"25".**'

The application view or appearance is demonstrated, the application user interface is presented in Figure 5. The interface showing different controls with different event or action is seen, the serial port controller before opened shows whether the SMS modem is ready to receive/send data, next is what is seen after opening the port (COM).


SMS Modem Communication
A Secured Automatic Notification System
COM Port:
Serial Port Controler Display
Message:
Send
test
Messages recieved from terminals
Stored infor from DB
By Phone #
Delete from DB

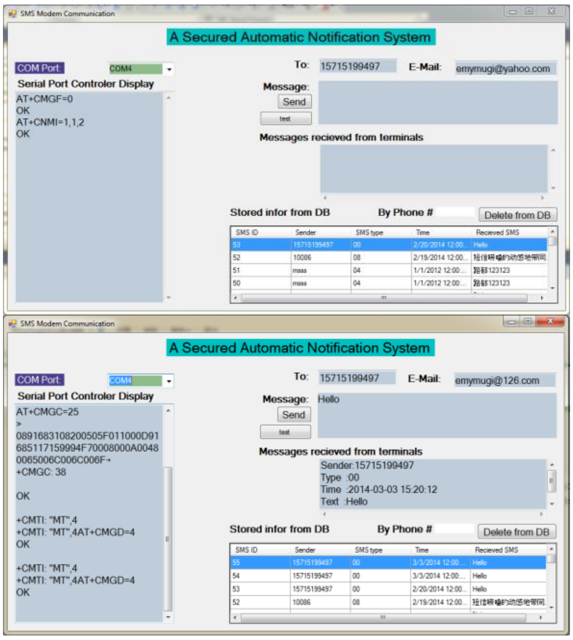
To: 15715199497

E-Mail: emymugi@yahoo.com

SMS ID	Sender	SMS type	Time	Recieved SMS
1	15715197174	00	8/22/2013 12:00...	Hello??
3	15715197174	00	8/14/2013 12:00...	Hello
4	15715197174	00	8/14/2013 12:00...	Emmy
5	13914792414	00	8/14/2013 12:00...	wasaze

Figure 5. Application user interface

The "hello" message was used to test if the SMS modem can function accordingly, and lastly an online decryption web page with extraction panel is shown in Figure 6.


SMS Modem Communication
A Secured Automatic Notification System
COM Port:
Serial Port Controler Display
Message:
Send
test
Messages recieved from terminals
Stored infor from DB
By Phone #
Delete from DB
SMS Modem Communication
A Secured Automatic Notification System
COM Port:
Serial Port Controler Display
Message:
Send
test
Messages recieved from terminals
Stored infor from DB
By Phone #
Delete from DB

COM Port: COM4

To: 15715199497

E-Mail: emymugi@yahoo.com

```
AT+CMGF=0
OK
AT+CNMI=1,1,2
OK
```

SMS ID	Sender	SMS type	Time	Recieved SMS
53	15715199497	00	2/20/2014 12:00...	Hello
52	10086	08	2/19/2014 12:00...	短信晰嘛的动感地带同
51	mass	04	1/1/2012 12:00:...	路邮123123
50	mass	04	1/1/2012 12:00:...	路邮123123

COM Port: COM4

To: 15715199497

E-Mail: emymugi@126.com

Message: Hello

```
AT+CMGC=25
>
0891683108200505F011000D91
685117159994F70008000A0048
0065006C006C006F→
+CMGC: 38

OK

+CMTI: "MT",4
+CMTI: "MT",4AT+CMGD=4
OK

+CMTI: "MT",4
+CMTI: "MT",4AT+CMGD=4
OK
```

```
Sender:15715199497
Type  :00
Time  :2014-03-03 15:20:12
Text  :Hello
```

SMS ID	Sender	SMS type	Time	Recieved SMS
55	15715199497	00	3/3/2014 12:00:...	Hello
54	15715199497	00	3/3/2014 12:00:...	Hello
53	15715199497	00	2/20/2014 12:00...	Hello
52	10086	08	2/19/2014 12:00...	短信晰嘛的动感地带同

Figure 6. Serial Port opened ready to receive/send a messages

An automatic SMS notification application is implemented based on SMS and SMTP services using Visual Studio C# tool. A remote device can therefore send data with metadata information to an SMS Modem, and then message content (body) can be shared to specific Internet users using content forwarding i.e. SMTP services. The application was tested to prove the basic functionality of both the Remote Surveillance Device data reporting to SMS Modem and content forwarding through SMTP service on Internet medium. The generated results illustrate that the SMTP services has been successfully integrated into C# environment and properly fixes expectations.

4. Conclusion and Recommendation

A secured automatic notification application based on SMS/SMTP communication, it is maintained and discovered. It provides: sending/receiving secured SMS from SMS modem using AT command; storage of sent/received SMS into database; developed a communication interface (User Interface) between devices and end-users through a SMS Modem; ways sent/received data can be forwarded on Internet with security issues. The application is expected to meet user's needs to promote technology more useful in the field of computer engineering in terms of communicating securely through GSM network and beyond.

The study recommends that end-users be trained and get used on the application functionalities and usage, there is need of understanding 'how', 'when', 'who' to access its functionalities, requirements and basic knowledge required to execute it on remote offices. The SMS modem should always be 'on' state, wherever it is set. The SIM Card in-SMS modem should be available on cellular network and recharged for sending and receiving short messages. The receiving end should be well aware of retrieving or extracting exact key or cipher for correctness of expected output.

5. Acknowledgements

The authors are grateful to the entire *Nanjing University of Science and Technology (NJUST) &* Nanjing University of Information Science and Technology for giving them the opportunity and facilities to work on this paper. One of the authors; Emmy, sincerely expresses his gratitude to Prof. Gongxuan Zhang, Prof. Liu Qi Frank and Mr. Lu Yu for giving constant inspiration to carry out the research work.

6. References

[1] S.L. Cheung. (2008). "Using mobile phone messaging as a response medium in classroom experiments". Journal of Economic Education, 39. pp. 51-67.

[2] S. Reimers, and N. Stewart. (2009). "Using SMS text messaging for teaching and data collection in the behavioral sciences". Behavior Research Methods, 41, pp. 675 – 681

[3] A. Rashdi, R. Malik, S. Rashid, A. Ajmal, S. Sadiq. (2013). "Remote Energy Monitoring, Profiling and Control Through GSM Network". Arabian Journal for Science and Engineering, 38, pp. 3249–3257. DOI 10.1007/s13369-012-0432-x

[4] K. Yadav (2011). "SMSAssassin: Crowd sourcing driven mobile-based system for SMS spam filtering", in *Proc. Workshop Hotmobile*, pp. 1–6.

[5] J. Chen, L. Subramanian, and E. Brewer. (2010). "SMS-based web search for low-end mobile devices", in *Proc. 16th MobiCom*, pp. 125–135.

[6] I. Gurol-Urganci, T. de Jongh, V. Vodopivec-Jamsek, R. Atun, and J. Car. (2013). "Mobile phone messaging reminders for attendance at healthcare appointments". *Cochrane Database of Systematic Reviews*, Issue 12. Art. No.: CD007458. DOI:10.1002/14651858.CD007458.pub3.

[7] N. Zhang, H. Huang, B. Su, J. Zhao, and B. Zhang. (2014). "Information Dissemination Analysis of Different Media towards the Application for Disaster Pre-Warning". PLoS ONE 9(5): e98649. doi:10.1371/journal.pone.0098649

[8] K. Park, G.I. Ma, J.H. Yi, Y. Cho, S. Cho, and S. Park. (2011). "Smartphone remote lock and wipe system with integrity checking of SMS notification", in *Proc. IEEE ICCE*, Jan. 2011, pp. 263–264.

[9] N. Gligoric, T. Dimcic, D. Drajic, S. Krco, and N. Chu. (2012). "Application layer security mechanism for M2M communication over SMS", in *Proc. 20th TELFOR*, pp. 5–8.

[10] J. Rapeli. (2001) "Future directions for mobile communications business, technology and research". Wireless Personal Communications, 17, pp. 155 -173.

[11] A. Idris, A.H. Basari, and N.H. Zubir. (2009). "An application of SMS technology for customer service centre". International Conference of Soft Computing and Pattern Recognition, pp. 633-636.

[12] J. Datta, S. Datta, S. Chowdhuri, and J. Bera. (2012). "GSM based Condition Reporting System for Power Station Equipments", 3rd International Conference on Emerging Applications of Information Technology (EAIT), 30 Nov. - 1 Dec. 2012, Kolkata. IEEE Publication, pp. 256 - 259. DOI: 10.1109/EAIT.2012.6407917

[13] W.J. Jameson Jr., M. Kejarawal, T. Herreid, C. Mitten, and J.M. Ray. (2009). "Automatic Medical Emergency Telephone Communications Device", Proceedings of the Annual International Conference of the IEEE Engineering, 09 -12 Nov. 1989, Seattle, WA. IEEE Publication, 6, pp. 2009 - 2010. DOI: 10.1109/IEMBS.1989.96569

[14] Atmel. (2010). "'ATMEGA 32 datasheet" Pp. 1-233. www.atmel.com/atmel/acrobatldoc2503.pdf (1 May, 2011)

[15] T.F. Aula (2011). "Using SMS in Mobile Phone for Home Appliances Controlling through PC Parallel Port Interfacing". Pp. 1 - 4. www.emo.org.tr/ekler/8808cfb5939be38_ek.pdf (21 April 2011).

[16] Maxim (2004). "MAX232 Datasheet". pp 1-7. www.datasheetcatalog.org/datasheet/texasinstruments/max232.pdf (19 May 2011).

[17] M. Nikolova, F. Meijs, and P. Voorwinden. (2003). "Remote mobile control of home appliances". IEEE Transactions on Consumer Electronics, 49(I) pp.123-127.

[18] H. Shih-Chia. (2011). "An Advanced Motion Detection Algorithm with Video Quality Analysis for Video Surveillance Systems". IEEE Transactions on Circuits and Systems for Video Technology, 21(1), pp. 1-14. DOI: 10.1109/TCSVT.2010.2087812