International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 4, Issue 11, ISSN No. 2455-2143, Pages 232-238
Published Online March 2020 in IJEAST (http://www.ijeast.com)

SECURED AND EFFICIENT SHORT MESSAGE SERVICES BASED MOBILE BANKING SYSTEM USING DYNAMIC DUAL KEY ENCRYPTION ALGORITHM (SESMBS)

[1]Aluko Augustine Oli, [2]Omoniyi Akintunde Ojo
[1,2] Computer Science Department, Rufus Giwa Polytechnic,
Owo, Ondo State, Nigeria

ABSTRACT - Global System for Mobile Communication (GSM) provides services such as Unstructured Supplementary Data (USSD) and Short Message Services (SMS), among other services. In the design of GSM architecture, SMS and USSD services are designed for subscribers to send non-sensitive messages across the GSM network between two or more devices. The existing USSD protocol provides efficient services with weak security mechanism, while the SMS provides flexible but inefficient services with no security mechanism. Therefore, despite the high flexibility and usability advantages of SMS across GSM network, it has not enjoyed wide usage in security critical applications such as medical, banking, military and business information systems. This research was therefore designed to harness the strength of the enhanced Dynamic Dual Key Cryptography Algorithm to provide secured and efficient SMS services. Window Application Server was implemented using Visual Studio.Net Framework. The security and efficiency of SESMBS was demonstrated with prototype of an e-banking system with 10 unauthorized users and 10 authorized users. The security performances of SESMBS were evaluated based on attack success in the instances of brute force, while the efficiency performances were evaluated based on throughput and latency. The results of attack success showed that with 120 attack trials in the instances of both brute force and dictionary attack threats, none of the unauthorized users was successful on SESMBS, while all the authorized users were successful, with average throughput of 0.8778 i/s and 0.3833 i/s for fixed messages and varying messages respectively, and latency of 6.1 seconds. Also, the messages were processed efficiently with the highest processing time of 10-seconds, which fell below the 20 seconds maximum threshold of SMS.

Keywords: Global system for mobile communication, short message services, efficiency.

I. INTRODUCTION

Mobile commerce (M-commerce) is the buying and selling of goods and services through wireless handheld devices such as cellular telephone and personal digital assistants (PDAs). Also, new generation e-commerce, m-commerce enables users to access platforms such as Internet, GSM, Wi-Fi, and others without needing to find a place to plug in. The emerging technology behind m-commerce, which is based on the Wireless Application Protocol (WAP) such as Wireless Local Area Network (WLAN), Global System for Mobile Communications (GSM), etc, has made far greater strides in Europe, where mobile devices equipped with Web-ready micro-browsers are much more common than other parts of the world. Tiwari and Buse (2007).

Short Message Service (SMS) was developed as part of the services rendering by GSM network providers which was on the increase since the year 2000. The use of SMS was focused on marketing, transmission of unsecured information in text format, etc. Since the architectural design and development of SMS platform was done to transmit unsecured information, little or nothing was majorly thought of having M-commerce driven by SMS for security intensions. The GSM network as the backbone of SMS has become the most used and popular network in the world.

The use of Short Message Service in mobile banking system needs a touch of security enhancement for efficiency. The security challenges such as confidentiality, eaves dropping, and phone memory hacking are addressed for the efficiency of the mobile banking system using secured SMS protocol. This paper proposed the use of Enhanced Dynamic Dual Key Encryption Algorithm Based on joint Galois Fields for a secured and efficient mobile banking system.

II. LITERATURE REVIEW

The exponential growth of smart phones has assumed an exponential form. 89.4% of world population use mobile phones. Among the 89.4%, 46.4%, uses internet and application enabled mobile phones and devices (Tejas *et al.*, 2013).

Many countries with mobile communication services use Global System for Mobile Communication (GSM) architecture to network their mobile connections. GSM network was initially designed to be used for voice communication. As the usage of mobile phone increases, people begin to use their mobile phones for additional means of data transmissions. GSM network as most popular environment for mobile transactions has some shortcomings during the design and development of this architecture. Five most pronounce of these flaws are: Eavesdropping, Impersonation of user, Impersonation of the network, Man-in-the-middle and Compromising authentication vectors in the network. Gadaix (2001) and O'Brien (2009) reported a German computer engineer that announced the deciphered of a secret code used to encrypt most of the world's digital mobile phone calls. The security provided by GSM network can be viewed as inadequate which is as a result of general shortcomings in wireless networks.

Recent researchers have done several research works to meet the demand of the market needs. Manoj, (2011), proposed SMS based secured mobile banking system. His introduced the use of symmetric encryption techniques and hashing algorithm for system security and integrity. However, the researcher does not look into device constrains and one to one mapping of key distribution. Raghavend *et al* (2011), proposed secure SMS with identity based cryptography in mobile telecommunication networks. In their work, a scheme using identity based cryptography for a secure messaging channel was developed by implementing Advanced Encryption Standard (AES) algorithm to provides integrity, authentication, and confidentiality of SMS messages by binding a message with a private key possessed only by a particular mobile phone to prevent prevents the activities of attackers on SMS. However, the researchers did not pay attention to revocation issue that is, when a public key is compromised, the corresponding private key can no longer be used. Ashish *et. al*, (2012), proposed a secure SMS based m-commerce, with the objectives to exploiting Tiny Encryption Algorithm (TEA) and Message Digest 5 (MD5) that takes cognizance of the processing power and memory limitations of the mobile device. Their model was able to reduce memory footprint, maximize speed and also the amount of cipher text produce. The limitation to their model was the omission of message integrity. Mulliner *et al.* (2013) present SMS-based One-Time Passwords: Attacks and Defence. In their research work, One-Time Passwords were introduced to counter phishing and other attacks against authentication and authorization of Internet services. A virtual dedicated channel mechanism was developed to secure Short Message Service (SMS) based One-Time Passwords (OTPs) against mobile phone attacks such and prevent anti SIM Swap Attack. However, message integrity and higher cost amounted from multiple SMS involved in each transaction process were not put into consideration in their research work.

Ravishankar, (2013) presented Dirty use of USSD codes in cellular networks. The objective of his research work was to outline possible attacks on both network infrastructure and end-user mobile phone and the possible services of USSD in telecommunication. The research work of Ravishankar does not portray real life scenario in his experiment but rather, he based his paper majorly based on assumption. Kingslin & Dhanalakshmi, (2018) presented a Security Based Technique for Handling Secure SMS in Mobile Phones using Text Steganography. The objective of their research work was to provide a secured SMS via steganography techniques by introducing a Binary look up table used for text conversion for Message integrity and confidentiality. The limitations of their research work were the number of bytes that can hide message (28-bytes) and maximum message capacity 140 characters.

Abdul-Monem, S. R. and Basima, Z.Y. (2011) presented Dynamic Dual Key Encryption Algorithm Based on joint Galois Fields. Their research objectives were to present an efficient and secured mobile banking system using dynamic dual key encryption algorithm. There system demonstrated a high computational speed, secured SMS transmission in SMS mobile banking, and anti decryption means using brute force and other message attacking models. However, their proposed model focuses only on

International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 4, Issue 11, ISSN No. 2455-2143, Pages 232-238
Published Online March 2020 in IJEAST (http://www.ijeast.com)

numerical values which are impossible. There algorithm does not put into consideration, the issue of alphabetical values, alphanumeric values and special characters.

MATHEMATICAL MODEL FOR 3, 4, 5, AND 6 BITS BLOCK SIZE

In the Galois field, commutative ring are all nonzero elements with a multiplication inverse. Nakahara and Abrah (2009). A field of order p, GF (p) is defined as a set of Zp of integers {0, 1, … , p-1} together with the arithmetic operations modulo p Stallings William (2011). The number of element are limited in all finite fields. A polynomial f(x) in GF_(2_) in equation 1 below is represented as:

$$\mathbf{f(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1x + a_0} \quad (1)$$

In Abdul-Monem and Basima 2011, a finite field of GF (2^3, 2^4, 2^5, and 2^6) respectively was presented with the table 5, 6, 7, and 8 consecutively. Addition and multiplication operation are carried out upon each field. In addition operation in GF (2^n): a(x) = 001 + 001 = 000, a(x) = 010 + 001 = 011, etc, the addition operation on GF (2^3, 2^4, 2^5, and 2^6), addition operation required an exclusive OR. The addition inverse on a GF (2^3, 2^4, 2^5, and 2^6) remains unchanged based on the fields operating upon. The multiplication operation is carried out by a bit shift and multiplication of binary operation.

RESEARCH OBJECTIVES

This research focuses on the modification of Dynamic Dual Key Encryption Algorithm (DDKEA) to accommodate alphanumeric values for complete mobile banking system transactions with a minimal effect on mobile host battery life.

III. METHODOLOGY

THE ENHANCED ENCRYPTION ALGORITHM

The enhanced dynamic dual key encryption algorithm was designed to improve the use of SMS in mobile banking services. The algorithm allows for alphanumeric, numeric and binary information in mobile banking services.

Input:
One-Time Password
IF (One-Time Password) = = FALSE THEN **:** EIXT SUB
ELSE
Plaintext, KeyOne, KeyTwo
Output:
Break String
IF (IsNumeric = = FALSE) THEN
WHILE (KeyOne (Len) > 0) DO:
Step1: Get equivalent number of alphabet from the lookup table
Step2: Read a portion of KeyOne (Control Key)
Step3: Select the block size (3, 4, 5 or 6 bits) from plaintext
Step4: Perform the following Encryption Equation (V = Q + R)
Step5: Read the next byte
END WHILE
END IF
IF (IsNumeric = = TRUE) THEN
Ciphertext
No_K_1 /* number of bits from keyOne that are used in first round*/
No_K_2 /* number of bits from keyTwo that are used in first round*/
Step 0:
-Round = 0
-While Round < 2 Do:
Step1: Read a portion of KeyOne (Control Key)
Step 2: Depending on the value of KeyOne's portion do the following
Select the block size (3, 4, 5 or 6 bits) from plaintext
Read from KeyTwo A and B keys
Perform the following Encryption Equation (Y = X * A + B)
Step 3: Compute the number of bits for KeyOne and KeyTwo that are used in first round
Check If Round = 0 then
$No\_K_1 = No\_K_1 + 2$
$No\_K_2 = No\_K_2$ + block size * 2
End if
Step 4: Repeat step 1, 2, and 3 until plaintext is finished
Round = Round + 1
End While
END IF
END IF

THE ENHANCED DECRYPTION ALGORITHM

The enhanced decryption algorithm can be described by the following steps in the algorithm below:

Imformation:
IF (MESSAGE CHECK SUM) = = INCORRECT**:** EXIT SUB
ELSE
Ciphertext, KeyOne, KeyTwo
Output:
Plaintext

International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 4, Issue 11, ISSN No. 2455-2143, Pages 232-238
Published Online March 2020 in IJEAST (http://www.ijeast.com)

Break String
IF (IsNumeric = = FALSE) THEN
WHILE (KeyOne (Len) > 0) DO:
Step1: Get equivalent number of alphabet from the lookup table
Step2: Read a portion of KeyOne (Control Key)
Step3: Select the block size (3, 4, 5 or 6 bits) from plaintext
Step4: Perform the following Encryption Equation (U = Q – R)
Step5: Read U
END WHILE
END IF
Step 0:-apply a circular shift of (No_K_1) bits and (No_K_2) bits for KeyOne
and KeyTwo consecutively
-Round = 0
While Round < 2 Do
-Step 1: Read a portion of KeyOne (Control key)
Step2: Depending on the value of KeyOne's portion do the following
Select the block size (3, 4, 5 or 6 bits) from plaintext
Read from KeyTwo A and B keys from the following decryption equation
X = (Y + addition inverse (B)) * multiplication inverse (A)
Step3: Repeat steps 1 and 2 until Ciphertext is finished
Round = Round + 1
End While
END IF

IV. SYSTEM ARCHITECTURE OF SESMBS

The model development of this research work addressed the scientific and the logical methods used in achieving step by step objectives of this research work. The architecture shows

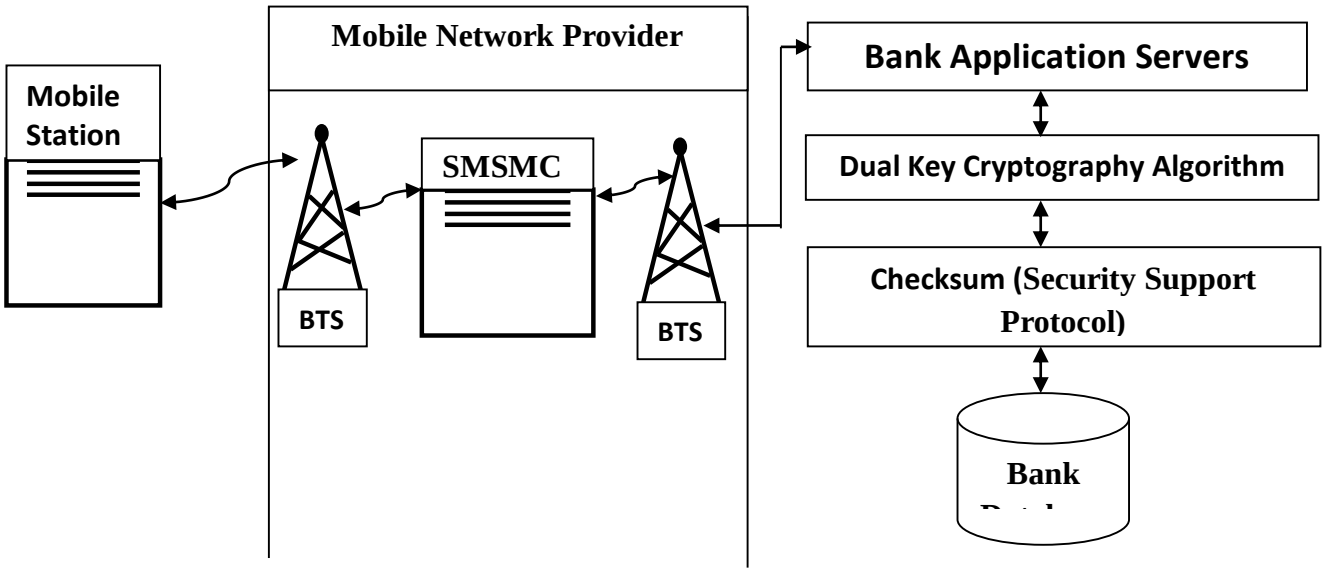

Fig. 1 Secured mobile banking system architecture

In the architecture above, the mobile phone user sends encrypted information via the mobile application installed on the user's phone. The encrypted message is sent through the Base Transmission Station (BTS), of the network service provider, to the Short Message Service Message Centre (SMSMC) where all message temporarily resides as a buffer, The message is sent to the destination point via a BTS. The bank server application picks up the incoming message via the bank Short Message Service (SMS) gateway. A decryption operation is performed to obtain a decipher text. Furthermore, a message integrity test is performed to check out for a possible SMSMC attack. If the decipher message passes the integrity test, a needful banking transaction is carried out and a transaction report is sent to the transaction initiator's mobile station else such message is discard and report sent back to the mobile station.

International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 4, Issue 11, ISSN No. 2455-2143, Pages 232-238
Published Online March 2020 in IJEAST (http://www.ijeast.com)

V. EVALUATION OF SESMBS RESULTS

The results of SESMBS and AbdulMonem and Basima (2011) were compared and summarized below in the following tables below:

i. **Data encryption and decryption:** various date sets were sent across SESMBS and AbdulMonem and Basima model and the results shown in table 1.

MODE	Binary	Alphabet	Alphanumeric	String
AbdulMonem and Basima (2011)	YES	NO	NO	NO
SESMBS	YES	YES	YES	YES

Table 1.

ii. **Brute force attack on** SESMBS**:** high password entropy is adopted by having a randomly generated one time password with the combination of alphanumeric and keyboard special characters. 10 attackers attacked SESMBS using bruit force method as shown in table 2.

SN	Attackers	Frequency	Failure	Success	Failure Rate %	Success Rate %
1	Attacker_1	120	120	0	100	0
2	Attacker_2	120	120	0	100	0
3	Attacker_3	120	120	0	100	0
4	Attacker_4	120	120	0	100	0
5	Attacker_5	120	120	0	100	0
6	Attacker_6	120	120	0	100	0
7	Attacker_7	120	120	0	100	0
8	Attacker_8	120	120	0	100	0
9	Attacker_9	120	120	0	100	0
10	Attacker_10	120	120	0	100	0

Table 2

iii. **Latency test on** SESMBS: Comparism between SESMBS and AES was carried out and the results were presented in table 3 and table 4 below respectively.

SN	information	Location	Sent time (s)	Received time (s)	Latency x (s)
1	Message_1	1	12:14:21	12:14:24	3
2	Message_2	1	12:15:16	12:15:19	3
3	Message_3	1	12:16:41	12:16:45	4
4	Message_4	2	9:30:08	9:30:15	7
5	Message_5	2	9:32:12	9:32:22	10
6	Message_6	2	9:34:01	9:34:09	8
7	Message_7	2	9:36:27	9:36:34	7
8	Message_8	3	3:30:34	3:30:43	9
9	Message_9	3	3:33:14	3:33:19	5
10	Message_10	3	3:35:03	3:35:08	5
				SESMBS	$\sum (x)/n = 6.1$

Table 3

SN	information	Location	Sent time (s)	Received time (s)	Latency
1	Message_1	1	12:14:21	12:14:27	6
2	Message_2	1	12:15:16	12:15:22	6
3	Message_3	1	12:16:41	12:16:48	7
4	Message_4	2	9:30:08	9:30:16	8

International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 4, Issue 11, ISSN No. 2455-2143, Pages 232-238
Published Online March 2020 in IJEAST (http://www.ijeast.com)

5	Message_5	2	9:32:12	9:32:19	7
6	Message_6	2	9:34:01	9:34:10	9
7	Message_7	2	9:36:27	9:36:35	8
8	Message_8	3	3:30:34	3:30:43	9
9	Message_9	3	3:33:14	3:33:22	8
10	Message_10	3	3:35:03	3:35:09	6
				AES	$\sum$ (x)/n =7.4

Table 4

iv. THROUGHPUT OF SESMBS: throughput of a system is the number of request such system can process per second. The results of AES and SESMBS throughput are shown in table 5 and 6 below

SN	Information	Location	Sent time (s)	Received time (s)	Throughput (i/s)
1	Message_1	1	12:14:21	12:14:24	1.000
2	Message_1	1	12:15:16	12:15:19	1.000
3	Message_1	1	12:16:41	12:16:45	1.000
4	Message_1	2	9:30:08	9:30:15	1.111
5	Message_1	2	9:32:12	9:32:22	0.333
6	Message_1	2	9:34:01	9:34:09	1.000
7	Message_1	2	9:36:27	9:36:34	1.000
8	Message_1	3	3:30:34	3:30:43	0.333
9	Message_1	3	3:33:14	3:33:19	1.000
10	Message_1	3	3:35:03	3:35:08	1.000
				AES	$\sum$ (i/s)/n = 0.877

Table 5

SN	Information	Location	Sent time (s)	Received time (s)	Throughput (i/s)
1	Message_1	1	2:14:00	2:14:51	02:14:51
2	Message_2	1	2:20:00	2:20:42	02:20:42
3	Message_3	1	2:30:00	2:30:41	02:30:41
4	Message_4	2	3:35:00	3:35:41	03:35:41
5	Message_5	2	3:42:00	3:42:42	03:42:42
6	Message_6	2	3:48:00	3:48:39	03:48:39
7	Message_7	2	3:52:00	3:52:51	03:52:51
8	Message_8	3	4:20:00	4:20:21	04:20:21
9	Message_9	3	4:40:00	4:40:25	04:40:25
10	Message_10	3	4:51:00	4:51:30	04:51:30
				SESMBS	$\sum$ **(i/s)/n** = 0.3833

Table 6

VI. CONCLUSION

This paper presented a secured and efficient short message services based mobile banking system using dynamic dual key encryption algorithm (SESMBS) was developed based on the Galois field irredeemable polynomial mathematical principles. The algorithm combined the strength and computational speed of the Dynamic Dual Key Algorithm for information security, confidentiality and Checksum for data integrity. The researchers observed that most financial organizations such as banks focuses more on financial gains from customers rather than efficiency and security of system users. Adopting SESMBS will led to secured and efficient mobile application for both financial related organizations, medics, military, and other aspect of the society which efficiency and security are their primary objectives.

VII. REFERENCE

1. Abdul-Monem, S., and Basima Z. Y. (2011**).** The Dynamic Dual Key Encryption Algorithm
2. Based on joint Galois Fields. *International Journal of Computer Science and Network Security*, *Volume11, issue (8),* pp.190-199.
3. Ashish R, Rajashekara, M. S. and Ramakanth K. P. (2012). A Review of Secure SMS Based M-
4. commerce. *International Journal of Engineering Sciences & Emerging Technologies, Volume 1, Issue 2,* pp1-7
5. Gadaix, E. (2001, October 1). "GSM and 3G Security", Bulletin Online. Retrieved from
6. http://bulletin.credit-suisse.ch/ebusiness/970481920.html.Access date: Sep.2018
7. Kingslin, S. and Dhanalakshmi, R. S. (2018). Design of a Security Based Technique for
8. Handling Secure SMS in Mobile Phones using Text Steganography. *International Conference on Advancements in Computing Technologies, Volume 4 Issue 2,* pp.139 – 147.
9. Manoj, V. B. (2011). SMS Based Secured Mobile Banking*: International Journal of*
10. *Engineering and Technology, volume 3, Issue* 6, pp472-479.
11. Mulliner, C., Borgaonkar, R., Stewin, P., and Seifert, J.P. (2013). SMS-Based One-Time
12. Passwords: Attacks and Defense. In: Rieck K., Stewin P., Seifert JP. (Eds) Detection of Intrusions and Malware, and Vulnerability Assessment. *DIMVA*. Lecture Notes in Computer Science, *Volume 7967,* pp. 150–159
13. Nakahara Jr. J., and Abrahao (2009): A new MDS matrix for the AES, *International Journal of Network Security*. Vol. 9, Iss. 2, pp109-116
14. O'Brien, K. J. (December 28, 2009). "Cellphone Encryption Code Is Divulged" The New York
15. Times. Retrieved from http://www.nytimes.com/2017/12/29/technology/29hack.html? (accessed August 31, 2018)
16. Raghavendra, V., Sunanda, M., and Maruthi P. V., (2011): Secure SMS with identity based cryptography in mobile telecommunication networks. IJCST vol.2, Iss.4, pp166-169
17. Ravishankar, B. (2013). "Dirty use of USSD codes in cellular networks", Security in Telecommunications, Technische Universität Berlin TelcoSecDay, Heidelberg.
18. Tiwari, R. and Buse, S. (2007). The Mobile Commerce Prospects: A Strategic Analysis of Opportunities in the banking Sector, Hamburg University Press, Hamburg
19. William, Stallings (2011). Cryptography and network security principles and practice, Fifth Edition. New Jersey, United States of America: Pearson Education, Inc.