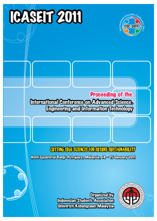
Proceeding of the International Conference on Advanced Science, Engineering and Information Technology 2011

Hotel Equatorial Bangi-Putrajaya, Malaysia, 14 - 15 January 2011

ISBN 978-983-42366-4-9



Data Privacy Framework on Multi Check-out Timestamp Order for Secured Transaction in Mobile Network

Byambasuren Byamba* and Su-Cheng Haw#

Faculty of Information Technology, Multimedia University,
Persiaran Multimedia, 63100 Cyberjaya, Selangor, Malaysia

E-mail: byambasuren.byamba06@mmu.edu.my, sucheng@mmu.edu.my#*

Abstract—**Data transaction over distributed network has gained much attention in the database communities since the last decade, especially in terms of security support. There are several data privacy models for mobile computing such as Data Encryption Standard, Skipjack, RC5 and so on. Most of the cipher algorithms are designed for huge data size of encryption and decryption processes. Therefore, a suitable secure cipher algorithm is needed if the encryption and decryption is merely for small amount of data such as in the mobile database environment. In this paper, we discuss on the five well-known symmetric key cryptographic ciphers and propose a framework for the security model on top of Multi Check-out Timestamp Order (MCTO) data transaction model.**

Keywords— **Mobile database security, symmetric cryptography, distributed database privacy, cryptographic cipher**

I. INTRODUCTION

In the recent years, several research articles on security databases were published [1],[2],[3],[4],[5],[6]. These articles revealed that mobile database security management is still one of the current issues in distributed database that has yet to be resolved. It was on this basis that this study was initiated.

Security is the act of protecting against intentional or unintentional threats [7]. In dictionary, security is activities that is involved in protecting a country, building, person and data against attack, danger and lose [8]. In terms of database security, it is the act to protect a database from unintended activity. Security in database and networking are most important and necessary for safety communication through the network. Vulnerability of any system constitutes unsafe condition in itself. Lu [3] described the movement of nodes in wireless network commits vulnerabilities for network and database. When there are vulnerabilities in database network, data replication process may be damaged and the data in the database may be steal, and the act of the data hacking easily break-in [10], [11]. For instance, customer credit card information is compromised at online retailer either due to the fact that poor privacy database design or insecure application usage.

Herlihy and Tygar [12] described about the distributed system, which consists of a collection of computers that are geographically distributed and connected by a wireless communications network, is exposed to malicious attack on database, data replication and the entire system. Lu [3] explained that the traditional security in wired network systems is not suitable for the distributed wireless network environment because there are many blocks, restrictions and accesses to data which causes the process to delay due to traffic congestion. Therefore, a fast and dynamic security system for both wired network and wireless network is required. However, the replicated database security is still vulnerable in mobile networks, as it faces challenges with attack to the data; thus, it requires the creation of reliable dynamic security system by adopting the rapid development in information technology and new discoveries.

Abdul-Mehdi et al. [13] mentioned the Multi Check-out Timestamp Order (MCTO) is one of the latest data transaction techniques in distributed database system. It allocates part of the database at fixed network to the mobile clients while it does database manipulation between fixed computer (server) and mobile computers (clients) through the wireless network. This model has significant advantages at distributed database allocation but it does not have data transaction privacy at all. The vulnerability appeared insecure transmission when data transaction is performed between the wired and wireless network. If this condition is kept longer for a period of time in the model, the data over the wireless transaction leads to attacks or unwanted access. In order to resolve existing problem, this research work focuses on proposing a suitable secure model and implement it as an efficient security system to the MCTO mobile data transmission.

II. Preliminary Requirement & Related work

A. Requirement for Secure Data Exchange

According to [6], the cryptography should provide several aspects of the security related to the exchange of data through the network. These aspects are Confidentiality, Integrity, Authentication and Non-repudiation of the data. Detailed definitions on these aspects are elaborated as below:

- ***Confidentiality***: It is difficult to open an envelope and read the content without being detected. Cryptographic has both the encryption and decryption algorithms. The encryption algorithm is used to change the data structure to an unknown structure to be exchanged over the network. The decryption algorithm is utilized to revert the unknown structure to the initial data structure so that it could be readable.

- **Integrity**: It you receive a sealed letter in an envelope, you might not know whether it has been modified unless you know that it has been sent directly to you by the right person. Similarly, the cryptography can provide the integrity service but it is useless unless authentication for the data origin is provided. Therefore, it should always be combined with authentication system. As the result, integrity service guarantees the content of the data, but it could not verified that the content has not been tampered from the original data.

- **Authentication**: It can help you to know that who is the sender of the sealed letter and the letter is passed without being tampered from the right person to you. The cryptography provides user authentication and data authentication. The user authentication guarantees that the user's communication to another user is accessed through the right communicator (server). The data authentication governs that the data has not been modified (data integrity) and the sender of the letter (data origin authentication).

- **Non-repudiation**: The sender cannot deny sending the letter if there is specified signature (certificate) inside the letter. The cryptography provides the non-repudiation that protect against any refusal by one of the parties involved in all or a portion of the communication. There are two types of non-repudiation in terms of: (1) origin proof, and (2) delivery proof. Non-repudiation with origin proof guards against any attempt by the sender to repudiate having sent a message. On the other hand, non-repudiation with delivery proof defences against any attempt by the recipient to falsely receive a message.

B. Related Work

Basically, cryptography is technically classified into two groups, symmetric and asymmetric key cryptography. Since our research focuses on the security aspect of transaction in mobile network, it is therefore necessary to review the existing security mechanism in our paper.

This section provides a general overview on the five well-known symmetric key cryptographic algorithms. The cryptographic algorithms covered are: Data Encryption Standard (DES), Triple Data Encryption Standard (3DES), Skipjack, RC5 and Advanced Encryption Standard (AES).

1) Data Encryption Standard (DES)

DES is a.k.a Data Encryption Algorithm (DEA) by ANSI and ISO [14], [15]. It was previously the most widely used symmetric algorithm with 64 bits data block and the encryption key [16]. The encryption key is basically 64 bits binary composing of 56 bits for information and 8 bits of parity. The 8 bits are used to detect error and are not employed to encoding data process. As such, the encryption key length of the DES is 56 bits [14], [17], [18], [19].

According to [20], the DES algorithm is based on Feistel cipher, which use to process two half blocks in a swapping fashion. All of 16 rounds are used in the DES, and every single round has a function *f* with associated key from key schedule and XOR operation.

There are several weaknesses in DES. Firstly, the key length is insufficient to resists attacks. In studies respectively, Diffie and Hellman, the inventors of the public-key cryptography, claimed that a $20 million machine with a million specially designed VSLI chips, each capable of searching one key per second and working in parallel, could break a DES-encoded message in about a day [21], [22]. The second weakness is that the design of the DES is not robust enough to resist attacks. Jorstad and Smith [15], it reported that the best attacks on DES is the brute force attack, differential and linear cryptanalysis (differential and linear cryptanalysis both are computationally complex). Successful cryptanalytic attacks, in general, require substantial quantities of plaintext-cipher pairs. Third, the DES is several weak keys. They also reported that there are four "weak" keys that, if selected, may decrease the security of DES by a factor of two.

2) Triple Data Encryption Standard (3DES)

The 3DES is a.k.a. Encryption-Decryption-Encryption (EDE). It is also referred to as the Triple Data Encryption

Algorithm (TDEA) [15], [19]. The 3DES is a minor variation of the DES [23]. The single DES reviewed earlier suffers from limited key length. As the result, the 3DES technique was developed to expand the length of DES keys and, thus, strengthen the security. The 3DES algorithm uses an ordinary DES with 16 rounds and typically ciphers each block of plaintext as encrypt, then decrypt and finally encrypt the block of plain text again by using different keys. Hence, the name 3DES is derived from this iterating cipher action. The double DES technique is not used because it includes serious cryptographic weakness and result of the double DES would be equivalent to single encryption with a single 56 bits key [23].

Most 3DES implementation uses two keys; however, 3DES can use two 112 bits or three keys 168 bits [15], [19]. Nevertheless, the 3DES with two keys is more commonly used compared to three keys because of the computation for 2^{112} possible keys is beyond what is practical now [23]. The 3DES performs encryption, decryption, and encryption (EDE) operations by different keys instead of encryption, encryption and encryption (EEE). The 3DES is formerly popular being used as security protection in the financial programming and ATM machine. However, since the evolution of AES, 3DES popularity has drop tremendously.

One of the weak points of 3DES is encryption and decryption process time is three times longer than single DES. Another disadvantage is that both DES and 3DES use 64 bits block size. A large block size is usually more desirable as it more efficient and secured.

3) Skipjack

Skipjack is a symmetric block cipher and developed by National Security Agency (NSA) [18], [24]. The skipjack algorithm is implemented for use of the PC cards, which are single chip crypto processors. The Skipjack is based on the Feistel design, which is cipher design that breaks input into two equal size blocks and swaps them repeatedly cycled through the algorithm while encryption process is then repeated a number of times. It uses 64 bits plain text block and produces 64 bits block cipher text. Encryption key used in the skipjack is 80-bits, and iterative 32 rounds are used in this cipher.

Skipjack is anticipated to be better than DES with 56 bits. The cipher initially proposed to encrypt all levels of the classified data but subsequently, the cipher was declassified due to the secret trapdoor found in Skipjack. This may be due to an oversight by the designers, or it was left with a intention [25]. As the result, Skipjack was declassified by the NSA in June of 1998. Nevertheless, the early cryptanalysis has failed to find any other significant weakness in this cipher besides the secret trapdoor. The best know public cryptanalysis on this cipher is 31 rounds with impossible differential cryptanalysis [26].

4) RC5

The RC5 is a symmetric block cipher designed by Prof. Ronald Rivest in 1994 [27]. This cipher has a word-oriented architecture for variable word size, w=16, 32, or 64 bits [28]. The round number, key length and block size of this cipher are variable but the "nominal" choice of parameters is 32 bits words, 12 rounds and a 16 bytes key, referred to as RC5-32/12/16. In this cipher, rotation operation and the mixed use of the XOR and addition of words are utilized heavily. Thus, it offers simple implementation and easy analysis than many other block ciphers.

One of the weakness in the RC5 is there exists several weak keys. However, this weakness is not very dangerous in practice despite the fact that the weak keys should be avoided in the implementation if possible [29], [30]. The best known public cryptanalysis on this cipher is 12 rounds with RC5 (with 64 bits block) that is susceptible to a differential attack using 2^{44} chosen plaintext [31].

5) Advanced Encryption Standard (AES)

AES is a modern symmetric block cipher and is widely used as the c standard algorithm [32]. It was a successor of DES [33]. The AES algorithm was designed by two Belgium cryptographers named Daemen and Rijmen in 2001. AES has 128 bits block length and allows encryption with three different key lengths, which comprises 128 bits, 192 bits and 256 bits respectively. The number of the rounds in the ciphers depends on the key length; it is an either 10, 12 or 14 rounds. AES operates 128 bits plaintext blocks, which are organized in quadratic arrays (states) of 16 bytes and produces the same 128 bits ciphertext blocks.

AES is evaluated to be more efficient than DES [34]. AES is on average about three times faster compared to its predecessor, 3DES. However, it spends almost the same time when it operates on little amount of the data, especially, when the data amount is less than 16 bytes. This is because the state in AES consists of 16 bytes.

The best known cryptanalysis on this cipher is related to key attack that can break the 256 bits AES with complexity of 2^{119}. Another attack known as the chosen plain text attack can breaks 8 rounds of the 192 bits and 256 bits of AES, and also 7 rounds of the 128 bits AES. However, this workload is impractical at 2^{128} [35].

III. Proposed Framework

This research focuses on the security data transaction between the base station (BS) and the mobile nodes (MN) of MCTO over the insecure wireless network. In research frame, this pilot explore a suitable security model to mobile data transmission of the MCTO and build strong security system which we named it as SMCTO (Secured MCTO) to the insecure transaction by using cryptographic model. Fig.1 depicts the architecture of SMCTO.

The system model consists of one personal computer (PC), two laptop computers and a wireless router switch as illustrated in Figure 4.1. The personal computer represents one of the BS(s) that manages part of master database (DB) in the fixed network. The two laptop computers represent various Mobile Nodes (MN(s)) that connect to the BS over the wireless network. The wireless router switch acts as wireless access points that used to establish the wireless connection between the BS and MN(s).

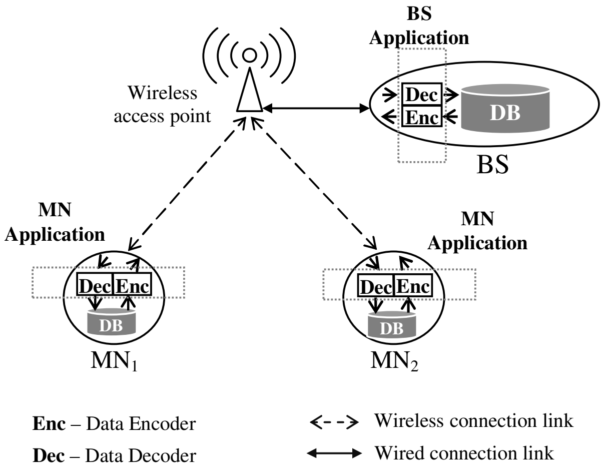


Fig.1 The framework for SMCTO

General structure of designed protection model is presented in Fig 2. The model is based on symmetric cryptographic system to encrypt data and combined with asymmetric cryptographic system to exchange secret key. The SMCTO mobile database transaction security model is a set of the models which are generally consisted of data encryption, data decryption, key encryption, key decryption and client authentication models. The set is resided and performed at both BS and MN(s). When a MN has an access to the BS, the connection between the BS and MN is confirmed through the client authentication model. If access is accepted by the authentication, connection is established else the access and connection are denied. Once the connection is established, the data at the sender (either at BS or at MN) is encrypted via encryption model, and key of encryption is encrypted via key encryption component. The encrypted data and key are combined and transferred through the established wireless connection to the receiver (either at BS or at MN). After the encrypted data and key are received, the encrypted key is decrypted firstly via the key decryption component, and then the encrypted data is decrypted via the data decryption model.

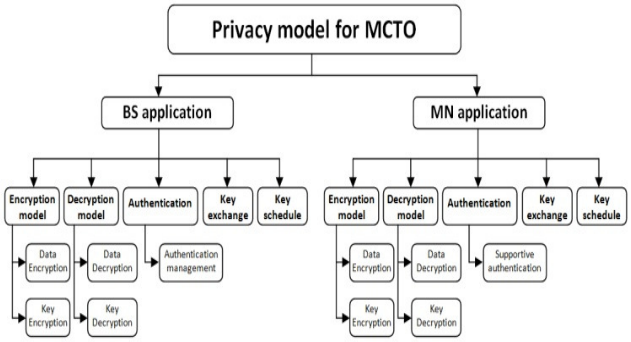


Fig.2 Basic structure in the designed model

IV. Summary, Discussion and Future Work

We had reviewed on the symmetric key based on the five common ciphers. Each cipher shows its vulnerability in the Confidentiality of data security. Table 1 depicts the comparison on the five ciphers reviewed earlier. Most of the cipher algorithms are designed for huge data size of encryption and decryption processes. We observed that the process of encryption and decryption spend the same amount of time for the smaller dataset. Therefore, a suitable secure cipher algorithm is needed if the encryption and decryption is merely for small amount of data such as in the mobile database environment.

TABLE I
COMPARISON ON THE VARIOUS CIPHERS

Cipher	Pros	Cons
DES	Process speed fast	Short key length and cracked several times. De facto standard
3DES	3 key options and last key is stronger	Slower process time and 3 times slower than usual DES
Skipjack	Stronger than usual DES and Confidential data encryption cipher was	Secret trapdoor included and vulnerability appeared. Restricted from confidential data encryption
RC5	Suitable for both hardware and software, Simple implementation	Several weak keys attached in key schedule and suspected to some attacks.
AES	Stronger 3 key options and considered as fast	Suspected to several attacks but impractical. no time difference at little amount of data encryption

In our future work, we will implement the SMCTO and compare the performance of SMCTO against other security models in terms of the process speed, number of rounds, key length and so on for encryption and decryption operation. Finally, the implemented model could protect data transaction of the MCTO and satisfy confidentiality and authenticity of the security properties by using the encryption and authentication model.

REFERENCES

[1] Notargiacomo, L. (1994). *Architecture for MLS database management system.* Information Security: An integrated Collection of Essays. Essay 19.

[2] Lubinski, A. (1998). Security issues in Mobile Database Access. *International Working Conference on Database Security XII: Status and Prospects*, 223 – 234

[3] Lubinski. A, *Adaptation Concepts for Mobile Database Security*. University of Rostock, Rostock, Germany, 2000.

[4] Garuba, M. (2005). Impact of external security measures on data access implementation with online database management system. *International Conference on Information Technology: Coding and Computing*, Vol.1, 243 -248

[5] Drosatos, G. C., Efraimidis, P. S., and Karakos, A. (2006). *Secure Mobile Database Application: A Case Study*. Greece: Technical report.

[6] Forouzan, B. (2007). *Data Communications and Networking* (4th Ed). Singapore: Mc Graw Hill, ISBN 007-125442-0.

[7] Afyouni, H. A. (2006). *Database Security and Auditing: Protecting Data Integrity and Accessibility*. Thomson Course Technology. Boston, MA, United States.

[8] Wehmeier, S., Mclntosh, C., Turnbull, J., and Ashby, M. (2005). *Oxford Advanced English Dictionary*. Seventh edition

[9] Lu, Q. (2002). *Vulnerability of Wireless Routing Protocols.* University of Massachusetts, Amherst.

[10] Popescu, B.C., Gamage, C., and Tanenbaum, A. S. (2002). *Acess Control Reverse Access Control and Replication Control in a World Wide Distributed System.* Proc. 6th IFOP Communications and Multi security Conference, Portoroz, Slovenia.

[11] Popescu, B. C., Crispo, B., and Tanenbaum, A. S. (2003). *Secure Data Replication over Untrusted Hosts.* In Proc 9th Workshop on. Hot Topics in Operating Systems (HotOS IX).

[12] Herlihy, M. P., and Tygar, J. D. (1987). How to Make Replicated Data Secure. *Lecture Notes In Computer Science,* 379-391

[13] Abdul-Mehdi, Z., Mamat, T., Ibrahim, H., and Dirs, M. (2006b). Multi-Check-Out Timestamp Order Technique (MCTO) for Planned Disconnections in Mobile Database. *International Conference on Information and Communication Technologies*, Vol.1, 491-498.

[14] Bruce, S. (1996). *Applied Cryptography* (2nd Ed). Hoboken, NJ, US: John Wiley and Sons, Inc.

[15] Jorstad, N. D., and Smith, L. T. (1997). *Cryptographic Algorithm Metrics*. Available: http://csrc.nist.gov/nissc/1997/proceedings/128.pdf [2007, March 16].

[16] William, M. D., and Raymond, G. K. (1999). *Data Encryption Standard (DES)* US: Federal Information processing Standard (FIPS), Publication 46-3.

[17] Menezes, A., Oorschot, P. V., and Vanstone, S. (1996). *Handbook of Applied Cryptography.* Boca Raton, FL: CRC Press LLC.

[18] Keller, S., and Smid, M. (1998). *Modes of Operation Validation System (MOVS):Requirements and Procedures*. Gaithersburg, MD 20899: National Institute Standard Technology.

[19] Stamp, M. (2006). *Information Security Principles and Practice*. Hoboken, New Jersey: John Wiley and Sons, Inc. ISBN-10 0-471-73848-4 (cloth) ISBN-13 978-0-471-73848-0.

[20] Mao, W. (2004). *Modern Cryptography: Theory and Practice.* New Jersey, USA ISBN: 0-13-066943-1.

[21] Bruce, S. (1996). *Applied Cryptography* (2nd Ed). Hoboken, NJ, US: John Wiley and Sons, Inc.

[22] Landau, S. (2000). *Standing the test of time: The Data Encryption Standard.* Notices of the American Mathematical Society 47(3) 341-349.

[23] Stallings, W. (2006). *Cryptography and Network Security: Principles and Practices*. (4th Ed) Upper Saddle River, NJ: Prentice Hall. ISBN-10: 0-13-187316-4, ISBN-13: 978-0-13-187319-3.

[24] National Security Agency. (2001). Specification for the Advanced Encryption Algorithm. US.

[25] RSA Data Security, Inc. (1998). RSA Laboratories' Frequently Asked Questions About Today's Cryptography. v 4.0 US: RSA Data Security, Inc.

[26] Biham, E., Biryukov, A., and Shamir, A. (2005). Cryptanalysis of Skipjack Reduced to 31 Rounds using Impossible Differentials. *Journal of Cryptology, 18(4)***,** 291 – 311.

[27] Kaliski, Jr. B. S., and Yin, Y. L. (1998). *On the Security of the RC5 Encryption Algorithm.* (RSA Laboratories Technical Report). US: RSA Laboratories, a division of RSA Data Security, Inc.

[28] Menezes, A., Oorschot, P. V., and Vanstone, S. (1996). *Handbook of Applied Cryptography.* Boca Raton, FL: CRC Press LLC.

[29] Heys, H.M. (1997). Linearly weak keys of RC5. *Electronic Letters*, 33(10), 836 – 838.

[30] Elbaz, L., and Bar-EI, H. (2000). *Strength Assessment of Encryption Algorithm* (white paper). CA, US: Discretix Technologies Ltd.

[31] Biryukov, A., and Kushilevitz, E. (1998). Improved cryptanalysis of RC5. *Lecture Notes in Computer Science*, Volume 1403/1998, 85-99

[32] Scheidemann, V. (2007). *Rijndael –the Advanced Encryption Standard (AES).* Technical white paper.

[33] Shafi, G., and Mihir, B. (2001). *Lecture Notes on Cryptography.* pp.53.

[34] Denis, T., and Johnson, S. (2007). *Cryptography for Developers*. Hingham Street, Rockland, MA, US: O'Reilly Media, Inc.

[35] Ferguson, N., Schroeppel, R., and Whiting, D. (2001). A simple algebraic representation of Rindael. [Online]. Available: http://th.informatik.uni-mannheim.de/people/lucks/papers/Ferguson/RdAlgEq.pdf [2007, March 6]