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 in 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 resist 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 VLSI 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
The round number, key length and block size of this cipher architecture for variable word size, w=16, 32, or 64 bits [28]. Ronald Rivest in 1994 [27]. This cipher has a word-oriented impossible differential cryptanalysis [26]. The best known public cryptanalysis on this cipher is 31 rounds with weakness in this cipher besides the secret trapdoor. The best known cryptanalysis on this cipher is related to key attack that can break the 256 bits AES with complexity of $2^{128}$. Another attack known as the chosen plaintext 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 (Secure 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).
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.

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

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