Security Model for the MCTO Data Transaction Management

Ziyad Tariq Abdul-Mehdi, Byambasuren Byamba and Mohammad M. N. Hamarsheh

Faculty of Information Science and Technology, Multimedia University, Melaka, Malaysia

Abstract

In this paper work is related with security model for the Multi Check-out Timestamp Order (MCTO) data transaction. By research, weakness of the MCTO is determined and considered as security risk involved with data transmission over the wireless network. Since the research focused on this vulnerability, it has explored regarding with a suitable security transmission management system to the MCTO data transaction. During the research, a fully secure transmission model is found and designed. This paper discuss about the security model, which is based on a hybrid cryptography system, is used to encrypt and decrypt data for the security transmission between Base Station (BS) and Mobile Host (MH)for the MCTO model.

Key words:
Data network security, Data transmission security, Hybrid cryptography, Authentication, Comparison

1. Introduction

Data security is one of the most important issues for modern information technology. Recently a several research papers concentrated on the security database that involved with data transmission. The published articles discussed about data transaction security management in the distributed database that has not solved yet. In previous study of this research, four data transaction models were covered and discussed. The MCTO model [1, 2, 3], which is one of the four data transaction models, has been resolved some solutions in the other data transaction models and has gained less problem. The main idea of this model is that transaction execution can be done at the BS and MH(s). The main advantages of this model are recovered all the transactions management models from other three models and good data allocation management. These cases influenced that the MCTO is selected from the four models and developed for the further secure data transaction model. However the model resolved some problems, the model still has weakness. The major weakness of the MCTO model is that data transaction over the wireless network is performed without security.

Manuscript received June 5, 2008.
Manuscript revised June 20, 2008.

This unsafe condition makes vulnerability to the MCTO model. The vulnerability is showed in the figure 1.

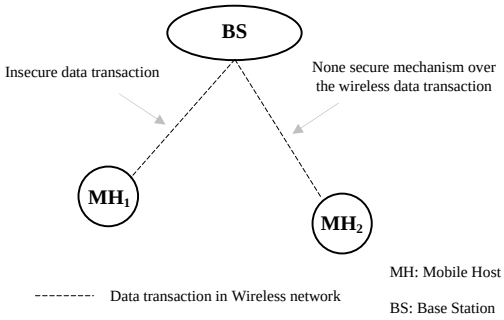

Fig. 1 Insecure transmission for the MCTO data transaction

After the MCTO function at the BS allocates portion of the data to the MH, the data is transferred from the BS to the MH though the wireless network without security. It is also same at opposite data transaction. The data at the MH is transferred to the BS through the insecure wireless channel. This insecure data transaction of the MCTO makes unsafe condition in the system. When the unsafe condition in the model, it always keep easy possibilities to the hackers and attackers to damage, delete and steal the data. During the research, fundamental knowledge and understanding of security and cryptography [4, 5, 6,…, 25] are taken and studied previously. This research explored a suitable security model over transmission of the MCTO data transaction and built strong security data transmission channel by using cryptographic model.

2. Motivation

2.1 Proper security model: Cryptography

In most cases, the security of information technology focused on the cryptography that encrypt plain data and decrypt the encrypted data for protecting data against attacks, any malicious actions and other kind of dangers. This research has started to explore a proper security model to the insecure data transaction of the MCTO since the vulnerability determined. During the research, a fully secure transmission model is found and designed.

The security model, which is a hybrid cryptography system, is consisted of encryption and decryption model with authentication system. The encryption model is used to encrypt data before it is transferred, and the decryption model is used to decrypt the encrypted data after it is received. The authentication model assumes the MH connection to the BS. The encryption and decryption models with authentication model are combined together as single set application that is worked at both the BS and MH(s) as shown in figure 2.

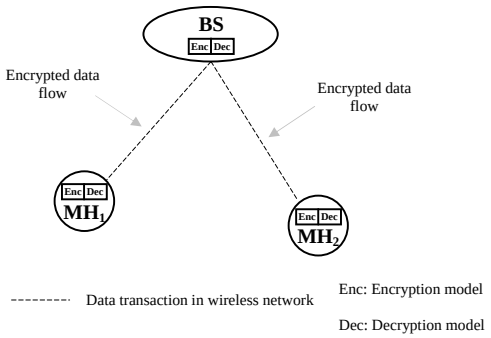

Fig. 2 Secure data transmission for the MCTO

Every data transaction between the BS and MH is encrypted by encryption model before the data is transferred, and after the encrypted data is received, it is decrypted by decryption model. Before the data transaction between the BS and MH is operated, the MH connection to the BS is assured by the authentication model. The authentication model assumes that the MH verification is correct or not. Once the connection is accepted, the MH is approved to operate the data transaction.

2.2 Internal architecture of the security model

The encryption model, which is a hybrid key cryptography, consists of the *data encryption model* and *key encryption model*.

The *data encryption model*, which is symmetric key encryption cipher and consists of the data encryption functions and a key generator, is used to encrypt data. The encryption functions, which are collection of conversion, expansion, inversion and three rounds with Inverse, Shift and Substitution operations, is used to encrypt data. The key generator, which is a function that generates random key, supports generating key to the Inversion operations. The *key encryption model*, which is hybrid key encryption cipher and consists of key encryption functions and key exchange protocol with an authentication model, is used to encrypt key *(symmetric key)* of the data encryption model. The key encryption functions are collection of the inverse shift and substitute operation with 4 rounds. The key exchange protocol is Diffie Hellman key exchange protocol that is used to establish key encryption key (shared secret key). The authentication model is used to approve correctness of the MH connection between BS and MH. Figure 3 shows general structure of the encryption model that includes data encryption model and key encryption model which consists of key encryption model, key exchange protocol and authentication model.

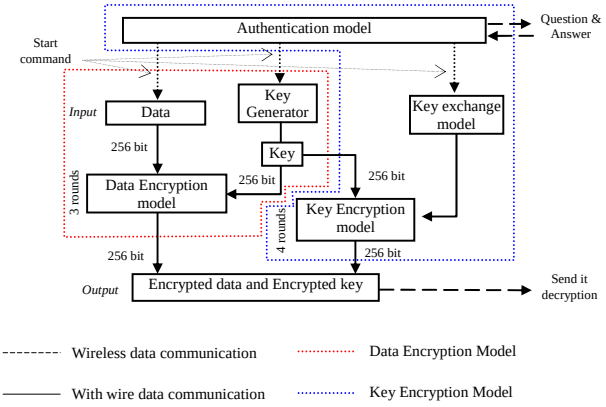

Fig. 3 Internal structure of the encryption model

When the MH connects to the BS, the authentication model at the BS checks the connection of the MH and approves the MH as hand off or hand on. If the MH approved as hand on then it can be received data from the BS. Otherwise the BS rejects the MH connection as hand off. The MCTO model has own data allocation function that allocates portion of the data to the MH, which connected and wanted data with hand off (disconnection). The function supports input data to the data encryption model. The data allocation function is shown in function 1

$$\delta_i = f(n_i, m_i) = \left\lfloor \frac{((AV + (\varepsilon * r)) * d)}{n_i + m_i} \right\rfloor \qquad (1)$$

Where, n_i = number of new mobile hosts that wants hand off with data; m_i = the number of previous MH wanted hand off with data; r = reconnection number; d = current data at the BS; AV= average and usually form 0 to 1 the average equal to 0.5; ε is a smallest increments number for MH who multi visited BS.

Once the MCTO function calculates the portion of the data to the MH(s), the portion of the data is encrypted by encryption model and transferred to the MH.

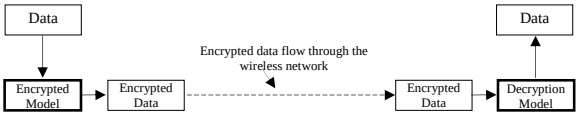

Fig. 4 Internal structure of the encryption model

When the encrypted data is received at the MH, it is decrypted by decryption model.

The decryption model is consisted of the data decryption and key decryption models. The data encryption model is collection of the inverse, shift and substitution operations. The key encryption is consisted of key encryption model and key exchange protocol with authentication model as shown in figure 4.

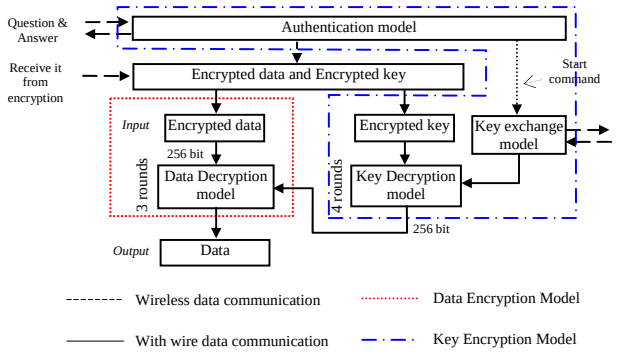

Fig. 4 Internal structure of the decryption model

After decryption, the decrypted data at the MH can be executed. The execution update (*update data*) at the MH is encrypted by encryption model before it is transferred back to the BS. The *update data* encryption process at the MH is same with data encryption at the BS. After the encryption, the encrypted data at the MH is transferred to the BS as shown in figure below.

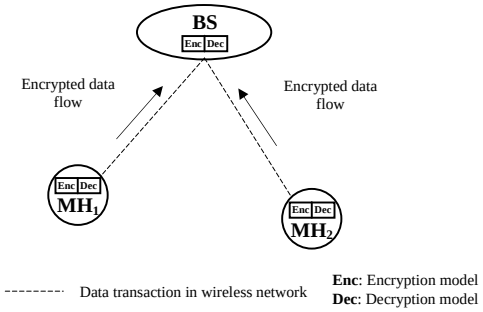

Fig. 5 Encrypted data flow to the BS

After the encrypted *update data* is received at the BS, it is decrypted by decryption model. The decryption process is same with the decryption at the MH. The decrypted *update data* is re executed at the BS and update to the master data by MCTO function 2.

$$d = d - (update.data - \delta_i) \quad (2)$$

If the *update data* at the MH was requested more than balance at the MH then it would be a *requested data* and it is encrypted with *update data* by encryption model and transferred to the BS. Once encrypted data is received at the BS, the requested data with update data is decrypted by decryption model, and update data is updated to the master data at BS firstly by function 3. After that requested data is updated. If only requested data is received at the BS, the requested data is updated directly to the master at BS by MCTO function 3.

$$d = d - requested.data \quad (3)$$

Update notification is sent to the MH after update and requested data is done. If the master data at the BS is not enough to the requested data then the BS send abort message to the MH else the BS sends a successful message to the MH.

2.3 Design and structure of the security model

The security model, which is hybrid cryptography, is consisted of encryption model and decryption model. The encryption model includes *data encryption model* and *key encryption model*.
The *data encryption model* contains data encryption functions and key generator as shown in figure below.

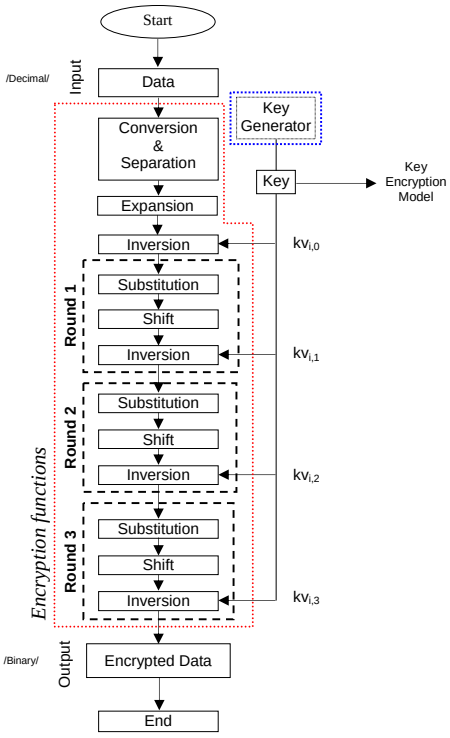

Fig. 6 Data encryption model

The data encryption functions, which are used to encrypt data, include Conversion, Separation, Expansion, Inversion operations with three rounds; each round consists of Substitute, Shift and Inverse operations as shown in Figure 6.
The key generator, which is a function in java, generates key data in 8 bits randomly.

2.3.1 Operation in the data encryption functions

The Conversion operation in the data encryption model is used to convert number (0 ÷ 4294967295) in the decimal data to binary data in 32 bits by a using conversion technique as shown conversion part in figure 7. The conversion method is based on the division of 2. Each division result takes a reminder as “0” or “1”. The reminder is given from an initial number until to the reminder value is reach to “0”. If dividing number is even, the reminder takes “0”. If the number is odd then reminder takes “1”. For example, an initial input data is 150 then initial value is even number and takes reminder as “0”. After a reminder, the number is divided by 2. Divided result is equal with 75, and it takes a reminder as “1”. The 75 is divided by 2, and the 37 takes a reminder “1”. The 37 divided by 2, and 18 takes a reminder as “0”. The 18 is divided by 2, and 9 takes a reminder 1. The 9 is divided by 2 and 4 takes a reminder 0. The 4 is divided by 2 and 2 takes a reminder as “0”. The 2 is divided by 2, and 1 is takes a reminder “1”. The 1 is divided by 2, and 0 is takes a reminder “0”. After division reach to the 0, the reminders from initial reminder to last reminder can express a value of 150 in 32 bits binary as shown in figure 7.

In the separation operation, the converted 32 bits are separated to the 4 eight bits (V_1, V_2, V_3, V_4) as shown separation part in figure 7.

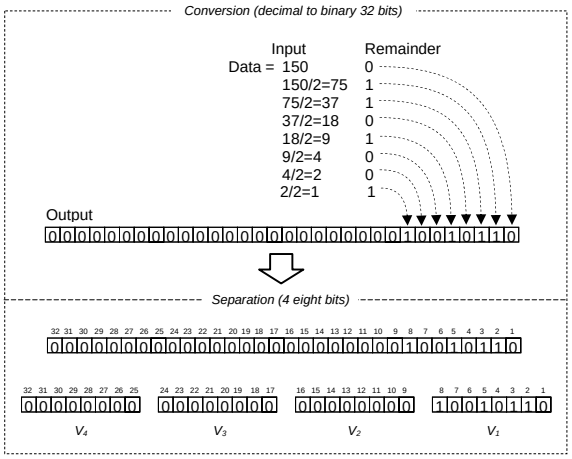

Fig. 7 Conversion and separation operations

In the expansion operation, input V_i byte (eight bits) is extended to 4 bytes (four separated eight bits). After that, each of them is duplicated 7 times down as shown in figure below. They are 28 bytes, and initial 4 bytes are added to the 28 bytes then they all become 32 bytes $V_{i,32}$ (256 bits).

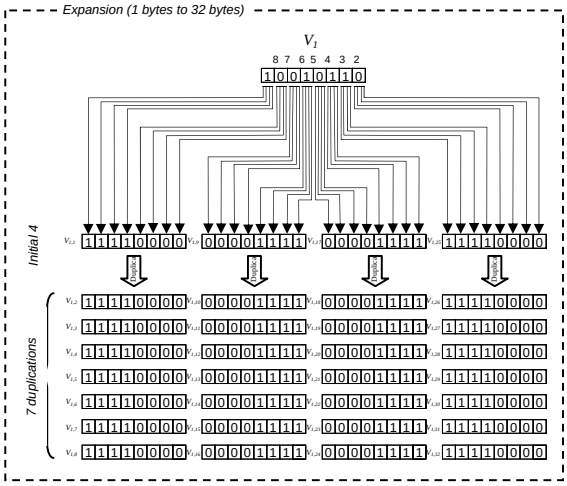

Fig. 8 Expansion operation in the data encryption model

The inverse operation is combination of the input data $V_{i,j}$ and encryption key ($kv_{i,j,m}$) by XOR operation as shown in figure 4.9. The XOR is mathematical operation and is used to inverse digits of the input data, stands for Exclusive-Or. The simple calculation of the XOR operation: /1⊗1=0; 1⊗0=1; 0⊗1=1; 0⊗0=0/.

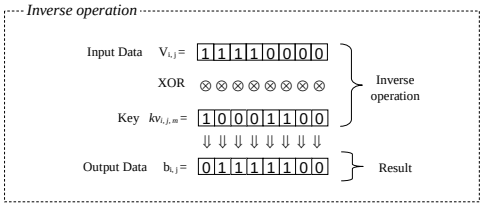

Fig. 9 Inversion operation in the data encryption model

For instance, input data $V_{i,j}$=10010110 is combined with a key $kv_{i,j,m}$=01110011 by the XOR operation. The result is $b_{i,j}$ = 01111100.

The Substitution operation operates that input data $V_{i,j}$ is substituted to another output data $b_{i,j}$ by a using S-Table as shown in figure 10. The S-table (a. k. a S-box), which is Rijndael substitution table, is used to substitute one byte to another one byte. The table was specially designed to resistant to linear and differential attack. For example, Input data $V_{i,j}$ = 00011110 then output data $b_{i,j}$ = 01110010 as shown in Figure 10. Note: "$V_{i,j}$" is input data and "$b_{i,j}$" is output data. The output data $b_{i,j}$ is equal with the input data $V_{i,j}$ in next operation. Then Shift operation in second round is committed after the substitution in the round.

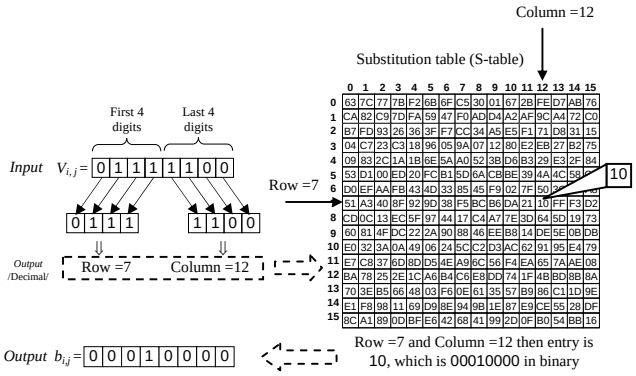

Fig. 10 Substitution operation in the data encryption model

The Shift operation performs that ever digit in the input data $V_{i,j}$ is shifted cyclically to the left side by 3 digits as shown in Figure 11.

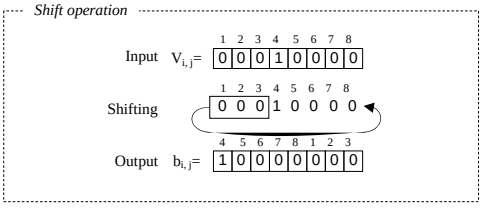

Fig. 11 Shift operation in the data encryption model

The inversion operation in each round is same with previous an inversion operation. The Inversion operation is used that an input data $V_{i,j}$ is combined with a key data $kv_{i,j,m}$ to another output data $b_{i,j}$ by XOR operation as shown in Figure 12. The key $kv_{i,j,m}$ is generated randomly in 8 bit binary by a using key generator.

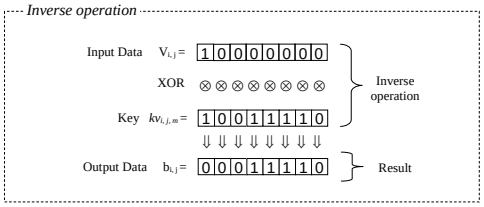

Fig. 12 Inverse operation in the data encryption model

The XOR, which is mathematical operation, stands for Exclusive-Or and is used to inverse digits of the input data. The simple calculation of the XOR operation: /1⊗1=0; 1⊗0=1; 0⊗1=1; 0⊗0=0/.

The *key encryption model* includes key encryption functions, key exchange protocol, key extension section and authentication model.

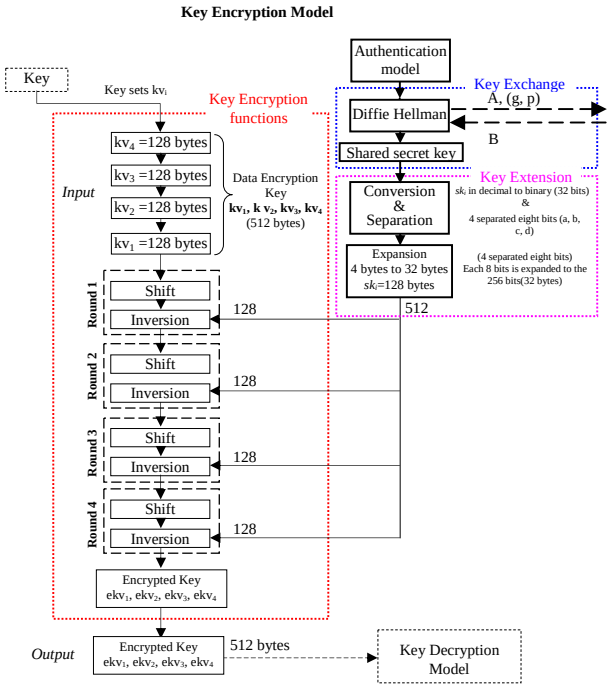

Fig. 13 Structure of the key encryption model

The key encryptions include four rounds. Each round contains Shift and Inversion operations. The shift and inverse operations are same with previous shift and inverse operations as shown in figure 11 and in figure 12.

The key exchange protocol is based on the Diffie Hellman (D-H) that is used to establish shared secret key between the BS and the MH. Simple D-H key exchange protocol does not support any authentication or verification. Therefore D-H is vulnerable to the man in the middle attack. There are many possible solutions on the authentication of the DH that may use digital signatures, the password based, cryptographic tokens, keys, biometrics and other cryptographic protocols. In this model, one of classic authentication methods, which involves the "human aspect" of authentication, is involved and implemented as using "life questions" or users to vouch for one another. The Life Question that authentication is a form of user verification that exploits personal data to validate identities, and process of the authentication is followed as shown in Figure 14. This life question authentication is related with the password based authentication model.

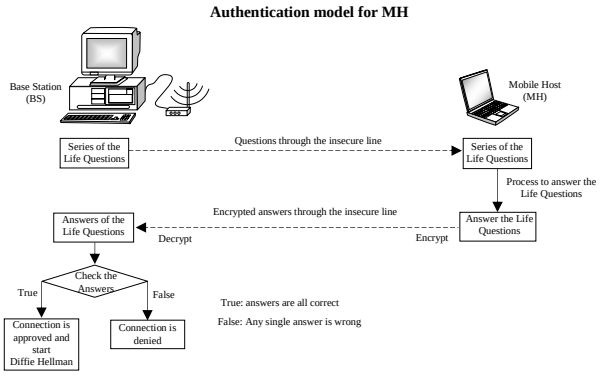

Fig. 14 Life question based authentication model

Users are presented with "life questions" for which the answers are theoretically known only by them. Such questions generally involve personal characteristics and preferences, life events or transactional facts. The Life Questions, which are serial of the questions, are selected tightly related with user's personal data.

List of the simple serial Life Questions:

a. What is your mother name?
b. What was your first teacher's name of elementary school?
c. What make was your first car or bike?

Most web users are familiar with c and b questions. However the design of a highly usable, the secure authentication system based on life questions is not easy.

Once the connection of the MH is accepted, the D-H is started to establish a shared secret key that is exchanged from the BS to the MH. For example, the BS selects two prime numbers g and p (g=13, p=97) and chooses an own secret number "a" (a=23) randomly, while calculate it as g^a mod p (13^{23} mod 97 = 39). After that, the BS transfers the result "39" only with g and p to the MH.

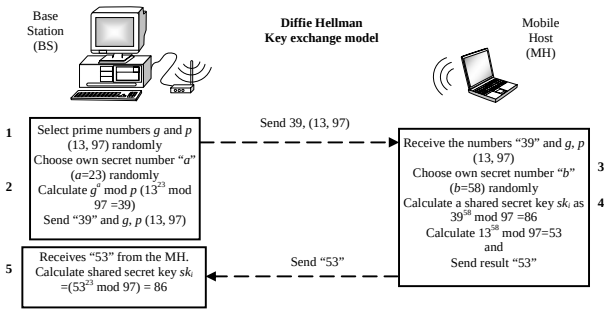

Fig. 15 Key exchange process by D-H

The MH receives the sending numbers "39", *g*, *p* (*g*=13, *p*=97) and agree with the numbers. The MH also chooses own secret number "*b*" (*b*=58) randomly and calculates their shared secret key sk_i as 39^{58} mod 97= 86. After that calculation, the MH calculates g^b mod *p* as 13^{58} mod 97 = 53 and send result "53" only to the BS. Now, the BS receives the result "53" and calculates a shared secret key sk_i as 53^{23} mod 97 = 86. After the shared secret key is established, the key is extended into extension part.

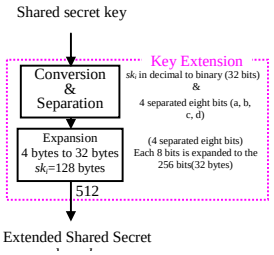

Fig. 16 Key extension in the key encryption model

The key extension part consists of three operations: conversion, separation and expansion. The operations are used to extend a shared secret key sk_i 32 bits to 1024 bits (128 bytes) and provide the extended keys to the key encryption functions. Figure below shows the extension process.

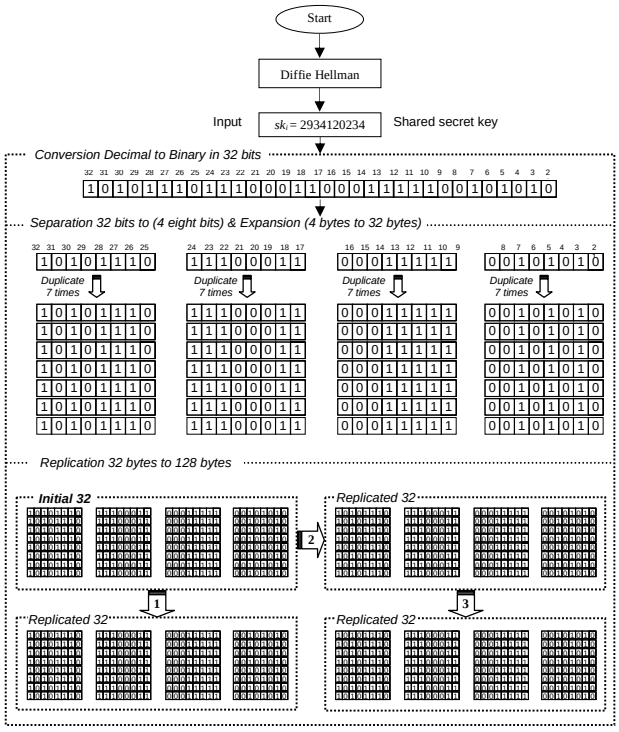

Fig. 17 Shred secret key extension in the key encryption model

After the shared secret key is extended, the key is transferred to the Inversion operation in the key encryption model.

The data decryption model, which is used to decrypt the encrypted data and encrypted key, consists of the *data decryption model* and *key decryption model* as shown in figure 18.

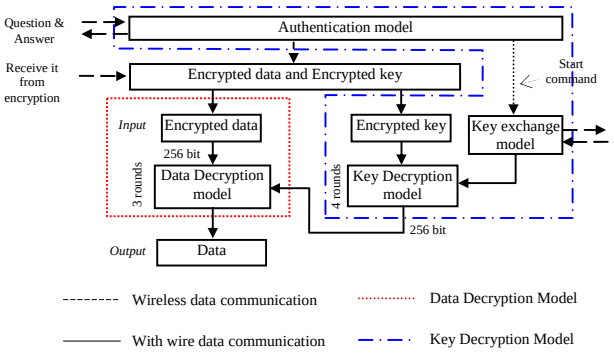

Fig. 18 Decryption model

The *data decryption model* is used to decrypt the encrypted data when it is received from the encryption. The data decryption model consists of data decryption functions that include Inverse, Reduction, integration, conversion operation and 3 rounds as shown figure 19.

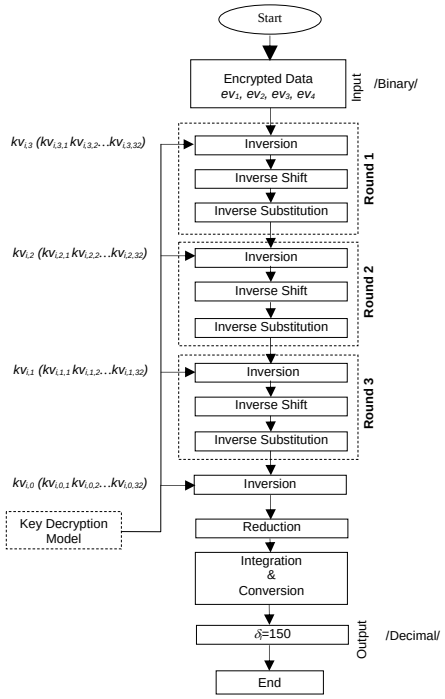

Fig. 19 Data decryption model

Each round has 3 operations: Substitution, Shift and Inverse. The three operations inside the round are same with previous operation's working principle but direction of the operation or using table in substitution are different.

2.3.2 Operation in the data decryption functions

The inverse in the decryption model is that input data ($ev_{i,1}$…$ev_{i,31}$) are combined with key data ($kv_{i,\ 1,\ m}$…$kv_{i,\ 32,\ m}$) to another output data ($b_{i,\ 1}$…$b_{i,\ 31}$) one by one by XOR operation as shown in Figure 20. The encrypted keys ($ekv_{i,\ 1,\ m}$…$ekv_{i,\ 32,\ m}$) are received and decrypted by the key decryption model. After that, the decrypted key ($kv_{i,\ 1,\ m}$…$kv_{i,\ 32,\ m}$) is supported as key in inversion operation in the data decryption model.

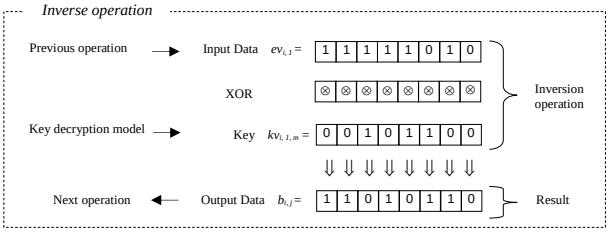

Fig. 20 Inverse operation in the decryption model

The Shift operation in the decryption model performs that each digit in the input data $ev_{i,1}$ is rotated to the right by 3 digits. For example, each digits of input data $ev_{i,1}$=11010110 from previous inversion operation is shifted cyclically to right by 3 digits then output data is $b_{i,\ 1}$=11011010 as shown in figure below.

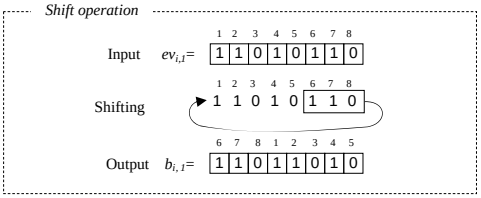

Fig. 21 Shift in the data decryption model

The Substitution in the data decryption model operates that input data $ev_{i,1}$ is substituted to the output data $b_{i,\ 1}$ by a using Inverse Substitution table (Inv. S-table). For example, input data $ev_{i,1}$ =11011010 is substituted to the output data $b_{i,\ 1}$=01111010 as shown in Figure 4.31.

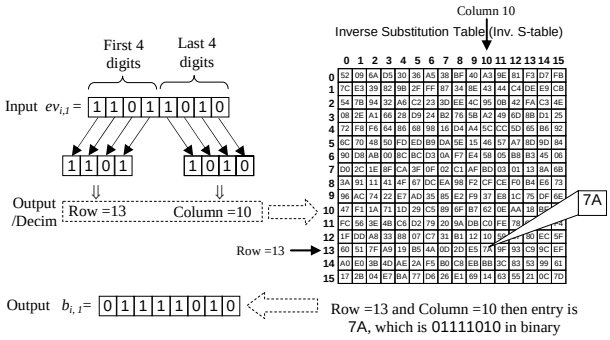

Fig. 22 Inverse Substitution in the data decryption model

Single inverse operation out of the round is same with inverse operation inside round. Main purpose of this inverse is to make re-inverse operation and back confusion of the encrypting data. The Reduction operates double operations: reduction operation and rejoining operation. The operations are that each ev_i , which includes 32 bytes ($ev_{i,\ 1,}$ $ev_{i,\ 2,}$ $ev_{i,\ 3,}$ …, $ev_{i,\ 32}$),of the separated data ($ev_{1,}$ $ev_{2,}$ $ev_{3,}$ ev_4) is reduced from 32 bytes to the initial 4 eight bytes ($v_{1,}$ $v_{2,}$ v_3 v_4), and the initial 4 eight bytes ($v_{1,}$ $v_{2,}$ v_3 v_4) are rejoined to the single byte as shown in the figure 23. For example, under the ev_i, there are related 32 bytes ($ev_{i,\ 1,}$ $ev_{i,\ 2,}$ $ev_{i,\ 3,}$…, $ev_{i,\ 32}$), and every byte inside the ($ev_{i,\ 2}$ to $ev_{i,\ 8}$) is combined to the $ev_{i,\ 1}$ byte. Next every byte inside the ($ev_{i,\ 10}$ to $ev_{i,\ 16}$) is combined to the $ev_{i,\ 9}$ byte. Another every byte inside the ($ev_{i,\ 18}$ to $ev_{i,\ 24}$) is combined to the $ev_{i,\ 17}$ byte. Last every byte inside the ($ev_{i,\ 26}$ to $ev_{i,\ 32}$) is combined to the $ev_{i,\ 25}$. Then every combined byte ($ev_{i,\ 1}$, $ev_{i,\ 9}$, $ev_{i,\ 17}$, $ev_{i,\ 25}$,) are rejoined to the single byte V_i (8 bits) as figure below.

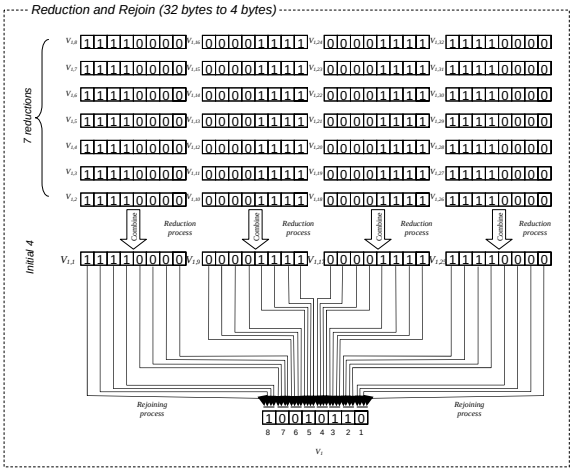

Fig. 23 Reduction in data decryption model

After each extended 32 V_i is reduced and rejoined to one byte V_i, the Integration operation is operated. The integration is that every single (V_1, V_2, V_3, V_4) is integrated to the one 32 bits as shown in figure 24.

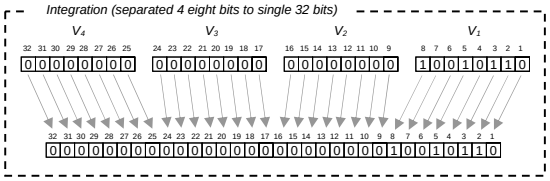

Fig. 24 Integration in data decryption model

Once the Integration is done, the conversion operation is continued. The conversion, which is one of the common binary to decimal conversion techniques, performs that the 32 bits in binary is converted to the decimal number by a using conversion technique. The figure below shows conversion method as well.

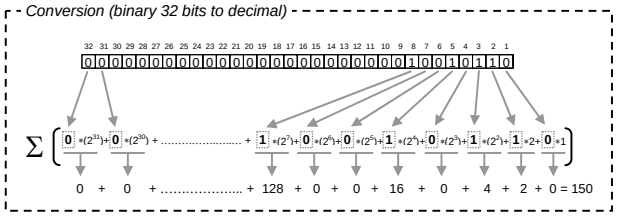

Fig. 25 Conversion in data decryption model

The multiplied digits are summarized, and the result is represented as an amount of the data in the decimal number. After the conversion is done, the converted amount of the data in decimal δ_l=150 can be updated locally at the MH.

The data update is stored at the MH until it is transferred to the BS. When the update data is transferred to the BS, the update data at the MH is encrypted by the encryption model. This encryption process is performed similarly with previous encryption at BS. After the encrypted update data is received at BS, it is decrypted by decryption model. The decryption process of the encrypted update data at the BS is performed same with the decryption process at MH.

The *key decryption model* is used to decrypt the encrypted key when it is received. The key decryption model includes the key decryption functions, key exchange and key extension parts as shown in key decryption model of figure 26.

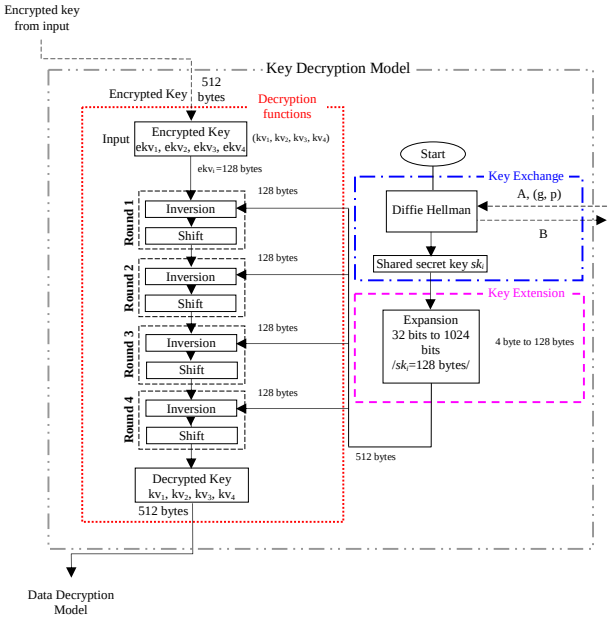

Fig. 26 Key Decryption model

Key decryption functions are used to decrypt the encrypted key by extended shared secret key. The functions consist of four rounds. Each round includes the Shift and the Inversion operations as show in Decryption function part in figure 26.

The Shift and Inversion operations in the decryption function are same with previous Shift and Inverse operation in the data decryption model as shown in figure 20 and in figure 21. The key exchange and key extension part are totally same with key exchange and extension at the key encryption model. Once authentication is done, the key exchange

5. Conclusion

The security is one of the most important issues in the data transaction management. By research frame, weakness of the MCTO is determined and considered as security risk involved with data transmission over the wireless network. Since the research focused on this vulnerability, it is explored a suitable security transmission management system to the MCTO data transaction. During the research, a fully secure transmission model is found and designed. The security model, which is a hybrid cryptography system, is used to data encryption and decryption for the security transmission. The model is consisted of encryption and decryption model with authentication system. The encryption model is used to encrypt data before it is transmitted. The decryption model is used to decrypt encrypted data after it is received. Authentication

system, which is password based authentication, assumes whether connection of the MH to the BS is accepted or rejected. If the connection was accepted, MH or BS could start security data transmission for the data transaction else the MH was rejected from system until connection is accepted. More over this security model is not only used in the wireless network but also it can be used through the wire network. Finally, this research work proposed efficient time to data transaction and strong security to data transmission.

References

[1] Abdul-Mehdi. Z and Hason. N. 2006 "Trusted Based Diagonal Replication on Grid Database", International conference For Business, Law and Technology, Copenhagen- Denmark, 5-7 December, Vol.2, p.p 441.

[2] Abdul-Mehdi. Z. T, Mamat. A. B, Ibrahim. H and Dirs, Mustafa.M. 2006."Multi-Check-Out Timestamp Order Technique (MCTO) for Planned Disconnections in Mobile Database", The *2nd* IEEE International Conference on Information & Communication Technologies*: from Theory to Applications* , 24-28 April, Damascus, Syria,Vol.1, p.p 491-498.

[3] Abdul-Mehdi. Z. T, Mamat.A, Ibrahim.H and Deris. M. 2006. "Transaction Management Model for Mobile Databases". Phd Thesis in Computer Science, Faculty of Computer Science and Information Technology, Univesrity Putra Malaysia, P.P.3.

[4] Abdul-Mehdi. Z. T and Ramlan. M. 2008. "Security Management for the data transmission between base station and mobile host" IETECH journal of communication techniques.

[5] Delf. H. 2007 "Introduction to Cryptography" Principles and Applications. Second edition. ISSN 1619-7100, ISBN-13 978-3-540-49243-6, Berlin, New York.

[6] Denis. T and Johnson. S. 2007. "Cryptography for Developers" Hingham Street, Rockland, MA, US ISBN-10: 1-59749-104-7, ISBN-13: 978-1-59749-104-4 in US and Canada.

[7] Dunham. M.H. and Kumar.V. 1999 "Impact of mobility transaction management" International Workshop on Data Engineering for Wireless and Mobile Access, Seattle, WA, USA, 14-21.

[8] Forouzan. B. 2007. "Data Communications and Networking", Fourth edition, Mc Graw Hill, Singapore, ISBN 007-125442-0.

[9] Garuba. M, 2005 "Impact of External Security Measures on Data Access Implementation with Online Database Management System" ITCC05 Volume 1-Volume 01, Pages: 243 -248.

[10] Gray. J, Helland. P, O'Neil. P and Shasha. D 1996 "The dangers of Replication and Solution" ACM SIGMODE International Conference on Management of Data.

[11] Jakobsson. M, Yung. M and Zhou. J. 2004 " Applied Cryptography and Network Security" Second International Conference, Yellow Mountain, China.

[12] Jorstad. N. D and Smith. L. T. 1997 "Cryptographic Algorithm Metrics" White paper in National information System Security Conference, US.

[13] Krause. M and Tipton. H. 1993. "Handbook of Information Security Management" ISBN: 0849399475. US.

[14] Lubinski. A. 1998. "Security Issues in Mobile Database Access" Mobile Visualization Project, Germany Research Association.

[15] Mao. W. 2004. "Modern Cryptography: Theory and Practice" New Jersey, USA ISBN: 0-13-066943-1.

[16] Maurer. U. 1994. "Towards the equivalence of breaking the Diffie-Hellman protocol and computing discrete logarithms" Advances in Cryptology - Crypto '94, Springer-Verlag, 271-281.

[17] National Security Agency. 1998 "SKIPJACK and KEA Algorithm Specification" US.

[18] 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).

[19] Rivest. R. L. 1994 "The RC5 Encryption Algorithm" US.

[20] Savola. R. 2006 "Node-Level Information Security monitoring for Mobile Ad Hoc Networks" VTT Technical Research Centre of Finland, Oulu, Finland.

[21] Schneier. B. 1996 "Applied Cryptography" Second Edition: Protocols, Algorithms and Source Code in C (cloth) ISBN: 0471128457 US.

[22] Sklavos. N and Zhang. X. 2007. "Wireless Security and Cryptogrpahy: Specification and Implementations" 6000 Broken Sound parkway NW Suite 300, Boca Raton, FL, US ISBN -10: 0-8493-8771-X(Hardcover), ISBN-13: 978-0-8493-8771-5 (Hardcover).

[23] Stamp. M. 2006. "Information Security Principles and Practice" ISBN-10 0-471-73848-4 (cloth) ISBN-13 978-0-471-73848-0.

[24] Venkaiah. V. Ch, Srinathan. K and Bruhadeshwar. B 2004 "Variations to S-box and MixColumn Transformations of AES" Hyderabad, India.

[25] Wilson. S. B and Menezes. A. 2005 "Authenticated Diffie Hellman Key Agreement Protocols" University of Waterloo, Waterloo, Ontario, Canada.