IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 14, Issue 12, December 2024, ||Series -1|| PP 18-22

Designing and Prototyping Encryption Algorithm Using Double Encryption Key on M-Commerce Background

[1.]Harakh J Trivedi, [2.]Prof (Dr.) Jaydipkumar H Trivedi,
[3.] Visvam P Trivedi, [4.] Prof. Sanjaybhai G Patel
harakhjtrivedi@gmail.com, mrjlecturer@yahoo.com,
vtpt2072@gmai.com, patel.sanjay.g@gmail.com
Received 01 December 2024; Accepted 11 December 2024

Abstract: Encryption algorithms are functioning on different stages of the M-Commerce background. Using double encryption key, the present algorithm, and the system have achieved level of security. Encryption and decryption are performing simultaneously on M-Commerce background. The present study is focusing on prototyping existing encryption algorithms. There is an advance implementation of encryption algorithm using double encryption key. The study is suggesting the performance of algorithm and its achievement of level of security. Broadcasting and Its Receding Agent Based M-Commerce Model and Its transaction are the key area for the performance of the Encryption algorithms. The study is also introducing about architecture and process of The Broadcasting and Its Receiving Agents Based M-Commerce Model.
Key Words: M-Commerce, Encryption Algorithms.

I. INTRODUCTION

Encryption and decryption are playing important role for computer systems. A level of security is achieved using encrypt of the text and decrypt of the text. Not only desktop but also network base system need its level of security. Using encryption algorithm data is to be viewed in encryption form in the system. A stakeholder can hide his data using encryption using encryption algorithm. Here, double encryption key is important aspect for establishment of the security on M-Commerce back ground. Encryption and Decryption perform using double encryption key. Broadcasting and Its Receiving Agents Based M-Commerce Model is the base model.[6]There are m-commerce transection using broadcasting and it's receiving agents.[7]

II. LITERATURE REVIEW

Designing and prototyping encryption algorithms: Working as Secure M-Commerce Transaction of Broadcasting and Its Receiving Agent Based M-Commerce Model by Trivedi J.H, Darji J.H, Patel H.D, Trivedi P.H is giving instruction of implementation of algorithm and its related background of M-Commerce.A new approach towards encryption schemes: Byte Rotation Encryption Algorithm, World Congress on Engineering and Computer Science 2012 Vol II, San Francesco, USA. ISSN 2078-0958.C.J.Date, A Kannan,Swamynathan, An Introduction to Database System, Eight Edition, Chapter 17 P 433, There is Encryption and Introduction.J.H.Trivedi,Dr J G Padya, P H Trivedi, Dr A N Jani, Broadcasting and Its receiving Agent Based M-Commerce Business Model, Presented as poster presentation in cross disciplinary international seminar held at H.N.G.University, Patan.India. And Published in the University Journal.

III. OBJECTIVES

1. Designing and prototyping encryption algorithms.
2. Study the architecture, transactions and process of Broadcasting and Its Receiving Agents Based M-Commerce Model.
3. Level of security is achieved using Encryption and Decryption.

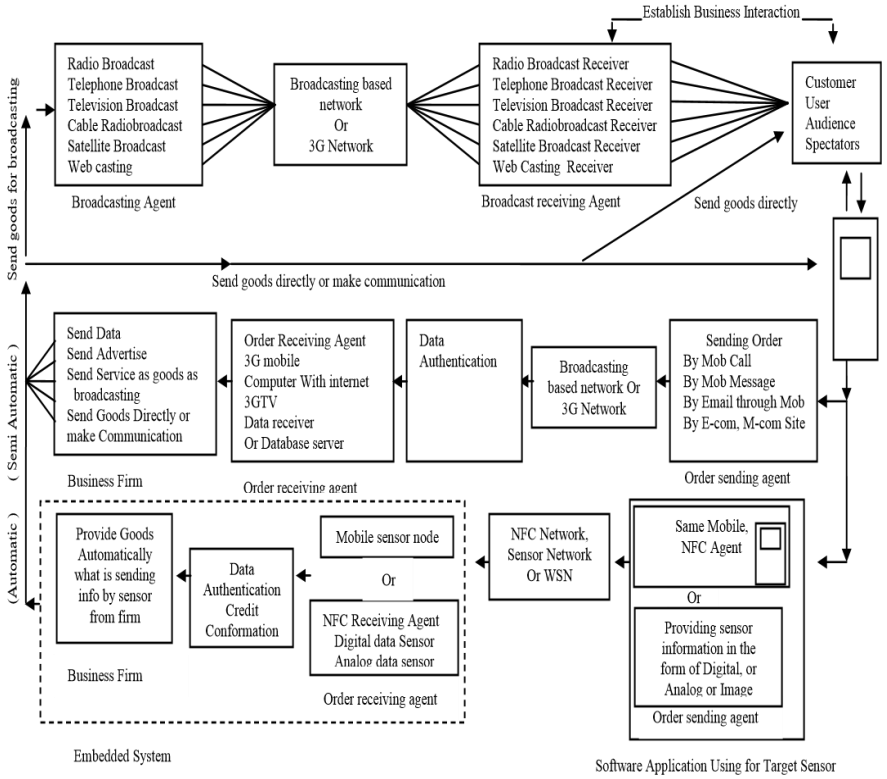
IV. RESEARCH METHODOLOGY

Experimental approach is using as a research methodology for the research work.

V.HYPOTHESIS

- Using double encryption key in encryption algorithm.
- Encrypted data is regarded as secure data.

VI. ARCHITECTURE



(Figure 1: Architecture, Broadcasting and Its receiving Agent Based M-Commerce Business Model)

The work is based on Broadcasting and It's Receiving Agent Based M-Commerce Model [7]. The study is showing the place where encryption algorithm play its crucial role, M-commerce transaction is observed and the work also indicated architecture [7]

VII. EXISTING ENCRIPTION ALGORITHMS

Existing Algorithm 1:

To achieve the security level, the research work is suggesting encryption and decryption. The study is focusing the functioning back ground is M-Commerce. Broadcasting and Its Receiving Agents Based M-Commerce Model is the fundamental model for working and executing transitions.[5]

At the initial stage data will be in unencrypted form and it is regarded as plaintext. The unencrypted data is encrypted using encryption algorithm. There is a double encryption key on a plain text and convert the result as encrypted form is regarded as cipher text.

There is a detail of the encryption and it's key. The plain text and the encryption algorithm are public. The encryption keys are not made for public.[5]

AS KINGFISHAR CATCH FIRE (Using as Plain Text)

ELIOT (Using as Encryption Key)

Step 1. AS+KI NGFIS HERS+ CATCH FIRE

(Indicating the plain text into a state of length equal to that of encryption key) **Step 2.** "+" (Space is indicating)

0119001109 1407060919 0805181900 0301200308 0006091805

(The plain text is converting by integer in the range 00-26 using blank = 00, A=01, B=02, J=10)

Step 3. 0512091520 (use the step second for converting encryption key into integer form.)

Step 4

0119001109 1407060919 0805181900 0301200308 0006091805

<u>05120915200512091520051209152005120915200512091520</u>

(Each block converting character by the sum modulo 27 of its integer encoding and the integer encoding of character of the encryption key)

Step 5 FDIZB SSOXL MQ+GT HMBRA ERRFY

(Converting all related integers encoding the result of step 4 by its character equivalent)

Existing Algorithm 2:
M-Commerce based encryption algorithm is using e-mail address as encryption key.[1] The study indicates that the user name is unique for the system on internet while it is using e-mail address as encryption key. User is performing M-commerce based transaction. The M-commerce based system needs authorization of the customer and after conformation the system allows them to perform M-commerce transactions. Here the study is indicating user name of e-mail address as encryption key.

Step 1:
TRIVEDI-JAYDIPKUMAR-H
(Taking Plain text as message obtaining)
(Converting the character to its related alphabetical digits like A=01, B=02, C=03, D=04 …..)
(In the plain text space seems as "-")
(Indicates Space as 00)

Step 2:
20180922050409001001 25040916112113011800 08
(Taking the digital block of the string as per the length of user name of e-mail address's digit)

Step 3:
mrjlecturer (Taking from mrjlecturer@yahoo.com)
(Encryption key is forming on the basis of user name of e-mail address and it is taking form e-mail message from business transaction. It is taking user name of e-mail address only without "@" and rest of the address like yahoo mail.com)
131810120503202118051813181012050320211805 (The encryption key is gating from email username)
(Converting the characters to alphabetical Digit like A=01, B=02, C=03, D=04…..)

Step 4:
2018092205040900100125 04091611211301180008
131810120503202118051813181012050320211805
33361934100729212806431727262326162139181 3 (Adding the digital block of the string with Encryption key)

Step 5:
CCCFAICDA00GBIBABH0FDC AGBGBFBCBFAFBACIAHAC
(The result got of the addition from step 4 converted the digital string into alphabetical string like 1=A, 2=B, 3=C, 9=I, and take Zero "0" and so on.)

Encrypted Message:
CCCFAICDA00GBIBABH0FDC AGBGBFBCBFAFBACIAHAC

Step 6:
CCCFAICDA00GBIBABH0FDC AGBGBFBCBFAFBACIAHAC
33361934100729212806 43 1727262 3261621391 813
(Now, Converting the alphabetical string into digital String like C=3, I=9, and take Zero "0" and so on, It means "0" is encrypted as "0" only.)

Step 7:
33361934100729212806 43 17272623261621391813
131810120503202118051813181012050320211805
2018092205040900100125 04091611211301180008
(It is subtracting the digital block of the string with Encryption Key)

Step 8:
2018092205040900100125 040916112113 01180008
TRIVEDI-JAYDIPKUMAR-H
(Resulted alphabetical string on the basis of result got from Step 7, subtraction)

VIII. CHALLENGES AND NEED FOR PROTYPING AND DESINING

- Single Encryption Key is not sufficient for security, so it need double Encryption Key
- Advancement need more competent encryption algorithm which achieve level of security.
- M-Commerce background need variation of algorithm for better transactions.

IX. DESINING ENCRIPTION ALGORITHM

Step 1. GANESHJI-PRABHU(Taking as Plain Text)
Step 2. 07011405190810090016180102082 1
(Changing the character to its related alphabetical digits like A=01, B=02, C=03, D=04 …..)
(In the plain text space seems as "-")
(Indicates Space as 00)

Step 3. SHRIGANESH (Take 1st Encryption Key)
1908180907011405 1908
(Changing the character to its related alphabetical digits like A=01, B=02, C=03, D=04 …..)
Step 4. ABABABABABABABABABAB
(Take 2nd Encryption Key, Take its length equal to the length of first encryption key)
01020102010201020102
(Changing the character to its related alphabetical digits like A=01, B=02, C=03, D=04 …..)
Step 5. 1908180907011405 1908(First Encryption Key)
01020102010201020102(Second encryption Key)

_____
20101911080315072010 (Sum of the two encryption keys)
Step 6.07011405190810090016180102 0821 (Taking plain Text using gap as two zero "00")
20101911080315070020102010191 1 (Use the sum of two encryption keys)

_____
27113316271125160036282112273 2 (Result of the above digit (SUM))
Step 7. 27113316271125160036282112273 2 (Result of the digit that is obtained at step.6 (SUM))
20101911080315070020102010191 1 (Use the sum of two encryption keys)

_____
07011405190810090016180102082 1 (Result of the above digit (SUBTRACTION))
(Changing the digit to its related alphabetical character like 01=A,02=B, 03=C… …..)
(In the plain text space seems as "-")
(Indicates Space as 00)
Result: GANESHJI-PRABHU

XI. ANALYSIS OF THE DATA

No	Algorithm	Background	Used Encryption Key	Understandability	Security Level
1	C.J Date, A Kannan, Swamynathan, An Introduction to Database Systems, Eighth Edition,	Data Base	1 (One)	Easy	Yes
2	M-Commerce based encryption algorithm	M-Commerce	1 (One)	Easy	Yes
3	Encryption Algorithm Using Double Encryption Key	M-Commerce	2 (Two)	Easy	Yes

XII. CONCLUSION

Thus the study has focused on designing and prototyping encryption algorithm. The research work also focused on existing encryption algorithms. There is M-Commerce Background and Its Architecture which is indicating broadcasting and its receiving agent based transactions. There is double encryption key based encryption algorithm, and the system has achieved level of security.

REFERENCES

[1] J.H.Trivedi, J.H.Darji, H.D.Patel, P.H.Trivedi, Designing and Prototyping Encryption Algorithms: Working as secure M-Commerce Transection of Broadcasting and Its receiving Agent Based M-Commerce Model, IOSRJEN e-ISSN:2250-3021, p-ISSN:2278-8719 Vol.3, Issue 8 (Auguest.2013),||V3||PP 25-33

[2] S Diego, T Joaquin, C Mildery, T Jesus, A new domain- based payment model for emerging mobile commerce scenarios, IEEE 2007.

[3] S Bhati, A Bhati, S Sharma, A new approach Towards encryption schemes: Byte-Rotation Encryption Algorithm, World Congress on engineering and computer science 2012 vol II, San Fransisco,USA.ISSN: 2078-0958.

[4] T Aphrodite, P Evaggelia, Business Models and Transactions in mobile electronic commerce: Requirements and Properties, Elsevier, Computer Networks 37(2001)

[5] C.J Date, A Kannan, Swamynathan, An Introduction to Database Systems, Eightth Edition, Chap.17 P.433.

[6] J.H.Trivedi,Dr J G Padya, P H Trivedi, Dr A N Jani, Broadcasting and Its receiving Agent Based MCommerce Business Model, Presented as poster presentation in cross disciplinary international seminar held at H.N.G.University, Patan.India. And gone for Publishing in the University Journal.

[7] Trivedi J. H, Trivedi P. H, Thakkar S. T, MakwanaM.N,Automatic and Semi Automatic Transaction of Broadcasting andIt's Receiving Agent Based M-commerce Business Model,IOSR Journal of Engineering (IOSRJEN)e-ISSN: 2250-3021, p-ISSN: 2278-8719Vol. 3, Issue 2 (Feb. 2013), ||V3|| PP 42-53