International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 05 | May-2018 www.irjet.net p-ISSN: 2395-0072

IMPLEMENTATION OF ETSFS ALGORITHM TO MAKE SECURE TRANSACTION ON E-COMMERCE SITE

Dr. V. S. Gulhane[1], Dr. H. R. Deshmukh[2], Miss. Diksha S. Nitnaware[3], Prof. S.V. Khedkar[4], Prof. O. A. Jaisinghani[5]

Professor, Dept of Information technology, Sipna college of Engineering, Amravati
Head of department, Dept of Computer Science & Engineering, Dr. R.G.I.T. &R, Amravati
Student, Dept of Computer Science and Engineering, Dr. R.G.I.T. &R Amravati
[4,5]Assistant Professor, Dept of Information Technology, Dr. R.G.I.T. &R, Amravat.

Abstract: In this paper, we propose a model of E-transaction based on ETSFS. It will show that how much secure payment and customer order of information will be efficiently handled by ETSFS based on atomicity between transactions. Secure transaction using ETSFS is new ecommerce Security algorithm and plays a more and more important role in our lives. We have proposed file recovery technique by the concept of cloud mirroring. With the help of cloud mirroring technique we provide the high availability, integrity as well as recovery of user data (files). This paper proposes implementation of the ETSFS algorithm in Ecommerce site to make the transaction secure and by using the mirroring technique to recover the data to provide high security to Ecommerce site.

Keywords: Ecommerce security, Transaction security, Encryption, ETSFS algorithm, Mirroring Technique

I. INTRODUCTION:

E-commerce is an online business trade on the Internet. To provide secure trade in the form of E-commerce web service security plays an important role in such business processes. In E-commerce, more and more security issues are increasing day by day on the open Internet like client information leakage, credit card clowning etc. So, it is the cause that people's interest using of E-commerce decreasing day by day. They feel panic when they want to pay on Internet [3]. To develop the Ecommerce, security is the main issue on the Internet. So, to avoid the security issues we should have some secure conditions that should provide the adequate protection to the transaction information for each and every entity in Ecommerce transaction. Customers are cautious to take participate in e-commerce due to security problems like hacking customers' information and many other attacks exist in the open network which is dangerous to the customer information[4]. Electronic commerce or e-commerce provides participants, including consumers and merchants, with a number of benefits, such as convenience and time savings. E-commerce transactions can be categorized into business to business (B2B), business to consumer (B2C), consumer to consumer (C2C), and public/private sectors to government [2]; we focus on B2C transactions in this paper. In B2C transactions, the credit card is the most widely used method of payment for Internet ecommerce transactions. The research reported here builds on the electronic payment security; we study the security of e-commerce protocols and we propose a new efficient protocol to ensure a high security for electronic payment transactions. Enhanced Transposition, Substitution, Folding and Shifting ETSFS algorithm, known as the ETSFS algorithm [1]. The ETSFS algorithm provides a high degree of security, using a number of features. However, it supports all the numbers and alphabetic characters. This paper provides a secure and efficient encryption method that encrypts only sensitive data without using special hardware.

II. LITERATURE REVIEW:

Due to the important role that encryption techniques play in securing database systems, numerous algorithms have emerged with different techniques and performance. Data plays a very important role and is stored in database system which should be organized such that it safeguards the data. Most of the organizations sensitive data is housed in database and a backup is maintained for future use. Unauthorized access is one of the serious threats and should be addressed to enhance database security. Encryption, which plays a important role in safeguarding the information, is defined as the process of transforming information into no readable form except by those holding a key to decrypt.[1] The database security mechanisms, algorithms like TSFS, DES, and AES came into focus, which are different from other and had a few advantages and disadvantages based on their optimization ways.[7] The DES algorithm is one of the well- known symmetric key algorithms considered as insecure for many applications and presents AES as a replacement. Manivannan and Sujarani [1] proposed efficient database encryption techniques using the TSFS algorithm, which is a

symmetric-key algorithm. Its main features include using transposition and substitution ciphers techniques that are important in modern symmetric algorithms as they have diffusion and confusion. Also, it encrypts only the sensitive data, so, it limits the added time for encryption and decryption operations. The algorithm utilizes three keys and expands them into twelve sub-keys using the key expansion technique to provide effective security for the database and e-commerce transaction. In order to improve the security, this algorithm uses twelve rounds and two different keys in each round. However, TSFS algorithm applies only to alphanumeric characters; it does not accept special characters or symbols.

III. ETSFS ALGORITHM

The main objective of this paper is to secure the transaction using ETSFS algorithm and accordingly to provide a high security to the databases whilst limiting the added time cost for encryption and decryption by encrypting sensitive data only. The ETSFS algorithm can encrypt the data that consists of alphabetic characters from A to Z, all numbers and the symbols. It included almost all the special characters. The ETSFS algorithm is a symmetric encryption algorithm, meaning each transformation or process must be invertible and have inverse operation that can cancel its effect. The key also must be used in inverse order. ETSFS algorithm uses four techniques of transformations, which are transposition, substitution, folding and shifting. The following sections describe the four techniques.

A. Transposition

Transposition transformation changes the location of the data matrix elements by using diagonal transposition that reads the data matrix in the route of zigzag diagonal starting from the upper left corner after getting the data and pads it with *s if it is less than 16 digits [2]. Fig. 1 shows the transposition process.

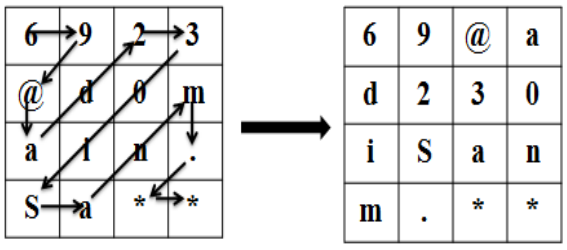

Fig. 1 Transposition example

B. Substitution

The second algorithm is substitution transformation. It replaces one data matrix element with another by applying certain function [2]. If the element represents an alphabetic character, it then will be replaced with another character. If the element represents a number, it will be replaced with a number, Confusion happens if the data is composed of alphabetic and numeric digits, and the modulus size (M) will be 26 for any digit, as illustrated in the next example. If one element in the data was 4, k1=5, K2=5, M = 26, then the result of substitution process is 14 as the paper presents. This result causes two problems. The first problem is that the length of the data will be changed and increased; for example, when the plane text size is 16 digits, the cipher text size will be 17 digits if one element only changes and that contradict the TSFS algorithm's feature. The second problem, since the inverse operation decrypts the data digit by digit also, is that then it will deal with each element in the cipher text individually (1 then 4). As a result, the decrypted data will be different from the data that have been encrypted. Therefore, the ETSFS algorithm gives M the following values: 26 if p is aliphatic, 10 if p is numerical and 7 if p is symbolic.

The decryption function [1] D is:

$$D(E(x)) = (((E(x) - K2) \bmod M) - k1) \bmod M \quad (2)$$

Since most of the programming languages such as Java and C++ deal with the modulus as the remainder of an integer division, some of the results may have minus sign, and this will create a problem because there is no data that have minus sign representation. So, one more step has been added to the ETSFS algorithm implementation to check if the result includes the minus sign, and then apply:

$$D(E(x)) = M - |D(E(x))| \quad (3)$$

The following Fig. 2 shows the result of substitution. From the same example in fig. 2, if we implemented the decryption operation (2) on the first element, the result would be -4, so the ETSFS algorithm applies function (3) to get the correct result, which is 6.

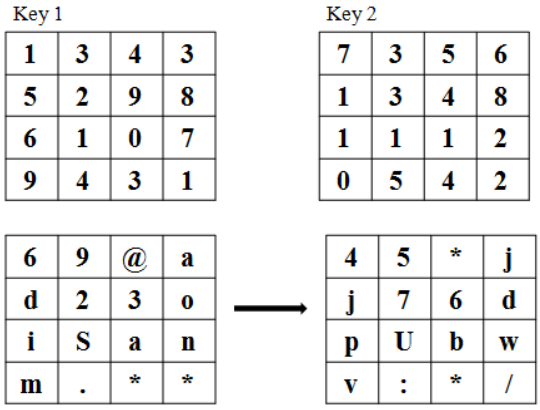

Fig. 2 Substitution example

C. Folding:

The third algorithm is folding transformation. It shuffles one of the data matrix elements with another in the same entered data, like a paper fold. The data matrix is folded horizontally, vertically and diagonally [2]. The horizontal folding is done by exchanging the first row with the last row. The vertical one is done by exchanging the first column with the last column. The diagonal fold is done by exchanging the inner cells, the upper-left cell with the down-right cell and the upper-right cell with the down-left cell.

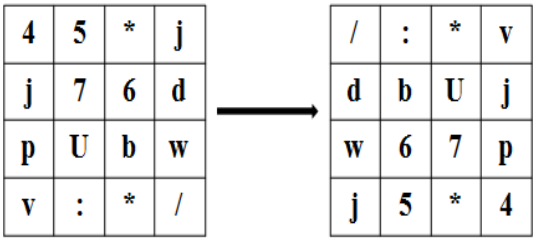

Fig.3 Folding example

D. Shifting :

The shitting transformation is the last phase of the methodology where the given array elements of digits exchange with their letter elements respective to the array elements. Alphabetical characters are referenced with an upper and lowercase array element of numbers ranging 0-25 with each number representing an alphabet respectively .Another array element is considered numeric characters ranging from 0-6 (7 characters) is also reflected .Each element in the data matrix is given reference with its location in the array in the array of elements (taken) and its appropriate positioned element is considered from its array elements. For example, if an element in the plain text is 4 and its position within the array is 15, then the shifting process in [2] returns 15, which is causing the same two problems that were described in substitution transformation. So, the ETSFS algorithm separates each type from other. The ETSFS algorithm uses four 16-arrays, one for numeric, one for symbols, the last two 16-arrays are used for alphabetic, where one for capital letters and the other for small letters. We used that to enhance TSFS algorithm and make it is sensitive for the type of letter.

I/P	Array Elements	O/P
/	0 1 2 3 4 5 6	/
:	1 2 3 4 5 6 0	/
*	2 3 4 5 6 0 1	@
v	3 4 5 6 7 8 9 1 0 11 12 13 14 15…23 24 25 0 1 2	s
d	4 5 6 7 8 9 10 11 12 13 14 15 16…24 25 0 1 2 3	z
b	5 6 7 8 9 10 11 12 13 14 15 16…24 25 0 1 2 3 4	w
u	6 7 8 9 10 11 12 13 14 15 16…24 25 0 1 2 3 4 5	O
.		.
.		.
4	1 5 4 6 0 7 2 8 3 9	2

Fig.4 Shifting example

IV.PROPOSED MODEL:

We proposed a model for Ecommerce Transaction. Now, our model is based on the ETSFS algorithm. Till now, ETSFS is used for to database security purpose but we used it in E-commerce first time. Suppose, we have two orders, one is goods order and other is payment order. We encrypt the goods order and payment order by ETSFS algorithm and send the encrypted customer and payment order information parallel to Internet open network. These encrypted messages of payment and the customer order information is merged with each other and then encrypted by ETSFS. In this system there will be two servers, bank server (admin) and merchant server (product admin). Product admin will add the products and product related information in its database. Admin i.e. bank server will add users and merchant servers. User specific data includes user name, user id, transaction password and user password. While merchant server specific data includes server id, password and URL in the Admin's database. Client will select the product and log in to respective site. Details about the purchases are sent by checkout to the payment gateway for processing. The payment gateway forwards transaction information to seller's bank. The seller's bank forwards transaction information to the bank that issued the buyers credit card to authorize the transaction. Then verification request is sent to merchant server. Merchant server will verify the user name, user id and along with that it will add server id, server key and send it to the bank server for the verification. Bank server

will verify the server id, server key of merchant server. If it is ok then bank server will response to client.

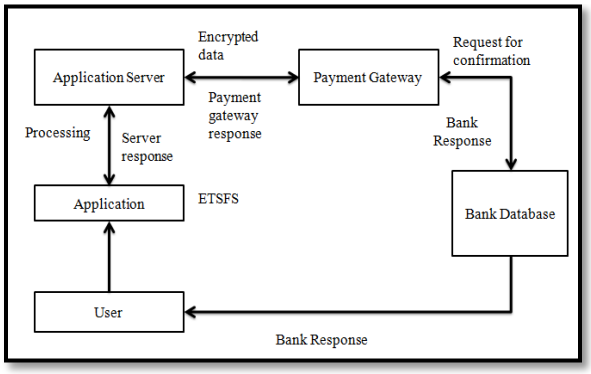

Fig.5 Block Diagram of proposed system

V. IMPLEMENTATION:

5.1 Implementation of ETSFS algorithm:

A php & Java-based project has been built to test the ETSFS algorithm correctness and performance. The implementation uses three-tier architecture, as represented in Fig. 5. The three-tier separate the functions into interface, processing and data management functions. The multi-tier architecture allows developers to create flexible and reusable applications. In addition, this architecture provides "encryption as a service" to facilitate the interaction between the interface and the encryption/decryption model, and makes the process of encryption or decryption transparent to application [2]. In this paper, the interface-tire is used to enter and retrieve data from the database. The processing-tier is used to garner the data or query from the interface-tier and then to complete the encryption or decryption processes to apply the query over the secure database. It stores the keys in a separate file instead of storing them in the database to increase the security. Finally, a data management-tire stores the data.

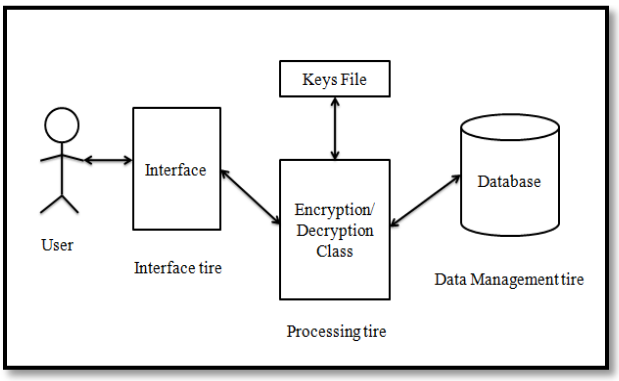

Fig.6 Implementation Architecture

5.2 Mirroring architecture:

Two unique but related methods for maintaining nearly real-time copies of databases in additional locations, referred to as mirroring and replication. Both mirroring and replication use the same terminology for the roles of databases: the original, updateable database is called the master. From one master database, one or more slave copies can be created and dynamically maintained. The terminology comes from the idea that the,

1. Master database controls the generation of data, and

2. The slaves respond only when changes have been made on the master.

Two copies of a single database reside on different computers called server instances, usually in physical locations separated by some distance. The principal (or primary) server instance provides the database to clients. The mirror (or secondary) server instance acts as a standby that can take over in case of a problem with the principal server instance. If 100-percent accuracy is required, database mirroring requires that the mirror server instance always stay current; in other words, the system must immediately copy every change in the principal's content to the mirror and vice-versa. In this mode, known as synchronous operation, the mirror is called a hot standby. While database mirroring can also work when the content is not fully synchronized, some data loss may occur if one of the server instances fails or becomes inaccessible. In this mode, called asynchronous operation, the mirror is called a warm standby.

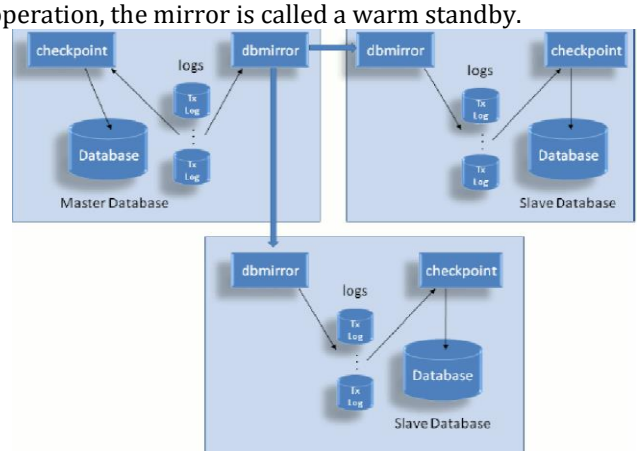

Fig. 6 Mirroring Architecture

VI. RESULT ANALYSIS:

The ETSFS algorithm provide the encryption to the sensitive information in the Ecommerce transactional data such as Credit card number, CVV number, Password, bank etc. It will show that how much secure payment and customer order of information will be efficiently handled by ETSFS based on atomicity between transactions. . ETSFS provides a high degree of privacy for customers by encrypting payment information so that only the bank can see it. ETSFS has the potential to reduce the chance of fraud by providing rigorous authentication measures in addition to encrypting transactions

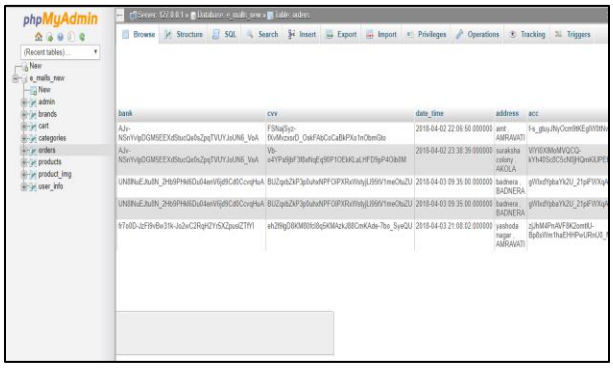

Fig.7 This figure shows that we have an orders table as described earlier this is the main table where you can easily observe that the intensity of the encryption.

The following figure shows the result of Mirroring technique which is the recovery technique of project. The purpose of recovery technique is to help user to retrieve information from any mirror server when server lost his data and unable to provide data to the user.

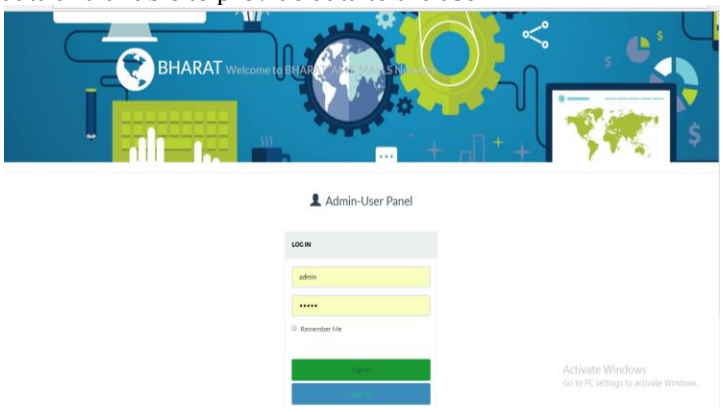

Fig.8 This figure of project depicts the Cloud mirroring Admin-User panel.

Fig.9 This figure of project depicts that both the Main and Mirror server are running.

Fig.10 This figure of project depicts that if the Main Sever fails the data is transferred to the Mirror server.

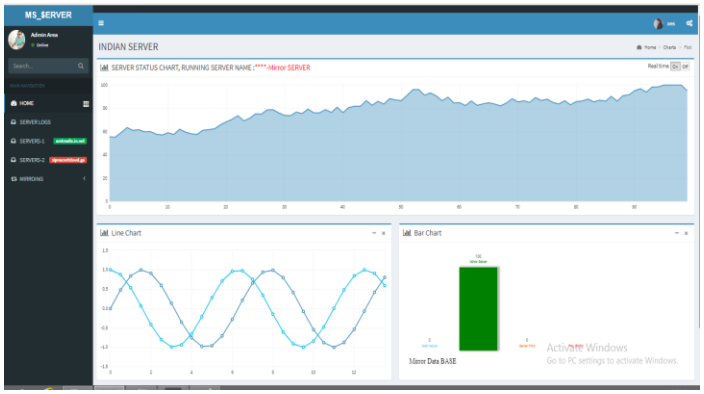

Fig. 11 This figure of project depicts that if the Mirror Sever fails the data is transferred to the Main server.

CONCLUSION:

Data-storing and exchanging between computers and in E-commerce transaction is growing fast across the world. The security of this data has become an important issue for the world. Transaction security is vital in e-commerce. Fraud exists in current commerce systems: cash can be counterfeited, checks altered, credit card numbers stolen.

This paper proposes the enhancement of the ETSFS algorithm to support the encryption of special characters, providing more than one modulo factor to differentiate between data types and prevent increasing the data size, and provide four 16-arrays.ETSFS algorithm successfully encrypted important symbols, as well as alphanumeric data.. Using well-established encryption algorithms as benchmarks, such as DES and AES, the proposed ETSFS algorithm was shown to have consumed the smallest space and encryption time compared to the other algorithms. With the help of cloud mirroring technique we provide the high availability, integrity as well as recovery of user data (files). So for this issue we need file recovery mechanism for recovering the corrupted file. We have proposed file recovery technique by the concept of cloud mirroring.

REFERENCES:

1. D. Manivannan, R.Sujarani, Light weight and secure database encryption using TSFS algorithm, Proceedings of the International Conference on Computing Communication and Networking Technologies, 2010, pp.1-7

2. Hanan A, Abeer, Heba, "Lightweight Symmetric Encryption Algorithm for Secure Database." IJACSA International Journal of Advanced Computer Science and Applications, Saudi Arabia

3. Pratyusha Uduthalapally, Bing Zhou, Improvement of ETSFS algorithm for secure database,4th *International symposium on digital forensic and security(ISDFS'16),25-27 April 2016,Little Rock, AR ©2016 IEEE*

4. Amandeep kaur, Mrs. Shailja Kumari "Secure Database Encryption in Web Applications" International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 7, July 2014 IJARCCE, vol. 3 issue 7, July 2014

5. L. Liu, J. Gai, A new lightweight database encryption scheme transparent to applications, Proceedings of the 6th IEEE International Conference on Industrial Informatics, 2008, pp.135-140.

6. Pooja Saini1, Kanchan Narula2, A Review: Enhancing Data Security in Cloud Computing with WEBOS using TSFS Algorithm, International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064 Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

7. Khandare Nikhil B., Transaction Security for Internet E-commerce Application, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 2, February 2015

8. Miss Nikita A. Rathi Prof S. R. Gupta, Optimizing security in E-Commerce Transaction: An Overview , International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 3 Issue 12, December 2014

9. Mr.Amit N. Chaudhari, Prof. Priya V. ShirbhateThe study of E-Commerce Security Issues and Solutions, International Journal of Research In Science & Engineering Volume: 1 Special Issue: 1

10. Pradnya B.Rane and Dr. B.B.Mehsram, Application level and Database Security for Ecommerce Application, Proceedings of International Journal of Computer Application(0975-8887)Volume 41-no.18 March 2012

11. Houssam E Ismaili, Hanane Houmani" A Secure Electronic Transaction payment protocol Design and Implementation, IJCSNS International Journal of Computer Science and Network Security, VOL.15 No.5, May 2015

12. Khalid Haseeb, Dr. Muhammad Arshad, Shoukat Ali, Dr. Shazia Yasin, "Secure E-Commerce Protocol, International Journal of Computer Science and Security, Volume (5): Issue (1): 2011

13. Ankur Chaudhary , Khaleel Ahmad, M.A.Rizvi, E-Commerce Security through Asymmetric Key Algorithm, 2014 Fourth International Conference on Communication Systems and Network Technologies

14. Shilpi U. Vishwakarma and Praveen D. Soni, Cloud Mirroring: A Technique of Data Recovery, International Journal of Current Engineering and Technology, Vol.5, No.2 (April 2015)+