ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 4, April 2017

Implementing ETSFS Algorithm for Database Security : A Review

Nandkishor B. Jawanjal [1], Pritish A. Tijare [2] , Swapnil N. Sawalkar [3]

P.G.(Computer Engineerin) Student, Department of CSE, Sipna COET, Amravati, Maharashtra , India[1]

Associate Professor, Department of Information Technology, Sipna COET, Amravati, Maharashtra, India[2]

Assistant Professor, Department of Information Technology, Sipna COET, Amravati, Maharashtra, India[3]

ABSTRACT : In the present time, one of the major issue is the database security. Most of the Organization store their information in enormous databases that empowers uncomplicated recovery, controls, and furthermore helps in a proficient method for sharing. Database security has now turned into a more dynamic issue as information is the best advantage for any association. Because of the quick increment in the database issue as data is the greatest asset to any organization. It is defenceless against numerous dangers like unapproved get to and so on. To beat these issues, various security strategies have developed to ensure the information in databases. Database encryption - a security system includes different encryption algorithms for database security. for example, Data Encryption Standard (DES), Triple DES and Enhanced-Transposition-Substitution-Folding-Shifting (ETSFS). Each of them has its particular benefits and faults. Not at all like ETSFS, has imperative on information size and number of exceptional characters, the proposed technique change concentrates on the encryption of expansive information considering a wide range of unique characters and an arbitrary generator is utilized for producing keys in substitution stage. The proposed strategy of the review paper concentrated on the future work of the ETSFS algorithm for sensitive database security and effectively actualized for securing database with the comparison of the insert select queries of the Three encryption Algorithm (AES, DES, ETSFS).

.

KEYWORDS: Transposition, Substitution ,Shifting ,Folding, Encryption, Decryption.

I. INTRODUCTION

Important any Information means your organization data ,these data an accessible asset to an organization, these data store in database system .Database is used to store the data for quick and secure processing of requests. Data is very important to some boundary and need high level of protection. It is a critical system as almost all the organizations are highly dependent on the data. Databases are designed to be shared among a number of users, where security is of prime concern and if it is compromised then they are vulnerable to malicious attacks that results in great loss. Hence, database system is maintained with many security mechanisms that include prevention of unauthorized access to data from insider or outsider of an organization. Therefore, an effective encryption algorithm should be necessarily applied to secure database.

Database encryption would be one of the possible solutions where be one of the access to sensitive information is dependent on the key available, which promises a minimal damage and high performance when it is effective[1].

The most successful encryption algorithms such as, DES and Advanced Encryption Standard (AES), secure the data by converting it into unreadable form which cannot be understood to the common people. An innovative encryption algorithm, known as ETSFS is put forward with the inclusion of number of features which provides a great level of security but still needed further enhancement as it supports only few special characters and the data size constraint leading to undesirable errors during the process.[2]

The ETSFS algorithm provide by avoiding the constraint on the data size and special characters by proposing the usage of all special characters on the data size. This improvement allows handling all special characters and

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 4, April 2017

different sizes of input data for processing performed dynamically depending on the input data given by the user; and based on the input size, keys are generated that shows a variation from existing DES algorithm. It showed a successful implementation by accepting almost all special characters proved to show better performance than the existing DES algorithm.

II. LITERATURE REVIEW & RELATED WORK

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.

Based on 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. The DES algorithm is one of the well-known symmetric key algorithms considered as insecure for many applications and presents AES as a replacement. D. Manivannan, R. Sttjarani [3] proposed well-organized encryption technique using the symmetric - key. popularly known as TSFS algorithm, which includes transpositions and substitutions as features in the techniques that limits encryption and decryption operation times. Later an enhanced TSFS is proposed which is an extended work on TSFS which can encrypt the data that contains alphanumeric and few special characters ensuring high level of security to encrypted data but imposes few constraints on the data size and the special characters used [3].

III. ANALYSIS OF PROBLEM

Security of databases has become increasingly very important in all application areas. Database security has imperial importance in industrial, civilian and government domains. Organizations are storing huge amount of data in database. Challenges for security in database are increased due to the excellence popularity of e-business. In recent years, insider attacks gathered more attention than periodic outbreaks of malware.

Database systems are usually deployed deep inside the company network and thus insiders has the easiest opportunity to attack and compromise them, and then steal the data. So data must be protected from inside attackers also. Many conventional database security systems are proposed for providing security for database, but still the sensitive for data mining and other types of analysis. Some of this data is considered sensitive and has to be protected from disclosure data in database are vulnerable to attack because the data are stored in the form of plaintext only. The main objective is to enhance the TSFS algorithm which will support special characters to provide a high security to the databases at low time cost for encryption and decryption by encrypting sensitive data only from substitution [2]

IV. PROPOSED WORK

The proposed algorithm involves the collection of new key values to the existing ETSFS algorithm which have four phases - Transposition. Substitution. Folding, and Shifting. The explanation of ETSFS algorithm and its augmentation is as given below:

The ETSFS algorithm includes the following alphanumeric characters and a few of special symbols (*, -, /, :,@ and _) only used to encrypt the data that is taken as input. But in the proposed methodology it included almost all the special characters. It is a symmetric encryption algorithm which can be inversed that cancels the encryption.

The constrained restricted on the number of characters is successfully imposed by accepting different data sizes dynamically depending on the user input length and if the length of data is less than the near square matrix size then the characters are replaced by *'s. Let say, the input string is 24 in length, then the nearby square matrix is 4x4 and the one character that is left is replaced by *'s. The four techniques of ETSF S are described as;[1]

A) Transposition :

For a given input data matrix, the diagonal transposition is carried out starting from top leftmost corner till the end of the matrix by moving laterally in one step followed by diagonal transition continually.

For example. consider a text **"sipna@gmail.com"** to be encrypted.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 4, April 2017

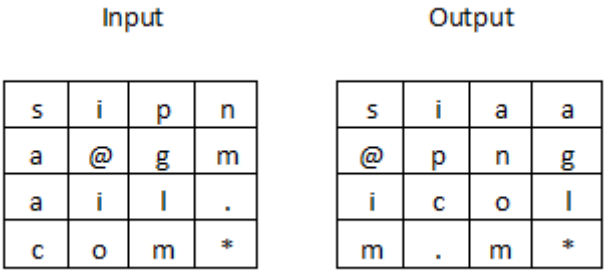

Fig. No: 1. Transposition Phase

As shown in the example figure, the output data is obtained by retaining the first element in the matrix. The transposition in the given input is performed such that zigzag pattern (siaa@ ....*) is followed by starting at the initial index of the matrix which is in the data matrix and continued by following a pattern till the end of matrix. The output data matrix will be the insertion of elements followed as it is in zigzag pattern. This is given as input to the substitution phase.[1]

B) Substitution:

The transposition is followed by the substitution method where each character is substituted by its encoded character. The encoding involves two keys Kl and K2 and the modulus size M. The Kl and K2 key values are generated using a random generator and the modulus size is dependent on the type of character. If the character is an alphabet letter then M :26. if the character is a digit then M=l0 or if the character is one of the special characters mentioned above. then M is considered to be 30 (in the enhanced ETSFS). The encryption of the character is given by:

E(x)=(((K1+p)mod M +K2)mod M ….(1)

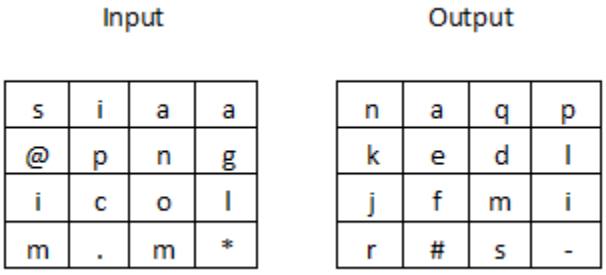

Fig. No: 2. Substitutions Phase

The encryption is performed on each element of the data matrix by using the function given in (1).

Here the keys Kl and K2 are used from [2].The elements are replaced by its corresponding type of characters respectively. For example, consider the first element “a” from the input then the E(x) is applied by taking key values from [2] and p is given as 0 as it is the first alphabet. The range of alphabets is addressed from 0-25,numbers (0-9) and special symbols (0-7).

A reverse operation can also be performed to decrypt the encoded data using the same keys and the decryption of encrypted data is:

D(E(x)) = (((E(x) — K2) mod M) — Kl) mod M ....(2)

The above figure shows the example of encryption of data matrix with the given keys. And their decryption is shown as by applying D(E(x)) shown in (2). The output from E(x) is taken as input and processed by using the function in (2) which produces the input of substitution phase which enables that the encryption and decryption is accurate.[1]

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 4, April 2017

C) Folding:

The third technique is folding in which the first row is exchanged with last row along with the exchange of first column with last column. And the center elements are exchanged diagonally. The below example illustrates the technique of transformation as shown in the below figure:

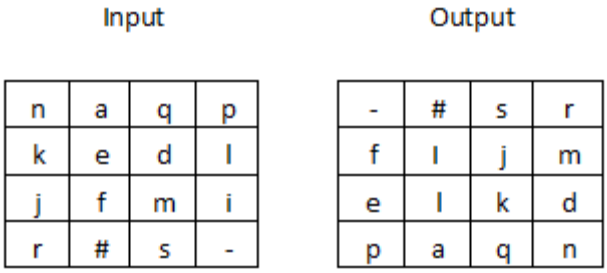

Fig. No: 3. Folding Phase

In this example, it is illustrated that folding is applied on data matrix where the first row is exchanged with last row and simultaneously first column with the last column and the inner elements are diagonally exchanged Where upper left inner element is exchanged with lower right inner element and vice versa. The obtained output is passed to shifting.[1]

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 for searching an alphabet “h” which is in position 8 of data matrix then it should verify its position from array elements of alphabetical characters and should start counting from 8^{th} array element considering it as “a” in it and continue searching till the “h” position is witnessed from array elements. From the array it is at 15^{th} position but the alphabet presents at 15 is “p”. So "h" should be replaced with "p". similarly for the other categories.[1]

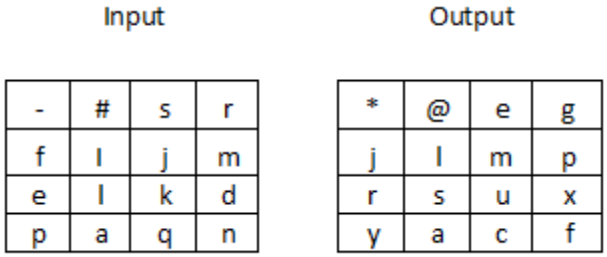

Fig. No: 4. Shifting Phase

V. CONCLUSION

Data storing and exchanging between computers is growing quick across the world. The compromise on security is leading to several database attacks. Many organizations store the sensitive data in database which is easy and quick way to retrieve information. An effective measure is to encrypt the data before storing into database where risks can be minimized through security leaks and the sensitive data is protected. The best way to this approach of securing sensitive data is by using encryption techniques and ensuring database security from attackers.

In this review paper, Enhanced TSFS algorithm an existing methodology is explained in which security is ensured in databases by simultaneously increasing the performance of encryption and decryption process. This review

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 4, April 2017

paper proposes an enhancement to ETSFS, in which the special characters are increased from limited 7 symbols and the data size is much more than the constraint of using only l6 or less digits which is improved to different sizes of data performed dynamically by user input size.

REFERENCES

[1] Prathyusha Uduthalapally,Bing Zhou "Improvement of ETSFS Algorithm for secure Database" 4th international Symposium on Digital Forensics and Secirity (ISDFFS-16)25-27 April 2016 Little Rock .,AR
[2] Hanan A, Abeer, Heba, "Lightweight Symmetric Encryption Algorithm for Secure Database." IJACSA International Journal of Advanced Computer Science and Applications, Saudi Arabia
[3] D. Manivannan, R. Sttjarani, Light weight and secure database encryption using TSFS algorithm. Proceedings of the International Conference on Computing Communication and Networking Technologies, 2010, pp. l-7.
[4] L. Liu. J.Gai,A new lightweight database encryption scheme transparent to application, proceeding of the 6th IEEE International Conference on Industrial Informatics,2008,pp 135-140.
[5] M Susithra;M.Lawanya Shri;;K.S.Umadevi, "An Implementation of Database Image Encryption Using TSFS Techniques",vol 3,Issuse7 July 2013 ISSN:2277 128X,ijarcsse.
[6] H. Alanazi, B. Zaidan, A. Zaidan, H. Jalab, M. Shabbir, Y. Al-Nabhani. New comparative study between , 3DES and AES within nine factors, Journal of Computing 2 (2010) 152-157.
[7] A. Sterbenz, P. Lipp, Performance of the AES candidate algorithms in java, Proceedings of the AES Candidate Conference, 2000, pp.161-165.
[8] T. Subashri, R. Arunachalam, B. Kumar, V. Vaidehi, Pipelining architecture of AES encryption and key generation with search based memory, The International journal of VLSI design & communication systems (VLSICS) 1 (2010) 1-13.
[9] Wu Xing-hui ; Ming Xiu-jun, "Research of the Database Encryption Technique Based on Hybrid Cryptography", Computational Intelligence and Design (ISCID), 2010 International Symposium, Publication Year: 2010 , Page(s):68 – 71
[10] Jiang Yu-yan ; Pi Xiao-yan ; Xing Guo-Zheng , "Database Encryption and Confirmation Mechanism Research", Multimedia Technology (ICMT), 2010 International Conference, Publication Year: 2010 , Page(s): 1 – 4.
[11] Pooja, Kanchan Narula"Enhancing Data Security in Cloud Computing with WebOS Using TSFS Algorithm"ISSN : 2319-7064.
[12]Vocal,"http://www.vocal.com/cryptography/dsadigital-signature-algorithm/," Dated: l3- dec-2012 atl3:l8.