Sabareesan M, Gobinathan N / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 3, Issue 1, January -February 2013, pp.1748-1752

Network Database Security Issues and Defense

Sabareesan M[1], Gobinathan N[2]

Assistant Professor, Department of Computer Science and Engineering, VRS College of Engineering & Technology, Arasur, Tamilnadu, India

Abstract:-

Database security is the mechanisms that secure the database against deliberate or accidental threats, unauthorized users, hackers and ip snoopers. In this paper we proposed two mixed techniques to secure the database ie one is authentication followed by cryptography of database. In existing system the algorithm is less secure, less complex and much superior to implement in any system. The encryption algorithm is built on genetic algorithm, it is used to encrypt the database and validate the user's login id and password, it must verify the user and allow the user to access the database. The decryption also has a login and password based on decryption algorithm and genetic algorithm. The database used is SQL Server 2003. This paper researches and analyzes the issues of security and defense .

Keywords:- Network database, cryptography, genetic algorithm, encryption and decryption

I. INTRODUCTION

The database security is the mechanism used to secure the database from unauthorized access, hackers, ip snoopers and also prevent accidental damages. The major areas of losses are theft and fraudulation, loss of confidentiality, loss of privacy, loss of security, loss of integrity and availability. The database security mainly focus on both database management and security. The data protection of network database is the protection of data's security, integrity and concurrency of data.

The security risks in database are unauthorized or unintentional activity or abuse by authorized database users, database administrators, or network managers, or by unauthorized accusers or hackers[1]. The malware infections causing difficulties such as unauthorized access, leakage or revelation of personal or proprietary data, deleting records or damage to the data, interruption or rejection of authorized access to the database, attacks on other systems and the unexpected failure of database services[1].

To overcome this problem we proposed two techniques to secure the databases, one is authentication followed by genetic algorithm. In SQL Server 2003 each user having individual user login Id and password. For example in company they maintaining the database of employee details, in that they having employee name, personal details, designation, salary details include the credit card number, bank. If the hackers or unauthorized user can access and retrieve the database easily, so they can change the credit numbers or hacking the employee credit cards and their account numbers also. So we implement cryptographic techniques and genetic algorithm to secure the databases.

Cryptography is a method used to protecting data either over the network or in any stand alone device. It has two methods, encryption and decryption. Encryption is the process of converting plain text to cipher text and Decryption is the reverse process. Both encryption and decryption are done by private keys. This keys are secretly known by the end users, they keeping it highly confidential. The cryptographic techniques are of two types, Symmetric encryption and Asymmetric encryption. Before initiating security in symmetric encryption, the keys used are secretly shared by the user. The keys are generated based on a functionality by the end users during the process in a asymmetric encryption.

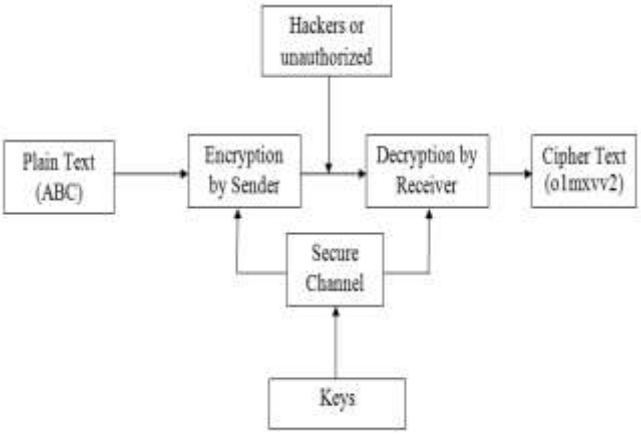


Fig 1 Secret communication between end user

Genetic algorithms were first introduced by John Holland at university of Michigan in the year 1970s.Genetic Algorithms are a family of computational models stimulated by evolution. This algorithm used most often in the fields where optimization is an important criteria. But it tends to be operationally expensive and time consuming at a time. A solution must be proposed which is called chromosome or genome. After this fitness function evaluates the best of the set of chromosomes, called as

population. If it is accepted as best is chose. If it is not satisfied then the operators in genetic algorithm such as reproduction, crossover [6] are applied to obtain better chromosomes.

II. PREVIOUS PROBLEM:

From webcohorot reports that atleast 92% of the network application may be subject to some form of hacker attacks, of which 60% may be subject to SQL injection attacks. UK IT security and control firm Sophos and Internet Crime Complaint Centre have issued a report that this year the number of SQL Injection attacks is rising, especially related to financial services i.e hacking credit card numbers, account numbers and banking details and online retail website. Sophos's network security threat reported SQL Injection attack will be the top five network security threats[2]. Therefore, defense against SQL injection attacks is very important.

III. PROBLEM STATEMENT

1.Invulnerability of Alpha numeric data

It is a cryptographic algorithm[3] technique that encrypts and decrypts alpha-numeric records i.e data. It works on principle of octal encoding and genetic algorithm includes operators of crossover, reproduction and fitness function. This algorithm having various advantages like the encoding scheme, crossover type. The decryption parts takes much lesser time than the encryption part. The encryption and decryption parts can run autonomously. The only disadvantage is that the algorithm cannot be simply used and implemented.

2. Cryptography based on Chaos

Chaos technique is much used in the field of Cryptography due to its deterministic environment and its sensitivity to initial values. This cryptography uses the ergodic property of the simple low-dimensional and chaotic logistic equation. This type of cryptography generates random but deterministic behaviour. The advantage of using chaos cryptography is that it can be directly implemented in a hardware without using digital to analogue conversion. The other advantages of chaos encryption are confrontation to traditional forms of attacks and complexity in detecting spectral peaks. There are a few disadvantages for this technique. The security of the system cannot be readily quantified, and hence the level of security is as yet not very well characterized. This system is insecure to encrypt very long messages as chaos mappings can repeat.

3. The responsibility of Cryptography in database security

Classical database security relies on many dissimilar mechanisms and techniques, including access control, information flow control, operating system and network security, prevention of statistical inference, data and user authentication, encryption, time-stamping, digital signatures, and other cryptographic mechanisms**[4]** and protocols. These methods together have the required mechanism to tackle any kind of attack on the database, since it uses all the techniques. But at the same time it may not be user friendly and it is time consuming because of the number of security measures that are to be satisfied. These type of techniques also require communication bandwidth so that the data transfer occurs between the database server and the client.

4. New Challenges in teaching database security

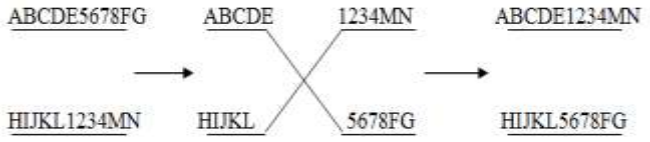
Traditional Database Security has determined primarily on creating user accounts and managing user privileges to database objects. The extensive spread use of databases over the web, heterogeneous client-server architectures, application servers, and networks creates an urgent need to widen this focus to secure the database from SQL injection, Multilevel Security**[5]** and Data Warehouse/Data Mining/Statistical security. Scheming a mechanism to secure a database is an necessary part of database security. Though many mechanisms are existing cryptography of a database is much chosen as it deals openly with data in it rather than on the associates to it. It seems to be cryptographic algorithm is most required for encryption/decryption of data in database that has less computing power.

IV. PROPOSED SYSTEM

To secure the database two techniques are implemented, one is cryptography and another one is genetic algorithm. The genetic algorithm can be used to choose the best key from encryption and also for decryption. Genetic algorithms consist of three phases as following:

1. Reproduction Operation[7]: The old string is carried through into a new population depending on the performance index values. The fitness values are calculated for each candidate string using a fitness function, which depends on a goal for optimization problems. According to the fitness values, string with larger fitness values give rise to a larger number of copies in the next generation.

2. Crossover operation[7]: The strings are randomly mated using the crossover operation. Each pair of candidate strings will undergo crossover with the probability cross. This operation provides randomized information exchange among the strings.



3. Mutation operation[7]: Mutation is simply an occasional random alteration of the value of a string position. In a binary code, this involves changing a 1 to 0 and vice versa.

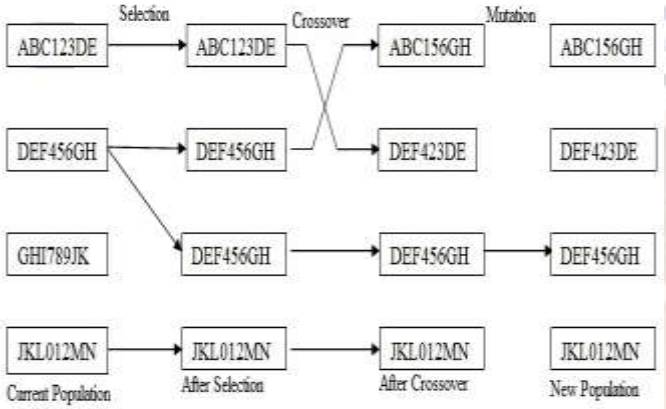


Fig 2 shows simple technique of genetic algorithm

V. PROBLEM IMPLEMENTATION

The method used for inserting, updating and viewing the data in the database is explained below and work as it is in Fig

I. Inserting values into the database

The method used for insertion is explained below and works as it is in Fig.3

1. Authentication

This is a basic security measure that is available in most of the systems. This Authentication feature has a valid user name and password. The feature has been designed in such a way that a particular userid cannot be used to login after three continuous unsuccessful attempts, i.e., that particular userid would be blocked and for further access the administrator has to reset the password.

Fig.3 Schematic Block Diagram for Insertion

2. Input Record

The record for the database is accepted. The type of encoding has to be specified for insertion the values of the fields in database are given. For Updating, initially the primary key value and the encoding type are given. If it is found to be valid then the other field values are obtained. The encoding type of a row cannot be changed while updating. In updating if the encoding type or the primary key value of the database is specified wrongly then the system automatically comes out of application.

3. Encryption Algorithm

All the data given in the above step are given to the encryption algorithm for encryption. These are the data that are to be encrypted before adding to the database. The encryption process has the following processes.

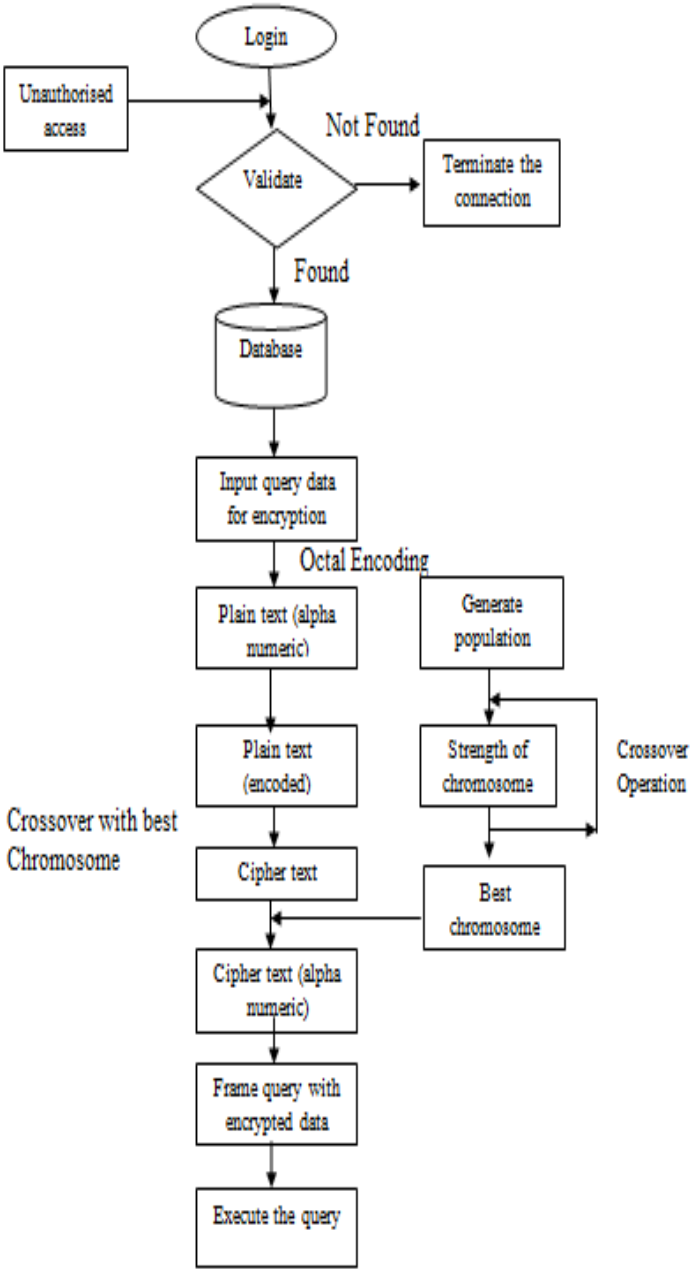


Fig 3. Schematic diagram of inserting records into the database

4. Encoding of plain text

The type of encoding depends on the problem. In this paper we have chosen octal encoding and binary encoding. Here each character has a specific

octal/binary representation. Considering the plain text as a stream of characters, the characters of the plain text are converted to an octal/binary format which is used in the further process of encryption.

5. Generating population (Key)

A population is an abstract representation of the keys. The set of keys generated are called chromosomes. The various chromosomes generated are of same length as the length of the octal/binary encoded plain text. Since the plain text is encoded, the population is generated in encoded format, depending on the encoding method used.

6.Manipulating potency of each key

The best key is to be chosen from the population so as to encrypt the data for which the strength of each key is required. The potency can be manipulated either through comparison within the keys or by comparing the encoded plain text with each key generated. In this paper the strength is calculated by comparing the keys with the encoded plain text. The strength is computed in a series of iterations so that the best is chosen.

7. Choosing the best key

From the above step the genome with the maximum strength is considered as the best key. The best key will be the key to facilitate particular encoded plain text. This process is continued for each set of encoded plain text. The population is generated for each and every input based on the length of the input given.

8. Crossover operator

Crossover is a genetic algorithm operator. This is the main part of encryption , the best key is selected and operated by crossover operator. Any type of crossover operator can be implemented. In this proposed paper we have chosen multi point crossover operator where some parts of the plain text are encoded and some parts of the best key are interchanged for creation of new cipher text. The newly formed genomes are combined together to produce a single output.

9. Alpha numeric cipher text

The cipher text obtained in the previous step is again converted back to alpha-numeric form by using the same encoding scheme.

10. Outline Query

The result of the above step gives us the encrypted data that is to be put in the database. With the encrypted data the query is formed with them as input to database.

11. Query Execution

The query framed with the encrypted data is then executed to put the values into the database. The database is verified for successful insertion or updating or viewing.

II. Updating and viewing the records in the database

1. Encoding

The receiver obtains the cipher text which is in alphanumeric format. But since the encryption was done in an octal/binary format, the cipher text is again encoded to octal/binary format. The sender and receiver use the same type of octal encoding schemes so as to maintain integrity and this is decided before the encryption and decryption of data starts.

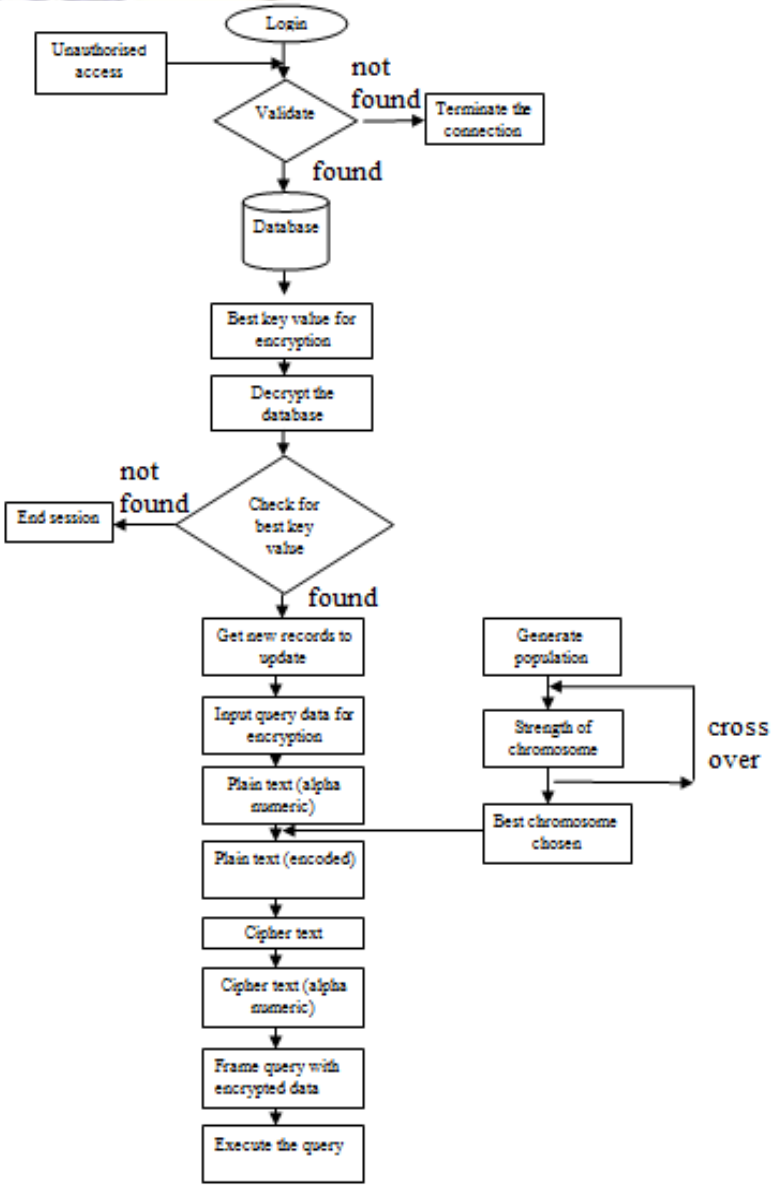


Fig.4 Schematic Block Diagram for updating data

2.Interchange Characters

After converting the cipher text to octal format, the receiver proceeds to get back the octal encoded plain

text and the original best key are obtained. The process is done by taking the alternate characters with first one for data and the next one for key. This process is repeated for all the data that he receives. Since our paper used multi point crossover during encryption, which both the users share before starting the communication.

3. Octal Decoding

The decryption is not complete after reverse crossover of the cipher text. The reverse crossover gives only the octal
encoded plain text. But the plain text is not octal encoded according to sender. So the octal decoding is to be done with the octal encoded plain text. Thus after this step the receiver gets the complete plain text. The method used for updating is as shown below

VI CONCLUSION

With the rapid development of network database, it facing major difficulties like accessed by unauthorised users, hackers and others. So overcome this problem we use cryptography and genetic algorithm. The encryption of the database into alpha-numeric form is achieved by performing octal encoding, crossovers and octal decoding and then sent to the receiver where the receiver decrypts the cipher text by performing octal encoding, reverse crossover and octal decoding the octal sequence. The number of iterations increased rapidly based on the growth of population and crossover operations. It is pointed out the increase in iteration, is more probability of the best one to be produced and chosen. This algorithm can be used to secures the data by encrypting it and then storing into the database. Also we observe that the implementation of genetic algorithm in symmetric encryption provides security in the style of encoding, crossover type, length of the data and key used. Another advantage of the algorithm is that there will not be same cipher text for a single plain text at two different times.

REFERENCES

1. website:http://www.wikipedia.com/database security
2. Zixin Wag, Guoyuan Lin, Computer Network Database attack and defense, 978-1-61284-459/11/$2600©2011 IEEE
3. R.Chella Govindarajan, V.Veda Narayanan, G Vinodhini, Prof.C.D.Suriyakala. Immunity of Alpha-Numeric Data. In Proc. Of 6th Control Instrumentation & System Conference (CISCON-09), PP. 190-192, Nov. 2009
4. Ueli Maurer, The Role of Cryptography in Database security. SIGMOD 2004, June 13–18,2004, Paris, France. Copyright 2004 ACM 1581138598/04/06
5. Mario Guimaraes, New Challenges In Teaching Database Security, InfoSecCD Conference'06, September 22-23, 2005, Kennesaw, GA, USA. Copyright 2006 ACM 1-59593-437-5/00/0006.
6. website: http://www.obitko.com/tutorials/ geneticalgorithms/ crossover-mutation.php
7. A Genetic Algorithm for Cryptanalysis with Application to DES-like Systems, International Journal of Network Security, Vol.8, No.2, PP.177–186, Mar. 2009
8 Bagnall A., The Application of Genetic Algorithm Cryptanalysis, Mater Degree Thesis, 1996, School of Information Systems, University of East Anglia
9. Cryptography with chaos by Baptista, M. S. Physics Letters A, Volume 240, Issue 1-2, p. 50-54.