Database Security – Attacks and control Methods Using REA and ROT

Dileep Kumar Rawat[1], Ram Singar Verma[2]
[1]Student, [2]Assistent Professor
Department Of Computer Science, CET (UIET)
Babasaheb Bhimrao Ambedker University, Luck now, India

ABSTRACT: Database, which is collection of huge sensitive and important data. Therefore, Security of data and database has become an important issue in technical world. Database often hold the backbone of an organization. Its transactions, customers, employee info, financial data for both the company and its customers and much more. Therefore, in this paper, we have focus on attacks related to database as well as several control methods and techniques related to database security. Encryption algorithm is one of the way to give protection to the database from various threat or hackers who target to get confidential information. This paper discuss about the proposed encryption algorithm to give security to such database.

KEYWORDS: **Database Security, Attacks, Threats, Encryption, REA and ROT.**

I. INTRODUCTION

Database is an integral part of our day-to-day life and many database users store their sensitive data in their databases. Information or data is one of the most valuable assets in any organization. Almost all organization like social, governmental, educational etc…have now automated their information system and other operational or non-operational working function. They have maintained database that contains important and sensitive data so database security is very important and serious issues in technical world. Now we shall first discuss what Database Security is?.

Database Security

Database security is the mechanism that protect database against international or accidental threats. Database security refers to the collective measures used to protect and secure a database or database management software from illegitimate use and malicious threats and hackers

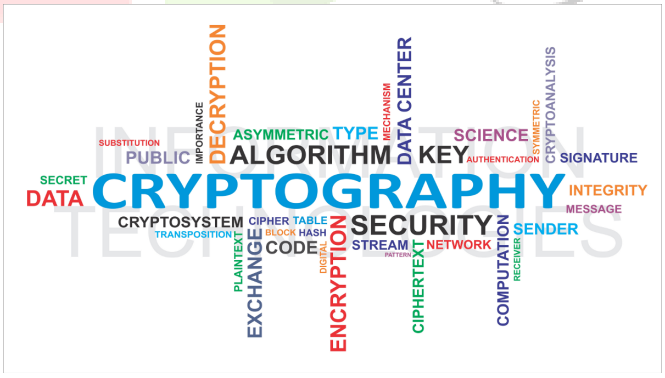
Database security techniques

1.2. Encryption

Encryption is the process of encoding or transforming information by means of a cipher or a code so that it becomes unreadable to all other people except those who hold a key to the information. The resulting encoded information is called as encrypted information.

1.3. Cryptography

Cryptography is the science of encoding information before sending via unreliable communication paths so that only an authorized receiver can decode and use it. The coded message is called cipher text and the original message is called plain text. The process of converting plain text to cipher text by the sender is called encoding or encryption. The process of converting cipher text to plain text by the receiver is called decoding or decryption.



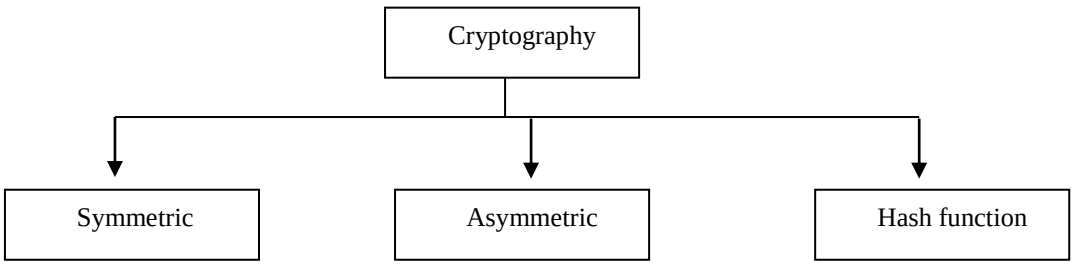


Figure 1 : Cryptography

1.3. Steganography

Steganography is data hidden within data. It is the art and science of embedding the hidden content in unremarkable cover so that the existence of the secret gets hidden. Steganography protects from pirating copyrighted materials, as well as from unauthorized viewing. People used hidden tattoos or invisible ink in the past to convey hidden (stenographic) content.

1.4. REA

Reverse Encryption algorithm or REA is a symmetric encryption algorithm that is used to protect sensitive data in database. REA is simple, secure and efficient, and takes a variable-length key, making it flawless for data security.

1.5. ROT13

The ROT13 encryption algorithm is a special case of the Caesar cipher, with a fixed key of 13.ROT13 has been under wide use for over 30 years for email and Usenet (network). ROT13 was mostly useful for encrypting messages.ROT13 is based on the principle that every letter in a reference alphabet corresponds to another letter in a rotated alphabet.

2. Attacks

An **attack** is any attempt to expose, alter, disable, destroy, steal or gain unauthorized access to or make unauthorized use of an Asset.

There are four types' attacks in database.

2.1 Direct attacks: Directly hitting the target data is known as direct attack. These attacks are accessible and successful only if the database does not accommodate any protection system. If this attack fails, the attacker moves to the next.

2.2 Indirect attacks: As its name implies indirect attacks are not directly executed on the target but data from or about the target can be collected through other transitional objects. For purpose to cheat the security system, some of the combinations of different queries are used. These kinds of attacks are difficult to track.

2.3. Passive Attack: In this, attacker only inspects data present in the database and do not perform any alteration. Passive attack can be carried out in following ways:

1) Static leakage: In this attack, information about database plaintext values can be attained by examining the snapshot of database at a particular time.

2) Linkage leakage: in this information about plain text values can be achieve by linking the database values to position of those values in index.

3) Dynamic leakage: changes performed in database over a period of time can be observed and analyzed and information about plain text values can be obtained.

2.4. Active Attacks: In active attack, actual database values are modified. These are more problematic than passive attacks because they can misguide a user. There are various ways of performing such kind of attack which are mentioned below:

1) Spoofing – In this attack, cipher text value is replaced by a generated value.
2) Splicing – in this, a cipher text value is replaced by different cipher text value.
3) Replay – It is a kind of attack where cipher text value is replaced with old version previously updated or deleted.

3. Threats

Threats are potentials for vulnerabilities to turn into attacks on computer systems, networks, and more. They can put individuals' computer systems and business computers at risk, so vulnerabilities have to be fixed so that attackers cannot infiltrate the system and cause damage.

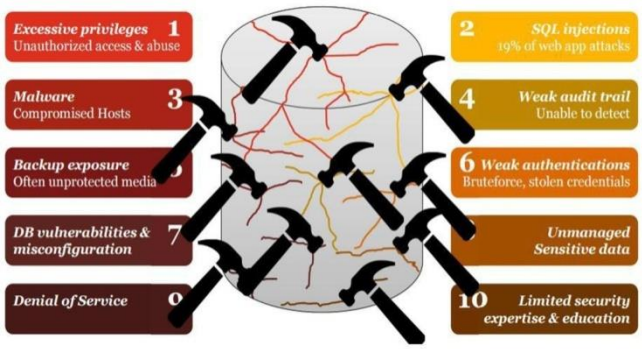


Figure 6 : Threats in Database

Threats to security in Database

3.1. Excessive privileges

When database users are granted enormous allowance that exceeds then their required job function, than these privileges may be abused for malicious purpose. E.g. a user in a company have the rights to change employee contact information may take advantage of excessive database update privileges to change salary information.

3.2. Legitimate Privilege Abuse

Legitimate privilege abuse is when an authorized user mistreats their legitimate database privileges for illegal purposes. Legitimate privilege abuse comes in existence when the database administrators or a system manager misused their rights and doing any unconstitutional or unethical activity. But this threat is not bound to, any misuse of sensitive data or unjustified use of privileges.

3.3. Privilege Elevation

Sometimes there are errors in software and attackers can take it as a chance to convert their access rights from normal user to those of an administrator, which could result in fake accounts, funds transfer, and misunderstanding of certain analytical information.

3.4. Platform Vulnerabilities

Vulnerabilities in operating systems such as window 98, window 2000 etc. and additional services installed on a database server may lead to illegal access, denial of service or corruption of data. E.g., the Blaster Worm which is a type of computer worm that spread on Windows 2000 vulnerability to construct denial of service conditions.

3.5. SQL Injection

In this attack, an attacker execute (or "injects") random unauthorized SQL statements into a liable SQL data channel. Targeted data channels consists stored procedures and Web application input parameters. Inserted statements are then passed to the database where they are executed.

3.6. Weak Audit Trails

A database audit policy assures automated, on time and appropriate tracking of transactions performed in database. This kind of feature must be a part of the database security policy since all the crucial database transactions have an automated record and if it is missing in it may causes serious risk to the organization's databases and could results instability in working.

3.7. Denial of Service

This type of attack prohibit the all legitimate users of a database to access some specific service in database. Attacker may crash the server by getting access to the databases. There are various conditions of DOS which may be created via many techniques like data corruption and network flooding etc.

3.8. Backup Data Exposure

Backup database storage media is often not safe from an attack and exposure to high risk as well as a natural disaster like flood, earthquake etc. As a result, many high profile security breaches have involved theft of database backup tapes and hard disks.

II. Literature Review/Related work

In this area significant amount of work is found. Here we have reviewed and used following references for this article.

2.1. Shelly Rohilla, Pradeep Kumar Mittal

Databases are a favorite target for attackers because of their confidential and important data. There are many ways in which a database can be compromised. There are various types of attacks and threats from which a database should be protected. In this paper, solutions of most of the threats mentioned, although some solutions are good while some are only temporary. Different types of threats are discussed in this paper

2.2. Shivnandan Singh, Rakesh Kumar Rai

Databases form the backbone of many applications today. They are the primary form of storage for many organizations. So the attacks on databases are also increasing as they are very dangerous form of attack. They reveal key or important data to the attacker. Various attacks on databases are discussed in this paper.

2.3. Mubina Malik, Trisha Patel

Data is stored in database for easy and efficient way to manage these data. All the operations of data manipulation and maintenance are done using Database Management System. Considering the importance of data in organization, it is absolutely essential to secure the data present in the database. A secure database is the one which is reciprocated from different possible database attacks. Security models are required to develop for databases. Different types of control methods discussed in this paper.

III.Methods

The Proposed Database Encryption Algorithms

1. **REA- Reverse Encryption Algorithm**

The keys are concatenated to the text in the encryption process and removed from the text in the decryption process. Mathematical Divide operation is performed on the text data by 4 in the encryption process and multiple operations on the text by 4 have been done in the decryption process. Divide by 4operation is performed on the text to narrow the range domain of the ASCII code the cost time of the encryption and decryption operations can be reduced and the performance is also improved by REA. Fig. Shows the working principles of REA encryption algorithm and Fig. shows the simple example of the existing algorithm REA.

1.1. REA Encryption Algorithm:

1) Add the key before the data to be encrypted.
2) Replace the data to ASCII code and change that ASCII to binary data.
3) Reverse the binary data and convert 8 bits binary data in the form of ASCII code
4) Divide the converted ASCII code by 4 from Divide operation put the Quotient as the 1st character and Remainder as the 2nd character
5) Return encrypted data.

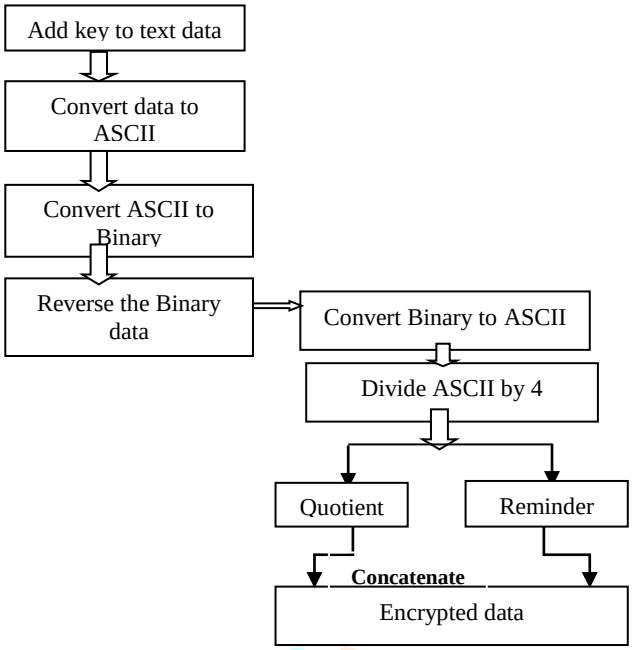


Figure3: Working of REA

1.2. Correlation Coefficient

Statistical analysis such as correlation coefficient factor Eq. (1) is used to measure the relationship between two variables the plaintext and its encryption for the REA Encryption Algorithm

$$CorrCoef\,(x,y) = \sum_{i=0}^{n}(x' - \mu(x)(y' - \mu(y)\,/\partial(x)\partial(y) \quad \text{..... (1)}$$

Where μ(x) and μ(y) are the respective means of x and y in Eq. (2):

$$\mu(x) = 1/n\sum_{i=0}^{n} x', and\ \mu(y) = 1/n\sum_{i=0}^{n} y' \quad \text{..... (2)}$$

x and y are variables of the plaintext and cipher text and the terms in the denominators (It is called the Standard deviation of x and y are Eq. (3) :

$$\partial(x) = \sqrt{\sum_{i=0}^{N}(x' - \mu(x)^2} \qquad \text{And}$$

$$\partial(y) = \sqrt{\sum_{i=0}^{N}(y' - \mu(y)^2} \quad \text{..... (3)}$$

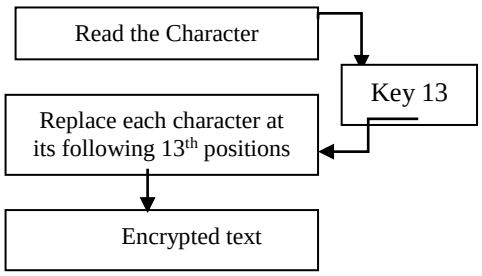
2. ROT18

ROT18 is a very simple encryption method.ROT18 is a combination of ROT5 and ROT13.It converts both numbers and characters. ROT18 replaces each one letter by 13th character further along the alphabet. The rotation of 18 was chosen because the Latin alphabet that is common in the western consists of 26 letters. The letter A of the reference alphabet corresponds to the letter N of the rotated alphabet and the letter N of the reference alphabet corresponds to the letter A in the rotated alphabet. Fig. 4 narrates the working of ROT18 encryption algorithm. The secret key of ROT18 encryption algorithm is 18 and the example of the same is depicted in Fig.4.

2.1 *The steps of Rot18 algorithm are presented as follows:*

1) Read the char and the Rot value 13
2) Get the ASCII value of the char
3) If the ASCII value of the char Read is in between (‘65’ and ‘90’) or (‘97’ and ‘122 ‘) do step 4
4) Add previous ASCII value with ROT
5) If the summed value is (>90)
6) Compute Subtraction of ROT with the ASCII value
7) Obtain the char for the Previous Result
8) Repeat step – 1 to 7 for all the characters to be encrypted

Return the Encrypted text



Example for ROT18

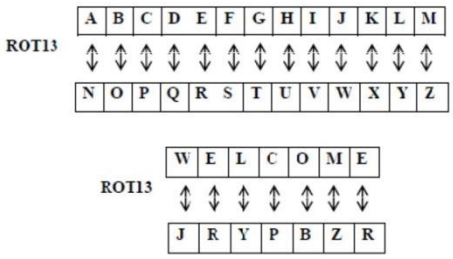


Figure4: ROT18 encryption

IV.RESULTS AND DISCUSSION

1. Proposed system

The proposed system "Database security-Attacks and Control methods using ROT18 & REA" includes the main concepts from the REA with the ROT18 encryption algorithms. The detailed steps of the existing and the proposed algorithms were discussed in the remaining of the paper

6.1. Proposed Algorithm

The proposed algorithm is the combination of REA and ROT13 encryption algorithm. As previously said more rounds of encryption bring more security. Instead of executing the same algorithm, the proposed approach combines two existing algorithms, which already proved to be to be best in database security. The steps of proposed encryption algorithm are given

6.1.1. Steps of the proposed Algorithm

1. Input the data and key value.
2. Concatenate the key to the data.
3. Convert the previous data to binary code.
4. With each 8 bits binary data divided into two portions and perform Rotate operation by 3 place for both the portions each.
5. Again gather each 8 bits binary data from step 4 and convert to the decimal data.
6. Divide the previous decimal code by 4.
7. Obtain the ASCII code of the previous result of divide operation put the Quotient as the 1st character and reminder as the 2nd character.
8. Return encrypted text.

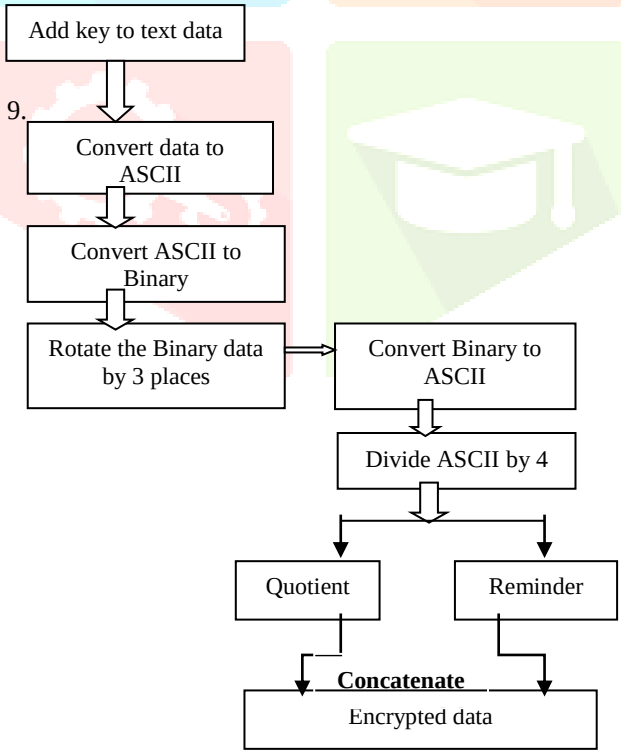
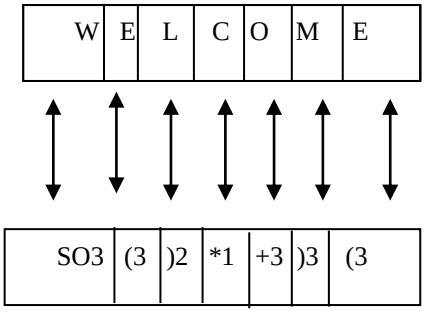


Figure5: Implementation of Proposed Algorithm

2. Example for proposed algorithm (Rotate by 3)

Fig. 5 gives the encrypted content using the proposed algorithm and the processing steps were discussed followed by that.



Proposed Algorithm

Fig.6 Encrypted data using the proposed algorithm Algorithms Steps

Example

1. Add the key to the data.
   123Welcome
2. Convert the data to ASCII code.

   1-> 49, 2 -> 50, 3 -> 51, 4-> 52, W -> 87, e ->101, l ->108, c ->99, o ->111, m ->109, e->101

3. Convert the ASCII code to binary data.
4. 00110001 00110010 00110011 00110100 01010111 01100101 01101100 01100011 01101111 01101101 01100101 4) Separate the each 8 binary data divide into two halves rotate it by 3 place and leave the 4th place as it is Eg: 0011 0001 □ 1001 0001
   10010001 10011000 10011001 10010010 00111011 10100011 10100110 10101001 10101111 10100111 10100011

5. Gather each 8 bits from the binary data and obtain the ASCII code.
   152 153 59 146 163 166 169 175 167 163

6. Divide the previous ASCII code by 4 and obtain the ASCII of the result (put it as one ASCII character) and obtain the remainder (put it as second character).
   145/4 = 36 -> $(ASCII of 36) and the remainder = 1(join ASCII of quotient and remainder $1).
   152/4 = 38->& (ASCII of 38) and the remainder = 0 (join ASCII of quotient and remainder &0).
   153/4 = 38 ->& (ASCII of 38) and the remainder = 1 (join ASCII of quotient and remainder &1).
   59/4 = 14 ->SO (ASCII of 14) and the remainder = 3 (join ASCII of quotient and remainder SO3).
   163/4 = 40 -> ((ASCII of 40) and the remainder = 3 (join ASCII of quotient and remainder (3).
   166/4 = 41 ->) (ASCII of 41) and the remainder = 2 (join ASCII of quotient and remainder) 2).
   169/4 = 42 -> * (ASCII of 42) and the remainder = 1 (join ASCII of quotient and remainder *1).
   175/4 = 43 ->+ (ASCII of 43) and the remainder = 3 (join ASCII of quotient and remainder +3).
   167/4 = 41 ->) (ASCII of 41) and the remainder = 3 (join ASCII of quotient and remainder) 3).
   163/4 = 40 -> ((ASCII of 40) and the remainder = 3 (join ASCII of quotient and remainder (3).
7. And the encrypted text is
   $1(2)&0&1SO3(3)2*1+3)3(3

V.CONCLUSION

Any organization, data is a most valuable property. Security of sensitive data is always a big challenge for an organization at many levels. A Number of encryption algorithms are designed in a way that the process of encrypting the data is several times, so called “Rounds” to protect the database from unauthorized users and other risks security. Security provided by the proposed algorithm will be high enough, because it combines the features of the Existing algorithms ROT13 and REA, as they are individually proved best. The proposed algorithm might take more execution as it combines the two algorithms.
The future work could be carried out make encryption more effective and efficient.

VI. ACKNOWLEDGMENT

We take this opportunity to thank our teachers for their support and encouragement for completing this report. Without their willingness to help us, this could not have been an easy task to complete.

VII.REFERENCES

[1] M.Sujitha ,An encryption algorithem for improving Database Security using REA and ROT, Indian Journal of Computer Science and engineering, Vol. 6 No.3 Jun-Jul 2015**.**

[2] Thomas M.Connolly, Carolyn E.Begg(2008).” Database Systems: A Practical Approach to Design, Implementation, and Management”,4th Edition, Pearson Education .pp.[541-542]..

[3] Mubina Malik, Trisha Patel, Database Security- Attacks and Control Methods. International Journal Information Sciences and Techniques, Vol. 6 (1/2) , 2016.

[4] Deepika, Nitasha Soni, and Database Security: Threats and Security Techniques, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 5, May 2015.

[5] RobiniA.Chirde, KulkarniS.S.(January 2014),”Assessing Performance of Encrypted Databases under query processing with the REA Algorithm”, International Journal of Advance Research in Computer Science and Management Studies, Volume 2,Issue 1,ISSN:2321-7782.

[6] Emil BURTESCU, Database Security- attacks and Control Methods, Journal of Applied Quantitative Methods, Volume 4, Issue 4, 2009

[7**]** Ayman Mousa, Osama S.Faragallah, EL-Rabaie, S., NigmE.M. (March 2013),"Security Analysis of Reverse Encryption Alogrithm for Databases", International Journal of Computer Applications(0975-8887),volume 66-No.14,pp.19-26.