IJIRMET ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 9, Issue 10, October 2024

Secure Transformation of Data in Relational Database Management System

[1] Aravindhan . N
[1] Assistant Professor, Department Of Mca, Er Perumal Manimekalai College Of Engineering(Autonomous),Hosur, Tamil Nadu, India

Abstract: ***Cryptography is the art or science encompassing the principles and methods of transformation an intelligible message (Plain Text) into one that is unintelligible (Cipher Text), and then retransforms that message back to its original form. For this transformation (or) conversion some critical information called as key (secret key) is used by the sender and receiver.***

Security mechanisms involve more than a particular algorithm or protocol. They also require that participants be in possession of some secret information (e.g., an encryption key), which raises questions about the creation, distribution, and protection of that secret information. There also may be a reliance on communications protocols whose behavior may complicate the task of developing the secret mechanism.

Here a mechanism is proposed for data security based on secure embedding Algorithm. This approach overcomes a major weakness in previously proposed techniques, by reducing probability of decoding errors. An Implemented results shows that our techniques delivers the data in secure manner without any alterations.

I. INTRODUCTION

The software for a relational database is called the Relational Database Management System (RDBMS), it controls reading, writing, modifying, and processing the information stored in the databases. The data is formally described and organized according to each database's relational model (database schema), according to the design.

Each database is a collection of related tables. Each table is a physical representation of an entity or object that is in a tabular format consisting of columns and rows. Nowadays the secure transformation of these databases takes more important.

In my Thesis contents are Problem specification, Methodology, Relational Database System, Module Description, Implementation, Results and Discussion and conclusion.

II. Problem Specification

Nowadays databases play vital role in day to day office activities. Database management system stores, organizes and manages large amount of data within a single software application. The main problem in this database is security. Data security is critical for more business and even home computer users.

Database is used to collect and store information. The main problem in this database management system is Data Security. Data security is critical for most businesses and even home computer users. Client information, payment information, personal files, bank account details - all of this information can be hard to replace and potentially dangerous if it falls into the wrong hands. Data lost due to disasters such as a flood or fire is crushing, but losing it to hackers or a malware infection can have much greater consequences.

Database security is the business of the entire organization as all people use the data held in the organization's database and any loss or corruption to data would affect the day-to-day operation of the organization and the performance of the people. Therefore, database security encompasses hardware, software, infrastructure, people and data of the organization.

Now there is greater stress on database security than in the past as the amount of data stored in corporate database is increasing and people are depending more on the corporate data for decision-making, customer service management, supply chain management and so on. Any loss or unavailability to the corporate data will halt today's organization and will seriously affect its performance.

Now the unavailability of the database for even a few minutes could result in serious losses to the organization.

Getting unauthorized access to computer systems is known as hacking. Computer hackers have developed stylish methods to obtain data from databases, which they may use for personal gain or to harm others. This investigation deals with providing security to transformation of data in relational database management system.

III.Methodology

Microsoft .NET is a set of Microsoft software technologies for rapidly building and integrating XML Web services, Microsoft Windows-based applications, and Web solutions. The .NET Framework is a language-neutral platform for writing programs that can easily and securely interoperate.
There's no language barrier with .NET: there are numerous languages available to the developer including Managed C++, C#, Visual Basic and Java Script. The .NET framework provides the foundation for components to interact seamlessly, whether locally or remotely on different platforms. It standardizes common data types and communications protocols so that components created in different languages can easily interoperate.

".NET" is also the collective name given to various software components built upon the .NET platform. These will be both products (Visual Studio.NET and Windows.NET Server, for instance) and services (like Passport, .NET My Services, and so on).

IV.Relational Database Management System

The software for a relational database is called the Relational Database Management System (RDBMS); it controls reading, writing, modifying, and processing the information stored in the databases. The data is formally described and organized according to each database's relational model (database schema), according to the design. Each database is a collection of related tables. Each table is a physical representation of an entity or object that is in a tabular format consisting of columns and rows.

Features of RDBMS

1. It stores data in tables.
2. Tables have rows and column.
3. These tables are created using SQL.
4. And data from these tables are also retrieved using SQL

V. Module Description

Encoding and Decoding

Encoding is the process of putting a sequence of characters (letters, numbers, punctuation, and certain symbols) into a specialized digital format for efficient transmission or transfer. Decoding is the opposite process, the conversion of a digital signal into a sequence of characters.

Encoding and decoding are used in data communications, networking, and storage. The code used by most computers for text files is known as ASCII (American Standard Code for Information Interchange, pronounced ASK-ee). ASCII can depict uppercase and lowercase alphabetic characters, numerals, punctuation marks, and common symbols. Other commonly-used codes include Unicode, BinHex, Uuencode, and MIME. In data communications, Manchester encoding is a special form of encoding in which the binary digits (bits) represent the transitions between high and low logic states.

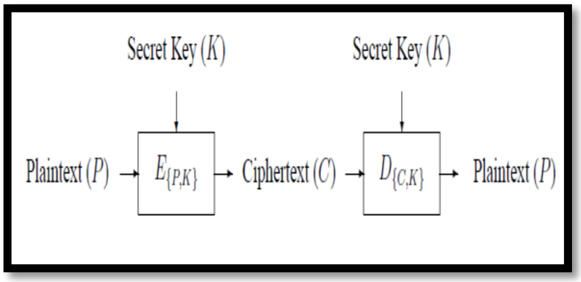
In radio communications, numerous encoding and decoding methods exist, some of which are used only by specialized groups of people (amateur radio operators, for example). The oldest code of all, originally employed in the landline telegraph during the 19th century, is the Morse code.

The terms encoding and decoding are often used in reference to the processes of analog-to-digital conversion and digital-to-analog conversion. In this sense, these terms can apply to any form of data, including text, images, audio, video, multimedia, computer programs, or signals in sensors, telemetry, and control systems.

During encoding, a database is selected as input and it is converted as encoded file using base64string technique. During decoding the reverse process is taken place using from64string technique.

Encryption and Decryption

Encryption is a process of coding information which could either be a file or mail message in into cipher text a form unreadable without a decoding key in order to prevent anyone except the intended recipient from reading that data. Decryption is the reverse process of converting encoded data to its original un-encoded form, plaintext. A key in cryptography is a long sequence of bits used by encryption / decryption algorithms.



Encryption algorithm takes the original message, and a key, and alters the original message mathematically based on the key's bits to create a new encrypted message. Likewise, a decryption algorithm takes an encrypted message and restores it to its original form using one or more keys.

To accomplish encryption, most secret key algorithms use two main techniques known as **substitution** and **permutation**. Substitution is simply a mapping of one value to another whereas permutation is a reordering of the bit positions for each of the inputs. These techniques are used a number of times in iterations called **rounds**. Generally, the more rounds there are, the more secure the algorithm. A non-linearity is also introduced into the encryption so that decryption will be computationally infeasible without the secret key. This is achieved with the use of **S-boxes** which are basically non-linear substitution tables where either the output is smaller than the input or vice versa.

One of the main problems with secret key cryptography is **key distribution**. For this form of cryptography to work, both parties must have a copy of the secret key. This would have to be communicated over some secure channel which, unfortunately, is not that easy to achieve. As will be seen later, public key cryptography provides a solution to this.

Data Encryption Standard (DES) is used as symmetric algorithm to encrypt the data in this investigation. DES is a 64 bit block cipher which means that it encrypts data 64 bits at a time. The DES algorithm is a basic building block for providing data security. To apply DES in a variety of applications, five modes of operation have been defined which cover virtually all variation of use of the algorithm.

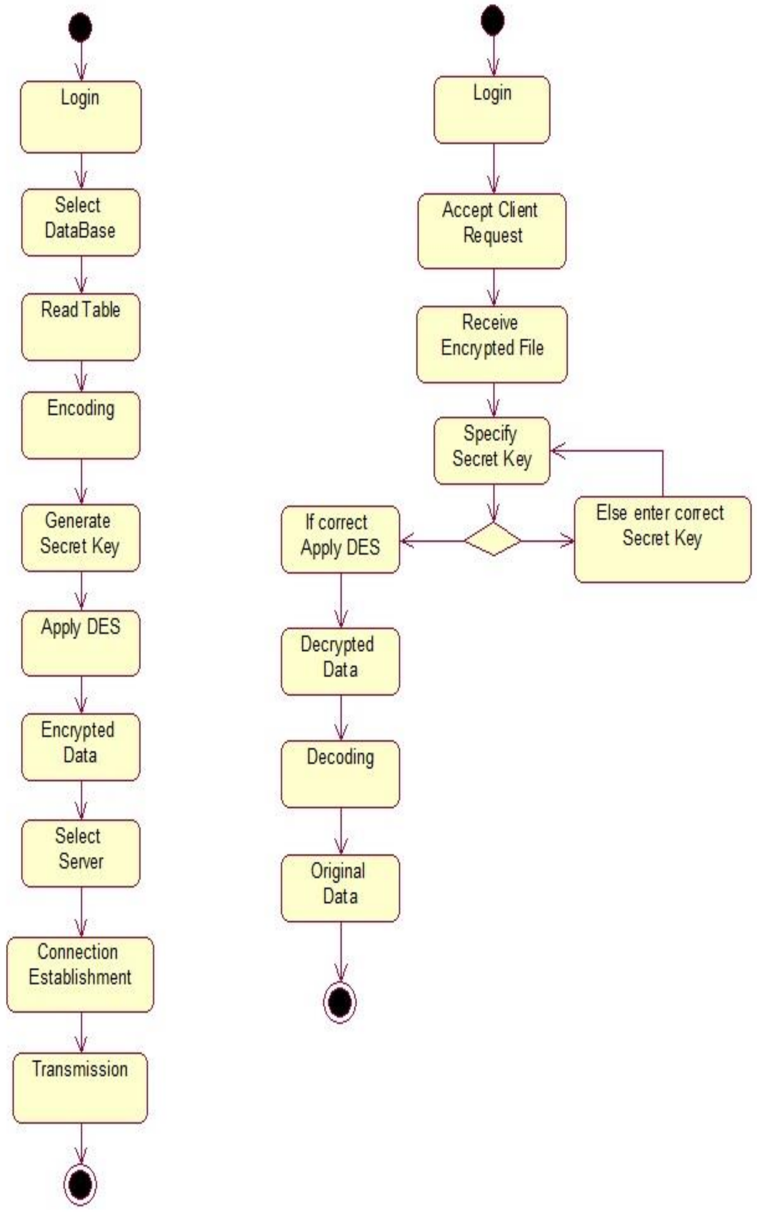
Connection Methods

1. When Connected with TCP
2. When not Connected with TCP.

1.When Connected with TCP

Transmission Control Protocol (TCP) is one of the main protocols in TCP/IP networks. Whereas the IP protocol deals only with packets, TCP enables two hosts to establish a connection and exchange streams of data. TCP guarantees delivery of data and also guarantees that packets will be delivered in the same order in which they were sent.

Activity Diagram



2.When not connected with TCP

Single system acts as a client and also server. So, there is no need of TCP connection. Encode, decode and encryption, decryption processes are done in the same system. A single key automatically generated for encryption technique and the same key used for decryption technique.

VI. Implementation

In this investigation two concepts are implemented based on connection. First one is when connected with TCP and second one is when not connected with TCP. In this process I used MS Access and SQL Database tables. This Database tables refers to rows and columns it is called as tuples.

When connected with TCP, connection establishment made between two systems and the encrypted file is transferred from a system to another system via LAN cable. After receiving the encrypted file, the system sends the acknowledgement to another one.

When not connected with TCP, Single system acts as a client and also server. So, there is no need of TCP connection. Encode, decode and encryption, decryption processes are done in the same system. A single key automatically generated for encryption technique and the same key used for decryption technique.

VII. Results and Discussions

While increasing the file size, the time for encryption and decryption also increased

Original File Size	Encoded File Size	Encrypted File Size	Encryption Time	Decryption Time
300 KB	380 KB	380 KB	3s: 67ms	3s: 67ms
500 KB	580 KB	580 KB	4s: 05ms	4s: 05ms
700 KB	780 KB	780 KB	4s: 30ms	4s: 30ms

VIII. Conclusion

Database plays major role in data storage and retrieval. Many organizations and institutions use this database management system to maintain their information. Basically, several types of databases are available like MySQL, SQL, Microsoft Excel and Microsoft Access Database. People uses these databases based on their purpose. Here, security is an important issue to keep up their files safe. Data security is critical for most businesses and even home computer users. Client information, payment information, personal files, bank account details - all of this information can be hard to replace and potentially dangerous if it falls into the wrong hands. Data lost due to disasters such as a flood or fire is crushing, but losing it to hackers or a malware infection can have much greater consequences. So, to overcome this issue, data security concept is implemented using cryptographic technique. In this investigation, two different methods have been implemented to secure the data named with and without TCP connection. To provide security Encoding and Encryption techniques are implemented based on Data Encryption Standard. It transfers the data in secure manner with less packet loss. Also this technique minimizes the decoding error. Developing the same data security concept for wireless network will be done in future to increase the scalability and mobility.

References

1. R. Agrawal and J. Kiernan, “Watermarking Relational Databases,” Proc. 28th Int’l Conf. Very Large Data Bases, 2002.
2. M. Atallah and S. Lonardi, “Authentication of LZ-77 Compressed Data,” Proc. ACM Symp. Applied Computing, 2003.
3. M. Atallah, V. Raskin, C. Hempelman, M. Karahan, R. Sion, K. Triezenberg, and U. Topkara, “Natural Language Watermarking and Tamperproofing,” Proc. Fifth Int’l Information Hiding Workshop, 2002.
4. G. Box, “Evolutionary Operation: A Method for Increasing Industrial Productivity,” Applied Statistics, vol. 6, no. 2, pp. 81- 101, 1957.
5. E. Chong and S. Z_ ak, An Introduction to Optimization. John Wiley & Sons, 2001.
6. D. Coley, “Introduction to Genetic Algorithms for Scientists and Engineers,” World Scientific, 1999.
7. C. Collberg and C. Thomborson, “Software Watermarking: Models and Dynamic Embeddings,” Proc. 26th ACM SIGPLANSIGACT Symp. Principles of Programming Languages, Jan. 1999.
8. I. Cox, J. Bloom, and M. Miller, Digital Watermarking. Morgan Kaufmann, 2001.
9. E. Dolan, R. Lewis, and V. Torczon, “On the Local Convergence of Pattern Search,” SIAM J. Optimization, vol. 14, no. 2, pp. 567-583, 2003.
10. F. Hartung and M. Kutter, “Multimedia Watermarking Techniques,” Proc. IEEE, vol. 87, no. 7, pp. 1079- 1107, July 1999.
11. Darshana Mistry, “Comparison of Digital Water Marking methods,” International Journal on Computer Science and Engineering - Vol. 02, No. 09, 2010, 2905-2909
12. Dolley Shukla and Manisha Sharma, “WATERMARKING SCHEMES FOR COPY PROTECTION: A SURVEY,” International Journal of Computer Science & Engineering Survey (IJCSES) Vol.3, No.1, February 2012
13. K.Ganesan and Tarun Kumar Guptha, “Multiple Binary Images Watermarking in Spatial and Frequency Domains,” Signal & Image Processing: An International Journal (SIPIJ) Vol.1, No.2, December 2010