International Journal of Scientific Research & Engineering Trends
Volume 8, Issue 3, May-Jun-2022, ISSN (Online): 2395-566X

To Provide Security for Database Using Encryption and Decryption

Asst. Prof. M.Thangamani M.Sc, M.Phil, B.Ed
352, Holy Cross Arts and Science College for Women,
Tirupattur-Tirupattur Dt. India
Affiliated To Thiruvalluvar University, Serrkadu, Vellore
Email: mthangamani17@gmail.com

Abstract- Encryption is the process of transforming information from an unsecured form or Plain Text into coded information or Cipher Text, which cannot be easily real by strangers. An algorithm and key. control the entire transformation process. This process may be reversible, so that the intended recipient can return the information to its original readable form. But reversing the process, without the appropriate encryption information is not possible. This means that the details of the key must also be kept secret. The use of cryptography in daily life is growing immensely. This is due to the necessity for hiding the content from unauthorized person. As the days pass by the old algorithms used in crypiography may not remain as strong as it was before Hence, the cryptanalysts suggest new algorithms for the same. Currently the computers are faster and in future its speed will also increase rapidly Brute force attacks are made to bereak the encryption and are emerging faster. These attacks are the main drawbacks for the older algorithms. In future these algorithms will be replaced by new algorithms that will enhance a better protection. In this investigation, a new encryption technique is proposed, which is more faster, better immune to attacks more complex, easy to encrypt and many more advanced security features are comprised. Encryption can also provide strong security for data, but developing a database encryption strategy will take many factors into consideration "Combination of encryption and decryption for secure communication" is an application which combines both encryption and decryption techniques, to make the communication more secure. It is concerned with embedding information in a secure and robust manner. Providing security speedily is the aim of this investigation, Relational databases are very important in satisfying today's infirmation needs. This investigation provides a method to provide security by using encryption algorithm which is alone sufficient to protect the same.

Keywords- Encryption, Security, Cryptography, Decryption.

I. INTRODUCTION

Security is becoming one of the most urgent challenges in database research and industry, and the challenge is growing due to the enormous popularity of e-business. Nowadays the use of internet in society for various purposes including information distribution is familiar worldwide Data transmitted over the Internet passes through many servers and/or routers and there are many opportunities for outsiders to interrupt that transmission.

Preventing interception is impossible instead; the data must be made unreadable (encrypted) during transmission, with a way for the intended receiver to be able to transform the received transmission back to its readable form (decryption process). When a message is encrypted, that means that it is transformed into a form when the data is passed through some substitute technique shifting technique mathematical operations and All those processes generate a different form of that data and that is not readable The encryption process will be applied to a particular message, and matching keys must be used to encrypt and decrypt. When a message is decrypted, it is returned to its original readable form.

The goal of encryption is to make data unintelligible to unauthorized readers and very difficult to decipher when attacked. Encryption refers to the practice of confusing the meaning of a piece of information by encoding it. The encoding of data is to prevent unauthorized parties from viewing or modifying it. Encryption can also be used to provide high levels of security to network communication, e-mail files stored on hard drives or floppy disks and other information that requires protection.

II. RELATED WORKS

An easy way to comply with the conference paper formatting requirements is to use this document as a template and simply type your text into it.

Fernando Perez Gonzalez and Juan R.Hernandez, proposed a mechanism that was resilient or insensitive to additive attacks, to embed and detect watermark in relational database. In additive attack the attacker simply inserts his/her own watermark in original data in their proposed system they can draw graphs and original ownership claim can be resolved by locating the overlapping regions of the two watermarks in which the hit values of the marks conflict and determining which owner's mark win. (1999).

Agrawal proposed a watermarking algorithm that embeds the watermark bits in the least significant bits (ISB) of selected attributes of a selected subset of tuples. This technique does not provide a mechanism for multibit watermarks instead only a secret key is used. For each tuple, a secure message authenticated code (MAC) is computed using the secret key and the tuples primary key.

The computed MAC is used to select candidate tuples. Attributes and the LSB position in the selected attributes. Hiding bits in LSB is efficient. However, the watermark can be easily compromised by very trivial attacks.(2002)

M Atallah and S. Lonardi proposed a system, in which a simple variation on the classic 17-77 algorithm that allows one to hide within the compressed document enough information to warrant its authenticity and integrity. The design is based on the unpredictability of a certain class of pseudo-random number generators, in such a way that the hidden data cannot be retrieved in a reasonable amount of time by an attacker (unless the secret bit-string key is known (2003)

Gross-Amblard proposed a watermarking technique for XML documents and theoretically investigates links between query result preservation and acceptable watermarking alterations. Another interesting related research effort is to be found in where the authors have proposed a fragile watermark technique to detect and localize alterations made to a database relation with categorical attributes (2003).

Radu Sion proposed a watermarking technique that embeds watermark bits in the data statistics. The data partitioning technique used is based on the use of special marker tuples which makes it vulnerable to watermark synchronization errors resulting from tuple deletion and tuple insertion; thus such technique is not resilient to deletion and insertion attacks.

Furthermore, R. Sion recommends storing the marker tuples to enable the decoder to accurately reconstruct the underlying partitions: however this violates the blinded watermark detection property. The data manipulation technique used to change the data statistics does not systematically investigate the feasible region instead naive unstructured technique is used which does not make use of the feasible alterations that could be performed on the data without affecting itsusability. (2004).

Wilfred Ng and Ho-Lam Lau "Effective Approaches for Watermarking XMI Data Presented two different watermarking schemes on XML. Data: the selective approach and the compression approach. The former technique embedded non destructive hidden information content over XMI data. The latter takes verbosity and the need in updating XML data in real life into account. We conduct experiments on the efficiency and robustness of both approaches against different forms of attack, which shows that our proposed watermarking schemes are reasonably efficient and effective (2005)

Yingjin La Vipin Swarup, and Sushil Jajodia presented a technique for fingerprinting relational data by extending Agrawal watermarking scheme. The primary new capability provided by their scheme is under reasonable assumptions; it can embed and detect arbitrary bit-string marks in relations. This capability, which is not provided by prior techniques, permits their scheme to be used as a fingerprinting scheme and then presented quantitative models of the robustness properties of our scheme.

These models demonstrate that fingerprints embedded by our scheme are detectable and robust against a wide variety of attacks including collusion attacks (2005).

Ms. Arti Deshpande und Mr. Jay ant Gadget presented a mechanism that is resilient or insensitive to additive attacks, how to embed and detect watermark in relational database. In additive attack the attacker simply inserts his own watermark in original data. In their proposed system one can draw graphs and original ownership claim can be resolved by locating the overlapping regions of the two watermarks in which the hit values of the murks conflict and determining which owner's mark win. The attacker must have inserted the watermark later. Clearly having more marked tuples increases collisions and hence we can easily identify the owner of the data (2009).

Nagarjuna. Seitipalli, R Manjula proposed a paper Databases Watermarking Relational Optimization Based Techniques According to him in earlier existing systems the relational data will be watermarked and directly send to the client system, in these systems while sending relational data from server to client attacker casily copy the data and create same copy of relational data.

Here there is no security to watermarked relational data In their proposed system before sending the watermarked relational data to client side he encrypted the relational data and send it to the client side, at client side decryption will be done to get the original watermarked Data Because of using this encryption technique even an attacker copy the data he she may not read the watermarked relational data (2011) But the problem with

the above paper is that two techniques were used to provide security to the relational database that is watermarking and encryption algorithm And the encryption algorithm used in their approach was based on serialization which can be easily decrypted. So to overcome this limitation our paper uses the approach for providing security which is alone sufficient to protect the data and also the concept of key generation and then cipher text generation and then padding of the cipher text with hexadecimal digits makes the encrypted data very difficult to get decrypt.

Abhi Tamrakar and Vinti developed an approach for compression of non oracle database with the table compression algorithm of oracle 11g. but that approach does not provide security to the relational database whose limitation is compensated in the approach used in this paper. Abba Tamrakar and Vinti also presented another paper that deals about that provides a method to provide security by using encryption algorithm which is alone sufficient to protect the relational database.

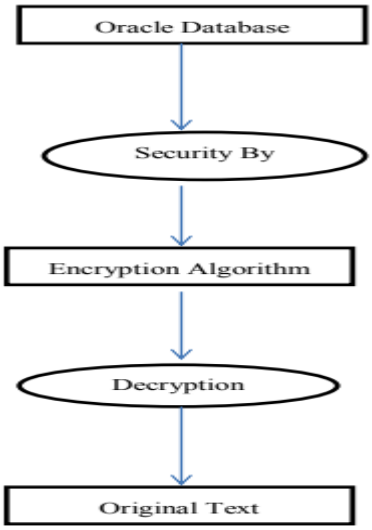

Fig 1. Block Diagram of Proposed Encryption and Decryption Process.

III. ENCRYPTION ALGORITHM

This algorithm is original text is converted into cipher text by using encryption algorithm with help of some secrete key, then cipher text again converted into plaintext using decryption algorithm with help of same secrete key, so finally get the original information.

- Create a relational table in oracle database
- Select the username and the table name to which one wants to provide security
- 3 .Selected table, will be converted into flat file for encryption
- Apply the encryption algorithm on the selected table.

1. The Steps of Encryption Algorithm are as Follows:

- With the file and the secret key as input to the encrypt function a key is generated.
- That key with the input file, cipher text file is generated
- Cipher text file's words are padded with the hexadecimal digit tocomplete the encryption process.
- Apply the decryption algorithm which is just reverse of encryption to get the original table.

IV. PROCESS OF PROVIDING SECURITY

The aim of this paper is to come up with a technique to hide the data in a text file, audio file, video file and image file in such a way such that there are no perceivable changes in the audio file after the message insertion. At the same time if the message that is to be hidden is also encrypted, then the level of security would be further raised to a more satisfactory level. Now, even if the hidden message is to be discovered, the person who gets the message would only have the encrypted form of the message with no way of decrypting it.

To secure the data using encryption algorithm and again retrieve the original data using decryption algorithm. In this investigation the variety of information can be used such text, audio, video and image.

1. Text:

First this investigation deals about text information, getting the text input and generate a key for this text input. Then, using encryption algorithm to encrypt the text which change the original text data into cipher text. This encryption done for to hide the data. Then the decryption process is started. Again cipher text is converted into original text using decryption algorithm. The given key must be same as the generated key. Then only retrieve the original text. This encryption and decryption helps to secure the information form the hackers. This investigation based on cryptography.

Fig 2. Text.

2. Image:
In today's world it is acrucial concern that while transfer image from one network to another network over the internet, the proper encryption and decryption should be applied so that unauthorized access can be prevented.The algorithms must support color image data with logical key. It can be applied on Network Communication for sending encrypted images. So it can be useful in the military services. Getting the image input and generate a key for this image input. Then, using encryption algorithm to encrypt the image which converted the original image data into cipher image. The image must be in .jpg file format.

Fig 3. Text.

3. Audio:
Audio file it can be attack by the any unauthorized person so that to avoid the problem before to encrypt the audio file and generating byte code using encryption algorithm. Then apply decryption algorithm to get into original audio using same key. It is more secure. The audio must be in .wmv file format.

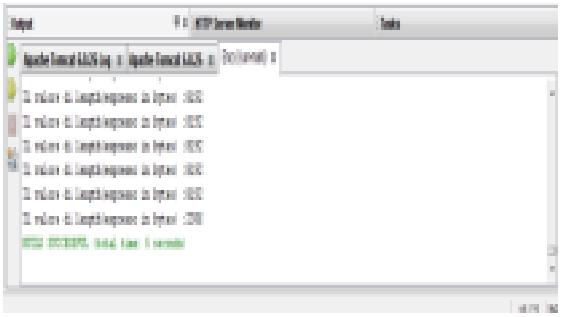

Fig 4. Image.

4. Video:
Audio file it can be attack by the any unauthorized person so that to avoid the problem before to encrypt the audiofile and generating byte code using encryption algorithm. Then apply decryption algorithm to get into original audio using same key. It is more secure. The given key must be same as the generated key. Then only retrieve the original audio. This encryption and decryption helps to secure the information from the hackers.

Fig 5. Video.

IV. CONCLUSION

Now a day, securing the precious information that is very tedious task. So that, using encryption algorithm to overcome this problem. This encryption algorithm which hides the text information, videos, audios, and image it makes the information in the more secure. Security is becoming one of the most urgent challenges in database research and industry, and the challenge is growing due to the enormous popularityof e-business. Such a way, using decryption algorithm to recover, the original information that are hidden.

In proposed system deals about two concepts such as encryption and decryption. Cryptography method is used for this investigation. Thus, encryption and decryption help in secure transmission of the message and in protecting the message from unauthorized persons. This system provides highly reliable, more securable, good, efficient method for hiding the information from the unauthorized persons.

A given 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. This investigation will allow authorized person to view the data who knows the secrete key so unauthorized persons will be restricted to some extent.

REFERENCES

[1] A. Tamara, V. Nanda,"A Compression Algorithm for Optimization of Storage Consumption of Non Oracle Database". (Waiting for Publication).
[2] N.Settipalli, R Manjula, Securing Watermarked-Relational Data by Using Encryption and Decryption" ARPN Journal Vol. 1, pp. 70-74, May 2011.
[3] A. Deshpande, J. Gadget, "New Watermarking Technique for Relational Databases." Department of Computer

[4] Engineering, Thadomal Shahani Engineering College, Mumbai, ICETET-2009.
[5] Y. Li, V. Swarup, and S. Jodie, "Fingerprinting Relational Databases: Schemes and Specialties." Vol. no. 2, pp. 456- 460, March 2005.
[6] 5. W. Ng and H. Lau, "Effective Approaches for Watermarking XML Data." Department of Computer Science, the Hong Kong University of Science and Technology, Hong Kong, 2005**.**
[7] 6. R. Sion, M. Atallah, and S.Prabhkar, "Right Protection for Relational Data." IEEE Trans. Knowledge and Data Engineering, Vol. 16 no.6, June 2004.
[8] D. Gross-Amblard, "Query-Preserving Watermarking of Relational Databases and XML Documents." In PODS „03: Proceedings of the 22nd ACM SIGMOD-SIGACT SIGART Symposium on Principles of Database Systems, pp. 191-201. ACM Press, 2003.
[9] 8. M. Atallah and S. Lonardi. "Authentication of LZ-77 Compressed Data." In Proceedings of the ACM Symposium on Applied Computing, Florida, USA, 2003.
[10] R. Agrawal, J. Kiernan, "Watermarking Relational Databases." IBM Almaden Research Center, china, 2002.