Available online at www.qu.edu.iq/journalcm
JOURNAL OF AL-QADISIYAH FOR COMPUTER SCIENCE AND MATHEMATICS
ISSN:2521-3504(online) ISSN:2074-0204(print)

Comparative study on encrypted database techniques

Atheer Metaab Abbas[a*], Abdul Monem S. Rahma[b], Nidaa F .Hassan[c]

[a,b,c] Department of Computer Science, University of Technology, Baghdad, Iraq

[a]*Email: etheer_78@yahoo.com*

ARTICLE INFO

Article history:
Received: 27 /08/2020
Revised form: 09/ 09/2020
Accepted : 16 /09/2020
Available online:17/11/2020

Keywords:

Encrypted Database; Techniques; Security; Encryption; Performance; breaches.

ABSTRACT

Protecting data is the core of many secure systems and many users depend on a database management system (DBMS) to manage the protection. Databases are essential to many business and government organizations, holding data that reflect the organization's core competencies. Database encryption refers to the use of encryption techniques to transform a plain text database into a encrypted database, thus making it unreadable to anyone except those who possess the knowledge of the encryption key(s). Encryption is becoming the last line of defense in database management system(DBMS)security. There is the essentiality of algorithms which are protected from intruder as well as maintain the performance of the system. Therefore, this paper presents most of the recent works that have been conducted on encrypted database techniques and analyzes them to clarify the pros and cons points in each related work. This paper has focused on previous studies for both symmetric and asymmetric encryption techniques. However, they missed to show some numerical analysis that would help readers to deeply understand the difference among different techniques.

MSC : 30C45 , 30C50

DOI : https://doi.org/10.29304/jqcm.2020.12.3.710

1. Introduction

Data Base Management System (DBMS) can be defined as data collection in addition to collection of programs for accessing such data. The database includes certain information related to an organization. The main aim of DBMSs is providing an approach for storing and retrieving database information which is simple and effective. The encryption process in the database systems is considered to be an area of high importance, since protected and effective algorithms

∗Corresponding author : **Atheer Metaab Abbas , Abdul Monem S. Rahma , Nidaa F. Hassan**
Email addresses: ***etheer_78@yahoo.com***
Communicated by : **Alaa Hussein Hamadi**

are vital because they offer the capability of querying over the encrypted databases as well as allowing enhanced encryption and decryption of the data [1] [2].

1.1 **Database system Applications :**

- **Finance:** To hold certain information related to holding sales, purchasing stocks and bonds
- **Credit card transaction:** Purchasing on credit cards
- **Human resources:** Information related to paychecks, salary, and employees
- **Banking:** Information related to customer information such as bank transactions and account loans.
- **Airlines:** Used for schedule information and for reservations.
- **Universities:** Used for information related to students, such as grades and course registration.
- **Telecommunications:** To maintain the balance on prepaid calling cards as well as keep records on the calls.

A lot of organizations consider the database as very important due to the fact that it has sensitive information of data that range from the private competitive information and personal details of customers to intellectual properties. Stolen or lost data, particularly data of customers, might cause serious fines, competitive disadvantages as well as brand damage. With regard to high-profile conditions, the data that is compromised present the organization with long-term customer acquisitions as well as retention difficulty. Thus, in recent IT world, securing the database is a major domain. However, there are certain drawbacks related to some conventional techniques of database security like application security and firewalls were exposed recently and it has been indicated that such methods of securing databases are not effective anymore for protecting data and businesses in the recent complex and open IT environments. In an attempt of mitigating the risks of security breaches as well as for complying with a lot of present and advancing regulations, database encryption is regularly indicated as the solution. Encryption regularly indicated as the optimum defense against breaches related to the database security.

2. Encryption

The process of encryption involves the transformation of data or information to unreadable texts through the use of encryption and decryption key, that might not be simply detected via intruders or unauthorized readers. Therefore, the encryption process is defined as the translation of the original data or text (called plain-text) to encrypted data or text (cipher-text). At the same time, decryption can be defined as the process used to take the cipher-text and take it back to the original form. Therefore, the decryption process indicates the translation of encrypted data or text (cipher-text) to the original data or text (plain-text) [3].

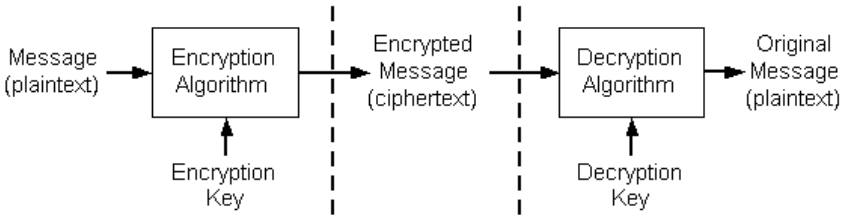

Fig 1 : Encryption and Decryption [3].

2.1 Why data encryption

The main reasons for using the methods of encryptions are protecting the data from theft, fraud, as well as protecting the data from loss and maintaining confidentiality [4].

2.2 Types of encryption

2.2.1 Asymmetric encryption: this type of encryption involves using 2 distinctive keys to secure the data from cryptanalysis. Such keys consist of a public key that can be encrypted by other users in addition to private key that is decrypted via the owner [5]. Such encryption type is considered to be unusable in the presented study since it requires overhead and extra time. Figure 2 displays an example related to the asymmetric encryption algorithm.

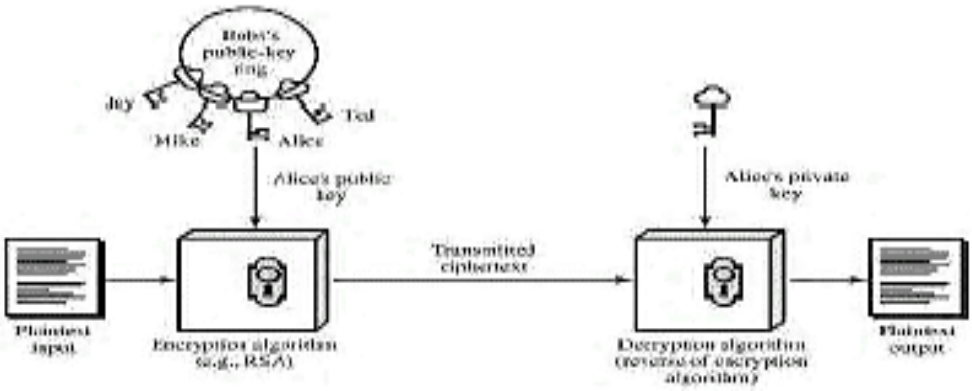

Fig 2 : Asymmetric Encryption algorithm [5].

2.2.2 Symmetric encryption: It offers a general approach for storage as well as for data transmission, also it includes secret communication through the use of single-key encryption. The main 5 elements of symmetric encryption are: plaintext, encryption algorithm, secret key cipher text and decryption algorithm [5]. Figure 3 show example related to symmetric encryption algorithm.

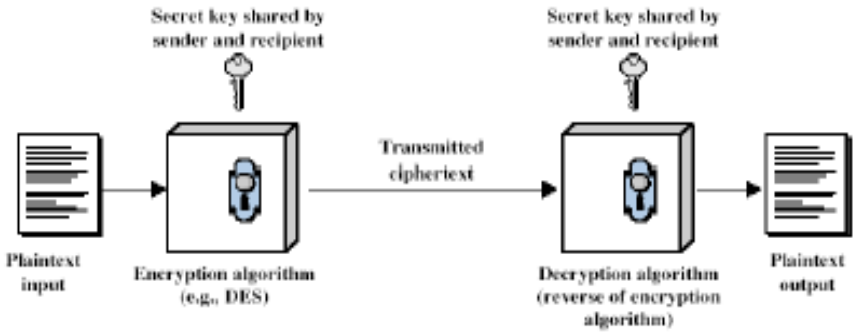

Fig 3 : Asymmetric Encryption algorithm [5].

Symmetric algorithm is considered to be faster in comparison to public key encryption methods in hundred or thousand times, at the same time, each time encryption process is applied, there will be 2 generated distinctive keys, the safety regarding private key storage can be considered as difficult to ensure in the approaches of public key. With regard to database encryption, the keys number is going to be very large. Typically, it is not practical to use the public key encryption methods for database encryption [6].

3. Previous works of Encrypted Database Techniques

The criteria regarded to encrypting databases for protecting them against attacks has been provided via a lot of studies. George et al. [7] indicated a scheme for database encryption with sub-keys according to Chinese Reminder theorem which enable field's encryption and decryption in record. Samba et al. [8] suggested a scheme for database encryption which offer highest maximum security, while limit the added time cost regarding the encryption process and decryption process and thus, increase the system's performance. Data Encryption Standard (DES) is the used encryption approach, for reducing the time spent on the processes of encryption and decryption, the method is going to divide the database to non-sensitive and sensitive data. The non-sensitive data will form bulk of databases which are stored in clear form for the purpose of easing their rapid retrieval while the sensitive data will be stored in encrypted form, their process of decryption is considered to be rapid, since just single key is required for decrypting the whole column of the encrypted classified data. Ayman et al. [9] suggested new encryption algorithm referred to as Reverse Encryption Algorithm (REA). The suggested algorithm is uncomplicated, yet it results in cipher. Strong security has been achieved by this algorithm, also it is fast for the majority of Data base (DB) applications and it limits the added time cost for the processes of encryption and decryption for the purpose of not degrading the database system's performance.

The results related to the experiments in the study has indicated that the encryption and decryption time related to the REA has optimum performance in comparison to the other algorithms of encryption such as (Blowfish, Ron's Code (RC2), DES, Advanced Encryption Standard (AES), 3DES). Yet, this approach not used in distributed database. Prabhsimran et al. [10] Proposed a database encryption scheme used three ways to encryption database, first way

applied encryption algorithms (RC2, AES128, AES 256, and DES) to encryption all data in database, second way used hashing to convert into encryption form (hash value) this ways not used to encrypted database because not back the data but used to encrypt username and password to login database, third used hybrid approach by using Rivest Shamir Adleman (RSA) and International Data Encryption Algorithm (IDEA) which are public key and symmetric key respectively. In this method the keys first encrypted through the use of RSA algorithm and after that such keys applied for encrypting the plain-text via the use of IDEA algorithm. Such method improves the data security via making it hard to break. Adeem et al. [11] presented a new database encryption scheme using Enhanced Simplified Data encryption standard(E-SDES) algorithm. The security related to the S-DES has been enhanced, also the shift row and transposition approaches have been added before S-DES algorithm carry out its process. Developed S-DES can improve security, that is of high importance in Database encryption and communication. In the case when shift tow and transposition are utilized prior to main S-DES, then the intruders will initially break the main S-DES and after that shift row and transposition are used. Thus, security is dual and contrasted with a simple S-DES algorithm. Hariharan et al. [12] proposed a novel, fast and secure database encryption schema for indexing in Column-Oriented DBMS. It Presents a new column-oriented encryption which encrypt just certain columns in order than the sensitive data will be chosen for encryption and therefore the encryption and decryption time will be decreased. It ensures fast indexing operations. This study deal with 2 main issues: The first one is the security for encryption. The second one is related to rapid performance regarding the query on a database. In this approach, Block cipher will be utilized for encrypting tiny bytes (byte by byte), unlike, other block ciphers which are encrypting unit of at least 8 bytes. J. Raja et al. [13] presented a new symmetric database encryption method named Enhanced Transposition-Substitution-Folding-Shifting encryption algorithm (ETSFS). The main aim of this study is enhancing TSFS and thus providing higher security to database while decreasing added time cost for the processes of encryption and decryption via encrypting the sensitive data for increasing the DB system's performance. There are 4 methods of transformations used in ETSFS (transposition, substitution, folding, and shifting), also it has the ability of encrypting data which include alphabetic characters (A-Z), all then numbers as well as these symbols: (*, -, ., /, :, @ and _). The experimental results indicated that improved TSFS encryption algorithm is superior to AES and DES with regard to database added size and query execution time.

4. Analysis of related work

As previous study, many researchers work on encrypted of database based on techniques of encrypted databases which can be summarized in following table.

Table (1): pros and cons of Pervious Works

Reference	Methodology	Pros	Cons
[7]	Database encryption schema with subkeys.	Error propagation regarding the block ciphers.	The scheme's security cannot be verified.
[8]	Database encryption schema by using (DES)	Provide highest security, while reducing added time cost related to the processes of encryption and decryption	Queries like counts, averages, sums, as well as other statistical functions which are aggregating across the data in database cannot be achieved directly.
[9]	Database encryption schema by using (REA)	Provides a strong security and it is rapid for the majority of DB applications, increase the DB system's performance	It is not used in distributed database
[10]	Hybrid database encryption schema	More Security via using two encryption algorithms, also it cannot be easily broken	More computations regarding the processes of encryption and decryption.
[11]	Database encryption schema by using Enhanced S-DES algorithm	Security is approximately dual	High complexity
[12]	Database encryption schema by using column oriented encryption.	Simple, Fast and Secure.	It creates problems on straightforward attacks.
[13]	Asymmetric database encryption method (ETSFS) algorithm	Provides small space, maximum security, while reducing the added time cost regarding the processes of encryption and decryption	Balance between complexity and time not found

5. conclusion

This paper presents most of the recent works that have been conducted in Techniques of Encrypted Database and analyzes them to clarify the cons and pros points in each work separately based on set of encryption techniques. Some of them, like paper [9] provide high security but cannot use in distributed database and others like paper [12] and paper [13] provide fast and strong security but don't create a balance between time and complexity also, it creates problems on straightforward attacks. Some of them, developing a methods that are directly deals

with the encrypted data without decrypting them but they have set of issues. In order to satisfy balance between time and complexity in Techniques of Encrypted Database , a novel proposal must be suggested to achieve high security and performance in encryption and time of Query on encrypted database techniques.

References

1. Hacigumus, H., Iyer B., and Mehrotra, S., "Providing database as a service" in Proceedings of ICDE, (2002), pp. 29–38.
2. Pfleeger, C. and Pfleeger, S., "Security in Computing", third edition. (2004).
3. Arasu, A., "Querying encrypted data", Proceedings of the ACM SIGMOD International Conference on Management of Data, June 22-27, ACM Press, New York, USA, (2014). pp: 1559-1261.
4. Baba, A. M., Yusuf, A., Ahmad, A., and Maijama'a, "Performance Analysis of the Encryption Algorithms as Solution to Cloud Database Security" International Journal of Computer Applications (0975 – 8887) Vol. 99 , No.14, (2014).
5. Stallings, W., "Computer security: principles and practice", Upper Saddle River, N.J.: Pearson Prentice Hall, (2008).
6. Tingjian, G. and Zdonik, S., "Fast, Secure encryption for indexing in a column-oriented DBMS, " IEEE 23rd International Conference on Data Engineering, (2007), pp. 676-685.
7. David, G., "A Database Encryption System with Subkeys " , ACM Transactions on Database Systems, Vol.6, No.20, (1981).
8. Sesay, S., "A Secure Database Encryption Scheme". Second IEEE consumer Communications and Networking Conference, (2005).
9. Mousa, A., "Security Analysis of Reverse Encryption Algorithm for Databases", International Journal of Computer Applications (0975 – 8887) Vol. 66, No.14, (2013).
10. Singh, P. and Kaur, K., "Database security using Encryption", International conference on futuristic trend in computational analysis and Knowledge management (ABLAZE), (2015).
11. Akhtar, A. "Enhancing the Security of Simplified DES Algorithm Using Transposition and Shift Rows". International Journal of Computer Science and Software Engineering 6.5, (2017).
12. Hariharan, P., " Various Schemes for Database Encryption - A Survey", International Journal of Applied Engineering Research ISSN 0973-4562 Vol. 12, No. 19, (2017).
13. Raja, J., "Database Encryption Using TSFS Algorithm", International Journal of Scientific Research in Computer Science, Engineering and Information Technology ©IJSRCSEIT, Vol. 4, No. 2, (2018).