



“Database Security Using Encryption”

Technical Writing and Seminar I

MCS15

MASTER OF TECHNOLOGY

In

Computer Science and Engineering

Name of the Student: Ashraf Ali S

USN: 1MS18SCS03

Under the guidance of

DR. MOHANA KUMAR S

Associate Professor

Department of Computer Science & Engineering

RAMAIAH INSTITUTE OF TECHNOLOGY

(An Autonomous Institute affiliated to VTU)
MSR Nagar, MSRIT Post, Bangalore – 560054

www.msrit.edu

2018-19



RAMAIAH INSTITUTE OF TECHNOLOGY

(Autonomous Institute, Affiliated to VTU)

MSR Nagar, MSRIT Post, Bangalore – 560054

CERTIFICATE

This is certified that the technical seminar work entitled “Database Security Using Encryption” is carried out by ASHRAF ALI S 1MS18SCS03, a bonafide students of M. S. Ramaiah Institute of Technology, Bangalore in partial fulfillment for the award of TECHNICAL SEMINAR-I MCS15 during the year 2018-19. It is certified that all corrections/suggestions indicated for Internal Assessment have been incorporated in the Report deposited in the department library. The seminar report has been approved as it satisfies the academic requirements in respect of technical seminar work prescribed for the Degree.

Signature of the Guide

External Viva

Name of the examiners Signature with date

1

2.

DECLARATION

I ASHRAF ALI S student of Master of Technology in Computer Science and Engineering Ramaiah Institute of Technology, Bangalore hereby declare that the Technical Seminar entitled “*Database Security Using Database*” has been carried out independently at the Institute under the Guidance of Dr. Mohana Kumar S, Associate Professor Computer Science and Engineering Department Ramaiah Institute of Technology

I hereby declare that work submitted in this thesis is my own, except where acknowledge in the text and has not been previously submitted for any other evaluation.

Signature of Student

Place: Bangalore

Name of Student: ASHRAF ALI S

Date: 24-01-2019

USN: 1MS18SCS03

Database Security Using Encryption

Abstract:

Security of Data is the most important task in today's world. Over the years various encryption schemes have been developed in order to protect the database from various attacks by the intruders. This paper discusses the importance of database encryption and makes an in-depth review of various database encryption techniques and compare them on basis of their merits and demerits.

The need to protect the database is growing especially in this age of e-commerce. Many conventional database security systems are bugged with holes that can be used by attackers to penetrate the database. No matter what degree of security is put in place, sensitive data in database are still vulnerable to attack. To avoid the risk posed by this threat, database encryption has been recommended. However, encrypting all of database item greatly degrades the performance of the database system. As an optimal solution this paper presents a database encryption scheme that provides maximum security, whilst limiting the added time cost of encryption and decryption.

A key way to protect the data within one's database is to use database encryption. Data encryption can be done at many different points in the application depending on the goal that one is trying to meet. It is important that there are so many options as to how one can encrypt the database. However, encrypting all of database item greatly degrades the performance of the database system. As an optimal solution this paper presents a database encryption scheme that provides maximum security, whilst limiting the added time cost of encryption and decryption.

Table of Contents:

Declaration	I
Abstract	II
List of Figures	III
List of Tables	IV
1. Introduction	1
2. Need of Encryption	2
3. Database Encryption	3
3.1 Encryption	4
3.2 Hashing	5
4 Literature Survey	7
4.1 A Standard Encryption Approach	7
4.2 Hybrid Approach	10
4.3 Hashing Approach	10
5 Results and Findings	11
6 Conclusion	13
7 References	14

List of Figures

1. Intruder accessing the content of Database	3
2. Database Encryption and Decryption Process	4
3. Working of Encryption Process	5
4. Working of Hashing Process	6
5. Comparison of FCE with DES and Plain Text	9
6. Flowchart of 3KDEC Algorithm	10

List of Tables

1. Database in Normal Form	7
2. Database in Encrypted Form	7
3. Database Table using MD5 Hash Function	11
4. Compare various Database Encryption Research Paper	12-13

1. INTRODUCTION

In this age of technology, all our work is being done by the computers. From chatting with friends on social networking websites, to making online payments through Net Banking, everything is being done online through computers. Since these facilities are efficient and make our work easy, we use them in one way or the other. This means to use the se online services we are storing all our personal and sensitive data in the databases of these websites and applications, which indeed make this data prone to various security threats. So, protection of this important user data is one of the major priorities, in order to avoid any misuse of data.

Authorization and Authentication are two major processes that are used to protect the data from the frontend (i.e. User Side) that is being accessed by the user, where authorization means whether a person has the rights to access the data or not, while authentication means identifying the user which is generally done by the use of username/password [1].

Another important way of protecting this data is by encrypting the data being saved in the databases of these websites. In this paper we will discuss the various database encryption schemes proposed by different authors, and also study their merits and demerits of these schemes.

2. WHAT IS THE NEED OF ENCRYPTING THE DATA

The need of encrypting the data before saving it in a database is that by restricting the access through authorization and authentication of data can help to a certain limit, but what if the intruder somehow gets to the database. He has all the data of database and can misuse it as he likes, here encryption of data before saving it in database comes into play. If the data is encrypted before saving it in the database, even with access to the database the intruder cannot misuse this data. Fig 1, show how the intruder can access the contents of database.

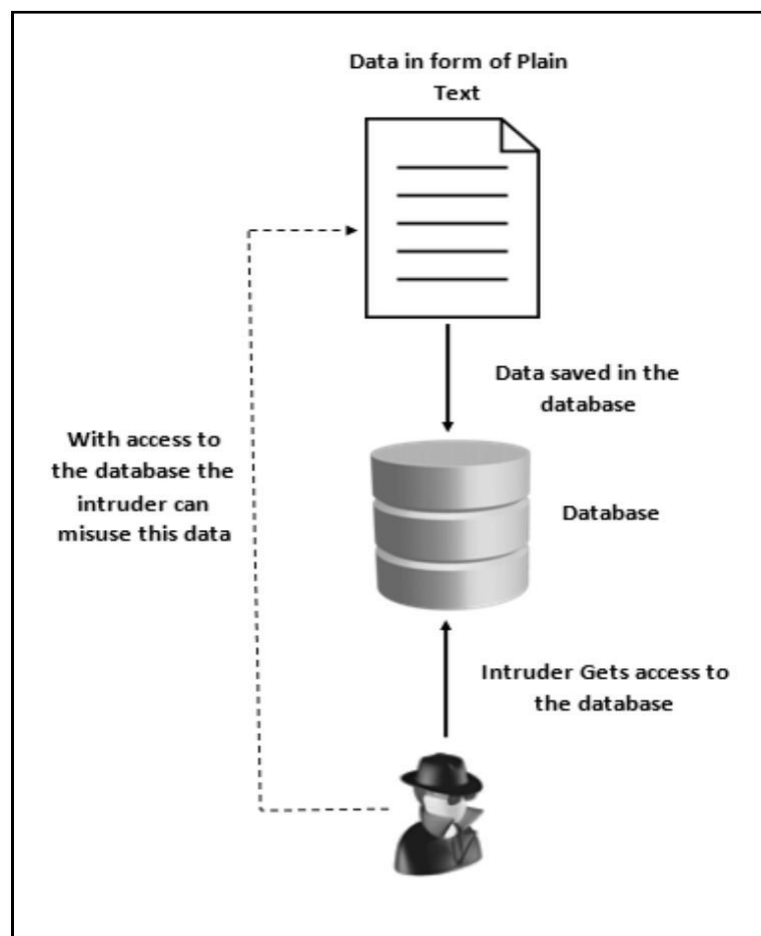


Fig.1. Intruder accessing the contents of Database

3. DATABASE ENCRYPTION

Database Encryption is a process of encrypting the data in the database [2]. It is a key strategy to protect the contents of data within the database. The main idea behind this is that in case the intruder somehow is able to get to the database of the system; due to encryption he should not be able to misuse the data in the database.

Figure 2, shows basic working of the Database encryption and decryption process. The plain text/data to be saved in the database is first converted into cipher text using an appropriate algorithm and a specific key. Then this cipher text is saved into the database. When the user wants to extract the data from the database, the cipher text is converted back to plain text using the decryption algorithm and the same key used in encryption. This will return the plain text to the user, when requested.

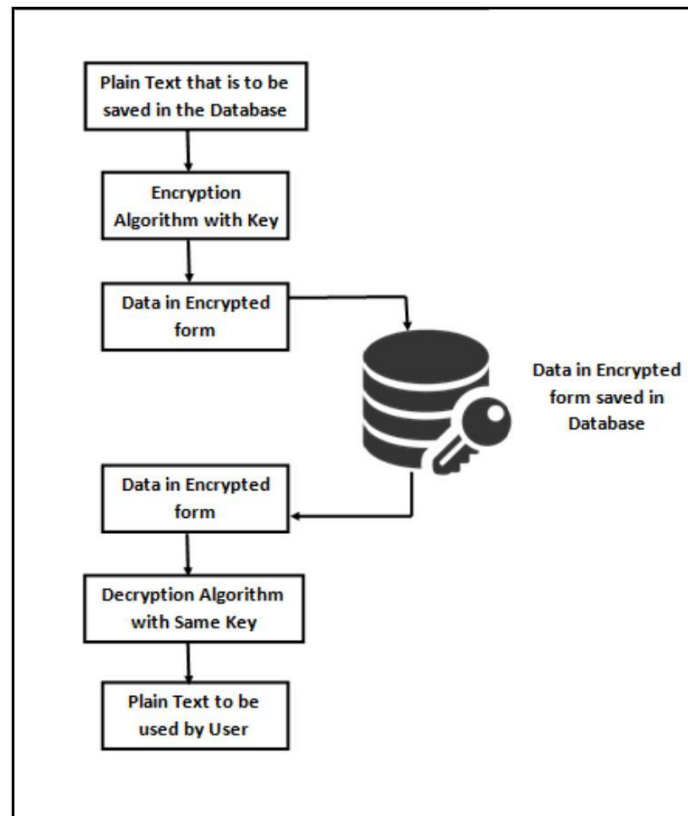


Fig.2. Database Encryption and Decryption Process

Database Encryption can be done in two possible ways [2]:

3.1 ENCRYPTION

It is a process in which plain text is converted to cipher text with help of key, and then using the same key we can decrypt the cipher text back to plain text [3]. Encryption is performed using various algorithms, with each algorithm having his own advantages and disadvantages. Most commonly used encryption algorithms are DES, RC2, AES_128, AES_256 etc. Figure 3, shows working of simple encryption process.

The primary purpose of encryption is to protect the confidentiality of digital data stored on computer systems or transmitted via the internet or any other computer network. A number of organizations and standards bodies either recommend or require sensitive data to be encrypted in order to prevent unauthorized third parties or threat actors from accessing the data. For example, the Payment Card Industry Data Security Standard requires merchants to encrypt customers' payment card data when it is both stored at rest and transmitted across public networks.

Some applications tout the use of end-to-end encryption (E2EE) to guarantee data being sent between two parties cannot be viewed by an attacker that intercepts the communication channel.

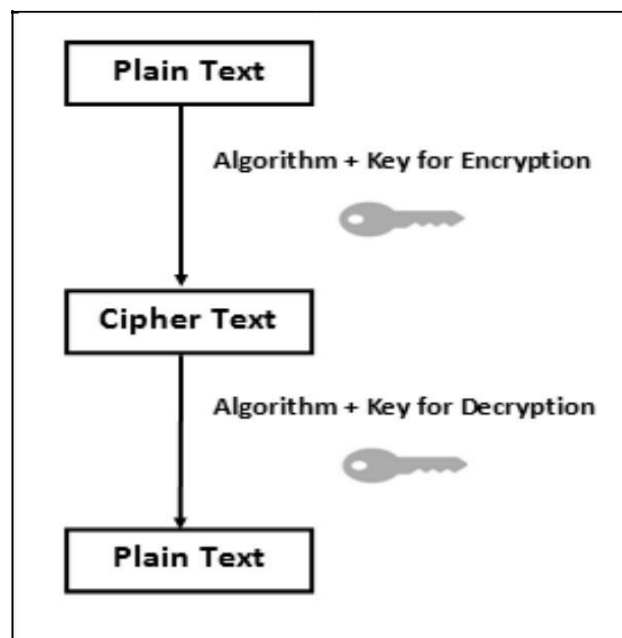


Fig. 3. Working of Encryption Process [3]

3.2 HASHING

It is a one-way process, in which plain text is converted into hashed value (encrypted form). Once the data is hashed using a Hash Function it cannot be changed back to plain Text [3]. Generally, this approach is used for password encryption, whenever we need to login the password entered is encrypted using hash function and then matched with the password stored in the database which is already in encrypted form, if both matches the user get access else it gets the message of invalid username/password. Most commonly used Hash Functions are MD4, MD5, SHA, SHA-1 etc. Figure 4, shows working of hashing.

The hashing algorithm is called the *hash function*-- probably the term is derived from the idea that the resulting hash value can be thought of as a "mixed up" version of the represented value.

hashing is also used to encrypt and decrypt digital signatures (used to authenticate message senders and receivers). The digital signature is transformed with the hash function and then both the hashed value (known as a message-digest) and the signature are sent in separate transmissions to the receiver. Using the same hash function as the sender, the receiver derives a message-digest from the signature and compares it with the message-digest it also received.

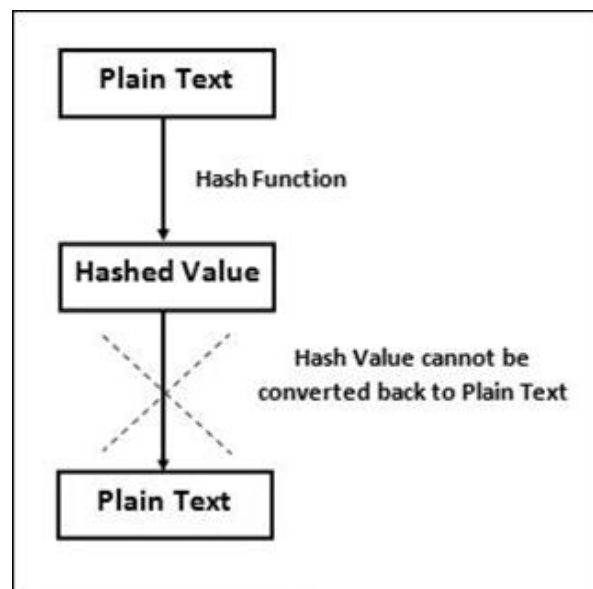


Fig. 4. Working of Hashing Process [3]

Table 1 and 2 shows database in normal and encrypted form. In Table 2, the contents in the database cannot be understood, so it becomes almost impossible for the intruder/hacker to misuse this data.

An encryption algorithm changes information into incomprehensible characters through a mathematical process. While other security tools protect a system from intrusion or attack, encryption is a fundamental form of defence that deals with security of the data itself. This means that even in the event of a system breach, compromised data is still only readable by authorized users in possession of the right encryption keys.

For encrypted tables, each table page is encrypted when written to the disk, and is decrypted when read in from the disk. This process is invisible to applications. However, there may be a slight negative impact on performance when reading from, or writing to, encrypted tables. Encrypting or decrypting existing tables can take a long time, depending on the size of the table. Encrypting tables does not impact storage requirements.

Table 1, Database in Normal Form

ID	Email_Id	Password
1	abc@gmail.com	abc@pwd
2	def@gmail.com	def@pwd
3	ghi@gmail.com	ghi@pwd

Table 2, Database in Encrypted Form

ID	Email_Id	Password
1	3F009D72559F51E7E454B16E 5D0687A1	26184EC4EBCA487B5479AF00 89371E6B
2	5EDBC06C5A81FD1EAA480212 D5F278F5	56F0F7BCD13F9A6FE1362190 3D911DA5
3	B62882E7D610B4DDB86FA3AC 9AB5F8D1	E608BE034CE09BE0B9FD1B03 064584A2

4 LITERATURE SURVEY

All the work done by various researchers and authors can be broadly classified into 3 main categories; standalone encryption approaches, hybrid approaches and hashing.

4.1 STANDALONE ENCRYPTION APPROACHES

Samba Sesay, et al [4], discuss the importance of database security in activities like E-Commerce and Enterprise Resource Planning (ERP). They also discuss the various loopholes that attackers use to access the database. Finally, they proposed a system for database encryption which minimizes the time cost of encryption and decryption process, while covering all aspect of security like confidentiality, access control, integrity, authentication and non-repudiation. Although their system possesses various advantages but also suffer a major disadvantage that queries like sum, average and counts cannot be performed directly.

Min-Shiang Hwang and Wei-Pang Yang [5], proposed a 2-way encryption scheme based on the concept of one-way function and subkeys that ensures full security; moreover 2 additional algorithms were given that efficiently handles a of key management problem. They also compared their proposed scheme with the schemes of GI Davida, et al [6] and Lin, et al [7,8] on the parameters like storage space, number of keys etc. The result of the comparison shows that the 2-way encryption scheme is clearly the best among the three.

T. Ge and S. Zdonik [9], gave a new encryption algorithm Fast Comparison Encryption (FCE) for data warehouses. This algorithm was clearly better than tradition Data Encryption Standard (DES) in terms of low decryption overheads which makes it really efficient for encryption of large databases. The results of the comparison are shown in figure 5, where FCE-1 and FCE-2 are 2 different versions of Fast Comparison Encryption (FCE). However, S. Jacob [10], performed cryptanalysis on the proposed algorithm and proved that although it is efficient and fast but the keys can be easily generated and hence not secure. He further proposed the use of AES-CTR or eSTREAM [11], to improve the security.

Noor Arshad, et al [12], proposed a new encryption algorithm by making improvements to existing Cipher encryption which removed all its weakness. The main changes were made to the mode of encryption and decryption operations. At end they also

suggested this improved algorithm can be used in other fields where security of data is required, moreover suggested that there is further scope of improvement in the security by using the proposed algorithm in a hybrid fashion.

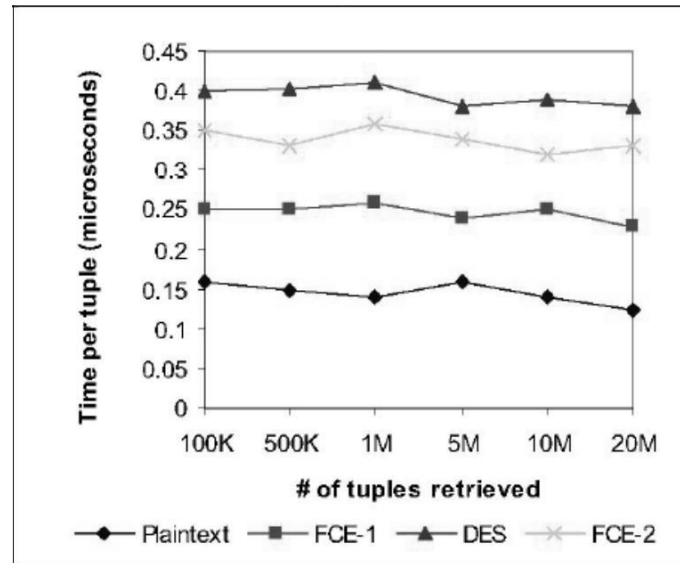


Fig. 5. Comparison of FCE with DES and Plain Text [9]

Chin-Chen Chang and Chao-Wen Chan [13], gave two schemes of database encryption. Scheme 1 for field-oriented encryption system, and Scheme 2 for record-oriented encryption system. Both schemes based on RSA Master Keys, which also solves the key management problem and also helps in providing access rights to different users. The proposed schemes overcome the weakness of the schemes proposed by GI Davida, et al [6] and D. Buehrer [14].

Erez Shmueli, et al [15], evaluated all the traditional 5 architectures for database encryption and gave a new encryption architecture which removed the weakness of all earlier architectures. This scheme places the encryption module just above the database cache, inside the database management system (DBMS) and uses a dedicated technique to encrypt each database value together with its coordinates.

Kamaljit Kaur, et al [16], discussed the importance of security in today's world. They proposed encryption of numeric data in the database using 3KDEC algorithm. The algorithm is easy to use and takes very less computations. Further they simulated various attacks like Brute Force Attack; Statistical Attack etc to show the encrypted numerical values cannot be cracked by the attackers. Moreover, they stated that the algorithm is not limited to databases but can even be used in other areas where security is required. The flowchart of the proposed algorithm is shown in figure 6.

ZhaoYong-Xia [17], discussed the various schemes like substitution and transposition, along with various traditional standard encryption algorithm like Data Encryption Standard (DES), AES (American Advanced Encryption Standard) etc that are being used in database encryption. They further discussed the various advantages and disadvantages of database encryption, and possible ways of improving them.

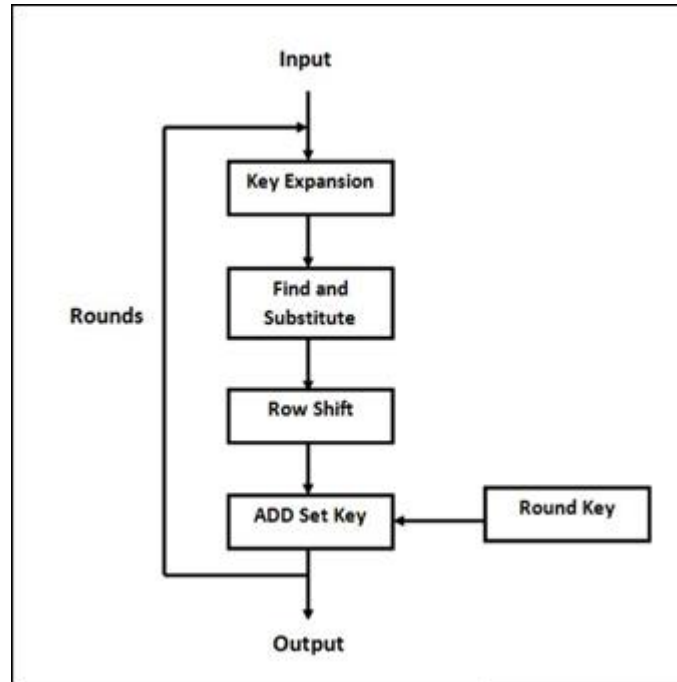


Fig. 6. Flowchart of 3KDEC Algorithm [16]

Zhou Xing and Liu Jun [18], proposed an encryption technique by using multi-granularity encryption. This scheme takes 4 granularities to provide maximum security. The main idea behind his research was that with encryption the efficiency decreases, so to improve that he proposed this new scheme which uses B+ trees for indexing.

Lianzhong Liu and Jingfen Gai [19], discussed the various properties and features that a good database encryption method should possess. They further proposed a new method for database encryption, according to which an encryption to the database can be provided as a service. Another important feature which they proposed was to save the keys away from the encrypted data in order to enhance the security.

Lianzhong Liu and Jingfen Gai [19], discussed the various properties and features that a good database encryption method should possess. They further proposed a new method for database encryption, according to which an encryption to the database can be provided

as a service. Another important feature which they proposed was to save the keys away from the encrypted data in order to enhance the security.

4.2 HYBRID APPROACH

W Xing-hui, M Xiu-jun [20], gave the use of hybrid encryption in databases. They used RSA and IDEA algorithm which are public key and symmetric key respectively. In this the keys were first encrypted using the RSA algorithm and then these keys were used to encrypt the plain data using the IDEA algorithm. This hybrid approach enhances the security of data and makes it really difficult to break it.

4.3 HASHING APPROACH

Mary Cindy Ah Kioon, et al [21], discussed the importance of password encryption using hashing functions like MD5 etc. It also suggests possible modification that can further enhance the security using hashing functions. Table 3, shows the snapshot of database using MD5 hash function.

Table 3, Database Table using MD5 Hash Function [21]

UserName	Pwd_hash	randomKey
cindy	@9NjL480BAAG0E=K7G0EIEA1L==M<5<2	iUUMk
felipe	=6J@9F2@IAILFH36O2BDM5HFD8407:LH	ig4j
jack	>C7L31O<851<>FA56M?H6I6EG1FLD>9=	EYIO
jake	7L87K@?CB@GL2<?M3C8BB3?0@<@A:BNH	25d
lina	EG@;1F<F1OLO8I<72E0@D0537H>9HKGO	ugK1
miranda	@D<LDO09EI7G93ONO=F42K2H?@OH>MHE	MUcdx
ranbir	3NCE>A1NDNDLM@4;HLJJK:967L2B81IO	3f8J9
richard	>5ED5NGMA3AK;J:MBDNI6CK7JK0ELEL7	XTW

5 RESULTS AND FINDINGS

A lot of research work has been done in field of database encryption, with a sole motive to improve security of data in the database. Table 4, compares the various Database Encryption Research papers on different parameters.

Table 4. Compare various Database Encryption Research papers on different parameters

Paper	Technique Used	Algorithm	Merits	Demerits
A Secured Database Encryption Scheme	Standalone Encryption Approach	Data Encryption Standard (DES)	Time Cost of Encryption and Decryption operation is minimum	Cannot directly perform queries of statistical function such as sum, count etc,
A two-phase encryption scheme for enhancing database security [5]	Standalone Encryption Approach	Data Encryption Standard (DES)	Security is guaranteed by use of two-phase encryption. Problem of key management is also efficiently handled	Lot of computation and Overheads
Fast, secure encryption for indexing in a column-oriented DBMS [9]	Standalone Encryption Approach	Fast Comparison Encryption (FCE)	Efficient and Fast for protecting the confidentiality of large databases	Key can be easily generated and hence not reliable.
Database encryption using enhanced affine block cipher algorithm [12]	Standalone Encryption Approach	General for all Block Cipher Algorithms	Improves the limitations of the traditional Block Cipher Algorithm	Added Computations and Time cost of Encryption and Decryption
A database record encryption scheme using the RSA public key cryptosystem and its master key [13]	Standalone Encryption Approach	RSA Public Key Algorithm	Master Key solves the problem of Key Management	Increased Time cost of Encryption and Decryption
Implementing a database	Standalone Encryption	Advanced Encryption	A new encryption architecture which	Since Encryption is done just above Cache

encryption solution, design and implementation issues, Computers & Security [15]	Approach	Standard (AES)	removed the weakness of all earlier architectures	the database server memory may still contain data in its plaintext form
Numeric to Numeric Encryption of Databases: Using 3Kdec Algorithm [16]	Standalone Encryption Approach	3KDEC (Symmetric key algorithm)	Less Computation and easy to Use. Full Protection of Numeric data	Cannot be used for numeric data with decimal data and non-numeric data.
The Technology of Database Encryption [17]	Standalone Encryption Approach	Various Encryption Algorithm	Every Algorithm has its merits	Every Algorithm has its Demerits
A novel efficient database encryption scheme [18]	Standalone Encryption Approach	New Proposed Scheme	Use of multigranularity encryption provide efficient protection to index information	Complex Computations and query processing
A new lightweight database encryption scheme transparent to applications [19]	Standalone Encryption Approach	New Proposed Scheme	Added security and Efficient key management	Complex query processing
Research of the Database Encryption Technique Based on Hybrid Cryptography [20]	Hybrid Approach	RSA+ IDEA	Added Security by use of 2 encryption algorithms	More computations for encryption and decryption process.
Security Analysis of MD5 algorithm in Password Storage [21]	Hashing	MD5 (Message Digest Algorithm 5)	Can't be broken easily. Easy to Implement	Can only be used to encrypt data, decryption is not possible. Hence can't be used where information retrieval is required

6 Conclusion

With advancement in Technology, nowadays everything is being done with computers, so security of these data in the database becomes an important issue. Many researchers have worked on this thing and proposed various algorithms and architectures. Each scheme has its own advantages and disadvantages. But none of them is fully secure, and contain certain loopholes or demerits which can be used by the attackers and the intruders to get access of the database. So, there is a scope of improvement in this area and researchers are already working on it to find the perfect solution of this problem and find a scheme that is fully secure from all the possible security threats.

7 References

- [1] Baraani-Dastjerdi, Ahmad, Josef Pieprzyk, and Reihaneh Safavi-Naini. "*Security in databases: A survey study.*" Department of Computer Science, The University of Wollongong (1996).
- [2] Denny Cherry and Thomas Larock, "**2 - Database Encryption, In Securing SQL Server**", edited by Denny Cherry, Thomas Larock, Syngress, Boston, 2011, Pages 27-71, ISBN : 9781597496254.
- [3] Kessler, Gary C. "*An overview of Cryptography.*" (2003). (<http://www.sciencedirect.com/science/article/pii/B9781597496254100022>).
- [4] Sesay, Samba, Zongkai Yang, Jingwen Chen, and Du Xu. "*A secure database encryption scheme.*" In Consumer Communications and Networking Conference, 2005. CCNC. 2005 Second IEEE, pp. 49-53. IEEE, 2005.
- [5] Min-Shiang Hwang, Wei-Pang Yang, "*A two-phase encryption scheme for enhancing database security*", Journal of Systems and Software, Volume 31, Issue 3, December 1995, Pages 257-265, ISSN: 0164-1212. (<http://www.sciencedirect.com/science/article/pii/0164121294001022>).
- [6] Davida, George I., David L. Wells, and John B. Kam. "*A database encryption system with subkeys.*" ACM Transactions on Database Systems (TODS) 6, no. 2, Page: 312-328, (1981).
- [7] Lin, C. S., "*An Application of an Encryption Algorithm to Database Security, Chap. 3, Ph.D. Thesis*", National Tsing Hua University, 1991.
- [8] Lin, C. H., Chang, C. C., and Lee, C. T., "*A record-oriented cryptosystem for database sharing*", in International Computer Symposium, pp. 328-329, 1990.

- [9] T. Ge and S. Zdonik, ***"Fast, secure encryption for indexing in a column oriented DBMS,"*** in International Conference on Data Engineering - ICDE 2007. pp. 676–685. IEEE, 2007.
- [10] Jacob, Stéphane. ***"Cryptanalysis of a fast encryption scheme for databases."*** In Information Theory Proceedings (ISIT), 2010 IEEE International Symposium on, pp. 2468-2472. IEEE, 2010.
- [11] Ecrypt – European Network of Excellence in Cryptology, ***"The eStream Stream Cipher Project," 2005*** <http://www.ecrypt.ed.org/stream/>
- [12] Arshad, Noor Habibah, Saharbudin Naim Tahir Shah, Azlinah Mohamed, and Abdul Manaf Mamat. ***"Database encryption using enhanced affine block cipher algorithm."*** In Proceedings of the 10th WSEAS International Conference on Mathematical Methods and Computational Techniques in Electrical Engineering, pp. 71-76. World Scientific and Engineering Academy and Society (WSEAS), 2008.
- [12] Chang, Chin-Chen, and Chao-Wen Chan. ***"A database record encryption scheme using the RSA public key cryptosystem and its master keys."*** In Computer Networks and Mobile Computing, 2003. ICCNMC 2003. 2003 International Conference on, pp. 345-348. IEEE, 2003.
- [13] Buehrer, D., and C. Chang. ***"A cryptographic mechanism for sharing databases."*** In the International Conference on Information & Systems. Hangzhou, China, pp. 1039-1045. 1991.
- [14] Erez Shmueli, Ronen Vaisenberg, Ehud Gudes, Yuval Elovici, ***"Implementing a database encryption solution, design and implementation issues"***, Computers & Security, Volume 44, July 2014, Pages 33-50, ISSN 0167-4048. (<http://www.sciencedirect.com/science/article/pii/S0167404814000509>)

- [15] Kaur, Kamaljit, K. S. Dhindsa, and Ghanaya Singh. *"Numeric to Numeri Encryption of Databases: Using 3Kdec Algorithm."* In Advance Computing Conference, 2009.IACC 2009. IEEE International, pp. 1501-1505. IEEE, 2009.

- [17] Yong-Xia, Zhao. *"The Technology of Database Encryption."* In 2010 Second International Conference on Multimedia and Information Technology, vol. 2, pp. 268-270. 2010.

- [18] Xing, Zhou, and Liu Jun. *"A novel efficient database encryption scheme."* In Fuzzy Systems and Knowledge Discovery (FSKD), 2012 9th International Conference on, pp. 1610-1614. IEEE, 2012.

- [19] Liu, Lianzhong, and Jingfen Gai. *"A new lightweight database encryption scheme transparent to applications."* In Industrial Informatics, 2008. INDIN 2008. 6th IEEE International Conference on, pp. 135-140. IEEE, 2008.

- [20] Xing-hui, Wu, and Ming Xiu-jun. *"Research of the Database Encryption Technique Based on Hybrid Cryptography."* In Computational Intelligence and Design (ISCID), 2010 International Symposium on, vol. 2, pp. 68-71. IEEE, 2010.

- [21] Ah Kioon, Mary Cindy, Zhao Shun Wang, and Shubra Deb Das. *"Security Analysis of MD5 algorithm in Password Storage."* Applied Mechanics and Materials 347, Pages: 2706-2711, (2013).