International Journal For Technological Research In Engineering
Volume 4, Issue 8, April-2017 *ISSN (Online): 2347 - 4718*

A NOVEL APPROACH TO ENSURE CONFIDENTIALITY AND DATA INTEGRITY FOR SECURITY IN RELATIONAL DATABASE

Ramesh Selana[1], Ashil Patel[2]
[1]ME Student, [2]Assistant Professor
Information Technology Department, LD College of Engineering, Ahmedabad, Gujarat.

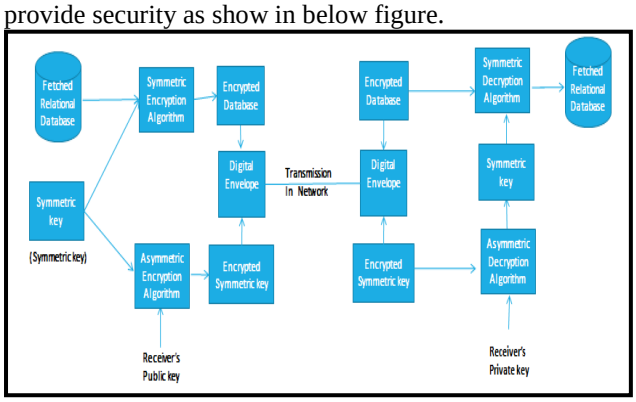
ABSTRACT: A Novel Approach to ensure Confidentiality with Data Integrity for Security in Numerical Relational Database is proposed in this research work to secure Relational Database. In this approach we ensured Confidentiality with help of Proposed Symmetric Encryption Algorithm and Data Integrity with the help of Message Digest using MD5 Function. In this Novel Approach We can Create Digital Envelope with help of Hybrid Approach (Combination of Symmetric and Asymmetric Cryptography) which consists of encrypted relational database, digest of selected important fields and encrypted symmetric key using RSA Asymmetric Algorithm. In Client-Server Architecture Digital Envelop contains encrypted data so that no one is able to get or modify confidential information of the requested relational database during transmission in insecure Network .To check Data Integrity Client generates Message Digest for same important fields for which Server generated Message Digest is sent in Digital Envelop. This way we achieved Confidentiality and Data Integrity of Relational Database in this Novel Approach of Proposed Research Work. The main objective of this designed approach is to boost up the performance of a System when Digital Envelop Processes at Client/Server Side. The quality of measures such as memory usage and processing time or execution time are taken as an important measure in this research work to justify the performance of the Proposed Approach.
Keywords: Relational Database Security, Digital Envelop, Encryption Algorithm , Message Digest.

I. INTRODUCTION

Security is one of the important aspects in the field of computer science. Out of the various types of securities database security plays a significant role in protecting the sensitive data during the Database transmission in insecure Network. To perform a secured database transfer, few methods are available and one of them is an encryption of database. The database is to be transferred in an encrypted way while sending and decrypted when they are used. The volatility of the present day, online business environment has left organizations with no alternatives to share sensitive information of database with their systems, suppliers and business partners. Most of the cryptographic algorithms provide the security of information to be transferred into an insecure medium. Algorithms of those types are in need of data protection from interruption, interception, modification and fabrication. In this way, the security of the data communication is mainly based on the cryptographic algorithms along with their key values.

II. RELATED WORK

Symmetric and Asymmetric Cryptographic algorithms are used the Specialized procedure to encrypt or decrypt the data. There is a possibility that, the hackers may decrypt the message which is either encrypted with symmetric or asymmetric encryption algorithm. Hence, it is essential to hybrid the approach of Symmetric and Asymmetric technique. When using only Symmetric or Secret-Key Cryptosystems, users must first agree on a session key, that is, a secret key to be used for the duration of one message or communication session. In completing this task there is a risk the key will be intercepted during transmission. This is part of the key management problem. Public-key or Asymmetric Cryptography offers an attractive solution to this problem within a framework called a digital envelope. The Digital Envelope consists of a message encrypted using Symmetric Cryptography and an encrypted secret key using Asymmetric Cryptography Algorithm. As we discussed above Hybrid Approach has advantage of both Symmetric and Asymmetric Algorithm we can implement it on Relational Database to provide security as show in below figure.



III. LITERATURE REVIEW

In this section the various performance factor and technique for encrypting the database used by various papers are listed. In this research paper [1] proposed methodology of the paper provides an enhancement to ETSFS(Enhanced Transposition-Substitution-Folding-Shifting) algorithm by avoiding the constraint on the data size. The improvement allows handling all special characters on the data size. In this paper of proposed algorithm involves the accumulation of new key value to the existing ETSFS algorithm which have four phases:

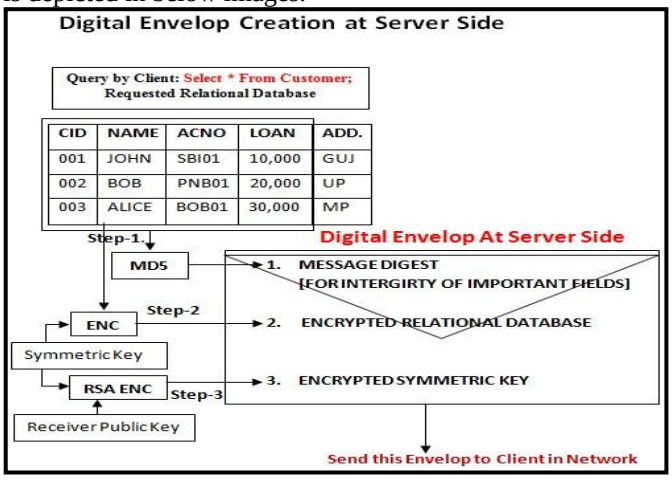
1. Transposition, 2.Subsitution, 3.Shifting, 4.Folding.

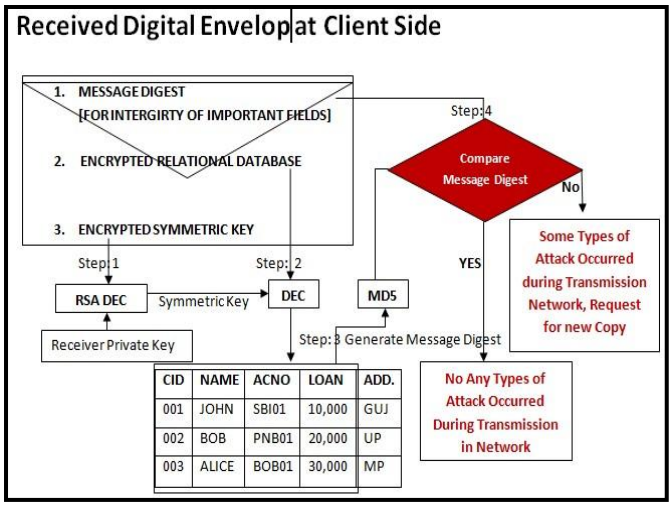
In this research paper [2] proposed design methodology, the new protocol design using Symmetric cipher (Ping Pong-128) and public key cryptography (RSA) with hash function

MD5. In this paper hybrid encryption is a mode of encryption that merges two or more encryption systems. These strengths are respectively defined as speed and security. Therefore, we are suggest design of hybrid cryptographic for secure email based on Android OS. In this survey paper[3], the survey was conducted to identify the issue and threats in database security, requirements of database security, and how encryption is used at different levels to provide the security. This paper[4] discusses the importance of database encryption and makes an in depth Review of various database encryption techniques. In this paper discusses various database encryption techniques using either different encryption algorithm or using hashing function. The author of this paper [5] has highlighted the difference between the two encryption algorithms and further concluded that Asymmetric key cipher technique is way more secure compared to that of the symmetric key cipher technique. The author has also compared two prominent public key cryptography algorithms namely RSA algorithm and Diffie-Hellman algorithm and concluded that each such algorithms has its importance on particular context and each one holds the advantage over the other in specific context. This paper [6] is based on the performance analysis of message digest 5 and secure hashing algorithm. These two topics are related with cryptography and cryptography is an extension of cryptology and cryptanalysis. The purpose of this paper is that to compare the time taken to build a hash as well as it also compares the bit rate passes through a hash value. Here we are going to perform a deep analysis for these two algorithms.

IV. PROPOSED WORK

This proposed method proposes a hybrid encryption technique for secure the relational database. The aim of the proposed hybrid encryption technique is to provide better confidentiality, integrity and availability among other security protocols. A method of encryption that combines two or more encryption schemes includes a combination of symmetric and asymmetric encryption to take advantage of the strength of each type of encryption. Workflow of this Proposed System is different at Client and Server Side which is depicted in below images.





METHODOLOY OF PROPOSED WORK:

Step 1: Retrieve requested data by Client from Server.

Step 2: Server Generates Digital Envelop for Fetched Relational Database

Step 3:To achieve Relational Database Confidentiality Generate Digital Envelop Which Consists data in un-understandable form=Using Proposed Encryption Algorithm Encrypted Relational Database + Message Digest with MD5 + Encrypted Symmetric Key with help of RSA.

Step 4: Server send Generated Digital Envelop to Client.

Step 5: Client Received Digital Envelop and First decrypt encrypted symmetric key using It's Private Key.

Step 6: Using Symmetric Key Client decrypt encrypted Relational Database and get Original Relational Database.

Step 7: After getting Original Database Client generate message digest for same fields for which Sever generated message digest.

Step 8: To Check Data Integrity Client have to Compare both message digest generated at Client and Server. If both digest are same means no any types of attack (Data integrity achieved) else request for new copy of database because some attack occurred during transmission in network.

Data Confidentiality using Symmetric Key Encryption/Decryption Algorithm in Proposed Approach: Relational Database encryption is the process of converting data within a database. That is, the plain text (Readable) format is converted into a cipher text (Unreadable format) using keys generated by the encryption algorithm. Relational Database decryption is converting the cipher text into the Plain text (original information) using keys generated by the encryption algorithms. Relational Database encryption can be provided only in file format or column format.

Encryption Algorithm□

Input : Fetched each attribute or column value of Relational Database as Plaintext (PT) into Algorithm with Key K length is 128 bits.

Output: Return Cipher text or Encrypted Text for given PT.

Step 1. Select Symmetric Key of 128 bits as a K

Step 2. Select an attribute as a Plain text (PT) of 128 bits size from relation database (R). If it's not 128 bits in size then padding will apply.

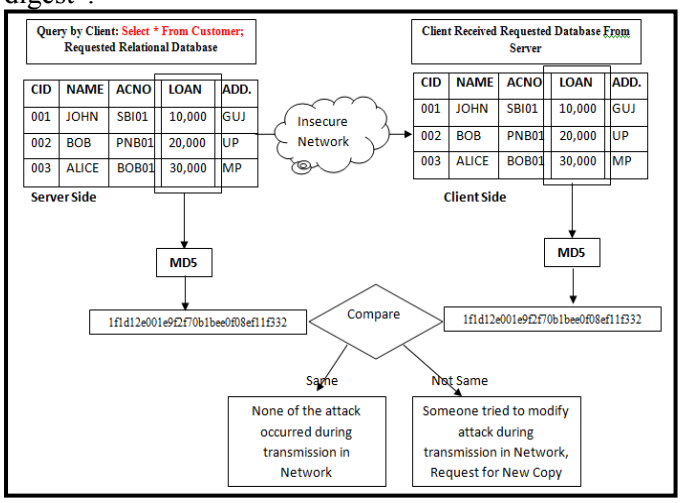
Step 3. Divide K and PT into two equal parts K11, K12 for Key (K1) and PT1, PT2 for PT.

Step 4. Apply 2 bits right circular shift on K11 and perform XOR operation with PT1. Output of this step called C1.(C1 = (K1>>2) XOR PT1).
Step 5. Apply 2 bits left circular shift on PT2 and perform XOR operation with K12. Output of this step called C2.(C2 = (K2 XOR (PT1 << 2)).
Step 6. Divide C1 and C2 into two equal parts C11, C12 for C1 and C21, C22 for C2 .
Step 7. Apply 2 bits right circular shift on C12 and perform XOR operation with C21. Output of this step called C3. (C3 = (C12 >>2) XOR C21).
Step 8. Apply 2 bits left circular shift on C22 and perform XOR operation with C11.Output this step called C4. (C4 = (C22 <<2) XOR C11).
Step 9. Apply 2 bits right circular shift on C12. Output of this step called C5.(C5=C12 >> 2).
Step 10. Apply 2 bits left circular shift on C22. Output of this step called C6.(C6=C22 << 2).
Step 11. Perform XOR operation between C6 and C3.Output of this step called C7.(C7 = (C6 XOR C3)).
Step 12. Perform XOR operation between C4 and C5.Output of this step called C8.(C8 = (C4 XOR C5))
Step 13. Now finally combine C3, C4, C7, C8 to get Cipher text (C) of 128 bits.

Decryption Algorithm:

Input : Generated Cipher Text for Column value with same Key value K which used in Encryption Algorithm as input.
Output: Original Plaintext of Column value.
Step 1: Select Cipher text CP as a cipher text (CP) of 128 bits.
Step 2: Divide CP into four equals parts CP1, CP2, CP3,CP4 of 32 bits each.
Step 3: Perform XOR operation between CP2 and CP4.Output of this step is called CP5. (CP5=CP2 XOR CP4)
Step 4: Perform XOR operation between CP1 and CP3.Output of this step is called CP6. (CP5=CP2 XOR CP4)
Step 5: Apply 2 bits left circular shift on C5.Output of this step is C12. (C12=C5 << 2)
Step 6: Apply 2 bits right circular shift on C6.Output of this step is C22. (C22=C6 >> 2)
Step 7: Perform XOR operation between C1 and C12.Output of this step is called CP11. (CP11 = C1 XOR C12)
Step 8: Perform XOR operation between C4 and C22.Output of this step is called CP21. (CP21=C4 XOR C22)
Step 9: Apply 2 bits right circular shift on C11 (C11= C11 >> 2).Apply 2 bits left circular shift on C21.(C21 = C21 << 2)
Step 10: Combine C11 and C12.Output of this is C1 (C1=C11 + C12).Combine C21 and C22.Output of this is C2. (C2= C21 + C22)
Step 11: Divide selected key K into K1 and K2.Apply 2 bits right circular shift on K11. (K11 = K11 >> 2).
Step 12: Perform XOR operation between C1 and K1.Output of this step is called PT1(PT1 = C1 XOR K1)
Step 13: Perform XOR operation between C2 and K2.Output of this step is called PT2.(PT2 = C2 XOR K2)
Step 14: Now combine PT1 and PT2 to get original plain text PT of 128 bits. (PT=PT1+PT2).

Data Integrity using MD5 Hash Function in Proposed Approach: The hash function is a deterministic procedure that takes an arbitrary block of data and returns a fixed size of bit string as the (cryptography) hash value, such that an accidental or intentional change in that data will change the hash value. The hash value is sometimes called the "simply digest".

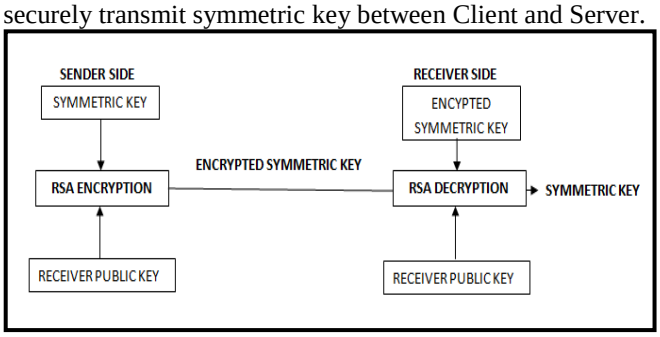


In above fig we can see that loan amount is very confidential field of Customer database. We need to provide data integrity for this field during transmission in insecure network. So compute message digest for this field at Server Side before transmitting into network. When relational database reached at Client Side client generates message digest for same filed for which Server generated and sent to Client. Then Client match both generated and received message digest, If both are same then none of the modification attack occurred during transmission during insecure Network. If both are not same at Client side that means someone tried to modify our confidentiality field of relational database. So request new copy of this requested relational database again. This way we achieve data confidentiality in Proposed Approach. We can achieve data integrity for more than one field also as same procedure.

Asymmetric (RSA) Algorithm in Proposed Approach:
As we discussed we are using hybrid approach of cryptography algorithm. That means we are using

combination of symmetric and asymmetric algorithm. This concept implemented with help of Digital Envelop. In this Novel Approach we are using RSA algorithm as asymmetric key algorithm. In Digital Envelop Symmetric Key of Encryption Algorithm encrypted using RSA Algorithm with Receiver Public Key at Server Side. And put this encrypted key into Digital Envelop and send to Client.

When Digital Envelop reached at Client Side , Client first get encrypted symmetric key and decrypt it using RSA algorithm and Receiver Private Key. So in this way proposed algorithm securely transmit symmetric key between Client and Server.

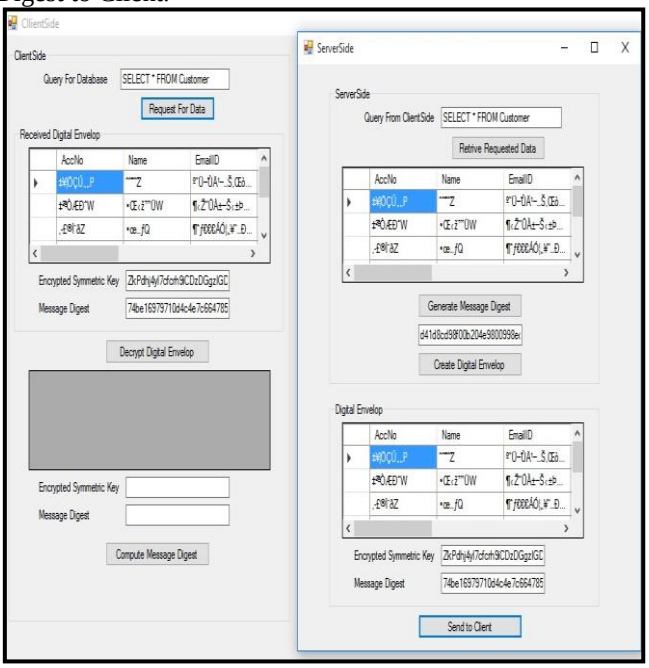


V. IMPLEMENTATION

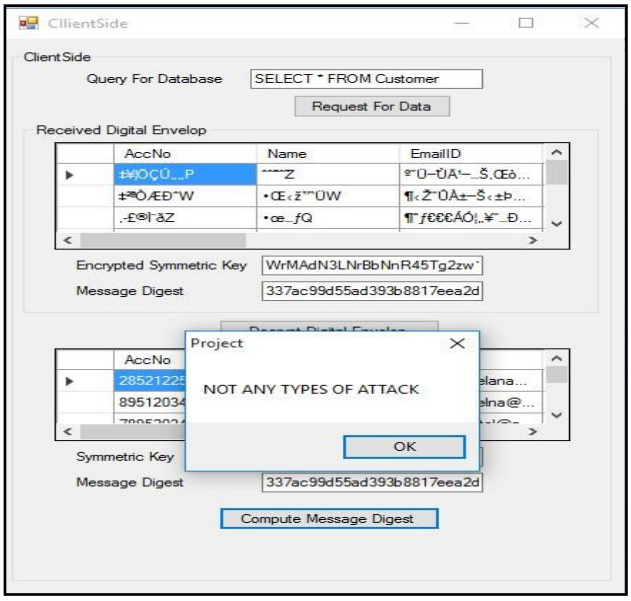
Implementation Tool and Platform:

The experimental results of proposed Novel approach of relational database security are implemented in visual studio .net.

Server creates Digital Envelop which contains encrypted relational database, encrypted symmetric key and Message Digest to Client.



After received Digital Envelop Client decrypt and get original relaitonal database client compute message digest for same field which is generated by server and compare it. If both message digest value s are same then no any types of attack modification occur during transmitting database on network. This way we achieve database integrity for selected field of relational database.

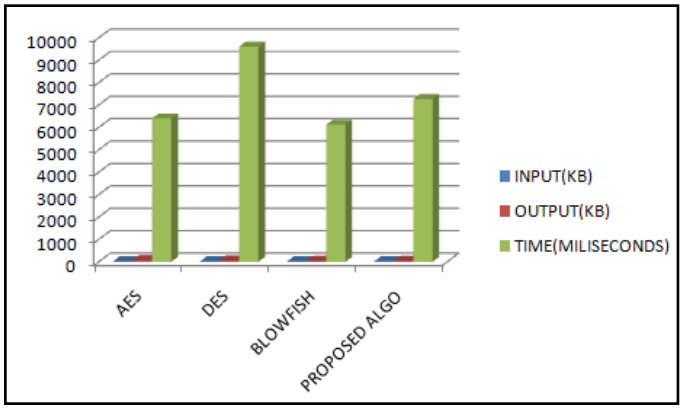


VI. RESULT AND ANALYSIS

The role of result and discussion part is essential in research and it justifies the performance and efficiency of the proposed research work. The main objective of this Proposed Novel Approach is to improve performance parameters of System (Client/Server) when Digital Envelop processes at Client or Server Side. For example Memory Size, Execution Time. In this Novel Approach require fast symmetric encryption algorithm which encrypt requested relational database by client and put encrypted database in digital envelop is necessary because which help to improve performance parameters of System. The time require in encryption and decryption process is more compare to other procedure of this Proposed Novel Approach. If we reduce this time then we will get better performance compare to existing encryption algorithm i.e DES ,AES ,Blowfish. The algorithm has evaluated with the parameters such as Memory usage, Execution Time. The following table shows the comparison of DES, AES, Blowfish and Proposed Encryption Algorithm. Here Input size is requested relational database size in Digital Envelop which as input in encryption algorithm.

PARAMETER/ ALGORITHM	AES	DES	BLOWFISH	PROPOSED ALGO.
INPUT SIZE	35 KB	35 KB	35 KB	35 KB
OUTPUT SIZE	70 KB	60 KB	57 KB	48 KB
TIME(MILISECONDS)	6397.87930	9604.44760	6123.4397	7264.94700

The parameters used for the comparison is Input size of the file, execution time and memory size of the file after encryption. Execution time and storage of output memory size in DES, AES and Blowfish are more than Proposed Encryption Algorithm for given input size of the file 35kb. The graphical representation of the above table is as follows. As per below charts we can decide the proposed encryption technique returns better performance than the existing one.



VII. CONCLUSION

The proposed research work has successfully implemented and tested with existing algorithm of DES, Blowfish and AES algorithms to enhance the relational database security. The performance of proposed research work improves the strong security to protect the data and it will yield good impact on the relational database fields. The quality of measures such as memory usage and processing time or execution time are taken as an important measure in this research work to justify the performance of the Proposed Approach.

REFERENCES

[1] Prathyusha Uduthalally,Bing Zhou ,"Improvement of ETSFS Algorithm for Secure Database" , IEEE-2016.

[2] Saranzaya Purevjav, Teeing Kim, "Email Encryption Using Hybrid Cryptosystem Based on Android", IEEE-2016.

[3] Iqra Basharat,Farooque Azam, "Database Security and Encryption: A Survey Study", IJCA-2012

[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] Prabhsimran Singh and Dr.Kuljit Kaur," Database Security Using Encryption ",IEEE-2015.

[6] Brief comparison of RSA and diffie-hellman (public key) algorithm. Ayan Roy* Department of Computer Science, St. Xavier˝s College, Kolkata(Autonomous) ©2016 ACCENTS.

[7] A Comparative Analysis of SHA and MD5 Algorithm.Piyush Gupta, Sandeep Kumar Department of Computer Science and Engineering Jagannath University, Jaipur. IJCSIT), Vol. 5 (3) , 2014, 4492-4495.

