International Journal of Applied Engineering Research ISSN 0973-4562 Volume 10, Number 14 (2015) pp 34369-34371

Software Based Prototype for Data Confidentiality in Databases

T.Sasikala[1] ,Naveen Kumar Ala [2]& Ramesh Gorantla[3]
Assistant professor[1], UG Scholar[2]&UG Scholar[3]
Department of Computer Science and Engineering,
Amrita School of Engineering, Amrita VishwaVidyapeetham, Bangalore, India.
jivishnaa@gmail.com& naveengowtham@outlook.com

Abstract- In recent times huge amount of data is getting generated and is stored in the databases. These databases are either outsourced or maintained by the companies. The data stored can be highly confidential, but there is no guarantee whether that data is secure or not [4][6]. The databases can be attacked and sensitive information can be leaked. So to provide security for data in databases we came up with a software prototype which is cost effective, efficient and ensures high data security. This prototype encrypts the data before storing in the database with a secret using strong cryptographic algorithms and hence ensures data security.

Keywords- *Database, Data confidentiality, Data security, Cryptographic algorithms*.

1. Introduction

There are many hardware prototypes [5] for encrypting the data before saving into the database. But it involves more cost and time. So we came up with a software prototype for encrypting the data which is cost effective and takes minimal time.

Database is a collection of related data that is stored at a common place from which useful information can be retrieved when needed. The biggest concern is whether the data is secure or not. The data stored may contain confidential information, but we can't ensure whether the data is secure from any unauthorized person. Data security ensures that the data stores in databases is protected from unauthorized access.

Cryptography is a way of manipulating the data in such a way that it can be processed and readable only by the intended persons. There are many cryptographic algorithms currently which can be used to achieve this. Encryption means transforming the plain text into cipher text using cryptographic algorithms. Securing the data is needed everywhere now a days. The data stored in the database is prone to attacks, which might cause the leak of valuable

information. In most scenarios the data is stored as it is in the database i.e., without encryption so whenever the database is hacked private information is getting leaked. So we came up with a prototype which is cost effective and uses cryptographic algorithms to encrypt the data before storing in the databases. The prototype acts as new layer between the middle ware and database, the content from the middle ware is encrypted and then send to the database, similarly while retrieving the data is decrypted and then send to the middle layer. The prototype uses AES (Advanced Encryption Standard) algorithm for encrypting or decrypting the data. AES is one of the strong cryptographic algorithms which is difficult to crack. More details of the algorithm are explained below.

2.Literature Survey

Advanced Encryption standard (AES) it is a symmetric encryption algorithm[1] implemented in both hardware and software to encrypt the sensitive data. It is a block cipher. It contains a 128 bit fixed block size and key lengths of 128, 192 and 256 bits. The key length that we use specifies number of times the transformations are repeated while converting plain text to cipher text. We are using 128 bit key length so we have to repeat the rounds for 10 times. The algorithm is based on several substitutions, linear transformations and permutations, each executed on data blocks of 16 byte.

A .Encryption in AES

Encryption contains several different stages such as Key Expansion, Initial Round, Rounds (Sub Bytes, Shift rows, Mixed Columns and Add Round key) and Final Round. The rounds are repeated several times (based on the key length size). In each round, a unique round key is calculated out of encryption key, and is incorporated in the calculations. Based on the block structure of AES, the change of a single bit either in plain text or key results in an entirely different cipher text block.

B. Decryption in AES

AES takes 128 bit cipher text to decrypt, which results in 128 bit decrypted data. The AES decryption [1] is same as the encryption but in opposite direction. The basic modules that are present in AES decryption are

(i).Key Expansion: Performs the key expansion on the 128 bit key that creates all the intermediate keys which are generated from the original key during AES encryption for every round.

(ii).Inverse Add Round Key: In these we do XOR operation between the intermediate expanded key of the particular step and the cipher text.

*(iii).Inverse Shift Row: I*n this step we shift the rows in 4*4 matrix in right wise in circular way.

(iv). Sub Bytes: In this Step we replace every cell values in the matrix with corresponding values in the inverse S-box [2].

(v).Inverse Mix Column: In this step the operations are performed using the cipher text along with the shift rows step and this is the main source for the 10 rounds of diffusion[2]. In this each column in 4*4 matrix is treated as a polynomial which is a fixed inverse polynomial and is then multiplied

with modulo x^4 +1. At the 10 iteration, it does all the steps except the inverse mix column step to generate the original plain text. By cracking an AES 128 bit with a super computer it will take longer than the age of universe.

3. Existing System

In current system[3] data to be stored in the database is send from the web client to the web server and then web server stores it in the database. The data gets stored into the database in the same form as given by the user/web client. This data may contain highly sensitive/confidential information, but we can't ensure that the data is secure as it was not encrypted and anyone who hacks the database can view and manipulate the information.

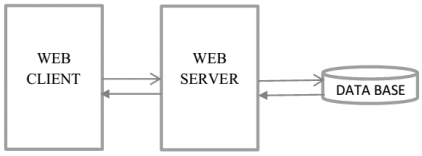

Fig.1:Flow of theExisting System

4. Proposed System

In the proposed system we added a new prototype in between the web server and database. This layer encrypts/decrypts the data going from the web server to database and from database to web server. We used AES algorithm to encrypt/decrypt the data. This prototype ensures that the data is encrypted/decrypted properly. This prototype is highly efficient, cost effective and fast.

A. Encryption :

The data from the user/web client is send to the web server for storing in the database. Our prototype lies in the middle of web server and database. Data to be saved in database is encrypted using a secret key with AES 128 bit algorithm. Now this encrypted data is stored in the database. The data is encrypted properly into human unreadable format. In this way we store only the encrypted data in the database.

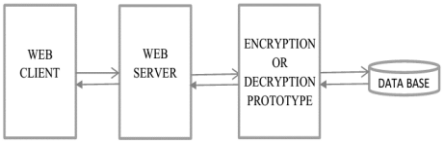

Fig.2:Flow of theProposed System

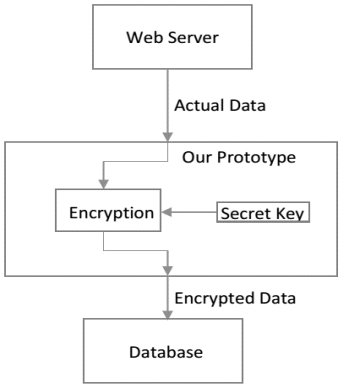

Fig.3: Encryption of the data

B.Decryption :

The data from database is sent to the web client/user via web server. Our prototype gets the encrypted data from the database as requested, decrypts that with the same secret key using AES algorithm and then send it to the web server, web server then send it to the web client.

This prototype provides high data security, so even when the database is hacked the information is safe as decrypting the information without appropriate key is impossible.

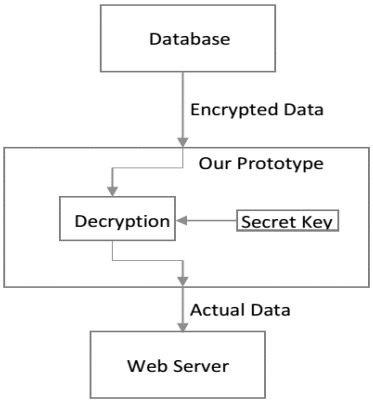

Fig.4: Decryption of the data

5 .Experimental Analysis

The results are verified in windows operating system with the following system specifications

RAM: 2GB
Hard disk capacity: 250GB
Processor: i3 Intel processor
Clock speed: 1.9GHz

Different datasets which has a single column have been taken and our prototype has been implemented on it. The datasets chosen has 2000 records, 5000 records, 10000 records and 100000 records. The results obtained with these datasets are represented as a Bar graph as shown below in Fig. 5. The results include encryption and decryption times.

Graph representation:

X-axis: number of records

Y-axis: Time taken in milliseconds for encryption and decryption

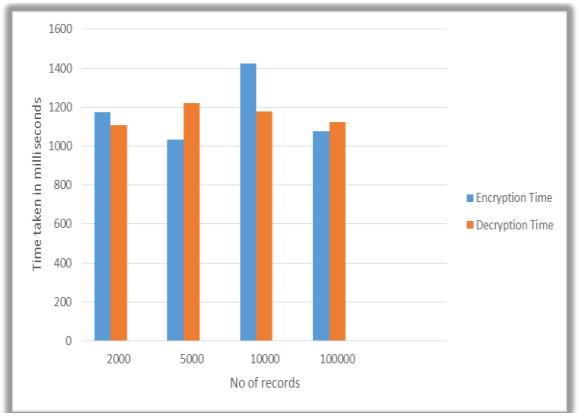

Fig.5: Timetaken to encrypt and decrypt different records

We also tested our prototype by encrypting/decrypting entire file with varied sizes. The files we tested are of sizes 100kb, 200kb, 800kb, 8000kb. The encryption and decryption times of the files are plotted as a Bar graph as shown below in fig.6.

Graph representation:

X-axis: Size of the file in KB

Y-axis: Time taken in milliseconds for encryption and decryption

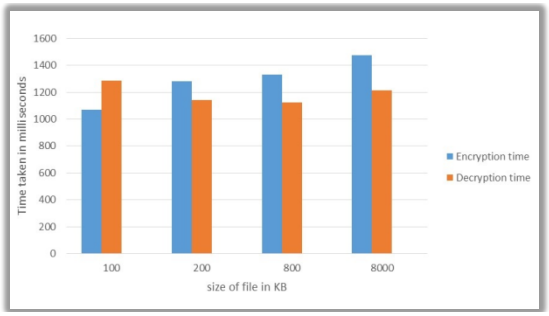

Fig.6: Time taken to encrypt and decrpt the datastored in file

6. Conclusion

Data security in databases has become the major concern in today's scenario. Highly sensitive data is being stored in the databases, but we can't ensure that data is secure there. So to meet today's data security issues in more efficient and cost effective way we developed this prototype which uses strong cryptographic algorithms to encrypt the data. This process is highly efficient, cost effective and ensures data security in the database. Using this prototype we can ensure data confidentiality to a maximum extent.The secret key used in the existing approach is common for all databases. In future we would like to input the secret key for a database from the user and the same key will be used for encryption or decryption of data corresponding to that database. In this way there can be a one to one correspondence for the secret key used and the database. We can also implement a feature where user can change the secret key at any point of time and the entire content present in the database will be re-encrypted for the new secret key given. In this way we can ensure even more high security to the data.

References

[1]. William stallings "Cryptography and Network Security" 3rd Edition published by Pearson Education Inc and Dorling Kindersley Publishing Inc. Advanced Encryption Standard (AES), Nov. 26, 2001

[2]. ShrivathsaBhargav, Larry Chen, AbhinandanMajumdar, and Shiva Ramudit, "CSEE 4840 128-bit AES decryption", spring 2008, Columbia University, pages 4-6.

[3]. G.L. Heileman, "web application architectures", module 1, lecture 4,University of NEW MEXICO.

[4]. Dorothy E. Denning, and Peter J. Denning, "Data Security", Computer Science Department, Purdue University, Indiana.

[5]. Sumeet Bajaj, and RaduSion, "TrustedDB: A Trusted Hardware based Database with Privacy and Data Confidentiality", IEEE Transactions on Knowledge & Data Engineering, Issue No.03 - March (2014 vol.26) pp: 752-765.

[6]. Elisa Bertino and Ravi Sandhu "Database Security—Concepts, Approaches, and challenges ",IEEE Transactions on Dependable and Secure computing, V0l2,No 1,Jan 2005.