Database Protection System Depend on Modified Hash Function

Alaa K. Farhan
Computer Science Department
University of technology,Baghdad- Iraq
dralaa_cs@yahoo.com

Mohammed Abed Al-jabber Ali
Computer Science Department
University of technology,Baghdad- Iraq
mo_force@yahoo.com

DOI: 10.24086/cocos17.15

Abstract— **the aim of this research is to protect data using enhanced MD5 with 1024 bits length of input block message and output with 160 bits, by using multi techniques. Database is protected using two techniques; first, maintains the integrity of the data by relying on hash technique, as well as enhanced MD5 which is used to generate the password for users with a length of 160 bits; second technique is used to maintain the confidentiality of the data using AES algorithm to encrypt sensitive data.**

Keyword: DATABASE, ENHANCED MD5, AES.

1. INTRODUCTION

There is a set of security demands for a data-base such as physical, logical, and element integrity in addition to auditability, access-control, user-verification, and data-availability. The safety of the actual database is concerned with physical issues connected to data such as power-outages base. Therefore, a data-base must undergo recovery from this type of problems. The integrity of the logical data-base is concerned with the management and preservation of the structures and relations in that data-base [1].

Cryptography is the technique of making the plaintext understandable by the unauthorized parity in which cryptology is made up of, while crypto-analysis (cryptanalysis) try undoing what cryptography attempts to do. [2]

Encryption is the procedure that modifies the message (or is other words the plain-text) for the sake of rendering it insignificant to everybody except the ones that are in possession of the decryption-key. The insignificant message (encrypted message) is typically known as the cipher text. Decryption is the opposite procedure that works on recovering the plain-text from the cipher text [3].

A hash function is a term implemented in the field of the computer sciences a long time ago and it means a function which performs a compression on a string of some input to a fixed-length string. On the other hand in the case where it meets a set of extra requirements, it can be utilized in cryptography applications and therefore called as hash-functions which are of the most vital tools of the cryptographic area and are utilized for achieving a set of security criteria such as authenticity, digital-signatures, pseudo-random number generation, digital steganography, digital time stamping and so on. [4, 5].

The rest of this paper is organized as follows: section 2 provides an overview of the related works, the proposed system details and implantation are presented in section 3, and section 4 presents the conclusions.

2. RELATED WORKS

The objective of this study is combining some function for the sake of reinforcing them and to increase the hash-code's length up to 512 as well, which generates stronger algorithm to face the collision attacks. [6]

The protection and confidentiality of sensitive information in outsourced multi-relational databases is by improving an existing approach based on a combination of fragmentation and encryption. Then a secure and effective technique is defined for querying data hosted on several service providers. Finally, improve the security of the querying technique in order to protect data confidentiality under a collaborative Cloud storage service provider's model [7].

Data security is an emerging concern proved by an increase in the number of reported cases of loss of or exposure to sensitive data by some unauthorized sources. Security is a composed part in which it protects and secures the sensitive data or database management software from some unauthorized user or from malicious attacks. In this paper we will be presenting some of the common security techniques for the data that can be implemented in fortifying and strengthening the databases [8].

3. PROPOSED SYSTEM FOR PROTECTING DB

The following subsections are discussing the implementation details of the proposed system.

3.1 SYSTEM ARCHITECTURE

In this proposed system, the database is protected using two levels. The first one, which is the responsibility of the system, which is relies on enhanced MD5 at the database to protect it against intrusion of the authorize parity, the second protection level is the encryption of sensitive data by the system administrator which is determined in advance based on the stored information about the official of encrypting a column based on AES block Cipher (Advanced Encryption Standard) , the design of this system is based on the strength points of every key length of the this method (i.e. 128, 192 and 256 key length) which are efficient for protecting secret information.

3.1.1 Enhanced MD5

The enhanced method depends on multi techniques such as DNA coding, non- Linear Feedback Shift Register (NLFSR), and Logistic function of Chaos theory. Enhanced MD5 will expand the input of the algorithm to 1024 bits instead of 512 bits, and the output to 160 bits instead of 128 bit.

The complexity try's to increase the data inputs by preprocessing before entrance MD5 operation, where, will use NLFSR and DNA coding in addition the use Logistic function of Chaos theory with each rounds of MD5. In the following steps, the proposed system based on enhanced MD5 will be explained. The Development which based on the MD5 includes amplified complexity against brute force attacks and increase the percentage of probability to know the explicit provision of attackers on the previous algorithm, figure (1) shows one block algorithm of the proposed algorithm.

3.1.2 Enhanced MD5 via classic MD5 for hash value

The enhanced MD5 algorithm applies to messages that have different size as (64byte, 128byte, 512byte, 1KB, 5KB, 10KB, 1M, 5M, and 10M) that encodes process of Milliseconds and the test message in five times for the sake of ensuring that results are clear due to the fact that the CPU can be involved in some other procedure. Table (1) explains the processing-time measured by the Milliseconds that was computed by subtraction from the time of starting the operation and the time of its ending.

Table (1): Time in Milliseconds

File size	Classical MD5	Enhanced MD5
64 byte	00:00:00.0002232	00:00:00.0002297
128 byte	00:00:00.0003828	00:00:00.0004023
512 byte	00:00:00.0005683	00:00:00.0005923
1KB	00:00:00.0006722	00:00:00.0006803
5KB	00:00:00.0007175	00:00:00.0008125
10KB	00:00:00.0007706	00:00:00.0007966
1M	00:00:00.0026558	00:00:00.0027326
5M	00:00:00.0033024	00:00:00.0034589
10M	00:00:00.0043451	00:00:00.0044295

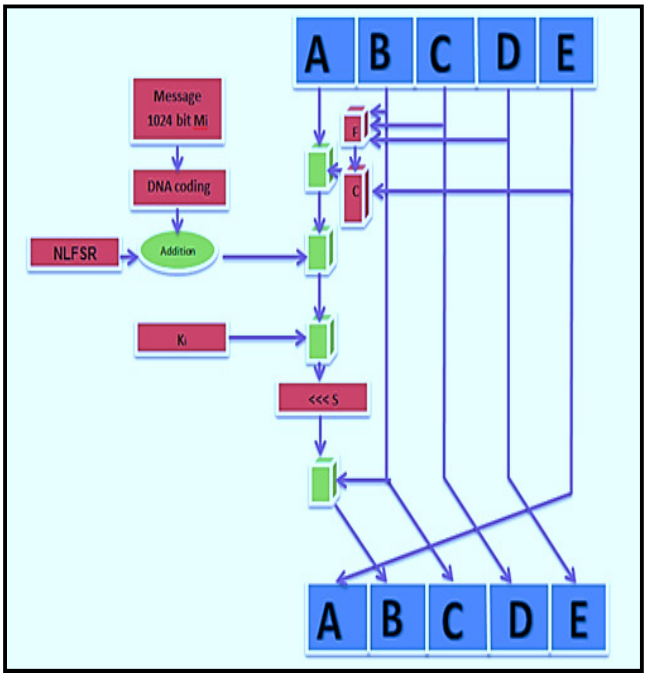

Figure (1): Enhanced MD5 algorithm.

Curves are used to explain the differences in time which have been illustrated in figure (2) below:

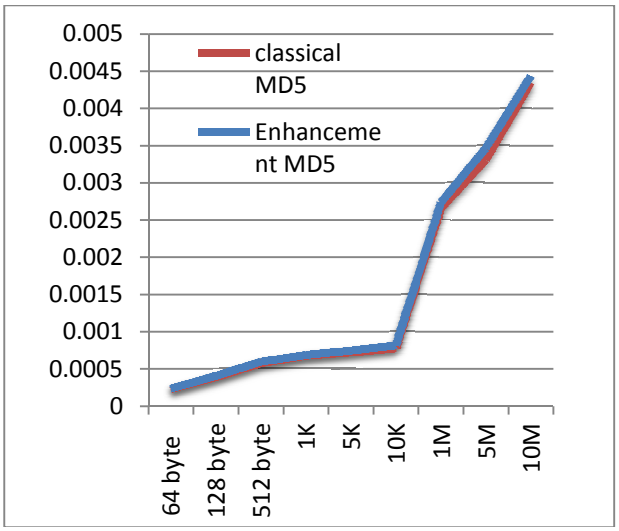

Figure (2): Time of Hashing process.

3.1.3 Complexity Enhanced MD5 via classic MD5

- The MD5 algorithm uses four round each one has sixteen steps, in enhancement add complexity to the round by using DNA coding, logistic function and NLFSR.
- Expand the size of the block message from 512 bits to 1024 bits in the enhancement of MD5 algorithm which led to maintain its speed.
- Generation key form polynomial primitive by using function having GF (2^{32}) this is generates max period number ($2^{32}-1$) binary key, that key is used for preprocessing message, in MD5 original doesn't have key .Enhancement of MD5 puts DNA coding work to convert binary message with key that results from NLFSR in final output new message before entering round. That step is preprocessing message, in MD5 original not preprocessing found is just transposition inside round.
- The MD5 algorithm outputs 128 bits, enhancement algorithm outputs 160. No. Of attacks needed to find original message is 2^{128} bits operations required in MD5 original and needs 2^{160} bits operations.

3.1.3 First phase of Protection DB

The first phase of DB protection would be the responsibility of the system administrator to protect the database. In the first step, proposed system reads first record of table in database and performs the hash function by using the proposed MD5, then, this value is placed in a separate table on the main table for the database. The link between the hash value and the record is the value of prime key. After this step, the proposed system reads value of columns that will be encrypted by AES algorithm which selects data from the encrypted record and then is stored in the new database. Figure (3) illustrates the creation of hash table and the table of encrypted sensitive data. This process is done for all fields in the table, the system takes a period of time to create database protection filed for the server and shared by users through such measuring as the base size and the number of records that the encryption key of AES generated which is based on the number of columns. For example, if the database contains ten columns, the system will generate ten keys; each key is different from the other. This step is exclusively the responsibility of the system administrator and not anyone else who had the authority to generate keys for encryption or log encryption.

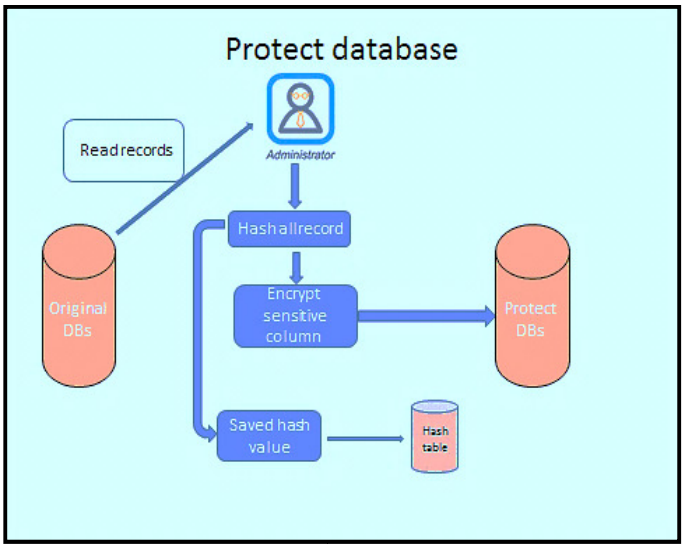

Figure (3): Create hash table to protect database

To create an encrypted table for sensitive data in addition to creating a hash table from the original table, this will be lifted on the server. The following steps explain the steps of encrypted the DB tables:-

1. Read table from database.
2. Read record of table.
3. Apply hash function of data onto the record by using enhanced MD5.
4. Encrypt sensitive data onto the columns by using AES algorithm.
5. Insert hash value in new table.
6. Save table after encrypting data onto new table.
7. Purplish database on server.

After creating a hash table and encrypt sensitive data by the system administrator, columns are encrypted depending on the data that can be filed for the type of server and shared with many users to take advantage of the data according to the nature of the query. Sensitive data encryption process maintains the confidentiality of data and encryption of table maintains the integrity of the data, figure (4) shows the flowchart of restructuring and creating a table of hash and encryption of sensitive.

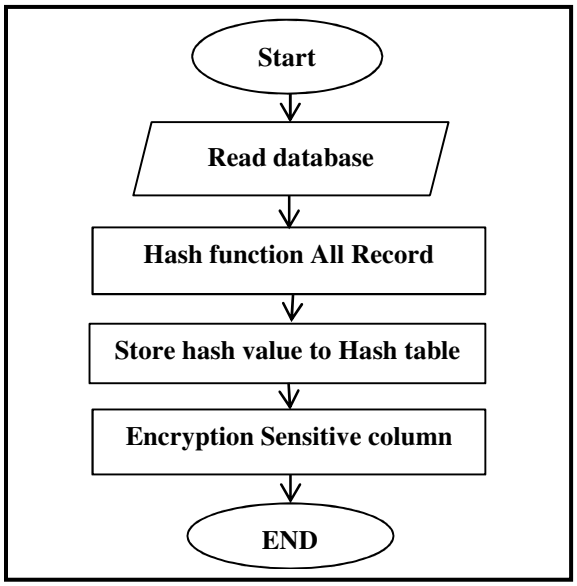

Figure (4): Flowchart of DB protection.

3.1.4 Second phase of DB protection

After put the encrypted database with hash table on the server and work with the participation of everyone, this phase is applied, Here begins the role of the system to be protected, in this section the detailed steps to protect the database is explained also measures to ensure data integrity to deliver it to user with truth.

The common protections for the processes of protecting the database from unauthorized access to the system in all data systems are using user name and password.

The process of accessing the protected data base is through the introduction to user name and password. The password of hash function is processed by enhanced MD5 with size of 160 bites and matches them with passwords stored in the database and when matching the system allows access to the database to be able queries the data.

The operations conducted by users on the database vary according to their powers. This feature is not making all users have the same possibilities in the query and insertions and deletions and update the database.

In the event of the completion of registration of the system, the user can query within the database. The system administrator grants some users free access and limited to be held on the database. When the user name and password entered to the system, a matching process is taking place on the field of accesses to the user to not allowing him/her to hold operations on the system.

3.1.5 System Scenario

In figure (5), system works fully to illustrate the beginning of user login and conduct operations on the database until they return the result to ensure the protection for information.

The following steps describe the scenario of the proposed system:

1. Sends a query to the system.
2. The system receives query from the user if the search for specific data to be matched with the data onto the database.
3. Using SQL language to Search as "select * from * where?", and retune the result.
4. Connect the database with the system.
5. After obtaining the result from step (3), fetch all data of record.
6. Decrypt sensitive data and encoding the record by MD5 enhancement.
7. Connect with hash table and compare results from step (6) with hash store in the table to same record by id number.
8. Retune results to compare process from hash table.
9. Retune results to application.
10. If correct data with no any manipulation retune results to user.

In Figure (6) illustrates the query structural data onto the database, when searching for data encrypted within the database system confirmed the query therefore if encrypted information encrypts the query and research and match. In this section the process of ensuring and match data onto the agenda for her not to make sure that the manipulation and, consequently, if the information was held by any slight change started examining the notice to the director of the system directly.

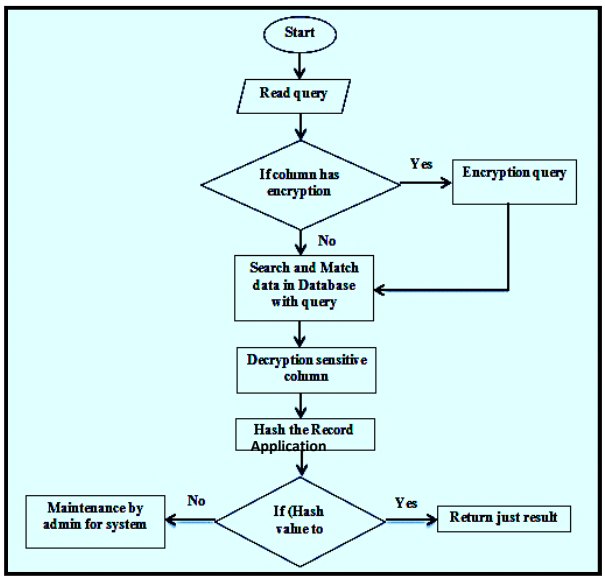

Figure (5): System Scenario

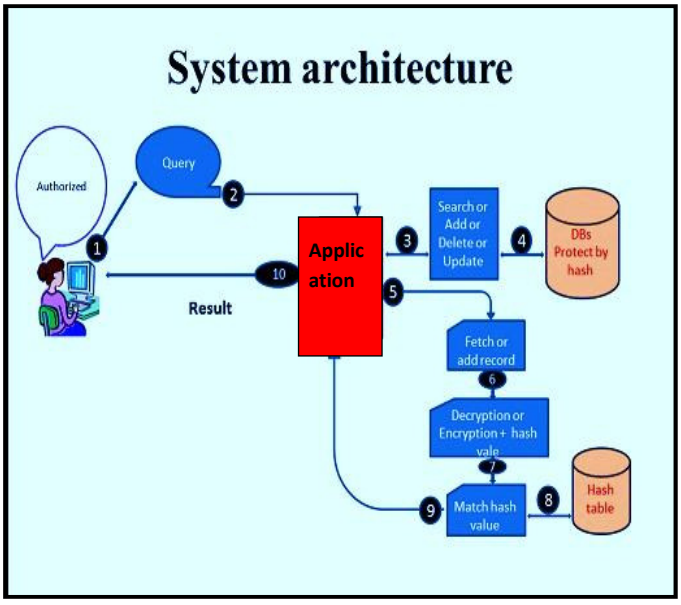

Figure (6): Query structure

4. CONCLUSIONS

Oversized database is difficult to identify data that was manipulated by the attacker and determine the constraint that contains those statements, in the proposed system have the potential to determine constraint depending on the configured hash value (MD5 enhancement) for each constraint and matched with the original version. use MD5 enhancement increased to protect DB to access control , where encoding password has user by it and don't need to add salt to original algorithm when encoding password user in system traditional. Also grants the administrator the flexibility to encrypt sensitive data which reduces the time spent in answering in the program spend in search and decrypt database, the system is a security system help to administrator determine the powers and responsibilities of users to ensure that no tampering by spirited.

Disadvantage of proposed system is the size increment of database by adding tables contain the hash value for each entry and attached file size in algorithm which contains the keys to the size (2^32), through step enhanced MD5 faced slaw of speed the process after adding complexity to it and process by expend block input to 1024 instead 512 to keep of speed the algorithm.

REFERENCES

[1] Saurabh. K. and Siddhaling U.," Review of Attacks on Databases and Database Security Techniques ", ISSN 2250-2459, Volume 2, Issue 11, November 2012.

[2] Anwar Pasha G. D. and Riyazuddin Q., "Transparent Data Encryption- Solution for Security of Database Contents", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 2, No.3, March 2011.

[3] Joseph S. Grah," Hash Function in Cryptography", MS. Thesis, University of Bergen, Norway, June 1, 2008.

[4] Rajeev S. and G. Geetha," Cryptographic Hash Functions: A Review", IJCSI, Vol. 9, Issue 2, No 2, March 2012.

[5] Deniz T.," Cryptanalysis of Hash Functions" PHD. Thesis, Technical University of Denmark, March 2013.

[6] Priyanka W. and Vivek T..," Implementation of New Modified MD5-512 bit Algorithm for Cryptography", International Journal of Innovative Research in Advanced Engineering (IJIRAE), Volume 1 Issue 6 (July 2014).

[7] José M. F. and David G.A.," Preserving Multi-relational Outsourced Databases Confidentiality using Fragmentation and Encryption", Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, volume: 4, number: 2, pp. 39-62, 2013.

[8] Nitasha S.," Database Security: Threats and Security Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 5, MAY 2015.