International Journal of Technical Innovation in Modern Engineering & Science (IJTIMES)
Impact Factor: 5.85 (SJIF-2019), e-ISSN: 2455-2585
Volume 06, Issue 03, March-2020

Encryption Data Webhouse of Enterprise Information System

Dhuha Khamees Khalaf [1] , Murtadha M. Hamad [2]

[1,2]*Department of Computer Science, University of Anbar*
[1] *msc.dhuha@gmail.com*
[2] *dr.mortadha61@gmail.com*

Abstract*— Within the business world, many corporations store, hospitals, universities, prepare and update their data of activities in massive databases. As years pass, massive quantity of records is collected in the systems of the corporations. Because the system grows rapid, some issues in the comprehension and evaluation of the records collected arise. Within the recent years, the idea of data warehouse has all started to seem as a new kind of complicated selection support platforms. These records are organized in a manner so that it will present easy use and extremely good reporting performance. The main goal of making a proposed data webhouse is to allow a better and secured control of the hospital doctors and patients who are inside the hospitals in order to be able to perform evaluation for patients and doctors. In this paper, the proposed data webhouse system is secured by using Advanced Encryption Standard AES technique in order to encrypt all information inside proposed system's database and providing each person username and password so that avoiding any misuse of the system. The records can also be utilized by the proposed a data webhouse website whilst figuring out a hospital policy for different hospitals. The purpose of this paper is to design and develop a data webhouse using AES technique with help of asp.net language and hospital's database of different hospitals. AES technique helps to secure data file which will be upload in proposed system's database. So, the proposed system will be secure all patients and doctors information. Advanced encryption standard technique used in proposed system in order to secure stored data in database. The results of the proposal are good in terms of time. In addition, securing data inside the web protects it from attackers and increases accuracy in dealing with that data.

***Keywords*— Webhouse, Enterprise Information System, Advanced Encryption Standard AES, WebOLAP, Web Analysis**

I. Introduction

The web is used by the warehouse of web-enabled data to record transport and cooperation amongst clients. In the surroundings of a maturing data warehousing, data warehouses were increasingly related to the internet. Basically, an access increase is indicated for records inside the warehouse of data. The boom approach in data access, in flip, is increased within the company's understanding level. Even before it is connected to the web, access may be provided to records to many clients in addition to a lot of issues and a corresponding increase in the expenses of communication. All that has been changed with the invention of the internet. Nowadays, more clients have become much easier to be added[1].

End-user software developers are developing more and more programs about internet pages. The desire for a user-interface developmental environment is now the development of the internet page environment. A new shape of the warehouse of data is represented by the webhouse. The web which presents great data resources helps collect information from different resources and then integrate them. The decisional platform is to be secured because of the critical sensitivity of the records stored in the data webhouse (DWB). In the context of the internet, the information mega-volumes help in growing a wide variety of clients and the necessities of being heterogeneous present difficulties like the data nature, the resources' lack of control, and data modification frequency (See "Fig 1")[2].

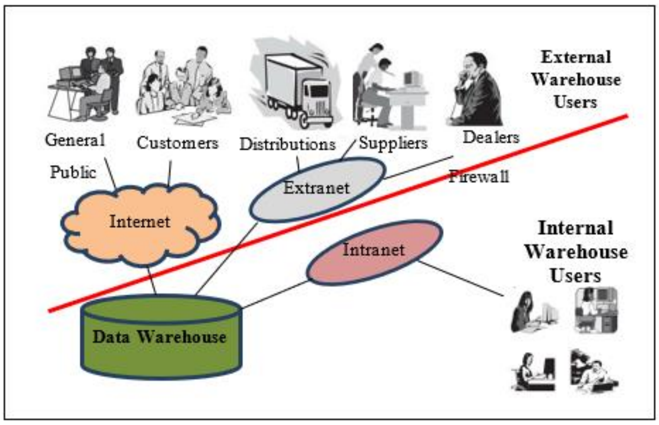

Fig. 1 Warehouse of Data and The Web.

In general, an enterprise system is composed of a suite of different modules. Typical modules include executive direction and support, customer integration, engineering integration, manufacturing integration, and support service integration. An enterprise can make its enterprise systems available by integrating a number of modules such as sales, quality management and accounts receivable, communicate and share data[3].

Achieving reliable storage of remote servers and securing the transfer of outsourced data between two clouds are hard to achieve. This is because, firstly, the web does not provide the users with enough storage space to retrieve their data temporarily. Secondly, the providers of the cloud storage providers are not all totally trusted and because of many motivations, Clouds behave dishonestly towards users regarding their outsourced data[4]. Transferring data from one cloud to another causes concern to the data owners about the intactness and the confidentiality of their data because they have no physical control over them. Despite of the effective techniques of data encryption like "Advanced Encryption Standard" (AES) that presents effective data protection, data corruption threats still present serious concern to the users[5] [6]. A simple user mistake can bring about an overwritten or deleted document. Moreover, lost devices like tablets or smartphones may lead the company documents to fall into the wrong hands. No matter what the form of a data breach is, the corporation will certainly experience severe consequences like downtime and costly legal charges. It is consequently vital that corporations hire data security mechanisms and tactics to guard the data against threats and to guard the brand reputation[7].

II. RELATED WORKS

This section presents several previous studies that tackle Webhouse which are close and related to our study.

- Musliyana, Zuhar et al. (2016) [8] propose an approach handling encryption data by using Advanced Encryption Standard (AES) algorithm. The study was to encrypt the system's data over the web. In addition, the study modifies the key scheduling of the algorithm. The study obtained good results for encryption data. The execution time was significant in the implementation of encryption and decryption operations.
- Dammak, Salma et al. (2017) [9] propose an approach handling security requirement for the designer of Web-ETL processes named Goal-Question-Vulnerabilities-Metric (GQVM) and uses the XML for design. The GQVM approach proposes a quantitative security method of measurement in ETL procedures on the Web. Software standard Common Vulnerability Scoring System (CVSS) was adopted as a score factor of measuring the sever impact of vulnerabilities of different categories.
- Chen, I-Min A. et al. (2019) [10] deal with the web-enabled data warehouse designed for community health decision support: the catch platform revolutionized aid allocation and health care policy components in a comprehensive and systematic way. The advantages of building the DSS warehouse consistent with the authors are: (a) it makes it feasible for local decision-makers to arrange and interpret the information genuinely; (b) produces some core reviews for local groups at an affordable price; (c) in combination with the web, the data can be provided in a spread of codecs and allotted more extensively within the community. But, the authors of this paper do not properly address the high-level dimensional modeling and layout required for a complex platform.
- Dhuha Khalaf and Murtadha Hamad (2019) [11] proposed most optimal and simplest algorithms for handling and controlling data from institutions. The algorithms were for entering, cleaning data for webhouse and display fragmentation with OLAP. The methods used yield excellent results in terms of data recall and performance. The performance of the user leads to good results in appropriate decision making. The time taken to extract the inventory data was good depending on the Internet service.

III. THE PROPOSED WORK

The proposed system implements ASP.net in visual studio 2015 with C# as a programming language and Structured Query Language (SQL) Server 2014 express LocalDB as data storage language. Each one has its own criteria to make suitable use of it. The ASP with C# is strong support for the establishment of Web interfaces using the language options in the auto addition page. The ASP uses the graphical interface tools as well as the tags for HyperText Markup Language (HTML) and Personal Home Page (the original name for PHP server-side scripting language (PHP)).

IV. DATA RESOURCES

Data handled by data Webhouse must be clean and integrated. Therefore, the data healthcare must be within the study area in the same specifications. Official communications and audits to hospitals and health centers were of little use, with little electronic data available to be used within the proposed work. The data used were collected from Al-Hussein Teaching Hospital in Dhi Qar Governorate. The data were entered in 2017 electronically into the Excel program and handled for export to the webhouse. The number of records entered in the hospital was 57,600 records, representing a very small number compared to the data volumes in the data warehouses. Therefore, these data were added manually. The added data were in the same format as the previously entered data. All data were cleaned by the proposed algorithm before being added to the webhouse. This Data webhouse was used from study [11].

V. ENCRYPTION VIA AES ALGORITHM

After the data are cleaned up, they can be easily handled on a webhouse where they are encrypted. The AES encryption algorithm is used because it has a high level of security despite numerous attempts to break its encryption. AES is specifically designed to replace the aging Data Encryption standard, its choice procedure started back in January 2, 1997, by National Institute of Standards and Technology (NIST) of the United States of America while they summoned world's best minds within the field of cryptography to cooperate through providing their ideas for a new encryption algorithm to be known as advanced Encryption standard. AES Algorithm uses three different key sizes which are 128 bits, 192 bits, and 256 bits (See "Fig 2"). A 256-bit encryption key was used in the proposed work. The proposer assumes there is a private server running a private key exchange for this algorithm with encryption for each site. The steps of the AES 256-bit algorithm are as follows:

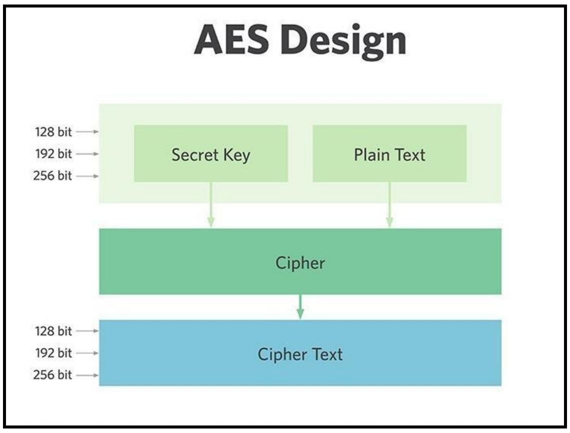

Fig. 2 Advanced Encryption Standard (AES) Algorithm Design.

AES Encryption Algorithm

- **Input**: Data will be divide by 128-bit to enter (Plaintext), Secret Key as 256-bit
- **Output**: Collect 128-bit to find text (Ciphertext)

Start

Part I: Key Scheduling

Input: Secret Key as 256-bit

Output: Fifteen Keys (128-bit)

step 1: The element of the original input key is arranged in byte-wise such as K0 K1 … … … K15 K16, … … … … K30, K31, starting from most significant byte to least significant byte key length. It is divided into four words and each is the equal size of 32 bit hence form 8 words in each row.

step 2: All the subkeys are stored in key expansion array with elements W[0], W[1], … ... W[59] because there are 15 subkeys used for maintaining 14 rounds and 7 iterations are required. The first subkey K0 is obtained from taking firsts four words starting from the original key of AES and the key is copied into the first four elements of key array [W0, W1, W2, W3]. The second key is obtained from the least significant 4 words of the original keys [W4, W5, W6, W7] each word of size 32 bit and remaining subkeys are obtained by the steps below.

step 3: The two functions g() and h() are computed where g() is computed over the least significant word of key length that rotates its 4 input bytes, then performs byte-wise S-box substitution and adds Round Coefficients(RC) that is an element of Galois Field(2^8) i.e. an 8-bit value. It adds only the leftmost byte in the function g() and the round coefficient varies from iteration to iteration.

step 4: All other elements of the array are computed as follows: the left most word of the key of iteration 1 to 7 are $W[6 * i]$ where i = 1 to 7

a. $w[8 * i] = W[8 * i] + g(W[8 * i - 1])$

b. $W[8 * i + j] = W[8 * i + j - 1] + W[8*(i - 1) + j]$ where i =1 to 7 and j = 1,2,3

c. $W[8 * i + j] = h(W[8 * i + j - 1]) + W[8*(i - 1) + j]$, for i =1 to 7 and j = 4

d. $W[8 * i + j] = W[8 * i + j - 1] + W[8*(i - 1) + j]$, for i =1 to 7 and j = 5,6

step 5: After computing all the elements of word Matrix [W0,W1,………..W59] , we compute 15 sub keys starting from K0 to K14 by taking first four words for making K0 = [W0, W1, W2, W3], K1 = [W4, W5, W6, W7], … … K14 = [W56, W57, W58, W59].

Part II: Encryption Algorithm

Input: Plaintext, Fifteen Keys (generated by Part I)

Output: Ciphertext

step 1: Initialize the state array (4×4) with the plaintext data.

step 2: Add Key (K0) to Plaintext by using bitwise operation (eXclusive-OR).

step 3: For (i = 0 to 13)

a. The SubBytes phase involves splitting the input into bytes and passing each one through a Substitution Box or S-Box, AES uses the same S-Box for all bytes. The AES S-Box implements inverse multiplication in Galois Field 2^8.

b. ShiftRows operation, each of these rows is shifted to the left by a set amount: their row number starting with zero. The top row is not shifted at all; the next row is shifted by one and so on.

c. MixColumns phase provides diffusion by mixing the input around. MixColumns perform operations splitting the matrix by columns instead of rows. Unlike standard matrix multiplication, MixColumns perform matrix multiplication as per Galois Field 2^8. It is important to note that this multiplication has the property of operating independently over each of the columns of the initial matrix, i.e. the first column when multiplied by the matrix, produces the first column of the resultant matrix.

d. The key (i+1) generated is used as the round key input to the AddRoundKey operation. AddRoundKey operation uses bitwise operation (eXclusive-OR) for adding the key to round. An identical transformation on the round key is performed to produce the next round key.

step 4: The final round includes three operations (SubBytes phase, ShiftRows operation and AddRoundKey operation - Uses the last key generated-)

step 5: Convert array stat to the string, the string will represent the ciphertext of the entered text.

End.

VI. DATA WEBHOUSE STORAGE

The data Webhouse must be in a more secure location to protect it from tampering, damage or loss. Data are generally held on hard disk drives of computers whether internal or external. It can save data on CDs but may not be safer than hard disk drives added to the specified capacity. By using the Web, all developed countries provide online storage space. The storage spaces can be accessed through the selected Internet. The important two determines are server and services. The server is very important in securing data storage as it depends on the choice of where to store data for the Webhouse. This protection is a service that must be identified with the server as a service. Some companies provide storage space with a range of services to beneficiaries. One of the most important services is how to securely store data and keep it safe from hacking. Also, the companies provide secure data paths and email groups to track the movement of the data. The companies add many services, including data analysis and fast processing in addition to other services. The site of the server is chosen based on the security strength and fast data exchange according to storage capacity and cost. The data security power is represented by encryption in storage, which is a service provided by some provider's sites. This service may be expensive for customers but lead to high confidence in storing data. Data are gradually magnified daily. They require testing the server that its storage can be automatically increased. Because of the use of the Internet, there are a lot of attackers on the network who grab data to take advantage of tampering with. So, the path is the gateway to the data Webhouse and to where the attackers access it. It can show the path that it goes back to a government institution, university, organization or others which give the path more secure through the Web.

VII. SYSTEM EVALUATION

A simple website is designed to implement the proposal. The design is corrupted from easy pages that implement encryption and decryption. The purpose of this page below in the proposed system is to encrypt data files before being uploaded into a data webhouse system database (See "Fig 3"). The encrypted file is encrypted by AES Algorithm. All encrypted files will be in the form of _enc, as shown "Fig 4".

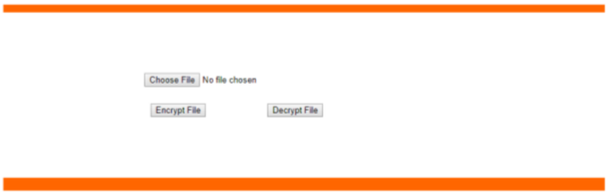

Fig. 3 Choosing Encrypted Data File.

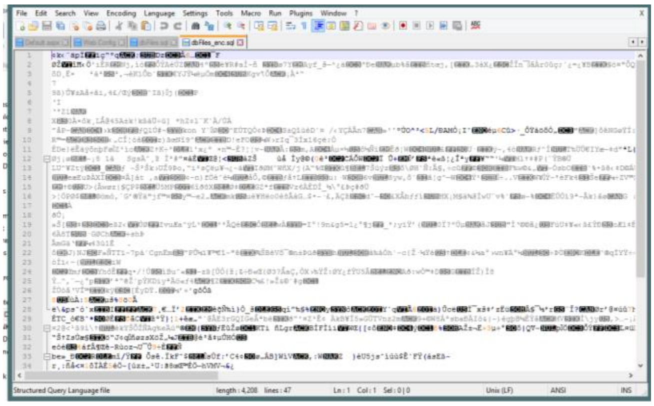
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
dbFiles_enc.sql
Structured Query Language file
length : 4,208 lines : 47
Ln : 1 Col : 1 Sel : 0 | 0
Unix (LF)
ANSI
INS

Fig. 4 Encrypted File.

The decrypted file is decrypted by the AES Algorithm. All decrypted files will be into the original form with _enc_dec, as shown in "Fig 5".

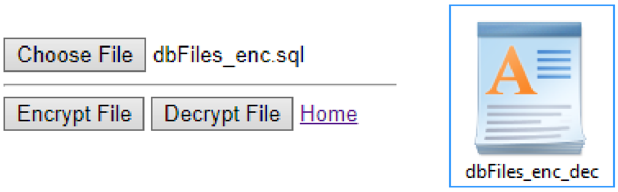

Fig. 5 Choosing Decrypted Data File.

The time it takes to encrypt clean data within the proposed system is 10-4 seconds. This time was measured in encryption of the uploaded data on the web. The execution time is only for encryption without other proposed system actions and also without the time of uploading data to the server. Table 1 shows the results obtained in the proposed system with the previous study [8] which used the AES encryption algorithm to secure data over the web. The same volume of previously studied data is encrypted for the best comparison.

TABLE 1
Compare Execution Time between Previous Study and Proposed Work

File Size (kb)	Execution Time based on Previous Study	Execution Time based on Proposed System
10 kb	5300	5200
15 kb	7950	7800
20 kb	10600	10400
25 kb	13250	13000
30 kb	15900	15600

It is clear from the table that the proposed study was faster in the implementation of data encryption in various file sizes. The speed of execution depends on the cleaning data used within the encryption. Also, improvements were made to the AES encryption algorithm while the basic algorithm was adopted in the proposed system.

VIII. CONCLUSION

In this paper, we encrypted the data stored inside the webhouse. This step is very important in securing data for Enterprise Information Systems. In the increasing number of piracy operations, we are required to keep data more safely. The data encryption service on the web is based on two principles: the speed of the available internet and the algorithms used. The AES algorithm was used and is safe to use as it was used in a 256-bit case. Good results were obtained in terms of speed compared to previous work, where the wick took to encrypt clean data was 10-4 seconds. The study suggests using two-key algorithms where the public key is generated from the system login process.

REFERENCES

[1] P. Ponniah, *Data Warehousing Fundamentals for it Professionals*, Second Edi. Canada: Wiley & Sons, Inc, 2012.

[2] S. Dammak, F. G. Jedidi, and F. Gargouri, “Security Measures for Web ETL Processes,” *Comput. Inf. Sci.*, vol. 614, pp. 13–27, 2016.

[3] O. González-Rojas and L. Ochoa-Venegas, “A decision model and system for planning and adapting the configuration of enterprise information systems,” *Comput. Ind.*, vol. 92–93, pp. 161–177, 2017.

[4] Y. Wang, X. Tao, J. Ni, and Y. Yu, “Data integrity checking with reliable data transfer for secure cloud storage,” *Int. J. Web Grid Serv.*, vol. 14, no. 1, pp. 106–121, 2018.

[5] P. Kodeswaran, V. Nandakumar, S. Kapoor, P. Kamaraju, A. Joshi, and S. Mukherjea, “Securing enterprise data on smartphones using run time information flow control,” in *IEEE 13th International Conference on Mobile Data Management, MDM 2012*, 2012, pp. 300–305.

[6] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends,” *Proc. - 2017 IEEE 6th Int. Congr. Big Data, BigData Congr. 2017*, pp. 557–564, 2017.

[7] T. Lead, “Data Mining with Big Data,” in *Proceedings of 2017 11th International Conference on Intelligent Systems and Control, ISCO 2017*, 2017, pp. 246–250.

[8] D. Qiu, J. Liu, and G. Zhao, “Design and Application of Data Integration Framework Based on Web Services,” *Comput. Technol. Dev.*, vol. 2016, no. 11, pp. 253–256, 2016.

[9] P. Patil, “Application for Data Mining and Web Data Mining Challenges,” *Int. J. Comput. Sci. Mob. Comput.*, vol. 6, no. 3, pp. 39–44, 2017.

[10] J. Barnes, “Getting started with Azure Machine Learning,” *Azur. Mach. Learn. Microsoft Azur. Essentials*, 2015.

[11] D. Dhuha and K. Khalaf, “Data Webhouse for Monitoring the Use of Enterprise Information System,” in *12th International Conference on Development in eSystem Engineering*, 2019.