IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 10, Issue 4 (Mar. - Apr. 2013), PP 63-70
www.iosrjournals.org

Privacy and Security in Online Examination Systems

Omar Zughoul[1], Hajar Mat Jani[1], Adibah Shuib[2], Osama Almasri[1]
[1(]*College of Information Technology, Universiti Tenaga Nasional, Malaysia)*
[2]*(Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA (UiTM), Malaysia)*

Abstract : *A new method for key generation using Data Encryption Standard (DES) is proposed in order to make it more secure for Online Examination System (OES). Privacy and security are crucial in an OES. Privacy represents the ability to maintain a personal space such that there is certain user control on what and how much of personal information can be shared with others. Security describes the level of data integrity and protection the system offers. There are two main factors that affect the student's privacy and security in an OES: exam score and impartiality. The exam score is encrypted before being saved in the database and can only be accessed by the respective authorized student. Impartiality is accomplished by using the proposed cryptography scheme that encrypts the student's identification before sending the paper to the examiner for grading.*

Keywords – *Online Examination, Privacy, Cryptography Scheme, DES*

I. INTRODUCTION

Online Examination System (OES) has become important in e-learning because it reduces costs as compared to face-to-face examination. This is due to its paperless activity and time saving ability. OES also offers greater accessibility such that it can include remote candidates and flexibility in assessment in which the examination can be evaluated manually or using an automated system. OES is a powerful tool for e-learning and online education by providing a more efficient platform for creating, conducting, and evaluating examinations. It offers an effective alternative in evaluating students' knowledge, and also improves efficiency and accuracy of the overall examination process. However, privacy and security management has been a challenge to an OES. Security in an OES includes both the security and reliability of data transmission and also the security of data in the OES database. There are three major elements of data security; the first one is "confidentiality". This means that the data is only readable by authorized people. The second is "integrity", which ensures that the data sent and received are the same without any interference or change, and lastly, is "authentication", which basically ensures that users are well-identified [1].

Recently, insider attacks have gathered more attention than outsider attacks [2]. One of the solutions for avoiding the risk of attackers is to encrypt the data inside the database, which means to create a cipher text from plain text. There are two basic techniques for encrypting data; the first one is "Symmetric cryptography", which means using the same key to encrypt/encode and decrypt/decode the data. The second one is "asymmetric cryptography". This technique imposes the use of both the public and the private keys. Symmetric cryptography requires the party encrypting the data and the party decrypting the data to know the private key. Asymmetric permits anyone to use the public key to encrypt the data to be sent but only the person who has the private key can decrypt it.

A few well-known examples of symmetric algorithms are DES, Triple-DES (3DES), IDEA, CAST5, BLOWFISH, and TWOFISH. Well-known asymmetric algorithms are RSA, DSA, and ELGAMAL. Two models that are used in online examination systems are the Browse/Server model (B/S) and Client/Server model (C/S) [3, 4]. The Online examination system that is based on B/S model is easy to maintain and install, and this is considered as a main advantage [5]. On the other hand, C/S model is more convenient for sophisticated processes like "install" and "update". In addition, the examination system based on C/S executes faster than the system based on B/S [6].

This research study focuses on the encryption algorithm of an OES. The paper is organized as follows: an overview of OES and security of data in OES is discussed in Section I; the literature review is given in Section II; Data Encryption Standard (DES) algorithm is described in Section III; the proposed method is explained in Section IV; the framework is presented in Section V; and lastly, the conclusion and future work of this paper are provided in Section VI.

II. LITERATURE REVIEW

2.1. Introduction

In this section, we describe the reviews and research performed pertaining to privacy and security of online examination. This section contains information on OES and the encryption algorithms used to encrypt

the database. It also contains information on database security and the methods or techniques used in database security.

2.2. The security of online examination system (OES)

Zhang et al. [7] created a web-based examination system for computer education. They divided the system into four subsystems: preparation, examination, monitor, and auto-grading. The authors proposed methods to handle security problems. For example, a digital certification and the webcam-based face tracking techniques have been applied in their web-based examination and evaluation system.

Guo, Yu, and Yao [8] made their online examination system secure and reliable by using five methods. Data security of system and transmission were discussed, and 3DES was used to encrypt the packages and increase the security. The authors also discussed the issue of preventing the students from plagiarism or any types of cheating. The system will be installed in the PCs inside the labs and students are forbidden to do any processes, except taking the exam. This will prevent students from browsing the Internet in order to cheat.

Jun [6] designed his system as three layer where the first layer is database server layer, the second is business layer, and the third layer is the presentation layer. Siyao and Qianrang [9] discovered two solutions for cheating problems after analyzing the strategy of anti-cheating in online examination system (OES). The first solution is based on algorithm for the automatic generating of examination papers, while the second solution is based on the self-developed ActiveX control to defend illegal operations on the client machines.

Olufisoye and Ola [10] presented an advanced online examination system; the model is a combination of multiple-choice questions (MCQs) with other assessment systems such as long answers, short answers like fill-in gap or true/false questions, and other assessments. Sample users responded that the combined assessment is better than the MCQ alone.

2.3. Database security and privacy

According to Xing-hui and Xiu-jun [11], the best way to protect the database is to encrypt the sensitive data by saving plain text as cipher text and decrypt it while visiting. They proposed a new encryption algorithm based on the hybridization of two algorithms, which are the RSA and IDEA encryption. They took advantage of the efficiency and ease of implementation of the IDEA algorithm and convenience in the key management of the RSA algorithm.

2.3.1. Comparative study on database encryption algorithms

Table 1 below shows the most widely known algorithms that are used in database encryption and how each one works and the differences when compared with DES.

Table 1. Comparative study: database encryption algorithms

Encryption algorithm	How it works	Compare to DES
3DES [12]	Same like DES but it has three keys (56 bits for each one) with 3 options of keys : All key are independent K1 and K2 are independent and K3=K1 All three key are identical (K1=K2=K3)	Is more secure than DES Is much slower than DES Is not in the range of brute force attack
AES [13,14]	Is a sequence of 128, 192, or 256 bits and it makes 10, 12, or 14 round depend on the key Key Expansion (16*(number of rounds)+1 In each round it do four operation which are SubBytes, ShiftRows, MixColumns, and AddRoundKey In last round don't do the MixColumns	It has different structure of DES It is more secure than DES Its slower than DES because of the size of the key.
BlowFish [15]	The length of the key is 64 Consist of two part Key expansion: convert key to 448 bits into sub-key arrays Data encryption: it's occurred through 16 round, each round consist of key independent permutation. All operations is XOR operation	Better performance than DES Worse than DES in time consumption "battery and time consumption " Speed increasing slower than DES because it needs memory
RSA [16]	Generate two large prim number , p and q N=pq , M=(p-1)(q-1) Choose small number e , coprime to M Find d, such that d*e%m =1 Here , publish (e) and (n) as public key , d and n as secret key	More complicated than DES More secure than DES

2.3.2. Comparative study on methods used in database encryption

There are many methods that were used to encrypt the database and to increase the security. We have carried out investigation on these methods and found the best six methods used in database security. Table 2 shows these methods.

Table 2. Comparisons among six algorithms used by the six best methods

Methods	Algorithms
Mixed Cryptography Technique based on data classification methods [17]	Any symmetric Encryption algorithm can be used
Hash Security Module Encryption Strategy [18]	State of the art algorithm and mode of operation should be used.
Transparent Data Encryption used by Master database key [19]	Any algorithms can be used
Fast Comparison Encryption [20]	Symmetric Encryption algorithm
Hybrid cryptography encryption program [11]	IDEA combined with RSA
Light-weight database encryption method [2]	Use TSFS (Transposition, Substitution, Folding, Shifting)

2.3.3. The advantages and disadvantages of each method

Each method has its advantages and disadvantages. For example, Ge and Zdonik [20] highlighted the advantages and disadvantages in the "fast comparison encryption methods". The advantages are fast indexing operation and low decryption overhead. Being protected is the only disadvantage of these methods or techniques.

Kadhem, Amagasa and Kitagawa [17] reported that the "Mixed Cryptography Technique method" has two advantages and two disadvantages. The first advantage is that the sensitive data are protected from attacks even at multiple levels because of having many keys to different parties, whereas the second one is secure data storage and data transmission, which is performed to ensure the maximum protection of sensitive data. However, at the same time, this method has disadvantages. The first one is that performance of queries and security analysis is affected because of encryption algorithms, while the second one is access control methods are not defined.

Bouganim and Guo [18] found that although the "Hash Security Module Encryption Strategy" method is complicated, it has two advantages; the first advantage is that Security server is not tampered, and the second advantage is that Encryption keys are hidden.

Xing-hui and Xiu-jun [11] designed a hybrid cryptography encryption of IDEA and RSA. They analysed and compared the advantages and disadvantages of symmetric and asymmetric key encryptions before choosing these two algorithms. The main advantage of RSA is its convenience in key management and the core advantage of IDEA is that it shows high efficiency and makes implementation easy.

Manivannan and Sujarani [2] wanted to improve the efficiency in protecting just the sensitive data; so, they focused just on the security solution. Through "light-weight database encryption method", this method uses the TSFS (Transposition, Substitution, Folding, Shifting) algorithm. Because their method provides maximum security to the database and increases the process of encoding/decoding, they considered it efficient.

Deshmukh and Qureshi [19] considered the "Transparent Data Encryption used by master database key" method as a weak method because it has many disadvantages. One of its disadvantages is that Database could not be opened if the certificate is not available and the backup of certificate and private key is not maintained. The other advantage is that encryption within communication channels is not provided. They found that changing the certificates to be protected by password after being used by transparent data encryption method will affect the database and makes it inaccessible after restarting it. In addition, they found two advantages, which are the cost of user management is reduced, and privacy management is provided.

III. DATA ENCRYPTION STANDARD (DES)

3.1. Introduction

Data encryption standard (DES) algorithm is a strong cipher; however, according to Grabbe [21], its key length is too short to provide much security against a "well-financed" attacker. Moreover, DES is a block cipher algorithm, which means that it takes a fixed length of the message and encrypts it (encrypts the block), and returns a string of the same size. DES is the first encryption algorithm recommended by NIST (National Institute of Standards and Technology). It has been developed in the early 1970s by IBM for NBS (National Bureau of standards). After that, in 1976 the NBS selected a modified version of DES after deliberation with the NSA (National Security Agency) and published for the US in 1977 as a Federal Information Processing

Standard (FIPS) [22]. After 25 years of researching and analyzing, researchers found that the only security problem with DES is its key length which is too short [23].

DES algorithm has been a popular secret key encryption algorithm, and it is used in many commercial and financial applications. Although it was introduced in 1976, it has proven resistant to all forms of cryptanalysis. However, as stated by Chang [24], its key size is too small by current standards and its 56-bit key space can only be searched in approximately 22 hours. Fig. 1 below shows how DES algorithm works [25]:

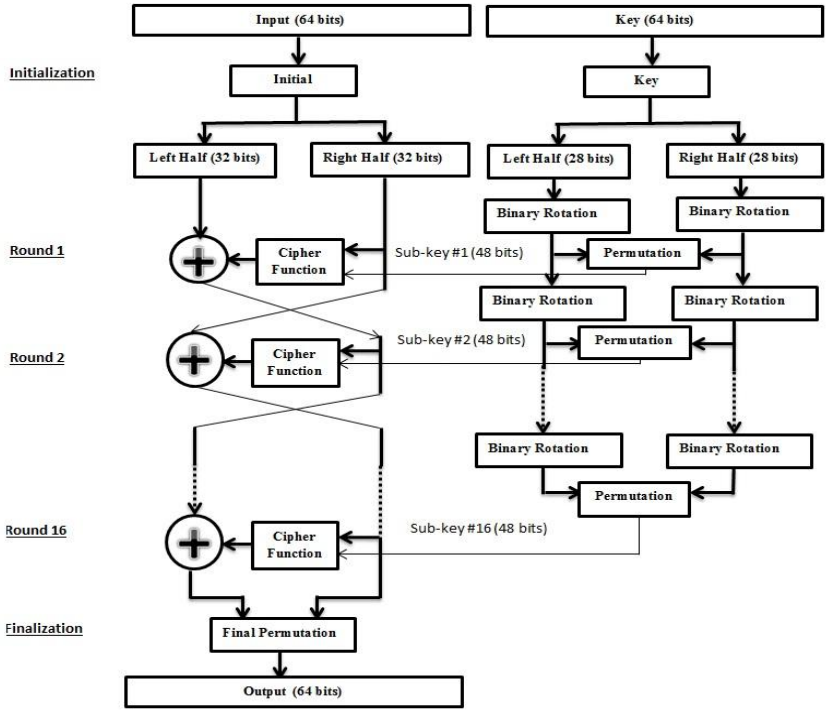

Figure 1. The DES algorithm [25]

3.2. Descriptions of DES

DES is a symmetric algorithm that consists of one key for encryption and decryption. In this section, we will explain the process of DES encryption and DES decryption. But, first, we will define the concepts and what do they stand for. Some notations that will be used in the next sections are given as the following:

(M): Message
(K): Key
(PC1): Permuted choice 1
(PC2): Permuted choice 2
(E): Expansion function
(IP): Initial permutation
(IP^{-1}): Final permutation
(S-box): Substitution box

There are two steps to encrypt the message using DES, the first one is *key generation* and the second one is the *message* itself. We will start with the general description of key generation.

3.2.1. Step 1: key generation

The key of DES algorithm originally consists of 64 bits. It is reduced to 56 bits through a fixed table which is called PC1 (Table 3). The new key has 56 bits; here, the key splits into two parts or two 28-bit halves. The first one is called C0 and the second one called D0, where each one consists of 28 bits. To get C1, D1, both C0 and D0 are rotated one bit to the left using a fix table, which is called shifting table or iteration (Table 4). Then, C1 and D1 are combined to get the 56 bits, out of which we choose the 48-bit key K1 using the key choice table called the permuted choice table 2, or PC-2 (Table 5). To generate all keys, the same steps in generating the first key are repeated for 16 rounds. In general, for each key Ki ($i > 0$), Ci and Di must first be obtained by rotating each Ci-1 and Di-1 one bit to the left, respectively, using the shifting table (Table 4), i.e., C1 and D1 are obtained from C0, D0, C2 and D2 from C1, D1, and subsequently, Cn and Dn are obtained from Cn-1, Dn-1, where n takes the value from 1 to 16, because DES has to undergo 16 rounds for the keys and messages. Then, the 48-bit key Ki is produced by combining Ci and Di and using PC-2. That is, C1 and D1 are

used to generate the key output K1 by combining them and permuted the combination using PC-2, C2, and D2 to generate K2, and so on until finally, Cn, Dn are combined and permuted to get Kn, where n is from 1 to 16.

Table 3. PC-1 [21]

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

Table 4. Iteration [21]

Round :	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Left Shifts:	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Table 5. PC-2 [21]

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

3.2.2. Step 2: the message

DES (and most of the other major symmetric ciphers) is based on a cipher known as the Feistel block cipher. The basic principle of Feistel ciphers is that the plaintext block is split into two halves and each half is used to encrypt the other half over a predetermined number of rounds. Thus, DES is a symmetric, 64-bit block cipher as it uses the same key for both encryption and decryption and only operates on 64-bit blocks of data at a time. In general, DES algorithm divides a message into blocks where each block consists of 64 bits. The encryption begins with an initial permutation using the fixed initial permutation (IP) table that rearranges the 64 bits of the message data in a fixed pattern. The result of the initial permutation is divided into two blocks L0 and R0, and each block consists of 32 bits. Subsequently, DES generates L1 to L16 and R1 to R16 using the formula, which is given as the following:

$$L_j = R_{j-1} \quad (1)$$

$$R_j = L_{j-1} (+) F(E(R_{j-1}), K_j) \quad (2)$$

where j = 1, 2, ... , 16.

Thus, for example, from equation (1), when j = 1, L1 = R0 while R1= L0 (+) F(E(R0), K1) according to equation (2). Equation (2) can be further described as follows. For any j, F(E(R j-1), K j) means that the function F takes the 32-bit R half, i.e., R j-1, and 48-bit sub-key Kj, in which E(R j-1) denotes that the 32-bit R j-1 is expanded to 48 bits using the E-box expansion permutation table. The expansion of R j-1 to 48 bits is because K1 is 48 bits. The result of E(R j-1) is then XORed (+) to the key Kj. Next, the XOR result will then be grouped to 8 blocks where each block consists of 6 bits. This result is then passed through S-Box substitution to get 32-bit result and then the permutation using the P-box permutation is applied to permute the output of the S-box without changing the size of the data. Finally, this result is then XORed (+) to the key Lj-1 in order to get Rj as in equation (2). These steps are then iterated 15 more rounds to produce L2 and R2, L3 and R3 and so on until L16 and R16. The total number of iteration is 16 rounds if including L1 and R1.

At the end of the 16^{th} round, the 32-bit Li and Ri output quantities are swapped to create what is known as the pre-output. Finally, the preoutput is passed through the final permutation (Fb) using the (IP^{-1}). In other words, the final permutation is the inverse of the initial permutation; the table is interpreted similarly, that is IP^{-1} is the inverse of the IP table. This final process is converting the Fb into hexadecimal (the encrypted text) such that the output of $\mathbf{IP}^{-1}$ is the 64-bit cipher text.

IV. THE PROPOSED METHOD

In the second section, which is the literature review, a comparative study between four algorithms that are most commonly used to encrypt database and make it secure has been carried out. These algorithms were also compared with DES algorithm. It is found that the only security problem in DES is its key, which is not very powerful and also too short, as stated by Deshmukh and Qureshi [19]. Thus, the 3DES becomes the choice

to solve this problem of DES. 3DES uses three keys (K1, K2, K3), where each key consists of 56 bits. The plain-text block is encrypted with the first key (K1), then decrypted with the second key (K2) and, finally, encrypted with the third key (K3). To decrypt the cipher text, the functions is reversed, that is decrypt with K3, encrypt with K2, decrypt with K1 and XOR the previous cipher-text block.

As we mentioned in Section 2.3.1, DES is faster than 3DES but, 3DES is more secure than DES [12]. Our system needs an encryption algorithm, which is more secure than DES and at the same time faster than 3DES. We propose a new algorithm, XS-DES (Extra Secure-DES), which is more secure than DES and at the same time faster than 3DES. We propose to increase the size of the key from 64 bits into 128 bits, and split the key into two halves: left and right (Kl, Kr), each one consists of 64 bits. Here, the proposed algorithm will decrease each key to 56 bits by applying the PC-1; after that it will divide each key into two parts (C0, D0). Then, (C1, D1) will be generated from (C0, D0) and the next (Ci, Di), i = 2, 3, ..., 16 will be obtained through similar step iteration. K1 will be produced by combining the left side from Kl (C0 from left key) and right side from Kr (D0 from right key). The last operation is to decrease the size of a key to 48 bits to encrypt the message. Fig. 2 shows our proposed method for the key generation in DES.

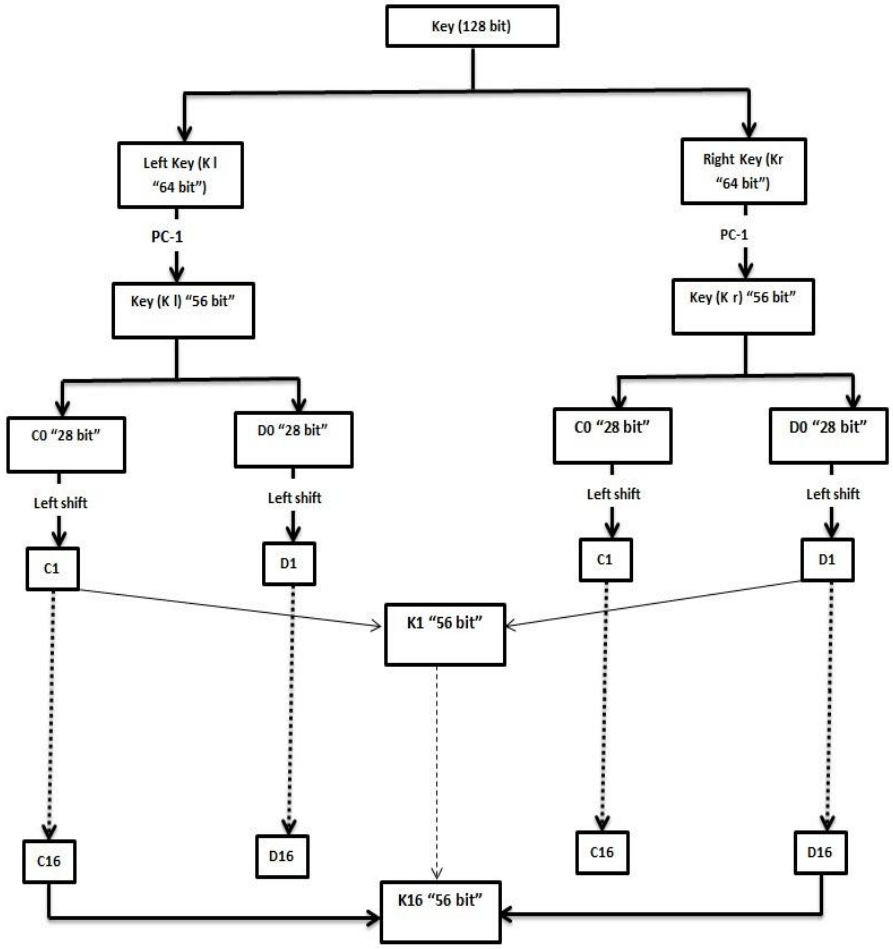

Figure 2. Key generation for XS-DES algorithm

V. THE FRAMEWORK

Our framework is illustrated in Fig. 3. Here, we will explain where we can apply our proposed method to make an OES more secure. When a student enters into an OES, there are two options; the first one is *Login*, which includes the *Admin*, *Examiner* and *Student* logins, and each one has a specified level of authority to perform some tasks. *Admin* can add or delete examinations and he/she also can add or delete *Examiner*. The *Examiner* can just evaluate the exam paper and send the result; he/she cannot see the students' name (or identification), because the system will encrypt the students' name by applying our proposed method. The second option is *Register*, which is meant for new students (without an account).

Once a student logs into the system, he/she has three tasks that he/she can perform. He/she can first select the desired exam file, and secondly (second task), answer and submit the exam; after that he/she can request (third task) for the results. Whenever there is a request for exam results, the OES will send an email containing the decrypted results, but the system will first validate if this student has the authority to see the

decrypted results through the answer given to a security question that has been determined earlier before taking the exam.

It should be noted that the student has to register first to allow him/her to take the exam, and during the registration process he/she must enter his/her name, password, email, and also select a security question (and answer it). If all fields are filled and the username does not exist, then the student's username will be created and stored in the database to allow him/her take the exam later.

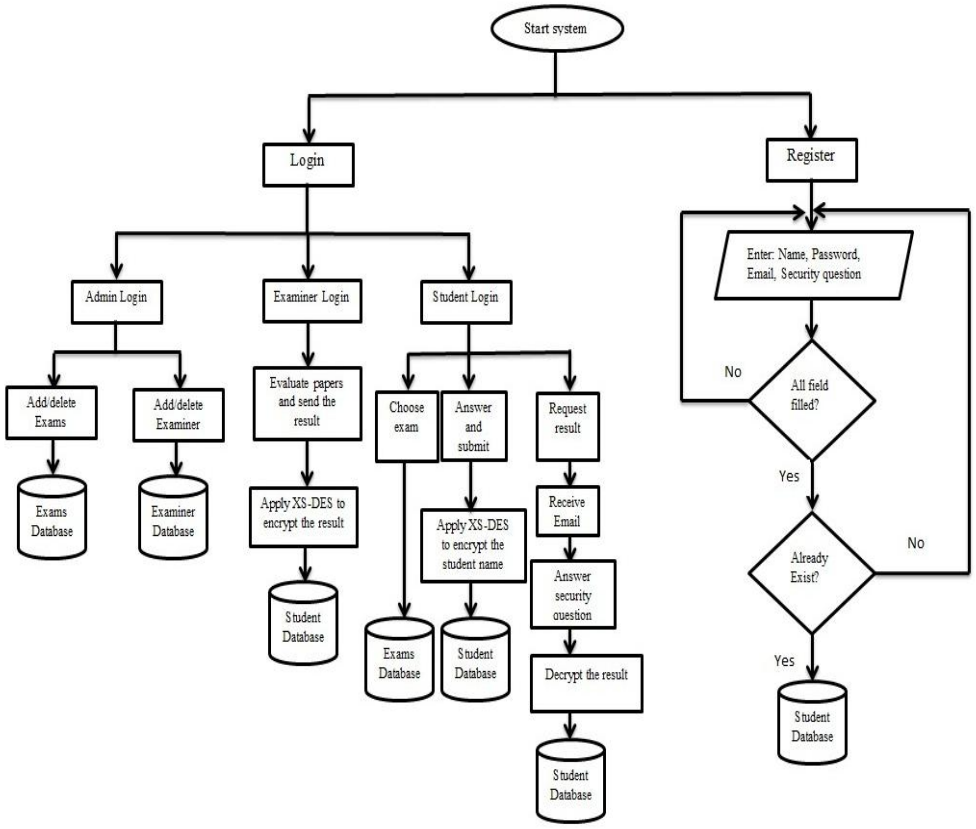

Figure 3. The framework

VI. CONCLUSION AND FUTURE WORK

Online examination or e-exam has become so important in these days because of the rapid evolution in the Internet and education. Online Examination System (OES) is more efficient than face-to-face examination. It is also more economical in the long run because we do not need to print and store papers. In addition, we do not have to invigilate the students to prevent cheating; thus, it also saves time and efforts. As mentioned earlier, privacy and security are the most important elements in e-learning, especially in OES. In this paper, we propose a new method named Extra Secure-DES (XS-DES) for key generation in DES algorithm in order to make it more secure and applicable for OES.

A workable prototype of the OES that uses the proposed XS-DES is currently being developed, and it is hoped that the resulting OES system performs as expected.

In the future, the XS-DES will be applied to other web-based applications related to education and other types of online business applications so that more people can benefit from the proposed encryption method.

Acknowledgement

This research study is funded by the Fundamental Research Grant Scheme (FRGS), Ministry of Higher Education (MOHE), Malaysia.

REFERENCES

[1] R. Raitman, L. Ngo, N. Augar, and W. Zhou, Security in the online e-learning environment, *Proc. Fifth International Conference on Advanced Learning Technologies (ICALT)*, 2005, 702-706.

[2] D.Manivannan and R.Sujarani, Light weight and secure database encryption using TSFS algorithm, *Proc. International Conference on Computing Communication and Networking Technologies (ICCCNT)*, 2010, 1-7.

[3] H.Tan and S. Hou, Design and development of the universal testing system based on LAN, *Journal of Central South University, 31(4)*, 367-370.

[4] Z.Liu, L.Wang and M.Dong, Design and implementation of test paper reviewing system for NIT network-based test, *Journal of Control Engineering of China, 11(2),* 108-110.

[5] R.Hundhausen, S.Borg, C.Francis and K.Wilcox, *Building web applications with ADO. net and XML web services* (2003).

[6] L.Jun, Design of Online Examination System Based on Web Service and COM, *Proc. 1st International Conference on Information Science and Engineering (ICISE)*, 2009, 3276-3279.

[7] L.Zhang, Y.Zhuang, Z.Yuan and G. Zhan, A Web-Based Examination and Evaluation System for Computer Education, *Proc. Sixth International Conference on Advanced Learning Technologies (ICALT'06)*, 2006.

[8] P.Guo, H.Yu and Q.Yao, The Research and Application of Online Examination and Monitoring System, *Proc. IEEE International Symposium on IT in Medicine and Education* , 2008, 497-502.

[9] L.Siyao and G.Qianrang, The Research on Anti-Cheating Strategy of Online Examination System, *Proc. 2nd international conference in Artificial intelligence*, 2011, 1738-1741.

[10] A.Olufisoye and A.Ola, An Integrated E-Learning Examination Model Using Combined MCQ and Essay Based Full Blind Marking Assessment Technique, *Journal of Automation and Control Engineering, Vol. 1, No. 2,* 2013.

[11] W.Xing-hui and M.Xiu-jun, Research of the Database Encryption Technique Based on Hybrid Cryptography, *Proc. IEEE International Symposium In Computational Intelligence and Design (ISCID),* 2010, 68-71.

[12] C.M.Wee, P.R.Sutton, and N.W.Bergmann, An FPGA network architecture for accelerating 3DES-CBC, *Proc. IEEE International Conference In Field Programmable Logic and Applications*, 2005, 654-657.

[13] J.Daemen and V.Rijmen, AES proposal: Rijndael, *Proc. Conference In First Advanced Encryption Standard (AES),* 1998.

[14] C.Sanchez-Avila and R.Sanchez-Reillol, The Rijndael block cipher (AES proposal): a comparison with DES, *Proc. IEEE 35th International Conference In Security Technology*, 2001, 229-234.

[15] T.Nie and T.Zhang, A study of DES and Blowfish encryption algorithm, *Proc. IEEE Region 10 Conference in TENCON*, 2009, 1-4.

[16] D.Boneh, G.Durfee and Y.Frankel, An attack on RSA given a small fraction of the private key bits, *Journal of Springer Berlin/Heidelberg In Advances in Cryptology—ASIACRYPT*, 1998, 25-34.

[17] H.Kadhem, T.Amagasa and H.Kitagawa, A novel framework for database security based on mixed cryptography, *Proc. Fourth International Conference (IEEE) In Internet and Web Applications and Services*, 2009, 163-170.

[18] L.Bouganim and Y.Guo, Database encryption, *Published in Encyclopedia of Cryptography and Security*, 2009, 1-9.

[19] A.Pasha and R.Qureshi, Transparent Data Encryption-Solution for Security of Database Contents, *International Journal of Advanced Computer Science and Applications, Vol. 2, No.3*, March 2011, 25-28.

[20] T.Ge, and S.Zdonik, Fast, secure encryption for indexing in a column-oriented dbms, *Proc. IEEE 23rd International Conference In Data Engineering*, 2007, 676-685.

[21] J.O.Grabbe, The DES algorithm illustrated, Laissez Faire City Times, 2(28), 1992, Retrieved from http://www.orlingrabbe.com/des.htm on Jan 20, 2013.

[22] R.Davis, The data encryption standard in perspective, *Communications Society Magazine, IEEE, 16(6),* 1978, 5-9.

[23] C.Ding, The Data Encryption Standard in Detail, Department of Computer Science, Hong Kong University of Science and Technology, Hong Kong, China, 2000, Retrieved from http://www.cs.ust.hk/faculty/cding/COMP364/SLIDES/readdes.pdf. Jan 29, 2013.

[24] H. S. Chang, International Data Encryption Algorithm, CS-627-1, Fall 2004. Retrieved from http://scholar.googleusercontent.com/scholar?q=cache:WXJPT0eEM7EJ:scholar.google.com/+International+Data+Encryption+Algorithm&hl=en&as_sdt=0,5 on 30 February 2013.

[25] S. William, *Cryptography and network security* (4th Edition., Pearson Education India, 2006).