IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 10, Issue 4 (Mar. - Apr. 2013), PP 55-62
www.iosrjournals.org

Improving Security Measures of E-Learning Database

Osama Almasri[1], Hajar Mat Jani[2], Zaidah Ibrahim[3], Omar Zughoul[1]
[1](*College of Graduate Studies, Universiti Tenaga Nasional, Malaysia)*
[2](*College of Information Technology, Universiti Tenaga Nasional, Malaysia)*
[3](*Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA (UiTM), Malaysia)*

Abstract : *E-learning is a platform that provides materials online with the objective of improving the users' teaching and learning experience. The main objective of this paper is to provide security to users' passwords within the E-learning Password Management System (EPMS) in order to protect the database from hackers. The protection process is done by implementing a symmetric encryption algorithm named International Data Encryption Algorithm (IDEA) on the passwords. The algorithm will be improved by modifying the size of the same secret key that is used in both the encryption and decryption operations of the data. The proposed algorithm is known as Double-Secure IDEA.*

Keywords – *Database Security, E-Learning, Symmetric Encryption, IDEA, Double-Secure IDEA*

I. INTRODUCTION

E-Learning is a platform for providing information online. The rapid evolution of web-based application has led to the utilization of online operations to enhance the learning methods. One of the methods used in e-learning environment is displaying the marks sheets or certificates to the user. But, the materials must be protected from any modification or piracy. The data protection is performed by implementing some security measures. The most common security measures are confidentiality, integrity and availability (CIA) [1].

Database security refers to the protection of the database against unauthorized access that may be intentional or accidental. So, the organizations must take into account the potential threats to their computer system seriously. Database encryption is one of the most effective methods of the database security. It protects the database during the transmission and storage of data. The encryption concept is based on applying a certain encryption algorithm to convert an original message (plain-text) into unreadable message (cipher-text) [2]. The security strength without reducing the system's performance is a critical issue in e-learning systems.

International Data Encryption Algorithm (IDEA) is one of the encryption algorithms that can be implemented in e-learning systems [3]. IDEA is a post-DES algorithm that is widely used because of its high safety, and it covers the Data Encryption Standard (DES) problems. The high speed in encryption/decryption process, resisting difference, and correlation analysis are benefits of IDEA algorithm. It operates on 64-bit plain-text/cipher-text blocks and uses 128-bit key.

According to Alex Biryukov et al. [4], there are large numbers of keys in IDEA that are weak. Because of the attack in round 6 has been detected, the need to increase the security of the algorithm has become paramount [4]. This paper aims to increase the strength of IDEA algorithm by modifying the key-size to make the algorithm more secure, and hence, increasing the diffusion process. Diffusion means one arbitrary bit influences all the cipher-text [5]. The key-size is increased from 128 bits to 512 bits. It increases the algorithm's complexity. The diffusion is increased by using four MA (Multiplicative Additive) blocks that are used in one single round. The algorithm divisions will be running in parallel operation that is suitable for real-time applications especially in online high-speed networks [6].

The proposed algorithm is known as Double-Secure IDEA. It is a modified version of IDEA with four 64-bit sub-blocks of plain-text that are running in parallel. Each round contains four divisions i.e., transformation and sub-encryption. The algorithm still contains eight rounds plus a half-round for output transformation. It uses 24 sub-keys in each round, 16 in transformation round and 8 in sub-encryption round. The final half round uses 16 keys. The total sub-keys are 208 sub-keys in 8+1 rounds. The algorithm is designed in Electronic Codebook (ECB) mode and implemented in an E-learning Password Management System to protect the database materials using encrypted passwords that are stored in a certain database file [7].

II. E-LEARNING

According to Alwi and Fan [8], "e-learning describes the use of the web applications and technologies for improving the learning and teaching experience [8]". Eklund, Kay and Lynch [9] describe e-learning as a form of flexible learning that uses applications such as electronic media. The maturity of e-learning has begun since 1983 when most of the institutions adopted Information and Communication Technology (ICT). Currently, the next-generation web has started through advanced website design to streaming media.

Web applications have become the goal of the threats by using the Internet. Many e-learning institutions do not understand the importance of the security concerns in the ever-present such as reliability, course contents, accessibility and legitimate users. To face the threats and risks that e-learning has, a security risk analysis need to be conducted starting from assets identification to monitoring of the risks [8].

III. DATABASE SECURITY

The development expansion of hardware capability, communications technology, World Wide Web revolution, e-World environment i.e., e-commerce, e-business, and e-learning has made the database as the underlying framework of the information system. Thus, the web database security plays an important role and it has to meet the security measures of confidentiality, integrity and availability (CIA).

Confidentiality (secrecy), integrity, and availability are fundamental resources that should be secured using appropriate controls. Security measures should not hold on the data itself within the database because it may affect the database and the breaches may affect other parts of the system [10]. Confidentiality (secrecy) means protecting the data or information from unauthorized people. Data integrity means protecting the data from any alteration or falsification. Availability means making the information available and easy access to authorized users [1].

Data is a valuable resource that should be controlled and managed. Organizations should keep data confidentiality. The system that has functions and services to manage and maintain data is called Database Management System (DBMS). Authorization services are functions in DBMS to ensure that only authorized users access the database [10].

There are millions of data being transferred everyday via the Internet, and also numerous of operations executing online, such as critical data transfer and online money transfer and transaction. The demand of data security in databases is essential especially the transferring process over unreliable communication networks [11]. The database is the container of stored data. The security relies on the level and the nature of data or information. The organization can determine the level of security of data and information. For example, the database of ministries of defences has a high level of security because the data is critical and the system cannot be accessed by unauthorized users whether inside or outside the organization. The database contains sensitive and important data such that it is necessary to encode it as protection against external threats or illegal access. DBMS can access data after decoding it, but there is reduction in performance because of time, and this consideration must be taken.

3.1. Database attacks

Recently, because of the expansion size in the systems of organizations, the authorization, authentication, and access controls began to be used. But, the security measures or countermeasures became more complex because of the highly sophisticated threats. There are some threats for the databases; for instance, the user who has excessive privileges could abuse his/her privileges intentionally or unintentionally. Data extracted for illegal purposes is called legitimate privilege abuse. The attacker can benefit from the software vulnerabilities to access the sensitive data (Privilege Promotion) or also exploits the operating system vulnerabilities (OS Vulnerabilities) [12].

3.2. Database security techniques

Encryption is a process or mechanism to encode/encipher the sensitive data (plain-text) by a special algorithm (encryption algorithm, such as IDEA and DES) to become unreadable (cipher-text). Some DBMS provides an encryption facility for this purpose. Encryption also protects the data that are transmitted over communication lines. There are some techniques for encoding data to conceal information either irreversible or reversible. Irreversible means not permitting the original data to be known. To transmit data securely over insecure channel or network, the use of the cryptosystem is needed. Cryptosystem includes [12]:

- The data (plain-text) is encrypted by an encryption key.
- An encryption algorithm with the encryption key transforms the plain-text to the cipher-text.
- The cipher-text is decrypted by a decryption key.
- A decryption algorithm with the decryption key transforms the cipher-text back into the plain-text.

There are two techniques of encryption, namely symmetric encryption and asymmetric encryption. A symmetric encryption depends on the safe channel for exchanging the key, and uses the same key in encryption/decryption process. An example of this technique is International Data Encryption Algorithm (IDEA) [3]. Symmetric algorithm is much faster than asymmetric algorithm that uses two different keys (private and public keys) such as RSA (the name is derived from Ron Rivest, Adi Shamir and Leonard Adleman). Generally, they are often used together, in which public key (asymmetric) encrypts a randomly generated encryption key, and the random key encrypts the actual message (using a symmetric algorithm).

Encryption scheme of a database should enhance sharing of data within the database without losing data privacy. The researchers address two impacts, which are, how to enhance the security without reducing the performance and devise some techniques to manage the keys. The contribution of this research is an increase in the security of the database by using a new web database security that has some modules, login module, audit module and program control module. The audit module keeps track of the user's activity in log files and the conformation of legality of the user. The log file is an important approach in keeping track of the user's activities related to the database and the changes that are made in the database [10]. Program control module disallows the user to access to web applications in the system.

3.3. Development of a database encryption strategy

The factors that need to be considered in developing a secure database encryption technique are as follows [12]:

- Encryption basics: The sensitive data should be in encrypted form, legal for authorized users and difficult to decrypt. This depends on the type of the algorithm and key size.
- Influencing the encrypted data on the database applications: Encryption increases the data size and decreases the performance. This determines the type of data that should be encrypted.
- The data flowing in application: The data may be at risk, especially when transmitting the data over the Internet or the internal network.
- Managing the key: The number of keys that are used, the location of stored keys and protecting the access to the encrypted keys need to considered as they have some effects to the level of security of the database.

IV. IDEA ALGORITHM

IDEA is a block cipher described in 1991 by Lai and Massey of ETH-Zürich [3, 13]. It is an earlier cipher, PES (Proposed Encryption Standard) that is a minor revision [3, 13]; IDEA was originally called Improved PES [14]. In the seventies, IDEA was to develop a strong encryption algorithm, which would replace Data Encryption Standard (DES) [15]. It also entirely avoids the use of any lookup tables or S-boxes. IDEA algorithm has some benefits as listed below:

- Resists difference and correlation analysis.
- Encryption and decryption in high-speed.
- It is achievable by hardware and software.

4.1. IDEA description

IDEA is a part of a class of cryptosystems called the secret-key that is characterized by the symmetry of encryption/decryption processes [3]. It is also the possibility of implying the symmetry decryption key from the symmetry encryption key and vice versa. It operates on 64-bit plain-text as inputs and creates 64-bit cipher-text as outputs using a 128-bit key. The design of IDEA is based on mixing operations from different algebraic groups including XOR, addition modulo (2^{16}), and multiplication modulo (the Fermat prime $2^{16}+1$). All these operations work on 16-bit sub-blocks. The IDEA block cipher [5] (as depicted in Fig. 1) consists of a sequential of eight identical blocks known as rounds, followed by a half-round (output transformation). In each round, three algebraic operations are applied. IDEA is characterized as cryptographic strength because its operations consist of three distinct algebraic groups of 2^{16} elements; multiplication modulo $2^{16}+1$ that provides preferable statistical between the plain-text and the cipher-text, and also having iterative rounds made differential attacks difficult [3].

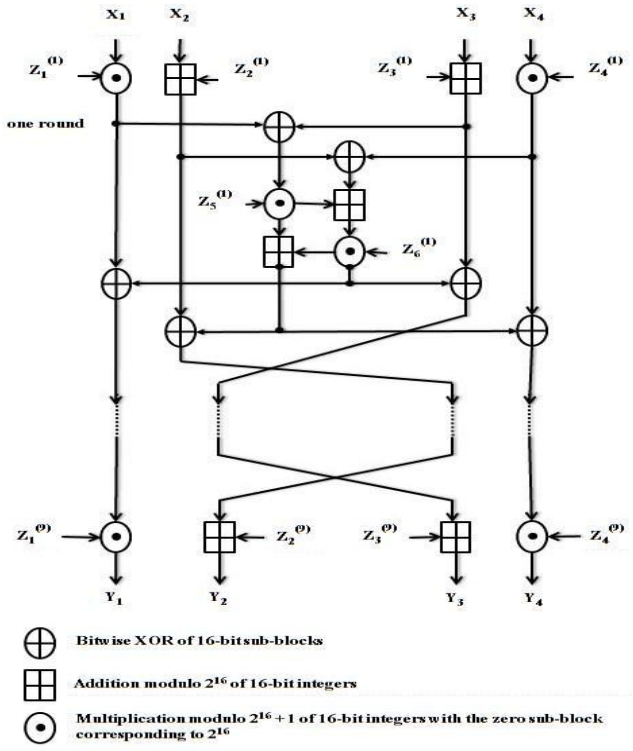

Figure 1. Block diagram of the IDEA algorithm [3, 5]

4.2. Encryption process

The important security characters in the encryption design are confusion and diffusion. Confusion gives the relationship between the plain-text/cipher-text and the key, and it is complex. Diffusion means one arbitrary bit influences all the cipher-text [5]. The confusion consists of three algebraic operations [3]:

- XOR operation $\oplus$ with bit unit.
- Addition modulo $\boxplus$ (2^{16} = mod 65536).
- Multiplication modulo $\odot$ (2^{16}+1= mod 65537).

The plain-text (64-bit) is divided into four 16-bit sub-blocks; X_1, X_2, X_3 and X_4. The algorithm converts the plain-text blocks into the cipher-text blocks of the same bit length, and similarly divided into four 16-bit sub-blocks, Y_1 to Y_4. Fifty-five of 16-bit sub-keys, $Z_i^{(r)}$, where "i" is the sub-key number and "r" is the round number, are computed from the 128-bit secret key. Each round uses six sub-keys and the remaining four sub-keys are used in the output transformation [5].

Computing the encryption sub-keys involves only logical rotations. Arranging the fifty-two sub-keys as "$Z_1^{(1)}, \ldots, Z_6^{(1)}, Z_1^{(2)}, \ldots, Z_6^{(2)}, Z_1^{(3)}, \ldots, Z_6^{(3)}, Z_1^{(4)}, \ldots, Z_6^{(4)}, \ldots, Z_1^{(1)}, \ldots, Z_4^{(9)}$" (as depicted in Table 1) [3, 5]. The process starts with dividing the 128-bit secret key "Z" into eight 16-bit blocks then assigning them directly to the first eight sub-keys. The left rotation of "Z" is done by 25 bits, divided into eight blocks of 16 bits and again assigned to the next eight sub-keys. The procedure continues until all 52 sub-keys are assigned. For a complete round there are fourteen steps as following [13]:

1. First Multiplication between X_1 and the first sub-key Z_1.
2. Addition operation of X_2 with the second sub-key Z_2.
3. Addition operation between X_3 and the third sub-key Z_3.
4. Second Multiplication between X_4 and the fourth sub-key Z_4.
5. Calculating Bitwise *XOR* from the results of steps 1 and 3.
6. Calculating Bitwise *XOR* from the results of steps 2 and 4.
7. Third Multiplication between the result of step 5 and the fifth sub-key Z_5.
8. Addition operation between the results of steps 6 and 7.
9. Multiply the result of step 8 and the sixth sub-key Z_6.
10. Add the results of steps 7 and 9.
11. Bitwise *XOR* the results of steps 1 and 9.
12. Bitwise *XOR* the results of steps 3 and 9.
13. Bitwise *XOR* the results of steps 2 and 10.
14. Bitwise *XOR* the results of steps 4 and 10.

A swap occurs for each round, except the output round (final transformation). The input to the next round is the result of step 11, the result of step 13, the result of step 12, the result of step 14, which becomes X_1, X_2, X_3, X_4, the input for the next round. After round 8, a ninth "half round" final transformation occurs [5]:

- Multiply X_1 and the first sub-key.
- Add X_2 and the second sub-key.
- Add X_3 and the third sub-key.
- Multiply X_4 and the fourth sub-key.

The output is the concatenation of the blocks.

Table 1. Encryption and Decryption of the Sub-keys [5]

Round No.	Sub-keys of Encryption	Sub-keys of Decryption
1	$Z_1^{(1)}\, Z_2^{(1)}\, Z_3^{(1)}\, Z_4^{(1)}\, Z_5^{(1)}\, Z_6^{(1)}$	$Z_1^{(9)-1}\, -Z_2^{(9)}\, -Z_3^{(9)}\, Z_4^{(9)-1}\, Z_5^{(8)}\, Z_6^{(8)}$
2	$Z_1^{(2)}\, Z_2^{(2)}\, Z_3^{(2)}\, Z_4^{(2)}\, Z_5^{(2)}\, Z_6^{(2)}$	$Z_1^{(8)-1}\, -Z_2^{(8)}\, -Z_3^{(8)}\, Z_4^{(8)-1}\, Z_5^{(7)}\, Z_6^{(7)}$
3	$Z_1^{(3)}\, Z_2^{(3)}\, Z_3^{(3)}\, Z_4^{(3)}\, Z_5^{(3)}\, Z_6^{(3)}$	$Z_1^{(7)-1}\, -Z_2^{(7)}\, -Z_3^{(7)}\, Z_4^{(7)-1}\, Z_5^{(6)}\, Z_6^{(6)}$
4	$Z_1^{(4)}\, Z_2^{(4)}\, Z_3^{(4)}\, Z_4^{(4)}\, Z_5^{(4)}\, Z_6^{(4)}$	$Z_1^{(6)-1}\, -Z_2^{(6)}\, -Z_3^{(6)}\, Z_4^{(6)-1}\, Z_5^{(5)}\, Z_6^{(5)}$
5	$Z_1^{(5)}\, Z_2^{(5)}\, Z_3^{(5)}\, Z_4^{(5)}\, Z_5^{(5)}\, Z_6^{(5)}$	$Z_1^{(5)-1}\, -Z_2^{(5)}\, -Z_3^{(5)}\, Z_4^{(5)-1}\, Z_5^{(4)}\, Z_6^{(4)}$
6	$Z_1^{(6)}\, Z_2^{(6)}\, Z_3^{(6)}\, Z_4^{(6)}\, Z_5^{(6)}\, Z_6^{(6)}$	$Z_1^{(4)-1}\, -Z_2^{(4)}\, -Z_3^{(4)}\, Z_4^{(4)-1}\, Z_5^{(3)}\, Z_6^{(3)}$
7	$Z_1^{(7)}\, Z_2^{(7)}\, Z_3^{(7)}\, Z_4^{(7)}\, Z_5^{(7)}\, Z_6^{(7)}$	$Z_1^{(3)-1}\, -Z_2^{(3)}\, -Z_3^{(3)}\, Z_4^{(3)-1}\, Z_5^{(2)}\, Z_6^{(2)}$
8	$Z_1^{(8)}\, Z_2^{(8)}\, Z_3^{(8)}\, Z_4^{(8)}\, Z_5^{(8)}\, Z_6^{(8)}$	$Z_1^{(2)-1}\, -Z_2^{(2)}\, -Z_3^{(2)}\, Z_4^{(2)-1}\, Z_5^{(1)}\, Z_6^{(1)}$
Output transformation	$Z_1^{(9)}\, Z_2^{(9)}\, Z_3^{(9)}\, Z_4^{(9)}$	$Z_1^{(1)-1}\, -Z_2^{(1)}\, -Z_3^{(1)}\, Z_4^{(1)-1}$

V. COMPARATIVE STUDY: DES, IDEA AND BLOWFISH

Table 2 shows the comparisons among DES, IDEA and Blowfish algorithms.

Table 2. Comparisons among DES, IDEA and Blowfish

DES	IDEA	Blowfish
It is the first encryption standard. It uses 56-bit key and 64 bits of input blocks to produce 64 bits of output blocks [15]	It belongs to a class of iterated block ciphers involving the sequential repetition of a round function and a particular sub-key for each round [3]	Key expansion: converting key to 448 bits into sub-key arrays [7]
DES with the 768-bit key	IDEA with 832-bit key	Blowfish with 64-bit key
DES needs sixteen 48-bit sub-keys, in this way we will obtain the 768-bit secret key to protect a 64-bit block of data	The IDEA needs fifty two 16-bit sub-keys for protecting 64-bit plain-text block - it means that the modified secret key for this algorithm can contain 832 bits	The data encryption is occurred through sixteen rounds which each round consists of key independent permutation. All operations is *XORed* operation

VI. DOUBLE-SECURE IDEA ALGORITHM (MODIFIED VERSION)

Large numbers of weak keys have been found in IDEA [4, 16]. Furthermore, a new attack on round 6 of IDEA has been detected [4]. This paper discusses an improvement made to the original IDEA algorithm to make it more secure. Two factors are included to increase the strength of the security level. Firstly, by increasing the key size, and secondly, by increasing the amount of diffusion.

The modified design is called DOUBLE SECURE-INTERNATIONAL DATA ENCRYPTION ALGORITHM (Double Secure-IDEA). The modified algorithm's main aim is to increase the existing IDEA's algorithm strength by exploiting its characters of confusion and diffusion operations. The modified algorithm can be made more powerful and less suggestible to cryptanalysis by increasing the amount of confusion as well as diffusion. The key features of Double-Secure IDEA are as the following:

- Number of rounds: 8 full rounds - 1 output transformation round.
- Key's length: 512 bits.
- Number of sub keys: 208.
- The sub-key size: 16 bits.

24 sub-keys are used in each round. Four MA blocks are used in each round. The decryption process is the same as the encryption process. In the decryption, the used sub-keys are different, and they are derived from the encryption sub-keys as depicted in Table 1.

6.1. The proposed method

The basic aim is to increase the security strength of the existing algorithm. It is required because of the attack on round has been detected. We can suggest the following to enhance the algorithm's security:

- Modifying the key size: The key size of original IDEA is 128 bits. This paper proposes to increase the key size to 512 bits. Increasing the key size adds more complexity to the algorithm and denies attacks.
- Increasing the amount of the diffusion: The diffusion can be defined as "the process of making the relationship between plain-text and cipher-text more complicated and complex [16]". If one letter within the plain-text changes, then several letters of the cipher-text must change accordingly. The diffusion is proposed by increasing MA (Multiplicative Additive) Block to become four MA blocks in each round.

6.2. Design implementation of Double-Secure IDEA

In the modified version, the proposed data is to be processed in 128-bit blocks. The 128-bit block is divided into eight 16-bit blocks. The algorithm still consists of 8 rounds plus 1 output transformation round; but now 24 sub-keys are used in each round; 16 in transformation round and 8 in sub-encryption round. The last round uses 16 keys. In total 208 sub-keys are used in 8+1 rounds. In the last round the eight 16-bit blocks are recombined to form a 128-bit cipher-text block.

VII. THE FRAMEWORK

The problem of the security for the confidential information in a database can be solved by password protection. E-learning Password Management System (EPMS) manages plenty of different usernames and passwords online, which are stored in a certain disk file (called password database) in the form of cipher-text. The system is using the modified version of IDEA with Electronic Codebook (ECB) operational mode.

ECB mode operates on block cipher. In ECB mode a block of plain-text encrypts into a block of cipher-text [7]. This mode is better than another mode named Cipher Block Chaining (CBC) [7]. ECB is faster than CBC because of its simplicity, and it also has the advantage of allowing any block to be decrypted independently of the others [7]. Although CBC provides more protection, the proposed modified algorithm is expected to have a strong protection by increasing the key size to operate in ECB mode to balance between the performance of the system and the strength of the algorithm.

When the user passes the authentication step by identifying the user name and the password correctly, he/she can handle the information according to the given privileges. After inserting a master key password, the user can add, modify and get information from the database. The modified information will be re-stored to the database after encrypted automatically by EPMS. The structure of the EPMS is depicted in Fig. 2.

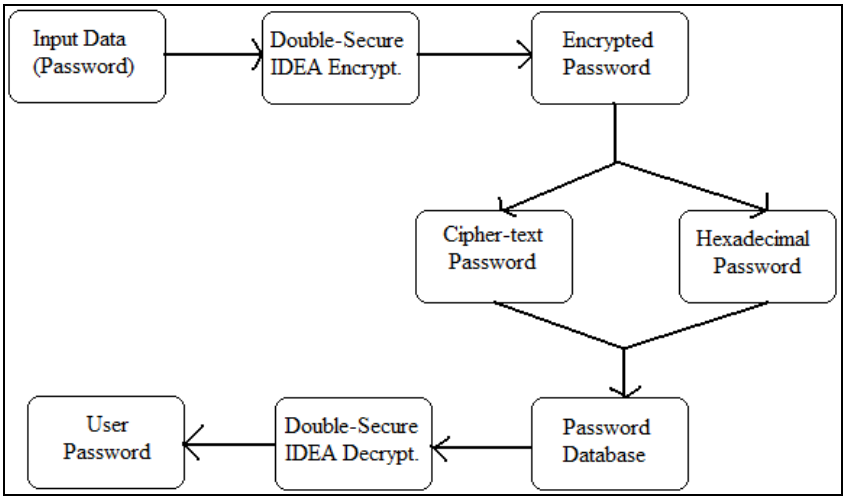

Figure 2. Structure of E-Learning Password Management System (EPMS)

Description of the system:

a. User searches account from already stored account list; if found then use it; otherwise, user can add new account with its password.
b. Adding new account will add website name, username and password.
c. EPMS uses Double-Secure IDEA key that encrypts users' passwords using Double-Secure IDEA (modified algorithm).

d. Double-Secure IDEA algorithm will generate encrypted password in the form of hexadecimal and unreadable cipher-text.
e. These encrypted passwords are stored in a database, which is locked with one master key that makes it more secure.
f. Deletion and edition operations can be performed on stored account.

The implemented system uses the modified algorithm, which operates on 512-bit key that is performed using EBC mode operation. The program structure is divided into front-end and back-end. Data processing in the backend is the core of the system and the implementation of Double-Secure IDEA is the key part. The framework of the e-learning system is shown in Fig. 3. When the user logs in for the first time to the system, he or she must create a new account by filling out the registration form as required. If he succeeds, the user's information will be displayed. The user can also handle the information according to the given privileges. If the user already has an account, he or she must insert the identification information with the password correctly. The system then determines if the user is a normal user or an administrator.

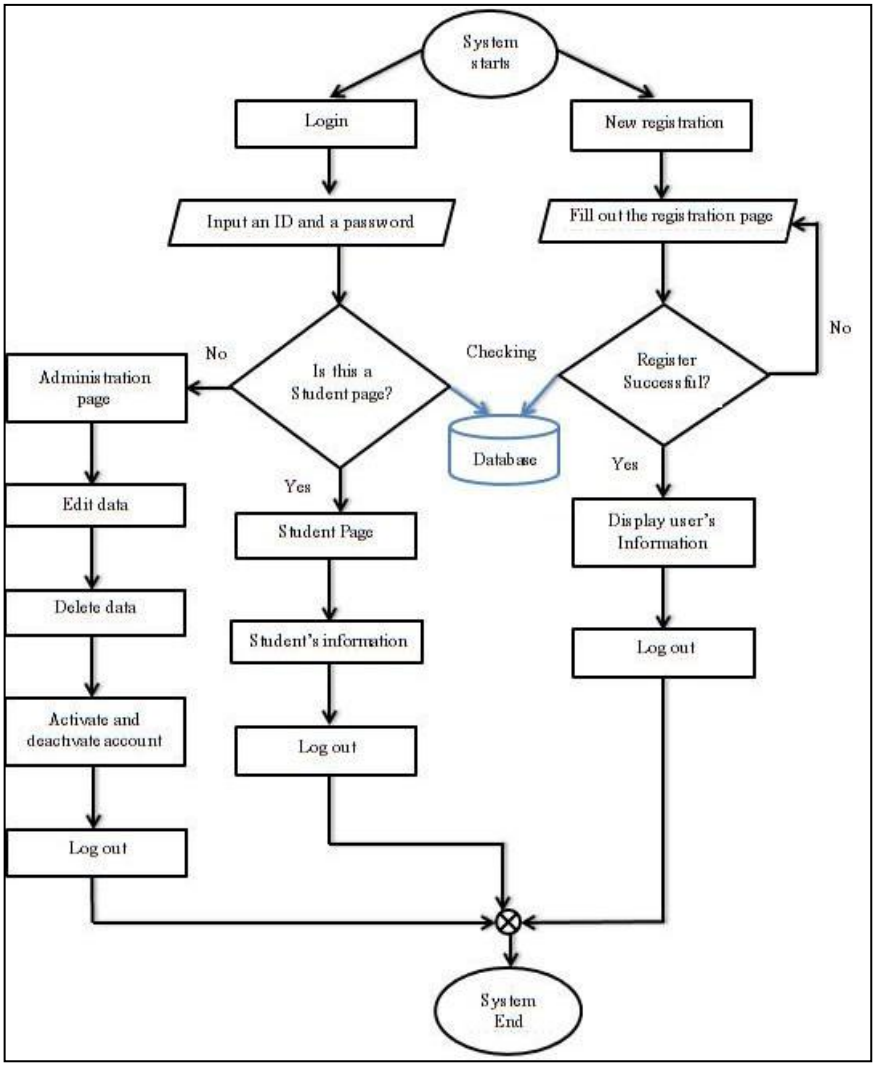

Figure 3. The framework of the proposed e-learning system

VIII. CONCLUSION AND FUTURE WORK

E-learning should meet all the requirements in implementing security measures, which are, confidentiality, integrity and availability. The main contribution of this paper is making e-learning system more secure and easier to access. Security in e-learning requires protecting the system from some threats or unauthorized access such as interception, modification and fabrication.

The main objective of the modified version of IDEA (Double-Secure IDEA) in E-learning Password Management System (EPMS) is to provide security to users' passwords in order to give protection against hacking. The EPMS uses modified IDEA algorithm in EBC mode with 512-bit key size.

Information in the database of EPMS are stored in the cipher-text and hexadecimal format that are unreadable by others. The user can use or access the database only by entering a master key password and passing the identification step, which means that the system is secure and reliable. It is hoped that it provides better security by using the Double-Secure IDEA algorithm.

In the future, this framework with the modified version of IDEA algorithm can be improved for e-business, e-commerce, and e-learning applications using different methods.

Acknowledgement

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

REFERENCES

[1] E E. Thambiraja, G. Ramesh, and R. Umarani, A Survey on Various Most Common Encryption Techniques, *International Journal of Advanced Research in Computer Science and Software Engineering, 2(7),* 2012, 226-233.

[2] Z. Yong-Xia, The Technology of Database Encryption, *Proc. 2nd IEEE International Conference on Multimedia and Information Technology, Vol. 2,* 2010, 268-270.

[3] 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 15 February 2013.

[4] A. Biryukov, J. N. Jr, B. Preneel, and J. Vandewalle, New Weak-Key Classes of IDEA, *Proc. 4th ICICS International Conference on Information and Communications Security,* Singapore, 2002, 315-326.

[5] X. Lai, and J. Massy, A proposal for a new block encryption standard, *Proc. Workshop on the Theory and Application of Cryptographic Techniques Aarhus,* Denmark, 1990, 389-404.

[6] O. Cheung, K. Tsoi, P. Leong, and M. Leong, Tradeoffs in parallel and serial implementations of the international data encryption algorithm IDEA, *Proc. 3rd International workshop,* Paris, France, 2001, 333-347.

[7] M. Wang, and Y. Que, The Design and Implementation of Passwords Management System Based on Blowfish Cryptographic Algorithm, *Proc. 9th IEEE International Forum on Computer Science-Technology and Applications, Vol. 2,* 2009, 24-28.

[8] N. H. M. Alwi, and I. Fan, E-learning and information security management, *International Journal of Digital Society, 1(2),* 2010, 148-156.

[9] J. Eklund, M. Kay, and H. M. Lynch, E-learning: emerging issues and key trends: a discussion paper, *Australian National Training Authority,* 2013, 2-45.

[10] B. Schneier, *Applied cryptography: protocols, algorithms, and source code in C* (John Wiley & Sons, 2007).

[11] H. Kayarkar, Classification of Various Security Techniques in Databases and their Comparative Analysis. *ACTA Technica Corviniensis, 5(2),* 2012, 135-138

[12] T.Connolly, and C. Begg. *Database systems a practical approach to design, implementation, and management* (Ed. England: Person Education Limited, 2005).

[13] W. Meier, On the security of the IDEA block cipher, *Proc.Workshop on the Theory and Application of Cryptographic Techniques Lofthus,* Norway, 1993, 371-385.

[14] X. Lai, J. Massey, and S. Murphy, Markov ciphers and differential cryptanalysis, *Proc. Workshop on the Theory and Application of Cryptographic Techniques Brighton,* UK, 1991, 17-38.

[15] E. F. Shaefer, A simplified data encryption standard algorithm. *Journal of Cryptologia, 20(1),* 1996, 77-84.

[16] H. P. Singh, S. Verma, and S. Mishra, Design Implementation of IDEA to S-IDEA, *International Journal of Engineering and Innovative Technology, 1(6),* 2012, 1-6.