Physics International 2 (1): 31-35, 2011
ISSN 1948-9803

Implementation of an Improved Data Encryption Algorithm in a Web Based Learning System

[1]Adeolu Olabode Afolabi and [2]Rotimi Adagunodo
[1]Department of Computer Science and Engineering,
Ladoke Akintola University of Technology, Ogbomoso, Nigeria
[2]Department of Computer Science and Engineering,
Obafemi Awolowo University Ile Ife, Nigeria

Abstract: Problem statement: This study proffered solution to some identified data insecurity problems in software development by the use of Web-based learning system as a test bed and development of an hybrid crypto-biometric security system. **Approach:** A variant of data encryption algorithm tagged (XOR-RSA algorithm) is developed in order to encrypt the messages being sent between the learner and the facilitator. **Results:** A comparative analysis of performance of this algorithm was carried out using cryptographic algorithm metrics in order to establish its stronger performance above the existing algorithms. The result shows that the improved algorithm (XOR-RSA) performed better than prominent data encryption algorithms in the likes of RSA, SKIPJACK, DES1 and 3DES. **Conclusion/Recommendations:** This was eventually implemented in a web based learning system. The work provides a prototype for the development of secured Web-based learning infrastructure and its contextual framework, which foster indigenization of electronic learning technology which will adequately address the related challenges in the phenomenon of system security in terms of confidentiality and integrity of the system.

Key words: Encryption algorithm, web-based learning system, cryptography, architectural framework, symmetric encryption, crypto-biometric, alphanumeric, symmetric cryptosystem, Hypertext Pre-Processor (PHP), Personal Identification Numbers (PIN)

INTRODUCTION

Several Web-based learning portals have been developed in recent times for the purpose of facilitating their operations, however the portals have been found to have some inadequacies and limitations in terms of functionality and performance. These are largely due to some attendant problems such as insecurity of the system (lack of authentication of the genuine users, loss of data content, performance evaluation of the students and proper deployment of needed courseware) as well as the weakness of the system which often times may not be sufficiently robust to withstand the attendant problems.

Arising from the identified problems of the new technology, this work demonstrates the effectiveness of a unique technique that will address insecurity issue that seems to hamper effective operation of various Web-based learning systems. There is need for a secured E-Learning portal that would guarantee learning within the virtual classroom. The use of electronic systems in an area of need entails additional security and privacy issues.

MATERIALS AND METHODS

The methodology involves the development of crypto-biometric hybrid system by implementing an optimized algorithm for data encryption (tagged XOR-RSA algorithm). As a test bed for this security paradigm, a web based learning system using Hypertext Pre-Processor (PHP), Scripting Language for the Web-based pages, Asynchronous JavaScript and XML (AJAX) to enhance Chatting and Macromedia Flash and other relevant application like Standard Query Language Database Management System for storing data will be developed.

The perceived system is a feedback system that can handle the performance evaluation of student and assessment online. A web cast of the developed Web-based learning portal will facilitates online interaction between the learners and the instructors, the user will gain access via authentication by facial recognition features and by the use of appropriate encryption key to the data within the framework of Web-based learning environment. The various techniques are used so that the

DOI: 10.3844/pisp.2011.31.35

courseware could be assessed and sent to the learner in a virtual classroom for learners' feedback in a fulfilled security conditions (Amirian and Alesheikh, 2008; Bartlett *et al*., 2002; Boukerram and Azzou, 2006; Hergli *et al*., 2005; Denning, 1983; Parry and Gangatharan, 2005; Sleit *et al*., 2007).

Generic requirements for security: There are four basic security requirements to which real-world (composite) system can be traced (Gollmann, 2011). They are secrecy, integrity, availability and non repudiation. Considering these scenarios, password and Personal Identification Numbers (PIN) have become recognizable tools for security over the years. Web-based learning system particularly has found in the literature, exhibit inability to guarantee the needed security. This problem informs the need for enhanced security tools. Password can get lost, be stolen or even be forgotten by the user. The use of password or PIN is considered not to offer the real identity of the user of the system in terms of authentication but just grant of access.

From the fore going, Encryption is one of the security tools that have been in use as further development on the use of ordinary passwords. Although till date encryption has not been applied in Web-based learning paradigms.

Encryption: Network Security threats fall into two categories, they are active and passive threats. A passive threat that is sometimes referred to as eavesdropping, involve attempts by attacker to obtain information relating to a communication (Stinson, 2006). Active threats involve some modifications of the transmitted data or creation of false transmissions. The essential technology underlying virtually all automated network and computer security is encryption. Two fundamental approaches are in use, conventional encryption also known as symmetric encryption and public-key encryption also known as asymmetric encryption. These are discussed below.

Conventional encryption: Conventional Encryption or single-key encryption that is also known as asymmetric encryption is the only type of encryption in use prior to the introduction of public-key encryption in the late 1970s. According to (Golman, 2006) conventional encryption has five basic features. They are plain text, secret key, cipher text, encryption algorithm and decryption algorithm:

- Plain text: describes the original message or data that is fed into the algorithm as input
- Encryption algorithm: refers to various substitutions and transformations performed by the algorithm depending on the key
- Secret key: is input to the encryption algorithm. Secret key describes the exact substitutions and transformations performed by the algorithm which also depend on the key
- Cipher text: This is the scrambled message that is produced as output. It depends on the plain text and the secret key for a given message; two different keys will produce two different cipher texts
- Decryption Algorithm: refers to encryption algorithm that run in reverse, the cipher text and the secret key, to produce the original cipher text RSA Laboratories 2002

There are two basic requirements for securing conventional encryption as discussed below:

- Strong Encryption Algorithm: is the procedure to be followed in encryption. The algorithms have to be such that an opponent who knows the algorithm and has access to one or more cipher texts will be unable to decipher the cipher text
- The Secret Key enables the sender and receiver who must have obtained copies of the secret key in a secured fashion. The key is kept secured in order to allow information exchange

RESULTS AND DISCUSSION

The test bed for this project is a web based application that makes use of web clients, business components and application server as well as a web server. It is written entirely in Java and is based on the J2 enterprise edition platform. The software consists of two major components, the web application and the Face recognitions module. The general overview of the software is shown in Fig. 1

Secured web-based learning architectural framework: The architectural framework of the secured Web-based learning is shown in Fig. 1 it describes the architectural framework graphically for the system being developed, the architectural design shows the various components of the development.

Development of an enhanced XOR-RSA algorithm: The XOR Encryption algorithm is an example of a symmetric encryption algorithm. This means that the same key is used for both encryption and decryption. The classical XOR encryption algorithm is derived from Boolean algebra. The XOR function, here on expressed as XOR (a, b) where a and b are binary valued variables. Another way to state the XOR function is to say that the function returns true when the values of the two arguments are different, let k be some key value represented in binary, using a byte (eight bits).

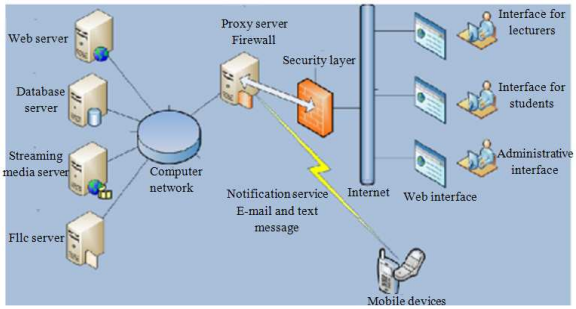

Fig. 1: Secured Web-based learning architectural Framework

Let m be a binary representation of the message one byte in length. To obtain the cipher text, which is also known as the encrypted text, one simply applies the XOR function to generate the cipher text:

c (c = XOR (m, k))

Not every message to be encrypted is one byte long, the above instance of the XOR algorithm is known as the 8-bit XOR Encryption algorithm.

Enhanced XOR-RSA algorithm: In order to develop a stronger algorithm, XOR-RSA algorithm there is a need to consider the basic principle of RSA algorithm. The algorithm capitalizes on the fact that there is no efficient way to factor very large (100-200 digit) numbers. Using an encryption key (e, n), the algorithm is as follows:

- Represent the message as an integer between 0 and (n-1)
- Large messages can be broken up into a number of blocks. Each block would then be represented by an integer in the same range
- Encrypt the message by raising it to the eth power modulo n
- The result is a cipher text message C. To decrypt cipher text message C, raise it to another power d modulo n. The encryption key (e,n) is made public, the decryption key (d,n) is kept private by the user
- Choose two very large (100+ digit) prime numbers, denote these numbers as p and q
- Set n equal to p * q
- Choose any large integer, d, such that GCD(d, ((p-1) * (q-1))) = 1
- Find e such that e * d = 1 (mod ((p-1) * (q-1)))

This algorithm has been broken by cryptanalysis and this informs the need for a better algorithm which gives rise to the development of XOR_RSA algorithm. The implementation of the improved version of this algorithm in the course ware of the Web-based learning System to be developed will provide a stronger data encryption than the use of just any one of the algorithm.

The proposed XOR-RSA algorithm for the encryption is as follows:

Step 1: Get ASCII for the chosen number
Step 2: Convert ASCII to binary
Step 3: Convert plaintext in RSA form to cipher text
Step 4: XOR Binary of ASCII with RSA cipher text
Step 5: Use public key V to convert XOR binary to encrypted text.

In order to decrypt, use the public key V to convert encrypted text to plaintext.

Cryptographic algorithm metric descriptions:
Key length metric: The security of a symmetric cryptosystem is a function of the length of the key. A key length of N bits has 2N possibilities.

Attack steps metric: Attack Steps is defined as the number of steps required to perform the best known attack.

Attack time metric: Attack Time is defined as the time required in performing the fastest known attack on a specified processor.

Time granularity: The year time granularity seemed consistent with the precision of the theoretical operation assumptions. The Mtops year was rounded to two decimal places in.

Algorithm strength metric: The Algorithm Strength (AS) metric is intended for use by experienced cryptographers to specify, or express an evaluation of, algorithm strength values. To provide a small representative sampling of well known cryptographic algorithms, five prominent algorithms are selected in comparison with the enhanced RSA-XOR algorithms, five symmetric or secret key (one-key) block ciphers and one asymmetric or public key (two-key) algorithm.

Metrics application: Table 1 shows the selected algorithms and illustrates their characteristics as they might be measured and specified with the metrics. There is clearly a difference between DES and 3DES. An alphanumeric trigraph (CS1, CS2) are used for a descriptor when the number of levels required are determined.

Table 1: Comparison of some cryptographic algorithms with XORRSA

Algorithms metrics	DES1	3 DES	SKIPJACK	RC6	RSA	XORRSA
Key length (Bits)	56	112	80	64	1024	2048
Attack time in years	1.37×1010^{11}	1.25×10^{28}	2.56×10^{18}	3.61×10^{13}	2.40×10^{17}	17.98×10^{92}
Attack steps	2^{56}	2^{112}	2^{80}	2^{64}	2^{1024}	2^{1757}

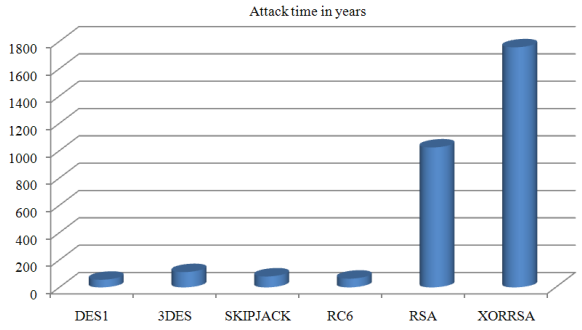

Fig 2: Comparison of some algorithms and their attack time in years

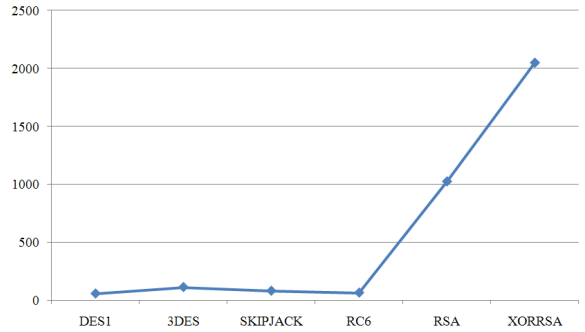

Fig. 3: Comparison of some algorithms and their key length

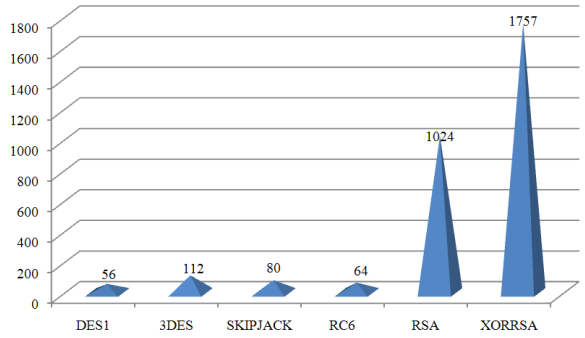

Fig. 4: Comparison of some algorithms and their attack steps

For example, perhaps a CS1 rating might is given to 3DES and SKIPJACK and a CS2 (or lower) for the others, as appropriate, 1 indicating the most computationally secure level.

CS rating for RC6 and RSA is conditional, which is the reason for the 5th, Conditionally Computationally Secure (CCS), rating. The keys used must be "long enough" to warrant a CS rating and this the case with RSAXOR which is found to be computationally secure as shown in Fig. 2. In the case of RC5, as with DES, there also must be "enough" rounds. These "enough" values are a function of the best method (s) of attack as well as the state of cryptographic mathematics, processor hardware and software technology. Street and Walker have recently suggested a three graduation scale for indicating the strength of cryptography based on key length: "Weak Cryptography," applications with secret keys of 40 bits (DES, RC2, RC4) and for public key 512 bits or less; "Good Cryptography," secret key of 56 bits (typically DES), public key 512-1024 bits; and, "Strong Cryptography," secret key lengths in excess of 56 bits and public keys that are 1024 bits and larger like XORRSA.

The attack times in years shown in Table 1 were derived by dividing the Attack Steps by the pilot Mtops per year (3.83×10 operations per year.) Obviously, these are enormous periods of time using the comparatively small Symmetrical Multiprocessor (SMP), which was chosen for this illustration. There are larger SMPs but there is a point, as you keep adding processors in the SMP architecture, at which efficiency declines due to memory contention since all the processors use the same memory.

Figure 2 shows comparison of some algorithms and their attack time in years with that of XOR RSA algorithm it is reflected in the figure that the attack time in years of the new XORRSA is greater than the other five algorithms. The implication of this is that XORRSA cannot be easily broken through it will take more time than the other algorithms.

Figure 3 shows the comparison of some algorithms and their key length with XORRSA key length and it is obvious that the key length of XORRSA is longer than the other five including prominent RSA algorithm this shows the number of alphanumeric characters that is embedded in the key. The longer the key, the more secured is the cryptography (Yang *et al*., 2004).

Figure 4 shows the comparison of some algorithms and their attack steps and it shows that XORRSA is more robust cannot be easily attacked like other algorithms.

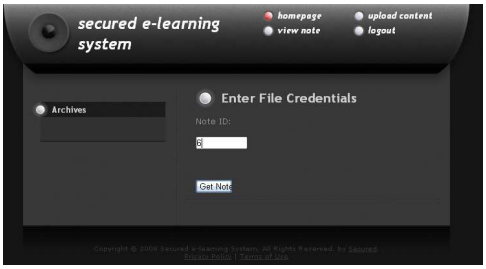

Fig. 5: View course materials

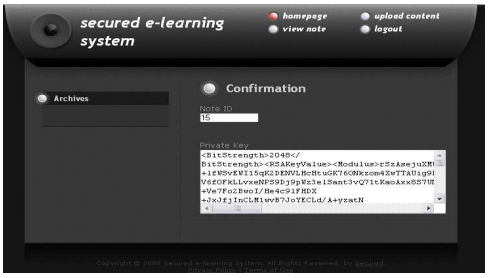

Fig. 6: Note and key generation page

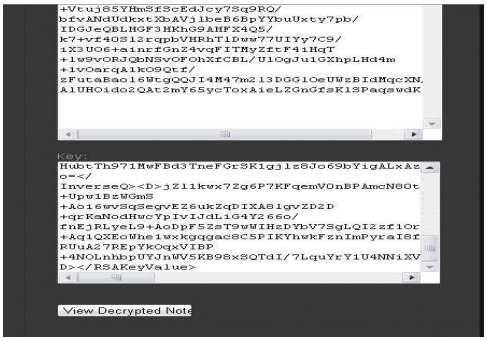

Fig. 7: Encrypted note using XOR-RSA algorithm

View course material: Figure 5 shows the form to register set of courses and Fig. 6 shows the form for generation of the key for encryption. Each course has a list of topics that have been created by the lecturers in charge. Each topic can be accessed through the link provided. Figure 7 shows the encrypted view of the course material to the student.

CONCLUSION

This study proffered some solution to insecurity in Computer systems, through development of a crypto-biometric system that implements an data encryption algorithm (tagged XOR-RSA algorithms) as solutions to insecurity of data and development of a Web-based learning System as test bed for these solution.

This study implements an improved security framework for Web-based learning operations and to facilitate secured multilevel involvement in Web-based learning, desire for pedagogical innovation through Web-based learning and designing student-centered approaches.

In Web-based learning, software design and educational design are intrinsically linked, the new security model proposed will make Web-based learning very suitable and secured for effective performance, particularly by the use of the duo of facial recognition and data encryption as security measure beyond the present scope.

REFERENCES

Amirian, P. and A.A. Alesheikh, 2008. Publishing geospatial data through geospatial web service and XML database system. Am. J. Applied Sci., 5: 1358-1368. DOI: 10.3844/ajassp.2008.1358.1368

Bartlett, M.S., J.R. Movellan and T.J. Sejnowski, 2002. Face recognition by independent component analysis. IEEE Trans. Neural Netw., 13: 1450-1464. DOI: 10.1109/TNN.2002.804287

Boukerram, A. and S.A.K. Azzou, 2006. Implementation of load balancing algorithm in a grid computing. Am. J. Applied Sci., 3: 1810-1813. DOI: 10.3844/ajassp.2006.1810.1813

Denning, D.E.R., 1983. Cryptography and Data Security. 1st Edn., Addison-Wesley, Reading, Massachusetts, pp: 400.

Gollmann, D., 2011. Computer Security. 3rd Edn., John Wiley and Sons, Chichester, ISBN: 0470741155, pp: 456.

Golman, K., R. Zandt and M. Thaning, 2006. Real-time metabolic imaging. PNAS, 103: 11270-11275. DOI: 10.1073/pnas.0601319103

Hergli, M., J. Baili, F. Bouslama and K. Besbes, 2005. A new compressing ultrasonic data algorithm based on wavelets. Am. J. Applied Sci., 2: 1615-1618. DOI: 10.3844/ajassp.2005.1615.1618

Parry, M. and N. Gangatharan, 2005. Adaptive data transmission in multimedia networks. Am. J. Applied Sci., 2: 730-733. DOI: 10.3844/ajassp.2005.730.733

Sleit, A., W. AlMobaideen, S. Al-Areqi and A. Yahya, 2007. A dynamic object fragmentation and replication algorithm in distributed database systems. Am. J. Applied Sci., 4: 613-618. DOI: 10.3844/ajassp.2007.613.618

Stinson, D.R., 2006. Cryptography: Theory and Practice. 3rd Edn., Chapman and Hall/CRC, Boca Raton, ISBN: 1584885084, pp: 593.

Yang, Z., S. Sesay, J. Chen and D. Xu, 2004. A secure database encryption scheme. Am. J. Applied Sci., 1: 327-331. DOI: 10.3844/ajassp.2004.327.331