International Journal of Engineering & Technology, 7 (2.32) (2018) 336-340

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Secured SO a for Interoperable e-Learning Platforms Based on Encryption Algorithms

G.Vijaya lakshmi[1], G.Dinesh kumar[2], M.V.Sai Lohith[3] ,Y.Akhil Reddy[4]

[1,2,3,4]*Department of CSE, Koneru Lakshmaiah Engineering Foundation,Vaddeswaram, Guntur, India -522 502*
**Corresponding author E-mail: vijayalakshmigundam@gmail.com*

Abstract

The Lionization of distance education is cake walking on day basis and is the most tendered process to obtain the information in any field. Compared to the traditional education it is providing many facilities in various aspects. As the improvements are rapid in this area, the requirements are also cake walking. A Service Oriented Architecture addresses issue by designing the views of reference architecture from the contents of various domains. It personalizes the delivery of e-content based on knowledge and preference of the learner. As the information provided in the e-learning systems is to be made secure along with the user information a specific security system is to be designed by using the concepts of system security. For this various algorithms such as Triple DES, RSA, AES are taken in to consideration as an experimental analysis. Only the authorized person can utilize the content without interfered by the other user. By the analysis experimentally AES is showing highest accuracy among all the algorithms.

Keywords:*Authorization, Matrix, Security, Service Oriented Architecture, System security..*

1. Introduction

E-Learning System or E-learning platform is learning through electronics technologies to access their educational curriculum outside of the traditional learning methods. It can be defined that students, teachers and authors work together for making student groups to work effectively.

E-Learning offers the flexibility to share material in various sorts of formats like videos, slideshows, word documents and PDFs. Conducting webinars and communication with professors via chat and message forums is the added advantage to the users.

For every institution there will be individual platform of E-Learning which provides its students the subjective knowledge. But, in order to gather more information every individual should communicate with or check various E-Learning platforms. Educational cost is very low compared to traditional education systems. Materials can be easily and quickly updated based on changing conditions.

E-learning platforms are made secure by for every user and from every user by providing authentication, authorization and then followed by reporting. All the unique credentials are provided in the database and thus only the authorized persons can access the data. Interoperability is the capability of different programs to exchange the data through a common set of exchange formats to read and write the same file formats and to use the same protocols.

1.1 Process in Service Oriented Architecture

A Service oriented reference architecture by designing the views of reference architecture from the contents of different and various domains and address the issue. According to the knowledge and preferences of the learners the e-content is delivered in a personalized way.

In authentication the received message is controlled from the database whether the login is valid or not. After the validation is done then the message is sent to the mediator service and then to the authorization center where an official permission is provided for the document and this combined message is sent to the reporting service where the received message is resolved and the information about platforms that can be accessed by this user is determined.

2. Literature Review

In the past few years there are many works done on securing the user E-Learning account that belongs to a particular education institution by storing the unique username and password of the student in the large data sets. Web services play a major role to provide communication of information and can work with any OS, programming language and platforms.

In order to extract the information present in the platform at first it must be made secure. So, providing security to the whole data in the E-Learning system is to be at maximum rate. Highly secure methods are to be used such that no content is misused or unauthorized usage of content is not to be observed.

For perfectly securing the E-content processes such as data encryption is to be done on the side of an educational institution and decryption is done by the user when he is going to access the online content.

3. Existing System

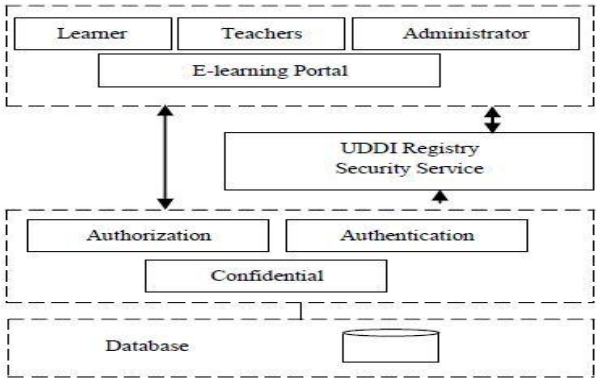
E-Learning platforms are secured in various phases. It includes web services such as SOAP, WSDL, and UDDI which made this process as easier as possible. Each service has its own functionality for e.g.:- SOAP (Simple Object Access Protocol) is used to integrate applications formatted with XML.

WSDL (Web Service Definition Language) defines the information such as web-service description, processes and message formats such as input and output in XML format.

Finally by publishing the services of the institutions a definition is provided such that it can be accessed by other institutions using UDDI (Universal Description Discovery and Integration).

Including the interoperability as a feature various programs will be exchanging their data on similar formats either to read or to write, this increase the performance of E-Learning platforms without re-designing and re-building the sites.

This approach doesn't help to secure the content in the E-Learning platform and only helps to secure user account by maintaining his unique credentials in a database.



The processing of the existing system is observed as the following steps that are represented in the form of the diagram:

Fig. 1. Working procedure using Web-Services.

4. Proposed Approach

Once the user is provided security for his e-learning platform by using a unique username and password, we are providing the security now for the content in the e-learning platform by encryption and decryption using a single key using the best ever AES algorithm. To overcome the problems of securing the online content which is related to misuse of institutional services a concept of computer networks is used. There are various encryption algorithms which are used to raise the standard of the E-content. The idea is "The user should access the real content that is provided by the institution but not the changed one". This can raise the information value provided in each institution's E-learning platform.

After satisfying the unique credentials the user uses the AES algorithm to decrypt the data as it is based on several substitutions, permutations and linear transformations, each executed on data blocks of 16 byte. This process is done in rounds so that the entire data is secured at a time.

4.1 Triple DES Algorithm

The Triple DES which is otherwise called Triple Data Encryption Algorithm is a symmetric key block cipher. It applies the DES calculation for three times for each square of information. Triple DES utilizes a key package which comprises of three DES keys ks1, ks2 and ks3 where each are of 56 bits barring equality bits.

Encryption by Triple DES is:

$$\text{ciphertext} = \text{EnKs3}\left(\text{Deks2}\left(\text{Enks1}(\text{plaintext})\right)\right) (1)$$

Decryption by Triple DES is:

$$\text{plaintext} = \text{DeKs1}\left(\text{Enks2}\left(\text{Deks3}(\text{ciphertext})\right)\right) (2)$$

For every triple encryption it encrypts one block of 64 bits of data.

4.2 RSA Algorithm

RSA algorithm is an asymmetric cryptography algorithm which involves two different keys such as public key and private key. The possibility of RSA calculation is on the way that to factorize a huge whole number which will be slightly troublesome. Here the public key comprises of two numbers where one number is the product of two large prime numbers and the private key is also derived from the same prime numbers.

The encryption strength lies totally on the key size. When the increases the same will be the change in the strength of encryption. Keys in RSA are 1024 and 2048 bits long, but as per the analysis of the experts' 1024 bits keys could be broken in the future.

For generating a public key:

1. Select two numbers a and b which are prime.
2. First half of public/open key is n = a*b
3. Small e (an exponent) where it must be a whole number, not a factor of n.
4. 1<e<k(n) (k(n) : check the private key)
5. Public key is observed by n, e.

To generate private key:

1. K(n) = (a-1)*(b-1)
2. Private Key p = (q*k (n) + 1)/e for some integer q.

4.3 AES Algorithm

AES algorithm is known by its unique name Rijndael and is contracted as Advanced Encryption Standard. As it is a symmetric key calculation that is same key is utilized for both encryption and decryption of data with the key sizes as 128, 192 and 256 bits. All the operations are repeated several times and are known as "rounds". Amid each cycle, an exceptional round key is computed out of the encryption key, and consolidated in the estimations. Cracking of the 128 bit AES key with any sets of super computers would take longer time and is even very much impractical. In this manner, AES will be the favored encryption standard for high security frameworks around the globe.

As per AES algorithm 128 bits of plaintext block is treated as 16 bytes. These are organized in four lines and four segments to process as framework (matrix). AES relies upon the length of the key and the quantity of rounds shifts with the span of key.
It is spoken to as:

Table1: Key Size versus Number of Rounds

Rounds	Key Size
10	128 bits
12	192 bits
14	256 bits

Encryption process

Each AES encryption has four sub processes and it continues for every round of providing security.

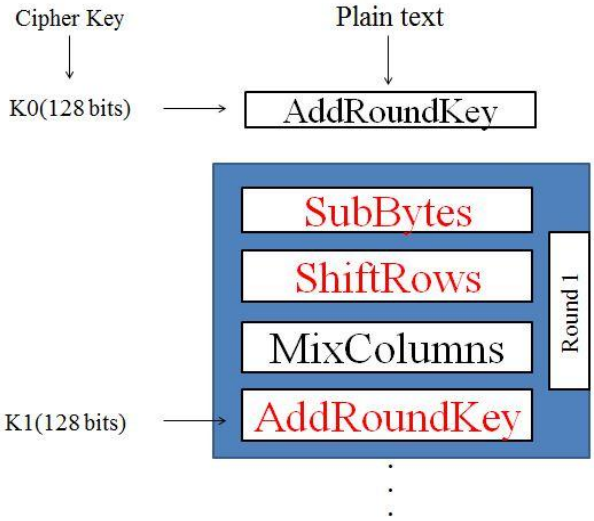


Fig. 2. Encryption process in AES algorithm.

4.3.1 Substitution of Bytes:

The total 16 input bytes are substituted by looking up an S-box (fixed table). The outcome will be a framework with four rows and four columns.

4.3.2 Shifting the Rows:

Each of the four columns of the network (matrix) is moved to left side. Any sections that tumble off are re-embedded on the correct side of the row.

The shift of rows will be processed in the following steps:

1. Shift of rows is not happened in the first row.
2. Shift is observed for one position to the left considering the second row.
3. Two positions to the left are shifted while taking into account of the third row.
4. Forth row is shifted left for about three positions. The outcome will likewise be a matrix with 16 bytes however moved as for each other.

4.3.3 Mix columns:

A special mathematical function is used to transform each column of four bytes.

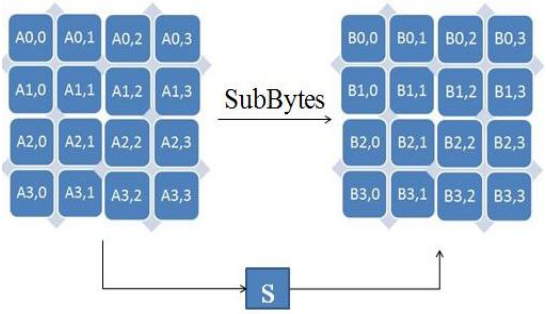


Fig. 3. Mixing of columns using Substitution bytes.

The following is the way to calculate the output at mix columns. It serves a better purpose to encrypt the data. It is a linear transmission technique.

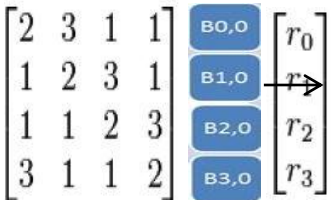


Fig. 4. Matrix multiplication in AES algorithm.

Where r0, r1, r2 and r3 will be the values that are to be considered in the case of next section (i.e.,) adding round key. The first matrix is also known as "other matrix" and the one multiplied to it is the first column of the resultant matrix from the previous step of shifting the rows.

4.3.4 Adding Round Keys:

The aggregate 16 bytes of the grid (matrix) are presently considered as 128 bits and are XORed with the 128 bits of the round key. For the last round the yield will be the cipher text. If not the result of 128 bits is again interpreted as 16 bytes and the process is done in the similar manner (round).

Decryption Process:

The reverse order of the AES encryption process will be the decryption of AES cipher text. Similar to the encryption it also consists of four rounds which are available in reverse phenomena.

1. Add Round key
2. Mix Columns
3. Shift Rows
4. Byte Substitution

The adjustment in the Encryption and Decryption is perceived just in the request of handling and they should be executed separately even though they share a close relation between them.

The flow of providing security using AES Encryption algorithm is as follows:

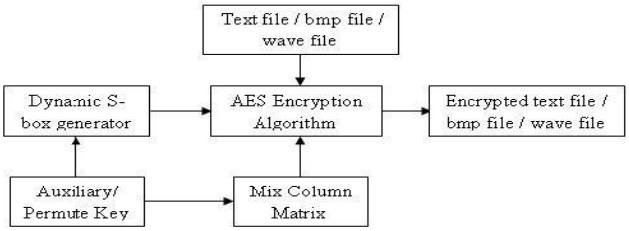


Fig. 5. Process of data securing using AES algorithm.

5. Experimental Analysis

The comparison of the results to secure the e-content using these three algorithms TRIPLE DES, RSA and AES is expressed by performing the individual processes and calculating the efficiency of each algorithm by finding out their notifying encryption and decryption times. The one which takes more time to encrypt will be having less efficiency than the other.

AES is the only algorithm that is maintaining the time period without depending on the size of the file. Since decryption is also similar process in AES with a change in the order of execution which is reverse to the encryption it is maintaining same time to decrypt the file of any size.

5.1 Graph of Encryption Time:

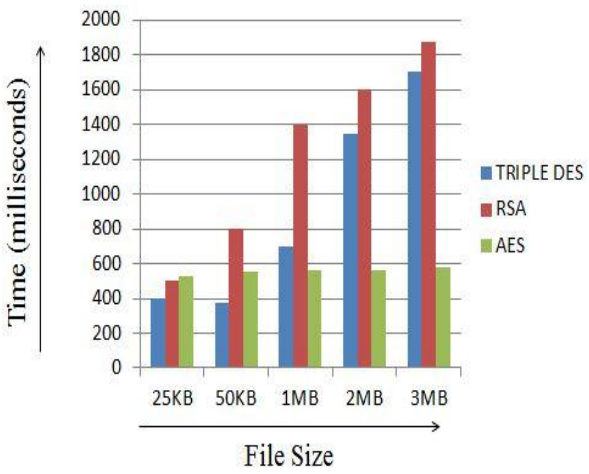


Fig. 6. Encryption time Vs File size of TRIPLE DES, RSA and AES algorithms.

Among all the algorithms RSA takes the maximum time and AES took the least time and is almost constant at any file size. This is the perfect feature that shows the implementation of AES will provide better results compared to the other algorithms.

5.2 Graph of Decryption Time:

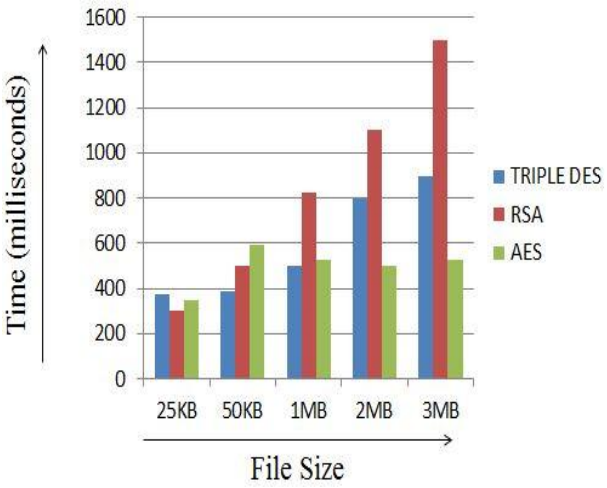


Fig. 7. Decryption time Vs File size of TRIPLE DES, RSA and AES algorithms.

Compared to the time taken for encrypting the data, the total time taken to decrypt is less in all the algorithms. RSA takes highest time for decryption and is same in both the cases. RSA being a public key crypto framework utilizes one way processing which is difficult to rearrange by using prime numbers.

Usage of multiplicative inverse, modular exponentiation and two keys namely the private key and the public key are the causes for making RSA slow compared to all the other techniques of cryptography.

6. Applications

1. Recommended when the content of any institution's E-learning system is misused or not used as per the norms.
2. When a change of data is observed while dealing with any user who are unauthorized.

7. Conclusion

In order to give the best platform for a user who may be a student, teacher or any educational designator, Advanced Encryption Standard algorithm is most popular to protect vast content which may be in various forms. So, we recommend a proper E-learning system which can secure both the user accounts and also the content in it. By using the best recommended algorithm which constantly maintains the time for both encrypting and decrypting the data, and also collecting the unique credentials of the client, for example, username and password in a database, everything will be secured from the individuals who misuse them. AES algorithm has more efficiency as it cannot be cracked for longest period of time.

By involving both the database and the security systems maximum security is provided to every institution's E -learning sites.

Acknowledgement

My sincere thanks to Mr. G.Dinesh Kumar who helped me in the study and preparation of paper with healthy discussions on various related topics till the end.

References

[1] Umit Kocabicak, Deniz Dural, Computer Engineering Department, Faculty of Computer and Information Science, Sakarya University, 54187Serdivan, "Secure and interoperable e-Learning platforms Based on Web Services, International Conference on New Horizons in Education INTE 2012."

[2] Buchmann, R. A., Jecan, S. (2008), "An Arbitration web service for E-Learning based on XML Security Standards. Wseas Transaction on Computers, 7, 1109-2750."

[3] Thomas C. Ford, John M. Colombi, Scott R. Graham and David R. Jacques. "A Survey on Interoperability Measurement, 12th ICCRTS."

[4] IEEE Standards Information Network. IEEE 100, the Authoritative Dictionary of IEEE Standards Terms, Seventh Edition. New York, NY: IEEE, 2000.

[5] E-Learning, Wikipedia (2017). http://en.wikipedia.org/wiki/E-Learning (2017 December 25).

[6] Alkouz, A., El-Seoud, S.A (2007). "Web services Based Authentication System for e-learning. International journal of computing &information Sciences, 5, 74-78."

[7] Mehedi Masud, "Collaborative e-learning systems using semantic data interoperability."

[8] Alonso, J., De Soria, I M., Orue-Echevarria, L., and Vergara, M.: "Enterprise collaboration maturity model (ECMM): preliminary definition and future challenges, Enterprise Interoperability IV, Springer, 2010."

[9] M.R.M.Veeramanickam, Dr.M.Mohanapriya, "Research paper on E-Learning Application Design Features" using cloud computing and software engineering approach. (ICICES 2016)

[10] Casati, F., U. Dayal, eds. (2002). "Special Issue on Web Services. IEEE Bulletin of the Technical Committee on Data Engineering, 25 (4), December 2002."
[11] AES, Wikipedia (2017). http://en.m.wikipedia.org/wiki/AES (2017 December 28).
[12] Suo, Y., Miyata, N., Morikawa, H., Ishida, T.: "Open Smart Classroom: Extensible and Scalability Learning System in Smart Space using Web Service Technology. IEEE Transactions on Knowledge and Data Engineering 21(6) (June 2009)"
[13] Mohammed Al-Zoube, Princess Sumaya University for Technology, Jordan: "E-Learning on Cloud."(2009)
[14] Chih-Ming Chen, "Intelligent web-based learning system with personalized learning path guidance" Computers & Education 51, 787 – 814, 2008.
[15] Analysis on Triple DES, RSA and AES algorithms, http://www.sciencedirect.com/science/article/pii/S1877050916001101
[16] Signe Schack Noesgaard, Rikke Qrngreen, "The Effectiveness of E-learning: An explorative and integrative Review of the Definitions, Methodologies and Factors that promote e-learning Effectiveness." (2015)