Al-Mustansiriyah Journal of Science
ISSN: 1814-635X (print), ISSN:2521-3520 (online) Volume 33, Issue 1, 2022 DOI: http://doi.org/10.23851/mjs.v33i1.1016

Research Article **Open Access**

Secure E-Learning System Based on ZNP and AES

Rand M. Rafee, Bashar M. Nema*

Department of Computer Science, College of Science, Mustansiriyah University, IRAQ.

*Correspondent contact: bashar_sh77@uomustansiriyah.edu.iq

Article Info

Received
06/08/2021

Accepted
14/10/2021

Published
10/03/2022

ABSTRACT

A secure electronic learning platform has been created to enable teachers and students to log into their accounts to learn efficiently and safely at any place and time. This platform has been proposed due to the urgent need to develop the education system and move it from traditional to interactive e-learning. In this paper, an application implemented that access remotely using a web browser interface and saved on a server depends on a Zero-Knowledge Proof (ZKP) system with an RSA algorithm was employed to solve registration and login challenges and securely transfer passwords. Using adapted AES to encrypt each user's personal information, Exams, and save it in in encrypted form in the database. The simulated results in this paper indicate the existence of a secure e-learning system, where security was achieved by performing the registration and login process without sending the password in its explicit form over an insecure network such as the Internet, in addition to encrypting the necessary information to be stored in an incomprehensible manner in the database, in the case of presence of an attack on the database.

KEYWORDS: E-learning; Zero-Knowledge Proof; Encryption; AES.

الخلاصة

تم إنشاء منصة تعليمية إلكترونية آمنة لتمكين المعلمين والطلاب من تسجيل الدخول إلى حساباتهم للتعلم بكفاءة وأمان في أي مكان وزمان. تم اقتراح هذه المنصة بسبب الحاجة الملحة لتطوير نظام التعليم ونقله من التعلم الإلكتروني التقليدي إلى التعلم الإلكتروني التفاعلي. هذا النظام عبارة عن تطبيق يمكن الوصول إليه عن بُعد باستخدام واجهة متصفح الويب وحفظه على خادم في هذا البحث، تم استخدام نظام Zero-Knowledge Proof (ZKP) مع خوارزمية RSA لحل تحديات التسجيل وتسجيل الدخول ونقل كلمات المرور بأمان. باستخدام طريقة AES، نقوم بتشفير المعلومات الشخصية لكل مستخدم والاختبارات وحفظها في شكل مشفر في قاعدة البيانات. تشير نتائج المحاكاة في الورقة إلى وجود نظام تعليم إلكتروني آمن، حيث تم تحقيق الأمان من خلال إجراء عملية التسجيل والدخول دون إرسال كلمة المرور بشكلها الصريح عبر شبكة غير آمنة مثل الإنترنت، بالإضافة إلى تشفير المعلومات اللازمة ليتم تخزينها بطريقة غير مفهومة في قاعدة البيانات، في حالة وجود هجوم على قاعدة البيانات.

INTRODUCTION

Online education is an important technology that has saved cost, effort and time for teachers and students, but it is a concern for many universities regarding the security of these systems and data. In the era of the COVID-19 pandemic and to mitigate its spread, the world has imposed severe restrictions such as social distancing measures and lockdown measures. [1]

The urgent need for this technology has emerged in order to continue the wheel of learning and development, which has led to the shift from traditional methods of education to online learning or the so-called e-learning. [2]

ELECTRONIC LEARNING (E-LEARNING)

E-learning is the expression used to describe the use of internet and web technologies to enhance the learning and teaching experience. [3]. Alternatively defined it is the process of learning achieved by the use of digitally delivered material or interaction. It primarily revolves around the use of PCs to provide information. [4]

E-learning is a modern dynamic that characterizes instructional processes that have a variety of features. The main characteristics of the E-Learning process [5] [6]:

- Accessibility: e-learning platforms can be accessed at any time, from any place, by anybody.
- Flexibility: define own learning schedule and strategies instead of following a specific course structure.
- Digital Communication: E-Learning platform provides a connection to access resources and courses.

- Interactivity: The synchronous and/or asynchronous mode of contact used for e-learning platforms.

E-Learning environments categories into three types. [7]

1. distance-learning or fully web-based classes delivered entirely on the Internet, without face-to-face interaction, with all facets of the course conducted in an online learning environment.
2. Web-based Supplements to traditional courses use Internet technologies to provide supplementary content for formal study in the classroom.
3. Hybrid classes or blended have both web-based and class lessons, with differing amounts of time available to each, depending on the scope of the class and the instructor's discretion.

RELATED WORK

There is great importance when building e-learning systems to achieve the principle of security and preservation of user information whether he is a teacher or student, as well as the mechanism for maintaining the database used in addition to maintaining the services against unauthorized use.
In light of this, the following is a summary of the most important previous studies that we believe are important in the design and implementation of the proposed system.
In [4] the researcher used windows Azure (microdot's cloud-based application) for create, administer, and host software applications that provide a level of safety such as client authentication and encrypt of data for sensitive information.by using MD5, with the use the security services provided by cloud computing such us HTTP.
In [8], researchers use neural networks in existing biometric technology and applications for basic biometric functionality that could be used for authentication of e-learning platforms.
In [9], the researcher employ encryption for secure issues, they use an RS coding scheme before the message is stored in an e-learning storage system in a cloud data center.
In [10], the research uses fingerprint detection as a primary tool of access control in order to address online education web portal security issues. The platform provides a way to acquire an understanding of the full scope of technologies for fingerprint recognition systems, Demonstrations such as improvement of the fingerprint image and extraction of the fingerprint functionality are used in the prototype of the platform.

DESIGN AND METHODOLOGY

Zero-knowledge proof

A zero-knowledge proof (ZKP) is a cryptographic protocol allowing one to prove they possess information to a verifying party without revealing any underlying information [11,12, 13]

Secure Remote Password (SRP) is a reliable authentication protocol for client-server applications is Secure Remote Password (SRP), a zero-knowledge proof protocol. [14]
Where the server does not have to store password equivalently information, and clients can securely authenticate to the server. The properties of zero knowledge proof [15]:

(a) Completeness: If the statement is correct, the verifier should be able to show it is prove repeatedly.
(b) Soundness: There would be no way for the prover to inform the verifier that the statement is valid if the statement is false. Unless there is a slim chance.
(c) Zero-knowledge: If the statement is true, the verifier has no knowledge about the sentence other than that it is right, and it does not return any information about the sentence.

RSA Encryption Algorithm

RSA encryption algorithm is a form of asymmetric key encryption, the algorithm appeared in 1977 by a group of cryptographers Rivest, Shamir, and Adleman [16], which is most important in encryption and authentication of data while transfer throw the internet. RSA algorithm is divide into three parts: key generation, Encryption, Decryption algorithms shown in Figure 1.

Advanced Encryption Standard (AES)

Advanced Encryption Standard Is one of the most popular and commonly used symmetric block cipher algorithms in the world.
The algorithm is use various key sizes and rounds, 14 rounds for 256-bit keys, 12 rounds for 192-bit keys, and 10 rounds for 128-bit keys [18]. Per round of cryptography consists of four phases [19, 22] as follows:

1- *SubBytes transformation*: This operation achieved by using S-box shown in Table 1,

ISSN: 1814-635X (print), ISSN:2521-3520 (online) Volume 33, Issue 1, 2022 DOI: http://doi.org/10.23851/mjs.v33i1.1016

which achieves a non-linear transformation by performing a permutation by the intersections of the numbers, to show that. If we have hex 53, it will be replaced by hex ED, ED generated by the junction of 5 and 3. [20, 21].

2- *ShiftRows transformation:* The principle behind this process is cyclically shift the bytes.

3- Mix Columns transformation: The process of the mix column stage done by multiplying the input column with a matrix called D-box.

4- AddRoundKey transformation: Applying Xor operation with the Key. Figure 2 shows the Flowchart of AES Algorithm.

RSA_Key_Generation ()
Input: Select two random distinct prime numbers w and x.
Output: Find Public Key (U), Private Key (R) and Modulus (j).
Begin
Procedure (w, x, U, R and j)
1. j ← w * x
2. Calculate Euler Ø () of j
Ø (j) ← (w-1) * (x-1)
3. Generate a public key U, such that, gcd (U, Ø (j)) = 1,
1< U < Ø (x)
4. Calculate the private key q, such that,
R ← U-1 mod (Ø (j))

End Procedure
End

RSA_Encryption ()
Input: Select Plain text (T1), Public key (U) and Modulus (j).
Output: Find Cipher text (C1).
Begin
Procedure (T1, U, j and C1)
C1 ← TP mod j
End Procedure
End

RSA_Decryption ()
Input: Select Cipher text (C1), Private key (R) and Modulus (j).
Output: Find Plain text (T1).
Begin
Procedure (T1, U, j and C1)
T1 ← C1 R mod j
End Procedure
End

Figure 1. Key generation, Encryption, Decryption algorithms of RSA [17].

Table 1. AES S-box.

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

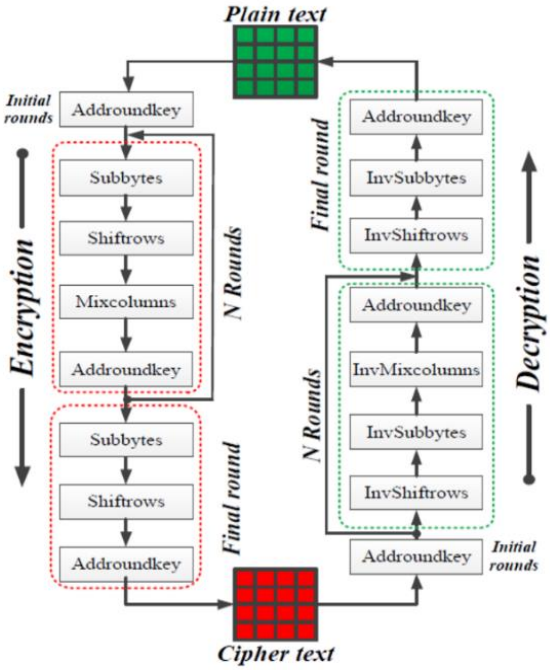

Figure 2. Flowchart of AES Algorithm [16].

Proposed Secure E-learning System

This section consists of two parts. The first is the secure registration and login process, which will utilize the concept of zero-knowledge proof, that use the logistic map, a kind of chaotic system, to produce random numbers with each recording process that makes it difficult for the attacker to attack, as there is no fixed number for all registrations. While the second part is the process of encrypting personal information and exams, using AES to prevent access by unauthorized persons.

Algorithm 1: Registration using ZKP.

Input:
Email, Password, and the rest information.
Output: Verifier, salt, Email.
Begin
Step1: Generate C- LIST using chaotic system.
Step2: Input Email, Password, and the rest information.
Step3: Salt = Random(C-LIST).
Step4: y = Hash (salt + password + Email). //using SHA56 Method
Step5: verifier = y.
Step6: Server = Client {send (verifier, salt, Email)}
Step7: DB = Server {store (verifier, salt, Email)}
END

Algorithm 2: Login and Authentication using ZKP.

Input:
Email, Password.
Output:
Authorize, no Authorize.
Begin
Step1: Input Email, Password.
Step2: Server = Client {send (Email)}
Step3: Server find (salt) based on email from DB
Step4: x = Salt. (Of the specific Email)
Step5: e = public key. // import from Xml file
Step6: d = private key. // import from Xml file
Step7: Client = Server {send (x, e)}
Step8: Y = Hash (x+ password + email). //using SHA56 Method
Step9: VERIFIER = Y.
Step10: Encryption (VERIFIER) by using RSA based on public key (e):
EncVERIFIER= (VERIFIER) ^e
Step11: Server = Client {send(EncVERIFIER)}
Step12: Server Decrypt (EncVERIFIER) by using RSA based on private key (d):
VERIFIER = (EncVERIFIER) ^d
Step13: if VERIFIER = verifier stored in DB then user is authorize or no authorize
END

Note that the verifier will be encrypted using the RSA algorithm before sending it to the server, the RSA use key length 1024-bit which is safe from attack and not slow. Figure 3 and 4 illustrate the sequence diagram of the previous algorithms.

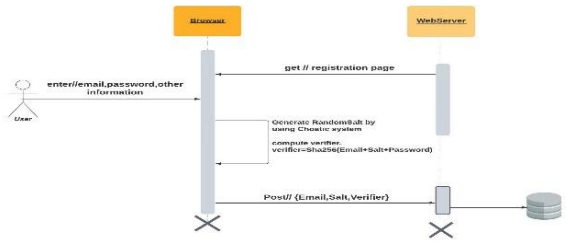

Figure 3. Sequence diagram for registration using ZKP.

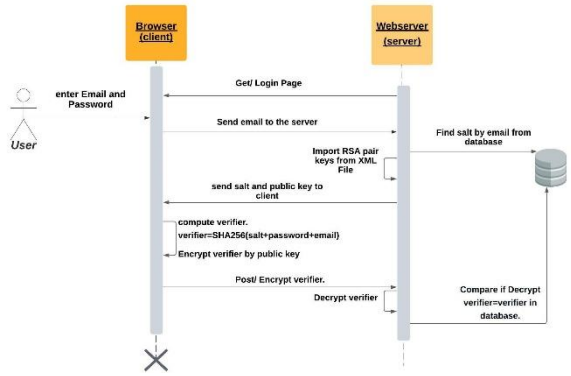

Figure 4. Sequence diagram for registration using ZKP.

Encryption Process in Proposed system

There is some sensitive information about the student and the teacher that we do not want to save in plain text. Therefore, we will take precautionary safeguards to ensure they are protected with the encryption process.
An Advanced Encryption Standard (AES) algorithm with key length 256-bit used where information would be encrypted while it was stored in the database to protect it from attackers and re-decrypt it while it was viewed in a web application.

Algorithm 3: Encrypt critical user information and Exam using AES.

Input: Personal information, Exam Information.
Output:
Encrypted personal information, Exam Information.
Begin
Step 1: Input personal information, Exam Information.
Step 2: Derive the set of round keys from the cipher key.
Step 3: Initialize the state array with the block data (plaintext).
Step 4: Add the initial round key to the starting state array.
Step 5: Perform the rounds of state manipulation (except the last round).
Step 6: Perform the final round of state manipulation.
Step 7: Insert to DB the final state array as the encrypted data (ciphertext).
END

Algorithm 4: Decrypt critical user information and Exam using AES.

Input: Ciphertext.
Output: Decrypted Information.
Begin
Step1: Input ciphertext personal information, Exam Information)
Step2: Derive the set of round keys from the cipher key.
Step3: Initialize the state array with the block data (ciphertext).
Step4: Add the InvInitial round key to the starting state array.
Step5: Perform the InvRounds of state manipulation (except the last round).
Step6: Perform the final InvRounds of state manipulation.
Step7: display the final state array out as the decrypted data (plaintext) on the screen.
END

CONCLUSION

In this paper, we summarize that a Zero knowledge Proof and RSA encryption used for validation purposes of e-learning platforms rather than using biometric that the researchers used in previous studies.

The system achieves for confidentiality, integrity and availability (CIA). Confidentiality prevents any unauthorized user from accessing confidential information. In our proposed system, only the authorized person who has the correct password will be allowed to enter the system and enjoy the services provided through it. integrity means that the data is accurate and reliable throughout the system's life cycle, as the system data can only be modified by authorized persons and availability is that the authorized user can access the information whenever they need it.

Take precautionary measures to ensure that sensitive information protected through the encryption process. In this paper, AES 256-bit key length is used which is safe against attacks because of the length of the key and different substitution and permutation functions.

REFERENCES

[1] M. A. Almaiah, A. Al-Khasawneh and A. Althunibat, "Exploring the critical challenges and factors influencing the E-learning system usage during COVID-19 pandemic," Education and Information Technologies, 2020.

[2] T. Favale, F. Soro, M. Trevisan, I. Drago and M. Mellia, "Campus traffic and e-Learning during COVID-19 pandemic," Computer Networks, 2020.

[3] A. El Mhouti, M. Erradi and A. Nasseh, "Using cloud computing services in e-learning process:Benefits and challenges," Education and Information Technologies, 2018.

[4] M.J. Mohammed," An Implementation of E-Learning Application Using Cloud Computing," M.S. thesis, Computer Sciences Dept., Technology Univ.,Iraq,2017.

[5] M. A. Rodrigues, P. Chimenti and A. R. Nogueira, "An exploration of eLearning adoption in the educational ecosystem," Education and Information Technologies, 2020.

[6] M.A.Ali, "Smart E-Learning Platform for Selective Courses," M.S. thesis, Informatics Institute for Post Graduate Studies, Iraqi Commission for Computers and Informatics.,Iraq,2019.

[7] B. Gilbert ," Online Learning Revealing the Benefits and Challenges," M.S. thesis , Education Dept., St. John Fisher College,2015.

[8] M. Messerschmidt and M. Pleva, "Biometric systems utilizing neural networks in the authentication for e-learning platforms," in 2019 17th International Conference on Emerging eLearning Technologies and Applications (ICETA), 2019, pp. 518-523: IEEE.

[9] G. S. S. Jose and C. S. J. C. C. Christopher, "Secure cloud data storage approach in e-learning systems," vol. 22, no. 5, pp. 12857-12862, 2019.

[10] E. Okoh, M. H. Makame, and A. I. J. I. S. J. A. G. P. Awad, "Toward online education for fingerprint recognition: A proof-of-concept web platform," vol. 26, no. 4, pp. 186-197, 2017.

[11] W. Major, W. J. Buchanan and J. Ahmad, "An authentication protocol based on chaos and zero knowledge proof," Nonlinear Dynamics, 2020.

[12] N.SH. Hameed, " Secure E-Voting System Using Biometrics and Zero- Knowledge Proof," M.S. thesis, Computer Sciences Dept., Mustansiriyah Univ.,Iraq,2020.

[13] N. S. Hameed and B. M. Nema, "Secure E - Voting System using Voiceprint," Journal of Al Rafidain University College, 2019.

[14] R. Lingappan, "What Is Secure Remote Password (SRP) Protocol and How to Use It?," medium.com, 20 NOV 2019. [Online]. Available: https://medium.com/swlh/what-is-secure-remote-password-srp-protocol-and-how-to-use-it-70e415b94a76. [Accessed 16 October 2020].

[15] B. Soewito and Y. Marcellinus, "IoT security system with modified Zero Knowledge Proof algorithm for authentication," Egyptian Informatics Journal, 2020.

[16] S. Saxena and B. Kapoor, "an efficient parallel algorithm for secured data communications using RSA public key cryptography method," in 2014 IEEE International Advance Computing Conference (IACC), 2014.

[17] SH.J. Mohammed," Secure Web Application Monitored By Intelligent Agent," Msc. thesis, Computer Sciences Dept., Mustansiriyah Univ.,Iraq,2020.

[18] M. A. eltatar , " Modified Advanced Encryption Standard Algorithm for Reliable Real-Time Communications," M.S. thesis , College of engineering, The Islamic Univ, Gaza,2017.

[19] O.G. Abbood, "Enhancing Cryptographic Security based on AES and DNA Computing," Ph.D. dissertation, Dept ofInformation Technology, Alexandria Univ,EGYPT,2019.

[20] A. M. Abdullah, "Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data," Cryptography and Network Security, 2017.

[21] B. M. Nema, " Automatic passkey generator using speech biometric features", AIP Conference Proceedings, Vol. 2290, Issue 1 , Dec. 2020; https://doi.org/10.1063/5.0027417

[22] A. N. Abdulraheem and B. M. Nema, "Secure IoT Model Based on PRESENT Lightweight Modified and Chaotic Key Generator," 2020 1st. Information Technology to Enhance e-learning and Other Application (IT-ELA, 2020, pp. 12-18, doi: 10.1109/IT-ELA50150.2020.9253079.

How to Cite

Rafee, R. M., & Nema, B. M., **Secure E-Learning System Based on ZNP and AES**. *Al-Mustansiriyah Journal of Science, 33*(1), 39–44, 2022. Doi: https://doi.org/10.23851/mjs.v33i1.1016