Journal of Theoretical and Applied Information Technology
31st March 2018. Vol.96. No 6

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A NOVEL AUTHENTICATION AND AUTHORIZATION MODEL BASED ON MULTIPLE ENCRYPTION TECHNIQUES FOR ADOPTING SECURE E-LEARNING SYSTEM

[1]SHADI R.MASADEH, [2]JAMAL S.ZRAQOU, [3]MOUTAZ ALAZAB

[1]Isra University, Faculty of Information Technology, Department of CIS, Amman, Jordan
[2]Isra University, Faculty of Information Technology, Department of Multimedia, Amman, Jordan
[3]College of Qatar, Faculty of Information Technology, Department of Information Technology, Qatar

E-mail: [1]Shadi.almasadeh@iu.edu.jo, [2]Jamal_sam@iu.edu.jo , [3]moutaz.alazab@ccq.edu.qa

ABSTRACT

The era of e-learning systems among educational organisations has grown exponentially. Educational organisations have a competition to provide a secure wireless network service to staff members. In this paper, a novel authentication and authorization model (NAAM) has been presented to securely transmit the data in e-learning environment without affecting the system resources. As a part of the analysis, multiple encryption methods and face recognition technique are utilized to develop a complete secure e-learning model. MAC address filtering over the wireless network together with the application of pretty good privacy (PGP) encryption algorithm are presented. This model may be termed as hybrid security and authentication scheme (HSAS). The main contribution of this research is to achieve maximum security level. This was achieved by integrating the strength of OpenVPN, HMAC, AES, VLAN, sWIFI, PGP, SSL and faces recognition. The conducted experiments revealed that the performance of the proposed model has surpassed the related works in terms of security enhancements during data transmission in e-learning environment systems.
.

Keywords: *OpenVPN, PGP, sWIFI, HMAC, cryptography, face recognition, and firewall.*

1. INTRODUCTION

In recent years, the popularity of e-learning among educational organizations has grown exponentially and is still growing. Nowadays, educational organizations provide wireless network to students, visitors and staff members for both academic and administrative works access materials at any time and place convenient for them. Consequently, tight security measure must be used to convert the wild-and-woolly wireless communication links into a connection with node-to-node protections.

In a wireless virtual class system, students and university servers need to authenticate each other. Various authentication protocols have been proposed over the past few years such as the authentication protocol of Aziz and Diffie [1] and that of Beller et al. [2] using mutual certificate between client and server. The public key cryptography techniques and off-line certification procedures were utilized in [3] [6] to maintain data transmission.

To our knowledge, MAC filtering and HSAS are considered as the main security services for most of e-learning systems. This can be lead providing fake MAC addresses and IP Spoofing. The presented work is the first which integrates face recognition along with the physical layer address filtering protocol over the wireless network to develop an enhanced security system (HSAS) in e-learning environment systems. The aim of this work is to present a more secure e-learning system model which can be applied in educational organisations. This model might facilitate e-learning services such as online learning, instant messaging, assignments, and online exams. Based on the wireless connection, which is provided by educational organizations, the proposed model offers a secure e-learning system by utilizing modern technologies such as firewalls, VLAN, VPN, PGP and AES that have been adopted and integrated along with faces recognition technique.

This paper is organised as follows: Section 2 discuss the contributions from the relevant literature. Section 3 describes our model, including

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

the e-learning environment, our hybrid secure and authentic scheme and face features detector method. Section 4 we analyse and discuss the experimental results. Section 5 delivers a discussion on the limitations of our work and its suggestions for future work.

2. RELATED WORKS

Several research articles in the field of e-learning security have been developed in the past few years, early research focused on information security management, installation of antivirus and firewalls, standard encryption, authentication and authorisation techniques. There have also been attempts to adopt complex models such as applying face recognition, data mining, intrusion detection system (IDS) and open virtual private network tunnel in both wireless and wired network.

Providing a secure e-learning system is the main key factors in building safe learning environment, protecting sensitive data and accessing the internet safely and responsibly. An in-depth study of a range of cyber-security concerns in e-learning educations by Bandara et al. [7] found that there are several internal attacks, deficient IT policies and procedures and security vulnerabilities in e-learning systems. This research is supported by Alwi and Fan [8], who address the most security threats to e-learning systems. Saleh and Whaid [14] content that e-learning system that contains basic security aspects (e.g. authenticity, access control list, confidentiality, integrity, availability and non-repudiation) are more likely to stay longer in education organisations. It is claimed by Warren and Hutchinson [9] that security perspective in e-learning systems is neglected. The purpose of this paper is to investigate weaknesses in e-learning systems and to develop a trustworthy model for protecting e-learning systems against these weaknesses. The issue of security of e-learning systems has been neglected until recently, as the majority of the research articles have focussed on the performance side of e-learning.

The research by Miguel et al. [10] develop a trustworthiness model based on hybrid evaluation to deliver a secure e-learning assessment. Five principles have been chosen to determine whether e-assessment is secure or not secure being as follows: Availability, Integrity, Identification and Authentication, Confidentiality and Non-repudiation. They select five factors types: types of subjects, specific evaluation model, evaluation application and agents. The authors employ the digital certificate in conjunction with PKI to ensure the integrity and authorship. In the next step, their model logs the ratings, questionnaires, student report and LMS usage indicators through statistical analysis of Pearson correlation coefficient. Since the collected data were very large, they applied a parallel processing approach to speed up the structuring and processing of the logged data. For future work, the authors plan to select real subjects, and then evaluate their methodology. Whilst this research is limited to e-learning assessment, it does point to that a complex security design is vital in any e-learning environment. It is with mentioned that our model is not limited to e-learning assessment, but our model is extended to cover other e-learning services such as (exams, assignments, instant messaging, dynamic visual, sound, user interactivity, reporting) to establish a secure connection between lecturers and students.

Fayyoumi and Zarrad [11] present an automated system that uses face recognition to authenticate students for attending their online exams. The system includes a face recognition biometric system which takes as input image, parse, encrypt and transmit the facial features to the server to match against the stored images. The system continuously compares the facial images during the whole session to check if the authorised user has accessed the exam and has not changed. Subsequently, they conducted two surveys on 8 instructors and 32 students respectively. The goals of the surveys were to identify the rate of image capture and the number of times the suspicious behaviour is accepted without affecting students' concentration during the exam. We demonstrate, in our work, that face-recognition are similarly could be applied in e-learning since it can restrict unauthorized access without affecting the students' concentration during the online exams.

The work of Pradhan and Kullkarni [12] focus on applying data mining techniques in e-learning environments. The authors demonstrate that e-learning system consists of enormous sensitive information such as student records, learning courses records, course materials, visualizations of media, and therefore it is very important to protect those sensitive data using a complex system. The proposed system consists of two modules as follows: Admin Panel and Learner Panel. The learner panel make use of the web browser to interact with e-learning system. While the admin panel performs the admission tasks such as managing the credential and observes learner behaviour. In their system, the authors also applied the concept of public key cryptography. In the next

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

step, they applied data mining approaches such as association rules, inter-session and intra-session to extract features that can help both students and educational administrators to assess the course activity. The results show that data mining techniques aids for proper recommendation and administration.

In the work conducted by Patel et al. [13], the authors propose a model that embraces network topology and associated network security techniques. They investigate various security threats in both wired and wireless networks, the authors assert that e-learning system should contain various security mechanisms such as VPN devices, IDS, Public-Key Infrastructure, LAN Switches, Network Infrastructure Switches, Use of Genetic Algorithm, Bring Your Own Device and Mac address filtering. Their model authenticates Mac addresses, IP Address and password in the RADIUS server. In order to create a neutral zone between the internet and intranet, they used DMZ (demilitarized zone), which have a centralized antivirus installed. The concept of Virtual Local Area Network (VLAN) has been adopted to increase the level of security and flexibility. In the last step, the authors use various IT security and policy mechanisms such as IT security policy, risk assessments, multilevel authentication mechanism, restrict unauthorized access, use of encryption and decryption, organize access control list, review access point regularly and training to all the network users. Their results indicate by implementing their proposed model, the number of security incidents has been diminished by 50%. In our case, our system is based on an automated process by using various multifaceted security techniques such open VPN tunnel, Mac filtering, firewall, HSAS, VLAN, a combination of TKIP and AES encryption on the same SSID rather than the use of standard techniques, which can be more useful to security and privacy.

The authors of Sun and Wang [15] investigate the effectiveness of using access control and authorization in e-learning environments. In their work, the authors propose a secure architecture application that based on client and server side to protect e-learning systems against unexpected or malevolent attacks. Their application consists of two modules as follows: access control model and authorization model. The access control model consists of eight components: subjects, subject attributes, objects, object attributes, rights, authorizations, obligations and conditions in a usage control model (UCM). While, the authorization model depends on three decision factors being as follows: authorizations, obligations and conditions. They assumed six possible cases for usage control: pre-Authorizations, ongoing-Authorizations, pre-Obligations, ongoing-Obligations, pre-Conditions and ongoing-Conditions. Subsequently, they deliberate a control mechanism of electronic documents using reference monitors. The authors discussed the implementation of reference monitors on the server side, on the client side and on both server and client sides. The authors found that implementation of reference monitors on both server and client side leads for better security. The authors plan to develop an algorithm in real implementations. Similarly, in our case, we integrate a MAC addresses filtering protocol over the wireless network with the pretty good privacy (PGP) encryption algorithm using unique features extracted from faces recognition method.

3. THE PROPOSED WORK

This section demonstrates the structural design of our proposed system to develop a secure e-learning model. The proposed methodology and implementation consist of three phases for building the model, are being discussed as follows: high secure E-learning environment that is introduced in section 3.1. Our hybrid security and authenticated system are presented in section 3.2. The Face Features Detector Method is used to generate private key is illustrated in section 3.3. The summary of our presented work is discussed in section 3.4.

3.1. The Proposed E-learning Environment

Nowadays in any academic institution, providing a securely wireless connection is a prominent requirement. E-learning systems encompass of a basic wireless connection, which can used by students, employees and academic staff, through connecting them to remote databases and online courses. The security requirements such as confidentiality, integrity and availability (CIA) must be considered to achieve safe data transmission. Hence, the security system sought must satisfy CIA requirements, which includes checking the e-learning vulnerabilities, abiding security rules, evaluating data security and standing against male violent attacks. To fulfil the CIA requirements, hybrid secure and authentic scheme (HSAS) is designed to exploit the aforementioned security measurements as illustrated in Fig 1.

Journal of Theoretical and Applied Information Technology
31st March 2018. Vol.96. No 6

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

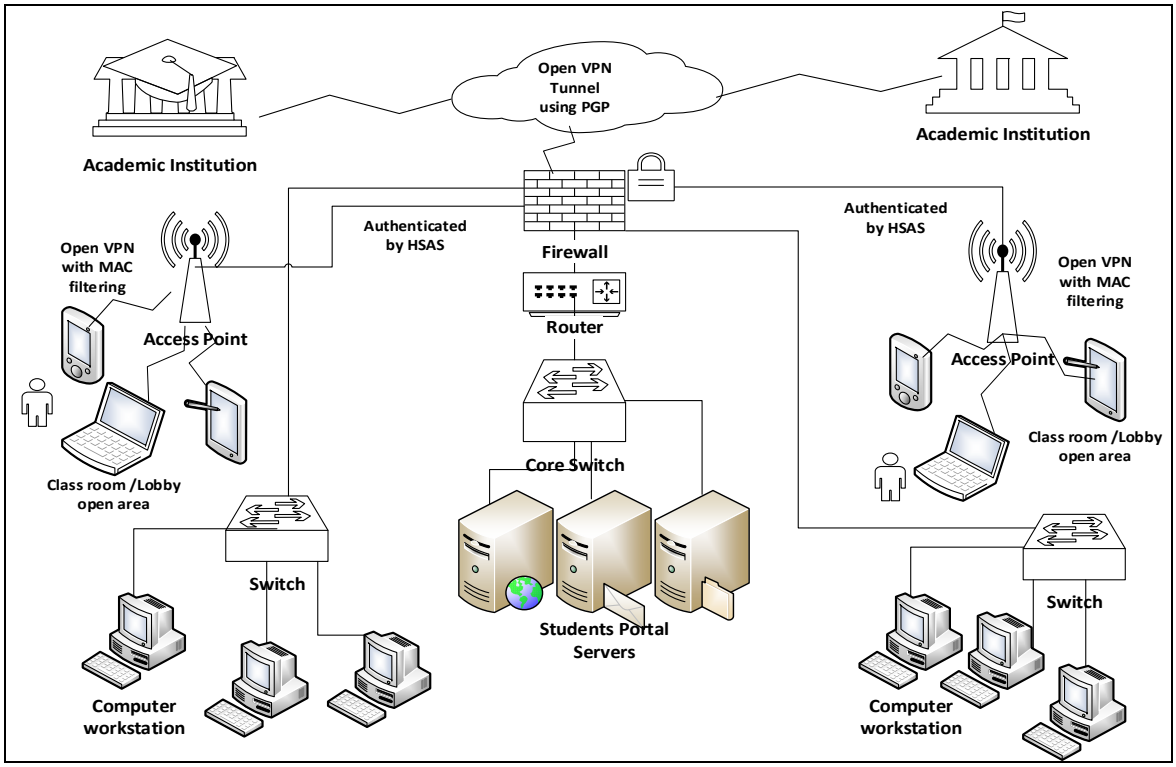

Figure 1:The proposed HSAS Framework

As shown in figure 1, educational organisation is composed of various groups of wireless applications (e.g. firewalls, routers, switches and servers) and computer workstations (e.g. personal computers, terminals, scanners, printers, Laptops, PDAs, tablets and smart phone devices). Those computer workstations are connected with wireless applications through either cable or WIFI connections. These academic sites are connected with each other through the internet.

Each one of the computer workstations are connected to the access point, where the validation is managed by VPN and MAC filtering. Users are authenticated by the proposed scheme (HSAS) prior the connection of the core switch via the firewalls and routers. Consequently, the core switch is being used to connect the servers of students' portal that guarantees more security features. The firewall that is connected with the core switch to provide more protection for the entire network. VPN tunnel using PGP is used to remotely connect academic institutions. Access points with VPN tunnel with MAC address filtering are used to establish the wireless connections. Temporary Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES) are employed to apply encryption. HSAS method is implemented to maintain integrity and authentication as shown in section3.2. Active directory service is activated on the server of students' applications to authenticate logged users.

All the switches in the entire network are connected to the protected core switch. VLAN connection is used to provide more security and efficient services by separating different networks that are related to several faculties and departments.

Firewall is also used to control the incoming and outgoing traffics based predefined conditions and rules. Replacing the IPSec VPNs service that has several drawbacks such as: not cheap, not easy to be used, costs more time for configurations; Open VPN is used. The complexity of IPSec is avoided by using SSL/TLS and SSH protocols

The most security features of VPN/SSL that includes load balancing of site-to-site remote access and Wi-Fi security are included in the VPN

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

service. There are two types of Open VPN authentication as follows:

- Static/Conventional key: The tunnel uses a pre-shared conventional/static key, which is created and shared between two nodes. The generated key includes four independent keys: Hash based Message Authentication Code (HMAC) send key, HMAC receive key and encrypt key\ decrypt key. The involved nodes are using the same keys.
- SSL/TLS and SSH: digital certificates of authentication and key management with the secure shell are employed with the involved protocols. The authentication is succeeded based on digital certificate provided for each node by applying encryption/decryption along with HMAC keys that are generated randomly over the SSL/TLS connection.

Emails are being secured using the PGP that exists at the presentation layer protocol by using one encryption/decryption key. In summary, the process of combining Open VPN and PGP provides two benefits: firstly, establish a secure channel between two nodes using VPN with SSL/TLS and second-layer of encryption that uses digital certificates and HMAC keys. Secondly, public and private key pairs using RSA are provided to apply the encryption/decryption of the PGP algorithm.

3.2. The Proposed Hybrid Secure and Authentic Scheme (HSAS)

To enhance the security and authentication of e-learning environment, the following scheme is proposed. We use of HMAC algorithm, secret random value (S_Value), RSA, PGP, and sWIFI algorithm. This scheme is termed hybrid secure and authentic (HSAS). The encryption of a message by HSAS is illustrated in Fig 2. In the HSAS algorithm, the hash of the message M (i.e. HMAC) is concatenated with a secret random value (S_Value) and together, they are encrypted by RSA using the sender's private key Krs which is obtained from the feature detector (FD) of the authenticated user (Please refer to section 3.3 for better understanding). This encrypted value is concatenated with original message M to be encrypted using PGP prior to the application of sWIFI algorithm. Finally the resulting encrypted message is sent to the receiver over the channel.To enhance the security and authentication of e-learning environment, the following scheme is proposed. We use of HMAC algorithm, secret random value (S_Value), RSA, PGP, and sWIFI algorithm. This scheme is termed hybrid secure and authentic (HSAS). The encryption of a message by HSAS is illustrated in Fig 2. In the HSAS algorithm, the hash of the message *M* (i.e. HMAC) is concatenated with a secret random value (S_Value), they are encrypted by RSA using the sender's private key Krs which is obtained from the feature detector (FD) of the authenticated user. This encrypted value is concatenated with original message M to be encrypted using PGP prior to the application of sWIFI algorithm. Finally, the resulting encrypted message is sent to the receiver over the channel.

3.3. Face Features Detector Method (FFD)

Feature selection is referred to as attribute selection, or attribute reduction. Finding a subset of features and discarding irrelevant, redundant, and noisy features among the entire features are imperative goals. Based on the literature review in the computer vision, several feature extraction schemes have been examined for recognizing faces. One class of methods extracts holistic face features such as Laplace an faces(He, Yan, Hu, Niyogi, & Zhang) [17],Eigen faces(Turk et al),[18],and Fisher faces(Belhumeur et al),[16] Extracting patches around eyes or nose is another class of methods to find meaningful partial facialand discard irrelevant and noisy features. Based on our experiments, it was revealed that the library of face recognition that is provided by the OpenCV(opencv.org) has approved efficient and robust face identification. The private key is represented by face identification as shown in Equation (1).

$$Krs = I(C) + I(A) - I(B) - I(D) \ldots\ldots. \text{ Eq (1)}$$

Where:

The points A, B, C, and D are related to the integral image (I)

The integral image (I) is a 2-D lookup table forming a matrix that has the same size of the original image.

The steps of HSAS authentication shown in Fig. 2 at the sender side are being addressedas follows:

1- The user creates the original message. The generator creates the HMAC along with the secret random value (S_Value).
2- Concatenate the S_value with HMAC.
3- Extract the value of *Krs* using the feature detector (FD).

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

4- Ciphering the result of step 2 by RSA using the private key of the sender as follows :

$$C = E_{Krs(S\_Value \| HMAC)} \ldots\ldots\text{Eq (2)}$$

5- Concatenate the result of step 3 with the original message as follows:

$$C = M \parallel E_{Krs(S\_Value \| HMAC)} \ldots\ldots \quad \text{Eq (3)}$$

6- Ciphering the result of step 4 by PGP as follows:

$$C1 = Epbk_{(M \| E_{Krs(S\_Value \| HMAC)})} \ldots \text{Eq (4)}$$

7- Ciphering the result of step 5 by sWIFI as follows:

$$C2 = E_{sWIFI(C1)} \ldots\ldots \text{Eq(4)}$$

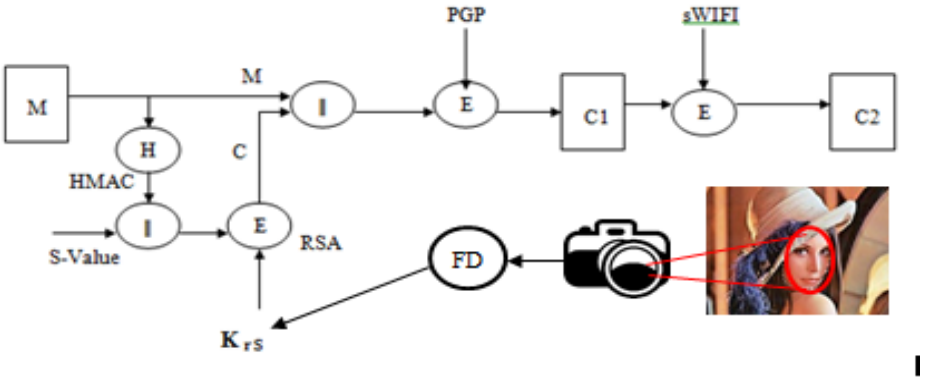

Figure 2: Sender's Authentication by HSAS.

Once the original message arrives receiver side,it can be decrypted using the HSAS algorithm in reverse order as illustrated in Fig 3.The HSAS authentication steps at receiver side:

1. Accept the cipher text from the sender side as shown in Equation (5).
2. The receiver will decrypt the cipher text (C2) as follows:

$$C1 = D_{sWIFI(C1)} \ldots\ldots\ldots\ldots\ldots\text{Eq (5)}$$

3. Decrypt the result of step2 by PGP as follows:

$$M = Dpbk_{(M \| E_{Krs(S\_Value \| HMAC)})} \ldots \text{Eq(6)}$$

4. Compare the input Krs value from the sender with the central database of the faces features values. If the match is passed then go to step 5.
5. Decrypt the result of step 3 as follows:

$$M = D_{Krs(S\_Value \| HMAC)} \ldots\ldots \text{ Eq (7)}$$

6. Extract the random S_value with HMAC
7. Compare the original messages between the sender and the receiver. The message will be considered authenticated if they are the same.

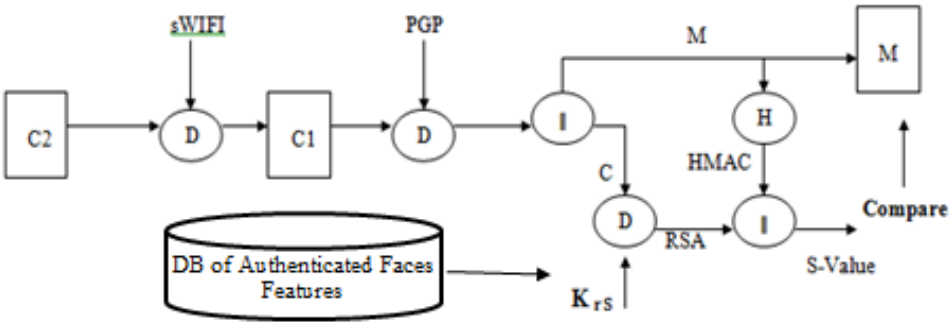

Figure 3: Receiver's Authentication by HSAS.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

3.4 Summary

A Hybrid Secure and Authentic system was proposed. Several Encryption Methods were employed using faces recognition technique to achieve more security level than the investigated related works. Hence, a set of extracted features for a given face was used to generate the private key. The novelty of this work is the process of integrating MAC address filtering technique with PGP, Open VPN tunnel, and Firewall together with image processing method such as FDD to build a robust security system in E-learning environment.

4. EXPERIMENTAL RESULTS & EVALUATION

Comparisons with the other eLearning models have been conducted to show the performance of our proposed model. ELearning systems at Isra University (IU), Al-Hussien Bin Talal University (AHU), Applied Science University (ASU), Al-Hasad School, and the International School of Choueifat are involved in the comparisons. Six types of comparisons were performed; the first is depending on the availability of the intrusion detection system (IDS). The second is using an OpenVPN with MAC filtering to guarantee the authority of logged users from specific terminals. The third is employing the new method called HSAS to authenticate logging users. The fourth is integrating the PGP service to encrypt the transmitted data over the network in the initial phase. The fifth is employing the sWIFI service as a secure second layer. Finally adding the face recognition technology to generate the private key for ensuring the authenticated users. Based on the proposed model, our model has outperformed the involved environments in terms of the availability of the six criteria as shown in Table 1.

Table 1: Comparisons between NAAM and ELearning systems at academic institutions

	Network Security			Encryption		
ELearning Environment	IDS	OpenVPN with MAC filtering	HSAS	PGP	sWIFI	Face Identification
NAAM	☑	☑	☑	☑	☑	☑
IU	☑	☑	☒	☒	☑	☒
ASU	☑	☑	☒	☒	☒	☒
AHU	☒	☑	☒	☒	☒	☒
AL-HASAD SCHOOL	☑	☑	☒	☒	☒	☒
THE INTERNATIONAL SCHOOL OF CHOUEIFAT	☑	☑	☒	☒	☒	☒

After investigating the eLearning environments of the involved academic institutions, it was founded that IU supports IDS, OpenVPN with MAC filtering, and sWIFI, ASU employs IDS and OpenVPN with MAC filtering, AHU only supports OpenVPN with MAC filtering, where the proposed NAAM approach employs IDS, OpenVPN with MAC filtering, HSAS, PGP, sWIFI, and Face Identification as shown in Figure 4.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

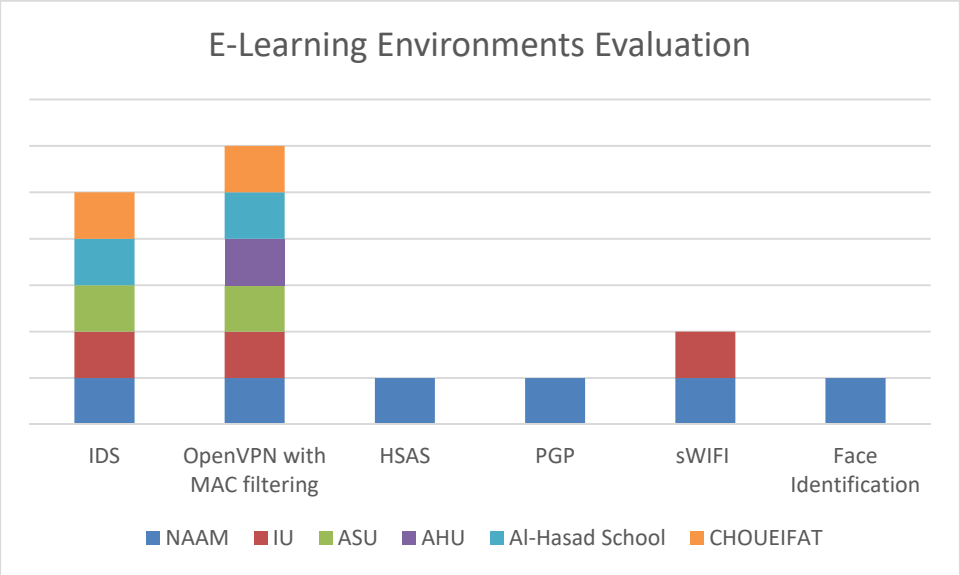

Figure 4: The results of the conducted experiments reveal the performance the proposed NAAM approach.

In summary, it can be concluded that the proposed NAAM approach is the only approach that satisfies the adopted criteria. This means the ELearning environment system with the proposed NAAM is under a more secure environment than related approaches in terms of security.

5. CONCLUSION AND FUTURE WORK

In this research study, the focus is to provide a more secure ELearning environment system by employing several techniques such as IDS, OpenVPN with MAC filtering, HSAS, PGP, sWIFI, and Face identification. This research presents several contributions as follows: Firstly, HSAS is employed to authenticate logging users. Secondly, PGP is integrated to encrypt the transmitted data over the network in the initial phase. Thirdly, sWIFI is used to protect data as a secure second layer.

Finally, Face identification is applied for users to create the private key for applying data encryption and to confirm the authenticity of users.

The future work can be extended to implement SHA-1 Algorithm to protect data transmission over the network and to ensure the identity of sender's. Thermal hand held technology which utilizing the blood tissues of the human's hand to identify users can be used to authenticate users.

ACKNOWLEDGMENT

The authors would like to thank of Isra University (Jordan) for giving us the opportunity to perform and publish this research work.

REFERENCES

[1] A. Aziz A., and W. Diffie, "A secure communications protocol to prevent unauthorized access: privacy and authentication for wireless local area networks", IEEE Personal Communications, 1994, PP25-31

[2] Diffie W., P. C. Van Oorschot and M. J. Wiener, "Authentication and authenticated key exchanges", Designs, Codes and Cryptography, vol. 2, 1992, PP107-125.

[3] Beller M. J. , L. F. Chang and J. Yacobi, "Privacy and authentication on a portable communication system", IEEE Journal on Selected Areas in communications, vol. 11, no. 6, pp. 821-829, 1993.

[4] Park C. S., "On certificate-based security protocols for wireless mobile communication systems", IEEE Network, vol. 11, no. 5, 1997, PP 50-55.

[5] Menezes A., L. Van Oorschot and S. Vanstone, "Handbook of applied cryptography ", CRC Press, Boca Raton, FL, USA, 1997.

[6] Garg V. K. and J. E. Wilkis, "Wireless and personal communication systems", Prentice-Hall, Upper Saddle River, NJ, USA, 1996.

[7] Bandara, I., Ioras, F. and MaherI, K., 2014, November. Cyber security concerns in e-

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

learning education. In Proceedings of ICERI2014 Conference, 17th-19th November.

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

[9] Warren, M. and Hutchinson, W., 2003, August. Information security–an e-learning problem. In International Conference on Web-Based Learning (pp. 21-26). Springer Berlin Heidelberg.

[10] Miguel, J., Caballé, S., Xhafa, F. and Prieto, J. "Security in online learning assessment towards an effective trustworthiness approach to support E-learning teams", In Advanced Information Networking and Applications (AINA), 2014 IEEE 28th International Conference on (pp. 123-130). IEEE.

[11] Fayyoumi, A. and Zarrad, A. (2014) Novel Solution Based on Face Recognition to Address Identity Theft and Cheating in Online Examination Systems. Advances in Internet of Things, 4, 5-12. doi: 10.4236/ait.2014.42002.

[12] Pradhan, P.R. and Kulkarni, R.B. (2016) Secure E-learning using data mining techniques and concepts. International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), (pp. 1498-1501). IEEE.

[13] Patel, A., Ghaghda, S. and Nagecha, P. (2014) Model for security in wired and wireless network for education. International Conference on Computing for Sustainable Global Development (INDIACom), (pp. 699-704). IEEE.

[14] Saleh, M.M. and Wahid, F.A. (2015) A Review of Security Threats by the unauthorized in the E-learning. Int. J. Comput. Technol, 14(11), pp.6240-6243.

[15] Sun, L. and Wang, H. (2011) Access control and authorization for protecting disseminative information in E-learning workflow. Concurrency and Computation: Practice and Experience, 23(16), pp.2034-2042.

[16] Belhumeur, P. N., Hespanha, J. P., & Kriegman, D. J. (1997). Eigenfaces vs. fisherfaces: Recognition using class specific linear projection. IEEE Transactions on pattern analysis and machine intelligence, 19(7), 711-720.

[17] He, X., Yan, S., Hu, Y., Niyogi, P., & Zhang, H.-J. (2005). Face recognition using laplacianfaces. IEEE Transactions on pattern analysis and machine intelligence, 27(3), 328-340.

[18] Turk, M., & Pentland, A. (1991). Eigenfaces for recognition. Journal of cognitive neuroscience, 3(1), 71-86.