The Role of SSL/TLS, IPsec & IKEv2 Protocols in Security of E-learning System's Communications, A Study & Simulation Approach

Afshin Zivi[1], Gholamreza Farahani*[2], Kooroush Manochehri[3]

[1]MSc Lecturer of Computer Networks at Department of Computer Engineering and IT, Parand Branch, Islamic Azad University, Parand New Town, Iran
[2*]Assistant Professor and Faculty Member of IT Engineering Group at Department of Computer Engineering and IT, Parand Branch, Islamic Azad University, Parand New Town, Iran
[3]Assistant Professor and Faculty Member of IT Engineering Group at Department of Computer Engineering and IT, Parand Branch, Islamic Azad University, Parand New Town, Iran

Abstract *—E-learning is a new educational concept that provides digital content and learner-centered environment for both student and teacher. Security on all systems is an important way to organize it, since internet as the backbone of all systems is considered unsafe and in fact transfers all the communicational transactions in the e-learning system, thus intruders and attackers can abuse security holes, and cause troubles for the system. E-learning system must be secure against threats and manipulations by intruders as well as to protect student privacy. Security is a basic principle in the development of networks, however, the lack of security procedures that can be easily implemented, is fully tangible, and because, an e-learning system mainly provides services through its varied services' networks to users, so the lack of security mechanisms can cause irreparable damage to the system. The aim of this study was to evaluate and compare the protocols of SSL/TLS, IPsec, and IKEv2 to secure communications of e-learning system. It should be noted that all obtained solutions including securing e-learning system with the help of the above-mentioned protocols is based on the administrative-technical model presented in the previous study.*

Key words —E-*learning system, security, SSL/TLS protocol, IPsec protocol, IKEv2 protocol*

I. INTRODUCTION

Recently internet has had a huge impact on the community and it has created a revolution in the 21st century. With the development of information and communication technology, the field of education cannot be isolated from internet and communication [1]. E-learning in a variety of fields such as distant learning, online learning, and network-based learning, and generally learning is made to promote interactions among students, lecturers and learning community [2]. This learning method has several advantages over the traditional learning, especially the ability to learn at any time and any place in this method is quite tangible [3, 4].

Security is very important for e-learning and M-learning (Mobile learning). In an end-to-end communication there are several security risks that should be identified. These risks are presented in Table 1 [5].

Table 1 provides multiple security threats, lack of safety, and security solutions for these kind of systems, and these solutions can generally be classified as follows [5]:

- Identifying the client, server, service, and instructor requires a strong authentication model to ensure legitimacy of components that have access to related channels.
- Maintaining the privacy of message is required for any channel that carries secure communications between server, teacher, and users. This goal is achieved by powerful encryption techniques.
- Message integrity is a security mechanism in which message privacy is not a problem, although messages should not be replaced by any illegal component. This goal can be realized by using hedonic functions.
- Non-denial models prevent legal users to deny their involvement in a legal relationship.
- A Man in the Middle (MITM) attack is a security breach or hole in which the attacker attempts to communicate with the user by forging the identity of a legitimate user and stop its' system, and as a consequence this attack would lead to further access and more advanced attacks.
- Denial of Service (DoS) attack, is a set of multilayer attacks where the attacker interrupts all channels with interrogative continuous and unusual messages and hence, the access of legitimate users to the channel is blocked; this attack may also lead to increased power

consumption and therefore, discharge of backup battery power [5].

Table 1: Security Issues in E-Learning and M-Learning Systems, Observations and Remedies [5]

Security Issue	Cause of Lack of Security	Security Remedy
Client Security	Illegitimate user accessing one channel	Strong client authentication
Server Security	Illegitimate entity servicing over many channels	Strong server authentication
Service Security	Illegitimate service running on many channels	Strong service ID authentication
Instructor Security	Illegitimate admin accessing all channels	Strong admin authentication
Message Privacy	Messages contents exposed to illegitimate users	Strong encryption algorithm
Message Integrity	Messages altered by illegitimate users	Strong hashing algorithm
Non-Repudiation	Legitimate users deny their involvements in a session	Strong digital signature algorithm
MITM Attack	Illegitimate user masquerading a user or a server taking over a session	Strong symmetric mutual authentication scheme
DoS Attack	Service unavailable to legitimate users	Multilayer deterrence schemes

II. LITERATURE REVIEW

Effectiveness of a system which states that a successful system, is in fact, placed within user satisfaction and its impact on individuals and organizations, was studied in the past. The basic parameters that affect the effectiveness of an information system depend on two things: the organizational context and the technical context. For the organizational context, the most important factors are: management support, user education, communication effectiveness, and organization size. Regarding the technical background, two necessary features are considered, including: quality of system and quality of information [6-8]. With this definition, it can be said that approximately in the previous research, investigation and analysis of the performance of the E--learning system was about 70% related to the system management, and 30% related to technical issues, since in order to provide security and technical solutions, the need for an administrative-technical model is quite obvious [9].
When developing a secure network, the following needs should be taken into account [10]:

- Access: allowed users must be able to communicate with the service provider's systems through a specific network.
- Confidentiality: in-network information should remain private and confidential.
- Authentication: ensure that the user is exactly the person who claims it.
- Integrity: ensure that the message has not changed during the transfer.
- Non-denial: ensure that the user who has used the network, cannot deny it.

Most of the innovations in the field of e-learning content concentrate on Sharable Content Object Reference Model (SCORM) and sending it, while in the field no attention is paid to the privacy and security as an essential component. However, there's an increasing need for higher levels of confidentiality and privacy in e-learning applications, and these security technologies must be designed and implemented in a way to cover the existing needs [11].

Compared to other studies such as: Suthilux Chansuc, Prasong Praneet Polgrang in 2008, Yasir Eltigani Ali Mustafa & Sami Mohamed Sharif studies in 2011, Ayman El Sayed Khedr studies in 2012, [14] as well as Yongmei Bentley, Habte Salassie, and Anjali Shegunshi in 2012 [15], evaluation and improvement of e-learning systems in terms of learning, quality of the issues raised, quality of the system, relationship between teacher and student, and to a degree the discussion of the effectiveness of this learning method is generally addressed. So according to the mentioned issues, the necessity of evaluating the e-learning system and generally the e-learning, taking into account security issues and covering the existing gaps in this area, as well as the issue of the integrity and optimality, this type of learning system seems to be more important than the past.

E-learning has a broad concept, and is divided into 2 types of synchronous and non-synchronous. Both methods have different features and use different methods to deliver learning content. Non-synchronous e-learning occurs when students begin and complete their training at different times according to their scheduling plan. Synchronous e-learning has a two-way interaction that generates and increases communication and sociality among students [1].

Features and methods of administration and management of each of these two methods is shown in Table 2. Synchronous e-learning is much more effective than non-synchronous, because student motivation can be enhanced which is obtained through face-to-face features or writing of views. Also, in the type of synchronous, the classroom has a higher degree of satisfaction during the course [1].

Table 2: Details of Synchronous and Asynchronous E-Learning Methods [1]

E-Learning Types	Common Features	Conducting Ways
Asynchronous E-Learning	Intermittent on-demand access	Message Boards
	Previously recorded or pre produced	Discussion Groups
	Just in time	Self-Paced Courses
	Individual or poorly collaborative	Computer aided System
	Independent learning	Podcasting
	Self-paced	Web-based Training
Synchronous E-Learning	Real-time	Shared Whiteboard
	Live	Virtual Classrooms
	Scheduled	Audio and Video Conferencing
	Collaborative	Online Chat
	Co-Presence of Learners	Application Sharing
	Concurrent Learning	Instant Messaging

A. Threats and Risks Associated with E-Learning System

The loss of assets is a result of the occurrence of threats or risks. All threats or risks occur through vulnerabilities. The main threats are:

- Confidentiality violation: an unauthorized person accesses the assets of the electronic learning system.
- Integration violation: an unauthorized person accesses to assets and manipulates the e-learning system.
- Denial of service: prevent legal access by disturbing traffic during a transaction between users of the electronic learning system.
- Illegal use: abuse of access rights by legal users.
- Infected and malicious program: programming codes to destroy other programs.
- Denial: participants deny participation in all transaction-related documents and systems.
- Changing face: behavioral way, so that the truth becomes hidden by the attacker.
- Traffic analysis: information leakage as an abusive means of communication channels.
- Brute-Force attack: try using all possible combinations to reveal the correct case.

Threats as a result of the above threats, the following risks may happen during a transaction of textual and non-textual messages among different participants in e-learning system [16].

B. Therapeutic Strategy for Risk

1) ***Access Control Using Firewall:*** A firewall is in fact a combination of software and hardware security systems implemented to prevent unauthorized access from outside the organization to the organization's network. Technically, a firewall system is a special version of router [16]. Apart from the basic routing functions and rules in routing, a router can be configured to execute a firewall with the help of additional software sources.

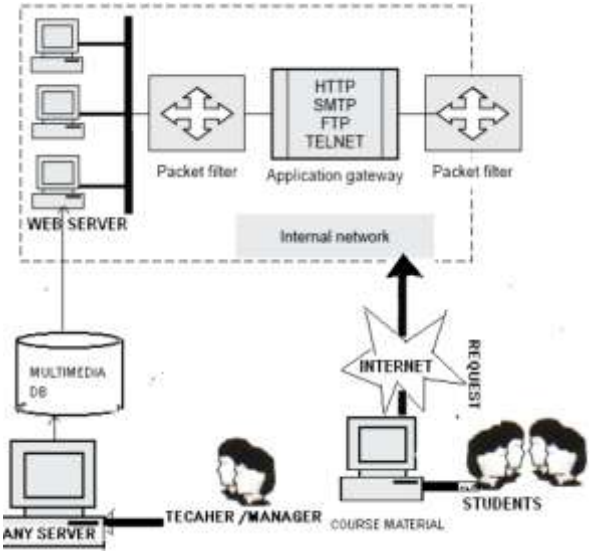

Figure 1: Organization of Firewall in E-Learning System [16]

2) ***Digital Rights Management (DRM) on the Assets ofE-learningSystem:***One of the main strategies that should be implemented to reduce the risk associated with the assets of e-learning system, is the digital rights management or DRM [17]. Sharable assets, are simple resources, such as a statistic Hyper Text Markup Language (HTML) page, a PDF file, or set of files, such as images and manual of style. On the other hand, the vital assets of the electronic learning system can be defined as the content of e-learning (quizzes, notes, etc.), encryption/decryption key content, user's personal data, messages between users, membership data in different groups, network bandwidth, message accessibility, and message integrity. DRM securitizes the system content [16]. In general, DRM should be used for license agreement and copyright protection or prevent publish [16].

3) ***Cryptography:*** The purpose of confidentiality is to ensure that information and data are not disclosed to any person or entity unauthorized. One of these techniques is called cryptography [16]. In general, there are 2 types of algorithms in cryptography.

- Secret key algorithms: In secret key algorithms, encryption and decryption key is

the same. This method requires an agreement between the sender and receiver on the key before the connection. The main function of this algorithm is data encryption. Examples of such algorithms include: Data Encryption Standard or DES and Advanced Encryption Standard or AES [16].

- Public key algorithms: Public key cryptographic systems, on the other hand, use a key (public key) to encrypt messages and a second key (secret key) to decrypt those messages. Two mathematical models for these algorithms are discrete logarithms and elliptic curves. There are different algorithms for this method: RSA, El-Gamal, Diffie-Hellman [16]. In general, all asymmetric cryptographic algorithms have potential advantages over symmetric algorithms that are:
  1. Securely distributing a secret key or shared key on the network
  2. Supporting hash algorithms
  3. Supporting digital signature to achieve non-denial purpose
  4. Supporting authentication methods for servers and users using digital certificates

But the great disadvantage of their asymmetric cryptographic algorithms is their low speed in transmitting information. That's why today in most scenarios where both security and performance factors are important, a combination of symmetric and asymmetric encryption algorithms are used, which is so-called Digital Envelope.

4) ***Authentication Techniques:***

- Password-based authentication: Password is still considered as a standard in user authentication. No specific hardware is needed to identify users. In a secure transfer networked context, passwords is a vital issue [18].
- Smart card authentication: Smart cards use cryptographic mechanisms known as public key cryptos for authentication and identification. The security of smart cards does not depend on the computer that it is used, and smart cards can be designed to be resistant to manipulation. They provide effective methods for identification and two-factor authentication, knowledge and ownership mechanism which also guarantee non-denial features. In order to use smart cards, all clients must be equipped with specific hardware and there must be an infrastructure for issuing smart cards. At present, there is no universal standard for smart cards and smart card readers as standard equipment on computers [18].
- Biometric authentication: Among all the authentication techniques, such as passwords, smart cards, digital signatures, and digital certificates, there is no guarantee that some students keep their password secret [19]. Passwords may be abused at the time of the passing of content, receiving questions, downloading the courses content etc., while the biometric authentication will provide better security, but this requires bigger investment [16]. Cryptographic and biometric authentication models are used to convert the original biometric data to the traceable biometric information. There are various biometric measures for authentication and encryption/decryption mechanisms, such as: models of faces, fingerprints, iris patterns and colors, geometry of finger/hand, sound, pattern of tapping on keyboard, gate, and DNA. Information inside biometric systems is unique and non-falsified. Biometric authentication and biometric encoding mechanisms, map the physical properties of a biometric property to digital keys, so-called the biometric template [5].
- Device authentication: Each device has a unique identifier, as a terminal point such as MAC Address, which can be used in the authentication model. A weak biometric authentication technique, such as voice, can be used with a surface-device authentication model to produce a stronger authentication mechanism. Username or ID of the device not only can be used for authentication purposes, but it may be used for digital signature pattern; for example using X.509 [5].

III. METHODOLOGY

Here's how to simulate the protocol used to secure the communications of the e-learning system. Generally 3 protocols are considered to create secure infrastructure and registration part and authentication server: SSL/TLS, IPsec protocol, and IKEv2 protocol. In the following, we explain this part of the simulation software used in this research and the scenarios for doing this simulation. It should be noted that in order to do the scenarios of the present OPNET Modeler 14.5 is used.

A. Communication Infrastructure for Conducting Experiments

In order to perform simulations on the 3 protocols, a communication platform with the following features are considered:

- 10 subnets of XDSL each of them with the following components:
  1. 25 Subnet
  2. 25 xDSL modems
  3. 25 client computer system ethernet_station
  4. A node of DSLAM_atm1_ip32
  5. A node of BRAS_ethernet4_slip8_gtwy

6. An interface switch node BN_Centillion100
7. Communication link Ethernet_100baseT to connect the client computer system to the xDSL modem and connect the interface with the BRAS router
8. Communication link of PPP_1.544Mbps to connect the XDSL modem with the DSLAM system
9. Communication link of ATM_51.84Mbps to connect the DSLAM system with the interface switch
10. Communication link of PPP_155 Mbps to connect the BRAS router with the core network

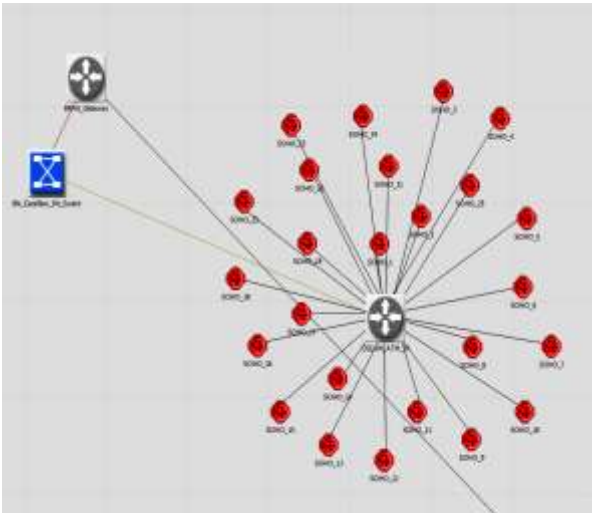

Figure 2: Plan of Internal Network of All 10 Subnets Related to Core Network

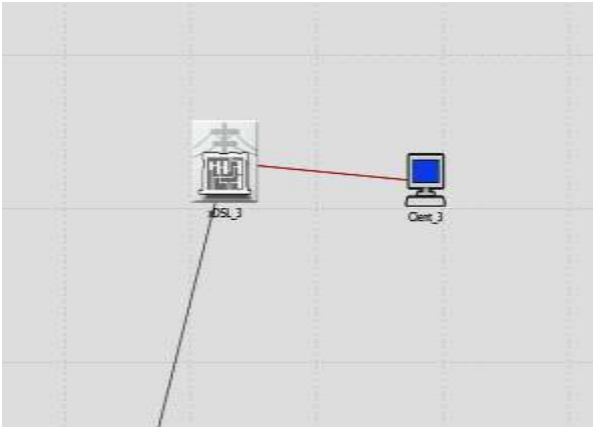

Figure 3: Plan of Internal Network of All 25 Subnets Connected to DSLAM Node

- A node of IP-Cloud-32 with 32 serial ports based on TCP/IP infrastructures
- A subnet for simulation of E-Campus Network with the following components:
  1. One Ethernet_server node for medium networks
  2. One CS_1900_1s_e12_fe2 switch node to connect with the network router
  3. One CS_3640_4s_e5_fe1_tr1_sl6 route node
  4. Communication link of Ethernet_100baseT to connect the server with the central switch as well as the connection between the switch and the central router network
  5. Communication link of PPP_155 Mbps to connect Gateway Router with the core network

Figure 4: Plan of E-Campus Internal Network

B. The Variables Used in the Simulation

In considering the interested scenarios and protocols in this simulation project, there are generally two variables for evaluation:

1) ***HTTP Variable:*** HTTP variable is measured and analyzed on the server and under the three following parameter:

- Task Processing Time (sec)
- Traffic Receive (Byte/Sec)
- Traffic Sent (Byte/Sec)

2) ***TCP Variable:*** TCP variable is evaluated on communication infrastructure and by considering a parameter called TCP Load (Byte) in seconds.

C. Simulation Scenarios

In this study, generally three scenarios have been considered for evaluating the performance of the protocols in different scenarios:

- With 10% Dynamic Backload and Low Application Load
- With 30% Dynamic Backload and Medium Application Load
- With 50% Dynamic Backload and with High Application Load

IV. THE THEORETICAL AND SIMULATION RESULTS

In general, this part of the comparison includes the introduction of features and algorithms used in these protocols. According to these functions and algorithms, a correct understanding of security of these protocols can be obtained, and eventually the reason of use of SSL/TLS protocol for authentication

model will also be more apparent by describing these elements.

Also in this section, 3 protocols of SSL/TLS, IPsec, and IKEv2 are also examined by application perspective and finally, they can be compared with each other based on the evaluation. In order to better understand the functionality of the protocols in the authentication model, we put their performance results under the named variables together.

SSL/TLS Protocol

SSL and TLS are encryption and decryption protocols, and cryptographic protocols to be better expressed that are designed in order to provide a secure connection on a non-secure infrastructure. This explanation means that if these protocols are properly developed, then we can open a communication channel to a desired service on the internet, where it is ensured that connection with the desired server has been definitely established, so data are not available to anyone else. These protocols protect Transport Layer, and therefore it is called TLS [20]. The following table shows the security components of this protocol.

Table 3: Security Components of TLS Protocol

Algorithm	Requirement Level		
	TLS 1.0	TLS 1.1	TLS 1.2
Symmetric Encryption Algorithms:			
AES GCM 128, 256	N/A	N/A	Supported
AES CCM 128, 256	N/A	N/A	Supported
AES CBC 128, 256	May	Supported	Supported
Camellia G0CM 128, 256	N/A	N/A	Supported
Camellia CBC 128, 256	May	Supported	Supported
ARIA GCM 128, 256	N/A	N/A	Supported
ARIA CBC 128, 256	May	Supported	Supported
SEED CBC 128	May	Supported	Supported
3DES EDE CBC 112	Not-Supported	Not-Supported	Not-Supported
GOST 28147-89 CNT 256	Not-Supported	Not-Supported	Not-Supported
IDEA CBC 128	Not-Supported	Not-Supported	N/A
DES CBC 40	Not-Supported	Not-Supported	N/A
DES CBC 56	Not-Supported	N/A	N/A
RC2 CBC 40	Not-Supported	N/A	N/A
ChaCha20-poly1305 256	N/A	N/A	Supported
RC4 40	Not-Supported	Not-Supported	Not-Supported
RC4 128	Not-Supported	N/A	N/A
Integrity-Protection Algorithms:			
HMAC-MD5	Yes	Yes	Yes
HMAC-SHA1	Yes	Yes	Yes
HMAC-SHA256/384	No	No	Yes
AEAD	No	No	Yes
GOST 28147-89 IMIT	Yes	Yes	Yes
GOST R 34.11-94	Yes	Yes	Yes
Asymmetric Encryption Algorithms:			
RSA	Yes	Yes	Yes
DH-RSA	Yes	Yes	Yes
DHE-RSA (forward secrecy)	Yes	Yes	Yes
ECDH-RSA	Yes	Yes	Yes
ECDH-RSA (forward secrecy)	Yes	Yes	Yes
DH-DSS	Yes	Yes	Yes
DHE-DSS (forward secrecy)	Yes	Yes	Yes
ECDH-ECDSA	Yes	Yes	Yes
ECDHE-ECDSA (forward secrecy)	Yes	Yes	Yes
PSK-RSA	Yes	Yes	Yes
DHE-PSK (forward secrecy)	Yes	Yes	Yes
ECDHE-PSK (forward secrecy)	Yes	Yes	Yes
SRP-DSS	Yes	Yes	Yes
SRP-RSA	Yes	Yes	Yes
Kerberos	Yes	Yes	Yes
GOST R 34.10-94/ 34.10-2001	Yes	Yes	Yes

B. IPsec Protocol

Generally, there are two versions of the IPsec protocol in operating mode. New IPsec or IPsec-V3 and old outdated IPsec or IPsec-V2. However, IPsec-V2 despite being outdated is still widely used. There are differences between the two versions of the protocol that we are referring to [21]:

- In IPsec-V2 one SA (Security Association) was specified by combining SPI field in the ESP protocol or AH and the destination address. In IPsec-V3, SA parameter is determined in two modes; in the unicast mode, it is determined by the SPI field and optionally by the protocol. In multicast mode, it is determined by combining the SPI field and destination address and the originating address is determined optionally.
- In IPsec-V3 selector SPD has more flexibility and includes a larger range of values and types of ICMP messages which can be used as selective.
- In the new database version, order-independent SAD has replaced the ordered type.
- In the second version of IPsec, AH protocol was required, however, in the third edition of IPsec-V3, the existence of AH is optional[21].

IPsec protocol is considered as a very powerful example in the field of securitization of relationships. This protocol has two versions, whose differences are displayed in Table 4.

Table 4: Security Components of IPsec Protocol [21]

Algorithm	Requirement Level	
	IPsec-V2	IPsec-V3
Encryption Algorithms:		
ESP-NULL	MUST	MUST
3DES-CBC	MUST	MUST-
Blowfish/CAST/IDEA/RC5	optional	optional
AES-CBC 128-bit key	MUST	MUST
AES-CBC 192/256-bit key	optional	optional
AES-CTR	SHOULD	SHOULD
Camellia-CBC	optional	optional
Camellia-CTR	undefined	optional
SEED-CBC	optional	undefined
Integrity-Protection Algorithms:		
HMAC-SHA-1	MUST	MUST
AES-XCBC-MAC	SHOULD+	SHOULD+
HMAC-SHA-256/384/512	optional	optional
AES-GMAC	undefined	optional
HMAC-MD5	MAY	MAY
AES-CMAC	undefined	optional
HMAC-RIPEMD	optional	undefined
Pseudorandom Functions:		
PRF-HMAC-SHA1	undefined	undefined
PRF-HMAC-SHA-256/384/512	undefined	undefined
AES-XCBC-PRF	undefined	undefined
AES-CMAC-PRF	undefined	undefined
Asymmetric Encryption Algorithms:		
DH MODP group 1	MAY	MAY
DH MODP group 2	MUST	MUST-
DH MODP group 5	optional	optional
DH MODP group 14	SHOULD	SHOULD+
DH MODP group 15-18	optional	optional
DH MODP group 22-24	optional	optional
DH EC group 3-4	undefined	undefined
DH EC group 19-21	undefined	undefined
DH EC group 25-26	undefined	undefined

C. IKEv2 Protocol

The IKEv2 protocol is a set of mechanisms designed in order to perform two important functions: to build a protected environment, which includes authentication of both sides of a relationship who have no familiarity with each other, and implementation and management of Security Associations (SAs0) between both authenticated

sides based on security policies approved between them [22].

IKEv2 protocol has differences with its first edition as follows:

- Using the NAT-T or Nat Traversal capability: this capability on devices with NAT capability such as home ports, allows the user to securitize their own data using the IPsec protocol security capabilities.
- Replacing several transmissions instead of a short kind: IKEv2 protocol is able to support various data transmit ways to create flexibility, and cooperation capability to use in multiple ways [21].
- Use of EAP (Extensible Authentication Protocol): the second version of the IKE protocol supports all of the family of EAP protocols and therefore both sides of relationship will be able to, even asymmetrically, use methods of different authentication; because the EAP family has several authentication methods.
- Resistance against DDoS attacks: IKEv2 protocol can resist against DDoS attacks, because this protocol, drops all the delivered packages until it has not recognized the sender information.

Protecting IKE messages according to the ESP protocol in IPsec protocol [21].

Table 5: Security Components of IKE Protocol [21]

Algorithm	Requirement Level	
	IKEv1	IKEv2
Encryption Algorithms:		
ESP-NULL	N/A	N/A
3DES-CBC	MUST	MUST-
Blowfish/CAST/IDEA/RC5	Optional	Optional
AES-CBC 128-bit key	SHOULD	SHOULD+
AES-CBC 192/256-bit key	Optional	Optional
AES-CTR	undefined	Optional
Camellia-CBC	Optional	Optional
Camellia-CTR	undefined	Undefined
SEED-CBC	undefined	Undefined
Integrity-Protection Algorithms:		
HMAC-SHA-1	MUST	MUST
AES-XCBC-MAC	undefined	Optional
HMAC-SHA-256/384/512	Optional	Optional
AES-GMAC	N/A	N/A
HMAC-MD5	MAY	Optional
AES-CMAC	undefined	Optional
HMAC-RIPEMD	undefined	Undefined
Pseudorandom Functions:		
PRF-HMAC-SHA1	MUST	MUST
PRF-HMAC-SHA-256/384/512	Optional	Optional
AES-XCBC-PRF	undefined	SHOULD+
AES-CMAC-PRF	undefined	Optional
Asymmetric Encryption Algorithms:		
DH MODP group 1	MAY	Optional
DH MODP group 2	MUST	MUST-
DH MODP group 5	Optional	Optional
DH MODP group 14	SHOULD	SHOULD+
DH MODP group 15-18	Optional	Optional
DH MODP group 22-24	Optional	Optional
DH EC group 3-4	MAY	Undefined
DH EC group 19-21	Optional	Optional
DH EC group 25-26	Optional	Optional

D. Comparing Under The TCP Load Variable

In 10% traffic, the IPsec protocol has the least TCP and then the IKEv2 and SSL/TLS are placed. The maximum load of TCP is likewise, and the IPsec protocol offers the best function.

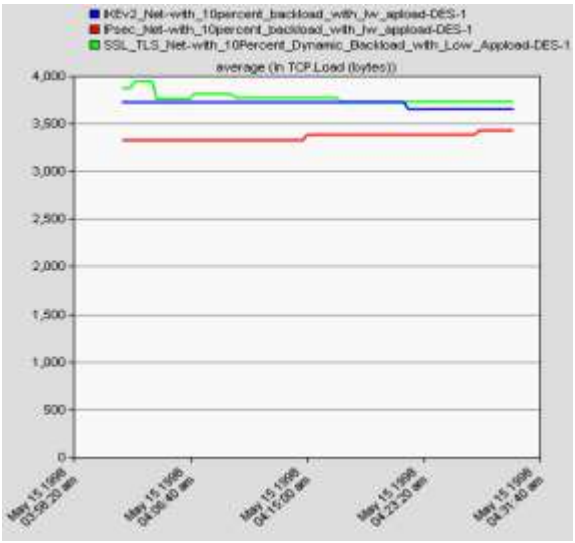

Figure 5: TCP Load Variable, Comparison in 10% Dynamic Backload

Table 6: TCP Load Variable, Mean and Peak Values in 10% Dynamic Backload

Simulation Scenario	Protocol					
	SSL/TLS		IPsec		IKEv2	
	Mean	Peak	Mean	Peak	Mean	Peak
10% Dynamic Backload and Low Application Traffic						
TCP Load (Byte)	3727.3	4012	3427	3518	3651	3724

In traffic behind 30% line and average traffic of applications, the SSL/TLS protocol outperformed the IKEv2 protocol, but still the IPsec protocol offers a better performance. Of course, about the maximum load, TCP is determined as the main reason for the result. Because the SSL/TLS protocol has encountered with an overload at the start of the network, it has generally affected the performance mean, but given this maximum load, SSL/TLS protocol load has generally offered a very good performance compared to its competitors.

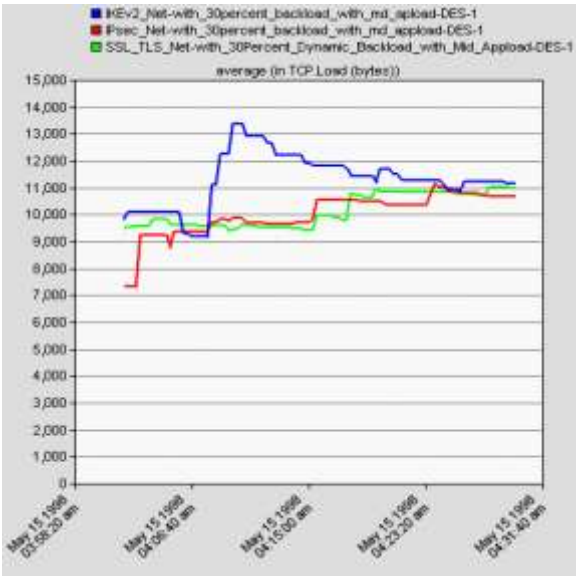

Figure 6: TCP Load Variable, Comparison in 30% Dynamic Backload

Table 7: TCP Load Variable, Mean and Peak Values in 30% Dynamic Backload

Simulation Scenario	Protocol					
	SSL/TLS		IPsec		IKEv2	
	Mean	Peak	Mean	Peak	Mean	Peak
30% Dynamic Backload and Low Application Traffic						
TCP Load (Byte)	10978	28406	10679	19348	11169	20153

Finally, in the 50% behind line traffic, SSL/TLS protocol has had the best mean performance. Even under the maximum TCP load, the SSL/TLS protocol has been successful to provide the best results among its competitors, i.e. the two IPsec and IKEv2 protocols.

Figure 7: TCP Load Variable, Comparison in 50% Dynamic Backload

Table 8: TCP Load Variable, Mean and Peak Values in 50% Dynamic Backload

Simulation Scenario	Protocol					
	SSL/TLS		IPsec		IKEv2	
	Mean	Peak	Mean	Peak	Mean	Peak
50% Dynamic Backload and Low Application Traffic						
TCP Load (Byte)	92876	216471	97648	245989	107244	269287

E. Compare Under the Variable of Task Processing Time

In the variable of Task Processing Time in 10% behind-line traffic, the IPsec protocol gives the best result as the previous variable. Then the protocols of IKEv2 and SSL/TLS stand.

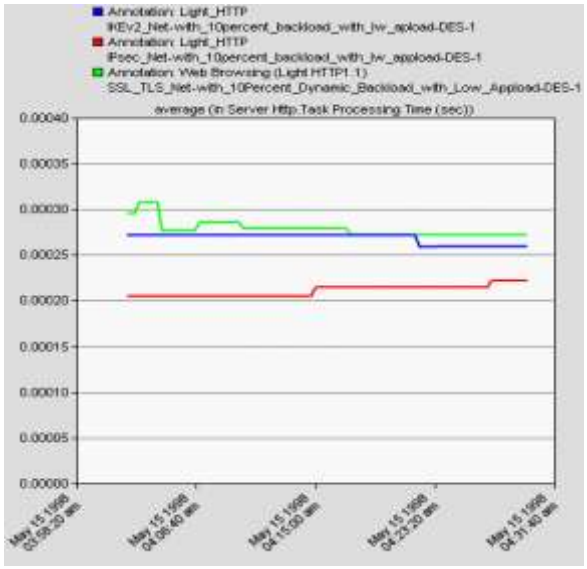

Figure 8: Task Processing Time Variable, Comparison in 10% Dynamic Backload

Table 9: Task Processing Time, Mean and Peak Values in 10% Dynamic Backload

Simulation Scenario	Protocol					
	SSL/TLS		IPsec		IKEv2	
	Mean	Peak	Mean	Peak	Mean	Peak
10% Dynamic Backload and Low Application Traffic						
Task Processing Time (m s)	0.272	0.319	0.222	0.237	0.259	0.271

In the 30% behind-line traffic, the best performance also belongs to the IPsec protocol. In this case, the SSL/TLS protocol gives a time between the two protocols of IPsec and IKEv2. But in the maximum task processing time, 2 protocols of SSL/TLS and IPsec offer 1.51 milliseconds and the protocol of IKEv2 has a time of 1.45 milliseconds. Overall, the mean time has a very special significance because the maximum generally occurs just a moment and is not stable. So in this case, the SSL/TLS protocol is in the middle position.

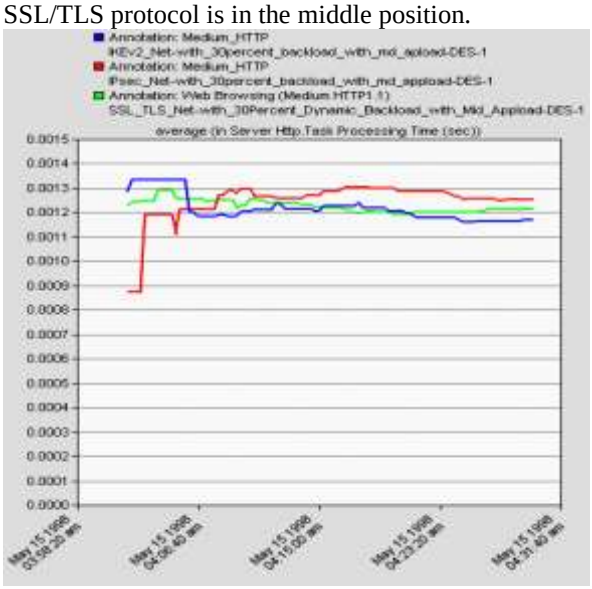

Figure 9: Task Processing Time Variable, Comparison in 30% Dynamic Backload

Table 10: Task Processing Time, Mean and Peak Values in 30% Dynamic Backload

Simulation Scenario	Protocol					
	SSL/TLS		IPsec		IKEv2	
	Mean	Peak	Mean	Peak	Mean	Peak
30% Dynamic Backload and Medium Application Traffic						
Task Processing Time (m s)	1.21	1.51	1.25	1.51	1.16	1.45

Finally, in 50% behind-line traffic, the SSL/TLS protocol stands in the second place after the IPsec protocol. Protocol IPsec with an average processing time of 5.31 milliseconds is in first place in the section.

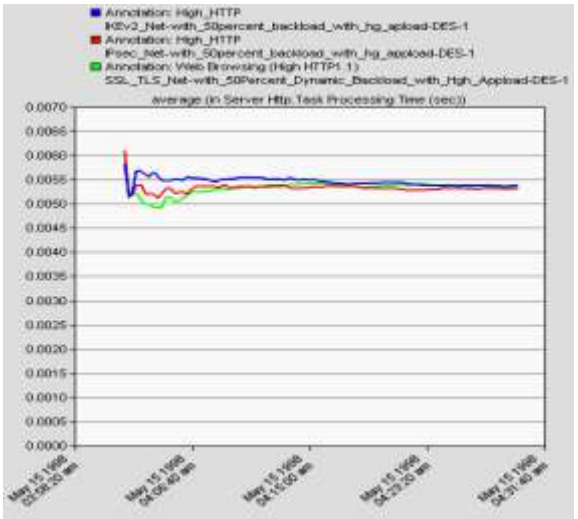

Figure 10: Task Processing Time Variable, Comparison in 50% Dynamic Backload

Table 11: Task Processing Time, Mean and Peak Values in 50% Dynamic Backload

Simulation Scenario	Protocol					
	SSL/TLS		IPsec		IKEv2	
	Mean	Peak	Mean	Peak	Mean	Peak
50% Dynamic Backload and High Application Traffic						
Task Processing Time (m s)	5.37	7.03	5.31	6.51	5.37	7.17

F. Comparing the Performance under the Variables of Traffic Received and Traffic Sent

The rate of received and sent data to the server for the SSL/TLS protocol for a 10% behind-line traffic and low traffic of applications, is 7 and 5.4244 bytes per second, respectively. However, this value for IPsec and IKEv2 protocols is 3.5 bytes per second for downloads, and 2.2117 and 2.585 bytes per second for upload. So in this part, the SSL/TLS protocol has the highest rate of sending which means that it has more processing compared with two other contenders.

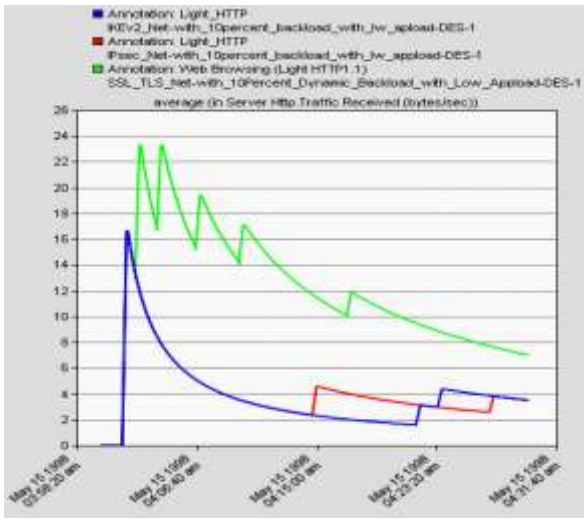

Figure 11: Traffic Received Variable, Comparison in 10% Dynamic Backload

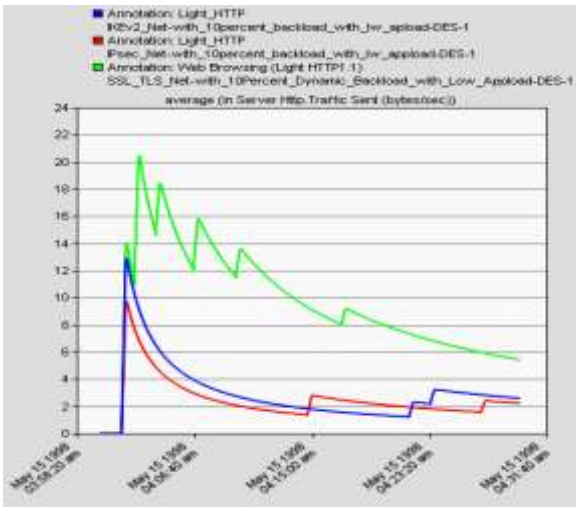

Figure 12: Traffic Sent Variable, Comparison in 10% Dynamic Backload

Table 12: Traffic Received and Traffic Sent Variables, Mean and Peak Values in 10% Dynamic Backload

Simulation Scenario	Protocol					
	SSL/TLS		IPsec		IKEv2	
	Mean	Peak	Mean	Peak	Mean	Peak
10% Dynamic Backload and Low Application Traffic						
Traffic Received (B/S)	7	116.67	3.5	116.67	3.5	116.67
Traffic Sent (B/S)	5.4244	106.22	2.2117	78.778	2.585	90.222

For the 30% traffic behind the line, IKEv2 protocol offers the best result. The receive rate in this part for this protocol has been 32.667 for receive and 110.04 bytes per second. After that, protocols of IPsec and SSL/TLS stand.

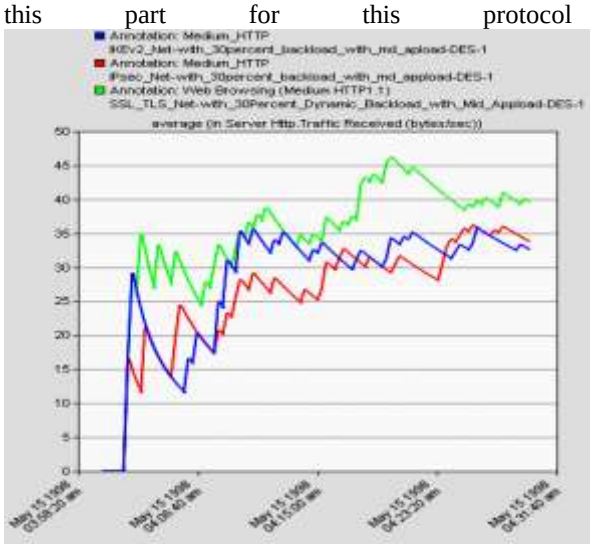

Figure 13: Traffic Received Variable, Comparison in 30% Dynamic Backload

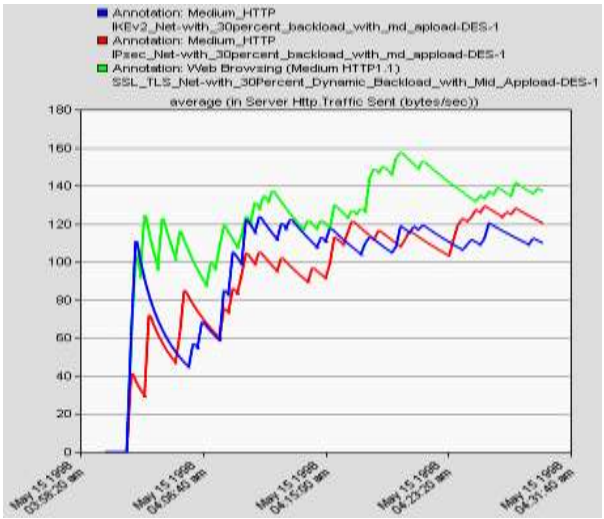

Figure 14: Traffic Sent Variable, Comparison in 30% Dynamic Backload

Table 13: Traffic Received and Traffic Sent Variables, Mean and Peak Values in 30% Dynamic Backload

Simulation Scenario	Protocol					
	SSL/TLS		IPsec		IKEv2	
	Mean	Peak	Mean	Peak	Mean	Peak
30% Dynamic Backload and Medium Application Traffic						
Traffic Received (B/S)	39.667	350	33.833	233.33	32.667	233.33
Traffic Sent (B/S)	137.21	1228.1	120.42	841.56	110.04	886.28

For a 50% behind-line traffic and high traffic of applications, the SSL/TLS protocol offers a very good performance and considering all the values, it could be said that despite the mean value of the receiving and sending rate, it generally gives a good performance.

Figure 15: Traffic Received Variable, Comparison in 50% Dynamic Backload

Figure 16: Traffic Sent Variable, Comparison in 50% Dynamic Backload

Table 14: Traffic Received and Traffic Sent Variables, Mean and Peak Values in 50% Dynamic Backload

Simulation Scenario	Protocol					
	SSL/TLS		IPsec		IKEv2	
	Mean	Peak	Mean	Peak	Mean	Peak
50% Dynamic Backload and High Application Traffic						
Traffic Received (B/S)	245.78	777.78	234.89	777.78	303.33	933.33
Traffic Sent (B/S)	3778.9	11248	3562.5	12888	4641.8	14027

According to the information given in the 3 protocols of SSL/TLS, IPsec, and IKEv2 in this section and in previous chapter of the research, it can clearly be stated that from a theoretical-security view, the SSL/TLS protocol is the best choice for securitizing communication between user and the e-leaning system of Islamic Azad University. This choice can be proved from several perspectives in this area of study.

As can be observed in Tables 3, 4, and 5, in the part of asymmetric encryption algorithms, 2 protocols of IPsec and IKEv2 definitely support only the Diffie-Hellman algorithm and their support of the algorithm of ECDH is not defined. While about the SSL/TLS protocol it can be seen that this protocol supports a wide range of asymmetric encryption algorithms. Also, the Diffie-Hellman algorithm has structural weaknesses against MITM attack followed by all the attacks that are subsets of MITM attacks [23], including Session Hijack attacks and Phishing attacks. Thus, according to this explanation, the SSL/TLS protocol is quite superior. Of course, mentioning this point is also necessary that the SSL/TLS protocol definitely supports the D-H algorithm as well, but the point is that one can choose the most secure, or according to the issues of security and performance, choose other options from among various options that this protocol offers the user.

In the part of hash functions also the SSL/TLS protocol has superiority in terms of support. In Table 3 we see that the SSL/TLS protocol supports the AEAD methods entirely under the version 1.2 of TLS. Given that the AEAD method has high security and even high performance speed, so as a result, the, SSL/TLS protocol shows its superiority in this field too. Protocols of IPsec and IKEv2 only support AES-XCBC and AES-CMAC modes to establish integrity and confidentiality of information as well as the production of disposable values such as IV.

In symmetric encryption algorithms, the previous states hold and the SSL/TLS protocol has superiority over its 2 competitors. About the 2 protocols of IPsec and IKEv2, the strongest algorithm are AES-CTR and Camellia-CTR. As seen in Table 5, the AES-CTR algorithms is supported only by IKEv2,

and also this state is optional which means that the IKEv2 protocol does not support this algorithm in all circumstances. But based on table 4, the IPsec protocol completely supports AES-CTR algorithms and is highly secure in this regard. Also under some circumstances, the Camellia-CTR algorithm is also supported by IPsec-V3 protocol. Finally, as seen in Table 3, the SSL/TLS protocol fully supports the scenarios of AES-CCM, AES-GCM, and ChaCha20-poly1305 under version of 1.2 of TLS. These algorithms have much higher security and even performance, compared to other algorithms and thus it can be concluded that the SSL/TLS protocol has superiority in all cases.

Finally, as another reason that the SSL/TLS protocol in the project, has advantages compared to the protocols of IPsec and IKEv2, is in fact, related to the issue of security and performance. If you use the protocols of IPsec and IKEv2 in order to secure user connection with the e-learning system, you need to perform settings and configurations on the side of user system, which is so-called Client-Side-Configuration. Even if we assume that the settings of these 2 protocols at the side of users is doable in order to create a secure connection using some algorithms and scripts, the process load, lengthened authentication process and even security dangers of this method cannot be ignored. Because in order to perform configuration we need to safely transmit parameters and if each of these parameters such as the encryption algorithm type, the key size, the credit time etc. are stolen by attackers during performing configurations, the connection would totally be endangered by different attacks. So in this situation, either another protocol should be used such as the SRP protocol, etc., or an algorithm should be designed for it. In any case, this would also raise the probability of attacks and will also affect the performance.

Due to all these reasons, it can be concluded that the SSL/TLS protocol from the perspective of security and theoretical components in this scenario is superior.

Generally, the SSL/TLS protocol is placed between the two protocols of IPsec and IKEv2. The point is the very good performance of the SSL/TLS protocol in the 50% behind-line traffic and this enhances it reliability. IPsec protocol gives the best result in most circumstances from the perspective of performance. But it would be important that the overall result is adopted considering the security and performance factors, and because the SSL/TLS protocol has a full superiority from the security perspective, and provides an acceptable performance compared to the other two protocols in terms of function, therefore, it is this protocol is considered a good candidate for this scenario. Furthermore, it was previously mentioned that if used, two IPsec and IKEv2 protocols need an algorithm implementation or lateral script to do configuration of the side of user which affects both performance and security. Finally, because the SSL/TLS protocol is fully compatible with standards raised in the field of secure remote connections such as: PKI, X.509, etc., it is considered as the best option to secure the connection.

Table 15 shows the comparison of the overall performance of each of the 3 protocol:

Table 15: Comparison of SSL/TLS, IPsec and IKEv2 Protocols in All three Scenarios

Simulation Scenario	Protocol					
	SSL/TLS		IPsec		IKEv2	
	Mean	Peak	Mean	Peak	Mean	Peak
10% Dynamic Backload and Low Application Traffic						
TCP Load (B)	3727.3	4012	3427	3518	3651	3724
Task Processing Time (m S)	0.272	0.319	0.222	0.237	0.259	0.271
Traffic Received (B/S)	7	116.67	3.5	116.67	3.5	116.67
Traffic Sent (B/S)	5.4244	106.22	2.2117	78.778	2.585	90.222
30% Dynamic Backload and Medium Application Traffic						
TCP Load (B)	10978	28406	10679	19348	11169	20153
Task Processing Time (m S)	1.21	1.51	1.25	1.51	1.16	1.45
Traffic Received (B/S)	39.667	350	33.833	233.33	32.667	233.33
Traffic Sent (B/S)	137.21	1228.1	120.42	841.56	110.04	886.28
50% Dynamic Backload and High Application Traffic						
TCP Load (B)	92876	216471	97648	245989	107244	269287
Task Processing Time (m S)	5.37	7.03	5.31	6.51	5.37	7.17
Traffic Received (B/S)	245.78	777.78	234.89	777.78	303.33	933.33
Traffic Sent (B/S)	3778.9	11248	3562.5	12888	4641.8	14027

V. Conclusion And Future Works

According to the investigations and simulations conducted, this research can be discussed in 2 dimensions. From a security perspective, the SSL/TLS protocol has definitely the highest rating among the 3 protocols studied, and in securing connections it is considered the best option. In terms of performance, as described in the previous section, generally, the SSL/TLS protocol is places in the second place and between the protocols of IPsec and IKEv2. According to the results, if in the operational scenarios, the performance factor is attended more than security, then the IPsec protocol can be used.

But in the scenarios where the security factor is very important, certainly SSL/TLS protocol is considered as the best choice. In scenarios where both security and performance is concerned, the SSL/TLS protocol wins this competition, because according to the previous section, if we use the IPsec protocol, we need to design algorithms and lateral scripts to configure user system to connect with the e-learning system and this would affect both performance and security. In addition to these issues, the discussion of policy and criteria developed by software and operating system companies also arises; because performing configuration on the user's system requires violating a set of rules in the OS of the host system along with endangered privacy of the user as a result of exerting executive codes, while the aim of such a system is in fact, securing the connection of user with the e-learning system as well as maintaining the privacy.

To continue this research, the most important subject is the design and evaluation of an authentication model or protocols through which we can authenticate users who enter the e-learning system. This model was in fact evaluated along with the SSL/TLS protocol in this article from various aspects; actually, it creates a fully safe, optimized, and integrated system to protect privacy of students against intruders and even themselves. So the most important thing for the future of this research is to design a model of authentication based on the SSL/TLS protocol.

REFERENCES

[1] D. Dharmawansa, K. T. Nakahira, Y. Fukumura, 'Detecting Eye Blinking of a Real-World Student and Introduction to The Virtual E-Learning Environment' *Procedia Computer Science*, Vol. 22, pp. 717-726, 2013.

[2] S. Karforma, B. Ghosh, 'on security issues in e-learning system' *Proceedings of COCOSY-09, University Institute of Technology, Burdwan University*, 2009.

[3] C. J. Richardson, K. Swan, 'Examining social presence in online courses in relation to students' perceived learning and satisfaction' *Journal of Asynchronous Learning Networks*, Vol. 7, Issue 1, pp. 68-84. 2003.

[4] K. Swan, P. Shea, E. Fredericksen, A. Pickett, W. Pelz, G. Maher, 'Building knowledge building communities: Consistency, contact and communication in the virtual classroom' *Journal of Educational Computing Research*, Vol. 23, Issue 4, pp. 359-383, 2000.

[5] S. Adibi, 'A Remote Interactive Non-Repudiation Multimedia-Based M-learning System' *Telematics and Informatics*, Vol. 27, pp. 377-393, 2010.

[6] A. Ortiz de Guinea, H. Kelley, M. G. Hunter, 'Information Systems Effectiveness in Small Businesses: Extending a Singaporean Model in Canada' *Journal of Global Information Management (JGIM)*, Vol. 13, Issue 3, 55-79, 2005.

[7] W. H. DeLone, E. R. McLean, 'Information systems success: The quest for the dependent variable' *Information Systems Research*, Vol. 3, Issue 1, pp. 60-94, 1992.

[8] W. H. DeLone, E. R. McLean, 'The DeLone and McLean model of information systems success: A ten-year update' *Journal of Management Information Systems*, Vol. 19, Issue 4, No. 9, 2003.

[9] A. Zivi, S. Rezaeian, N. Shahhoseini, 'A Survey Approach to Analyze E-Learning System of Islamic Azad University from the Perspectives of Optimality, Privacy and Data Protection, Review Phase, Analysis of Statistical Data and Providing a Managerial Model, *International Journal of Computer and Information Technology*, Vol. 5, No, 1, pp. 24-45 2017. Available Online: http://ijocit.org/IJOCIT/Vol%205,%20No.1/IJOCIT-Vol05I0103.pdf.

[10] B. Daya, 'Network Security: History, Importance, and Future' *University of Florida Department of Electrical and Computer Engineering*, p. 13, 2013.

[11] K. El-Khatib, L. Kobra, Y. Xu, G. Yee, 'Privacy and Security in E-Learning' International Journal of Distance Education, Vol. 1, Issue 4, pp. 1-15, 2003.

[12] S. Chanasuc, P. Praneetpolgrang, 'An Empirical Study on the Effect of Organizational Culture on the Acceptance of eLearning in Thai Higher Education' *Fifth International Conference on eLearning for Knowledge-Based Society*, pp. 1-6, 2008.

[13] Y. E. A. Mustafa, S. M. Sharif, 'An Approach to Adaptive E-Learning Hypermedia System based on Learning Styles (AEHS-LS): Implementation and evaluation' *International Journal of Library and Information Science*, Vol. 3, Issue 1, pp. 15-28, 2011.

[14] A. E. S. Khedr, 'Towards Three Dimensional Analyses for Applying E-Learning Evaluation Model: The Case of E-Learning in Helwan University' *International Journal of Computer Science Issues (IJCSI)*, Vol. 9, Issue 4, 2012.

[15] Y. Bentley, H. Selassie, A. Shegunshi, 'Design and Evaluation of Student-Focused eLearning' *The Electronic Journal of e-Learning*, Vol. 10, issue 1, pp. 1-12, 2012. Available online: www.ejel.org.

[16] N. Barik, S. Karforma, 'Risks and Remedies in E-Learning System' *International Journal of Network Security & Its Applications (IJNSA)*, Vol. 4, No. 1, pp. 51-59, 2012.

[17] Z. F. Zamzuri, M. Manaf, A. Ahmad, Y. Yunus, 'Computer Security Threats Towards the E-learning System Assets' *Communications In Computer and Information Science*, Vol. 180, pp. 335-345, 2011.

[18] H. J. Kim, 'E-learning Privacy and Security Requirements: Review' *Journal of Security Engineering*, Vol. 10, No. 5, pp. 591-600, 2013.

[19] C. C. Lim, J. S. Jin, 'A Study on Applying Software Security to Information System: E-learning Portals' *International Journal of Computer Science and Network Security*, Vol. 6, No. 3B, 2006.

[20] I. Ristić, 'Bulletproof SSL and TLS' *Fiesty Duck Limited*, p. 531, 2015. Available Online: www.fiestyduck.com.

[21] S. Frankel, S. Krishnan, 'IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap' *Internet Engineering Task Force (IETF)*, Request for Comments: 6071, ISSN: 2070-1721, p. 63, 2011.

[22] Z. Faigl, S. Lindskog, A. Brunstorm, 'A Measurement Study on IKEv2 Authentication Performance in Wireless Networks' *Proceedings of the 6th Swedish National Computer Networking Workshop (SNCNW)*, 2009.

[23] W. Stallings, 'Cryptography and Network Security: Principals and Practices' *Prentice Hall*, ISBN-10: 0-13-187319-9, 4th Ed. pp. 334-340, 2005.