REDUCING SECURITY CONCERNS WHEN USING CLOUD COMPUTING IN ONLINE EXAMS CASE STUDY: GENERAL ASSOCIATE DEGREE EXAMINATION (SHAMEL) IN JORDAN

Mohamad M. Al-Laham

Al-Balqa Applied University-Salt19117 - Jordan
Amman University College, MIS Dept.

ABSTRACT

The SHAMEL Exam is the second important exam in Jordan; accordingly, the preservation of confidentiality and security are the most important priorities of the exam managers. Recently, AL-Balqa Applied University (BAU) in Jordan has computerized the exam and one of the suggestions was to utilize the cloud computing applications. However, cloud computing entails many security concerns that may have impacts on the exam information security. This research discusses the current use the cloud computing in many life aspects and then concentrate on online exams aspect; also, this research clarifies the tangible and intangible risks associated with cloud computing adoption. Then, the research examined a specific case study related to the subject matter. Finally, this research explores the level of understanding risks and methods may be used to reduce it and help in protecting data from unauthorized persons.

KEYWORDS

SHAMEL Exam, BAU, Cloud Security, Cloud Service Provider, Cloud Computing.

1. INTRODUCTION

1.1 Historical information

The Medium University Degree (AL-SHAMEL) exam is considered as the second national exam in importance after high school exam (TAWJEEHI). It is the examination which grants whereby successful middle-class university's student (Diploma) after completing successfully the study of educational materials over two or three years, each according to his specialty. Consequently the exam has a great importance, because if the student fails or absent in this exam , this will lead to not giving him a medium university degree, as well this exam qualifies to the labor market, moreover the student who succeeds in this exam is entitled to bridge in the official or private universities in the Hashemite Kingdom of Jordan in accordance with instructions governing the process of bridging that are issued by the Ministry of Higher Education and Scientific Research(MOHE), or bridging in the Arab or foreign universities recognized in Jordan[22].

The history of this exam goes back to 1981, where the first exam "AL-SHAMEL" (as it was called at that time) was conducted for some of the specializations, then this exam began to apply

gradually on other specialties until all medium university degree specialties were covered. This exam was managed by the Ministry of Higher Education , but in 1997 Al-Balqa Applied University became technically and academically took over the supervision of the community colleges in the Kingdom ,also , the unit of assessment and public examinations that belongs to the university was assigned the organizing , managing and conducting the exam[21].

The exam's mechanism is based on the paper principle, where the paper contains a number of educational materials studied by the student, each according to his specialty, and the student must pass all the exams papers successfully so that students can pass the examination as a whole. Currently the exam is held in two sessions a year, winter and summer.

1.2 The evolution of the exam

The exam has gone through stages of development and is still undergoing development to this day. The most important development operation is represented in the mechanism of the exam, paper based exam method was the method used at the beginning and which was the prevalent method at that time, big halls was equipped to accommodate the students, in addition to the grading centers which grade and monitor the students answers. Then multiple choice questions pattern was used and which formed an updated and fast way of monitoring the grades, in which the answers were read electronically through the optical mark reader device, and then graded through special programs prepared for this purpose. The unit of assessment and public examinations in winter 2014 took the first step towards the computerization of medium university degree exam, so holding a one paper exam only once (the first paper) by a computerized approach through 17 exam centers that were distributed in all the governorates of the Kingdom, in addition to the exam center in the faculty of Granada in Galilee outside Jordan. The center includes several laboratories, so that the laboratory has a number of computer devices and servers as well as communication devices. On the summer session of 2014 the computerization of the rest of the exam papers was achieved, as of nearly 15,000 students applied for this exam session spread over nearly 90 majors in 11 study programs. The number of students was distributed over 13 test areas in the Kingdom in addition to the Granada exam center outside Jordan [20].

1.3 The future vision of the exam

AL-Balqa Applied University, represented by the unit of the assessment and public examinations looks forward to build exams center in the Hashemite Kingdom of Jordan to serve in the first place the medium-sized university exams and the educational, scientific and professional institutions in the second place, which will be able to conduct any kind of examinations in collaboration with the exams computerized center.

This may be useful in recruitment exams or professional exams or academic exams in university's faculties or colleges that are academically managed by the university or even other universities, especially since the unit earlier experiences to measure the performance or conduct competitive examinations for recruitment in collaboration with official bodies in the Kingdom such as the Civil Service Bureau and the Department of Customs.

The unit also looks forward to the possibility of doing a medium university degree exam at any time and not at specific times as it is currently in force .The unit will be able to move to this step in case of properly building a bank of the questions and provide adequate numbers of questions in

all subjects, and the student will be able to assign the date to do the exam, and determine the appropriate date for him to repeat the exam in case of failure. The students will be able to do the exam outside the territory of the Kingdom   without having to be present in the local exam centers, as would be possible in cooperation with the cultural missions of the Kingdom's embassies in brotherly and friendly countries to conduct the exam for these students. The most important step may be   generalization the idea of medium university degree exam (SHAMEL) on the rest of the Arab countries, where the Hashemite Kingdom of Jordan is the only country in the Arab world, which its students do such a test. Thereafter the exam center that is intended to be build will become the Arab's certified   center for the granting of medium university degree on the level of all Arab countries.

1.4 The evolution of Cloud Computing

The history of cloud computing began by Cluster Computing which means that several computers accomplish a single task, this will improve performance and achieve load/balancing as well as reducing overall cost. After clustering; Grid Computing appeared which is more loosely coupled, heterogeneous and geographically distributed. A concept called Utility Computing appeared which works as paying per use basis ;this facility of being served as a utility became the basis of the "On Demand" computing [1, 3].

1.5 The models of Cloud Computing

Software and hardware services over the internet offered by cloud computing. These services are classified into three categories [1, 12, 17, 18, 19, and 23]:

• **Software as a Service (SaaS)**: in this software model user will pay according to his usage and he will not be worry about the licensing and genuineness of demanded software and the vendor will provide the user by needed software in a short time [1, 6].
• **Platform as a Service (PaaS) :** It provides entirely through the internet all the services that are required during the life cycle of web applications. Users will only have to pay the subscription charges of the required software which in turn reduce the cost and complexity [1,6].
• **Infrastructure as a Service (IaaS):** it is also known as Hardware as a Service (HaaS), this model involves outsourcing. The cloud service provider delivers secure, scalable and robust infrastructure such as storage, hardware, servers, and networking components. The client only pays on per-use basis [1, 6].

2. PROBLEM STATEMENT

This research will investigate cloud security problems in cloud computing. I will build a model for reducing risks of cloud computing security issues that are affecting on SHAMEL online exam for general associate degree students i.e. the physical security and the security of virtual machine. This model will be able to help our exam's system to possess : data isolation, browser security, cloud malware injection attack, flooding attacks, protection of data, authentication, authorization, non-repudiation, trust and denial of service attacks.

3. SECURITY ISSUES AND RISKS IN CLOUD

Organizations that use internal infrastructure and those who already operate outsourcing models are usually familiar with the threats and challenges of the cloud. Threats to cloud are caused by

internal and external attackers [12].Attackers can be divided into four categories according to the level of their ability to carry out attacks: random, weak, strong and substantial attackers. It is worth noting that these categories are focused on the attackers' ability and do not describe the threat type. Most common attackers are random attackers, who use unsophisticated tools and methods that are usually known and easily discovered. The word random here describes the fact that such attackers randomly choose their victims on the internet. Attackers with somewhat minimal skills are known as weak attackers, and they are considered relatively more advanced. They usually use available applications or tools to target specific servers. Structured, funded and skillful attackers who usually target very specific cloud users are called strong attackers. Such groups tend to be part of an organized network working on wide-scale agendas. Finally substantial attackers are the ones with the highest ability to carry out attacks that usually are undetectable even by specialized governmental anti-cybercrime police. Organizations who are victims of such attackers usually find difficulty in disclosing the identity of the perpetrators and may resort to intelligence agencies or highly-specialized and professional experts [5]. The various problems faced by the cloud computing can be classified as listed below:

Confidentiality, integrity, availability, privacy, authentication, non-repudiation .we can summarized these classifications as below:

Confidentiality basically refers to the practice of protection data from unauthorized access. This important principle is applied by introducing security protocols, verification tools and data encoding measures over each network. Data integrity is making sure that the message sent is received without incurring any changes during transit. Availability is the ability to find the information needed from any location and guaranteeing this right to users. Ensuring the functionality of network infrastructures, security and connectivity is essential to uphold this principle. Network security, validation, and error handling are the common methods used to ensure availability. A simple definition of the word 'privacy' is the natural human need to be left alone away from public attention and being free from illegal interruption. Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. A guarantee to let the sender and recipient of a message admit that they did sending-receiving the message is called non-repudiation [1] ; this is necessary in online exams to be sure that the exam reach to specific student from the authorized person and the answers belong to the same student.

4. PREVIOUS STUDIES

A security framework was suggested by Takabi et.al they proposed a comprehensive security framework for cloud computing environments. In addition, challenges, existing solutions, approaches, and future work were fully discussed in order to maintain a secure cloud computing environment [8].

Saravg and Kant pointed out the importance of taking the security and privacy into account during the design using and cloud services. Furthermore, they revealed all the security issues and challenges encountered in cloud computing and its security standards and policies [1].

Agarwal and Agarwal have discussed the security issues associated with IT. Also they stressed on the fact that cloud computing includes risks concern in some aspects such as privacy, compliance regulations, identity, etc. They concluded that all risks issues in cloud computing are

the responsibility of both the IT department in the organization and the cloud computer service provider [2]

The status of the internet was fully discussed by **Vitkar**. He stressed on the need to adopt new technologies such as cloud computing is a must. This is due to the fact that it has the ability to the ability to create virtualized resources that may be provide to the users, also it is an excellent tools to be used in all educational institutions both in terms of educational environment and in reducing the cost of excess number of computers and network services [3].

Ukil et.al shed light on challenges and issues of security concerns of cloud computing and suggested different standard and novel solutions. They suggested an architecture generic that incorporates security schemes, techniques and protocols for cloud computing, Such as Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS) systems. Such architecture will affect positively the cloud computing system in providing solution to counter the threat. They have also indicated using experimental data how the charging based on the security service can be estimated by the cloud service provider [6]

Naseem and Sasankar presented security issues in context of the data and security issues provided by cloud services. The aim of work is to provide a better understanding of the security issues and risks in different services provided by cloud computing [10].

Tirthani and Ganesan have used the non-breakability of Elliptic curve cryptography for data encryption and Diffie Hellman key exchange mechanism to ensure secured data movement on the user side. Further they proposed encryption mechanism that uses the combination of linear and elliptical cryptography methods. This mechanism has security checkpoints like authentication and encryption of data [11].

Bora and Ahmad presented the benefits of using cloud computing for e-learning such as educational institutions that cannot afford the cost of the computers to be used in the e-learning investments, especially in the universities where the use of computers and networks to increase the benefits of common applications for students and teachers and cloud computing is the best solution [12].

Kumar et.al presented steps for creating a private cloud for universities, network and security issues in private cloud and how such implementation part benefits of creating a private cloud for universities [13].

Shahzada surveyed several research works on cloud computing related to security challenges and privacy issues. The main goal is providing a best understanding of the challenges that face security of cloud computing and suggest several approaches and solutions which have been proposed and adopted by the cloud service industry [9].

Navneetet.al suggested five security issues related to cloud computing, they summarized them in privilege access , data separation from its real location , the availability of data , authorized cloud center and the fifth issue concerned with what happen to useful data if the cloud vendor goes out of business [16].

5. LEGACY SYSTEM

Each of the exam sites is provided with a server, and then different exam sites and the center of the exam are connected by using Network of Al-Balqa Applied University for the university colleges and internet to the rest of the colleges. Figure 1 represents a way to setup this type of networks.
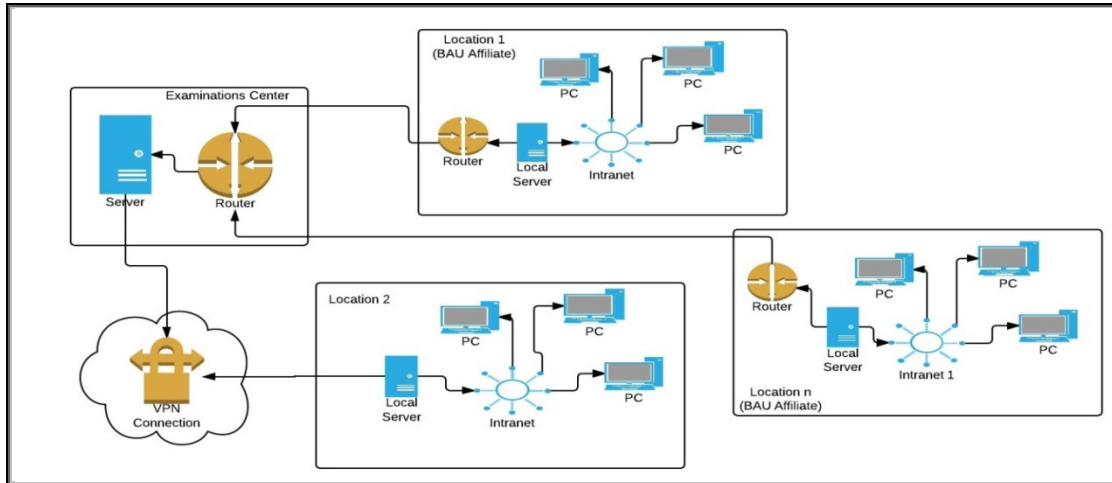

Figure 1: The method of preparation of the exam site through separate sites.

After the end of the exam, the system manager collects the student's answers from all of the exam sites by contacting an exam center .This method represents fewer loads on the server hardware, since the exam is local, and downloading the questions is through the central device in the university examination center across the network or over a VPN network.

Setting up this network is difficult, because there must be a server set up in each exam center, and this results to an additional cost, but this can be solved through the provision of personal computers and customize it to work as a server, or through simulation (Virtualization), which reduces costs. The current system also doesn't use data encryption and there is no restriction of devices, which means that any unauthorized person can enter to the exam. Moreover two students can use the same user name and password so one of them will not have an exam answers and this leads to put an incorrect result to this student.

6. PROPOSED SYSTEM

The proposed system divides dealing with data into three different stages: instructor, exam manager and student stages. The data in the first two stages can be encrypted by using **Advanced Encryption Standard** (AES) encryption\decryption algorithm before storing them in the cloud. The main objective is to enable data to be stored safely in order to avoid piracy and cut down the cost and time to encrypted data in the cloud computing [14]. Figure2 presents the framework of the proposed system.
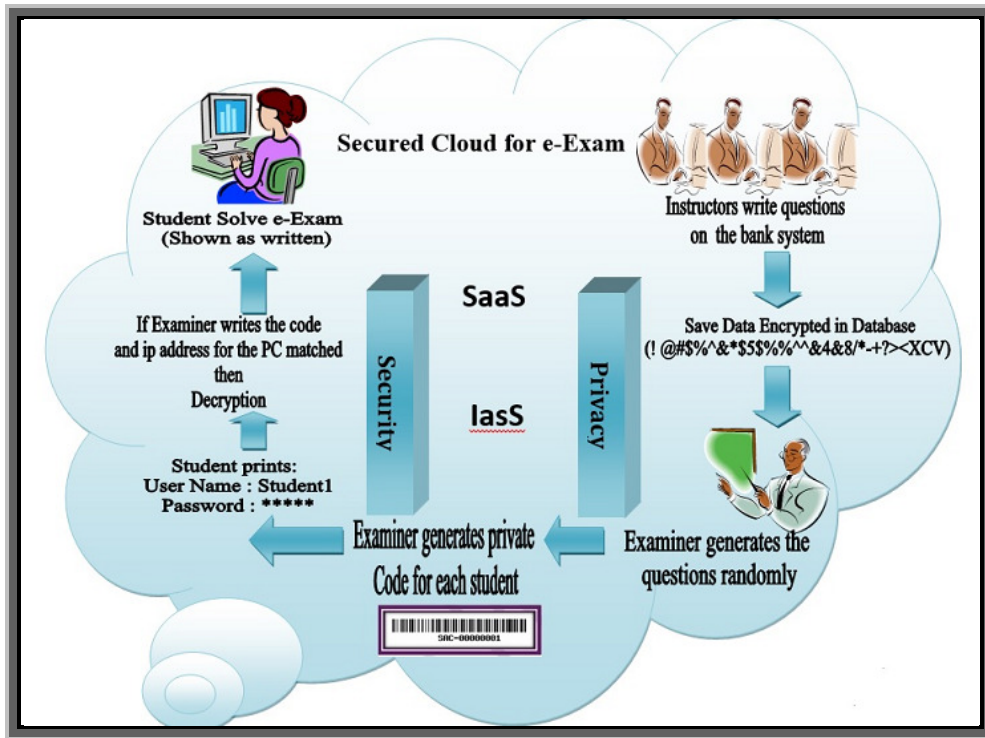
Figure 2: A framework of e-exam

The main steps of e-exam for instructors, manager and students:

Step 1: Add new exam by instructor

Figure 3: Adding a new exam

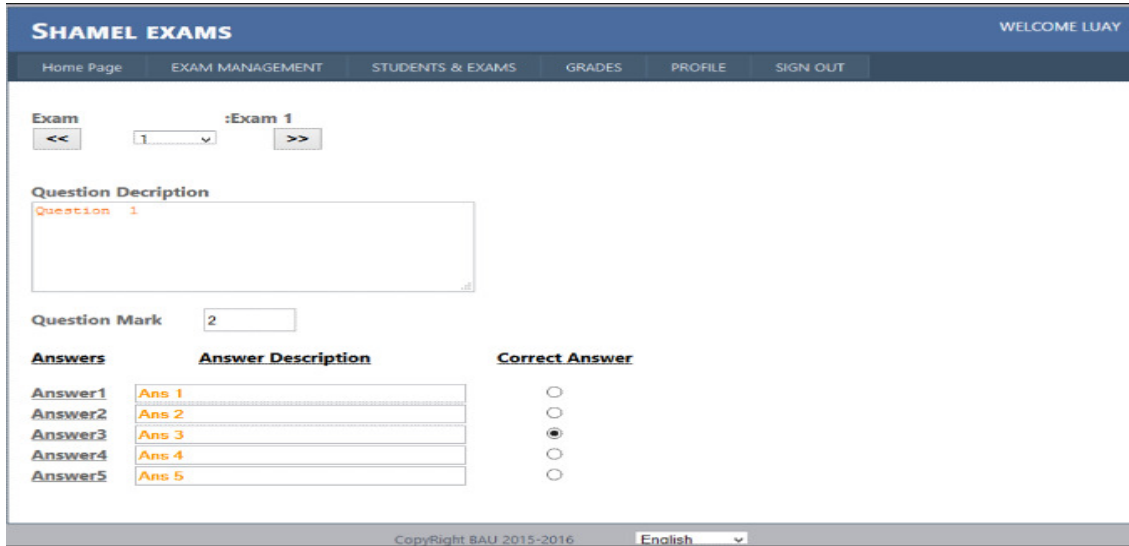**Step2**: Insert a new question and its answer choices

Figure 4: Adding a new question

Step 3: This is the database table that store questions

Note that all questions have been encrypted by AES algorithm

The previous "Question 1" has been encrypted and it will be stored as shown below:

	QID	QDesc	Exam	QMark
▶	6	mdC9cAS1Zev3MmxAkvdNxg==	21	2
	7	fhdQ7Cg0p12YbqRH0onqqw==	21	2
	8	mdC9cAS1Zev3MmxAkvdNxg==	22	5
	9	N8rs9wCPGuBmjQkfXIbbaQ==	23	5
	10	N8rs9wCPGuBmjQkfXIbbaQ==	23	5
	11	TphhkjcmZcMPIioVEDce/Q==	24	10
	12	49kcF6Yl05FDJxgXUscg+A==	25	5
✳	NULL	NULL	NULL	NULL

Figure 5: Question encryption

Step 4: This is the database table that store Answers.

Note that all answers have been encrypted by AES algorithm

The answers of the previous question "Ans1", "Ans2", "Ans3", "Ans4", and "Ans5" have been encrypted

	AID	ADesc	QuID	Validation
▶	16	QWB2NOJUOCm...	6	0
	17	OwV0SO7Flct6N...	6	0
	18	C1QYDd945mOa...	6	1
	19	J42YEzxPMTWj5...	6	0
	20	KihXLH1/r8uQ/p...	6	0
	21	QWB2NOJUOCm...	7	1
	22	OwV0SO7Flct6N...	7	0

Figure 6: Answer encryption

Step 5: This page used to assign students to selected exam. When assign student to an exam, each student will has a random key and distinct barcode to access the exam.

Figure 7: Security keys for each student

Step 6: This page used by student to access the exam, note that the distinct random key is required here and the student image must appear.
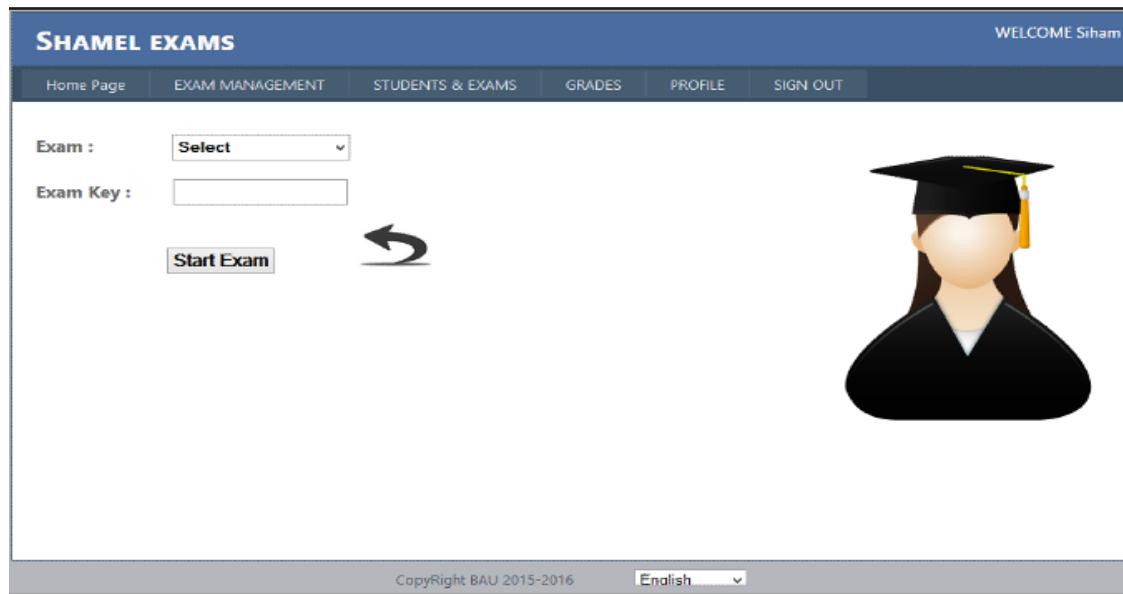
Figure 8: Access to exam

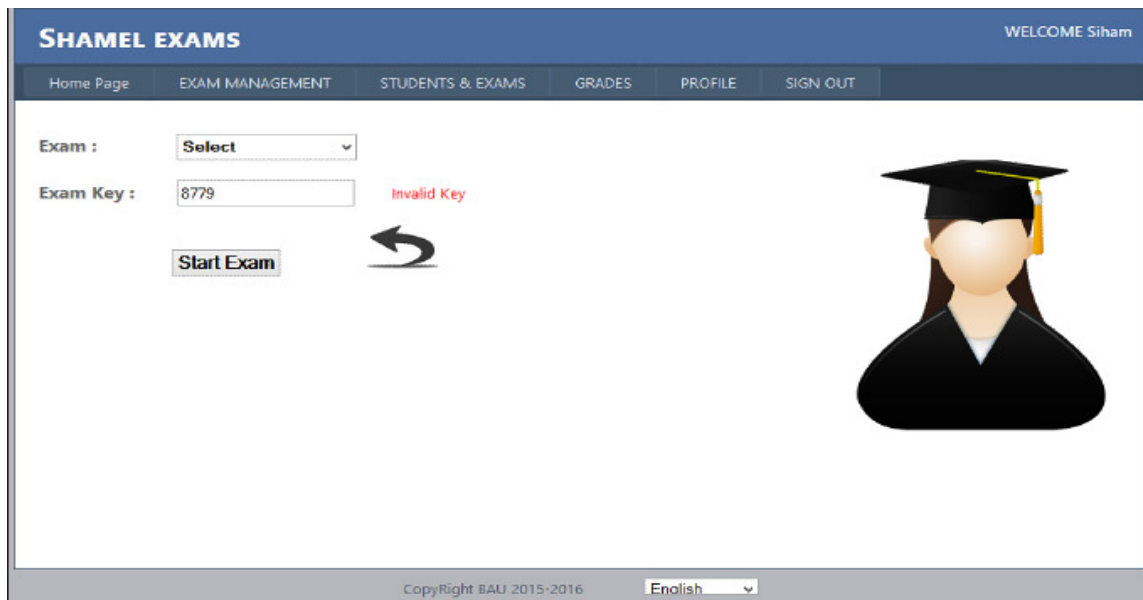**Step 7:** This case shows that this user tried invalid key.

Figure 9: Access denied because of using invalid key

Note that: All Flash memories, shortcuts and task manager (i.e: win+e ,win+d ....etc) will be disabled

Figure 10: Disable USP, Floppy and Shortcuts

Step 8: The student here starts the exam, the questions and answers have decrypted by AES algorithm.
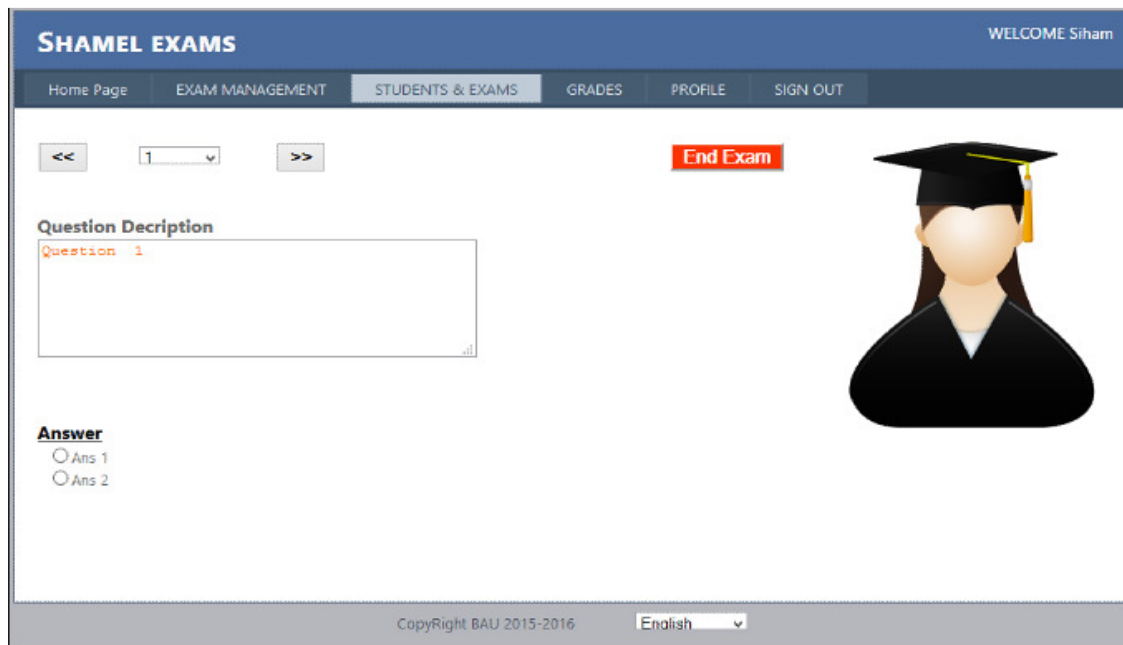

Figure 11: Question decryption

Step 9: A student in the right side tried to perform exam from outside or after the main session ended.
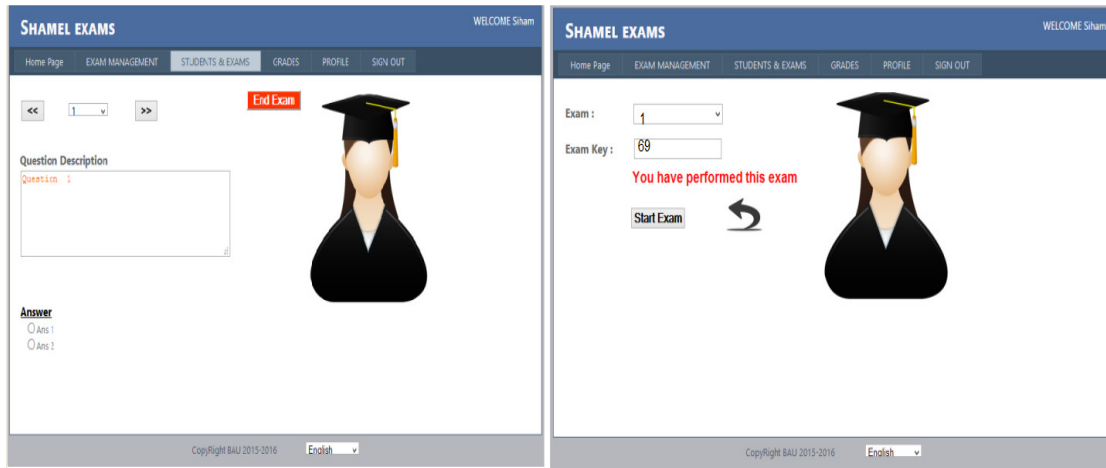

Figure 12: No additional persons can enter using the same keys

Step 10: This page used to determine IP addresses by that students can access Exam.
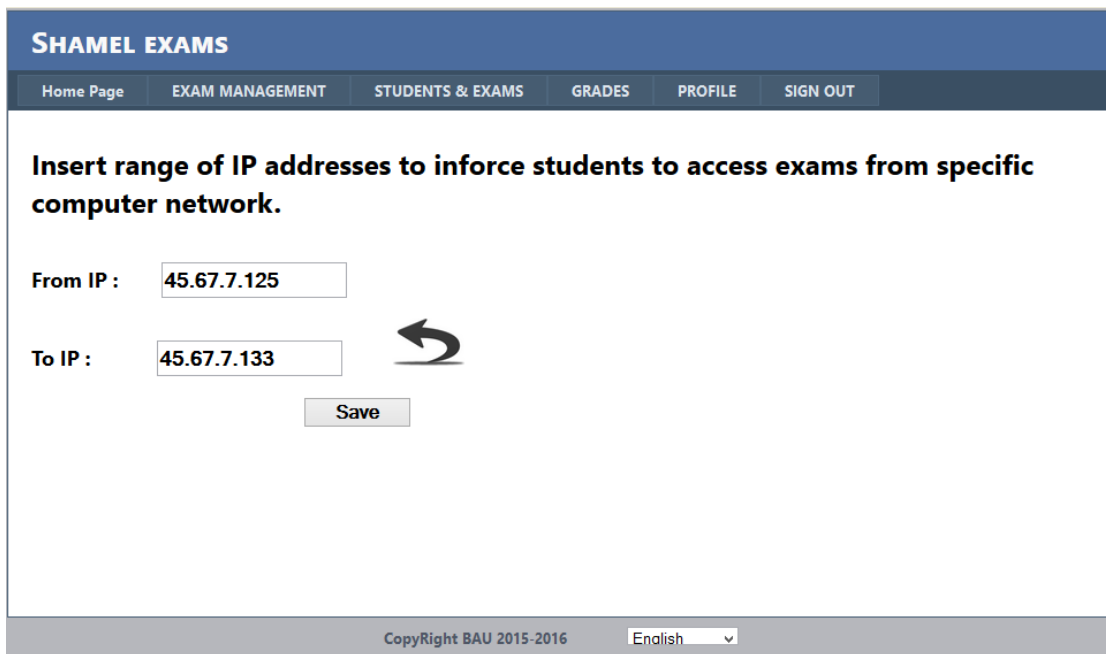

Figure 13: The IP's range that will be available in the exam

Step 11: In this case the student tried to access exam by IP which is not in range.
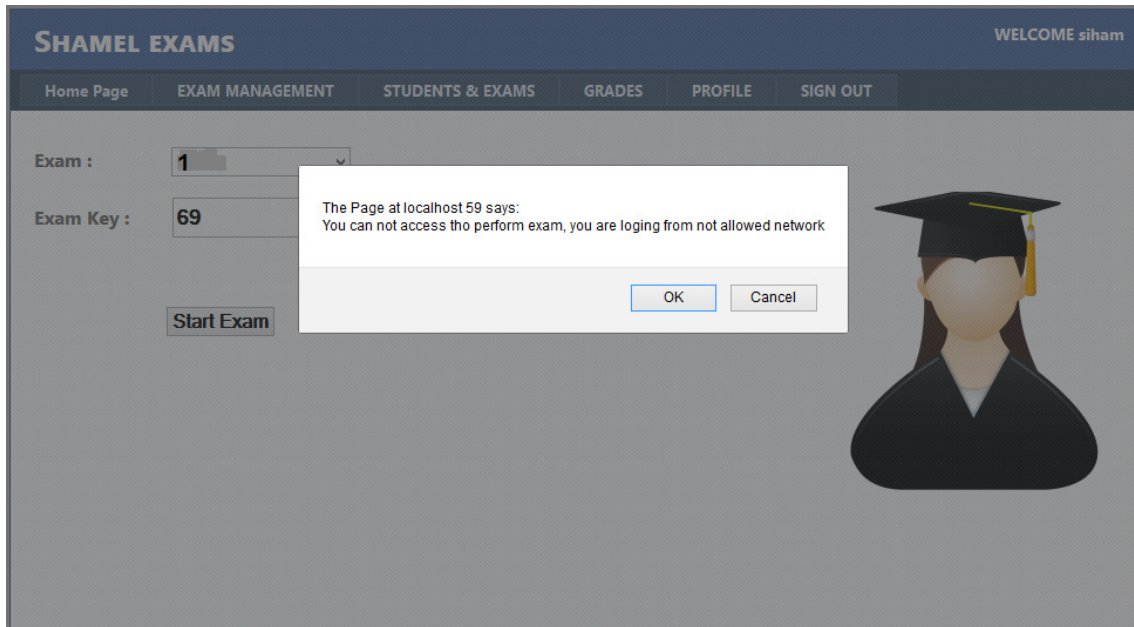

Figure 14: No one can use a device out of range

7. CONCLUSION

Using cloud services force us to take security and privacy into account while designing e-exam. This paper simply find out some of security issues and challenges commonly faced in cloud computing. A proposed system attempts to provide a secured environment for activities in online SHAMEL exam using the Cloud. This system provides an ideal model for the development and use of secured online SHAMEL exam in the Cloud.

ACKNOWLEDGEMENTS

REFERENCES

[1]   Saravg, A., & Kant, C. Cloud computing security and privacy concerns. *International Journal of Information Technology and Knowledge* , July-December 2012, Volume 5, No. 2, pp. 496-501
[2]   Agarwal, A., &Agarwal, A. (2011). The Security Risks Associated with Cloud Computing. International Journal of Computer Applications in Engineering Sciences, 1, 257-259.
[3]   Vitkar, S. (2012). Cloud Based Model for E-Learning in Higher Education. International Journal of Advanced Engineering Technology, 3(4), 38-42.
[4]   Malik, A., &Nazir, M. M. (2012). Security Framework for cloud computing environment: A review. Journal of Emerging Trends in Computing and Information Sciences, 3(3), 390-394.
[5]   Youssef, A. E., &Alageel, M. (2012). A Framework for A Framework for Secure Cloud Computing. IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 4, No 3.

[6]   Ukil, A., Jana, D., & De Sarkar, A.(2013). A security framework in cloud computing infrastructure. International Journal of Network Security & Its Applications (IJNSA), 5(5), 11-24.

[7]   Srivastava, H., & Kumar, S. A. (2014). Control Framework for Secure Cloud Computing. Journal of Information Security, 6(01), 12.

[8]   Takabi, H., Joshi, J. B., &Ahn, G. J. (2010, July). Secure cloud: Towards a comprehensive security framework for cloud computing environments. In Computer Software and Applications Conference Workshops COMPSACW, 2010 IEEE 34th Annual (pp. 393-398). IEEE.

[9]   Shahzad, F. (2014). State-of-the-art survey on cloud computing security Challenges, approaches and solutions. Procedia Computer Science, 37, 357-362.

[10] Naseem, S., &Sasankar, A. B. Cloud Computing Challenges & Related Security Issues. IOSR Journal of Computer Science (IOSR-JCE) e-ISSN: 2278-0661, p-ISSN: 2278-8727 PP 19-23

[11] Tirthani, N., &Ganesan, R. Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography. IACR Cryptology ePrint Archive, 2014, 49.

[12] Bora, U. J., & Ahmed, M. (2013). E-learning using cloud computing. Int. J. Sci. Mod. Eng, 1(2), 9-13.

[13] Kumar, S., Ali, J., Bhagat, A., &Jinendran, P. K. (2013). An Approach of Creating a Private Cloud for Universities and Security Issues in Private Cloud. International Journal of Advanced Computing, 36(1), 1134-1137.

[14] Bora,u& Ahmed ,M. E-Learning using Cloud Computing . International Journal of Science and Modern Engineering (IJISME), Volume-1, Issue-2, January 2013

[15] Tripathi, A., Mishra, A., IT Div., Gorakhpur Centre,Gorakhpur, India "Cloud Computing SecurityConsiderations", Signal Processing, Communications and Computing (ICSPCC), 2011 IEEE International Conference

[16] Navneet .S, Shailendra .S, The Amalgamation of Digital Watermarking & Cloud Watermarking for Security Enhancement in Cloud Computing , International Journal of Computer Science and Mobile Computing, Vol. 2, Issue. 4, April 2013, pg.333 – 339

[17] Sugam Sharma, U S Tim, ShashiGadia, and Johnny Wong.(2015).Proliferating Cloud Density through Big Data Ecosystem, Novel XCLOUDX Classification and Emergence of as-a-Service Era. (http://www.public.iastate.edu/~sugamsha/articles/Cloud%20Density%20in%20Big%20Data%20Eco system,%20Novel%20XCLOUDX%20Classification%20and%20Emergence%20of%20aaS%206%2 014%202015.pdf)

[18] Sugam Sharma. (2015). Evolution of as-a-Service Era in Cloud. Cornell University Library.(http://arxiv.org/ftp/arxiv/papers/1507/1507.00939.pdf)

[19] Sugam Sharma, U S Tim, ShashiGadia, and Johnny Wong.(2015).Growing Cloud Density & as-a-Service Modality and OTH-Cloud Classification in IOT Era. (http://www.public.iastate.edu/~sugamsha/articles/OTH-Cloud%20in%20IoT.pdf)

[20] http://shamel.bau.edu.jo/(S(4xbyg0didopnotle0vxiksob))/AboutUsPage.aspx visited date 20-8-014

[21] http://www.bau.edu.jo/Laws/files/laws/an/3.pdf , visited date 12-12-015

[22] http://www.mohe.gov.jo/ar/PublicUniversities/%D8%A3%D8%B3%D8%B3%20%D8%A7%D9%84 %D8%AA%D8%AC%D8%B3%D9%8A%D8%B1%202015.pdf , visited date 12-12-015

[23] National Institute of Standards and Technology (NIST) U.S department , NIST Cloud Computing Security Reference Architecture , NIST Special Publication 500-299

AUTHOR

Mohamad Al-Laham is an associate professor of Computer Information Systems at Al-Balqa Applied University in MIS department and has research interests in the areas of networking, internet, image processing and distributed systems.