Cloud computing security for e-learning during COVID-19 pandemic

Yassen AbdelKhaleq Najm[1], Suray Alsamaraee[2], Ahmed Adeeb Jalal[2]
[1]Department of English, College of Arts, Al-Iraqia University, Baghdad, Iraq
[2] Department of Computer Engineering, College of Engineering, Al-Iraqia University, Baghdad, Iraq

Article Info

Article history:

Received Mar 13, 2021
Revised Jun 16, 2022
Accepted Jul 14, 2022

Keywords:

Cloud computing
Cyber attacks
High education
Learning management system
video conference

ABSTRACT

The demand for e-learning services increased during the developments of the COVID-19 virus and its rapid spread, and the recommendations of the World Health Organization (WHO) that social distancing should be required. The rapid transition to the e-learning environment quickly led to the neglect of some security aspects, which led to an increase in cyber attacks targeting computer accounts, which is one of the most important pillars of e-learning. In these papers, the attacks that target the cloud computer used in the most important e-learning have been studied and classified according to the victim using an inductive methodology based on global statistics related to cyber attacks and recent research. And suggest appropriate solutions to avoid its occurrence in the near future and raise the level of protection for those computer clouds.

Corresponding Author:

Ahmed Adeeb Jalal
Department of Computer Engineering, College of Engineering, Al-Iraqia University
Baghdad, Iraq
Email: ahmedadeeb@aliraqia.edu.iq

1. INTRODUCTION

From the inception of computer networks to the present day, network security is one of the most important and complex issues related to networks. Network security or as so called cybersecurity, is the main challenge for network designers and operators [1], [2]. More specifically, the concept of informatio-security refers to the techniques and processes which are designed in form to protect all types of sensitive information and data whether in electronic or printed form from unauthorized-access. For the digital world or the fourth industrial age in which we live, information of all types considered as valuable asset in digital word for every company and individual, which increases its importance to protect them from damage or theft [3]. Whereas, cybersecurity is a branch of information-security which deals with protecting Internet systems including software, data and hardware from any type of cyber attacks. Protects network integrity from unauthorized electronic access [4], [5]. Network security is a branch of cyber security that is designed to protect network connectivity and secure data delivery through network components. Thus, the concept of network-security is a branch of information/internet security that deals with the implementation and planning of network-security measures to protect the integrity of software and networks from unauthorized-access and hacking [6]. It protects the network-accessible resources and information technology (IT) infrastructure of organization from all kinds of cyber-threats like viruses, malware, trojans, spyware, and spam. A network-security professional's job is to make transferring data over networks more safer by providing technical solutions including assistance with intrusion detection systems, firewalls, encryption, and digital certificates [3].

The development of technology, the increase in demand, and the use of Internet services has increased the opportunity for criminals to exploit these requests, and the number of users has increased to carry out cyber attacks that almost paralyze the movement of many websites [6]. During the past few years, all areas of life witnessed a rapid transformation to the digital world because of the spread of the Coronavirus disease or as so called COVID-19 pandemic. This rapid transformation did not allow many institutions to take into account the requirements of cyber security, which created a very suitable environment for saboteurs and criminals to carry out cyber attacks in a large way [7]. According to, the Federal Bureau of Investigation (FBI) report, the rate of cyber attacks increased during the year 2020 compared to 2019, and the report also indicated that we would be lucky if the rate of these crimes remained at this level, but the indications are that these attacks are constantly increasing [8]. The Corona crisis directly affected the education sector in particular. It prompted many schools and universities to close their doors to students, teachers, and administrative, which almost caused a complete halt to education operations. This caused great concern to everyone who has an interest in this sector, especially students who expect to take exams that determine their future, such as exams for middle and high school certificates or even university exams [7]. E-learning process depends mainly on cloud computing, which provides services to save students' data and grades in addition to files related to educational curricula such as google class room platform, Zoom, Microsoft teams and other educational platforms [9], [10].

Ibrahim *et al*. [11] proposed a hybrid cloud computing architecture. This architecture constitutes an ideal solution to the problems of e-learning in developing countries that do not have the components of e-learning. Nevertheless, none of the security risks that may face this structure or the development of security solutions or strategies to prevent its penetration were discussed.

Kanwal *et al*. [12] provided a comprehensive explanation of the risks faced by the cloud computer by presenting different types of potential cyber attacks. Also, their highlighted the importance of the policies followed by both the server and the client to maintain an acceptable level of security when using the computer cloud. But no practical solutions were presented for these cyber attacks. Arora and Nandal [13] presented a literary reading of the research related to cyber attacks. The research concluded that there is a real problem facing cloud-based e-learning. Because of students often neglect the security aspect while benefiting from cloud services and also the flexibility requirements that must be provided in the cloud that increase the risks of attacks However, no practical solutions have been presented to these risks.

Ahmad *et al*. [14] presented a detailed explanation of the structure of cloud computing used in IoT and machine learning applications, which is very similar to the structure of the ordinary computer cloud. He presented a new classification of the levels of security that must be available in the cloud according to four main categories. According to, Alexei and Alexei [15] the cyber attacks that e-learning suffers from can be classified according to the technologies used by e-learning (learning management system (LMS), Cloud Computing, volatile substance abuse (VSA)). The researcher suggested a solution for each technology separately, but without activating or trying the proposed technologies. The results concluded to the need to constantly update the software and applications used.

Hence, educational institutions face the threat of cyber-attacks that aim to access information related to exams or tamper with students' data and grades. The matter becomes more dangerous when talking about institutions of higher education and scientific research [16], [17]. Statistics indicate that the field of education in particular, the losses resulting from the data breach amounted to about 3.9 million dollars [18], while the losses caused by data breaches in scientific research will cost approximately 1.53 million dollars [19]. Perhaps the main reason for the high cost and rates of cybercrime is due to the rapid transition to e-learning applications, whose weaknesses have not been tested and tested well, as indicated previously. Therefore, there is great importance to study the cyber-attacks encountered by the e-learning process and determine its structure, which certainly contributes to the development of that process in terms of cyber security to ensure a higher level of protection. Thus, we identify all types of cyber attacks and discover weaknesses in the current applications used in e-learning in addition to recent research related to the analysis of these attacks to find appropriate solutions to these attacks and prevent similar occurrences in the future.

2. METHOD

2.1. Cloud computing

It is one of the most important internet applications in the field of e-learning. Where, cloud computing provides a suitable environment for both students, professors, and administrative bodies in universities and schools, where in health conditions that prevent the presence of students in the classroom and it is not possible to predict a specific date for the return to normal life [20]. Cloud computing comes as an option optimized to create a virtual environment for storing student data for the administrative body, as for students and professors. Cloud computing services include virtual laboratories within a modeling environment that enhances student understanding and makes it easier for teachers to perform their task. The following are the most important services provided by cloud computing in the field of e-learning, as shown in Figure 1.

a. Software as a service (SaaS): this service provides the use of various applications and programs such as Microsoft Office and online modeling programs through the user's account only without incurring licensing costs.
b. Platform as a service (PaaS): these services support software development through different programming languages, allowing the teacher to design a lab with specific tools and share the program with their students.
c. Infrastructure as a service (IaaS): that allows students to test and learn about operating systems and is very important for students of technology and computer engineering.

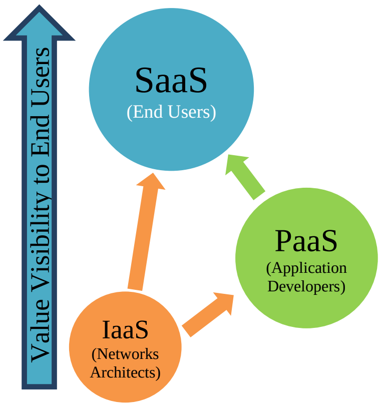

Figure 1. Cloud computing services

Addition to, setting online quarterly exams and canceling them after the end of the semester, creating accounts for many users to do their projects and training. It became possible to harness cloud computing technology to serve educational goals in several areas, including providing lessons remotely or lectures or even labs. The mechanism of work to achieve this is through teachers or lecturers uploading the necessary documents and notes to an electronic cloud directly or through a university or school application so that students can access and benefit from that data at any time. Courses and seminars can also be shared through the same cloud. Cloud computing service can include many benefits for learners [21], [22], including:

- Ease of sharing exercises and assignments to teachers and students as well and take tests directly.
- Easy access to exercises, tests and projects which submitted by students.
- Provides easy communication between students.
- Provides new educational means for both teachers and students.
- Provides a way to use apps and programs without downloading them and installing them on devices that may not meet the requirements of those applications, where they just need to connect to the internet.
- University students can access all programs at any time, from any where and using any portable device connected to the internet.
- Access to systems to develop programs and applications then store them in the university infrastructure.

2.2. Learning management system (LMS)

A LMS is an online program used to design, implement and evaluate a learning system within an educational institution. Universities and schools tend to use LMS to have a comprehensive digital structure of their education system [23], [24]. The LMS platform can be used as a communication platform between the school and students; whether it is to implement e-learning or integrate blended learning. The system can also be used to handle personnel matters, track student progress, generate monthly reports, and more. There are many LMS standards that must be in place for a successful and effective implementation. Here are the components of a LMS that you need to have a general idea of the system.

2.2.1. A platform for student-teacher communication

Mong the many advantages of the existing LMS is that it simplifies the interaction between the main users within the educational institution: teachers and students. Instead of switching between emails and chats, students and educators can easily communicate within a unified platform either individually or as a group.

These platforms for texting, messaging, and communication make it easier for teachers to send out assignments, reminders, and progress reports and communicate with parents and students.

2.2.2. Create calendars

A good LMS platform should be able to include an assessment feature. This is useful for many reasons: it constitutes a general calendar to keep each party informed of deadlines, important events, and holidays. Calendars can also be used for each course to specifically update lessons and activities.

2.2.3. User affairs management

Under a LMS, there is a huge range of users who take advantage of its features. These programs include teachers, students, managers, department heads, and even parents. The LMS must be able to create an easy-to-use and simplified interface for each participant. Another option also includes the ability to track work performance and generate monthly or annual reports accordingly [25].

2.2.4. Manage notifications

An important feature that can certainly be added to any LMS management system is the notification center. The LMS notifies people when an event occurs that they need to know about. This is especially useful for facilitating communication between users to get the latest ads that are shared among all.

2.2.5. Setting calendars

This function is fantastic for saving the instructor or department head time and effort. Rather than, squandering time developing and planning quizzes. This tool can handle that, allowing teachers to measure and compare student progress against learning objectives and expectations.

2.2.6. Material management and registration

LMS platforms can manage courses registration within the system and manage all aspects of a course. The LMS allows adding or withdrawing materials, assigning materials to teachers and students. Through LMS, teachers may create and integrate course materials, articulate learning goals, align content and assessments, track studying progress, and create customized tests for students.

2.2.7. Cloud storage system

Typically, LMS platforms integrate a cloud storage system for quick and easy access to materials. This is very useful for students as they do not have to browse through endless files to get the required files. Teachers also benefit from this feature as they can download lesson materials, tools, and assignments with the click of a button.

2.3. Video-conference

It is a relatively recent communication technology that relies on visual communication between a group of people, where the sound and image are transmitted directly between a group of people located in different geographical areas. These connections need a high connection speed in addition to a set of equipment such as a reasonable quality microphone and headphones, in addition to a web camera. Thus, the participants in the video communication can see each other and hear each other as if they were gathered in one place [26]. This type of communication has many applications, not only in the field of business, but also in the field of education, where it is possible to hold scientific seminars and lectures and conduct research discussions via the Internet and in the presence of people who may be difficult to be present in one place, which supports e-learning. Thus, it saves a lot of trouble and hardship by achieving the same goals of meeting people without travel costs or physical fatigue. This technology allows to exchange and display of files during the meeting session and directly. Visual communication technology can be classified into two main categories [27]:

a. The first type is point-to-point communication between two people.
b. The other is multi-point communication between groups of people [26].

This technology is one of the most important techniques used in e-learning, as it provided an interactive teaching method that contributes to the dissemination of education in places far from the teacher [27]. Where the video connection provides a means of communication between the teacher and the students, through which the teacher can explain the lessons to the students, and the students can in return for asking questions and participating in solving exercises, as well as exchanging files and taking attendance for students. Thus, e-learning based on cloud computing for educational institutions has some security issues that need to be addressed [28]. So, in the next section we will be discussing the security aspects and cyber attacks that threaten the security and integrity of cloud-based e-learning. We will also discuss the major security concerns and possible solutions to them.

3. RESULTS AND DISCUSSION

The security challenges become a significant challenge in order to ensure that only the right information is available to the right people at the right time. One of the most significant problems that has hampered the growth of cloud computing is security [29], [30]. In general, the security aspects and cyber-attacks that threaten the security and integrity of cloud-based e-learning can be classified into two main categories, as shown in Figure 2.

a. Security aspects and cyber attacks targeting cloud computing infrastructure and causing harm to a number of users.
b. Security approaches and cyber attacks targeting individuals who use cloud computer computing services and causing harm to the target person.

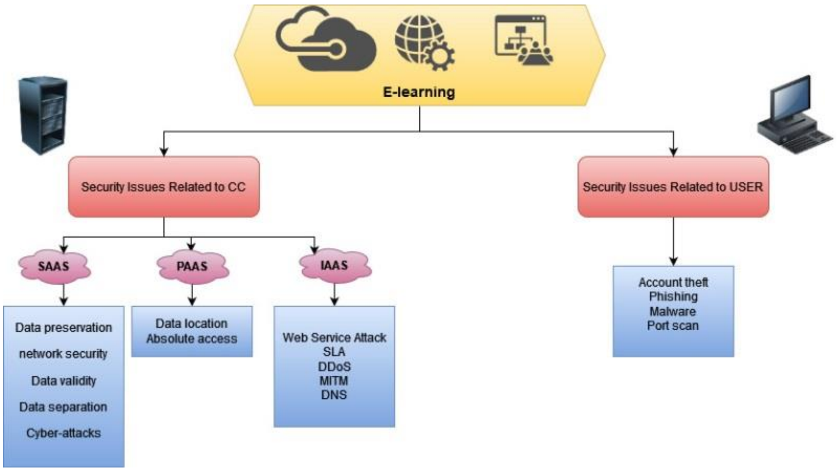

Figure 2. Security aspects related to e-learning

3.1. Security aspects and cyber attacks targeting the cloud computing infrastructure

Each type of cloud computing services (SaaS, PaaS, IaaS) has a specific pattern or type of cyber-attack that differs in terms of its intended goal. But all of these attacks combine to cause harm to the real beneficiaries of cloud computing services. These attacks can be categorized as:

3.1.1. SaaS

During SaaS programming of cloud computing services. The responsibility for information security rests with the service provider to prevent others from viewing information about a specific customer without his permission. Accordingly, it difficult for the customer himself to verify the existence of these security measures by the server [31]. The most important security problems faced by this service are:

a. Data preservation: the main task of cloud computing is to save customer information in a huge data bank and protect this information from damage, loss, unauthorized access or unauthorized modification. Because these banks are the main target of hackers and cyber attacks. Therefore, the cloud server must address these points and ensure that the privacy of customer data is not compromised to maintain a high level of security.
b. Network security: network security protects your network and data from breaches, intrusions and other threats. The security of the computer network in the cloud is related to the encryption mechanisms that the cloud service provider uses to protect data from leakage. For examples, transport layer security (TLS) and secure socket layer (SSL), man-in-the-middle attacks (MITM), port scanning, and packet sniffing.
c. Data validity: data verification is one of the operations that a program performs to make sure that the data entered is clean and not intended to sabotage the program or anything like that. The cloud computing must provide the safety of data stores and ensure access to them at any time without loss or damage. To ensure that this goal is achieved, the following criteria are used structured query language (SQL) injection flaws, data validation, and insecure storage.
d. Data separation: customer data is stored in the cloud contiguously. Consequently, it is difficult to distinguish customer data from another customer. In other words, the cloud service provider must

provide an appropriate protocol for separating the data of each client. Ordinarily, the separating done either physically or using a software architecture that secures this purpose.

e. Cyber attacks: being a data bank, the cloud is a valuable target for hackers who are trying hard to access users' data in order to use it for their personal purposes. Despite the high security precautions provided by the SaaS server. Hackers can still sometimes penetrate the fortifications of the cloud.

3.1.2. PaaS

It's a programming environment that allows users to access and use applications. The application is offered by the providers, who supply the development envi-ronment and toolkits against cloud computing security threats and countermeasures [32]. The most important security problems faced by this service are:

a. Data location: PaaS cloud services provide the ability to create and test applications and software. SaaS applications are used to obtain PaaS services. Therefore, the location of the data is not known to the user, what causes a risk for the data, as the data may be stored in a server that does not have a high reliability. For this reason, many countries are seeking to set strict standards about where customer data is stored so that it is not allowed under any circumstances to store sensitive data in places outside the borders of the country.

b. Absolute access: the cloud service provider has absolute access to the data and applications in the cloud. It makes the data available to the service provider who is likely to use it unauthorizedly. Therefore, must ensure the protection of critical data and applications, whether hosted in the cloud, as a service or on-premises.

3.1.3. IaaS

It's a type of cloud computing that uses the internet to deliver virtualized compu-ting resources. IaaS is one of the three primary categories of cloud computing services. This service faces some problems and challenges [33], the most significant problems and obstacles that this service encounters will be listed.

a. Web service attack: the cloud infrastructure is accessed via Internet services, more specifically the simple object application protocol (SOAP). SOAP uses XML techniques to pass messages. Despite of the security efficiency of XML, there are still some cyber attacks that succeed in achieving their goals in penetrating XML messages.

b. Service level agreement (SLA): SLA is a contract established between a customer and a cloud computing service provider in which the service provider guarantees a specified level of quality through a set of variables. They explicitly identify measurements, obligations, and expectations so that, in the case of service difficulties, all parties have a common knowledge of the needs. The cyber-attack may target the service level.

c. Distributed denial of service (DDoS): distributed attacks on networks or network-dependent services are called DDoS attacks. This type of cyber attack depends on the limited capabilities of service providers across the network, such as the cloud infrastructure or the website of an organization or company. This attack is often called a flooding attack. It is done by sending a flood of requests on the cloud server so that the cloud resources as processor and RAM, become insufficient to meet all the requests. Thus, cloud services become unavailable to the rest of the users. In such cases, the cloud server resorts to sharing resources from a nearby server. But the best solution is to distinguish the phantom requests in the CPU.

d. Man-in-the-middle (MITM): MITM attack is one form of eavesdropping where there is an untrusted person. The attacker is eavesdropping and monitoring the communication between two devices and capturing the information that is exchanged between these two devices in order to access that data, and sometimes the attacker change the data that is exchanged. In this pattern, the attacker targets the public key of the sent encrypted messages and then modifies that key with another task-specific key before sending it back to the receiver. During the occurrence of this attack, both the sender and the receiver do not feel that the attack has occurred and that the transmitted data has already been exposed or even changed by the attacker, and herein lays the danger of such attacks.

e. Domain name system (DNS): a DNS attack targets the DNS infrastructure. Both the IaaS cloud server and the client handle non-realistic internet protocol (IP) addresses and the DNS server translates the requested addresses into IP addresses. The attack on the DNS server aims to change the requested addresses and thus control the communication process between the server and the client.

3.2. Security aspects and cyber attacks targeting individual

3.2.1. Account theft

These attacks are considered among the most dangerous attacks. Where a specific customer is targeted to obtain login information for an account owned by a person or organization with the aim of taking full control on account, copying confidential information, deleting information or destroying it, which causes great losses to the real account holder on the physical and moral level. The level of complexity of the attack depends on the awareness of the user or customer and the protection measures to prevent account theft by hackers.

3.2.2. Phishing

Phishing attack is actually one of the complex account theft methods that need expertise by the hacker in web design. During a phishing attack, the attacker designs a website with an interface similar to the login interface to the cloud. Then, he sends the link of the fake page to the victim and asks them to log in, which prompts the victim to log in to the fake page. The fake page is designed to send the information entered by the victim to the attacker and thus the account is completely controlled by the vandal.

3.2.3. Malware

It is software that is written with the aim of controlling the computer after it is installed on it. The modus operandi of this software varies according to its different types, some of which target keyboard tracking or tracing logins saved on the computer. There are many types of malware, and they can be classified according to:

a. Viruses: which are parts or sections of program code such as functions those cybercriminals insert into normal code of programs. When a program is installed and starts working, it damages computers systems and damages the files. In addition, these codes may insert themselves into codes of normal software.

b. Worms: which are stand-alone malware that comes and transferring from one computer to another, and they are able to transform very quickly, literally making their way across the devices of network.

c. Trojans: which are programs that are not able to generate themselves, and users innocently allow them to go through their computers because trojans look like program or something else that user wants. Once in, the trojan horse enables other software "malware" to enter the system of device and may allow hackers to install harmful programs manually or accessing your computer personally or remotely.

3.2.4. Port scan

During this attack, the hacker penetrates the firewall. This allows to access open windows, and reads their data and information, which causes a loss of confidentiality of information and mechanisms of integration with the cloud. Therefore, it requires great experience in operating systems and mechanisms for penetrating various firewalls.

After a statement and clarification, security aspects and cyber attacks targeting the cloud computing infrastructure. Also, explain the security aspects and cyber attacks targeting individual. Some security steps that must be taken into consideration by both the cloud server and the end users:

a. Security measures and suggestions for cloud computing infrastructure: all of the above was a sufficient and strong justification for taking action to shift towards e-learning and its mechanisms and ways of integrating it with traditional education methods. E-learning harnessed the development of technology, such as increasing speed of communication and cloud computing, in addition to the technologies of the internet of things (IoT). The following are some practices that must be taken care of:
   - The cloud computer should provide protection tools to prevent unauthorized access and allow the user to take a backup copy of his data and adopt electronic signature mechanisms to ensure the validity of the data such as hash value.
   - Providing a layer of protection for the connection that analyzes data and requests such as SSL and TSL, in addition to identifying fake requests, which constitute one of the most dangerous cyber attacks.
   - Take appropriate mechanisms to separate the data of different users.
   - Ensuring appropriate encryption of data by adopting a unique encryption key for each client so that it is impossible for the cloud server to read user data, thus providing a secure environment within the cloud.
   - Adopting constantly updated servers to prevent hackers from entering.

b. Security measures and suggestions for the end user: awareness of potential security risks is the most important requirement that must be met by end users. Mahyoob's [7] study has proven that the rapid transition to e-learning under the current circumstances was not an option. Therefore, many users are not already prepared to engage in the e-learning process and bear its security risks. Thus, awareness must be spread among the user community towards these risks. The following are some practices that must be taken care of:
   - Saving personal account logins on devices not owned by the account holder.

- Click on any link and follow the instructions that ask for personal account information.
- Identify and report fake and suspicious emails.
- Keep your computers firewall up to date.
- Caution while using smart phone devices to access the computer cloud as much as possible for easy penetration and download malicious applications on it.
- Change account passwords periodically and choose passwords carefully so that they are difficult to hack.

4. CONCLUSION

In these papers, the mechanisms of e-learning and its various applications that depend almost entirely on Internet resources have been studied. Then the security risks and potential cyber attacks facing the use of computer clouds during the e-learning process were classified into two main categories, the first targeting the end user (teachers, students, educational institutions) and the second targeting the cloud server itself. In addition to a study of each type of those risks and attacks. As a result of this study, it can be said that the responsibility to maintain a high level of security rests with both the end users and the cloud computer server together, especially in light of the large and rapid demand for cloud computing resources, in addition to the fact that some strict security measures for the cloud server may be annoying some times for users, who demand more flexibility from the cloud server.

REFERENCES

[1] N. A. A. Rahman, I. H. Sairi, N. A. M. Zizi, and F. Khalid, "The importance of cybersecurity education in school," *International Journal of Information and Education Technology*, vol. 10, no. 5, pp. 378–382, 2020, doi: 10.18178/ijiet.2020.10.5.1393.

[2] K. H., F. M., M. R., and H. Fajraoui, "Cloud computing security challenges in higher educational institutions-a survey," *International Journal of Computer Applications*, vol. 161, no. 6, pp. 22–29, Mar. 2017, doi: 10.5120/ijca2017913217.

[3] M. Abu-Alhaija, "Cyber security: Between challenges and prospects," in *ICIC Express Letters, Part B: Applications*, 2020, vol. 11, no. 11, pp. 1019–1028, doi: 10.24507/icicelb.11.11.1019.

[4] J. W. Lian, "Understanding cloud-based BYOD information security protection behaviour in smart business: in perspective of perceived value," *Enterprise Information Systems*, vol. 15, no. 9, pp. 1–22, Oct. 2020, doi: 10.1080/17517575.2020.1791966.

[5] N. Taha and L. Dahabiyeh, "College students information security awareness: a comparison between smartphones and computers," *Education and Information Technologies*, vol. 26, no. 2, pp. 1721–1736, 2021, doi: 10.1007/s10639-020-10330-0.

[6] M. Durairaj and A. Manimaran, "A study on security issues in cloud based e-learning," *Indian Journal of Science and Technology*, vol. 8, no. 8, pp. 757–765, Apr. 2015, doi: 10.17485/ijst/2015/v8i8/69307.

[7] M. Mahyoob, "Challenges of e-Learning during the COVID-19 pandemic experienced by EFL learners," *Arab World English Journal*, vol. 11, no. 4, pp. 351–362, Dec. 2020, doi: 10.24093/awej/vol11no4.23.

[8] FBI's IC3, "2020 Internet Crime Report," *Federal Bureau of Investigation of Internet Crime Complain*, 2020. [Online]. Available: https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf.

[9] R. Radha, K. Mahalakshmi, V. S. Kumar, and A. R. Saravanakumar, "E-learning during lockdown of Covid-19 pandemic: a global perspective," *International Journal of Control and Automation*, vol. 13, no. 4, pp. 1088–1099, 2020.

[10] A. Kamysbayeva, A. Koryakov, N. Garnova, S. Glushkov, and S. Klimenkova, "E-learning challenge studying the COVID-19 pandemic," *International Journal of Educational Management*, vol. 35, no. 7, pp. 1492–1503, Nov. 2021, doi: 10.1108/IJEM-06-2021-0257.

[11] M. H. Ibrahim, M. Abbas, and M. Hassan, "Cloud computing for e-learning: a proposed model for higher education institutions in developing countries," *Article in International Journal of Scientific & Technology Research*, vol. 10, no. March, pp. 408–416, 2021, [Online]. Available: www.ijstr.org.

[12] I. Kanwal, H. Shafi, S. Memon, and M. H. Shah, "Cloud computing security challenges: a review," in *Advanced Sciences and Technologies for Security Applications*, 2021, pp. 459–469.

[13] S. Arora and N. Nandal, "Investigating scope and challenges in cloud based e-learning system," *Turkish Journal of Computer and Mathematics Education*, vol. 11, no. 2, pp. 640–649, 2020.

[14] W. Ahmad, A. Rasool, A. R. Javed, T. Baker, and Z. Jalil, "Cyber security in IoT-based cloud computing: a comprehensive survey," *Electronics*, vol. 11, no. 1, p. 16, Dec. 2021, doi: 10.3390/electronics11010016.

[15] A. Alexei and A. Alexei, "Cyber security threat analysis in higher education institutions as a result of distance learning," *International Journal of Scientific & Technology Research*, vol. 10, no. 3, pp. 128–133, 2021, [Online]. Available: www.ijstr.org.

[16] J. B. Ulven and G. Wangen, "A systematic review of cybersecurity risks in higher education," *Future Internet*, vol. 13, no. 2, pp. 1–40, Feb. 2021, doi: 10.3390/fi13020039.

[17] Y. Wang, M. Xia, W. Guo, F. Xu, and Y. Zhao, "Academic performance under COVID-19: The role of online learning readiness and emotional competence," *Current Psychology*, Jan. 2022, doi: 10.1007/s12144-022-02699-7.

[18] A. Alexei, "Cyber security strategies for higher education institutions," *Journal of Engineering Science*, vol. XXVIII, no. 4, pp. 74–92, Dec. 2021, doi: 10.52326/jes.utm.2021.28(4).07.

[19] A. M. Algarni, V. Thayananthan, and Y. K. Malaiya, "Quantitative assessment of cybersecurity risks for mitigating data breaches in business systems," *Applied Sciences (Switzerland)*, vol. 11, no. 8, p. 3678, Apr. 2021, doi: 10.3390/app11083678.

[20] E.-S. T. Abumandour, "Applying e-learning system for engineering education – challenges and obstacles," *Journal of Research in Innovative Teaching & Learning*, Oct. 2021, doi: 10.1108/jrit-06-2021-0048.

[21] M. Bosamia and A. Patel, "An overview of cloud computing for e-learning with its key benefits," *International Journal of Information Sciences and Techniques*, vol. 6, no. 1/2, pp. 1–10, Mar. 2016, doi: 10.5121/ijist.2016.6201.

[22] D. K. A.-R. Al-Malah, I. A. Aljazaery, H. T. S. Alrikabi, and H. A. Mutar, "Cloud computing and its impact on online education," *IOP Conference Series: Materials Science and Engineering*, vol. 1094, no. 1, p. 012024, Feb. 2021, doi: 10.1088/1757-899x/1094/1/012024.

[23] V. M. Bradley, “Learning management system (LMS) use with online instruction,” *International Journal of Technology in Education*, vol. 4, no. 1, p. 68, Dec. 2020, doi: 10.46328/ijte.36.

[24] CHRISTOPHER M. LEE, “Learning management systems (LMS) towards helping Teachers and students in the pursuit of their e-methodologies 1,” *Technological Institute of the Philippines*, no. March, pp. 1–9, 2021.

[25] C. Galarce-Miranda, D. Gormaz-Lobos, and H. Hortsch, “An analysis of students’ perceptions of the educational use of ICTs and educational technologies during the online learning,” *International Journal of Engineering Pedagogy*, vol. 12, no. 2, pp. 62–74, Mar. 2022, doi: 10.3991/IJEP.V12I2.29949.

[26] P. Gladović, N. Deretić, and D. Drašković, “video conferencing and its application in education,” *Journal of Traffic and Transport Theory and Practice*, vol. 5, no. 1, Mar. 2020, doi: 10.7251/jtttp2001045g.

[27] C. Coman, L. G. Țîru, L. Meseșan-Schmitz, C. Stanciu, and M. C. Bularca, “Online teaching and learning in higher education during the coronavirus pandemic: Students’ perspective,” *Sustainability (Switzerland)*, vol. 12, no. 24, pp. 1–22, Dec. 2020, doi: 10.3390/su122410367.

[28] M. Malhi, U. Iqbal, M. Nabi, M. M.-I. J. of, and undefined 2020, “E-learning based on cloud computing for educational institution: Security issues and solutions,” *Airitifile.Com*, vol. 12, no. 4, pp. 162–169, 2020, doi: 10.6636/IJEIE.202012_12(4).03.

[29] A. R. Malik, S. Sarfraz, U. Shoaib, G. Abbas, and M. A. Sattar, “Cloud based E-learning, security threats and security measures,” *Indian Journal of Science and Technology*, vol. 9, no. 48, Dec. 2016, doi: 10.17485/ijst/2016/v9i48/96166.

[30] M. A. Almaiah, A. Al-Khasawneh, and A. Althunibat, “Exploring the critical challenges and factors influencing the E-learning system usage during COVID-19 pandemic,” *Education and Information Technologies*, vol. 25, no. 6, pp. 5261–5280, 2020, doi: 10.1007/s10639-020-10219-y.

[31] A. Ali and A. Alourani, “An Investigation of Cloud Computing and E-Learning for Educational Advancement,” *International Journal of Computer Science and Network Security*, vol. 21, No. 11, pp. 216–222, Nov. 2021, doi: 10.22937/IJCSNS.2021.21.11.30.

[32] A. F. Alotaibi, M. A. AlZain, M. Masud, and N. Z. Jhanjhi, “A Comprehensive Survey on Security Threats and Countermeasures of Cloud Computing Environment,” *Turkish Journal of Computer and Mathematics Education*, vol. 12, no. 9, pp. 1978–1990, 2021, [Online]. Available: https://www.turcomat.org/index.php/turkbilmat/article/view/3662.

[33] A. Aljumah and T. A. Ahanger, “Cyber security threats, challenges and defence mechanisms in cloud computing,” *IET Communications*, vol. 14, no. 7, pp. 1185–1191, Apr. 2020, doi: 10.1049/iet-com.2019.0040.

BIOGRAPHIES OF AUTHORS

Yassen AbdulKhaleq Najm received the BSc degree in statistics and computer science from Al-Rafidain University College, Iraq in 1994. He received the Master degree in computer science from Universiti Teknikal Malaysia Melaka, Malaysia in 2020. Currently, he is a lecturer of Department of English, College of Arts, Al-Iraqia University, Baghdad, Iraq. His research interests include network technology, cloud computing security, and database applications. He can be contacted at email: yasin.abdulkhaliq@aliraqia.edu.iq.

Suray Alsamaraee received the BSc degree in Computer Science from Al Mamoun University College, Iraq- Baghdad in 2006. He received the Master degree in Computer Science from Southern Illinois University, United States of America in 2018. Currently, he is a lecturer of Computer Engineering Department, College of Engineering, Al-Iraqia University, Iraq- Baghdad. His research interests include computer security, network and security, cloud security, and blockchain technology. He can be contacted at email: suray.alsamaraee@aliraqia.edu.iq.

Ahmed Adeeb Jalal received the Engineer degree in Software Engineering from Al-Rafidain University College, Iraq in 2002. He received the Master degree in Computer Engineering from Yildiz Technical University, Turkey in 2016. Currently, he is a lecturer of Computer Engineering Department, College of Engineering, Al-Iraqia University, Iraq. His research interests include data mining, hybrid recommendation systems design, and web applications. He can be contacted at email: ahmedadeeb@aliraqia.edu.iq.