# Security performance In Online Education systems in Saudi Arabia

**Ahmed S. AlGhamdi**

Department of Computer Engineering,
College of Computers and Information Technology,
Taif University, Makkah, Saudi Arabia

**Abstract**
Due to the spread of the COVID-19 virus globally and the transformation of traditional education into virtual education to reduce human contact and maintain social distancing, the Ministry of Education in the Kingdom of Saudi Arabia decided to solve the problem through distance education using a blackboard. For universities, colleges and Madrasati platform for all school categories. This search aims to identify weaknesses in e-learning platforms and discuss possible solutions to avoid them; the focus will be on the problem of unauthorized access.
The percentage change in the percentage increase in the percentage increase in the area. The central issue of e-learning is that students can learn science courses in addition to sharing data. Viewpoint and contact in IS, study destination, international migration and other destination, network and international network. This virtual learning can help students develop new capabilities.
This project explicitly centred around security and protection worries as the significant issues limiting understudy commitment. Due to the spread of the COVID-19 virus globally and the transformation of traditional education into virtual education to reduce human contact and maintain social distancing, the Ministry of Education in the Kingdom of Saudi Arabia decided to solve the problem through distance education using a blackboard. For universities, colleges and Madrasati platform for all school categories. This search aims to identify weaknesses in e-learning platforms and discuss possible solutions to avoid them. The focus will be on the problem of unauthorized access.
The percentage change in the percentage increase in the percentage increase in the area. The central issue of e-learning is that students can learn science courses in addition to sharing data. Viewpoint and contact in IS, study destination, international migration and other destination, network and international network. This virtual learning can help students develop new capabilities. This paper explicitly centred around security and protection worries as the significant issues limiting understudy commitment.

***Keywords:***
*Learning Management System (LMS), Blackboard, Madrasati platform, OTP authentication*

## 1. Introduction

### 1.1 CONTEXT

Blackboard is an online learning executives framework that Blackboard Inc made. It was planned on an instructive basis that assists educators with giving an e-learning condition. It likewise offers an intelligent framework for sparing and recovery of understudy scores, just as test tests contend that Blackboard has numerous focal points, for example, conversation gatherings transferring and sharing documents, dispersing internet getting the hang of, supporting sound, video, and text supporting understudy self-learning and making individual tests for students, either with or without timing. It is likewise portrayed by adaptability in getting to the framework anyplace, and whenever, Blackboard is viable with worldwide guidelines, for example, Sharable Content Object Referent Model (SCORM) and Integrated Management System (IMS) [1].

Security system the primary goal of the security system is to shield the general association from different sorts of safety assaults—the executives' security changes for every field dependent on the centerline that manages the particular field. Furthermore, manages the web and the organization are to secure and guarantee the client wellbeing, data security, worker security from other assaults and shield the complete framework from other Virus assaults like Spam, WORM, Trojans, and Trapdoors [2].

E-learning Platforms Security Most E-learning advancements have zeroed in on-course improvement and conveyance, with almost no thought to protection and security as required components recognizing the reality of the absence of safety perspective on such programming. The jobs of safety in eLearning programming incorporate client assurance of private data from unintended access, confirmation/approval, and security of information honesty [3]. Asserted that security and protection issues in eLearning conditions are expanded, prompting a circumstance where security and security are fundamental for the clients. They express that in a climate like an eLearning suite, the trading of individual data is extreme, so a solid assurance of member's security ought to be a flat out must. In a similar paper, we find that clients (for example, understudies) are profoundly worried about their security, the utilization (and abuse) of their information and the conceivable commandeering [4]. The essential errands for learning administration and substance suppliers are to make sure about learning conditions and to make sure about the capacity of student information. As indicated by the examination, mindfulness raising, insurance of individual information, the validness of learning assets, consistent access, address and area protection, single sign-on,

Manuscript received October 5, 2021
Manuscript revised October 20, 2021
https://doi.org/10.22937/IJCSNS.2021.21.10.20

computerized rights the board [5], enactment and mysterious utilization are immeasurably significant variables of e-learning frameworks use demonstrated that when an understudy "… had moderately higher earlier information (regarding the matter educated in the e-learning condition) the inactive interest had a solid and constructive outcome on e-learning execution… " and "… detached cooperation is decidedly identified with e-learning execution. Therefore, the creators' reason that tactile understudies exhibit a more elevated level of online support. Subsequently, those understudies may not be the most helpless against security defects, yet they are certainly the prime suspects for abusing the information they gained through their cooperation in the e-learning stage [6]. They utilize the "traditional" CIA (Confidentiality, Integrity, and Availability) approach for security, asserting that all different prerequisites can be followed back to those three essential properties. Expanding those with other "hard to fit" classifications, for example, non-disavowal or responsibility is an open conversation today [5], expresses that the six essential security viewpoints (credibility, access control, privacy, trustworthiness, accessibility, non-renouncement) ought to be met for e-learning stages. The creator additionally refers to all the most well-known weaknesses influencing e-learning programming, including SQL infusion (SQL), Cross-Site Scripting (XSS), secret word splitting, seizing and speculating meeting ID [4].

**The double-authorization problem in the LMS:**

An understudy's communications on the web (admittance to assets and learning exercises) make and deal with much individual information that LMS stores on the information base and file system [7]. Therefore, the option to get to furthermore, change this data has touchy ramifications regarding classification and security [8].

The accompanying inquiries should be considered as far as access rights:

Who can get to a specific arrangement of data?

Who can utilize it and why?

Given a client and its part in the stage: which sets of data can get to and what sort of access rights (peruse, compose, read/compose)?

What is more, more inquiries emerge identified with security:

Where is the data put away?

How is the data put away?

Is it scrambled?

How secure is this encryption?

Who has the keys?

The lawful specialists we have counselled highlighted that a cautious understanding of General Data Protection Regulation (GDPR) necessitates that the character of the client and the related consents be approved each time that secret information is gotten to the client's approval status should be checked. However, in the LMS, secret information is gotten from the source code of the LMS constantly. Activities like perusing a class gathering where we can see the cohort's names and pictures and connections to their profile pages and getting to the rundown members or on the other hand the set of experiences tab on a wiki page, all require getting to private data about friend understudies. A client with an educator or teacher will continually get to, adjust, and add private data like grades [9]. In every one of these examples, appropriate use and admittance to confidential data are just ensured by the LMS source code. This implies a vast number of lines of source code. Would we be able to ensure that the code of your LMS of decision checks, what is more, regards the authorizations of each client and job cautiously before getting to classified data?

Off base not. Would we be able to ensure that the code is without bugs? Not one or the other. Furthermore, regardless of whether we could do it at the degree of the product merchant or opensource venture, we need to adapt to all the custom codes that the vast majority of the establishments run on their establishments for reconciliation with the GDPR. To exacerbate the situation, adjusting an LMS's code is moderately simple because a large portion of the programming dialects for web advancement is deciphered, so they are evident and editable from a straightforward content tool [10]. A worker or a programmer assault, particularly in those LMS that sudden spike in demand for deciphered dialects like PHP or Python, can adjust the source code. Any change at the code level can open one more penetrate in the secrecy or, on the other hand, security of individual information and break with the legitimate prerequisites. Along these lines, we are searching for an answer that can withstand bugs in the code and pernicious code alterations [8].

## 1.2 PROBLEM STATEMENT

Security is one of the critical exploration issues in an E-realizing where numerous information bases are associated through the regular entryway and correspondence lines. Moreover, various types of information are put away in various organization fragments in a particular worker. In this examination, the scientist zeroed in on the unapproved access on homogeneously dispersed information bases in the learning the board framework concerning security concerns. These days, versatile LMS applications empowered by disconnected learning (admittance to preparing without the Internet association) are gradually entering the LMS market. For such applications, it is significant that all preparation downloaded by clients on their private or organization provided cell phones be

scrambled to forestall information abuse. In addition, severe verification of student accreditations on the Mobile application is significant as well.

In some educational organizations, students go to computer labs to enter the blackboard portal, do their homework, perform electronic tests, or view the course contents, books, etc. Unfortunately, because of their ignorance, some students save passwords on the lab computers, and another student comes and breaks into another student's privacy.

The lab supervisor should educate students about the importance of keeping passwords.

To solve this problem, a temporary password must be sent to the student's email. The student enters a new temporary number every time he logs into the Blackboard.

## 2. LITERATURE REVIEW

### 2.1 E-Learning Security Threats:

E-Learning security dangers are only the security issues that address the wellbeing of the clients who work with e-learning climate. This segment manages the key security dangers engaged with E-learning [11-13].

**1) Essential E-Learning security concerns:**

Essential security worry of E-Learning innovation, as a rule, emerge when we use it to upgrade the usefulness of the customary learning climate. They are recorded here:

**• User approval and verification:**

The client approval is fundamental and significant with regards to E-learning. Overall, the e-students are far off places, furnished with a client id and a secret phrase. With this utilization, one can log in to the e-learning worker and get to the highlights. The student or the understudy can get to the charging account as indicated by the levels. Given the charging strategy, he might be permitted to the following level of the learning arrangement [2].

**• Entry focuses:**

The section focuses on the number of terminals or aloof ways where a safety break may happen on E-learning. As there are many customers in far off areas for every e-learning worker, there is part of passage focuses for every one of them, and the probability of a security danger is more. To dispose of this danger, the architects need to decrease the number of the section focuses. Nevertheless, it cannot be carried out as several customers in various physical and geological areas simultaneously [14].

**• Dynamic nature:**

One of the significant worries with e-learning is that more cycles are accessible in the powerful meetings where interaction can join and end the meeting without the notification of the others. This is helpless for many security infracts where they can undoubtedly assault the worker and the customer areas. To dispose of these happenings, one ought to keep up exacting meetings, and a few security accreditations must be kept up at both the destinations, i.e., customer and worker [15].

**• Protection against manipulation:**

Assurance against control is one of the vital undertakings to be carried out in an e-learning climate. It is explicitly carried out on account of understudies where control is more conceivable. It very well may be kept from different clients by utilizing specific strategies like computerized marks, firewalls, etc. Comparably, a few different measures must be taken to evade control from the enlisted clients. Hence e-learning climate gets upgraded by following and utilizing the safety efforts cautiously, which will make a smooth construction of the information stream along with the organization [2].

**• Non-Repudiation:**

In the progression of data security, instances of information misfortune or contamination with infection, Trojan pony and other noxious threats are average. Therefore, the framework should be furnished with the capacity to alter the information by these assaults [16].

**2) Social aspects of security:**

Online e-taking in climate is not the same as custom learning climate. The primary change is an accommodation of tasks by understudies to educators. In the conventional learning climate, understudies present their tasks in printed copy configuration to their educators straightforwardly in study halls. While in an online e-learning climate, understudies need to transfer their delicate duplicate of a task. Thus, this technique in e-learning innovation brings the dangers and weaknesses from the web to e-learning frameworks. To conquer these issues, essential security necessities like honesty, secrecy and accessibility are noticed [17]. Those security concerns are explained in detail here:

**• Confidentiality:**

Classification is a significant viewpoint in security concerns, where the information or data sent online is to stay discreet and not to be revealed to an unapproved outsider. However, under the e-learning viewpoint, understudies like to affirm that their submitted delicate duplicates of tasks online are kept mysterious and just uncovered to their educators on e-learning climate [18, 19].

**• Respectability:**

Data or information is not incidentally or vindictively erased or changed, and it ought to be kept precise as in a

unique structure. Understudies feel guaranteed if uprightness guidelines are kept up. This can happen when others remain their tasks submitted to educators carefully in unique configuration with no other version.

**• Availability:**

The reliable data ought to be available to get to and adjust by approved people. Data present in e-learning workers should be available for understudies and instructors or other approved people in a practical way for their work. Understudies need affirmation for a continuous, dependable e-learning framework to present their tasks. There are two principal kinds of accessibility tackles, which make an issue on E-learning frameworks for the accessibility issues [2].

**i. Blocking attack:**

Situation 1 needs to screen the assailants IP address and square that address to dispose of this issue. Generally, in this attack, the external user will attack the e-learning content, obtaining permission to access the E-learning material. Therefore, in this case, one has to monitor the attacker's IP address and block that address to get rid of this problem [20].

**ii. Flooding attack:**

Flooding assault is a tremendous measure of solicitations to a particular help or colossal measure of information as little messages are sent obstructing the whole assistance or the meeting [21]. This may likewise cause the deficiency of accessibility for additional time because of handling delays. The countermeasures for 32 these kinds of assaults are to productively approve the approaching solicitation or the message [2].

**Security in Blackboard**

Security and protection are undoubtedly vital to a framework like Blackboard. However, we distinguish three modules where it is significant that classification, respectability or potentially accessibility are ensured [22].

**• Grade cent**

re

Respectability is likewise significant. At college, there is no direct coupling yet between the evaluations in the evaluation community and the authority grades in the workforce's understudy organization. The average circumstance currently is that instructors present the evaluations to the understudies through Blackboard's grade community. At that point, compose the evaluations physically on a paper list, which is then gone into the staff's organization framework physically by another person [23]. Because of new standards like BSA1, there were plans to accelerate this cycle and do a module to naturally download the evaluations from Blackboard's grade community to the personnel's organization. The trustworthiness of the evaluation community is pivotal in such a situation [16].

**• Online exam:**

It is feasible to utilize the modules for making on the web tests and reviews inside Blackboard. Again, secrecy is significant because the substance of the tests ought not to be known before the tests are taken. Honesty is critical to ensure that there is no debate conceivable about the legitimacy of the put-away replies. If answers can be changed after the test, that is a problematic issue [16].

**• Assignments:**

Numerous educators utilize the tasks module where understudies need to submit schoolwork. These tasks consequently get a timestamp when submitted [24]. Thus, again, trustworthiness is significant, and it should be confident that an accommodation is not changed after it was submitted. In addition, the tasks ought to be secret since it ought not to be feasible for different understudies to duplicate their work [16].

**• Course records:**

For most course records like talk, notes classification is not the primary issue. Nonetheless, uprightness and accessibility are significant. Understudies ought to have the option to believe the substance of archives introduced to them, and precisely, they also ought to have the option to get to them generally [16].

## 3. RESEARCH METHODOLOGY

**• One-Time Password Authentication:**

In e-learning systems, a user name and password are required to log in, which can be easily penetrated. Therefore, the temporary password sent to the email was proposed to log in [25].

When a client account is made in OTP validation conventions, the record is bound by the ownership of some data explicit to the client, for example, a cell phone number or an email address [26]. At login, an OTP is made for the client, who should accurately bring it back [27, 28]. E-adapting frequently uses email OTP verification, where the worker produces a pseudo-arbitrary incentive as an OTP and sends it through email clients. Such a pseudo-irregular worth is shared uniquely between the worker and the client possessing [28, 29].

**• OTP Generation**

The framework depends on a coordinated stream figure that utilizes pictures rather than passwords as the mystery key [30]. A coordinated stream figure is a symmetric critical calculation that produces a pseudo-arbitrary arrangement of pieces, called the keystream, autonomous of the plaintext and code text. These pieces are then joined with the plaintext bits (ordinarily utilizing elite or) to create the code text, and afterwards, we select the initial eight characters

and once more scrambled by ECC technique to created encoded OTP. That will be ship off the client's email ID [31]. The determination of pictures and text fields are irregular so that it will be safer [2].

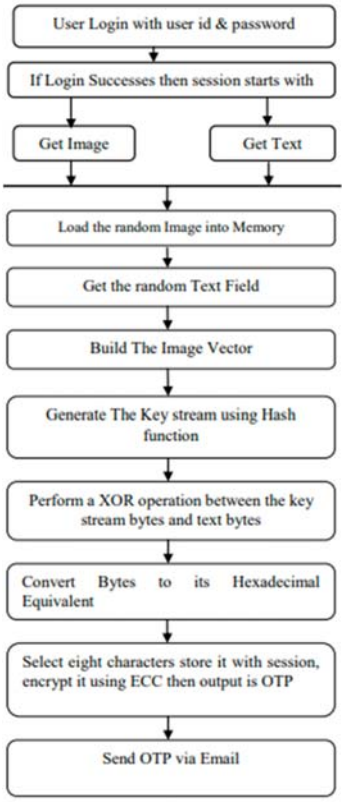


**Fig. 1** OTP Generation [32].

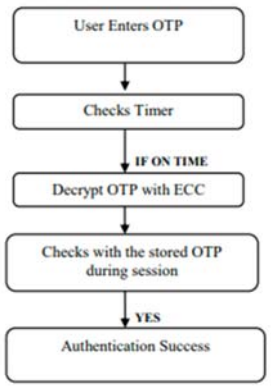


**Fig. 2** OTP Authentication [32].

## 4. PROPOSED SYSTEM:

The Proposed framework depends on the OTP existing framework. In the proposed, the first client needs to produce an essential set, utilizing any open critical cryptography calculation (for example, RSA calculation). In the proposed framework client will demand login with ID and PIN (static secret phrase). On the off chance that it matches with information put away in information-based, the worker creates an arbitrary secret key (OTP) and scrambles it with the put-away client's public key and sends it to the client. The client will unscramble the scrambled one-time secret word (EOTP) and send it to cut off, and if it coordinates with a unique one-time secret phrase (OTP) client is verified. RSA calculation is utilized in the proposed framework as open critical cryptography calculation [33]. In the proposed framework, outsiders such email. The client will produce an essential set utilizing RSA calculation and store the public key into the information base during enrollment of the client's account [34].

1. Customer will demand login with ID and PIN.
2. Worker will confirm ID and PIN, create an OTP, and encode it with the client's public key, which is put away in the information base and send the scrambled OTP to the client.
3. Client will unscramble the encoded OTP with a private key and send the outcome to the worker.
4. Worker will coordinate with it with produced OTP; if it matches, the client is validated. Fig 3. Proposed System Flow Advantages of proposed framework over existing framework are:
1. Proposed framework is autonomous of the outsider (for example, email, GSM mobile number).
2. Proposed framework is profoundly secure, dependent on the critical size.

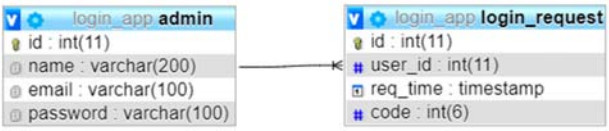


**Fig. 3** ERD for the system.

3. Proposed framework is more effective. Albeit this proposed framework is intended for cloud verification yet additionally it very well may be utilized in other regions which are depicted howl:
1. All the long-range informal communication locales: The proposed framework will give a safer confirmation framework contrasted with existing frameworks utilized by interpersonal interaction destinations.
2. All the electronic-trade destinations: The proposed framework will give a safer verification framework contrasted with existing frameworks utilized by electronic business locales.
3. In the e-banking areas, likewise proposed framework is precious [34].

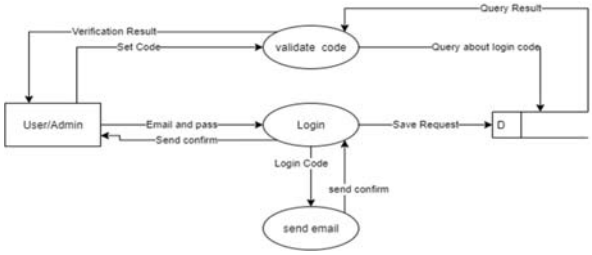


**Fig. 3** DFD

## 5. CONCLUSION

Lately, some specialist co-ops associations in the schooling area have been found in the act utilizing individual data of understudies and metadata for ridiculous business reasons. This has added to raising concerns and doubt about administering individual data in the Learning Management System (LMS). This is particularly important in Learning Analytics (LA) since it includes gathering, putting away, and investigating understudy individual information and metadata of their conduct. This reasonable circumstance of doubt in the utilization of individual information can be tended to by a) actualizing legitimate guidelines, for example, GDPR and moral codes into the business measures b) and a sound mechanical execution to help it. Therefore, we propose a consolidated activity with the goal that the innovative methodology robotizes the business rules to guarantee consistency with lawfulness and concurrences with clients and the moral code.

This project has a productive and secure one-time secret word confirmation. The proposed conspire is secure against disguise assaults, pre-play assaults, the worker's mocking assaults, dynamic and disclosure of message substance assaults, off-line dictionary attacks, stolen-verifier attacks, and replay attacks [35].

## 5. FUTURE WORKS

E-learning apparatuses make it imperative to guarantee that the apparatuses are secure. No last "score" can be appointed to every stage tried, nor it can be structured a table with the stages tried in a climbing request dependent on such rules since there is no generally acknowledged instrument or strategy accessible today that doles out a particular weakness to a "seriousness" scoring number. If such an apparatus existed, we could summarize the scores of every one of the weaknesses found for a particular stage and think of the last score for each one. This would prompt a scientific classification that could be shorted. Future examination courses could be the precise assessment and scientific categorization of weakness scanners concurring to definite guidelines and rules. This will help all partners converse with a pretty much "regular language", clearly understanding security associations. For example, OWASP is unmistakably expressed that e-learning extraordinarily improved the scholarly execution and fruitful consummation of courses among scholastically more grounded understudies. It would be fascinating for a devoted specialist to research the connection between the abovementioned contention and the security issues of the different e-learning stages.

## References

[1] R. Almoeather, "Effectiveness of blackboard and Edmodo in self-regulated learning and educational satisfaction," *Turkish Online Journal of Distance Education,* vol. 21, no. 2, pp. 126-140, 2020.

[2] G. Kumar and A. Chelikani, *Analysis of security issues in cloud-based e-learning*. University of Borås/School of Business and IT, 2011.

[3] K. El-Khatib, L. Korba, Y. Xu, and G. Yee, "Privacy and security in e-learning," *International Journal of Distance Education Technologies (IJDET),* vol. 1, no. 4, pp. 1-19, 2003.

[4] M. Bhatia and J. Maitra, "E-learning Platforms Security Issues and Vulnerability Analysis," in *2018 International Conference on Computational and Characterization Techniques in Engineering & Sciences (CCTES)*, 2018, pp. 276-285: IEEE.

[5] C. Virmani, T. Choudhary, A. Pillai, and M. Rani, "Applications of machine learning in cyber security," in *Handbook of research on machine and deep learning applications for cyber security*: IGI Global, 2020, pp. 83-103.

[6] A. Barth, C. Jackson, and J. C. Mitchell, "Robust defences for cross-site request forgery," in *Proceedings of the 15th ACM conference on Computer and communications security*, 2008, pp. 75-88.

[7] P. Modesti, "Integrating Formal Methods for Security in Software Security Education," *Informatics in Education-An International Journal,* vol. 19, no. 3, pp. 425-454, 2020.

[8] D. Amo-Filvà, M. Alier Forment, F. J. García Peñalvo, D. Fonseca Escudero, and M. J. Casany, "GDPR Security and Confidentiality compliance in LMS'a problem analysis and engineering solution proposal," 2019.

[9] M. Boban, "Digital single market and EU data protection reform with regard to the processing of personal data as the challenge of the modern world," *Economic and social development: book of proceedings,* p. 191, 2016.

[10] F. Boninger, A. Molnar, and K. Murray, "Asleep at the Switch: Schoolhouse Commercialism, Student Privacy, and the Failure of Policymaking--The Nineteenth Annual Report on Schoolhouse Commercializing Trends, 2017," *National Education Policy Center,* 2017.

[11] T. McMillion and C. S. Tucker King, "Communication and security issues in online education: Student self-disclosure in course introductions," 2017.

[12] W. Nie, X. Xiao, Z. Wu, Y. Wu, F. Shen, and X. Luo, "The research of information security for the education cloud platform based on AppScan technology," in *2018 5th IEEE International Conference on Cyber Security*

*and Cloud Computing (CSCloud)/2018 4th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom)*, 2018, pp. 185-189: IEEE.

[13] E. Baran, "A review of research on mobile learning in teacher education," *Journal of Educational Technology & Society,* vol. 17, no. 4, pp. 17-32, 2014.

[14] A. Al-Drees, M. S. Khalil, S. A. Meo, and H. M. Abdulghani, "Utilization of blackboard among undergraduate medical students: Where we are from the reality?," *Journal of Taibah University Medical Sciences,* vol. 10, no. 1, pp. 16-20, 2015.

[15] M. Pollán *et al.*, "Prevalence of SARS-CoV-2 in Spain (ENE-COVID): a nationwide, population-based seroepidemiological study," *The Lancet,* vol. 396, no. 10250, pp. 535-544, 2020.

[16] M. van Eekelen, R. B. Moussa, E. Hubbers, and R. Verdult, "Blackboard Security Assessment," 2013.

[17] A. eM Elsawy and O. Ahmed, "E-Learning using the Blackboard system in Light of the Quality of Education and Cyber security," *International Journal of Current Engineering and Technology,* vol. 9, no. 1, 2019.

[18] Y. Imai, S. Hara, S. Doi, K. Kagawa, K. Ando, and T. Hattori, "Application and Evaluation of Visual CPU Simulator to Support Information Security Education," *IEEJ Transactions on Electronics, Information and Systems,* vol. 138, no. 9, pp. 1116-1122, 2018.

[19] C. Pérez-Sola, A. Ranchal-Pedrosa, J. Herrera-Joancomartí, G. Navarro-Arribas, and J. Garcia-Alfaro, "Lockdown: Balance availability attack against lightning network channels," in *International Conference on Financial Cryptography and Data Security*, 2020, pp. 245-263: Springer.

[20] P. Shrivastava, M. S. Jamal, and K. Kataoka, "EvilScout: Detection and mitigation of evil twin attack in SDN enabled WiFi," *IEEE Transactions on Network and Service Management,* vol. 17, no. 1, pp. 89-102, 2020.

[21] J. Dong, K. Wang, W. Quan, and H. Yin, "InterestFence: Simple but efficient way to counter interest flooding attack," *Computers & Security,* vol. 88, p. 101628, 2020.

[22] M. D. Ciampa, "Security+ guide to network security fundamentals/Mark Ciampa," ed: Boston, MA: Course Technology, Cengage Learning, 2012.

[23] B. A. Jacob and J. E. Rockoff, *Organizing Schools to improve student achievement: Start times, grade configurations, and teacher assignments*. Brookings Institution, Hamilton Project Washington, DC, 2011.

[24] Y. S. Lee, H. Lim, and H. Lee, "A study on efficient OTP generation using stream cipher with random digit," in *2010 the 12th international conference on advanced communication technology (ICACT)*, 2010, vol. 2, pp. 1670-1675: IEEE.

[25] C.-H. Ling, C.-C. Lee, C. C. Yang, and M.-S. Hwang, "A Secure and Efficient One-time Password Authentication Scheme for WSN," *Int. J. Netw. Secure.,* vol. 19, no. 2, pp. 177-181, 2017.

[26] P. Crocker and P. Querido, "Two factor encryption in cloud storage providers using hardware tokens," in *2015 IEEE Globecom Workshops (GC Wkshps)*, 2015, pp. 1-6: IEEE.

[27] A. Singer, R. S. Canon, R. Hartman-Baker, K. Rowland, D. Skinner, and C. Lant, *What Deploying MFA Taught Us About Changing Infrastructure*. eScholarship, University of California, 2020.

[28] S. Ma *et al.*, "An empirical study of SMS one-time password authentication in android apps," in *Proceedings of the 35th Annual Computer Security Applications Conference*, 2019, pp. 339-354.

[29] M. H. Eldefrawy, K. Alghathbar, and M. K. Khan, "OTP-based two-factor authentication using mobile phones," in *2011 eighth international conference on information technology: new generations*, 2011, pp. 327-331: IEEE.

[30] H. S. Seo and T. H. Cho, "An application of blackboard architecture for the coordination among the security systems," *Simulation Modelling Practice and Theory,* vol. 11, no. 3-4, pp. 269-284, 2003.

[31] Y. Atwady and M. Hammoudeh, "A survey on authentication techniques for the internet of things," in *Proceedings of the International Conference on Future Networks and Distributed Systems*, 2017.

[32] N. Vishwakarma and K. Gangrade, "Secure image-based one time password," *Int. J. Sci. Res. (IJSR),* vol. 5, no. 11, pp. 680-683, 2016.

[33] J. L. Ortega-Arjona and E. B. Fernandez, "The secure blackboard pattern," in *Proceedings of the 15th Conference on Pattern Languages of Programs*, 2008, pp. 1-5.

[34] K. S. Hlaing and N. A. Aung, "Secure One Time Password OTP Generation for user Authentication in Cloud Environment," *Int. J. Trend Sci. Res. Dev.,* vol. 3, no. 6, pp. 89-92, 2019.

[35] C.-C. Lee, C.-T. Li, and S.-D. Chen, "Two attacks on a two-factor user authentication in wireless sensor networks," *Parallel Processing Letters,* vol. 21, no. 01, pp. 21-26, 2011.

**Ahmed S. AlGhamdi** was born in Jeddah, Saudi Arabia, in 1975. He received the B.E. degree in electronic engineering from the technical college, Riyadh, Saudi Arabia, in 1997, and the Master degree and Ph.D. degrees in computer and electrical engineering from the Curtin University Perth, Western Australia, Australia, in 2008 and 2014, respectively.

In 1998, he joined the Department of instrumentation, at KEMYA Company. Since September 1990, he has been with the Department of Computer Engineering, faculty of Computer Information Technology, Taif University, where he was an Assistant Professor. His current research interests include Fuzzy logic, transportation system, communication, 3D printing.