A Common Framework Based on Multi-Factor Authentication to Secure Students Log in to Educational Digital Platforms

By

Dr. Elsaeed. E. Mohamed Abd Elrazek

&

Esraa.M.Ramadan

Department of Computer Teacher Preparation, Faculty of Specific Education

Damietta University, Egypt

Educational Technology & Digital Learning

DOI :10.21608/jetdl.2022.136241.1027

Volume 3, Issue 6, February 2022

ISSN-Print: 2785-9754 ISSN-Online: 2785-9762

Egyptian Knowledge Bank:
https://jetdl.journals.ekb.eg/

A Common Framework Based on Multi-Factor Authentication to Secure Students Log in to Educational Digital Platforms

Elsaeed. E. Mohamed Abd Elrazek[1]&Esraa M.Ramadan[2]
[1]Faculty of Specific Education,Damietta University,Egypt
[2]Faculty of Specific Education,Damietta University,Egypt
elsaeed2004@hotmail.com
esraaramadan16102017@gmail.com

Abstract

Recently, and after the spread of the COVID-19 pandemic, the importance of using educational digital platforms to expand the employment of distance education in order to achieve safety for members of the human system in education, and on the other hand, provide modern learning environments using interactive technologies to enable the student and teacher to access to learning resources in any time and from anywhere, which achieves the targeted learning outcomes in no time and with the least effort. The current research aims to deal with educational digital platforms and increase their effectiveness and procedures for securing their uses and dealing with their resources through the use of the modern technology called multi-factor authentication in order to control the access to the resources of these platforms so that the user will have the right to access to the resources of these platforms and deal with them by going through stages It requires providing several independent evidences from each other that includes at least two of the following categories: knowledge, possession, and biometric features.

Security within digital platforms and data protection is a source of great concern to users, and this can be achieved by integrating more than one security factor to log into these platforms and increase security in them. Therefore, there is a need to develop a mechanism to enhance the use of multi-factor authentication within educational digital platforms to reduce security threats , ensure confidentiality and the safety of user data within those platforms.

Key words

Educational digital platforms, multi-factor authentication, biometrics, fingerprint scanning

1. Introduction

Digital transformation has become an inevitable necessity for the development of a society based on the knowledge economy. This transformation has had a great impact on the sectors of society in general and the education sector in particular ; to shorten time, reduce costs and achieve more flexibility and efficiency.

Recently, the outbreak of the Corona virus, COVID-19, quickly escalated into a global pandemic because of its ability to spread rapidly among humans around the world. Schools and universities were closed, which led to the shift towards virtual communities and the use of educational digital platforms to implement policies of isolation and social distance to continue the educational process. Students and university professors were able to Communicate with each other.[1,2]

Educational digital platforms are one of the e-learning tools compatible with the requirements of the digital age, as they represent learning resources to achieve an interactive learning environment; university education has used educational digital platforms for distance learning in light of the Corona pandemic, developing education systems, benefiting from global experiences in their application, and training professors and students on their use, so that faculty members will be able to publish lectures, set assignments, divide students into groups, exchange ideas, share content, and communicate With learners through multi techniques [3].

One of the most famous digital educational platforms is the Microsoft Team, Zoom, coursera, Webex, edx, Google Classroom platform, where there is an agreement in dealing between Microsoft Team and digital learning platforms, and a global study by Microsoft revealed that there is a continuous increase in the employment of digital tools for distance

education in all around the world, as well as new ways that will contribute to reshaping the the coming school year.

The results revealed that 61% of the participants in the study expect that the school year will be in a learning environment characterized by a combination of distance education and self-education approaches, while 87% expect to use modern technologies more than the previous period.

On of the advantages of educational digital platforms is flexibility and the use of different ways to convey information, saving time, effort and cost, making content available and sharing it, interaction between students and teachers and between students and each other and ease of access to information at any time and from anywhere.

Logging in to these platforms to deal with their resources depends mainly on traditional authentication (one-factor authentication) which is based on the user name and password, the identification number or the address of the teacher and the student which can hack servers, steal password files of users, access to their accounts, ease data loss, and ease security breach when passwords or PIN numbers who are unauthorized users, which weakens the security level of those platforms, increases security threats, and lowers the level of confidentiality, integrity and security of users' data.[6]

And since the security and privacy of data represents the greatest interest among users of educational digital platforms, from teachers, learners, and providers of those services alike, the need to apply advanced techniques to raise the degree of data security in educational digital platforms by using more than one method, factor or several factors (word Password ,User Name, Fingerprint, Facial Recognition, Voice Recognition, Eyesight Recognition) to verify the identity of the user before giving them permission to access to the data on educational digital platforms, as it is assumed that the more layers of protection, the less the threat of data breach these factors or layers are called MFA-Multi-factor Authentication [4].

The level of security within educational digital platforms is intended to prevent unauthorized persons from entering these platforms and achieve

this by dealing with several levels of security to verify the identity of the user and to verify the login process and to restrict the access of persons who are not permitted to penetrate those platforms by adding additional layers of security called Multi-factor authentication (MFA), which requires knowledge factor (data that the user knows), possession factor (a device owned by the user), and inheritance factor (physical and biometric attributes of the user) in order to fill gaps in traditional authentication techniques and raise the degree of privacy, and improve security and protection for educational digital platforms [4].

The knowledge factor represents the minimum level to protect user data using the password, which is still widely used and depends on the user's memory, as the user must remember a password consisting of 16 characters or characters (and change it every three months), and in the event of losing it, the system offers the user some The questions that must be known to be answered accurately in order to retrieve the password, and the user often faces the problem of forgetting to answer those questions. [6] Therefore, there was a need to achieve better data protection that does not depend on the user's memory, and from here a second factor appeared away from human memory related to the user possesses a mobile device through which a security code is received and sent to the user, but with the rapid technological development, hackers have been able to penetrate the security code that is sent to users on their mobile devices, which required the discovery of a third factor to protect their data that depends on the user's physical characteristics or biological factors that can be Scan it digitally such as eye gaze, voice print, handprint, facial features.[7]

There are many types of authentication systems, the most important of which are the following:[31]

-A two-factor authentication system: It combines only two authentication factors, one of which is the username and password factor (which alone is not a multi-factor authentication system).

-Multi-factor authentication system: combines more than two authentication factors together with the username and password factor

It should be noted that all authentication factors have their own challenges that can be overcome, and the required and appropriate authentication for the user must be determined according to the degree of importance of the data to be protected. The more secured the data is, the higher risk and the stronger the validation of the transaction is.

And that requires strong multi-factor authentication.

User authentication plays a crucial role in ensuring access to resources and services can only be accessed by authorized persons, so authentication is a secured, efficient, and important encryption tool for both wired and wireless networks.

Therefore, the current research aims to design a proposed system to secure access to educational digital platforms using multi-factor authentication.

RESEARCH AIMS

The research seeks to achieve the following main objectives:

1- Learning about digital platforms and using them in education

2- Understanding the concept of multi-factor authentication to achieve data security

3- Determining the requirements for employing educational digital platforms

4-Designing a proposed system for multi-factor authentication to secure students ' login to educational digital platforms

5- Measuring students' attitudes towards the proposed system of multi-factor authentication within educational digital platforms

RESEARCH QUESTIONS

The research seeks to answer the following main question: What are the stages of developing a proposed authentication system to determine the appropriate level of security to log students into educational digital platforms?

The following sub-questions emerge from the main question:

1- What is the importance of using digital platforms in education?

2- What are the requirements for employing digital platforms in education?

3- What are the stages of developing a proposed authentication system to determine the appropriate level of security for students to log into educational digital platforms?

4- What are the students' attitudes towards the proposed authentication system for accessing educational digital platforms?

2. RESEARCH METHODOLOGY

The study depends on:

1- The analytical descriptive approach for its relevance to the nature and topic of the research to identify the concept of multi-factor authentication, as well as identifying the most important security threats faced by the educational digital platforms associated with it , through the exploratory study, the current methods and methods in identifying the identity of the user and to identify the importance of using digital platforms in education, and to determine the most commonly used authentication methods preferred by users of educational digital platforms, and to identify the users' tendency towards using the proposed authentication system.

2- The semi-experimental approach: to design the proposed authentication system to secure student login to educational digital platforms, which includes several factors to verify the identity of the user (knowledge factor - possession factor - biometric features), and measure the students' tendency towards using the proposed authentication system.

THE RESEARCH SAMPLE

The data was collected through the community of students of the third and fourth year (175 students) of the Computer Teacher Preparation Division at the Faculty of Specific Education, Damietta University, users of the Microsoft teams platform, and the Zoom platform for the academic year 2019/2020 in the second semester.

THE STATISTICAL METHODS USED

The SPSS program was used for statistical analysis of the data, calculating frequencies, percentage, Q^2, significance level and Facronbach equation.

SEARCH TOOLS

To achieve the research objectives, the researchers prepared the following:

1- A questionnaire form for students to identify the importance of using digital platforms and the requirements for their employment in education

2- An attitude scale for students to measure their attitudes towards using the proposed authentication system based on the combination of tenure and biometric factors as additional security layers for the authentication process every time they want to log into educational digital platforms.

The research tools have been sent to the students' university emails, as the research was applied online during the period of the Corona pandemic during the second semester of the academic year 2019/2020.

Steps for preparing research tools (questionnaire - trend scale)

The researchers determined the questionnaire terms and the attitude scale phrases after reviewing studies related to the subject of the research and compiling the theoretical framework, and to judge the research tools, they were presented to a number of specialists in the faculties of Damietta and Mansoura University, and their number was (10) arbitrators to arbitrate the research tools in terms of clarity of phrases and their connection to content and their suitability In terms of wording, and the search tools phrases were modified by deleting some phrases whose degree of agreement was less than 90%. Thus, the number of questionnaire phrases became (11) phrases, and the number of attitude scale phrases (23) were phrases presented under two axes: the first axis was the options of the validation factors, and the second axis Using the proposed validation system, and to determine the weights of the questionnaire items and the trend scale items, the researchers set a three-point scale for the responses for each statement (strongly agree - somewhat agree - disagree) so that 3 degrees are given to the response strongly agree, two degrees to the

response to some extent, and one degree to the response no I agree, and the Facronbach equation was used to ascertain the internal consistency of the questionnaire items and the trend scale and to calculate the reliability coefficient as its value for the questionnaire was 0.85, and its value for the trend scale was 0.89 b Based on these values, the stability level is considered appropriate for both the questionnaire and the trend scale

3. Theoretical framework

The theoretical framework includes two main axes: educational digital platforms, and multi-factor authentication

The first axis: Educational Digital platforms

Educational digital platforms have become an inevitable necessity in recent times for the continuation of the educational process and the achievement of its goals, especially in light of the spread of the Corona pandemic, and digital platforms represent educational sites through which modern technological technologies are used, as they are considered an educational environment through which a set of experiences and interactive services are provided via the Internet, The provision of courses electronically, class management, and student assessment, as well as allowing the exchange of ideas and the sharing of educational contents between faculty members and students, and between students each other.[8]

Digital platforms are also known as an interactive learning environment that employs web technology and combines the advantages of electronic content management systems and social networks and enables teachers to publish lessons and goals, set assignments, implement educational activities, and communicate with teachers through multi technologies, dividing students into working groups, which help to exchange ideas and opinions between teachers and students, and to share scientific content which helps achieve high quality educational outcomes.[16]

There are tools that can be used within educational digital platforms, including synchronous tools (conversation - interactive whiteboard - forum - video conferencing) and asynchronous ones (e-mail).

Digital platforms are used within the educational process to create virtual classrooms and facilitate the access to information for the student and to learn at home, especially in light of the COVID-19 pandemic, and their use is increasing because they support synchronous and asynchronous communication, the most popular of which is (Google classroom - Zoom - Microsoft teams) and every educational digital platform It has various aspects that can support learning objectives, promote cooperation, interaction, interest and motivation of students and their sense of belonging, student-student and student - teacher interaction, peer support and feedback [9,19]

Among the most widely used digital platforms are:

- Zoom platform

It is a free platform that is widely used after the spread of the Corona pandemic COVID-19, as it has more than 200 million daily users, and it is one of the most preferred video conferencing platforms for its ease of use and its ability to support 100 participants and allow 49 videos on the screen, and the ZOOM platform also features sharing and recording screen, chats, search by date, it also allows adding custom wallpapers to meetings and video conferences, in addition to the ability to save videos and files that are shared and restored by the user [10]

The ZOOM platform has security and privacy issues and issues where many unwanted participants can join a meeting and breach the privacy and negatively affect its security level

-Microsoft Teams platform

It is a platform that combines video meetings, chats, file storage, and application integration. The number of users of that platform reached 44 million daily users on March 19, 2021 due to the spread of COVID-19. One of its advantages is that the student can join the platform via the teacher's URL, and it also allows members of The faculty prepares interactive educational channels that help in communication. It also allows the use of images and videos, publishing links, holding meetings and scheduling them through the lecturer, assisting the faculty member in distributing students in class, providing notes and monitoring the

student's progress during the study, preparing opinion survey forms, preparing the exams.[12]

-Cisco WebEx platform

It is a video conferencing platform developed by Cisco that provides video support for up to 200 users of applications such as One Drive, Google Cloud and is also associated with Microsoft Office365, Microsoft Exchange, Google cloud, which is an easy to handle platform and the ability to call back and access the lecture easily, And file sharing of all kinds, it also supports chatting, creating a group defined by teachers, monitoring students with their assignments, and creating virtual classes [13]

-Go To Meeting platform

It is a web-based platform used for meetings, lectures, and video conferencing that allows audio meetings to be recorded and converted into texts.

-Google Classroom platform

A free platform from Google that allows sharing of files and videos between teachers and students, and uses Google applications for various purposes, for example, Google Drive is used to create and distribute tasks and publish Google Docs, Slides for writing, Gmail for Research and Google Calendar to make a timetable Student can join a class using a special code and create separate folders To upload files of different categories for easy access and help in giving assignments to students by teachers, and Google Classroom allows a two-way communication[14]

Several studies have shown the impact of integrating educational digital platforms into the educational process because of their positive and effective impact in raising the level of effectiveness of the educational process in universities, and these studies include: study (2014, Benta et al), study (2014, Almarabeh et al). Building the students' personality and self-reliance helps in obtaining this information, in addition to developing a love for cooperative teamwork. [21,22]

The study of Herbrot, Jackime and Patricia (2017) aimed to describe the methods and strategies used by teachers, which were implemented

through educational digital platforms, where the study sample consisted of 35 teachers, and observation and interview tools were used. There are different strategies that teachers use through educational digital platforms such as face-to-face classroom support.[20]

There are many advantages to using digital platforms in education, the most important of which are increasing students' motivation towards learning, acquiring self-learning skills, increasing opportunities for cooperative learning, enhancing communication, exchanging information and educational platforms enable faculty members to conduct electronic tests, and allow parents to communicate with faculty members. and see the results of their children which helps to achieve high quality educational outcomes, facilitates the role of the faculty member during the educational process, increases its efficiency, improves the level and quality of learning, increases interaction between students and the subject, and between students and faculty members, and break through temporal and spatial barriers and trust in the source. The information is correct because it is provided by experienced professors and correct scientific knowledge, digital platforms also allow to easily evaluate students' work and send home assignments with the possibility of a faculty member communicating with his students in all groups and also communicating with colleagues, exchanging ideas, improving learning and shifting towards the method of research and exploration instead of presentation and lecturing by members of the teaching staff.[13,16]

He mentions ([23,24]) other advantages of educational digital platforms, which are: involving students in the academic content, which helps to create a safe psychological atmosphere and encourage permanent research, the possibility of downloading digital platforms on smartphones and tablets, updating teaching methods to achieve increased interaction between students and the subject, lower costs compared to traditional education, deepening understanding of the educational material, increasing students' motivation towards learning., applying the cooperative learning strategy, taking into account individual differences among students, and improving the level and quality of learning.

Despite the advantages of using digital platforms in education, there are some limitations that limit the effectiveness of its employment, the most important of which are [25,26]: Weak infrastructure in terms of devices and networks necessary to accommodate technological changes with rapid and continuous development, lack of Internet in some areas, The interruption of the Internet connection, which constitutes an obstacle to the communication and interaction of professors and students, the loss of the social aspect of learning, the weakness of direct interaction with the teacher and the absence of his real role, the increase in the tasks required of those in charge of the educational process and the intensity of the courses, the incompatibility of the curriculum with the use of technology tools, the exposure of information to internet piracy , its misuse, the increase in the number of hours students spend in front of computers, which leads to social and psychological isolation, and it is also misused on digital platforms that it still depends on unilateral authentication that depends on the user name and password or on the identification number or address of the teacher (the lecturer) to achieve interaction among the components of the educational process.

The second axis: authentication (concept - patterns)

Authentication is a mandatory process used to verify the identity of the user and prevent unauthorized persons from accessing the system, where the user enters an identifier (username) to log into a system or network in which the username is the unique identity of the person to that system.[5]

When creating an account on the internet, this requires adding a layer to protect and secure the user's personal information based on the username and password, and this process is called a two-factor authentication to prevent hackers from obtaining more personal information

There are two types of a two-factor authentication:[11]

One-Time Password: OTP- One Time Password codes sent via SMS to the mobile phone number associated with accounts are the most common form of a two-factor authentication, often used by social media platforms, and vilified this type that it’s not the most secured form of a two-factor

authentication, as hackers can trick the system and trick carriers into diverting a user's phone messages to their own number.

Time-based One-time Password TOTP: This form of a two-factor authentication is more secured than a one-time password (OTP) as the code is generated on the user's mobile phone number rather than being sent to them via SMS and requires the user to download an application such as-Google Authenticator-Microsoft Authenticator-1Password-

With the increasing use of mobile devices, hackers were able to enter different forms of usernames, guess passwords, and perform data breaches, which required attention to add more layers of protection to confirm the identity of the user and secure his personal data, and the emergence of the so-called multi-factor authentication

Multi-factor authentication is defined as a secured system that requires more than one form of transaction validation, which is called independent credentials, and is represented by three independent factors: the knowledge factor, which is what the user knows (the password), and the possession factor, which is what the user has (the token Security), and the heredity factor, i.e. what is the user (biometric verification) with the aim of verifying the identity of the user in accessing the electronic system and information, where multi-factor authentication combines two or more factors to provide a better and secured way to authenticate user data [4] MFA Multi-Factor Authentication also aims to provide a higher degree of assurance of the identity of the user trying to access a specific resource (site - cloud computing - network - database) where the multi-factor authentication method is based on several layers that the user must pass through and pass it in order to reach the required resource.

The current research defines multi-factor authentication as a method of controlling access to information technology resources on the internet, where the user is not granted the right to access and deal with those resources except after providing several separate evidence called verification mechanisms that include at least two of the following categories: Knowledge (something the user knows), possession

(something the user owns), and biometrics (an adjective that is closely related to the user).

There are three factors used to create a digital identity for multi factor authentication, which are [15]:

1- The knowledge factor, which is something the user knows, such as: (password - answering challenge questions or secret questions - identity numbers - personal identification number)

2- Ownership factor, which is something that the user owns, such as: (mobile phone - personal computer)

3- Biometric factor, which represents a part of the user, such as a fingerprint, eye examination, or voice pattern

Biometrics refers to measures related to human characteristics. Biometric authentication is used in computer science as a form of identification and access control and is also used to identify users in closed groups. Biometrics includes the means of automatically identifying people on the basis of the morphological, physiological and anatomical characteristics of each person, the most important of which are fingerprints, facial features, voice, or the iris of the eye because these organs are unique in each person, and biometrics is the most common form Distinguished from a two-factor authentication, biometrics are processed through programming and encryption for the unique features of each person and stored in the database to match them with the features and characteristics of the persons to be verified, and more than one means can be used to identify the identity of the person[17]

The physiological characteristics are as follows:

Fingerprints: The fine lines called Minutiae on the surface of a human finger are used to identify the user.

Face Recognition: Facial features are analyzed for authentication and to identify the user's identity. Most facial recognition systems use either Eigen faces or Local Feature Analysis.

Eyes - Iris Recognition: The features of the iris are used to identify the user.

Eyes - Retina Recognition: The patterns of veins in the back of the eye are used to achieve this examination.

Whereas, the behavioral characteristics are both voice recognition and signature recognition.

The results of the study by Veerendra and Prasad (2017), Soni, P., & Sahoo, M. (2015), Panse, D., & Haritha, P. (2014, August) showed that there are security challenges in data storage on the Internet. The Internet and the need to develop authentication systems that give the user a higher level of protection and privacy for their data, and to choose encryption algorithms that depend on more than one authentication factor that is more applicable, and to ensure that data breaches do not include knowledge factors, ensuring that the current user is the person authorized to deal with that data.[7,27,28]

Panse, D., & Haritha, P. (2014, August) study also emphasized that the main challenge that must be addressed on the internet is to achieve security and the need to integrate multi factors of authentication to secure cloud data as the traditional methods of securing data which are used extensively. Single in authentication has shortcomings and loopholes for attacks on those sites, which leads to undesirable people accessing the system and accessing user data.[7]

The study also targeted Naveed, G., Rakhsh, & Batool, a. (2015) disclosed the different biometric authentication factors that can be used in cloud computing authentication and their advantages and disadvantages and recommended that the biometric features of the user should be widely used because they are easy to use and generally accepted in a large part of the world to achieve high accuracy of authorization in dealing with sites with an error rate Too low.[29]

Choudhari, E., & Bodhe, KD (2017) study also confirmed that the biometric factor is the safest and most suitable for proving the identity of the user and to overcome the weakness points of other factors. It also recommended the combination of two or more factors to achieve reliable authentication and the use of biometric methods for the user. Such as thumb scanning as an authentication tool for cloud services as an

alternative to traditional username and passwords that are exposed to security attacks through the various hacking methods available [30]

Proposed System

The design of the proposed system in this research included the use of multi factors of authentication for users of educational digital platforms, and those factors were as follows: knowledge factor (username and password), possession factor (OTP security token), genetics factor, physical characteristics or biometrics (fingerprints). fingers,)

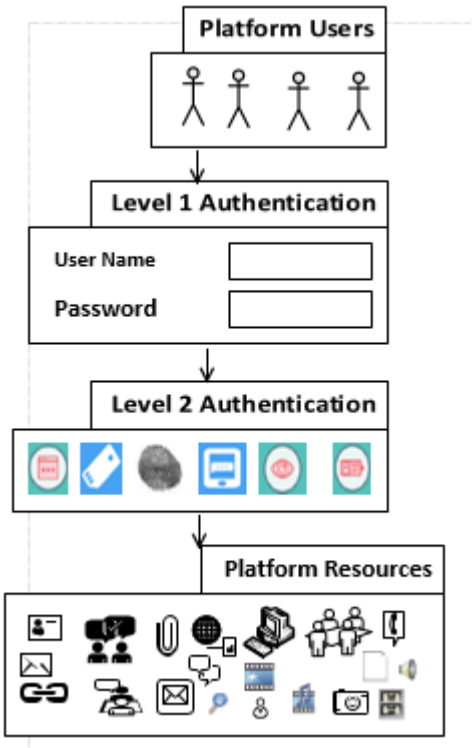


Fig (1) shows the general conceptual diagram of the proposed system

4. 1 Proposed authentication system for educational digital platforms

A proposed authentication system based on several levels has been developed to determine the appropriate level of security and guarantee for entering the educational digital platforms and benefiting from their resources. The proposed system includes the user name, password and fingerprint to control access to the educational digital platform resources.

4. Design and development of the proposed system

The proposed authentication system for educational digital platforms is designed using the waterfall model according to the following stages:

The first stage: determining what is required

At that stage, the main objective of developing the proposed authentication system for educational digital platforms was determined, which answers the question: What will the proposed system do? This goal was to secure entry to educational digital platforms using multi-factor authentication by dealing with several levels of security to verify the identity of the user and to audit the login process and prevent the access of persons who are not allowed to penetrate these platforms by adding additional layers of security called multi-factor authentication

The second stage: designing the proposed authentication system

It means designing the user data model and how it will be entered through the levels of the proposed authentication system for educational digital platforms, as well as designing the levels of the proposed system separately and understanding how to deal and move between those levels.

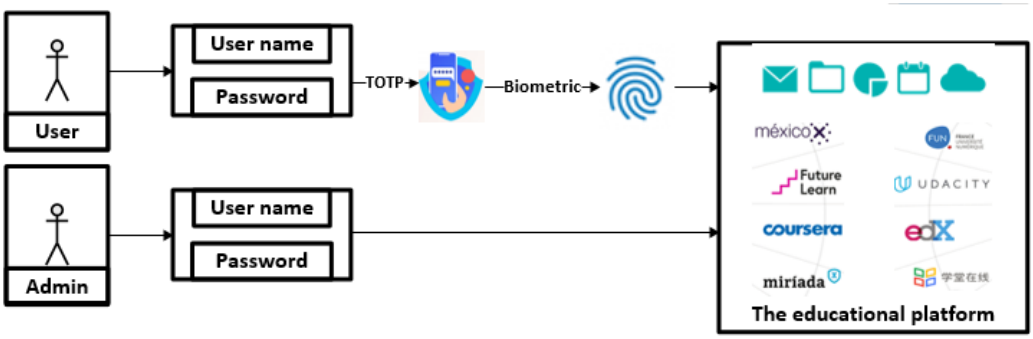


Fig (2) shows the levels of the proposed authentication system

In addition to defining the units of the proposed authentication system for educational digital platforms, which are as follows:

1- Registration module for the proposed authentication system

Where knowledge factors, possession factors and biometric characteristics were recorded and stored in the database whereas:

Registration of knowledge factors (usernames - passwords): where the user is required to enter credentials such as first name, second name, user name, password and email address

Fig(3) showing user data registration (knowledge factor)

Recording the tenure factors (security code) either as an OTP- One Time Password which is sent via SMS to the mobile phone number associated with the accounts, or a TOTP- Time-based One-time Password where the generating the code on the user's mobile phone number instead of sending it to him via SMS where a temporary passcode is verified by an algorithm linked to the current time and sent through the mail or phone number to verify the time-related code and the temporary passcode expires after 30 or 60 or 120 seconds

- Biometric feature registration: storing fingerprints of users and storing them in the database

It requires authentication to register the fingerprint from the connected devices, to extract the fingerprint and store it in the database.

2- Authentication Module

Once the registration success for all authentication factors is verified, the user is redirected to the login prompt where three steps are again done.

-Step 1: Verify the username and password registered on the login page and verified in the user database stored on it for matching, and if it is correct, access and login will be successful and the user is directed to the login page with the one owned by the OTP.

-Step 2: OTP(TOTP) verification

where the user is asked for a temporary passcode associated with the current time as a new token is generated if the token is not entered before it expires. The real-time algorithm is used to match and verify the authentication token associated with the current time and when the match is done with the one in the database, the authentication is successful and the user is directed to verify the fingerprint

-Step 3: Biometric feature (fingerprint verification) where the user is asked for the registered fingerprint by applying a matching algorithm to verify the fingerprint that is currently entered against the one that is stored in the database and upon matching, the user is successfully authenticated and the user is directed to the interface of the educational digital platform .

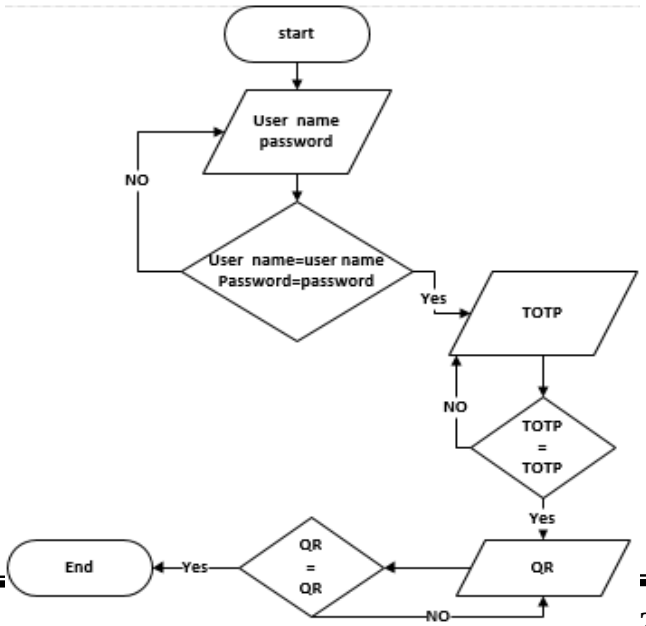
3- The educational digital platform unit

After the user has completed the authentication stage, he is transferred directly to the interface of the educational digital platform, where he is able to attend video or audio lectures, insert data and files, upload, download or delete them, communicate, comment, and etc...

Fig (4) Log in to the educational digital platform

The third stage: Algorithms of the proposed authentication system

In light of the proposed authentication system units (registration unit-authentication unit-digital platform unit), the necessary algorithms have been prepared that are suitable for multi-factor authentication by integrating all types of authentication, as these algorithms were relied upon in writing the code of the proposed authentication system.



Fig(5) shows the two-factor authentication algorithm 2FA

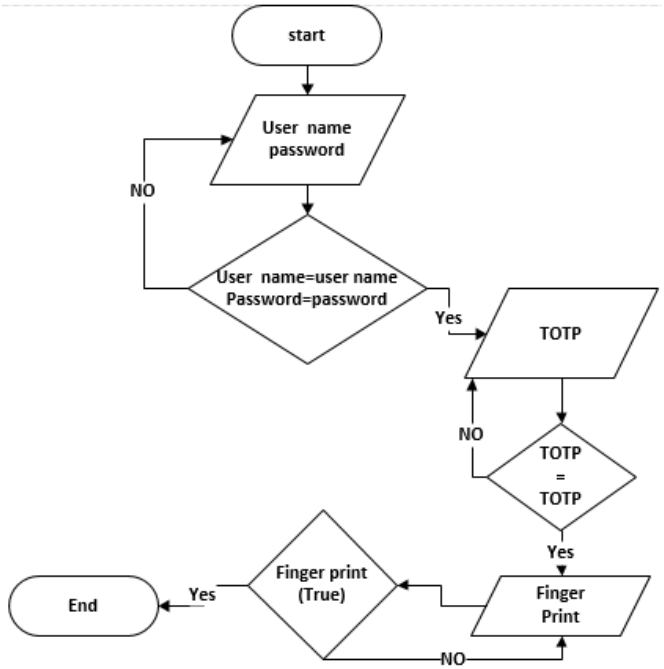


Fig (6) shows the three-factor authentication algorithm 3FA

The fourth stage: programming the proposed authentication system

Start programming the proposed system through the language used in the encryption algorithm (Python) and the languages used in designing the experimental program HTML, CSS, Javascript, SQL, Python

The fifth stage: Verification (testing the proposed authentication system)

The goal of this stage is to ensure that the proposed system works as it should and works as desired by the user, and this stage is based on the validity of the data entered in the units of the authentication system, where the exploratory experimentation of the proposed authentication system was carried out on a sample size (5) of students who are computer teachers in the fourth year, where The researchers held online interviews

with that sample to clarify the importance of the proposed authentication system and its objectives and to survey their opinion on its elements by answering the following questions: Does the proposed system meet their security needs when logging in to digital platforms? Does the proposed authentication system help to link between security levels and the possibility of access to the services of educational platforms? Are the biometric features available in the proposed system appropriate to their preferences? Do the security factors and options of the proposed authentication system allow users of digital platforms to have appropriate control over the confidentiality of their personal data?

In light of the results of the exploratory experimentation of the proposed validation system, the proposed design was revised and amendments and proposals were made in preparation for preparing the final version and preparing it for implementation and achieving this in a manner that ensures that the proposed system comes out in its final form in a way that contributes to achieving its objectives and is applicable to the research sample.

The sixth stage: the final evaluation (research experience)

The proposed authentication system was applied and its objectives were achieved on the research community, where all the students of the study community were assigned to deal with the proposed system. The researchers noted the students' commitment to deal with the proposed system due to the presence of self-motivation and the desire to raise the level of security when logging in to educational digital platforms, filling security gaps and blocking attacks that their personal data may be exposed to, then apply the research tools (Recognition of the Use of Digital Platforms in Education - Scale of Users' Attitude of the Suggested Authentication System) and put a mark (√) under the response identified with the Scale of Attitude (strongly agree - somewhat agree - disagree), then processing the data, where the frequency of the questionnaire and the frequency scale were monitored in preparation for its statistical processing.

4. 1 results

First: Before implementing the proposed authentication system (questionnaire)

To identify the importance of using digital platforms in education, a questionnaire was prepared that included some indicators, and for each

indicator there were three levels (strongly agree - moderately agree - disagree) as shown in the table(1).

Table (1) shows the frequencies, percentage, and ca2 for the questionnaire to identify the use of digital platforms in education

No	Phrases	Strongly agree		Somewhat agree		disagree		Q^2	Sig.	Ranking
		F	%	F	%	F	%			
1	Liberalizing the use of digital educational platforms 1st edition of texts and the expansion of e-learning	150	86	20	11	5	3	218	0.000	10
2	Implementing a unified policy for the use of digital platforms in education	90	51	70	40	15	9	51	0.000	11
3	Benefit from the experiences of countries in using educational digital platforms	160	91	15	9	-	-	268	0.000	8
4	Providing the necessary security across digital platforms to preserve personal data and scientific content	171	98	4	2	-	-	327	0.000	2
5	Develop a unified educational platform with which both the student and the lecturer interact	162	93	11	6	2	1	277	0.000	7
6	Developing interactive educational curricula for students and making them available on digital platforms	155	89	20	11	-	-	244	0.000	9
7	Users' lack of awareness at the present time of how to fill security holes within digital platforms and repel attacks that can be exposed	164	94	11	6	-	-	288	0.000	6

8	Personal data leakage and hacking is now a threat to learners	173	99	2	1	-	-	338	0.000	1
9	The health and safety of learners has become a data security factor side by side	166	95	9	5	-	-	299	0.000	5
10	Weak security factors and the lack of additional options that allow users of digital platforms to have adequate control over the confidentiality of their data	168	96	7	4	-	-	310	0.000	4
11	There is a close relationship between authentication factors and achieving security within digital platforms	170	97	5	3	-	-	321	0.000	3

By extrapolating the results of the previous table No. (1), it becomes clear that 95% of the research sample strongly agreed that the health and safety factor of learners has become alongside the data security factor when using educational platforms, and about 99% considered that the leakage and penetration of personal data has now become a threat to learners. This is due to the spread of the Internet, the widespread use of portable **digital devices and the global trend**

NO.	**measure axes**	**phrases**	**Strongly agree**		**Somewhat agree**		**Disagree**		**Q^2**	**Sig.**	**general attitude**
			F	**%**	**F**	**%**	**F**	**%**			
1	The first axis: options for authentication factors	Using the possession factor provides an additional layer of security when logging in to digital platforms	166	95	9	5	-	-	298	**0.000**	Strongly agree

2		The use of the biometric factor provides an additional layer of security when logging in to digital platforms	173	99	2	1	-	-	338	**0.000**	Strongly agree
3		Multi-factor authentication ensures data security within educational digital platforms	161	92	14	8	-	-	273	**0.000**	Strongly agree
4		The proposed system combines the advantages of two-factor authentication and multi-factor authentication	173	95	2	1	-	-	338	**0.000**	Strongly agree
5		The proposed system's multi-factor authentication replaces the traditional knowledge-factor-based authentication	168	96	5	3	2	1	304	**0.000**	Strongly agree
6		The best use of fingerprints as a main condition to enter the educational digital platforms	171	98	4	2	-	-	327	**0.000**	Strongly agree

7			The best authentication with a face recognize	33	19	10	6	132	75	144	**0.000**	Strongly agree
8	12	The second axis: the use of the proposed authentication system	Fingerprint authentication replaces the use of other authentication factors	173	99	2	12	17	-	-	283	338	**0.000**	Strongly agree	Strongly agree
			The interface of the proposed system is simple and easy to use			93									
9	13		I prefer using a voice tag when logging in to digital platforms	41	29	37	6	19	3	10	1	58	15	**0.000**	Strongly Disagree
			The proposed system is secure authentication process			73					-				
10			The best platform of the three	21	12	55	3	1	9	9	57	52	**0.000**	Disagree	
	14		The proposed system protects any unauthorized user from entering it	172	98	3	2	-	-	332	**0.000**	Strongly agree			
11			I prefer to use traditional identifiers	6	3	22	1	3	14	7	84	196	**0.000**	Disagree	
	15		The efficiency of the proposed system in recognizing the fingerprints of users	172	98	3	2	-	-	332	**0.000**	Strongly agree			
	16		The proposed system is based on additional layers of security beyond the traditional security layer	175	100	-	-	-	-	350	**0.000**	Strongly agree			
	17		Flexibility to operate the proposed system	175	100	-	-	-	-	350	**0.000**	Strongly agree			

18		The proposed system gives the user feedback indicating the correctness of the login stages	175	100	-	-	-	-	350	**0.000**	Strongly agree
19		The proposed system allows to take advantage of all the services of digital platforms	170	97	5	3	-	-	321	**0.000**	Strongly agree
20		The proposed system is based on a combination of acquisition and biometric factors as additional security layers for the authentication process	175	100	-	-	-	-	350	**0.000**	Strongly agree
21		The interface of the proposed system is characterized by the ease of familiarization of users with its components accurately	170	97	5	3	-	-	321	**0.000**	Strongly agree

22		The proposed system links security levels with access to educational platform services	170	97	5	3	-	-	321	**0.000**	Strongly agree
23		I really like to use the suggested authentication system every time I log into educational digital platforms	168	96	7	4	-	-	310	**0.000**	Strongly agree

towards digital transformation. 96% of the research sample students agreed that the weakness of security factors and the lack of additional options that allow users of these platforms to have appropriate control over the confidentiality of their data, and 94% strongly agreed On their lack of awareness at the present time of how to bridge the security gaps within digital platforms and repel attacks that can be exposed within those educational environments, especially with their continuous spread in the future and the increase in the number of people using these platforms and the expansion of the services provided by those platforms, and 97% strongly agreed that the presence of A close relationship between authentication factors and achieving security within digital platforms

Second: After applying the proposed authentication system (a trend scale)

To determine the most widely used authentication methods preferred by users of educational digital platforms, a trend scale was prepared that included some positive and negative statements, and the scale included three statements (strongly agree - somewhat agree - disagree) and the scale included three axes as shown in the table(2)

Table (2) shows the frequencies, percentage, and ca2 for the measure of user orientation for the proposed authentication system.

By extrapolating the results of the previous table No. (2), it becomes clear that:

The first axis: measuring users' attitudes towards the options of authentication factors used before entering educational digital platforms

99% of the research sample strongly agreed that the use of the biometric factor represents an additional layer of security, and therefore the

availability of that factor should be a main condition for entering the educational digital platforms, and 98% strongly agreed on their preference to use fingerprints as one of the most flexible and secured biometric features for the user and to prevent others from accessing the platform except through that, as (99%) of the sample confirmed that authentication using fingerprints dispenses with the use of other authentication factors, and fingerprints ranked first in users' preferences by (99%), as they are familiar to most users. In the sectors of society for many years in the past, while the voice print ranked second with a rate of (23%), and the face print ranked third with a rate of (19%), while the eye print ranked last with a rate of 12%, as most users reject it for fear Who damage their eyes

With regard to users' preferences for authentication factors, biometric features ranked first with a rate of (99%), while possession factors ranked second with a rate of (95%), while traditional knowledge factors based on username and password ranked third with a rate of (3%) because they believed that they did not It is the base layer that represents more security when dealing with these platforms, as 84% disagreed to add the knowledge factor layer as a traditional security layer for the previous two layers.

The second axis: measuring the users' attitude towards using the proposed authentication system

96% of users strongly agreed to use the proposed authentication system based on the combination of possession and biometric factors as additional security layers for the authentication process every time they wish to log into educational digital platforms, and 93% strongly agreed that the interface of the proposed system is characterized by simplicity flexibility of use and ease of familiarizing users with its components accurately and choosing the desired level of security, while 97% of the users of the proposed system agreed that there is a close relationship between the security levels of the proposed system and the accessibility of educational services on those platforms.

Conclusion

In an attempt to achieve more security processes for students' logins to educational digital platforms and to integrate the biometric factor into those platforms, it was clear from the results of the questionnaire that was prepared to identify the importance of using digital platforms in education that the health and safety factor of learners has become side by side the data security factor when the use of educational platforms, and the leakage and penetration of personal data has now become a threat to learners, and this may be due to the spread of the Internet and the widespread use of portable digital devices and the global trend towards digital transformation, and the weak security factors and the lack of additional options that allow users of these platforms to have appropriate control over the confidentiality Therefore, the current research sought to develop a proposed system based on integrating the biometric features (fingerprint factor) as an additional security layer when logging in to digital platforms the biometric features, and that a measure was applied to identify the users' attitudes towards the proposed system, where users strongly agreed that the interface to the proposed system is characterized by the ease with which users know its components accurately, and that the proposed system prevents any user who is not authorized to enter it, and that the proposed system gives the user feedback explaining the correctness of the stages of loggingin to ensure confidentiality and safety, and that the proposed system links security levels with the ability to access educational platforms

Future research

The focus point in the current research was to secure the stage of student login to educational digital platforms through the use of multiple authentication factors and biometrics (fingerprint factor) to ensure the confidentiality and safety of personal data, and multiple authentication factors can be used for faculty members in advanced stages when using digital platforms Such as analyzing data within digital platforms, implementing quality standards for digital platforms

References

[1]World Health Organization (WHO) Q&A on coronaviruses (COVID-19). (2020, April 17). who.int. Retrieved July 18, 2020, from https://www.who. int/emergencies/diseases/novel-coronavirus-2019/question-and-answershub/q-a-detail/q-a-coronaviruses

[2]Sahu, P.: Closure of universities due to Coronavirus Disease 2019 (COVID-19): impact on education andmental health of students and academic staff. Cureus (2020). https://doi.org/10.7759/cureu s.7541

[3] KUNA, (2020): University education and the distance learning process in light of the Corona pandemic, Al-Rai
https://www.alraimedia.com/article/899147/

[4]Nagaraju S, Parthiban L(2015). Achieving privacy protection of multi-factor authentication and access keys in cloud computing. Proceedings of 3rd National Conf on Frontiers in Applied Sciences And Computer Technology (FACT'15). p. 308–15.

[5] Eric G, Upadhyay M (2013) Authentication at scale. IEEE Comput
Reliab Sci

[6]Heim, P(2016). Resetting passwords to keep your files safe. https://blogs.dropbox. com/dropbox/2016/08/resetting- passwords- to- keep- your- files- safe/ .

[7]Panse, D., & Haritha, P(2014, August). Multi-factor Authentication in Cloud Computing for Data Storage Security. International Journal of Advanced Research in Computer Science and Software Engineering, 4(8).

[8] Homanova, Z. & Prextova, T. (2017): Educational networking platforms through the eyes of Czech primary school students academic conferences international limited, European conference on e- learning, kidmore end: 195- 204.

[9]Reimers, F., Schleicher, A., Saavedra, J., & Tuominen, S. (2020). Supporting the continuation of teaching and Learning during the COVID-19 Pandemic. Annotated Resources for online learning. OECD 2020, 1–38

[10]Novet, Jordan. "Zoom Has Added More Videoconferencing Users This Year than in All Of 2019 Thanks to Coronavirus, Bernstein Says." CNBC, CNBC, 26 Feb. 2020 www.cnbc.com/2020/02/26/zoom-has-added-more-users-so-far-this-year-than-in-2019-b
ernstein.html

[11] Symantec VIP Data Sheet (2015) Symantec™ validation and ID protection service: prevent unauthorized access to sensitive networks
and applications. Accessed date: 01 Dec 2016. URL: 7 http://www. symantec.com/content/en/us/enterprise/fact_sheets/b-validation_ and_id_protection_service_DS_21213686.en-us.pdf

[12]Chan, Rosalie. "Microsoft Teams Just Hit 20 Million Daily Active Users, Beating Its
Rival Slack Once Again." Business Insider, Business Insider, 19 Nov. 2019,

www.businessinsider.com/microsoft-teams-20-million-daily-active-users-slack-2019-11.

[13]Ozatok, M. & Brett, c., (2012): social presence and online learning A review of research, the journal of distance education, 26 (2)

[14]Etherington, Darrell (May 6, 2014). "Google Debuts Classroom, An Education Platform For Teacher-Student Communication". TechCrunch. AOL. Retrieved April 28, 2017

[15] Multi-factor Authentication (2016) Accessed date: 01 Dec 2016.
7 http://searchsecurity.techtarget.com/definition/multifactorauthentication-MFA

[16]Blog CAE, E-learning,(2019): 9 Advantages of Learning Platforms or LMS, https://www.cae.net/Ims-learning- platforms-advantages/

[16]Ryan,(2020): What is an online learning platform?, https://www.idtech.com/blog/what-is-an-online-learning-platform

[17] Ashbourn J (2014) Biometrics: advanced identity verification: the complete guide. Springer, Berlin

[19]Oproiu, G., C., (2015). The role of learning platforms in university teaching process, April, https://www.researchgate.net/publication/299638099_The_R ole_Of Learning_Platforms In_University_Teaching_Process

[20]Heriberto& Jackine&Patricia,)2017(Strategies Used By Professors Though Virtual Educational Platforms In Face –To-Face Classes: A View From The Chamilo Pltform,English Language Teching,10(8)

[21]Almarabeh, T., & et al, (2014), The university of Jordan E- learning Platform: State Students' Acceptance and Challenges, Journal of software Engineering and Applications, 7, pp. 999-1007.

[22]Benta, D. & et al, (2014), E- learning platforms in Higher education, case study 2nd international conference information technology and quantitative management ITGM, Procedia computer science, 2 (31), pp. 170-186.

[23]Mukerjee. S., (2014). Agility: a crucial capability for universities in times of disruptive change and innovation Australian universities Review, 56 (1), p56-60.

[24]Benta, D. & et al, (2014), E- learning platforms in Higher education, case study 2nd international conference information technology and quantitative management ITGM, Procedia computer science, 2 (31), pp. 170-186

[25]Mateia, A. & Vrabied, C., (2011), E- learning platforms supporting the educational effectiveness of distance learning programme, A comparative study on administrative sciences, Procedia- social and Behavioral sciences, 2 (3), pp. 123- 131.

[26] Uounie, S., & Leask, M., (2013), Implementing learning platforms in schools and universities: lessons from England and Wales, Technology, Pedagogy and Education, 22 (2), PP 247- 266.

[27]Soni, P., & Sahoo, M (2015). Multi-factor Authentication Security Framework in Cloud. International Journal of Advanced Research in Computer Science and Software Engineering Computing, 5(1).

[28]Veerendra, B., & Prasad, Y (2017). A Trusted Framework for Authentication and Security for Business Applications in Cloud. International Journal for Modern Trends in Science and Technology, 03(01)

[29] Naveed, G., Rakhsh, & Batool, a. (2015). Biometric Authentication in Cloud Computing. Journal of biometrics & biostatistics, 6(5). Retrieved 3 11, 2019, from https://omicsonline.org/open-access/biometric-authentication-in-cloud-computing-2155-6180-1000258.pdf

[30] Choudhari, E., & Bodhe, K. D. (2017). Biometrics Authentication Technique in Cloud Computing. International Journal of Scientific Research in Education, 5(01). Retrieved 3 11, 2019, from http://ijsae.in/index.php/ijsae/article/view/65

[31]Singh, C. and Singh, T. D. A Systematic Review of Various Multifactor Authentication Schemes. International Journal of Computer Sciences and Engineering,7(2), February 2019.