A Novel Two-Factor Authentication Scheme for Increased Security in Accessing the Moodle E-Learning Platform

Vasile Baneş 1,*, Cristian Ravariu 1, Bhargav Appasani 2 and Avireni Srinivasulu 3

Abstract: Moodle is a platform designed for universal learning to support pedagogical interactions and educational activities. The information technology (IT) administrator uses standard authentication methods for students logging into the Moodle platform. The need for two-factor authentication has grown as institutions, governments, and individuals realize that passwords are not secure enough to protect user accounts in their current technical format. The classic connection methods have vulnerabilities, and account passwords are easy to crack. Analyzing these aspects, the goal is to create a new safe and reliable alternative to the traditional authentication methods in e-learning platforms. The proposed solution introduces a new authentication factor using digital certificates stored on physical devices or the cloud to address the evolving authentication and security challenges effectively. The absence of this authentication within the Moodle ecosystem has imparted a sense of urgency for its implementation. With the innovative authentication scheme, the users have gained confidence, are satisfied with the new solution, and have not reported security breaches. The result is increased security, data protection, and better account management.

Keywords: Moodle; e-learning; digital certificate; devices; authentication

1. Introduction

Moodle is an e-learning platform created to provide students, teachers, and IT administrators with an easy-to-use system, the possibility to create personalized courses, and free, open-source software. Moodle is a platform designed for universal learning to support learning and teaching. It is an all-in-one learning platform with a simple and intuitive interface, copy functions, and continuous user improvements. Moodle is licensed under the GNU General Public License; it can be adapted, modified, and extended, free of charge, without license fees, and with an online support community [1]. Moodle is continuously improved and revised according to users’ needs, and it is customizable, secure, and private. It is web-based and can be accessed from anywhere in the world, and the interface is compatible with various browsers and operating systems [2]. The platform is available in different languages, with documentation and a wide range of plugins. In recent years, communication plugins and blocks have been developed to facilitate communication between students and teachers. Authentication allows users to log in to a Moodle site with a username and password. Moodle provides various authentication plugins for managing user authentication, including external databases, Shibboleth, email-based self-registration, OAuth 2, and manual accounts, with additional plugins available in the Moodle plugins directory.

In the specialized literature, utilizing digital certificates as a means of authentication was relatively uncommon until 2020–2021. This innovative authentication method has supplanted the previously prominent use of holographic signatures and the encryption...
of official documents. The implemented solution has led to improvement in the way to access the electronic services offered by the Moodle platform by implementing within this platform a new authentication method based on the user name, the password related to the user, and a digital certificate issued by a certification authority [3,4]. This ensures a unique and secure electronic identity for each user who uses the electronic services offered by this platform, with unified and secure access. The table below compares the authentication methods offered by e-learning platforms that offer similar services, Table 1. The information in the table was collected directly from the official websites of the e-learning platforms.

**Table 1.** Comparison between the created method and other platforms.

<table>
<thead>
<tr>
<th>Authentication Methods</th>
<th>Moodle Platform</th>
<th>Chamilo Platform</th>
<th>Canvas Platform</th>
<th>Blackboard Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>Two-factor authentication based on the name and password of the Moodle account and digital certificate issued by a certification authority (proposed method)</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>Single sign-on (SSO)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Lightweight directory access protocol (LDAP)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Email-based self-registration</td>
<td>✓</td>
<td>×</td>
<td>✓</td>
<td>×</td>
</tr>
<tr>
<td>Default internal authenticator</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>×</td>
</tr>
<tr>
<td>Web services authentication</td>
<td>✓</td>
<td>×</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>External database</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>×</td>
</tr>
<tr>
<td>Shibboleth</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Central authentication service (CAS)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

The table shows that the proposed two-factor authentication based on the name and password of the Moodle account and digital certificate issued by a certification authority is not found on the other e-learning platforms. Furthermore, the proposed solution is the only one based on the username, the password of the Moodle account, and the digital certificate issued by a certification authority. The novel contribution of this paper is the use of digital certificates issued by a certification authority and the development of a plugin, which introduces the second factor of authentication and additional security. Authentication with the digital certificate from a device (station, tablet, or laptop) is carried out using a token device or exported as a pfx file. When exporting the private key, the certificate cannot be moved from one device to another. The absence of this authentication mechanism poses significant challenges, prompting the development of a solution within the Moodle platform that would enhance the authentication process and benefit users. Implementing a digital certificate as an additional authentication factor enhances the viability and long-term security of the authentication process. Utilizing digital certificates in the authentication procedure and the requisite checks on both the certificate and user account ensures robust security. This new authentication factor addresses evolving authentication challenges and fortifies the process’s security. This novel authentication solution is introduced by thoroughly analyzing and comparing various authentication methods employed in prominent e-learning systems available in the market. This work involves meticulous analysis, a comprehensive understanding of the implementation requirements, and thorough testing, all while adhering to the best practices in the field of IT. Furthermore, the solution’s flexibility allows for customization by introducing qualified digital certificates stored on physical devices or in the cloud, accounting for future security protocols and technology advancements [5].

Blockchain technology is an authentication-based application that integrates several levels of authentication and security, making it almost impossible to hack or modify the system. It is expected that in the coming years, 6G mobile networks will be cloud-based and virtualized systems [6,7]. Another important aspect is that it will be essential for the Internet of Things [8]. The Internet of Things environment supported by a cloud server is an evolving theoretical model that integrates both the cloud’s and IoT’s benefits. As
outlined in the study led by Sharma et al., the central objective revolves around devising strategies to enhance security and safeguard interactive web-based learning platforms against cyber threats. This mission is underpinned by a thorough review of the relevant literature [9]. Nassani et al. expounded upon the substantive role occupied by e-learning in conjunction with blockchain technology, elucidating their symbiotic potential in enhancing the efficacy of privacy and security protocols. This exploration extends to electronics manufacturing, wherein the consequential impact of e-learning on privacy and security efficacy intersects with the transformative influence of blockchain adoption and integration [10]. Shahzad et al.’s investigation underscores the evolving security landscape, necessitating robust measures to protect sensitive data in rapidly advancing Internet technologies and artificial intelligence. They posit the significance of state-of-the-art networks like 6G and fortified data transfer protocols in meeting diverse security demands [11]. Collectively, these studies converge on the security challenges intrinsic to e-learning platforms. They identify intricate issues and propose innovative solutions to mitigate the vulnerabilities pervasive in these widely embraced interactive web domains. The articles mentioned above collectively address the thematic discourse concerning security challenges within e-learning platforms while concurrently endeavoring to delineate strategies for preempting security issues intrinsic to these widely adopted and functionally versatile interactive web-based platforms.

2. Evolution of Digital Certificate

A p12 file contains a digital certificate that uses (Public Key Cryptography Standard #12) encryption. The p12 file builds on PKCS #8 by adding essential information and improving security through public keys’ privacy and integrity modes [12]. It is a portable format for transferring personal private keys and other sensitive information. Various security and encryption programs use P12 files. P12 keys store a private key that encrypts information in such a way that decryption requires using the corresponding public key. In addition, data encrypted with the public key need the private key for decryption [13]. A P12 file may also contain a certificate revocation list, information about the chain of trust, and information about its holder, such as their name, surname, name of the company where they work, a position occupied, and other personal information data. Signing and encrypting this type of file blocks any modification, and thus, prevents unauthorized access. This helps validate the source of information transmitted. This method applies to migrating an entity certificate and its private key, with the signing certificate chain, from one platform to another. A certification authority to distribute a certificate chain and a private key can also be used when the certification authority generates the private key. For security reasons, the user authenticates directly with the PKCS#12 certificate, not the certificate stored in the operating system Keystore. For example, when using multiple desktop workstations and laptops, it is advisable not to leave the certificate on different devices. For increased security, access to the e-learning platform with the PKCS#12 certificate can be carried out using a USB stick [14]. The certificate standards are as follows: Rivest–Shamir–Adleman (RSA) encryption, RSA signature, password-based encryption, encrypted or cryptographic message syntax, private key information syntax, selected object category and attribute type, certificate request syntax or authentication, encryption interface or cryptographic token, personal information exchange syntax, encrypted information syntax or cryptographic token [15]. The issued digital certificate has a period of validity; it is protected against repetitive password attempts through a limited number of entries, with its blocking beyond this limit and the possibility of revocation when the student is no longer part of the system, see Table 2.
Table 2. Advantages and disadvantages of available two-factor authentication technologies.

<table>
<thead>
<tr>
<th>Two-Factor Authentication (2FA)</th>
<th>Advantages</th>
<th>Disadvantage</th>
</tr>
</thead>
</table>
| 2FA based on SMS text messages and voice | - It is easy to implement and intuitive for users.  
- Works both on desktops and mobile devices.  
- Easy to use and accessible to anyone. | - The phone number that must be declared to the respective electronic service may be used for advertising purposes, be included in spam lists, or end up in the wrong hands.  
- If the phone does not work or does not have access to a mobile network, the service does not work.  
- SMS can be easily intercepted with commercial equipment on the market.  
- Some malware aims to intercept SMS and voice code, which can be easily obtained through social engineering methods.  
- Passwords sent via SMS are vulnerable due to the portability of mobile phone numbers. |
| Push notification for 2FA | - The code is linked to the device ID; it cannot go anywhere else, the most secure method apart from the one with hardware tokens. | - When changing the device, the 2FA application must be enrolled again. If the device is unsecured, the 2FA notifications can be easily visible.  
- The push method must be more complex than a yes/no to avoid flood attacks with notifications.  
- The electronic device needs an internet connection. |
| Software tokens for 2FA/Authenticator App/TOTP 2FA | - A mobile network connection is not required.  
- Access to the code generator app can be secured with Face ID, Finger ID, password, etc. | - Third-party access to the device where the application is installed can very easily replicate the codes; the application is secured based on the device’s security.  
- If the device is insecure, so is the 2FA application. |
| Hardware tokens for 2FA | - It is probably the safest method.  
- Difficult to intercept, replicate, and manipulate. | - It is expensive to maintain and difficult to set up.  
- Depending on the security of the hardware device, new enrollment is required when the device is lost or changed.  
- Uncertainty regarding the existence of these devices in the long term. |
| Biometric 2FA | - Simple to use.  
- High level of security.  
- The biometric fingerprint/iris/voice cannot be revoked remotely.  
- Hard to fake.  
- Fast and reliable.  
- It provides more security and consumes less time. | - These technologies are in a process of improvement and expansion.  
- The biometric password lasts a lifetime.  
- Its use depends on the progress of technology.  
- There are possible errors that can lead to false acceptance and false rejection of an authentication attempt.  
- It depends on the technical capabilities of the device; depending on the device, they can have a high error rate (Palm ID and Finger ID give quite a lot of false errors). |
Two-Factor Authentication (2FA) | Advantages | Disadvantage
--- | --- | ---
2FA by email | - It is easy to implement and intuitive for users.  
- Works both on desktops and mobile devices.  
- Easy to use and accessible to anyone.  
- A convenient method to access an OTP from any platform that can provide emails.  
- The easiest to use and does not require a phone-type device yet. | - The least secure form of 2FA. Password security is too pervasive a problem to be effective.  
- Very easy to intercept and obtain the code through social engineering methods.  
- The email address that must be declared to the respective electronic service may be used for advertising purposes, may be included in spam lists, or may end up in the wrong hands. |

Twilio released Authy in 2012. It offers features, security, and support for two-factor authentication sites. It allows users to set up a new account but requires a working SIM card. It can enter a private password or PIN that Authy will use to encrypt their login details for cloud accounts [16].

Microsoft Authenticator is a two-factor authentication technology in the form of an app. It requires a QR code from the site or application to Microsoft Authenticator if the Microsoft site or product is not being used. The next step requires scanning the QR code in the app. Major disadvantages are that both are conditioned by the internet to have a program that reads QR codes or an active SIM card, and one must install the app to sign into the account. In addition, Authy will not be able to recover the account if the user no longer knows the password. Since 2014, attacks aimed at bypassing two-factor authentication have gained momentum. The methods used by the attackers range from intercepting software tokens to hacking the accounts of mobile operators and redirecting messages sent through the OTP service to the attackers [17,18].

Benefits of Two-Factor Authentication

IT departments across various industries are engaged in an ongoing battle against fraud and hackers. To fortify infrastructure security, companies should prioritize the adoption of two-factor authentication. This approach offers several benefits, including heightened security through utilizing alphanumeric passwords and special characters for both the certificate and the Moodle account. By activating a digital certificate, fraudulent attacks necessitate greater resources and effort. Even if hackers manage to obtain the password from the platform account, they cannot access the account unless they have the user’s certificate and password to gain access to the platform [19]. Implementing these dual layers of authentication substantially enhances data security and significantly diminishes the likelihood of unauthorized access to information. Consequently, users’ sense of security is heightened, and they are willing to provide additional information knowing that their data are better protected. Users appreciate the extra efforts undertaken by the IT department to safeguard personal information, thus fostering a strengthened security posture within the organization.

Furthermore, introducing a two-factor authentication system reduces costs associated with help desk support. Approximately 20% of help desk calls pertain to password resets [20,21]. Without a two-factor authentication system, password recovery can only be facilitated through the help desk, consuming time and resources exclusively. Implementing a secure self-service password reset mechanism reduces the frequency of user calls to the help desk. Consequently, the company experiences cost savings, alleviates the workload...
on help desk staff, and enhances employee satisfaction and productivity. With two-factor authentication, organizations can facilitate remote connections without compromising data security, enabling users to work securely from any device and location while accessing internal resources. This increased flexibility and freedom contribute to heightened employee productivity and job satisfaction.

Two-factor authentication offers user convenience, as it involves a straightforward process of downloading a single application that requires only one installation on the computer. Contrary to the misconception that implementing two-factor authentication is expensive and unnecessary, many small businesses and institutions underestimate the prevalence of cyberattacks targeting them [22]. In reality, more than 30% of cyberattacks occur against small institutions. Implementing a two-factor authentication solution is significantly lower than the potential cost of a successful attack on their system [23]. Moreover, numerous companies allow users to protect their accounts with two-factor authentication at no additional cost.

Issuing a digital certificate by an authorized certification authority is based on the identity document, which ensures that the user cannot subsequently refuse the original data in case of association of their account with security breaches or information leaks. Authentication with a digital certificate issued by a certification authority brings a high level of trust, secured by cryptographic mechanisms that do not allow the falsification of the holder’s security and identity. Each certificate has a period of validity and the possibility of revocation if the user ends their activity with the employer or changes their activity at work, which allows better management of the fees. When issuing the digital certificate for access within the Moodle platform, the user is asked for data such as their identity card, phone number, email address, and function within the institution [24]. In conclusion, the impact of a cyberattack can be financially costly, as well as reputationally damaging [25]. Two-factor authentication is a useful and unique tool to add an essential layer of additional security. Not only does it increase safety, but it also increases employee productivity, helping the company’s profit. Many institutions use two-factor authentication for users who want to introduce additional security. From the research carried out compared to the current connection methods, this new method brings extra security and trust.

3. Purpose of the Two-Factor Authentication Method

The Threats That Two-Factor Authentication Addresses

The need for two-factor authentication has increased as institutions, governments, and individuals realize that passwords alone are not secure enough to protect user accounts in the current technical format. The average cost of data breaches increases yearly, with financial losses of billions of dollars annually. 2FA protects against a multitude of threats. The most common threats include [26]:

1. Stolen passwords—A traditional password can be used by anyone who takes possession of it. For example, if a user writes down their password on a paper medium, that password can be stolen to gain access to an account. After entering a password, 2FA validates the user with a second device [27,28].
2. Phishing attempts—Hackers often send emails that include links to malicious websites designed to infect a user’s computer or persuade them to enter their passwords. Once obtained, a password can be used by anyone who manages the hacking attempt. 2FA combats phishing by adding a second validation layer after entering the password.
3. Social engineering—Hackers often simply manipulate users to give up their passwords. By posing as an IT professional at the user’s company, they can gain the user’s trust before asking for login credentials. 2FA protects against this by validating the location and IP of each login attempt after entering a password.
4. Brute-force attacks—In a brute-force attack, a hacker randomly generates passwords for a particular computer until it matches the correct sequence. The second level of protection of 2FA requires a login attempt to be validated before granting access.
Keylogging—If a user has not written down their password, hackers can use malware to track and copy a user’s password as they write it using the computer keyboard. Hackers track every keystroke and store the password. The second level of validation in 2FA allows a user to ensure that the login attempt is theirs, even if their password has been compromised.

4. Development of the Method with 2FA

This new method, developed by introducing another authentication factor with a digital certificate and connecting with a username and password, increases the degree of security in the Moodle platform. The correlation of the attributes related to the information in the digital certificate with the data of the account created in the platform is necessary for unique identification. The unique identification consists of reading the common attributes from the certificate and the Moodle account, such as the certificate’s serial number and email address. The site administrator and the certification authority enter these data when creating the Moodle account and generating the certificate. We made the attribute correlation functionality possible by writing the parameters in the newly developed plugin. Connecting a user to the site using the new 2FA solution is carried out by presenting the certificate and entering the related password, the first authentication factor. If the unique identification has been correctly associated, the user proceeds to the second authentication factor, wherein the user must enter their account and password from the platform in a new window. The validation occurs when the data are verified and correct, and the user reaches the site’s main page. Presenting a valid, revoked, or expired certificate that has not been associated with a site access account will generate an error message, and proceeding to the second authentication factor will not be possible. The wrong entry or other data of the platform account associated with the corresponding certificate will display an error message, and the user will no longer go to the site’s main page. Therefore, the wrong data entry to connect to the site by a user blocks the connection regardless of the situation. The process is described below.

The plugin works based on reading the pfx certificate using passphrases. It checks for the passphrases and pfx and then reads the pfx to obtain the user’s data and signatures. The pfx plugin overrides the login hook and constructor to load the pfx uploading page. Once the user has successfully uploaded and validated the password, the script will fetch the data from the database to check the specific users associated with the pfx file. This plugin reads the pfx file, which combines a certificate and a private file with a password. In addition, note that a certificate is created using a valid image address because the email address is used to identify the user from the Moodle database. Certificate authentication steps:

- Install the Open SSL program on Windows to generate a certificate and private file.
- Create a local host to run Moodle: install XAMPP, Apache distribution containing MariaDB, PHP, and SQL Server.
- Install Moodle in the local environment; the Windows version of Moodle 311 was installed on our local system.
- Create a script to validate the pfx file.
- Create a script to read the pfx file using open SSL; we created a function named readpfxfile.
- Create a script to read the cert file.
- Create a function to extract the data from the cert file.
- Create a script to upload the pfx certificate and enter the password.
- Create a script to read the uploaded file without moving to any location.
- Create a function read the pfx file.
- Create a script to obtain the certificate data from pfx.
- Create a script to extract the data from the certificate.
- Finish creating a script to read the pfx file and obtain the data using password.
- Create an authentication plugin that will override the login functionality, as seen in Figure 1.

![Manage authentication](image1)

**Figure 1.** Available authentication plugins.

- Create an authentication plugin structure.
- Create an authentication class to override the login hooks and function to load the login page.
- Create a custom authentication plugin, as seen in Figure 2.

![Plugins overview](image2)

**Figure 2.** Custom plugin.

- Extend the Moodle core authentication class.
- Create a function to show the custom page. This line of code is used to redirect to the custom login page.
- Create an authentication plugin with the pfx form upload, as seen in Figure 3.
The successful culmination of this endeavor can be attributed to an exhaustive analysis, profound comprehension of the solution’s requisites, and rigorous testing. The judicious application of established best practices within the realm of information technology further bolstered this achievement.
5. Simulation Results

5.1. Laboratory Studies on Five Two-Factor Authentication Methods Regarding Configuration, Use, and Evaluation by Users

Many widely used 2FA methods have insufficient or inadequate user usage and behavior analysis. Another aspect is that previous research on using 2FA is difficult to compare due to the wide variety of working environments. Below are some references for these studies. Reese K. et al. [29] conducted a two-week study of five common 2FA methods for collecting quantitative and qualitative data. Overall, the participants gave high marks to the methods used, and many expressed an interest in using 2FA to provide more security for their sensitive online accounts. A second laboratory study was carried out in which participants rated the overall usability of the setup procedure for the five methods. The results showed that only a few participants had difficulties setting up a hardware token and one-time password, but generally, users found the methods easy to set up. Das S. et al. [30] conducted two studies that measured the usability and acceptability of using the YubiKey (a type of FIDO U2F-compatible hardware token) as the second factor in securing a Google account. Using a think-aloud protocol, the participants encountered difficulties in use and proposed certain design changes. After repeating the study with a new group of users, they discovered that the ease of use increased but not the acceptability. The lack of acceptability was partly due to the lack of awareness of the risks and the fear of losing the device. Acemyan C. and collaborators [31] studied the configuration and authentication of four of Google’s 2FA methods. They found that participants experienced many failures and found that Google’s 2FA system was difficult to use and needed improvement. They found little difference among the four different 2FA methods when they compared efficiency, effectiveness, and satisfaction measures—illustrating that one method is not necessarily more or less useful than another. Lang J. et al. [32] reported on Google’s internal implementation of security keys to their employees. They reported a long-term reduction in authentication-related support calls after implementing hardware keys. In addition, they demonstrated a significant reduction in overall authentication time compared to other one-code-based methods. Reynolds et al. [33] described two studies of the use of YubiKeys. The study found many usability issues with the setup process and workflow of the YubiKey but found that day-to-day usage was significantly higher.

Platform administrators executed simulation parameters in the test environment on a Windows Server 2019 operating system while accessing the client from workstations configured with Windows 8, 8.1, and 10 operating systems. Compatibility tests were conducted with the Internet Explorer, Microsoft Edge, Mozilla, and Google Chrome browsers to ensure seamless site connectivity. Each workstation utilized antivirus programs, such as Bitdefender, and Windows Defender, spyware protection (Spybot), and a management console (ManageEngine) was installed.

Windows logs, application security logs, system logs, and logs from other relevant programs were collected to assess the presence of errors, security breaches, vulnerabilities, and cyberattacks. Security information was analyzed regularly at 24 h intervals throughout a 30-day simulation period. During this evaluation, the logs indicated the occurrence of several phishing attacks. Fortunately, the installed antivirus programs successfully blocked these malicious attempts without compromising the platform’s functionality or affecting the workstations.

5.2. Analyzing the Impact of the Developed Method

The proposed solution was implemented at the University of Bucharest, Romania. The study presented in this paper was conducted on 74 users divided into two groups of 37 people. The first group in the sample was authenticated only with the username and password from the Moodle account. The second group in the sample was authenticated using the proposed two-factor authentication scheme. The number of password reset requests for both schemes is shown in Figure 4.
Thus, it is noticed that when using the implemented authentication, the number of users who forgot their password decreased with the use of the new solution, having a visible and favorable decreasing trend compared to the solution related to the login with the user and password. On the first day, the number of users who forgot their password using the proposed solution was higher than those who used the username and password authentication. Considering that it is a new solution, this situation is understandable since users have not used it before; they need a little time to get used to the new method. Gradually, the number of those who forgot their password decreased, highlighting the solution’s ease of implementation and increased user convenience.

Upon analyzing the results presented in the chart above, it has been observed that on the first day of usage, employing the simple login method with the username and password, five users reported suspicions of unauthorized access to their accounts, while with the implemented solution, seven users had similar suspicions, as depicted in Figure 5. Similarly, on the seventh day of usage, employing the aforementioned simple login method, nine users reported suspicions of unauthorized access to their accounts, whereas five users reported similar suspicions with the implemented solution. This trend was observed to hold for intervals of 14, 21, and 31 days, with only minor variations in the number of users. Consequently, it has been noted that the employment of the implemented authentication method led to a marginal increase in the number of users suspecting unauthorized access to their accounts, followed by a substantial decrease compared to the simple username and password authentication solution. Notably, on the first day of usage, a higher number of users employing the proposed solution reported forgetting their passwords compared to those using the username and password authentication method. This observation is explicable, as the proposed solution was novel, and the users were not accustomed to using it. With continued use of the solution, the number of users suspecting unauthorized access to their accounts decreased, underscoring the confidence in the employed solution. Next, the number of suspicions of missing content was measured and is plotted in Figure 6.

From the analysis of the results obtained from the above chart, the following are identified: On the first day using the simple login with a user and password, four users suspected missing documents or deleted or modified courses, and with the implemented solution, two users suspected missing documents or deleted or modified courses (Figure 6). On the seventh day, using the simple login with a user and password, nine users suspected missing documents or deleted or modified courses, and with the implemented solution, five users suspected missing documents or deleted or modified courses. The same happened on days 14, 21, and 31; only the number of users varied. Thus, it was observed that when using the implemented authentication, the number of users who suspected missing documents or
deleted or modified courses had a slight increase, after which it decreased with the use of the new solution, having a visible and favorable decreasing trend compared to the related solution login with the user and password. Every day, the number of users who suspected missing documents or deleted or modified courses using the proposed solution was lower than those who used username and password authentication.

![Figure 5. Comparison between Moodle account and the proposed solution regarding suspicion of accessing the account.](image)

From the analysis of the results obtained from the above chart, the following are identified: On the first day using the simple login with a user and password, there was an equal number of external attack attempts—three for each solution (Figure 7). On the seventh day, using the simple login with a user and password, there were five external attack attempts, and with the implemented solution, there were six external attack attempts. The same happened on days 14, 21, and 31; only the number of attacks varied. Thus, it was observed that when using the implemented authentication, the number of external attack attempts had a slight increase, after which it decreased. Meanwhile, the number of external attack attempts using the simple login with a user and password increased,
which demonstrates the fact that attempts of external attacks decreased with the proposed solution, which proves its safety. Not knowing the new solution, suspicions were raised at the beginning of its use, but as the authentication method was used and understood, the number of those who gained confidence and wanted to use it increased. The main cause of data breaches in business is default or weak passwords [34]. The highest percentage of company data breaches is due to weak passwords, according to Verizon’s 2021 Report on Data Breach Investigations [35].

![Comparison between Moodle account and the proposed solution regarding external attacks.](image)

Figure 7. Comparison between Moodle account and the proposed solution regarding external attacks.

In summary, 2FA provides additional protection for users, as a username and password are not enough anymore. With this method, users must enter both factors to access their accounts. The originality of this functionality is given by the fact that it allows users to connect to their Moodle account with another authentication factor, a digital certificate issued by a certification authority. The advantages of two-factor authentication are that it adds a much-needed layer of security against attacks and can increase system security within the company. Immediately after the correct implementation, the 2FA method makes it impossible for hackers to access the account using only login information and stolen passwords. Analyzing the results obtained from the implemented authentication, we noticed a noticeable downward trend in the number of users who forgot their passwords. The number of those who suspected access to the account by others decreased, highlighting the confidence in the solution used. The number of users who suspected missing documents or deleted or modified courses was lower, and the number of external attack attempts decreased. As users used and understood the two-factor method, the number of those who gained confidence and wanted to use it increased. The analysis results show the net advantage and performance of the developed method compared to those existing on the Moodle platform. From a security point of view, the proposed solution does not present any risks in this regard but increases the degree of security. From the client station to the server, the user accesses the website address through the browser and enters the two authentication factors, connecting securely. Implementing the plugin with the new method does not affect the Moodle platform because there is the possibility of returning to the previous authentication method. This operation is carried out by uninstalling or disabling it from the console settings. A future direction for improving the security of accessing e-learning platforms would be through integration with 6G networks. Another direction for increasing the degree of security would be authentication with 2FA, where the digital certificate is in the cloud, and access to it is carried out by installing a client/program on the student’s device. Moreover, access to the platform is based on an email address and
password by validating a one-time password (OTP) code, where the code is generated on the user’s phone using Google Authenticator, and then using a digital certificate.

6. Conclusions

The traditional method of authenticating using only the user’s name and password presents an increased security risk for users and their organizations. Most of the time, content changes or the improvement of functions is impossible because most e-learning platforms have embedded systems or require access costs, unlike Moodle, a free, open-source platform. Students can log in using the default methods of the Moodle platform. It can also be used by the IT administrator when they want to improve the platform or there is a requirement from the users to create a new method using the plugin function found in the console settings menu. By writing the parameters and arguments necessary to connect with two authentication factors in the developed plugin, it was possible to operate new methods of connecting to the site. Users have access to the site regardless of the device they connect to, be it a computer, laptop, or tablet, the minimum and mandatory condition being to present the two factors. The purpose of this new method was to increase the degree of security, better account management, protection of information uploaded to the site, access to resources, and easy identification of the people connected to the platform.

Author Contributions: Conceptualization, V.B. and C.R.; methodology, V.B.; software, V.B.; validation, V.B., C.R. and B.A.; formal analysis, V.B.; investigation, C.R.; resources, V.B.; data curation, C.R.; writing—original draft preparation, V.B.; writing—review and editing, V.B., C.R. and B.A.; visualization, C.R. and A.S.; supervision, C.R.; project administration, V.B. All authors have read and agreed to the published version of the manuscript.

Funding: The National Polytechnic University of Science and Technology Bucharest financed this article through the project “PubArt”.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: For this paper, no new data has been created, no data in repository and we have nothing archived or published anywhere about results of this work.

Conflicts of Interest: The authors declare no conflict of interest.

References


**Disclaimer/Publisher’s Note:** The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.