Annals of the „Ovidius" University of Constanța – Political Science Series
Analele Universității „Ovidius" din Constanța – Seria Științe Politice
Volume 9 (2020): 7-25

M-LEARNING AND SECURITY ISSUES IN THE CORONAVIRUS ERA

Victor NEGRESCU*
Mihail CARADAICĂ**

Received: September 15, 2020 Accepted: November 5, 2020

Abstract: M-learning solutions (mobile Massive Open Online Courses – MOOCs) are key elements in a world affected by the coronavirus pandemic, considering that more than half of the world's student population was forced to stay at home during this crisis. Mobile MOOCs enable exchanges of information by using mobile devices without needing direct interaction. They have the potential to help users limit the risks and enable organizations, students and professors to continue their activities. The m-learning applications gained a lot of ground in the current context and can be seen significantly in areas such as online teaching, classroom management, language learning, and many more. In practice, the implementation of the mobile MOOCs adapted to the current challenges need to correspond to several criteria and recommendations identified by experts, in order to be viable on a large scale. This paper analyses the security issues related to the most used m-learning solutions in the current coronavirus pandemic by examining the existing empirical studies that provide a valuable insight into the requirements surrounding these applications. The findings of the study reveal that the m-learning solutions available today enable us to overcome one of the ever-growing challenges of our time, and it is essential to comprehensively evaluate them in order to enable future developers to create new and better secured mobile MOOCs adapted to the current needs.

Keywords: coronavirus, digital solutions, e-learning, online applications, education, IoT, MOOC, digital security, digital threats, digital gaps

◊◊◊

Rezumat: Soluţiile de învăţare de tip *M-learning* (*mobile Massive Open Online Courses* – MOOCs) au devenit elemente cheie într-o lume afectată din plin de pandemia generată de noul coronavirus, având în vedere că mai mult de jumătate din populaţia de studenţi din întreaga lume a fost forţată să rămână acasă în timpul acestei crize. Aceste aplicaţii permit schimbul de informaţii prin utilizarea dispozitivelor mobile fără a necesita interacţiuni directe. Ele au potenţialul de a ne ajuta să limităm riscurile şi să permitem instituţiilor de învăţământ, studenţilor şi profesorilor să îşi continue activităţile. Aplicaţiile de învăţare au câştigat tot mai mult teren în contextul actual şi pot fi întâlnite în domenii precum predarea online, managementul clasei, învăţarea limbilor străine şi multe altele. În practică însă, implementarea *MOOC*-urilor mobile adaptate provocărilor

* Victor Negrescu, Lecturer, SNSPA, e-mail: victor.negrescu@dri.snspa.ro.
** Mihail Caradaică, Lecturer, SNSPA, e-mail: mihai.caradaica@dri.snspa.ro.

actuale, trebuie să corespundă mai multor criterii şi recomandări pentru a fi viabile la scară largă. Lucrarea noastră îşi propune să analizeze problemele de securitate ale celor mai utilizate soluţii de învăţare de tip *m-learning* din timpul pandemiei de coronavirus. Ne propunem să realizăm acest lucru printr-o analiză a cercetărilor empirice deja existente pentru a obţine o perspectivă cât mai cuprinzătoare asupra cerinţelor de securitate specifice aplicaţiilor discutate. Rezultatele studiului au relevat faptul că soluţiile de învăţare *m-learning* disponibile astăzi ne permit să depăşim una dintre provocările în continuă creştere ale timpului nostru fapt pentru care este esenţial să le evaluăm de o manieră comprehensivă pentru a permite viitorilor dezvoltatori să creeze *MOOC*-uri noi şi mai bine securizate, adaptate nevoilor actuale.
Cuvinte cheie: coronavirus, soluţii digitale, învăţare electronică, aplicaţii online, educaţie, IoT, MOOC, securitate digitală, ameninţări digitale, decalaje digitale

I. Introduction

In the context of the coronavirus pandemic, students and professors are in search of education tools that would allow them to continue their classes and follow their educational activities. Over 850 million children and youth – roughly half of the world's student population – had to stay at home due to the COVID-19 pandemic. Nationwide lockdowns were in force in 102 countries and local shutdowns in 11 others[1]. In this regard, there is no doubt that e-learning solutions have become essential.

E-learning is known to be an educational instrument that allows relative freedom to formulate, organize, and create new distance-learning experiences. These new interactive methods make use of digital devices – computers or mobile devices – that enable the interaction between users[2].

The concept of e-learning is not new. Over time, it has evolved as a mainstream education tool employed by schools, universities, non-formal education organizations, individual professors, language trainers, and so on[3].

Few basic elements are needed for e-learning, such as an online platform, content, participants, and a technological infrastructure. While there are usually two perspectives associated with e-learning, pedagogical and

[1] UNESCO, "Half of world's student population not attending school: UNESCO launches global coalition to accelerate deployment of remote learning solutions", March 19, 2020, accessed April 15, 2020, https://en.unesco.org/news/half-worlds-student-population-notattending-school-unesco-launches-global-coalition-accelerate.

[2] Zlatko Bezhovski and Subitcha Poorani, "The Evolution of E-Learning and New Trends", *Information and Knowledge Management* 6, no. 3 (2016): 50.

[3] Anoush Margaryan, Manuela Bianco, and Allison Littlejohn, "Instructional quality of Massive Open Online Courses (MOOCs)", *Computers & Education* 80 (2015): 78.

technological[4], we are going to focus on the element that unites the two aspects which is the issue of security. In this process we regard, of course, several technologies, namely the smartphone / laptop? [MISSING WORD] or the mobile phone, e-mails, web browsers, internet connections, the software used for educational purposes, the microphone and camera used in the process, the application or the platform, and the list can continue[5].

Despite its complexity, there are also new trends in e-learning. Massive Open Online Course (MOOCs) are the new open, democratic version of e-learning, based on self-learning method courses and open-access[6]. The term was first used to describe an online open course "Connectivism and Connective Knowledge (CCK08)", which was developed at the University of Manitoba by George Siemens and Stephen Downes and had over 2200 participants from all over the world. Early MOOCs tended to have a decentralised, network based, non-linear structure focused on exploration and conversation rather than emphasising instructor-provided content[7]. The online e-learning website *Udemy* enrolled over 100,000 students online in 2011. Moreover, according to Dhawal Shah[8], in 2015, 35 million of students signed up for at least one course, 4200 MOOCs were offered, and more than 500 universities provided these types of courses. The development of the mobile technology generated a new change in e-learning and MOOCs and so mobile learning emerged. Basically, without any geographical constraint, the user can use any mobile-learning instruments[9].

Mobile learning is now a complex instrument, using intelligent user interfaces, context modelling, networking technologies, and communications. Many issues remain to be studied and some go even to announce the failure of this model due to the fact that it is mainly technology driven[10].

However, all these technology-enabled evolutions are influencing education and are clearly driven by context. Mobile devices are here, and they are here to stay. More than 5 billion people have a mobile device, and more than half are smartphones[11]. The coronavirus pandemic provides an opportunity to

[4] Vladan Devedzic, *Semantic web and education* (Chicago: Springer Science & Business Media, 2006).

[5] Vidyadevi Patil, "Technologies used in E – learning", *Scholarly Research Journal for Humanity Science and English Language* 1, no. 2 (2014): 280-285.

[6] Zlatko Bezhovski and Subitcha Poorani, "The Evolution of E-Learning and New Trends", *Information and Knowledge Management* 6, no. 3 (2016): 50.

[7] Margaryan, Bianco, and Littlejohn, „Instructional quality of Massive Open Online Courses", *Computers & Education* 80 (2015): 78.

[8] Dhawal Shah, "By the Numbers: MOOCS in 2015", December 21, 2015, accessed April 15, 2020, https://www.classcentral.com/report/moocs-2015-stats/.

[9] Zlatko Bezhovski and Subitcha Poorani, "The Evolution of E-Learning and New Trends", *Information and Knowledge Management* 6, no. 3 (2016): 51.

[10] Paul Muyinda, "MLearning: pedagogical, technical and organisational hypes and realities", *Campus-Wide Information Systems* 24, no. 2 (2007): 102.

[11] Laura Silver, "Smartphone Ownership Is Growing Rapidly Around the World, but Not Always Equally", *Pew Research Center*, February 5, 2019, accessed April 11, 2020

study the new educational trends around the world. Students and professors are limited in their interactions so for learning purposes, everyone is forced to find alternative solutions. Some of those solutions belong to educational institutions, some to public authorities, but a lot of them are open and available online and can be used through mobile devices. These are the MOOCs. Our study focuses on a specific category, the mobile MOOCs, more flexible, easier to use, more accessible.

II. Need for the Study

Given the current context generated by the coronavirus and the need to rapidly adapt the educational methods, open m-learning platforms (mobile MOOCs) seem to be a potential solution for global education. These new platforms have already changed educational practices and methods, but their impact today is bigger than ever. They bring with them all the positive aspects like distance learning, personalized educational tools, "learner-oriented design" or innovative teaching methods[12]. But there are also downsides to this form of education in the form of security threats, cyber-attacks or tech-quality issues. Child protection, data protection, invasion of privacy, unauthenticated access, or service limitations are just some of the potential threats that users might encounter. It is therefore important to understand the associated security issues of m-learning platforms, as well as their likely solutions.

III. Aim of the Study and Methodology

The aim of this study is to analyse the technological requirements, security issues, and defence solutions against the challenges related to the use of m-learning tools. The other objective of this research is to provide a brief overview of mobile MOOCs applications used in the context of the coronavirus pandemic and to analyze the type of security threats and common cyber-attacks on the m-learning applications. The methodology of the study is based on the empirical review of the available literature on the security challenges and the potential solutions to the security threats of m-learning solutions. This study is using the review method employed by Tariq Ahamed Ahanger and Abdullah Aljumah in their article "Internet of Things: A Comprehensive Study of Security

https://www.pewresearch.org/global/2019/02/05/smartphone-ownership-is-growing-rapidly-around-the-world-but-not-always-equally/

[12] Zlatko Bezhovski and Subitcha Poorani, "The Evolution of E-Learning and New Trends", *Information and Knowledge Management* 6, no. 3 (2016): 52.

Issues and Defense Mechanisms"[13]. The research will therefore focus on the practical implications of security in the m-learning applications (mobile MOOCs) and will seek to identify the potential differences in terms of results with the help of the above-mentioned article.

IV. Applications of M-Learning

M-learning applications have known a fast growth in the current coronavirus context. The concept is rather new, and few studies have analysed its impact and the security issues associated with it when used on a large scale. The fast development of what we have chosen to call mobile MOOCs is a sign of the need to address this issue in research.

Defining its characteristics is essential for the study in order to fully assess its implications and the security issues it raises. We have managed to address several dimensions of the concept when considering the aspect of security addressed by this article.

Among the essential traits illustrated in the definitions is that mobile MOOCs address the issue of open learning.

Open learning is an approach which combines the principles of student-centeredness, lifelong learning, flexibility of learning provision, the removal of barriers to access learning, the recognition of prior learning (RPL), the recognition for credit of prior learning experience, the provision of student support, the construction of learning programmes in the expectation that students can succeed, and the maintenance of rigorous quality assurance over the design of learning materials and support systems[14].

Another key element is that this learning method is mobile-dependent. M-learning is aligned with the trends in mobile technologies. The evolutions of mobile devices, the type of Internet connections, IoT (Internet of Things), the mobile operation systems are just some of the elements that influence mobile MOOCs[15].

Finally, mobile learning is linked with a personalized approach on education. These instruments are based on user model as well as on the perceived model of learning environment[16]. Mobile MOOCs not only meet the

[13] Tariq Ahamed Ahanger and Abdullah Aljumah, "Internet of Things: A Comprehensive Study of Security Issues and Defense Mechanisms", *IEEE Access* 7 (2018): 11020-11028.
[14] Department of Education, Parliament of the Republic of South Africa, "White Paper on Education and Training", Notice 196 of 1995, accessed April 12, 2020, https://www.education.gov.za/Portals/0/Documents/Legislation/White%20paper/White%20paper%20on%20Educati on%20and%20Training%201995.pdf?ver=2008-03-05-111656-000.
[15] John Traxler, "Distance Learning—Predictions and Possibilities", Education Science 8, no. 35 (2018): 7-8.
[16] M. del Puerto Paule Ruiz et al., "Adaptation incurrent e-learning systems", *Computer Standards & Interfaces* 30, no. 1-2 (2008): 62–70.

need of each individual learner to adapt to their learning goal, knowledge level, educational contexts, preferences and learning styles[17], but also structure the contents and its findings to facilitate instruction and information dissemination to the specific user, based on parameters such as age, personal attributes, and previous knowledge. Furthermore, many systems use cognitive models like learning styles or educational strategies.

This raises even more security issue and threats to the users of these specific mobile learning solutions. This issue becomes even more complicated since m-learning is based on mobile devices which sometimes require wireless communication and uses personal data[18].

In order to have a more appropriate overview of the m-learning applications, we have analyzed the most relevant literature on this topic. We found that many scholars discuss the issue of m-learning from various perspectives:

- by separating e-learning and m-learning based on criteria like mobility, materials and instructions, presentation, communication, connectivity or assessment[19];
- by the general e-learning categories of research like pedagogical, organisational, technical and socio-cultural[20];
- or by categories of provisions like course materials (interactivity), learning support and assessment[21].

The theoretical perspective that we identified to be the most relevant belongs to Bezhovski and Poorani[22]. Their approach is very useful for our research as it helps us better understand the necessities of the users that opted for a m-learning solution in the crisis generated by the spread of COVID-19. The two authors state that all the e-learning solutions can be described as synchronous and asynchronous. In the first situation, both the instructor and learner are present at same time and this situation includes virtual classrooms, webinars, video conferencing, and other similar methods. In the second case, learning tools can be used for self-paced learning and includes reading materials, audio and video, forums, wikis, etc. The category discussed by Bezhovski and

[17] Ibid.
[18] Shaibu Adekunle Shonola and Mike Joy, "Security issues in E-learning and M-learning Systems: A Comparative Analysis", 2nd WMG Doctoral Research and Innovation Conference (WMGRIC2015), Warwick, United Kingdom, June 30th– July 1st, 2015.
[19] Ibid.
[20] Najwa Hayaati Mohd Alwi and Ip-Shing Fan, "Information Security Threats Analysis for E-Learning", Tech-Education, Athens, Greece, May 19-21, 2010, 286.
[21] Council on Higher Education, *Distance Higher Education Programmes in a Digital Era: Good Practice Guide* (Pretoria: CHE, 2014), accessed April 15, 2020, https://www.saide.org.za/documents/CHE_-_Distance_Higher_Education.pdf.
[22] Zlatko Bezhovski and Subitcha Poorani, "The Evolution of E-Learning and New Trends", *Information and Knowledge Management* 6, no. 3 (2016): 52.

Poorani addresses the way people intend to use the applications in this difficult time.

Furthermore, another classification we identified is based on the necessity to access the Internet. This helps us understand the extent to which people need to be connected in the education process as well as how developed and complex the apps are. According to a study conducted by the Council on Higher Education of South Africa[23], there are Internet-supported programmes where online participation is optional for students; Internet-dependent programmes where participation via the Internet is a requirement – this second category could include online interaction, communication, and access to course materials via the Web; finally, there are fully online programmes where there is no physical face-to-face component, although there could be a virtual face-to-face one. Based on these categories, we acknowledge the high technical complexity of the mobile MOOCs. Some of the security issues underlined in the definitions illustrate the need for an integrated and personalized approach to these concerns especially in a crisis context like the one generated by the coronavirus pandemic.

Starting from the information provided by the definitions, we analyzed the use of m-learning applications during the coronavirus pandemic. More exactly, the studied period started on March 11th, 2020 – the day when the World Health Organization announced that the novel coronavirus posed a pandemic threat[24] and lasted one week, finishing on the March 18th, when the United Nations Educational, Scientific and Cultural Organization (UNESCO) announced that more than half of globe's students[25] were not attending school. Our analysis focused mainly on the countries that had – on March 18th – more than 200 confirmed cases of COVID19.

Based on this framework, we organized the data in order to illustrate the full global scale of the coronavirus. We drew a global map that included the countries that had the most cases. In total we had 41 countries that had more than 200 cases on the date of reference.

[23] Council on Higher Education, *Distance Higher Education Programmes*.
[24] World Health Organization, "WHO Director-General's opening remarks at the media briefing on COVID-19 – 11 March 2020", March 11, 2020, accessed April 15, 2020, https://www.who.int/dg/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020.
[25] UNESCO, "Half of world's student population not attending school: UNESCO launches global coalition to accelerate deployment of remote learning solutions", March 19, 2020, accessed April 15, 2020, https://en.unesco.org/news/half-worlds-student-population-notattending-school-unesco-launches-global-coalition-accelerate.

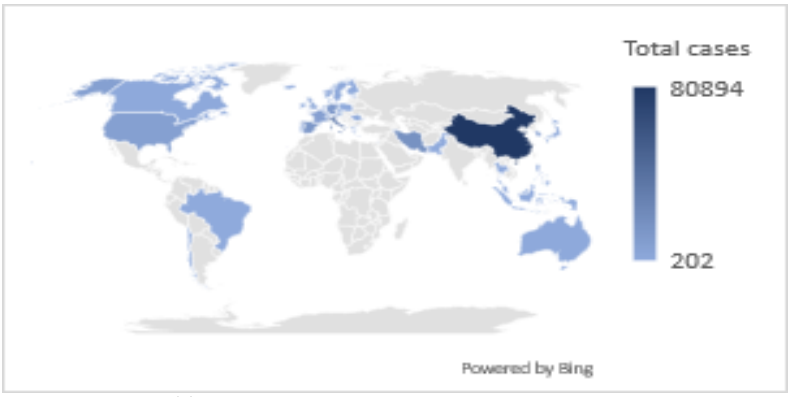

Figure 1: The coronavirus spread around the world on March 18th
(countries with more than 200 declared cases)

Starting from this list of countries, we tried to identify the trends in the use of m-learning applications. We analyzed, based on the data available online on a dedicated platform (app.apptweak.com), the most used educational apps, by country. Out of the 41 countries chosen for the analysis, we could find data only for 39 of them. Iran and Bahrain were not providing access to the use of apps in their countries. More exactly, we looked at the five most downloaded free educational solutions on the date of reference in those countries on Google Play and Apple Store. Using this data, we generated a top 10 of the most used free mobile MOOCs.

We found that the most used m-learning applications were Google Classroom, Edmodo, Duolingo, Simply Piano, Photomath, Moodle, Anton, Lingokids, Seesaw Class, and Minecraft Education. Based on the theoretical approaches we discussed above, five applications can be described as synchronous (Google Classroom, Edmodo, Moodle, Seesaw Class, and Minecraft Education). This is showing us that, during the limitations generated by the pandemic, the role of remote education became increasingly important. Meanwhile, asynchronous applications – also five in number – Duolingo, Simply Piano, Photomath, Anton, and Lingokids, do not involve interactions between students and teachers, or among students in general. Those applications can be described as a useful tool for a self-education process. At the top of the users' preferences, we have foreign languages applications for adults, with Duolingo leading the way, but also for kids, Lingokids also being in top 5. There is also an important interest for piano and math, as Simply Piano and Photomath are in this top as well. Anton is also a tool of self-learning but is not focused on a specific topic as it provides a wide range of possibilities for learning.

Regarding the necessity of having an Internet connection, the applications that fit into the synchronous category are Internet-*dependent* programmes where online participation is highly required given the existence of online interactions in the learning process. Here, the teacher guides the students through different online tools like quizzes, homework with deadlines, or digital

content. The applications in the asynchronous category can be better described as Internet-*supported* programmes because they do not necessitate student interaction, but the content is mostly located in the cloud and downloads are required in order to pass from one lesson to another.

V. The Security Threats of E-Learning

After identifying the list of applications and the theoretical categories in which the ones most downloaded during the COVID-19 crisis could be assigned to, we move to the next objective of our research in order to see how performant these programmes are in terms of security.

Threat analysis is a process of detection, identification, and evaluation of vulnerabilities present in an operation or system. Threats are analysed with respect to their likelihood of occurrence, their possible impact on individual users and systems, as well as in relation to the global risk they represent. Our study conducted a threat analysis for each mobile MOOCs considered to be essential in the current context[26].

Security is an essential requirement of any online platform. In online learning, security means that learning resources are available, and all authorised users have unhindered access to them whenever they need them[27]. Security is paramount when the number of users and participants is large and covering a wide geographic area, like it was the case in the pandemic crisis. Security is essential to retain users' trust in the online learning environment because any risk can dramatically affect their perception of the system's reliability and trustworthiness[28]. Online learning systems have attracted hackers and other malicious users. The risk is great; as the functionalities and features of online learning systems are becoming more complex, online learning is increasingly exposed to security threats[29].

The most important security threats that we have identified in the context of mobile e-learning are confidentiality, integrity and availability.

Availability is a way to guarantee that authorized people have reliable access to information. According to Dai, András, and Zoltán[30], the threat appears when the intruders use DoS or DDoS technology to attack the victims.

---

[26] Alwi and Fan, "Information Security Threats Analysis for E-Learning", 286.

[27] Anne Adams and Ann Blandford, "Security and Online learning: to protect or prohibit", in *Usability Evaluation of Online Learning Programs*, ed. Claude Ghaoui (UK: IDEA Publishing, 2003), 331–359.

[28] Ibid.

[29] Najwa Hayaati Mohd Alwi and Ip-Shing Fan, "E-Learning and Information Security Management", *International Journal of Digital Society* 1(2010): 148.

[30] Nguyen Huu Phuoc Dai, András Kerti, and Zoltán Rajnai, "E-Learning Security Risks and Countermeasures", *Emerging Research and Solutions in ICT* 1, no. 1 (2016): 20.

Availability is ensured by maintaining all hardware in a proper condition and by constantly upgrading the software.

Integrity is a way of assuring that the information is trustworthy and accurate. The threat appears when unauthorized users alter or modify the content of the information by executing malicious codes[31]. To prevent this threat, one has to take all required steps to ensure that the data is not altered when in transit.

Finally, confidentiality is about rules that limit access to information. The threat appears when we have insecure storage and information leakage[32]. This concept closely related to privacy is about making sure that sensitive information is not getting in the wrong hands.

Alwi and Fan[33] suggest that the way some security issues can be solved is by improving two key elements:

- Access management: The way to avoid all attacks to the e-learning environment is by controlling access. One of the ways to do this is through the authentication and authorisation process. As we can see, there is a technical aspect of access management that involves working on digital identity design and privacy preservation. Another aspect concerns the development of a better process of identifying legal users.
- Intellectual property: The main challenge here is to protect intellectual property by extending the control of the copyright holder to the entire lifetime of digital data.

VI. Cyber-Attacks on E-Learning Platforms

Since online learning takes place via the Internet, every element in an online learning system can be a potential target of hacking or other malicious attacks. This may lead to unauthorized modification and/or destruction of educational assets[34]. The inherent security risks that should be considered are: identity theft, impersonation, and inadequate authentication[35]. Online learning systems have attracted the attention of cybercriminals who thrive on their ability to hack into such systems. Thereby, as the features of online learning systems become more complex, they are increasingly exposed to security threats[36].

---

31 Ibid.
32 Ibid.
33 Alwi and Fan, "Information Security Threats Analysis for E-Learning", 286.
34 Vladimir Zuev, "E-learning security models", *Management* 7, no. 2 (2012): 25.
35 Taiwo Ayodele, Charles A. Shoniregun, and Galyna Akmayeva, "Towards e-learning security: A machine learning approach", Information Society (i-Society) International Conference, London, UK, June 27-29, 2011, 490-492.
36 Alwi and Fan, "E-Learning and Information Security Management", 148.

Some of the most common cyber-attacks on the mobile MOOCs are highlighted by Priya and Jayanthi[37] who provide the broadest evaluation of the cyber-attacks, as follows:

A. Security Threats in E-Learning Environment

- Virus
- Worm
- Trojan horse
- Malware
- Adware
- Spyware
- Rootkit
- B. Cyber Security Attacks in E-Learning Environment at User side
- Phishing
- Cross side scripting
- Click jacking
- Content Spoofing
- Brute force attack
- Authentication attack
- C. Cyber Security Attacks in E-Learning Environment over the internet
- Sniffing
- DOS
- DDOS
- Spoofing
- Replay attack
- D. Cyber Security Attacks in E-Learning Environment at Database Server
- SQL Injection
- LDAP Injection
- Weak Authentication

As one can see, there is a wide range of attacks that could come from all directions. Viruses, worms or Trojans are all part of malware software. Malware refers to any malicious program or software that is designed to exploit a computer user by attacking the computer programs and files or the user's confidential data[38]. To these attacks, we may also add phishing, cross side scripting, click jacking, content spoofing, brute force attack, and authentication

[37] R. Priya and J. Jayanthi, "Security Attacks and Threats in E-Learning", *International Journal of Emerging Technology in Computer Science & Electronics* 21, no. 3 (2016): 629-633.

[38] Ashish Mundhra, "GT Explains: What is the Difference Between Malware, Virus, Rootkits, Spyware, Worm and Trojans", *Guiding Tech*, December 6, 2011, accessed April 16, 2020, https://www.guidingtech.com/8888/difference-between-malware-virus-rootkits-trojans-worm-spyware/

attack. All these potential threats show us how exposed a regular user is and how many dangers a simple e-learning platform may involve. Many of these attacks can be avoided with proper cyber hygiene, but this implies an entire process of cyber education that should start in early school.

The attacks that occur on the Internet or on the software database are more particular because they refer to the company owning the e-learning application. Here, a guarantee of safety is ensued by the brand behind the app, given that the company is willing to invest significant financial resources in the security aspects of the e-tool. Therefore, the responsibility in the security field is understood to be split between users and companies.

VII. Set of Security Requirements Needed for Mobile Moocs – Empirical Analysis

This section presents the empirical analysis of the existing studies related to security and privacy concerns in mobile learning. As a general overview regarding the security of the m-learning system, Shonola and Joy[39] propose a set of robust mechanisms to support user authentication, authorisation and non-repudiation, management of data, content copying, editing and downloading, safeguarding learner examination and assessment processes. Without satisfying these issues, the trust in the m-learning application might suffer.

Another solid contribution was made by Ahmad and Elhossiny[40] who come with practical solutions for the security issues that concern an e-learning application. Where the protection from threats is concerned, any user should check if the computer is fully recovered from viruses, worms, and Trojan horses; they should think twice before they click a link in order to avoid social engineering and networking attacks; and they should use USB drivers with caution. To stay safe from email and communication attacks, users should constantly reduce spam volume and use digital signatures with caution. Regarding browsing security, one should constantly evaluate the web browser's security settings and website certificates; and review end-user license agreements. In terms of ensuring privacy control, users should effectively erase files, supplement passwords, install and use anti-virus programs, be careful when reading emails with attachments, install and use firewall programs, make backups of important files and folders, use strong passwords, be cautious when downloading and installing programs, install and use file encryption programs and access controls, safeguard data, etc.

---

[39] Shaibu Adekunle Shonola and Mike Joy, "Security of m-learning System: A Collective Responsibility", *International Journal of Interactive Mobile Technlogies* 9, no. 3 (2015): 64-70.

[40] Ateeq Ahmad and Mohammed Ahmed Elhossiny, "E-Learning and Security Threats", *International Journal of Computer Science and Network Security* 12, no.4 (2012): 15-18.

Based on the information obtained from the literature review, we have identified a series of potential security threats, attacks, and requirements applicable to mobile learning applications. In this regard, we have conducted an empirical analysis of the security of mobile MOOCs used during the coronavirus crisis (see Annex-Table 1). The results show potential patterns for security risks that should be the basis for guidelines and recommendations both for users as well as for the developers of m-learning applications.

Security issues are interconnected and, for example, one weakness regarding storage can lead to identity theft. In Table 1, we present the existent security threats and risks resulted from the interdependence of the security issues. The main security threats that we have identified as being relevant for our research and which have been examined in detail by the New Gen Apps Website[41], are:

- Insecure Data Storage: A common practice among developers is to depend on client storage for the data. This data can, in turn, be easily accessed, manipulated and used. The results could be: identity theft, reputation damage, and external policy violation.
- Unintended Data Leakage: It refers to the storage of critical app data on insecure locations on the mobile. The data is stored in a location on the device that could be easily accessible by other apps or users. The result is a breach of user privacy leading to the unauthorized use of data. Moreover, people often get confused when it comes to understanding the difference between unintended data leakage and insecure data storage.
- Insufficient Transport Layer Protection: It refers to the route through which the data is transferred from the client to the server and vice versa. In this situation, a hacker can gain access to the data and modify or steal it of his own accord. This could, then, result in frauds, identity threats, etc.
- Poor Authorization and Authentication: Mobile apps may require offline authentication to maintain the uptime. This offline requirement can create security loopholes that developers must consider when implementing mobile authentication. Poor or missing authentication allows a hacker to anonymously operate the mobile app or backend server of the mobile app.
- Security Decisions via Untrusted Inputs: Developers generally use hidden fields, values, or functionality to distinguish between higher and lower level users. An attacker might intercept the calls and mess with such sensitive parameters. Weak implementation of such hidden functionalities leads to improper app behavior resulting in higher level permissions being granted to a possible attacker.

[41] New Gen Apps, "Biggest Risks to Mobile Apps Security", November 28, 2018, accessed April 15, 2020, https://www.newgenapps.com/blog/10-biggest-risks-to-mobile-apps-security.

One can observe in Table 1 that, with the complexity of the growth of applications, security threats develop and diversify as well. Furthermore, 60% of vulnerabilities are on the client side. Meanwhile, Android applications tend to contain critical vulnerabilities slightly more often than those written for iOS (43% vs. 38%), but this difference is not significant, and the overall security level of Android and iOS mobile application for clients is roughly the same[42].

VIII. Conclusions

In a world affected by the COVID-19 pandemic, more and more people are forced to stay at home while, at the same time, continuing the learning process. For students and pupils in particular, e-learning and m-leaning solutions – given the mobile sector marked increase in importance – represent the best way to combine isolation with educational programmes and personal development objectives.

In this research we tried to identify the most downloaded applications in countries where the cases of coronavirus had already reached 200, given that after this threshold was reached, countries started to take significant actions regarding social distancing. Another objective was to identify the security vulnerabilities that users could face during this period while using mobile MOOCs.

In order to accomplish this, we started with an analysis of m-learning features, splitting them between synchronous applications, where both the instructor and learner are present at the same time, and asynchronous apps, where learning tools can be used for self-paced learning and can include reading materials, audio and video, forums, wikis, etc. By March 18th, 2020, 41 countries had more than 200 cases declared, and after analyzing the available data regarding the apps downloaded from the AppStore and Google Play, we found that the most downloaded apps were: Google Classroom, Edmodo, Duolingo, Simply Piano, Photomath, Moodle, Anton, Lingokids, Seesaw Class, and Minecraft Education.

Once the theoretical background was established, we argued that half of the applications can be described as synchronous (Google Classroom, Edmodo, Moodle, Seesaw Class and Minecraft Education). This reflects an emerging trend in using tools for remote education during the restrictions generated by the new coronavirus. The other half of the applications fit in the asynchronous category (Duolingo, Simply Piano, Photomath, Anton and Lingokids). These

[42] Positive Technology, "Vulnerabilities and threats in mobile applications, 2019", June 19, 2019, accessed April 14, 2020, https://www.ptsecurity.com/ww-en/analytics/mobile-application-security-threats-and-vulnerabilities-2019/.

programs do not involve interactions between students and teachers or among students in general. They are useful for self-education.

Afterwards, we proceeded to the next phase and we discussed the security threats posed by m-learning software. In this section, we identified the most important security threats that emerge in the context of mobile e-learning. These are: confidentiality (closely related to privacy, it refers to the ways we can ensure that sensitive information is not getting in the wrong hands); integrity (refers to the ways of assuring that the information is trustworthy and accurate); and availability (a way to guarantee that authorised people have reliable access to information).

While discussing the issue of security threats, we identified that the most dangerous cyber-attacks on the e-learning platforms are the following:

- Security Threats in E-Learning Environment (Virus, Worm, Trojan horse, Malware, Adware, Spyware, Rootkit);
- Cyber Security Attacks in E-Learning Environment at User side (Phishing, Cross side scripting, Click jacking, Content Spoofing, Brute force attack, Authentication attack);
- Cyber Security Attacks in E-Learning Environment over the internet (Sniffing, DOS, DDOS, Spoofing, Replay attack);
- Cyber Security Attacks in E-Learning Environment at Database Server (SQL Injection, LDAP Injection, Weak Authentication).

Consequently, we argued that the responsibility in the security field should be split between users and developers. Furthermore, in light of research we have conducted, we arrived at the conclusion that in order to avoid cyber-attacks, robust mechanisms are needed that support: user authentication, authorisation and nonrepudiation, management of data, content copying, editing and downloading, safeguarding learner examination, and assessment processes.

To conclude, the crisis generated by the new coronavirus not only led to an intensified use of the m-learning applications, but also came with many security risks. As the attention of the individuals and societies continues to be focused on the health crisis, hackers may target e-learning and m-learning platforms due to the big number of inattentive users. Our article conducted a literature review of the main academic studies in the field and also performed an assessment of potential security threats. The aspects highlighted in this analysis can represent a good starting point for a set of practical security requirements and recommendations that developers and users might take into account in the future. In the context of a prolonged pandemic crisis, we can expect that e-learning processes will further develop, while mobile MOOCs will continue to know an unprecedented growth. Additional research addressing the new security challenges is needed in order to better understand the emerging techno-educational avenues that have ushered in these threats.

ACKNOWLEDGEMENT

The article is part of the SNSPA Research Grant "Politica digitală a Uniunii Europene ca formă de răspuns la provocările globale", 2019.

REFERENCES

- Adams, Anne, and Ann Blandford. "Security and Online learning: to protect or prohibit". In *Usability Evaluation of Online Learning Programs,* edited by Claude Ghaoui, 331–359. London: Information Science Publishing, 2003.
- Ahanger, Tariq Ahamed, and Abdullah Aljumah. "Internet of Things: A Comprehensive Study of Security Issues and Defense Mechanisms". *IEEE Access* 7 (2018): 11020 – 11028.
- Ahmad, Ateeq, and Mohammed Ahmed Elhossiny. "E-Learning and Security Threats". *International Journal of Computer Science and Network Security* 12, no. 4 (2012): 15-18.
- Alwi, Najwa Hayaati Mohd, and Ip-Shing Fan. "Information Security Threats Analysis for E-Learning". Tech-Education 2010, Athens, Greece, May 19-21, 2010, 285–291.
- Alwi, Najwa Hayaati Mohd, and Ip-Shing Fan. "E-Learning and Information Security Management". *International Journal of Digital Society* 1 (2010): 148-156.
- Ayodele, Taiwo, Charles A. Shoniregun, and Galyna Akmayeva. "Towards e-learning security: A machine learning approach". Information Society (i-Society) International Conference, London, UK, June 27-29, 201, 490-492.
- Bezhovski, Zlatko, and Subitcha Poorani. "The Evolution of E-Learning and New Trends". *Information and Knowledge Management* 6, no. 3 (2016): 50-57.
- Council on Higher Education. *Distance Higher Education Programmes in a Digital Era: Good Practice Guide*. Pretoria: CHE, 2014. Accessed April 15, 2020, https://www.saide.org.za/documents/CHE_-_Distance_Higher_Education.pdf.

- Dai, Nguyen Huu Phuoc, András Kerti, and Zoltán Rajnai. "E-Learning Security Risks and Countermeasures". *Emerging Research and Solutions in ICT* 1, no. 1 (2016): 17–25.
- Department of Education, Parliament of the Republic of South Africa. "White Paper on Education and Training". Notice 196 of 1995. Accessed April 12, 2020. https://www.education.gov.za/Portals/0/Documents/Legislation/White%20paper/White%20paper%20on%20Educati on%20and%20Training%201995.pdf?ver=2008-03-05-111656-000.
- Devedzic, Vladan. *Semantic web and education*. Chicago: Springer Science & Business Media, 2006.
- Margaryan, Anoush, Manuela Bianco, and Allison Littlejohn. "Instructional quality of Massive Open Online Courses (MOOCs)". *Computers & Education* 80 (2015): 77–83.
- Mundhra, Ashish. "GT Explains: What is the Difference Between Malware, Virus, Rootkits, Spyware, Worm and Trojans". *Guiding Tech*, December 6, 2011. Accessed April 16, 2020. https://www.guidingtech.com/8888/difference-between-malware-virus-rootkits-trojans-worm-spyware/.
- Muyinda, Paul. "MLearning: pedagogical, technical and organisational hypes and realities". *Campus-Wide Information Systems* 24, no. 2 (2007): 97-104.
- New Gen Apps. "Biggest Risks to Mobile Apps Security". November 28, 2018. Accessed April 15, 2020. https://www.newgenapps.com/blog/10-biggest-risks-to-mobile-apps-security.
- Patil, Vidyadevi. "Technologies used in E-learning". *Scholarly Research Journal for Humanity Science & English Language* 1, no. 2 (2014): 280-285.
- Positive Technology. "Vulnerabilities and threats in mobile applications". 2019. Accessed April 14, 2020. https://www.ptsecurity.com/ww-en/analytics/mobile-application-security-threats-and-vulnerabilities-2019/.
- Priya, R., and Jayanthi, J. "Security Attacks and Threats in E-Learning". *International Journal of Emerging Technology in Computer Science & Electronics* 21, no. 3 (2016): 629-633.
- Ruiz, del Puerto Paule M., M. Jesús Fernández-Díaz, Francisco Ortín Soler, Juan Ramón Pérez Pérez, J. R. P. "Adaptation incurrent e-learning systems". *Computer Standards & Interfaces* 30, no. 1-2 (2008): 62–70.

- Shah, Dhawal. "By the Numbers: MOOCS in 2015". December 21, 2015. Accessed April 15, 2020. https://www.classcentral.com/report/moocs-2015-stats/.
- Shonola, Shaibu Adekunle, and Mike Joy. "Security issues in E-learning and M-learning Systems: A Comparative Analysis". 2nd WMG Doctoral Research and Innovation Conference (WMGRIC2015), Warwick, United Kingdom, June 30th – July 1st, 2015.
- Shonola, Shaibu Adekunle, and Mike Joy. "Security of m-learning System: A Collective Responsibility". *International Journal of Interactive Mobile Technlogies* 9, no. 3 (2015): 64-70.
- Silver, Laura. "Smartphone Ownership is Growing Rapidly Around the World, but Not Always Equally". *Pew Research Center*, February 5, 2019. Accessed April 11, 2020 https://www.pewresearch.org/global/2019/02/05/smartphone-ownership-is-growing-rapidly-around-the-world-but-not-always-equally/.
- Traxler, John. "Distance Learning – Predictions and Possibilities". *Education Science* 8, no. 35 (2018): 1-35.
- UNESCO. "Half of world's student population not attending school: UNESCO launches global coalition to accelerate deployment of remote learning solutions". March 19, 2020. Accessed April 15, 2020. https://en.unesco.org/news/half-worlds-student-population-not-attending-school-unesco-launches-global-coalition-accelerate.
- World Health Organization. "WHO Director-General's opening remarks at the media briefing on COVID-19 - 11 March 2020". March 11, 2020. Accessed April 15, 2020. https://www.who.int/director-general/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020.
- Zuev, Vladimir. "E-learning security models". *Management* 7, no. 2 (2012): 24-28.

ANNEXES

TABLE 1 - Empirical analysis of the security of Mobile MOOCs used during the coronavirus

Mobile Learning application (mobile MOOCs)	Insecure data storage			Unintended data leakage		Insufficient transport layer protection		Poor authorization and authentication	Security decisions via untrusted inputs
	identity theft	reputation damage	external policy violation	the breach of user privacy leading to the unauthorized use of data;	people often get confused between unintended data leakage and insecure data storage	a hacker can gain access to the data and modify or steal it on his will	this results in frauds, identity threats etc.	poor or missing authentication allows a hacker to anonymously operate the mobile app or backend server of the mobile app	weak implementation of such hidden functionalities leads to improper app behaviour resulting in higher level permissions being granted off to an attacker
Google Classroom	✔	✔	✔	✔	✔	✔	✔	✔	✔
Edmodo	✔	✔	✔	✔	✔	✔	✔	✔	✔
Duolingo: Learn Languages	✔	✔	✔	✔	✔	✔	✔	✔	✔
Simply Piano	✗	✗	✗	✗	✗	✔	✔	✔	✔
Photomath	✗	✗	✗	✔	✔	✔	✔	✔	✔
Moodle	✔	✔	✔	✔	✔	✔	✔	✔	✔
ANTON	✔	✔	✔	✔	✔	✔	✔	✔	✔
Lingokids	✗	✗	✗	✗	✗	✔	✔	✔	✔
Seesaw Class	✔	✔	✔	✔	✔	✔	✔	✔	✔
Minecraft education	✔	✔	✔	✔	✔	✔	✔	✔	✔