Iğd Üniv Sos Bil Der / Igd Univ Jour Soc Sci
Ek Sayı / Supplement, Ekim / November 2020
Araştırma Makalesi / Article: 127-143

The Rise of Distance Education during Covid-19 Pandemic and the Related Data Threats: A Study about Zoom*

Ceren ÇUBUKÇU[1], Cemal AKTÜRK[2]

Geliş Tarihi: 01.09.2020 | Kabul Tarihi: 10.10.2020

Abstract: Covid-19 pandemic required all of the world to make changes in their regular routines. Especially, the formal education processes needed to be updated in order to keep the students safe and healthy. Many educational institutions forced to switch to distance learning for the rest of the semester so as to continue their education without interruption. Along with this switch, there has been a rise in the usage of learning management systems and webinar platforms and as a result, more data started to be generated causing big data to be formed. However, the switch to online education along with big data bring security and privacy challenges into surface. This study uses case study method and focus on Zoom platform to analyze these challenges. Zoom has been chosen for this study due to its popular use for online live classes as a free platform. Problems are discussed via Zoom. Moreover, solutions are proposed to solve these problems. Directing students to distance education against the Covid-19 pandemic and forcing them to use free online platforms can cause both the students and the instructors to face many big data threats that may affect their private lives. This study highlights these threats and the big data risks of Covid-19 in the distance learning environment. It distinguishes from other studies by not only discussing the problems but also offering tangible solutions. Literature lacks resolutions to data threats in free platforms especially in education industry and this study aims to fill this gap by its contribution.

Key Words: Covid-19, Distance Education, Big Data, Security, Privacy

* This paper was presented as abstract paper at Online International Conference on Covid-19 on 12-14 June 2020.

[1] Maltepe University, Faculty of Engineering and Natural Sciences, Computer Engineering, ceren.cubukcu@gmail.com, ORCİD ID: 0000-0002-9253-2826

[2] Gaziantep Islam, Science and Technology University, Engineering and Natural Sciences Faculty, Computer Engineering Department, Cemalakturk79@gmail.com, ORCİD ID: 0000-0003-3764-3862

Covid-19 Pandemisi Sırasında Uzaktan Eğitimin Yükselişi ve İlgili Veri Tehditleri: Zoom Hakkında Bir Çalışma

Öz: Covid-19 salgını, tüm dünyanın düzenli rutinlerinde değişiklik yapmasını gerektiriyordu. Özellikle örgün eğitim süreçlerinin öğrencileri güvenli ve sağlıklı tutabilmek için güncellenmesi gerekliydi. Birçok eğitim kurumu, eğitimine kesintisiz devam etmek için dönemin geri kalanında uzaktan eğitime geçmek zorunda kalmıştır. Bu geçiş sürecinden dolayı öğrenme yönetim sistemleri ve web semineri platformlarının kullanımında da bir artış olmuş ve büyük verilerin oluşmasına neden olan daha fazla veri üretilmeye başlanmıştır. Bununla birlikte, çevrimiçi eğitime geçiş büyük veriyle de birleşince güvenlik ve gizlilik sorunlarını ortaya çıkarmaktadır. Bu çalışma, bu zorlukları analiz etmek için vaka çalışması yöntemini kullanıp Zoom platformuna odaklanmaktadır. Zoom, çevrimiçi canlı sınıflar için ücretsiz bir platform olarak çok tercih edildiğinden dolayı bu çalışma için seçilmiştir. Sorunlar Zoom platformu üzerinden tartışılmaktadır. Ayrıca bu sorunları çözmek için çözümler önerilmektedir. Öğrencileri Covid-19 pandemisine karşı uzaktan eğitime yönlendirmek ve ücretsiz çevrimiçi platformlar kullanmaya zorlamak, hem öğrencilerin hem de eğitmenlerin özel hayatlarını etkileyebilecek birçok büyük veri tehdidiyle karşı karşıya kalmalarına neden olmaktadır. Bu çalışma, bu tehditleri ve Covid-19'un uzaktan eğitim ortamındaki büyük veri risklerini vurgulamaktadır. Sadece sorunları tartışmakla kalmayıp aynı zamanda somut çözümler sunarak diğer çalışmalardan ayrılmaktadır. Literatür, özellikle eğitim sektöründeki ücretsiz platformlarda veri tehditlerine karşı çözüm getirmemektedir ve bu çalışma bu eksiği gidermeyi amaçlamaktadır.

Anahtar Kelimeler: Covid-19, Uzaktan Eğitim, Büyük Veri, Güvenlik, Gizlilik

Introduction

The delivery of education to students, who are not physically present, with the help of satellite, video, audio, graphic, computer and multimedia technologies is defined as distance education (USDLA, 2020; Egypt, 2007). The learner and the teacher started to come together on a platform called the learning management system (LMS) and continue their education activities with the mediation of internet technologies. LMS can be analyzed in two groups as those sold as commercial products and those distributed free of charge with an open source code. Some examples of commercial LMS products are Blackboard, ANGEL Learning, eCollege and these are the most known ones (Ozan, 2008). There are around 50 platforms worldwide as open source LMS. The most widespread of these are Moodle, Sakai, Atutor, Dokeos, Claroline and OLAT (Reis et al., 2012). In a study, 18 open source and commercial LMS were examined with various dimensions and 6 LMS consisting of Moodle, Dokeos, Learning Space, Kewl-Nextgen, Angel and Blackboard were shown to be preferable as a result (Aydoğdu Karaaslan, 2019). Among these LMS's, Blackboard, Angel and Learning Space are commercial and others are open source.

In parallel with the developments in internet technologies, many data are collected by means of tools such as e-commerce applications, blog and social media platforms. By analyzing the big data obtained by these platforms; it is possible to produce many commercial and scientific services in the fields of education, health, security and industry. Along with the rise of distance education and the use of LMS in the field of

education, all transactions and movements of the students on the learning platforms have begun to be analyzed with big data analytics. For example, all activities such as students' working times for a course content, the number of logs in the system and the length of their stay in the system, courses in virtual classrooms, and participation rates in the forum and discussion boards, the completion status of the course's assignment or project are being examined in learning analytics as big data.

Learning analytics is a concept that emerges by using big data in the field of education. It is used as a concept that covers many processes such as managing the learning and teaching processes in education, recruitment activities, financial planning and monitoring the students' academic performances (Songsangyos & Nilsook, 2015). It is stated that almost a third of students in America prefer online and blended learning (Picciano, 2012). Learning analytics is used to improve the existing learning environments accordingly by finding out the platforms where students interact better in order to decrease the dropout rate in the USA. Such platforms that increase students' interactions contribute to the reduction of school dropout rate by increasing success and interest in learning (Al-Kabi & Jirjees, 2019; Feinleib, 2014).

Recently, tools such as Google class, Zoom, Edmodo started to be used for free for virtual classroom purposes for e-learning, although they do not have extensive functions such as LMS (Oe, 2019; Tekin Poyraz and Özkul, 2019). In fact, it is stated that Google class is a competitor of Moodle due to its ease of use, flexible structure, openness to everyone and being mobile

(Tekin Poyraz & Özkul, 2019). In a study evaluating the use of social media in learning activities, Edmodo has been shown to be evaluated by students with a high score, since it has a Facebook interface. In the same study, despite the positive opinions of the teachers, it was stated that they had difficulty in preparing content on this platform (Dinçer & Balaman, 2019).

Due to the spread of the Covid-19 global epidemic, countries have stopped formal education activities and quickly switched to distance education with video conferencing programs and virtual classroom platforms. The Zoom platform, which is frequently used worldwide for this purpose, provides free, audio, video, screen sharing, recording and messaging rights for students and learners in sessions up to 40 minutes (Yaylak et al., 2020).

In a study conducted, it has been stated that invited speakers who have never used Zoom before have connected to Zoom from different states via an email link sent and held a successful training meeting for a vocational education seminar in the field of health (Halpin & Lockwood, 2019). It was shown to the educators in Africa that the training provided by the educators in America with 18 Zoom sessions within the scope of an international project is very beneficial. It was emphasized in the same study that although the trainings were done by video conferencing method, the participants were influenced by each other's culture and that the video conferencing method was too low in cost and sustainable enough compared to face-to-face training (Scanga et al., 2018). The zoom platform is used not only in learning activities but also as a scientific data collection

method. In a study, the feasibility of using the Zoom platform for a qualitative data research in the field of health was investigated. As a result of the study, it was shown that Zoom was evaluated more positively than face-to-face, telephone conversation and other video conference platforms, although it was reported that many participants experienced technical problems (Archibald et al., 2020).

2. Methods

The global COVID-19 pandemic brought a lot of changes into our lives. In order to protect the health of human beings, governments forced their citizens to transition their work, education and social lives to online platforms. Especially, with the shutdown of schools, millions of students around the globe started to get their education at home through distance learning environments such as television and the internet. Some schools including universities were already using learning management systems (LMS) for their classes. However, the schools without a LMS were forced to find out quick and inexpensive solutions in order to continue their classes. Therefore, they went towards using free platforms such as Zoom especially for their live classes.

The rise of using online platforms such as Zoom caused the inclination of data generation. Especially, due to online education, student and classroom data have increased rapidly. This raise obviously brought new challenges in terms of security and privacy of data. The biggest risks are present in free or open sources platforms. Unfortunately, big data cannot be controlled by traditional methods and verifying this control re-

quires more attention to security and privacy issues. The aim of this study is to draw attention to the security and privacy risks that will arise in this regard, and to make some recommendations regarding the precautions to be taken, as free distance learning platforms becomes more widespread and challenges related with these becomes more of an interest in education.

This study focuses on Zoom platform for discussing the problems of big data in online education. The problems will be explained through the case study of Zoom platform and in the upcoming section, solutions to these problems will be suggested. This study distinguishes from other studies about distance learning by not only examining the problems of a rising and free platform but also offering tangible solutions. Literature lacks resolutions to big data problems in education industry and this study aims to fill this gap by its contribution.

3. Case Study of Zoom

The biggest challenges for online education is data security and privacy. During the COVID-19 global pandemic, the data creation has increased tremendously and therefore, questions started to rise about how this data will be stored, collected, used and who will have permission to access it. Aside from the primary uses of this data, the secondary uses should also be considered. The following questions need to be answered about the data collection process; “Does this data really need to be collected?”, “How is this data going to be monitored, measured and mined?”, “Who will use this data- schools, universities, teachers, educational ministry, government?”, “What is going to be done with the trends, analysis and patterns in the data?”.

As of March 2020, due to Coronavirus outbreak in the world, many countries shut down the schools and continue the education online. Therefore, millions of students around the world currently receive their education using an LMS system. As a result, the security of these systems gained importance more than ever. The security and privacy problems are much bigger if the schools are using an open source or free platform as in the case of Zoom for their online classes. Zoom had 10 million active users in December 2019. Along with the pandemic, the number of active users have raised to 200 million as of April 2020. This remarkable raise makes Zoom a tempting target for hackers.

According to a recent discovery by IntSights' researchers, over 500,000 account credentials of video conference platform Zoom are being sold on the darknet and hackers have shared a database containing 2,300 records (Maor, 2020). In these records, the usernames and passwords of Zoom accounts are available. These accounts include corporate accounts belonging to banks, consultancy companies, educational facilities and schools, software vendors, and healthcare providers. Researchers also found out that there are various posts and threads of dark web forum members discussing different approaches of targeting Zoom's conferencing services (Townsend, 2020).

A new terminology called "Zoombombing" also came into surface when Zoom started to be used widespread. Zoombombing means the practice of hijacking video conferences as an uninvited party. Cybercriminals find Zoom calls to join

without an invite and they use an online tool called zWarDial. This is an automated tool that tries to find an ID which works. If there's no password on a meeting, the intruder will be instantly added to the call. They either share disruptive or offensive comments or media through screen sharing feature. In one class of a Massachusetts high school, a cybercriminal joined the live class and flashed the emblem of the German Nazi party (Holmes, 2020; Sayed, 2020).

There are also data leakage problems in Zoom. According to Business Insider, Zoom's reliability is a big question because it has been accused of passing on data to third parties, including Facebook, without notifying the users (Karnam, 2020). There is a security vulnerability in Zoom because Zoom uses "transport encryption" which is less secure compared to "end-to-end encryption" (E2EE) used by many other businesses over the internet when sending the data. In E2EE only communicating users can read the messages and prevents third parties from being able to hack and decrypt that data. Therefore, it is much more reliable for sending data over the internet.

Another major problem with the online classes through Zoom is privacy. Zoom not only collects name, physical address, email address, phone number and school information but also your IP address and the model of your device. There is also an attendee attention tracking feature in Zoom which notifies the owner of the meeting whether you are paying attention or not. If you are away from the meeting for more than 30 seconds, the host of the meeting is notified. However, there is a fine line between controlling the attendance of students and make them

feel that a "big brother" is watching (Picciano, 2012). Some students may feel their privacy is getting invaded due to this approach and may fear that this might be used against them in the future.

If you use Facebook to log into Zoom, it also collects information from your profile and analyze this data. In Zoom's privacy policy, it mentions that it doesn't sell personal data for money to third parties, but it shares personal data with third parties for "business purposes." This raises serious questions about its trustworthiness. Also, Zoom meeting URLs can easily be shared everywhere together with the meeting id. Therefore, anyone with the meeting id and URL can join the call. This has allowed cybercriminals to sneak into calls using publicly shared links and then take over the meeting. This is a big threat for the privacy of the meeting participants since cybercriminals can reach any data related to the meeting once they are in the call. In order to prevent this problem, many schools do not permit the use of Zoom for online classes. For example; Leiden University in Netherlands announced that it does not permit the use of Zoom because of privacy risks (Leiden University, 2020). The Education Ministries of Singapore and Taiwan also banned Zoom due to the security and privacy risks along with the education department in New York City (Vigliarolo, 2020).

4. Solutions

In this section, solution recommendations will be given towards the security and privacy problems discussed in the previous section.

In order to solve the security problems of Zoom and make data more safe, disaster recovery plans and strong password policies should be in place. Also, the most recent versions of firewalls, anti-virus software and encryption techniques should be implemented. Zoom announced on April 30th that Zoom 5.0 supports AES 256-bit GCM encryption. A system-wide account enablement to GCM encryption will occur on May 30, 2020 and only Zoom clients on version 5.0 or later will be able join Zoom calls. Therefore, Zoom is already making progress for a more secure encryption method.

Another method that Zoom can use to improve its security against cybercriminals is that Zoom can hire white hackers as employees or create a cyber-security competition to find the vulnerabilities of its system. For example; tech giants such as Google and Microsoft hired teenagers who hacked into their systems and showed them their bugs (Jackson 2011; Sharma 2015). Zoom can also follow this methodology to both improve their systems and direct the students' talents to a better purpose creating a win-win situation for all.

The security of the data can be protected by keeping track of the logs very carefully and by increasing the security measures for joining the meetings. Nonrepudiation security principle should be in place for system logs. In case, the data in the system is changed by unauthorized people, unauthorized data use and data processing must be prevented. Also, 2 Factor Authentication (2FA) can be used for joining the meetings. Along with the meeting password, an SMS code can be sent for verification for joining the meeting with this 2FA method.

In order to ensure the privacy of data, Zoom can be more transparent about its privacy policy. It can be more clear about how the data is processed, stored and who have access to this data. The data center used to store the data is also another concern for the users of Zoom. However, Zoom already announced that along with the new Zoom 5.0 version, the meeting hosts will have a chance to select their data center regions. The Zoom client will show which data center the user is connected and the user can also get additional details through the video settings.

Zoom is obviously not the only alternative to make online meetings or webinars. There are similar and more secure platforms such as Google Meet, AnyDesk, Skype, GoToMeeting and etc. Furthermore, using an LMS platform is a much better and safer alternative compared to using webinar platforms. There are many open source LMS platforms such as Moodle, Sakai, and etc. These are generally free to use and better suited for running classes as you can also use these platforms for grading the students. Schools and universities can also develop their own LMS system. However, the Covid-19 process was unexpected and therefore, the schools and universities didn't have enough time to develop an LMS system. For this reason, they used whatever free system they could find and Zoom was one of them. Nevertheless, Zoom's privacy policy is not very clear about what they do with the recorded meetings and that is why there is a privacy threat. Thus, it is recommended to use other LMS alternatives which has a clear privacy policy.

Governments or Education Ministries can restrict the use of webinar platforms or LMS systems which they do not find secure. As mentioned above several governments bring restrictions to the use of Zoom platform. They can publish a list of recommended platforms for education or develop a local LMS or webinar system. In Turkey, Education Ministry use EBA platform for primary and high school education. However, the universities in Turkey can choose between any platform they want. Also, using more than 1 LMS or webinar platform can be a good alternative for diversifying the security and privacy risks.

Conclusion

The Covid-19 pandemic and the closure of schools have forced the education system around the world to switch to online platforms such as Zoom in order to continue the education online. However, Zoom has major security and privacy issues and due to its current popularity during this process, it is within the target of cybercriminals. Although it is constantly updating itself and the switch to Zoom 5.0 version on May 30 is resolving some of these security and privacy issues, there are still many concerns related to the usage of the data which is getting stored. Therefore, governments and school officials should take precautions and protect student data against all kinds of security and privacy violations. In Turkey, there is the law of personal privacy (KVKK) which protects the data privacy of individuals. Nevertheless, this is a very broad law for all the data that is being stored in general and not specific to online education or the students.

One option for protecting and securing data is using alternative webinar platforms that are more secure such as Google Meet, AnyDesk, Skype or using open source LMS platforms such as Moodle, Sakai, and etc. The governments and education ministries can analyze these platforms and provide the list of approved distance learning and webinar platforms to schools and universities or support them developing their own in-house platforms. Finally, open source learning management system and webinar platforms can be developed centrally by the governments. The databases of these applications should be stored centrally in cloud systems without being left to the initiative of other third party companies. The biggest concern of everyone is who owns the data. In this case, the answer to this question will be the government as the greatest authority and as a result, the security and privacy concerns of students and instructors will be mitigated.

References

Al-Kabi, M. N., & Jirjees, J. M. (2019). Survey of Big Data applications: health, education, business & finance, and security & privacy. Journal of Information Studies & Technology (JIS&T), 2018(2), 12.

Archibald, M. M., Ambagtsheer, R. C., Casey, M. G., & Lawless, M. (2019). Using Zoom Videoconferencing for Qualitative Data Collection: Perceptions and Experiences of Researchers and Participants. International Journal of Qualitative Methods, 18, 1609406919874596.

Aydoğdu Karaaslan, I. (2019). Açık Kaynak Kodlu Ve Ticari Web Tabanlı Uzaktan Eğitim Yazılımlarının Karşılaştırılması. Journal of International Social Research, 12(62, 979-990.

Dinçer, S., & Balaman, F. (2019). Sosyal Medyanın Öğretim Faaliyetlerinde Kullanılmasının Öğrenci, Öğretmen ve Veliler Açısından Değerlendirilmesi: Edmodo Örneği. Trakya University Journal of Social Science, 21(2), 887-908.

Feinleib, D. (2014). Big data bootcamp: What managers need to know to profit from the big data revolution. Apress.

Halpin, P. A., & Lockwood, M. K. K. (2019). The use of Twitter and Zoom videoconferencing in healthcare professions seminar course benefits students at a commuter college. Advances in physiology education, 43(2), 246-249.

Holmes, A. (2020). Protect your Zoom meetings with a password now — otherwise, you're leaving the door wide open for hackers to 'Zoom-bomb'. Retrieved 22 May 2020, from https://www.businessinsider.com/protect-zoom-meetings-password-hackers-zoom-bombing-2020-4

Jackson, N. (2011). Yahoo is now a part of Verizon Media. Retrieved 23 May 2020, from https://finance.yahoo.com/news/Microsoft-Youngest-Employee-atlantic-533735795.html

Karnam, S. (2020). Top 5 security challenges with Zoom video conferencing | Sumo Logic. Retrieved 24 May 2020, from https://www.sumologic.com/blog/zoom-security-challenges/

Leiden University. (2020). Coronavirus updates. Retrieved 20 May 2020, from https://www.universiteitleiden.nl/en/dossiers/coronavirus-en/updates-en

Maor, E. (2020). Zooming in on the Target: Cybercriminals Automate Attacks Against Remote Workers. Retrieved 20 May 2020, from https://intsights.com/blog/zooming-in-on-the-target-cybercriminals-automate-attacks-against-remote-workers

https://scholarworks.boisestate.edu/under_conf_2019/123

Mısırlı, Z. A. (2007). Web Tabanlı Öğrenme Yönetim Sistemine İlişkin Öğrenci ve Öğretmen Görüşleri. Yükseklisans Tezi, Balıkesir Üniversitesi Fen Bilimleri Enstitüsü, Balıkesir.

Oe, Emily and Schafer, Ellen, "Establishing Presence in an Online Course Using Zoom Video Conferencing" (2019). 2019 Undergraduate Research and Scholarship Conference. 123.

Ozan, Ö. (2008). Öğrenme Yönetim Sistemlerinin (Learning Management Systems-Lms) Değerlendirilmesi. XIII. Türkiye'de İnternet Konferansı.

Picciano, A. G. (2012). The evolution of big data and learning analytics in American higher education. Journal of asynchronous learning networks, 16(3), 9-20.

Reis, A. Z., Baktır, H. Ö., Çelik, B., Erkoç, M. F., Özçakır, F. C., Özdemir, Ş. ve Şahin, K. (2012). Açık kaynak kodlu öğrenme yönetim sistemleri üzerine bir karşılaştırma çalışması. Eğitim ve Öğretim Araştırmaları Dergisi, 1(2), 42-58.

Sayed, A. (2020). Zoom Banned in Schools over Security Concerns. Retrieved 22 May 2020, from https://thespokesman.net/3453/news/zoom-banned-in-schools-over-security-concerns/

Scanga, L. H., Deen, M. K. Y., Smith, S. R., & Wright, K. (2018). Zoom around the World: Using Videoconferencing Technology for International Trainings. Journal of Extension, 56(2), n2.

Sharma, A. (2015). Google Hired 18-year-old: Kid Now Serves 1000 Businesses and Just Got $15 Million. Retrieved 26 May 2020, from https://fossbytes.com/google-hired-18-year-old-kid-now-serves-1000-businesses-and-just-got-15-million/

Songsangyos, P., & Nilsook, P. (2015). Big Data in the Cloud for Education Institutions. In The Twelfth International Conference on eLearning for Knowledge-Based Society.

Tekin Poyraz, G. ve Özkul, A. E. (2019). Bir öğrenme ortamı olarak Google Sınıf'ın incelenmesi. AUAd, 5(3), 8-27.

Townsend, K. (2020). Zoom Credentials Database Available on Dark Web | SecurityWeek.Com. Retrieved 21 May 2020, from https://www.securityweek.com/zoom-credentials-database-available-dark-web

USDLA, United States Distance Learning Association: "Definition of Distance Learning", http://www.usdla.org, Erişim Tarihi: 12.05.2020.

Vigliarolo, B. (2020). Who has banned Zoom? Google, NASA, and more. Retrieved 25 May 2020, from https://www.techrepublic.com/article/who-has-banned-zoom-google-nasa-and-more/

Yaylak, F., Özcan, G., & Gülbandılar, E., (2020). Etkin Sanal Öğretim için Rehber. Eskişehir Türk Dünyası Uygulama ve Araştırma Merkezi Bilişim Dergisi, 1(2), 25-28.