**American Journal of Software Engineering and Applications**
2022; 11(2): 31-37
http://www.sciencepublishinggroup.com/j/ajsea
doi: 10.11648/j.ajsea.20221102.12
ISSN: 2327-2473 (Print); ISSN: 2327-249X (Online)

# The Fundamental Use of Videoconferencing in Online Teaching

**Biclea Diana**

Department of Mathematics and Computer Science, Lucian Blaga University of Sibiu, Sibiu, Romania

**Email address:**
diana.biclea@ulbsibiu.ro

**To cite this article:**
Biclea Diana. The Fundamental Use of Videoconferencing in Online Teaching. *American Journal of Software Engineering and Applications*. Vol. 11, No. 2, 2022, pp. 31-37. doi: 10.11648/j.ajsea.20221102.12

**Received**: July 23, 2022; **Accepted**: August 8, 2022; **Published**: September 16, 2022

**Abstract:** The usage of the VM apps poses a degree of vulnerability to multiple privacy and safety risks. Within this article are presented certain aspects related to the usage of such apps, what to consider when using them during the training procedure and video meetings. The date gathered based of this paper on the analysis of VM applications, the establishment of some common characteristics, their most important and useful characteristics have been highlighted. Videoconference apps have been successfully used within training sessions during the pandemic, without taking into consideration the security, privacy and massage of such technological tools. A survey was conducted on the security and vulnerability aspects of the applications used by the teacher. It was sought the degree of knowledge of these problems. It was seen that the discussions held in video format occupy over 60% of the multimedia methods used in online classes. The exceptional utilization increased utilization of VM apps, it should be noted that cyber security problems connected to such techniques should be given an increased attention. One cannot imagine a teaching-learning procedure without having an online video meeting. As such, in the following chapter, are detailed solutions for teleconferences and the security aspects adherent to such and we conducted on the degree of use of VM applications, the application of security techniques and recommendations for a better application of VM applications.

**Keywords:** Education, Video Conferencing, Privacy, Abuse, Security

## 1. Introduction

The situation arising from the pandemic forced us to use modern methods of training by applying information technologies. At the same time, it made us more cautious about the technologies used to achieve a correct teaching process and with the same aims as in the case of face-to-face learning.

Any decision regarding classroom or virtual teaching is filled with implications and compromises that are difficult to assess, both nowadays as well as for the long-term. All these are but a fraction of the complex reality of functionality within a pandemic.

In the early days of the corona virus pandemic, many schools and educational institutions around the world have been forced to move on quickly to fully distanced models of learning, having little or no training at all [1, 16]. Parents and other guardians – more often than not grandparents and children must adapt to the new aspects at home, at school and at work, on the background of news and guidelines found under continuous evolution of the Corona virus. Often, parents and guardians found themselves offering additional support as "teachers" while children received schoolwork via text messages, web sites and e-mails. This aggravated the stress of living jam-packed together in one home for longer periods of time.

In other countries, this aspect was settled in a different way with most children being granted a postponement from school and from the complexity of remote learning during the summer months, while in other countries, teachers continued to work from home using videoconference methods and other technologies [20, 23]. By implementing several measures, this adaptation to remote working went remarkably well.

In this article a study is made of the application of video conferencing in the teaching process, some recommendations are given to improve the teaching process with video applications. The paper is a generalization of the paper [13] with other details regarding the main aspects we take into account when talking about the security and vulnerability of VC applications.

For many teachers in Romania and the Republic of Moldova, there have been great challenges regarding the use of information technologies in online teaching. They tried various ways to collaborate with students and not to lose the content of the curriculum. Even telephones were used for message communication, worksheet transmission with applications: WhatsApp, Viber, Messenger. But they have not been and are not enough to organize a proper teaching process. Free courses were organized in each institution, where teachers were trained and prepared for any form of online or physical teaching.

Thus, the statistical data show that in Romania 80.8% of the population have internet connection, in urban areas, 86.9% in rural areas only 73.1% of households [29]. In the Republic of Moldova, Internet access is 83%, including internet access, mobile internet, internet access in urban areas 62% and rural areas 42% [30].

These statistics also show us the accessibility of teachers and students to the internet, the access to the digital devices used.

The video conference is essential for distance education. Schools are using technology in a record number to conduct classes, to support school events and meetings, to offer advice and counseling, and to facilitate students and teachers alike to connect with friends and colleagues [6, 9, 10, 11, 16]. As any other technology, if it's not properly managed, video conferencing presents risks regarding students and employees' confidentiality and also the security of our personal information. Schools that are using this technology must be aware of these risks and they should have to implement protection measures in order to alleviate or prevent them.

During the pandemic, virtual meeting solutions like Zoom, Microsoft Teams or Google Meet have become well-known names and they have been highlighted by mass-media as viable solutions to meet the demands of distance education.

The videoconference technology is available via dedicated hardware, conference rooms, computers and mobile devices in order to facilitate communication anywhere a person has Internet access. In theory, this allows for a permanent contact with any other person using as many senses as possible in order to convey a massage, to discuss a topic or to offer training and education. This implies cameras, microphones, splitting the screen, surveys, file partition, instant messaging, chat, enhancing the background, noise cancelling and even attention monitoring technologies [14, 19].

A VM app is a method used by people to meet, regardless of their whereabouts, via video, audio and text and to connect or meet online rather than face to face [13, 17, 22]. It allows for a direct share of information without it being necessary to be at the same location. The setting up of VM rooms is considered cost efficient compared to travelling for short-period meetings. This option is less upsetting for office schedules and activities [1]. The usage of VM techniques poses multiple security issues that vary from unencrypted communication for the free accounts to significant issues taking the form of vulnerabilities that allow malware programmes to run on the user's devices.

# 2. Research Methodology

We analyzed the information related to the subject studied from several current sources. We conducted a survey on the degree of use and knowledge of the security and vulnerability of applications: Zoom, MS Teams, Google Meet. A list of guidelines has been developed to address security and vulnerability issues.

Choosing the right tool can pose a difficult problem, especially if one intends to use it for training sessions. The higher the risk all participants assume during a call the less compromises when selecting the venue hosting the conversation. The present article presents the security and privacy functions necessary to be taken into consideration when deciding on the platform used during the training procedure.

For a proper evaluation of video conferencing instruments, we need to consider the following aspects [4, 5, 7, 8, 13, 15, 20]:

1) Assessing the security properties of the platform.
2) Assessing the confidentiality properties of the platform.
3) Protecting users from abuse and prioritizing accessibility needs.

When we evaluate the security of any instrument, we are looking for signs that the platform takes into consideration very seriously the need to protect our data [24]. Besides granting technical warranties that limit the chances that the personal data will fall in the wrong hands, a service provider that deals with the safety features is also liable for the quick and transparent resolve of data breaches [2].

For daily meetings within a closed format, when only a small number of people will connect, the transit encryption industry standard [4] meets the safety requirements. Should privacy be needed for a video conference or a lesson displaying sensible material, it is necessary to search for a tool that accepts the end-to end encryption [7, 20].

Concerning platform safety, the following must be taken into consideration [13]:

1) A 2-step authentication and the authentication methods.
2) Encryption in transit and its' implementation techniques.
3) End-to end encryption and its' implementation techniques.
4) The existence of an independent safety audit.
5) Troubleshooting offered for the identified vulnerabilities.

We understand that in fact, not just any meeting needs a strict confidentiality; in fact, sometimes we may want a call to be streamed to a wide audience [15]. When privacy is important for us and for the participants to the call, we give priority in selecting a platform that collects very little or close to none information about the participant account, that registers only limited metadata during calls and does not share data concerning the users with third parties. A necessary aspect is to study the privacy promised by the platform and to realise just how well it fulfils our requirements.

There are a multitude of specifications regarding the privacy of the platform that we need to take into consideration when thinking about using a videoconference platform during a training session [19, 21]:

1) Usage of the platform without an account.
2) The metadata and content registered by the user.
3) The storage period of the user's data after he/she deleted or closed his/ her account.
4) The possibility of self-hosting.
5) The drafting of an annual transparency report.
6) The signalling warnings for the user's requests concerning his/her data.
7) The existence of certain public documents making reverence to the applicability of the law and regarding the processing of user data.
8) Usage safety without abuse and its' simple applicability.

When communicating with students, it is important to do so in the safest and most comfortable environment as possible.

The online abuse can become aggressive if it's left uncontrolled, especially since online lessons involve students who present a higher risk of being targeted by online harassment.

In cases where there is a possibility that a student from our call would say, send spam or share abusive content, we may want to use an instrument which provides features as password protection on the meeting's link and the disabling or elimination of the abusive call participants.

To participate in a video call, certain students require visual and audio assistance. These accessibility features can take the form of real time subtitles during the dialog or the projection of the interface in a way that crosses well with screen readers [2].

To make sure that a video conferencing instrument meets our minimum standards, this instrument has to be assessed according to all criteria in order to prioritize all accessibility needs.

*Google Meet* represents the main video chat tool launched by Google to be used by organisations and businesses, also called Google Workspace. In the future, Google Meet will also replace the older version of Google Hangouts [13, 26]. The service is not end-to end encrypted, and the users' data can be decrypted by the company. In order to simplify their service, compared to other Google offers, Meet is connected to the user's Google account. The company regularly surveys exceptional attempts to access your account and makes available a 2-step factor authentication in order to prevent another user from connecting. While using Goole Meet, participants will also be notified if someone is trying to join the meeting from outside the organisation. When Google Meet is embedded into Google Workspace, the organisation must have an administrator (admin) who, at his/ her option, can further block or limit the functionality of Google Workspace.

*Teams* is a relatively new product which to a great extent managed to shy away from the attention given to Zoom, while in the meantime rapidly increasing its user database [8] ever since the start of the Covid-19 pandemic. Its set of functions overlays many competing platforms, but the activity of the necessary functions, as in the case of other Microsoft offers, requires the exact finding of the corresponding account type combination, subscriptions and corresponding services. Moreover, its own default settings [12, 27] could, under certain conditions, be prone to attacks similar to those for which Zoom became famous [18].

The Zoom safety, privacy and abuse issues were well documented. The Zoom story is deeply rooted in the COVID-19 pandemic when millions of users switched to this platform for trusted video calls. Zoom was initially designed to implicitly allow anybody to join video calls. Due to the fact that joining a call could be that easy, it was exceptionally convenient for unwanted users to join in, most times causing havoc [3, 13]. Furthermore, their documentation and interface provided misleading statements [7, 25] regarding their encryption quality level. Following the large-scale control from the safety community, significant improvements have been implemented regarding safety, privacy and abuse issues encountered on this platform.

# 3. Results

After a while of using video dating applications, teachers learned how to use them and of course notice the pros and cons of using them. If teachers are not computer engineers, they can not notice some vulnerabilities in the use of these applications, but have difficulty implementing or improving them.

We did a survey on the degree of satisfaction and knowledge of these applications. Some used only one VM application, others used two or even all three applications.

We can list the main recommendations regarding VM of the 3 listed, all three generally have the same security measures only different only as a configuration - the effect is the same.

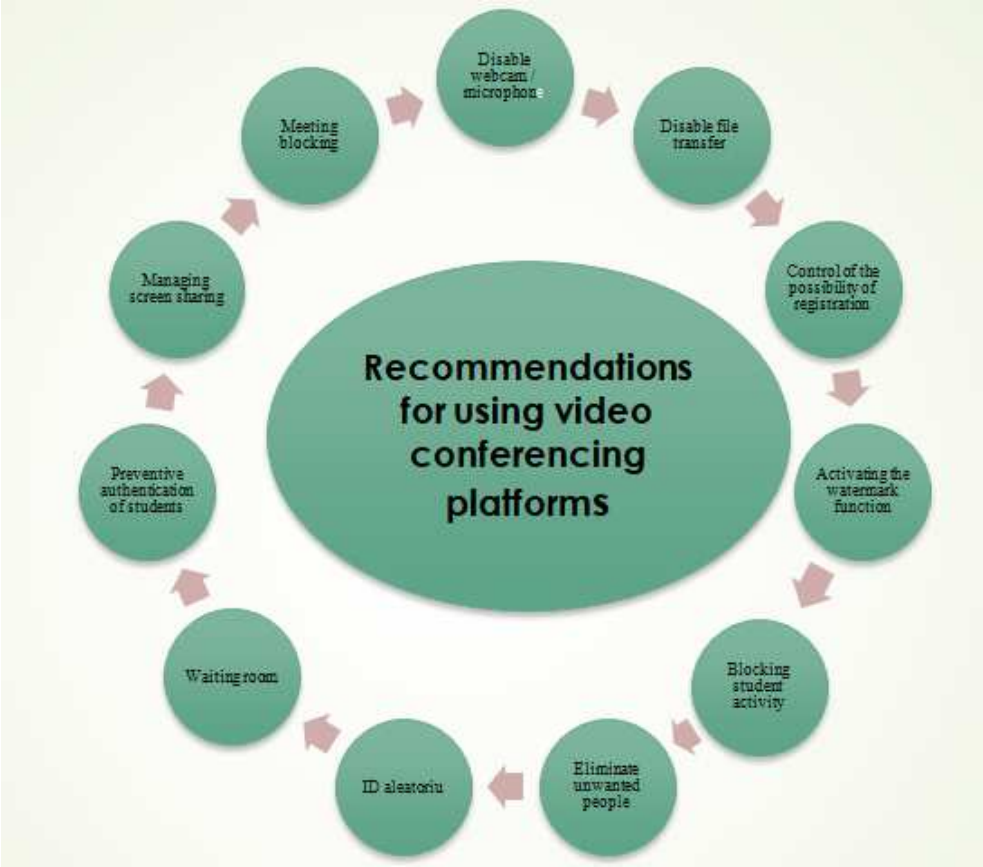
1) Avoid the use of personal meeting ID;
2) Use a randomly generated meeting ID;
3) Set up an appointment with a password;
4) Preventive authentication of students;
5) Only authenticated users can join meetings from Web client;
6) Screen sharing management;
7) Enable watermark sharing;
8) Blocking the activities of the participants.

More specifically for each VM application we have:

1. VM Zoom. Securing the use of the Zoom application can be divided into 2 steps: settings before starting the meeting and settings during the meeting. Before you start a lesson, there are some steps you can take to help reduce your chances of being interrupted by someone unwanted.
2. Microsoft Teams. The recommendations are the basis of Microsoft's official recommendations and can successfully serve as a theoretical basis for a security policy in the use of the Microsoft Teams application.

The first step, which is not just about Microsoft Teams, is to keep the app up-to-date with both us and students - so we can be sure that we'll benefit from the latest security settings.

3. Google Meet charms teachers with ease of use and integration with other Google components, such as Google Classroom. Configuring security settings when planning or conducting a lesson is as simple as [28].




Source: Authors

***Figure 1.*** *Recommendations for using video conferencing platforms.*

## 4. Discussions

Users are usually the weakest link in the security chain So the user's private security when using the VM application depends on the user himself. When an user joins a call through a video conferencing application from an insecure device or connection, they become vulnerable to unauthorized access.

The main point in VM applications is secure access, which means preventing the annoying intruder from signing up and gaining access to the data or devices of any meeting participant. VM applications such as Zoom, Google Meet, and Microsoft Teams provide the ability to easily set up to meet with teachers, classmates, workgroups, friends, and family members.

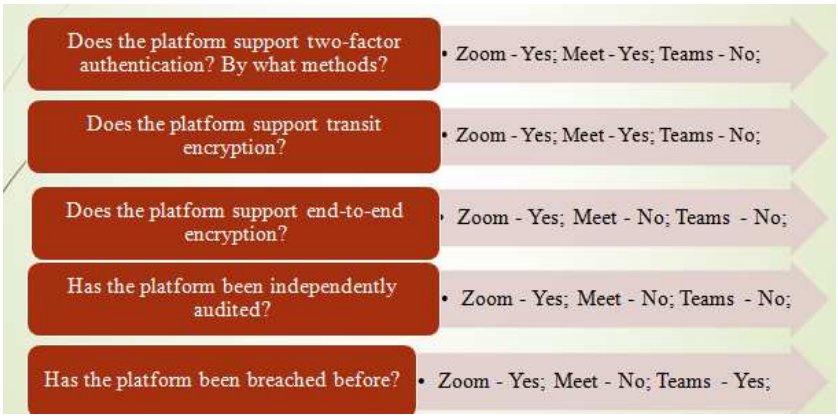
However, that ease of application could also make it easier for attackers to access information. The main idea is to be aware of the security risks before participating in a video call with students or a group of colleagues by properly configuring the functions of VM applications to exclude malware, hackers and identity thieves.

| | |
|---|---|
| Can I use this platform for closed lessons? | • Zoom - Yes; Meet - Yes; Teams - Yes; |
| Can I control who can access my call if I want to? | • Zoom - Yes; Meet - Yes; Teams - Yes; |
| What is the maximum size of the meeting group? | • Zoom – 100 - 1000; Meet – 100 - 250; Teams – 100 – 10 000; |
| Are there accessibility features - screen reader, transcript? | • Zoom - Yes; Meet –Yes; Teams - Yes; |
| Is there a way to remove participants from the call? Chats | • Zoom - Yes; Meet – Yes; Teams - Yes; |

Source: Authors

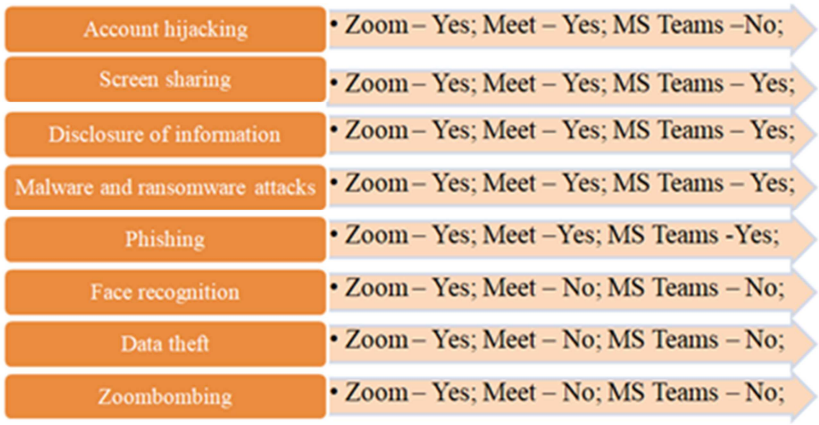
***Figure 2.*** *Aspects to prevent abuse in the use of video conferencing technologies.*

In terms of cybersecurity it is possible to attack them on the applications mentioned above, such as hijacking, screen sharing, information disclosure, malware, phishing, data breach and zoombombing [13].



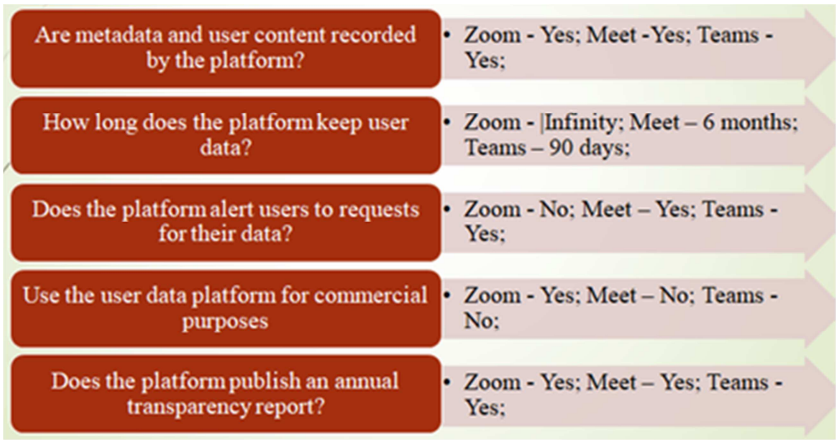

Source: Authors

***Figure 3.*** *Security issues in the use of video conferencing technologies.*




Source: Authors

***Figure 4.*** *Evaluation from the perspective of cyber security.*




Source: Authors

***Figure 5.*** *Confidentiality in the use of video conferencing technologies.*

Confidentiality is another concern. VM's privacy policies may allow the collection and storage of a large amount of data from many resources (for example, cloud recordings, videos, messages, files, on-screen documents, and whiteboards displayed during hours), and such data would may contain sensitive personal information. The webcam provides a window into the world of schooling through which hackers can spy on the participant when he

accidentally left the webcam activated. Another example of the issue of privacy is when hackers gain access to legal or financial information whenever students or teachers have an online meeting. The security and privacy of VM applications are vulnerable to several attacks, such as: screen sharing, disclosure and association of information, malware attacks, phishing attacks, face recognition attacks, data hacking, zoombombing [20].

We conducted a study with teachers using one of the three VM applications described above. 16 professors from different university and pre-university institutions (from the Republic of Moldova and Romania) were interviewed. The results are as follows: 60% use Google Meet, 10% Microsoft Teams, 30% Zoom application; most have known these applications on services and on the Internet; 60% said they had known them for two years and 40% said they had known them for more than two years.

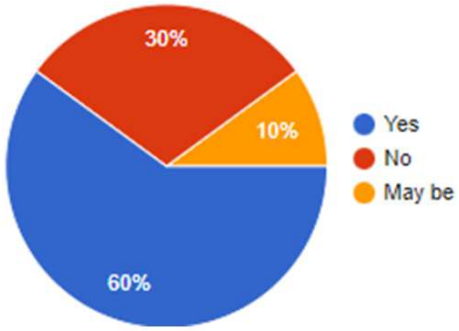



***Figure 6.*** *The answers to the question: have you heard about security and vulnerabilities in video conferencing applications?*

## 5. Conclusions

The three video conferencing platforms, Zoom, Google Meet and Microsoft Teams, experienced a dizzying development during the pandemic period. In this study we discussed the three applications in detail, both the side of social security and privacy, and the functionality. Zoom is a complex platform, but it still has security issues. Google Meet and Microsoft Teams are a little more secure, but they are less accessible in terms of usage, especially Microsoft Teams. On the other hand, for a Microsoft 365 Business user, the Teams application opens up all its chat, video, administration and security possibilities.

Choosing the best video conferencing application will depend on your purpose.

For example, if we only need basic video calling functionality, Google Meet might be the ideal solution. It's free and easy to use, but the requirement to create a Google Account may be a limitation for some.

On the other hand, if we need a robust collaboration tool with enterprise-level features, Microsoft Teams is probably best. Its wide range of integrations overshadows its competitors, and the ability to switch from video chat to video can be useful when managing a large group of participants. However, if our institution relies on platforms outside of the Microsoft ecosystem, we should consider another solution.

Finally, for a school or a small business, Zoom will probably be the best platform. It's simple and easy to use, and students won't even have to sign up for an account. In addition, it is great for online courses and presentations due to its interactive features and effortless screen sharing.

Most educational establishments and universities were forced to adopt VM apps for the continuous teaching process and to get in touch with students and staff during the COVID-19 pandemic. This study tackled the possible attacks on the aforementioned apps, like hijacking, splitting the screen, information disclosure, malware, phishing, data breaches and zoom bombing. The results show that Google Meet can be safely implemented within the educational sector, followed by MS Teams and last by Zoom, not taking into consideration factors like user friendliness and number of participants during a meeting. In addition, the safety features of these apps which need to be set correctly were further highlighted.

## Conflict of Interests

All the authors do not have any possible conflicts of interest.

## References

[1] Ali A. H., George L. E., Mokhtar M. R. An Adaptive High Capacity Model for Secure Audio Communication Based on Fractal Coding and Uniform Coefficient Modulation. Circuits, Syst. Signal Process., vol. 39, no. 10, pp. 5198-5225, 2020.

[2] Chakraborty P., Mittal P., Gupta M. S., Yadav S., Arora A. Opinion of students on online education during the COVID-19 pandemic, Hum. Behav. Emerg. Technol., vol. 3, no. 3, p. 357-365, 2020.

[3] Chawla Ajay, Coronavirus (COVID-19). 'Zoom' Application Boon or Bane, 2020. 10 p. Available at SSRN: https://ssrn.com/abstract=3606716.

[4] Costinela - Luminita D. Information security in E-learning Platforms. Procedia - Social and Behavioral Sciences, 15, 2011.

[5] Diesch R., Pfaff M., Krcmar H. A comprehensive model of information security factors for decision-makers, Comput. Secur., vol. 92, 2020.

[6] Eck C. J., Dale Layfield K., Dibenedetto C. A., Gore J. School-Based Agricultural Education Teachers Competence of Synchronous Online Instruction Tools During the COVID-19 Pandemic, Journal of Agricultural Education, vol. 62, no. 2, pp. 137-147, 2021.

[7] Isobe T., Ito R. Security Analysis of End-to-End Encryption for Zoom Meetings, in IEEE Access, vol. 9, pp. 90677-90689, 2021.

[8] Kagan D., Alpert G. F., Fire M. Zooming Into Video Conferencing Privacy and Security Threats, Cryptography and Security, 2020.

[9] Karim N. A., Shukur Z. "Review of User Authentication Methods in Online Examination," Asian J. Inf. Technol., vol. 14, no. 5, 2015, p. 166-175.

[10] Li C., Lalani F. The COVID-19 pandemic has changed education forever. This is how. World Economic Forum Covid Action Platform, 2020. Available: https://www.weforum.org/agenda/2020/04/coronavirus/education-global-covid19-online-digital-learning/

[11] Lynne Coventry. Video Conferencing in Higher Education. https://www.nyu.edu/content/dam/nyu/facultyResources/documents/ESMITS/vc_in_higher_education.pdf

[12] Mehta, Jay et al. "Rapid implementation of Microsoft Teams in response to COVID-19: one acute healthcare organization's experience." BMJ health & care informatics vol. 27, 3 (2020).

[13] Nader Abdel Karim, Ahmed Hussain Ali. E-learning virtual meeting applications: A comparative study from a cybersecurity perspective. Indonesian Journal of Electrical Engineering and Computer Science Vol. 24, No. 2, 2021, p. 1121-1129.

[14] Oeppen S., Shaw G., Brennan P. A. Human factors recognition at virtual meetings and video conferencing: how to get the best performance from yourself and others, British Journal of Oral and Maxillofacial Surgery, Volume 58, Issue 6, 2020, p. 643-646.

[15] Paolo Prinetto and Gianluca Roascio. Hardware Security, Vulnerabilities, and Attacks: A Comprehensive Taxonomy. http://ceur-ws.org/Vol-2597/paper-16.pdf

[16] Peter Abrahamsson Lindeblad, Yuliya Voytenko, Oksana Mont, Peter Arnfalk. Organizational effects of virtual meetings, Journal of Cleaner Production XXX, 2015, p. 1-11.

[17] Raan Saeed Al-Maroof, A. Salloum, Aboul Ella Hassanien, Khaled Shaalan. Fear from COVID-19 and technology adoption: the impact of Google Meet during Coronavirus pandemic. Interactive Lerning Environments. 2020.

[18] Ravinder Singh, Soumya Awasthi. Updated Comparative Analysis on Video Conferencing Platforms- Zoom, Google Meet, Microsoft Teams, WebEx Teams and GoToMeetings. EasyChair Preprint nr. 4026, 2020.

[19] Rubinger L. et. al., Maximizing virtual meetings and conferences: a review of best practices. Int. Orthop., vol. 44, no. 8, pp. 1461-1466, 2020.

[20] Secara Ion-Alexandru. Zoombombing – the end-to-end fallacy, Network Security VOL. 2020, NO. 8 2021.

[21] Vanessa Y. Oviedo, Jean E. Fox Tree. Meeting by text or video-chat: Effects on confidence and performance. Computers in Human Behavior Reports. Volume 3, 2021, 100054 p.

[22] Wlodarczyk, Jordan R. M. D., Wolfswinkel, Erik M. M. D., Carey, Joseph N. M. D. Coronavirus 2019 Video Conferencing: Preserving Resident Education with Online Meeting Platforms. Plastic and Reconstructive Surgery, Volume 146, Number 1, 2020. p. 110-111.

[23] Yoshiyasu Takefuji. Resilient Secured Education System for Online Lectures During the Pandemic, Journal of Applied Security Research, 2021.

[24] Zgureanu A. Security aspects of video conferencing services. Culegere de articole ştiinţifice ale Conferinţei Ştiinţific Internaţional "Competitivitate şi Inovare în economia cunoaşterii", Ediţia a XXII-a, 2, Chişinău, 2020.

[25] Zoom, "Zoom, Help Center," 2020. Available: https://support.zoom.us/hc/en-us/articles/201362153-Sharing-your-screen-content-or-second-camera

[26] Google Support, "Google Meet Security & Privacy for users," 2020. Available: https://support.google.com/meet/answer/9852160?hl=en#:~:text=All%20data%20in%20Meet%20is,encrypted%20at%20rest%20by%20default

[27] Microsoft, "Microsoft Docs," 2020. Available: https://docs.microsoft.com/en-us/welcome-to-docs

[28] Google Support, "Advanced phishing and malware protection Google Workspace Admin Help," 2021. Available: https://support.google.com/a/answer/9157861?hl=en

[29] https://economedia.ro/ins-in-2021-circa-8-din-10-dintre-gospodariile-din-romania-au-acces-la-internet.html

[30] https://www.unicef.org/moldova/media/3961/file/EVALUARE.html