Indonesian Journal of Electrical Engineering and Computer Science
Vol. 24, No. 2, November 2021, pp. 1121~1129
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v24.i2.pp1121-1129

E-learning virtual meeting applications: A comparative study from a cybersecurity perspective

Nader Abdel Karim[1], Ahmed Hussain Ali[2]
[1]Isra University, Amman, Jordan
[2]Ministry of Higher Education and Scientific Research, Studies Planning and Follow-up Directorate, Baghdad, Iraq

Article Info

Article history:

Received Jun 28, 2021
Revised Aug 28, 2021
Accepted Sep 2, 2021

Keywords:

E-learning
Google Meet
Microsoft Teams
Security
User privacy
Virtual meeting
Zoom

ABSTRACT

During the coronavirus disease 2019 (COVID-19) pandemic outbreak, the lockdown of all activities including schools and universities became a normal habit, forcing educational institutes to find new ways to ensure the continuity of the learning process. E-learning is considered the best choice at this stage whereas using video conferencing or virtual meeting applications (VM) apps is the most common solution. In this research, security issues and possible cyber-attacks that may occur due to the use of the most popular VM apps used by educational institutes (i.e., Zoom, Microsoft Teams, and Google meet) are discussed. Moreover, the security features of these applications are briefly explained. Furthermore, a comprehensive comparison from a cybersecurity perspective between VM apps was made. The results show that Google Meet was the most secure against cyber-attacks, followed by the Microsoft Teams and finally the Zoom app.

Corresponding Author:

Nader Abdel Karim
Isra University, Amman, Jordan
Email: nader.salameh@iu.edu.jo

1. INTRODUCTION

During the coronavirus disease 2019 (COVID-19) pandemic, the educational process in the whole world has changed dramatically. In 2020, the World Economic Forum mentioned that over 1.2 billion children cannot enroll in the schoolroom [1] and this led to more reliance on e-learning where the educational process takes place remotely on digital or online platforms [2]. Educational technology has been improved in the last few decades, and this was greatly valuable during this COVID-19 pandemic. Although many online platforms that support E-learning were ready to use, it is not easy for education institutes (e.g. schools, universities) to manage their educational activities in the online space. Furthermore, teachers and students faced a lot of logistic, technical, financial, and social challenges due to the use of this kind of education (i.e. e-learning) [3]. They started using VM apps instead of face-to-face meetings in schools and universities. Virtual meeting applications (VM) is one of the most common solutions that have been adopted and sometimes referred to as virtual conferencing or teleconferences such as Zoom, Microsoft Teams, and Google Meet [4]. A VM app is an application that is used by people to meet, no matter where they are, it uses video, audio, and text to link up or meet online rather than face-to-face. It allows direct sharing of information without the need to be in the same place. Creating a VM room is considered cost-saving compared to when individuals travel to meet one another for a short time. It is less disruptive to schedules and in-office work [5]. With the extraordinary growth of using VM apps, cybersecurity issues related to these techniques should be considered. Cybersecurity is focusing on the practice of defending information, operations, and communications from attacks. The main goal of cybersecurity is maintaining the integrity, confidentiality, privacy, authentication, and availability of any information system [6], [7]. The use of VM techniques

presents many security issues which vary from unencrypted communication for free accounts to vulnerabilities that permit malware execution on users' devices. Furthermore, the use of VM apps has increased privacy anxieties that could allow uninvited users to join meetings by guessing meeting IDs or by just looking for meeting links that were shared publicly such as social media webpages [8]. More specifically, using VM apps is vulnerable to many security and privacy risks, such as those related to social networks which include hijacking, screen sharing, information disclosure and association, malware, phishing, face recognition, data breach, and zoombombing attacks.

This manuscript is organized as follows. Section 2 presents the background in which the related works, virtual meeting apps, security features, and security and privacy issues are discussed. Section 3 covers the method adopted for the evaluation of the VM apps in this study. Section 4 highlights the results after the evaluation of the VM apps. Section 5 presents the discussion of the result of section 4. Finally, section 6 includes the conclusion and future work.

2. BACKGROUND

This section presents the related works that have discussed the VM apps. It also gives a brief explanation of Zoom, Google Meet, and Microsoft Teams apps. The security features and issues associated with the use of these apps are also discussed.

2.1. Related works

Security and user privacy are very important issues in the online environment. Further investigation is needed to improve the security of VM apps in the E-learning sector. This section demonstrates some articles that focused on the security and privacy issues due to the use of VM apps. Mahr *et al.* [9] performed a detailed forensic analysis on the primary disk, network, and memory of the Zoom VM app. The results show that user personal information may be found in its explicit and/or encrypted form, like chat messages, names, email addresses, and passwords. While using network captures, forensic imaging of digital devices, and memory forensics. Ling *et al.* [10] recognized 10 popular VM tools and pull outposts that contain invitations to meetings on two social networks (i.e. Twitter and 4chan). Then they do manual annotation to recognize zoombombing attack posts and then apply thematic analysis to establish a codebook to enhance and characterize the discussion surrounding calls for zoombombing. The findings show that most of zoombombing calls are not established by an adversary stumbling upon meeting invitations or brute-forcing their meeting ID, but actually through legitimate persons (i.e., insiders) who have access to these meetings, especially students in the educational institutes. This has serious security implications because it makes the protection methods used against zoombombing, like password protection, useless. Archibald *et al.* [11] studied the use of the Zoom for online qualitative interviews of nurses experiences and research observations. Regarding the security issue, the authors reveal that the Zoom app can securely record and store sessions especially when the protection of sensitive data is essential. Moreover, user-specific authentication, real-time encryption of meetings, and the ability to backup recordings to online remote server networks are included. Simple privacy and security options that enable the user to easily and securely log into Zoom represent the key strengths of the Zoom app. This study did not show any security issues due to app features like the ability to selectively invite users and monitoring the distribution of meeting access data. Kagan *et al.* [8] explored and analyzed the privacy issues that may exist through using VM by extracting private information from images of Zoom meeting members that are posted on the web publically. The result of this study showed that video conference users faced several privacy threats because of extracting personal information about the participants by an easy way of collecting thousands of existing images of video conference meetings including member's face images, age, gender, usernames, and sometimes even full names. Furthermore, the extracting data can put the security and privacy of the members at risk. However, this research focused on the privacy issue of Zoom app only. Kristóf [12] discussed the measures enforced in many countries about distance education. Moreover, the proposed solutions that were designed to manage the distance learning process and its characteristics and parameters were highlighted in this study (i.e., Skype, Zoom, Microsoft Teams, and Google Meet). The study revealed that there are security vulnerabilities and poor appearance in Zoom apps and they could be resolved by including passwords and enhanced encryption. Discussion of the security of the other two apps was limited. Khan *et al.* [13] identified the cybersecurity threats and privacy concerned that may occur using VM apps during the pandemic, COVID-19, at Healthcare Systems, financial services and government and media outlets sectors. The threats that were discussed in this study are distributed denial of service (DDoS), malicious domains, malicious websites, malware, ransomware cybercriminals, spam emails, malicious social media messaging, business email compromise, mobile threats and browsing Apps. However, the study did not link any threats with any VM apps. It was a general discussion for potential threats that may occur when using VM apps. The advantages and limitations of using

the preferable apps in the meeting of academic groups (i.e. Zoom and private Facebook group) are studied by authors in [14]. This study concludes that a hybrid format private Facebook group provides more suitable and satisfying result than Zoom in terms of the facilitator of a unique, health-related, narrative research group at the institution-a group tailored to critical thought, communication, cooperation, and creativity. However, the discussion of the security of these two apps was limited. Singh and Awasthi [15] provide a comparative study of video conferencing apps related to Google Meet, Zoom, Microsoft Teams, Cisco WebEx Teams and GoToMeeting. This comparison includes the features of security and privacy issues. However, the author states that there are security issues of using Zoom apps without giving any details, although the security features of the other apps are demonstrated.

By reviewing the above studies, we may come to the conclusion that some studies [8], [11], [14] are dedicated to discussing the features, security, and privacy issues of a particular app (i.e. Zoom). Other studies [12], [15], however, gave general information about the features and security of VM apps, while studies like [8], [13], highlighted the threats faced by the VM apps regardless of the app used. Moreover, some studies [9], [10] focused on certain types of attacks (i.e. zoom bombing and data breach) that could attack Zoom and other VM apps.

2.2. Virtual meeting apps

With the dramatic growth of using virtual meeting apps, many criteria should be considered to pick the suitable VM app which include:

- Cost: customizing user needs within budgets.
- Meeting duration: available time provided for each meeting.
- Compatibility: with all platforms and all types of devices
- Purpose: some apps are designed for particular purposes.
- Integration: apps should work well with other apps.
- The number of participants: differs from one VM app to another.
- Usability: user-friendly for effectiveness, efficiency, and satisfaction.
- Security: robust for users' data and maintain privacy.

Over the years, there have been many popular VM apps including Zoom, Microsoft Teams, Google Meet (Hangouts), Skype, Adobe Connect, CiscoWebex, and Freeconferencecall. Based on [12] Zoom, MS Teams, and Google Meet were the most frequently used VM apps in E-learning.

2.2.1. Zoom

Zoom is an American communications technology company. It supplies online chatting services over a cloud-based live calling application that is used for virtual meetings, distance learning, and social networks [12]. Zoom has become the most popular app for the education sector and more than 500 companies used it during 2019 and 2020. This number has been increased dramatically since 300 million users participate in the Zoom app daily [16], [17]. Zoom has many features such as compatibility, one-on-one meetings, group video conferences, screen sharing, meeting invitees do not need to download any application to attend the meeting. To join a meeting, it is sufficient to click on the send link if they use Chrome and Firefox browsers. The invitees are not required to create accounts on the application. Moreover, Zoom standard is 40 minutes free, 100 participants max [18]. However, the Zoom app suffered from security flaws and poor appearance. The company apologized for these security issues in April 2020, claiming that these issues arose because the application was not designed primarily for e-learning. Zoom has announced a focus on privacy and transparency issues; so, in April 2020, version 5.0 of Zoom was released in which many security and privacy issues were successfully resolved. Passwords, enhanced encryption, and a new security icon were included in the new Zoom app version [12].

2.2.2. Microsoft Teams

Microsoft (MS) created the Teams app in March 2017 in New York and launched its service. Microsoft Teams is essentially targeted for teams, classes or groups to collaborate, share and chat. Besides text chat, video calls and screen share are also supported. Microsoft reported that MS Teams now has around 44 million users [12]. It allows communities and groups to join links or invitations using a group administrator or owner. Administrators and teachers can generate groups for classes, professional learning communities and employees. Within the MS Teams app, users can set up channels that are conversation topics to communicate without email or group SMS. MS Teams also help teachers to distribute, give feedback on and classify student materials on the assignments tab which is offered to the Office 365 Education subscribers. Teachers can also make Quizzes for students through integration with Office Forms [12], [19]. However, there is some limitation since the structure of files confuses users and provides challenges regarding permission settings, adding members from outside the organization, receiving notifications and sending multimedia files through the app [20].

2.2.3. Google Meet

Google Meet (formerly Hangouts) is a video-communication service developed by Google [21]. The use of Meet increased between January and April 2020 during the 2020 COVID-19 pandemic, reaching 100 million users a day in the last week of April 2020 [12]. Google provides a 60 minutes limit for up to 100 participants for free accounts. However, everyone joining the meeting must sign in with a Google account [8]. Meet app has been downloaded millions of times from Play store where work-from-home numbers have grown through the COVID-19 pandemic period. Since January, Meet's peak daily usage has grown by 30 times, according to Google [22]. Joining a meeting requires no app to download; rather, any web browser can be used to join. To join a meeting through mobile via IOS and Android with screen sharing and 16 participants on a single screen, apps should be downloaded. Encryption, anti-hijacking and phishing, 2-step verification APP, and 2SV are provided by Meet to control and save those who access the app [8].

2.3. Security features

Following up the cybersecurity procedures in the right manner can help users to keep out unwanted attendees, secure users' data and privacy. Some features that can be helpful for users to manage secure access to VM apps and general recommendation are as follows [23]:

- Meeting IDs and Passwords: To prevent unauthorized users, meeting IDs should not be publicly shared and a unique, strong password of at least 12 uppercase and lowercase letters, numbers, and symbols should be set for the meeting. Two-factor authentication provides another layer of protection by delivering code to the user's simcard or email.
- Encryption: The most important feature to take into account to encrypt the meeting resources when using the VM apps is the encryption algorithms (for example, AES) with keys of 128, 256, 4096, and so on.
- Manage Joining and Calls: The host should control the joining and calls to identify unknown phone numbers.
- VM Meeting Apps Setting: These can improve the security. Alerts can be established so the host knows when meeting invitations are sent over email to participants. Other than the meeting coordinator or host, participants can be blocked from recording the meeting, or to identify which participant has started recording. File sharing can be restricted so that anonymous participants cannot open or receive private documents or transmit malware masked as an attachment to other participants of the call as the webcam on a user's device may be used by intruders as a tool to spy on the participant utilizing malicious software that infects participant devices. Expectations for privacy settings should be approved by the group or colleagues to ensure communications are secure on both ends.

Besides the above features, there are some recommendations for users that used VM apps that should be taken into consideration:

- Files and links: Clicking links and attachments in anonymous emails should be avoided.
- Use Enterprise License: Access the VM apps by purchasing an enterprise license that gives users more control and ensures security and privacy.
- Install security software: Beyond managing the settings of the VM apps, install security software on the devices.
- Avoid open meetings: Never use an open VM app. They make it easy for attackers to join in.

2.4. VM apps security and privacy issues

Users commonly represent the weakest link in the security chain [24]. So, the user's private security when using VM apps depends on the user himself. When a user joins a call through one VM app from an unsecured device or connection, he becomes vulnerable to unauthorized access. The main point in VM apps is secure access, which means avoiding the annoying intruder from enrolling and gaining access to the data or devices of any participant on the meeting. VM apps like Zoom, Google Meet, and Microsoft Teams can make it easy to meet your teachers, classmates, workgroups, friends, and family members. However, that ease of transmission might also make the mission of reaching the information easier for attackers. The main idea is to be aware of the security risks before getting on a video call with your work team or group of friends by setting up the features of the VM apps correctly to keep malware, hackers, and identity thieves out.

Privacy is another concern. The privacy policies of VM apps could enable the services to collect and store a lot of data from many resources (e.g., cloud recordings, videos, messages, files, documents shared on the screen, and whiteboards showed during service) and these data could contain sensitive personal information. The webcam provides a window to the world through which hackers can spy on the participant when he mistakenly left the webcam on. Another example of the privacy issue is when hackers gain access to the legal or finances information of the company or user sensitive healthcare information whenever the user has a meeting with the doctor. The security and privacy of the VM apps are vulnerable to multiple attacks, such as:

- Hijacking (HJK): shared by public social media or emails, VM apps have public or easily guessable IDs and PINs. Without protection, anyone with these meeting credentials could join, disrupt the proceedings or acquire sensitive information.
- Screen sharing (SS): Most VM apps have a screen sharing option. When an unauthorized participant shares inappropriate content, this is Cyberbullying.
- Information disclosure and association (IDA): With information disclosure, participant information is detected and extracted unintentionally. When used to connect with other accounts and get private information, it is information association. Where and how any recorded VMs are stored and protected is important. With improper access or lack of encryption, sensitive information can be compromised.
- Malware attacks (MA): Malicious software developed by the intruder to collect and gain access to confidential information.
- Phishing attacks (PA): Based on social engineering developed to mimic genuine sites, these online attacks steal the victim's sensitive data by hiding as a legitimate third-party website. URLs are sent to targeted users through email, spam messages, or social networking websites (e.g., Facebook) to retrieve passwords, bank details and credit card numbers. Since the COVID-19 outbreak, hackers have been increasingly impersonating video conferencing applications, including Zoom, Microsoft Teams, and Google Meet [25].
- Face recognition attacks (FRA): Identifying strangers from their face, by online or offline video or by photographs widely available on social network sites (e.g Facebook), used to expose personal information about the user. Face recognition algorithms can identify or verify a person from digital photos or a video source.
- Data breach: Some VM apps provide recording and cloud storage abilities for their users. These recordings could contain sensitive and private information such as user's full names, phone numbers, and addresses.
- Zoombombing (ZB): This attack denotes unwanted and annoying intruding participants who join and interrupt a meeting with aggressive talking. Although the term is taken from the Zoom app name, the phenomenon occurs on the other VM apps as well. The significant increase in the use of the Zoom app during the COVID-19 pandemic as an alternative to physical meetings led to an increase in intruders trying to exploit the flaws of this application in this way [26].

3. METHOD

To evaluate the VM apps system from a cybersecurity perspective, different types of cyber-attacks should be applied. This research focused on the three popular VM apps used around the globe currently: Zoom, MS Teams, and Google Meet [12], [27]. However, because these apps are closed source and commercial [28]-[30], it is not possible to apply these attacks while using the full features versions of these apps. Therefore, in this study, the literature and reports from reliable resources (accredited scientific journal or an article from a specialized body) related to the security of these apps are downloaded, reviewed, and the free version of these apps are used and examined for any vulnerabilities that may lead to any type of cyber-attack. Moreover, in this study the VM apps evaluation process focused on the most common cyber-attacks related to VM apps, which are hijacking, screen sharing, information disclosure, and association, malware attack, phishing attack, face recognition, data breach, and zoombombing [10].

4. RESULTS

After using the VM apps chosen to be examined and reviewing the literature and reports related to these VM apps, it is clear that the users of these VM apps could be vulnerable to the attacks shown in Table 1. Explanation of each of these attacks and the extent of their impact on the three VM apps are as follow:

- HJK: Users in Zoom are more vulnerable to this attack since the meeting ID consists of 10 or 11 digits, which can be easily guessed by the intruder [31]. In the case of MS Teams, a participant needs to be a member of the class administered by the class owner (admin) and must have an "outlook" email related to the school or university. As for Google Meet, the meeting ID consists of 10 alphabet characters, in addition to the two features which are APP (Advance Protection Program) and 2SV (2-Step Verification) [32].

Table 1. VM apps vs possible attacks

App Name/Attack	HJK	SS	IDA	MA	PA	FR	DB	ZB
Zoom	√	√	√	√	√	√	√	√
MS teams		√	√	√	√	√		
Google Meet		√				√	√	√

- SS: This feature is provided by all three apps, so the users in each meeting should expect to face this attack from any intruder who can gain the access to these meetings. In Zoom, the meeting coordinator can restrict members' capability to share their screen [33]. In Google Meet, preventing call participants from sharing their screen is currently only available for Google Workspace for Education users [34]. In MS Teams, the admin can configure screen sharing and let users share an entire screen. The admin also enables users to give or request control. Moreover, the admin can configure whether anonymous or external users request control of the shared screen [35].
- IDA: Hosts have the ability to collect user information from the meeting and share it. The policy of Zoom's privacy is similar to other VM apps. It claims the right to gather, store users' data, and share it such as in advertisers [36]. Also in MS Teams, any member of the Team's meeting can automatically access all meeting files [20]. Admin in Teams can use the Guest access settings in the Teams admin center to configure the level of access granted to guest users. For maximum security, admin can leave guest access disabled by default. The user can create a private meeting with a maximum of 30 channels [37] in a Team to create single permission for a specific meeting (for instance "Management"), but he cannot invite "guest users" to the selected meetings [20]. Moreover, by default, any class member can start recording without any permissions. After the session has finished, the videos will be shared and can be download from any member within the class on the class timeline for 20 days. Related to Google Meet and based on Google, each user owns their data. Google stated on its official website that they do not used the customer's data to target them with ads and does not sell their data to a third party [34].
- MA: Client Zoom apps allow attackers to exploit the developed animated GIF pictures located in a Zoom meeting chat to hack the client app on other mobile phones [38]. While in MS Teams, Microsoft warns the customers about the "FakeUpdates" campaigns in a private security advisory based on a report in Bleeping Computer [39]. Different types of companies are targeted by these campaigns. The recent campaigns target the K-12 education sector that is now dependent on Teams due to COVID-19 limitations. Cobalt Strike is an attack tool that hacker uses to spread malicious programs (e.g. Ransomware malware) [40]. With Google Meet, researchers from Check Point Software Technologies [41] have found fake Google Meet domains that sent people to malicious websites which look like a legitimate website to install malware on the user's devices. However, the number of these domains are incomparable with the number of domains that made for Zoom since January to May 2020 (6,576 Zoom-related domains have been registered globally). With respect to meet, Google made advanced phishing and malware protection against phishing and harmful software (malware) and users can use any modern web browser and no download is required [42]. Organizations can stop and restrict attacks and banish hacker attacks by blocking executable files that do not meet specific criteria or by blocking JavaScript and VBScript code from downloading executable content [39].
- PA: The Anti-Phishing Working Group (APWG) received only few reports of phishing attacks against the Zoom app in March 2020 while, in April, the number of reports reached around one thousand [24], [43]. The victims receive emails saying there is a Zoom meeting starting soon. The email also provides a link to the phishing page that impersonates the Zoom login page [44]. Then the phishing site asks for victims' zoom credentials to log in. Researchers from Abnormal Security [45], security warn users of a phishing campaign that may be an automated message send to MS Teams app. This phishing campaign was sent to between 15,000 and 50,000 Office 365 users [46]. Researchers in [46] mentioned: "Since MS Teams is an immediate-messaging service, receivers of this notification could be more susceptible to click on it so that they can reply fast to whatever message they believe they could have missed based on the notification,". The phishing email announces "There is new activity in Teams," in order to appear like an automated email notification from MS Teams. An example of the type of email a recipient might receive is a notification that their colleagues are trying to reach and warn them about missed chats. A chat could be shown telling the recipient to send something by a certain date. Data scientist at Abnormal Security, Erin Ludert, said that intruders are using more of a "spray" strategy, as the employee referenced in the chats does not seem to be an employee of the firm that received the attack [45]. To respond, the victim is asked by email to click on the "Reply in Teams" button and this will redirect the victim to a phishing page that impersonates the MS Team login page. The phishing page asks the MS Team members to enter their login information, email, and password. The phishing campaign targets up to 50,000 Office 365 users to notify them of a "missed chat" from the MS Team app [25], [45]-[47]. Regarding Google Meet, frauds in emails impersonating some public organizations like the world health organization (WHO) have been observed by Google and found in April 2020 more than 18 million malware and phishing emails associated with COVID-19 in one week. The problem becomes clear since the WHO has a web page devoted to information about COVID-19 hackers and scammers [48]. However, Google provides its apps with features that provide strong protection against phishing, which is specifically designed for the highest risk accounts, and they did not notice any successful phishing attempts for the users who participate in their apps, even if they are repeatedly targeted [34].

- FR: All the apps under this study allow hosts to record the meeting and store them whether, in their personal computer or cloud. These recordings are vulnerable to such attack.
- DB: Wagenseil [38] mentioned that Zoom declares its meetings use "end-to-end encryption" if each party calls in from a PC or a Zoom mobile app. But under pressure from the Intercept, the Zoom company spokesman disclosed that Zoom's descriptions of the team "end-to-end" and "endpoint" are different from other parties. "Once using phrase 'End to End," a Zoom representative expressed to the Intercept, "it is about the connection being encrypted from Zoom endpoint to Zoom endpoint." It sounds great, nevertheless, the Zoom representative explained that he counted a Zoom server as an endpoint, and this considered phoney end-to-end encryption. Moreover, based on [4], user's information was still found which including a plain text of user information, chat messages, profile pictures, files exchanged, and user's contact information. Furthermore, bits of this information can still be found and saved even while a user decided to delete a contact from their app [11], [38]. In MS Teams, the data (i.e., video files, audio files, and information) is encrypted on transition between different devices, users, or data centers compares with standard approaches. MS team encrypts user data, but it remains in possession of the encryption keys to user data. This enables Microsoft to access all data stored and used in Microsoft Teams in plain text [49]. Google meet saves recordings in cloud storage, so in this case, recordings could be vulnerable to this type of attack.
- ZB: New research conducted at the University of Boston and University of Binghamton [12] stated that efforts to stop "Zoom bombing," for example entering passwords to get access or making waiting rooms where a participant needs approval from the meeting coordinator to access the meeting, often would not work. That is because many attacks are executed by internal and authorized users (e.g., students in the class). The research results show that the vast majority of calls for Zoom bombing are not created by attackers stumbling upon meeting invitations or brute-forcing their meeting ID, but rather by legitimate participants who have legal access to these meetings, especially students in high school and college classes. Same researchers mentioned that Google Meet is also vulnerable to "Zoom Bombing" attack although the results showed that MS team is less vulnerable to "Zoom bombing" attack since the nature of MS teams makes it less vulnerable to this kind of attacks and users are already members within classes established by the admin [12].

5. DISCUSSION

From the results shown in the previous section, it can be concluded that all three VM apps still have security issues from a cybersecurity perspective. We notice that there is a discrepancy in meeting the security requirements between the three VM apps as shown in Table 1 as well. According to Zoom, we can notice that this application is vulnerable to all possible attacks mentioned in Table 1 including hijacking, screen sharing, information discloser and association, malware, phishing, face recognition, data breach, and zoombombing attacks. As for the MS Teams, the situation seems better, but this app is still subject to some attacks such as screen sharing, information discloser and association, malware, phishing, and face recognition attacks. According to Google Meet, it appears that this application performs well in terms of security; however, it still faces some kinds of attacks like screen sharing, face recognition, and Zoombombing. As a sum and based on our results, it can be concluded that Google Meet is a more appropriate VM app in terms of security, followed by the MS Teams, and then finally comes the Zoom app.

At the same time, it is worth noting that security is one of many factors that should be checked when choosing the suitable VM app to meet an institution's requirements as shown in Section 2.2. There is often a trade-off between security and usability/performance [50], [51]. This could lead some institutes to pick usability/performance to please their customers explaining the reason why Zoom is the world's first choice of VM apps [14], [16]. In addition to the above mentioned discussion, and to keep the privacy and the confidential information secure while using the VM apps, it is recommended to share as little personal information as possible, use a single app and an email that is not used for anything else such banking, healthcare, and social media accounts, turn off the camera and microphone whenever they are not using them, use the blurred background in order not to disclose the personal details that can be seen from anything behind or beside you [37].

6. CONCLUSION

The majority of educational institutions and universities have been forced to adopt the VM apps to continue learning and contacting students and staff during the COVID-19 pandemic. Many criteria should be considered to select an appropriate VM app, like cost, compatibility, purpose, integration, and number of participants, usability, and security. Three VM apps (i.e., Zoom, MS Teams, and Google Meet) were the preferred choice for most educational institutes. However, malicious attackers have considered this situation

as an opportunity to attack the online VM apps using their features such as meeting ID, screen sharing, personal information recordings, and emails. This study discussed the possible attacks on the above-mentioned apps, such as, hijacking, screen sharing, information discloser, malware, phishing, data breach, and zoombombing. The results reveal that Google Meet can be adopted securely in the educational sector, then MS Teams and, lastly is Zoom regardless of other factors such as the ease of use and number of participants and meeting period. Besides, the security features of these apps that should be properly to set are highlighted. Some recommendations when using the online VM apps have been included as well. Future work is required to re-evaluate the discussed VM apps in this study at the end of 2021, as well as, to evaluate the other available VM apps that could be picked by the education institutions as e-learning mediums.

REFERENCES

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

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

[3] P. Chakraborty, P. Mittal, M. S. Gupta, S. Yadav, and A. Arora, "Opinion of students on online education during the COVID-19 pandemic," *Hum. Behav. Emerg. Technol.*, vol. 3, no. 3, pp. 357-365, 2020, doi: 10.1002/hbe2.240.

[4] C. J. Eck, K. Dale Layfield, C. A. Dibenedetto, and J. Gore, "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, doi: 10.5032/jae.2021.02137.

[5] L. Rubinger *et al.*, "Maximizing virtual meetings and conferences: a review of best practices," *Int. Orthop.*, vol. 44, no. 8, pp. 1461-1466, 2020, doi: 10.1007/s00264-020-04615-9.

[6] R. Diesch, M. Pfaff, and H. Krcmar, "A comprehensive model of information security factors for decision-makers," *Comput. Secur.*, vol. 92, 2020, doi: 10.1016/j.cose.2020.101747.

[7] A. H. Ali, L. E. George, and M. R. Mokhtar, "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, doi: 10.1007/s00034-020-01409-7.

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

[9] A. Mahr, M. Cichon, S. Mateo, C. Grajeda, and I. Baggili, "Zooming into the pandemic A forensic analysis of the Zoom Application," *Forensic Sci. Int. Digit. Investig.*, vol. 36, p. 301107, 2021, doi: 10.1016/j.fsidi.2021.301107.

[10] C. Ling, U. Balcı, J. Blackburn, and G. Stringhini, "A first look at zoombombing," *2021 IEEE Symposium on Security and Privacy (SP)*, 2021, vol. 1, pp. 1452-1467, doi: 10.1109/SP40001.2021.00061.

[11] M. M. Archibald, R. C. Ambagtsheer, M. G. Casey, and M. Lawless, "Using Zoom Videoconferencing for Qualitative Data Collection: Perceptions and Experiences of Researchers and Participants," *Int. J. Qual. Methods*, vol. 18, pp. 1-8, 2019, doi: 10.1177/1609406919874596.

[12] Z. Kristóf, "International Trends of Remote Teaching Ordered in Light of the Coronavirus (COVID-19) and its Most Popular Video Conferencing Applications that Implement Communication," *Cent. Eur. J. Educ. Res.*, vol. 2, no. 2, pp. 84-92, 2020, doi: 10.37441/CEJER/2020/2/2/7917.

[13] N. A. Khan, S. N. Brohi, and N. Zaman, "Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic," *TechRxiv Powered by IEEE*, pp. 1-6, 2020, doi: 10.36227/techrxiv.12264722.v1.

[14] C. Nash, "Report on Digital Literacy in Academic Meetings during the 2020 COVID-19 Lockdown," *Challenges*, vol. 11, no. 2, 2020, doi: 10.3390/challe11020020.

[15] R. Singh and S. Awasthi, "Updated comparative analysis on video conferencing platforms- Zoom, Google Meet, Microsoft Teams, WebEx Teams and GoToMeetings," *EasyChair world Sci.*, pp. 1-9, 2020, [Online]. Available: https://easychair.org/publications/preprint/Fq7T

[16] D. Power and R. Hadidi, "Impacts of the Global Health Crisis on the Use of Information Technologies," *J. Midwest Assoc. Inf. Syst.*, vol. 2021, no. 1, 2021, doi: 10.17705/3jmwa.000062.

[17] A. Chawla, "Coronavirus (COVID-19)–'Zoom' Application Boon or Bane," *SSRN Electron. J.*, 2020, doi: 10.2139/ssrn.3606716.

[18] D. M. de Oliveira Dias, D. R. de O. Albergarias Lopes, and A. C. Teles, "Will Virtual Replace Classroom Teaching? Lessons from Virtual Classes via Zoom in the Times of COVID-19," *J. Adv. Educ. Philos.*, vol. 4, no. 5, 2020, doi: 10.36348/jaep.2020.v04i05.004.

[19] S. Ismail, and S. Ismail, "Teaching Approach using Microsoft Teams: Case Study on Satisfaction versus Barriers in Online Learning Environment," *Journal of Physics: Conference Series*, vol. 1874, 2021, doi: 10.1088/1742-6596/1874/1/012020.

[20] Storyal, "The pros and cons of Microsoft Teams | Storyals Blog," *Driving microsoft 365 Adoption*, 2020. [Online]. Available: https://storyals.com/blog/pros-and-cons-of-microsoft-teams

[21] E. E. Ogunseye and S. O. Akinola, "Empirical Quality and Usability Assessments of Five Common Online RealTime E-Meeting Platforms," *Journal of Science and Logics in ICT Research*, vol. 6, no. 2, pp. 2714-3627, 2021.

[22] O. Hughes, "Google Meet video-conferencing and chat app: A cheat sheet," *Software-TechRepublic*, 2020. [Online]. Available: https://www.techrepublic.com/article/google-meet-video-conferencing-and-chat-app-a-cheat-sheet/

[23] A. G. Johansen, "Internet security-emerging-threats-zoom-bombing-video-conference-threats," *NortonLifeLock*, 2020. [Online]. Available: https://us.norton.com/internetsecurity-emerging-threats-zoom-bombing-video-conference-threats.html
[24] S. Furnell, W. Khern-am-nuai, R. Esmael, W. Yang, and N. Li, "Enhancing security behaviour by supporting the user," *Comput. Secur.*, vol. 75, pp. 1-9, 2018, doi: 10.1016/j.cose.2018.01.016.
[25] A. Basit, M. Zafar, A. R. Javed, and Z. Jalil, "A Novel Ensemble Machine Learning Method to Detect Phishing Attack," *2020 IEEE 23rd International Multitopic Conference (INMIC)*, 2020, pp. 1-5, doi: 10.1109/INMIC50486.2020.9318210.
[26] S. Young, "Zoombombing Your Toddler: User Experience and the Communication of Zoom's Privacy Crisis," *J. Bus. Tech. Commun.*, vol. 35, no. 1, pp. 147-153, Jan. 2021, doi: 10.1177/1050651920959201.
[27] M. Said Elsayed, N. A. Le-Khac, and A. D. Jurcut, "Dealing with COVID-19 network traffic spikes," in *IEEE Security & Privacy*, vol. 19, no. 1, pp. 90-94, Jan.-Feb. 2021, doi: 10.1109/MSEC.2020.3037448.
[28] F. Porpiglia *et al.*, "Traditional and Virtual Congress Meetings During the COVID-19 Pandemic and the Post-COVID-19 Era: Is it Time to Change the Paradigm?," *Eur. Urol.*, vol. 78, no. 3, pp. 301-303, 2020, doi: 10.1016/j.eururo.2020.04.018.
[29] P. Ganesha, A. B. D. Nandiyanto, and B. C. Razon, "Application of Online Learning During the Covid-19 Pandemic through Zoom Meeting at Karya Mekar Elementary School," *Indones. J. Teach. Sci.*, vol. 1, no. 1, pp. 1-8, 2021.
[30] A. Aiken, "Zooming in on privacy concerns: Video app Zoom is surging in popularity. In our rush to stay connected, we need to make security checks and not reveal more than we think," *Index Censorsh.*, vol. 49, no. 2, pp. 24-27, 2020, doi: 10.1177/0306422020935792.
[31] N. Yaman and M. Muhlis, "Students' social presence and perceived learning toward CCU course in online classroom (An evaluating of learning process during pandemic coronavirus)," *Elit. English Lit. J.*, vol. 7, no. 1, p. 61, 2020, doi: 10.24252/elite.v7i1a6.
[32] Google Support, "Google Meet Security & Privacy for users," 2020. [Online]. Available: https://support.google.com/meet/answer/9852160?hl=en#:~:text=All%20data%20in%20Meet%20is,encrypted%20at%20rest%20by%20default
[33] Zoom, "Zoom, Help Center," 2020. [Online]. Available: https://support.zoom.us/hc/en-us/articles/201362153-Sharing-your-screen-content-or-second-camera
[34] Google, "Google Meet security & privacy for admins," 2020. [Online]. Available: https://support.google.com/a/answer/7582940?hl=en
[35] Microsoft, "Microsoft Docs," 2020. [Online]. Available: https://docs.microsoft.com/en-us/welcome-to-docs
[36] L. B. Andrews, C. Nace, and A. Chow, "Road Warriors to Zoom Masters: Development of the ACGME Remote Accreditation and Recognition Site Visit," *J. Grad. Med. Educ.*, vol. 13, no. 4, pp. 597-601, 2021, doi: 10.4300/jgme-d-21-00654.1.
[37] D. Knežević, "10 Pros and Cons of Microsoft Teams-Teams' Advantages and Disadvantages in 2021," *Office 365 & SharePoint Online*, 2018. [Online]. Available: https://www.syskit.com/blog/10-pros-and-cons-of-microsoft-teams/
[38] P. Wagenseil, "Zoom security issues: Here's everything that's gone wrong (so far)," *Security*, 2021. [Online]. Available: https://www.tomsguide.com/news/zoom-security-privacy-woes
[39] G. Karantzas and C. Patsakis, "An Empirical Assessment of Endpoint Detection and Response Systems against Advanced Persistent Threats Attack Vectors," *J. Cybersecur. Priv.*, vol. 1, no. 3, pp. 387-421, 2021.
[40] R. Panchal and D. Jadhav, "A Review On Protection Against Fileless Malware Attacks Using Gateway," *Turkish Journal of Computer and Mathematics Education*, vol. 12, no. 10, pp. 7302-7307, 2021, doi: 10.17762/turcomat.v12i10.5620.
[41] "Zoom, Google Meet And Microsoft Teams Are Hackers New Favourite Too," 2020. [Online]. Available: https://timesofindia.indiatimes.com/gadgets-news/zoom-google-meet-and-microsoft-teams-are-hackers-new-favourite-too/articleshow/75708403.cms.
[42] Google Support, "Advanced phishing and malware protection - Google Workspace Admin Help," 2021. [Online]. Available: https://support.google.com/a/answer/9157861?hl=en
[43] P. Unchit, S. Das, A. Kim, and L. J. Camp, "Quantifying Susceptibility to Spear Phishing in a High School Environment Using Signal Detection Theory," *International Symposium on Human Aspects of Information Security and Assurance*, 2020, pp. 109-120, doi: 10.1007/978-3-030-57404-8_9.
[44] B. Pranggono and A. Arabo, "COVID -19 pandemic cybersecurity issues," *Internet Technol. Lett.*, vol. 4, no. 2, pp. 4-9, 2021, doi: 10.1002/itl2.247.
[45] L. O'Donnell, "Microsoft Teams Phishing Attack Targets Office 365 Users," *Threatpost.com*, 2020. [Online]. Available: https://threatpost.com/Microsoft-teams-phishing-office-365/160458/
[46] A. Security, "Microsoft Teams Impersonation-Abnormal Security," 2020. [Online]. Available: https://abnormalsecurity.com/blog/microsoft-teams-impersonation/
[47] B. Heald, "Nereus: A Proposal for Implementing Anti-phishing Software Nereus: A Proposal for Implementing Anti-phishing Software Using Corporate Branding Color Matching Using Corporate Branding Color Matching," *Thesis, Rochester Institute of Technology*, 2020, [Online]. Available: https://scholarworks.rit.edu/theses/10644/
[48] J. Sultana and A. K. Jilani, "Classifying Cyberattacks Amid Covid-19 Using Support Vector Machine," *Security Incidents & Response Against Cyber Attacks*, pp. 161-175, 2021, doi: 10.1007/978-3-030-69174-5_8.
[49] J. Reisacher, "Do Not Forget to Securely Lock Your Data in Microsoft Teams," *Cyber Defense Magazine*, 2020. [Online]. Available: https://www.cyberdefensemagazine.com/do-not-forget-to-securely/
[50] N. A. Karim and Z. Shukur, "Using preferences as user identification in the online examination," *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 6, no. 6, pp. 1026-1032, 2016, doi: 10.18517/ijaseit.6.6.1412.
[51] N. A. Karim, Z. Shukur, and A. E. M. AL-banna, "UIPA: User authentication method based on user interface preferences for account recovery process," *J. Inf. Secur. Appl.*, vol. 52, Jun. 2020, doi: 10.1016/j.jisa.2020.102466.