Implementation of Identity and Access Management Application in Learning Management System to Mitigate Credential Hacking Issues

Yew Tuck Mun
School of Computing
Asia Pacific University of Technology and innovation (APU)
Kuala Lumpur, Malaysia
TP056191@mail.apu.edu.my

Dr. Intan Farahana Binti Kamsin
School of Computing
Asia Pacific University of Technology and innovation (APU)
Kuala Lumpur, Malaysia
intan.farahana@staffemail.apu.edu.my

***Abstract*- Privacy and data security is an extremely crucial thing for learning management systems such as Zoom. In the recent year, due to the covid-19 outbreak many educational, businesses field organizations continue their offline meeting and classes to online activities by using applications such as Zoom. Therefore, the daily increase of users in zoom has caught the eye of the hackers. The hackers tend to attack the credentials of those users in zoom and specifically steal the data that has been stored in zoom and sell the information obtained to the dark web. After reading some articles, the researchers suggested implementing the identity and access management application which authority can use to control the accessibility of each user in the zoom application. The application will be able to trace the reason of each user accessing into the system and to see if they have any suspicion on the activities that they were doing. The implemented application will bring a good impact where it can safeguard the user's privacy and data to allow the user to have worry free when using the application. However, after implementing the application, the researcher uses questionnaires to obtain the raw data from around 200 users from different backgrounds.**

Keywords— identity and access management, credential hacking, learning management system, zoom

I. INTRODUCTION

In this era of technology, utilizing the learning management system (LMS) to receive education has become one of the daily necessities for every student. In this research paper, the Zoom application will be targeted as the area of discussion as many people prefer to use zoom to conduct their meeting or class application as compared to the other LMS application such as teams, google meets. According to the internet, most of the students prefer to use zoom as the effectiveness of zoom application during online classes is very convenient to utilize. The significant increase of users of the Zoom application is because they provide free accounts to use. Users can create a free account to host meetings, classes or even events. Not only that, but the Zoom application also allows users to mute, share screens which makes it perfect for lessons and meetings to be hosted in Zoom. However, utilizing online applications has the risk of getting credentials theft. Nowadays, credential hacking issues have increased rapidly and remain unrestrained all over the country especially in the zoom application, zoom has been continuously reported that there are many unsolved security issues such as the privacy concerns of the user, zoom bombing, and most importantly lack of data protection (Secara, I.-A. , 2020). Although zoom has many issues, it is believed that with the researcher's implementation of identity and access management (IAM) into the zoom application, it will reduce, or it might even mitigate the credential hacking issue. This is because the mechanism of IAM will restrict any suspect access from the network. In these papers, the researcher has included 13 important components, which are the abstract, index terms, introduction, literature review, problem statement, research aim & objectives, research questions & significance, methodology, proposed system overview and conclusion. These components are used to provide detailed information of the research article.

II. LITERATURE REVIEW

A. Literature Review Listing

TABLE I. LITERATURE REVIEW LISTING

Domain	Article	Author	Years
Identity and Access Management	Systematic Review of Identity Access Management in Information Security	Ishaq Azhar Mohammed	2017
	Identity and Access Management in Cloud Environment: Mechanisms and Challenges	I.Indu,P.M. Rubesh Anand, Vidhyacharan Bhaskar	2018
	Identity and Access Management System: a Web-Based Approach for an Enterprise	Mohammed Kabiru Hamza, Hassan Abubakar, Yusuf Mohammed Danlami	2018
Learning Management System	Postgraduate student experiences on the use of moodle and canvas	Cedric Bheki Mpungose & Simon Bheki Khoza	2020

	learning management system		
	The Rise of Distance Education during Covid-19 Pandemic and the Related Data Threats: A Study about Zoom	Ceren Cubukcu & Cemal Akturk	2020
	Exploring Students Online Learning: A Study of Zoom Application	Dr.Shahid Minhas, Tasaddaq Hussain , Abdul Ghani, Kiran Sajid	2021
Credential Hacking Issues and its effects	Cyber Attacks in the Era of COVID19 and Possible Solution Domains	Isaac Chin Eian, Lim Ka Yong, Majesty Yeap Xiao Li, Yeo Hui Qi, Fatima Z	2020
	What is Credential Stuffing?	Debbie Walkowski & Jarrod Overson	2020
	Credential Spill Incidents Double as Hacker Sophistication Continues to Rise	Dan Woods & Sander Vinberg	2020

B. Identity and Access Management

The definition of IAM refers to the regulation of a system that allows the right user to have the right access to a specific reason. Identity and Access Management has the capabilities to approve or decline when the same identity is used in an application to ensure security (I.Indu, P.M. Rubesh Anand, Vidhyacharan Bhaskar, 2018).

As technology advances, more and more people have started to use online applications and the cloud to store their data and information. This has increased the challenges for businesses to safeguard the user's access while observing data regulations at the same time. Therefore, implementation of IAM in a system is very crucial in the area of security issues. This is because IAM systems are very efficient mechanisms in terms of the risk reduction in the organization's system. For example, mechanisms such as web access request, user provisioning, multi-factor authentication, enterprise single sign-on, privileged identity & access control and user activity compliance are included (Ishaq Azhar Mohammed, 2017).

TABLE II. IAM VS PAM (I. INDU, P.M RUBESH ANAND, VIDHYACHARAN BHASKAR, 2018).

IAM VS PAM			
	Mechanism	**Security Aspects**	**Attacks**
Identity and Access Management	Credential Synchronization, provisioning & Identity Federation	Any users that require to access the system	Synchronization leakage, Identity Theft, Data Tampering Attack & Spoofing Attack
Privileged Access Management	Shared access password management, Privileged session management, application access management	Privileged/ Administrative Access	Phishing Attack, Identity Theft, Synchronisation leakage

Referring to Table II, it can be seen that there are two types of access management that have been compared, each of them has similarities and differences. In the proposed system Identity and Access management will be implemented as it is more suitable to have in a LMS application. This is because Privileged Access Management mainly focuses on users that have privilege or administrative access to the system while Identity and Access focuses on any users that have access to the system. For example, it has security aspects where it will only allow the right person to access the right resource at the right time. Not only that, Identity and Access management uses the credential synchronization, provisioning & Identity Federation as its mechanism. Hence, it is dedicated for attacks such as synchronization leakage, identity theft, data tampering attack & spoofing attack.

C. Learning Management System

During this epidemic, the education environment has changed completely. Many institutions are forced to change their teaching method from face-to-face classes to E-learning due to the daily increases of covid-19 cases in every country (Dr.Shahid Minhas, Tasaddaq Hussain, Abdul, 2021). However, to completely convert face to face classes into E-learning it requires both parties from the student side and the teacher side to have a learning management system. The term LMS (Learning Management System) can be defined as a form of application software that uses pre-programmed instructions to guide all learning activities and it can store and retrieve the learning contents (Davis et al.2009) (Lamichhane et al.2007). LMS does not only support the learning industry, but it can also use it in the business and industrial spheres, it is just that people mostly use it as the education sector which affects it to have the highest percentage around the globe. On the other hand, LMS does not only use them for formal teaching, sometimes it can also include some informal learning such as students are able to communicate through the chat box or share their screen to watch videos together in the class. Not only that, it can also be used to carry out curriculum in LMS as it enables users to have ample space for interacting and sharing their content to everyone (Cedric Bheki Mpungose & Simon Bheki Khoza, 2020). There are many types of LMS nowadays such as Moodle, Google Meets, Learning Space. Angel, Blackboard and Zoom. Zoom has been one of the hot usage applications for users all around the world since the Covid-19 global epidemic. This is because when zoom invited speakers from America who did not use zoom before to conduct 18 zoom sessions and none of them had issues such as audio issue, video issue, screen sharing issue or messaging issue. It is the reason why many people prefer using Zoom as their main video conferencing application or even E-learning tools (Ceren Cubukcu & Cemal Akturk, 2020). In conclusion, out of so many LMS, zoom application has been picked as the research target to further elaborate the Credential Hacking issue within the LMS application, Zoom.

D. Credential Hacking Issues and Its Effects

The dependency of the internet nowadays has been increased in a way that is unpredictable because of various

online activities such as working at home, having classes by using online applications, and many more. This is where cybercrimes such as credential hacking issues occur. This kind of attack targeted the victims credential data through networks or applications that are not safe. By utilizing the programming code, it can find out the ways to crack the access point of the internet and once they have successfully hacked into the network or application, they will be able to do illegal activities (Isaac Chin Eian, Lim Ka Yong, Majesty Yeap Xiao Li, Yeo Hui Qi, Fatima Z, 2020).

On April 21st, 2020, during the busiest time where people were busy working on fighting the pandemic, the first case of credentials theft happened. One of the organizations who work to fight against Covid-19. The World Health Organization (WHO) has been targeted by the hackers. It is reported that the hackers were able to find out email addresses and passwords on online websites such as pastebin and twitter. Not only that organization has been targeted by the hackers, due to most of the people working from home. Zoom applications has fallen into the hacker's target where there were credential stuffing attacks in the application, the hackers were able to attack the victims account because zoom does not compare registration usernames and passwords with breached accounts details. It has been reported that more than 500,000 zoom accounts were selling on the dark web (CPO Magazine, 2020).

Although credential hacking attacks have existed for many years, some of the organizations may even have some prevention method to the attacks but one of the reasons that the attacks still work is because many users use the same password for other application accounts. This will have a negative impact where when some application has weaker security will be credentials theft and when the hacker obtains the legitimate credentials from the specific application it will then test the password on other website and when the website is sometime important for the user such as their bank account, that will be a big issue for the victim (Dan Woods & Sander Vinberg, 2020). However, there are some precautions that can be used by the victim. The victim should use a unique password for every account, or they can use websites such as haveibeenpwnd.com to see if your credentials have been compromised or not (Debbie Walkowski & Jarrod Overson, 2020).

III. SIMILAR SYSTEM

A. *IAMSys*

IAMSys is an Identity and Access Management system by using the Lightweight Directory Access Protocol (LDAP) to create. This system utilizes the ideas of IAM to focus on authentication, authorization, administration, or the identities of each user as well as to do audit reporting. With this system it could provide safety and more privacy towards the user's data and information as the admin could grant the correct level of access to the user in either the cloud environment or in the system. Fig 1. will provide a clearer explanation regarding the proposed system (Mohammed Kabiru Hamza, Hassan Abubakar, Yusuf Mohammed Danlami, 2018).

According to Fig. 1, it is the create permission page where it is to define what document can the user access based on the access policy. At this stage, the user is allowed to enter the URL to see if it is accessible (Mohammed Kabiru Hamza, Hassan Abubakar, Yusuf Mohammed Danlami, 2018).

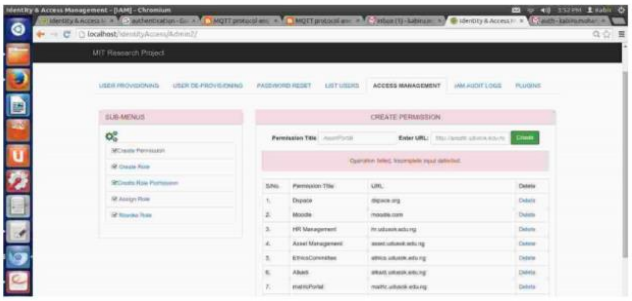

Fig. 1. Access management module displaying permission creation

In Fig 2., this page allows the admin to create roles for each user (Mohammed Kabiru Hamza, Hassan Abubakar, Yusuf Mohammed Danlami, 2018)

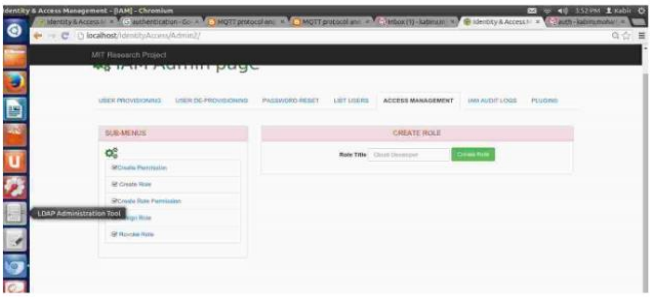

Fig. 2. Role creation page

In Fig 3., when roles are created, at this stage the system checks the permissions and roles that are mapped to see if the specific role will be able to view the URL or not (Mohammed Kabiru Hamza, Hassan Abubakar, Yusuf Mohammed Danlami, 2018)

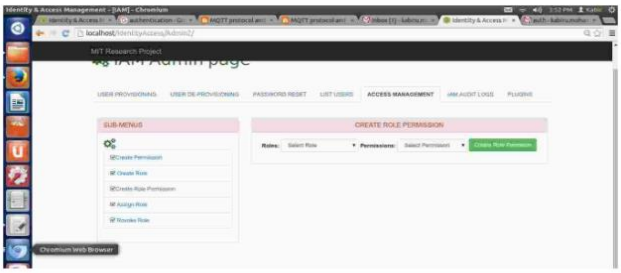

Fig. 3. Role permissions mapping page

In Fig 4., the purpose of the role is to assign users to the IAM system, and more than one role can be assigned to a user. With that means, if the website is only eligible for the authority to view, but the current user is just a normal user. Admin of the system can put an extra role for the normal user to become the authority so that they can see the content (Mohammed Kabiru Hamza, Hassan Abubakar, Yusuf Mohammed Danlami, 2018).

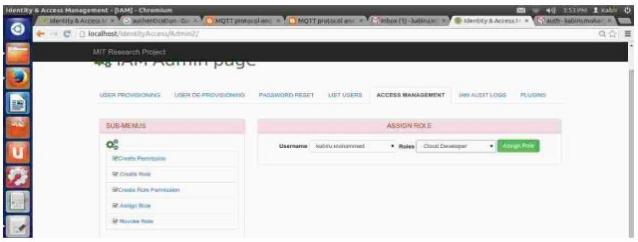

Fig. 4. Role assign page

In Fig 5., admin is allowed to revoke the user from the IAM system if the user does any suspicious activities on the website (Mohammed Kabiru Hamza, Hassan Abubakar, Yusuf Mohammed Danlami, 2018).

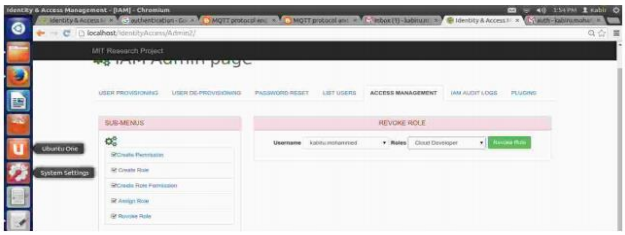

Fig. 5. Revoke role page

In Fig 6., the log report page where the admin can view the users' activity on the system (Mohammed Kabiru Hamza, Hassan Abubakar, Yusuf Mohammed Danlami, 2018).

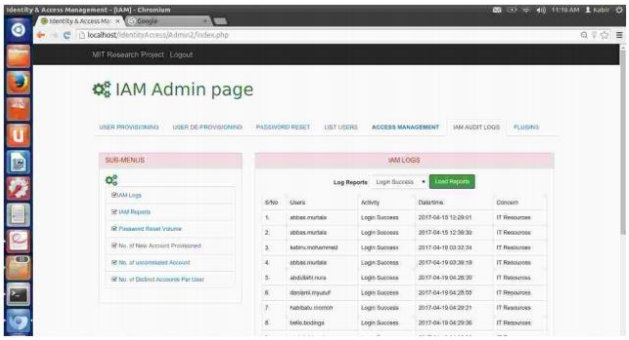

Fig. 6. Log Report Page

Figure 7 is the list of the user's page; the purpose of this page is to see which group the admin user has targeted. For example, ou=academic, ou= staff, ou=people, dc=udusok, dc=edu (Mohammed Kabiru Hamza, Hassan Abubakar, Yusuf Mohammed Danlami, 2018).

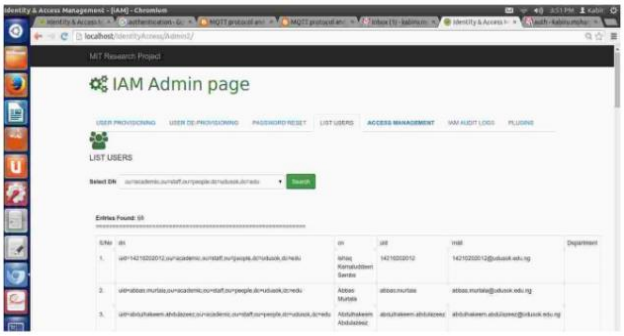

Fig. 7. List of the Users Page

B. *OneLogin*

OneLogin was invented by Thomas and Christian Pedersen. The idea of them creating OneLogin was to implement the identity & Access management solution to be used on cloud applications businesses. OneLogin was launched in 2010 and it has partnered with leading SaaS vendors such as Facebook, google drive, office 365, twitter and many more (OneLogin, Inc, 2020).

Fig. 8. Company which OneLogin supports

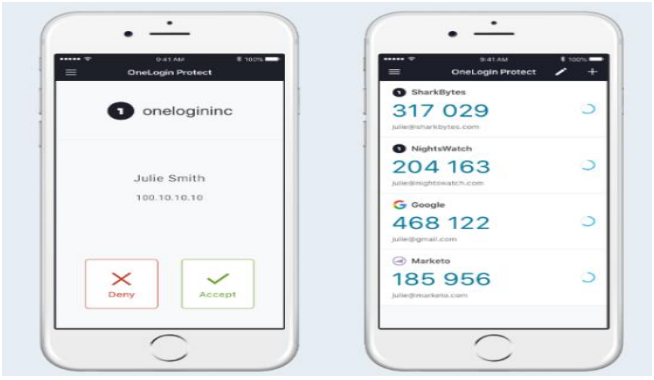

Fig. 9. OneLogin Protect

The purpose of building OneLogin is to provide a seamless, integrated user experience for multi factor authentication. In OneLogin, the user can simply just click a button and it will automatically sign into the specific application that they want to go to. This would be very beneficial towards users that have many accounts in different applications as OneLogin has a function called OneLogin Protect, once it is accepted in the application user can just use the OTP to sign into those applications (Multipoint Group, n,d).

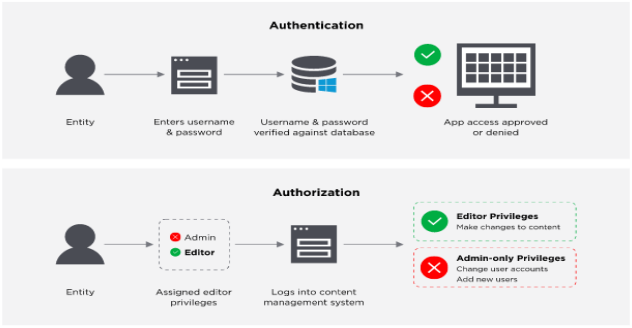

Fig. 10. Authentication VS Authorization

According to Fig 10., OneLogin ensures that the user is really themself by authenticating their credentials against a database. Besides, they only grant the appropriate level of access. Therefore, it only allows the specific people to be portioned out in a specific content management system (OneLogin, Inc ,2022).

IV. Problem Statement, Aims and Objectives

In 2020, students utilizing online E-learning platforms to receive their education has become something ordinary and also raised to be the point of concern. This is due to the anxiety that everyone has towards the online education platform's data security and privacy. The reason for students utilizing online learning platforms to keep up their study was because in March 2020, many countries were forced to close down their schools due to the cause of the coronavirus outbreak (Ceren Cubukcu & Cemal Akturk, 2020). This issue has forced the students and teachers to stop formal education activities and convert it to E-learning. Therefore, the majority of the students around the world are currently utilizing learning management systems (LMS) to continue their studies. This action was made to provide digital supplements that could overtake the issue where students need to study in the classroom.

However, a free online learning platform such as zoom was the choice of many schools as zoom was one of the free platforms to be used for conducting online classes. The rapid rise of users from 10 million active users in December 2019 has been raised to 200millions active users as of April 2020 (Adam Aiken, 2020). Thus, this expeditious increases have been targeted by the hackers, according to the research from IntSights' there are over 500,000 account's credentials of video from Zoom platform has sold on the dark web forums and hackers were able to share the database which consist of nearly 2300 usernames and passwords that are from Zoom's accounts (maor, 2020). Not only does this record consist of educational accounts but many corporate accounts belonging to banks, consultancy companies, healthcare providers and many more.

The data center of the zoom company is another thing to be concerned about, it is reported that zoom only uses transport encryption. This will allow hackers to have advantages of the user's credential as transport encryption allows data to transfer over the internet and on internal networks, which also means that if hackers are able to connect to zoom's internal networks, they will be able to easily obtain the credentials of an user.

Nonetheless, regarding the corresponding situation, there are some recommendations that the researchers will propose to be implemented in the application to minimize the chances of being credentials theft. The main aim of this research is to develop identity and access management to mitigate the data security & privacy issue in zoom applications.

- Minimize the chance of getting credentials hacked
- Develop a system that can secure access across computer network and user credentials
- System able to detect and block the hacker from stealing the credential of a user.

V. Methodology

A. Respondents

In this survey, around 200 Zoom application users from different backgrounds will be joining the research investigation by using a random sampling method. The reason for having around 200 respondents to take part in the investigation is because researchers will be able to obtain more information from different perspectives but not just from a person's feedback.

B. Sampling

In this survey, the researcher will be using simple random sampling as the sampling method. Random sampling is a technique which allows each sample to have an equivalent probability of being chosen. The purpose of this survey was to find out if users have any preferences regarding the recent credential hacking issues that happen in the zoom application. By using this simple random sampling method smaller sample size will be cull from a larger population and will be able to utilize it to make generalization. Not only that, by using this technique, it is easy to use and will be more accurate when it is performed in a larger population survey.

C. Data Collection

In this data collection procedure, the researcher has used both quantitative and qualitative questions in the questionnaire's method. Utilizing questionnaires allow a faster, efficient, and inexpensive result to be obtained. Moreover, it is preferable to perform in gathering large quantities of information from a sizable sample capacity and also it will be more effective to measure the behavior, preferences and the respondent's opinions. In the questionnaires, it consists of 10 multiple choice questions and 10 yes and no questions. The multiple-choice questions consist of content such as the proposed system usability and efficiency, while the yes and no questions are questions to ask respondents if they have any knowledge and the effectiveness of implementing identity and access management into the zoom application.

VI. Overview of the Proposed System

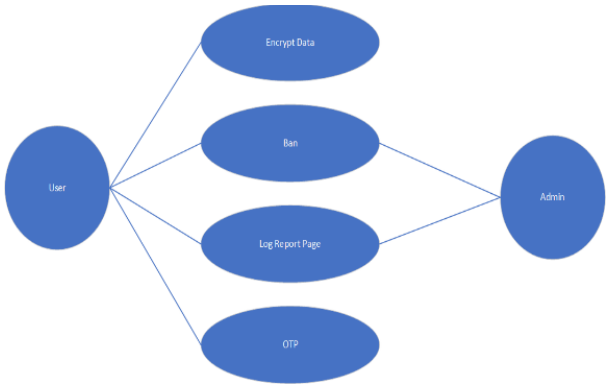

Fig. 11. Proposed system flow chart

DefenseZoom is a mobile application that is designed for IOS or OS. It uses the technologies of Identity and Access Management to implement it into the Zoom Application. By using the DefenseZoom application, the application will have the identity and access management technologies where it can detect unauthorized users such as credential theft from accessing. However, there are few steps in order to make sure that the user's account is safe to log in. The users need to link their zoom account to the application and when they want to log in to their accounts, they are required to provide the third factor verification where it can be obtained from the DefenseZoom application. Users need to press the OTP button to obtain third factor verification and once it is pressed, it will require the user's fingerprints or face verification of the user

in order to get it. By using this method to login, the admin will receive an alert of someone has accessed the Zoom application with a correct procedure, there will be a log report button in the application to let users and admin check if there are any third person accessing the accounts or not. Nonetheless, if there are third people accessing the account that the user does not know, the Ban button can be pressed in the application, and it will allow the user to select the suspicious account that has entered to be banned from the zoom applications. To completely secure the data and privacy of each user, the Encrypt Data button needs to be pressed and make sure that a message box "Data is Secured" appears. This button has implemented the AES-256-bit encryption technologies to secure the data of each user. Even Though Zoom application has its own encryption method, once the intruders were able to crack into their account, the user will have no alert against it but with the implementation application, if the encryption is cracked, a notification will be sent to both user and admin, and they can take action immediately.

VII. CONCLUSION

Throughout this research article, the researchers were able to find out the problems that were existing in the zoom application and implemented an application that can benefit society. With the application, organizations can take early precautions before letting the hackers steal the user's credentials in the application. With the newly implemented application, is it believed that the credential hacking rate will slowly drop until this issue passes from sight.

REFERENCES

About Us: SSO & MFA Provider Since 2010. (2022). OneLogin. https://www.onelogin.com/company

Aiken, A. (2020). 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 on Censorship, 49(2), 24–27. https://doi.org/10.1177/030642202093579 2

Ceren Çubukçu, & Cemal Aktürk. (2020, June). (PDF) THE RISE OF DISTANCE EDUCATION DURING COVID-19 PANDEMIC AND THE RELATED DATA THREATS: A STUDY ABOUT ZOOM. Www.researchgate.net. https://www.researchgate.net/publication/342561504_THE_RISE_OF_DISTANCE_EDUCATION_DURING_COVID-19_PANDEMIC_AND_THE_RELATED_DATA_THREATS_A_STUDY_ABOUT_ZOOM

Dan Woods, & Jason Rahm. (2022). Credential Spill Incidents Double as Hacker Sophistication Continues to Rise. Www.f5.com. https://www.f5.com/company/news/feature s/credential-spill-incidents-double-as-hack er-sophistication-conti

Eian, I. C., Yong, L. K., Li, M. Y. X., Qi, Y. H., & Z, F. (2020). Cyber Attacks in the Era of COVID-19 and Possible Solution Domains. Www.preprints.org. https://doi.org/10.20944/preprints202009.0630.v1

Hamza, M. K., Abubakar, H., & Danlami, Y. M. (2018). Identity and Access Management System: a Web-Based Approach for an Enterprise. Path of Science, 4(11), 2001–2011. https://doi.org/10.22178/pos.40-1

Indu, I., Anand, P. M. R., & Bhaskar, V. (2018). Identity and access management in cloud environment: Mechanisms and challenges. Engineering Science and Technology, an International Journal, 21(4), 574–588. https://doi.org/10.1016/j.jestch.2018.05.010

Ishaq Azhar Mohammed. (2017, July). (PDF) Systematic Review Of Identity Access Management In Information Security. ResearchGate. https://www.researchgate.net/publication/353887659_

Minhas, Shahid & Hussain, Tasaddaq & Sajid, Kiran. (2021). Exploring Students Online Learning: A Study Of Zoom Application. Gazi University Journal of Science. 34. 8. 10.35378/gujs.691705.

Mpungose, C. B., & Khoza, S. B. (2020). Postgraduate Students' Experiences on the Use of Moodle and Canvas Learning Management System. Technology, Knowledge and Learning. https://doi.org/10.1007/s10758-020-09475-1

OneLogin. (n.d.). Multipoint VAD. https://multipoint-me.com/onelogin/

Secara, I.-A. (2020). Zoombombing – the end-to-end fallacy. Network Security, 2020(8), 13–17. https://doi.org/10.1016/s1353-4858(20)30 094-5

Walkowski, D. (2020, October 13). What Is Credential Stuffing? F5 Labs. https://www.f5.com/labs/articles/education /what-is-credential-stuffing-