Proceedings of the International Conference on Smart Electronics and Communication (ICOSEC 2020)
IEEE Xplore Part Number: CFP20V90-ART; ISBN: 978-1-7281-5461-9

A Study of Security Threats in Cloud: Passive Impact of COVID-19 Pandemic

Sudakshina Mandal
Department of Computer Applications
National Institute of Technology, Jamshedpur
Jharkhand, India
2018rsca002@nitjsr.ac.in

Dr. Danish Ali Khan
Department of Computer Applications
National Institute of Technology, Jamshedpur
Jharkhand, India
dakhan.ca@nitjsr.ac.in

***Abstract*—Recently, the life in Earth becomes turbulent with the worldwide spread of novel coronavirus (COVID-19). This outbreak has been declared as a public health emergency in the level of international concern by world health organization (WHO). To reduce the spread of COVID19 entire world has adopted social distancing, where working and learning from home is the new normal for this new world. To sustain the economical revenue and business growth companies that radically move into cloud infrastructure to support employees, who work remotely. With the unprecedented growth of cloud, data breaches and cyber security takes a huge leap. Apart from big cloud vendor small cloud startups are getting huge leap currently. Starting from enterprise solution providers, cloud supports in education, e-commerce, and healthcare also. Hackers penetrating not only the cloud resources it also hampers the hosts and device connected with it. This paper discovers several security challenges due to the sudden use of cloud platforms without adequate precautions. The aim of this paper is to highlight these areas causing security breaches and propose generic preventive measures.**

Keywords— Cloud security, COVID-19, coronavirus pandemic, cyber-attack, data breaches

I. INTRODUCTION

The cloud faces visible rapid growth in the last few decades. The business of renting computing services has transformed enormously with the help of leading cloud vendors like Amazon, Microsoft, and Google [1] [7]. Besides these major players, small and medium-sized businesses (SMB) also adopted cloud services thus the beginner startup cloud strategies have also got a huge spike in the last two decades. But shifting to remote working in Coronavirus pandemic [2] gives an unexpected spike in cloud uses to manage internet infrastructure and adjust the computing needs. As a passive effect of COVID-19 to ensure the seamless work from home facility and to maintain the access the critical resources and improve scalability, organizations adopted cloud at a steady pace [8]. COVID-19 plays a catalyst for faster growth of the cloud this season. The organization aims to confirm the safety and reliability in remote working. Besides due to the severe economic recession in the fiscal year 2021 companies will cut the hardware spending which in turn substitute by cloud solutions [3]. By looking at the present situation the usage of Software-as-a-service (SaaS) and cloud storage strategies have increased in the maximum level to handle the real-time data [4]. Not only is the enterprise solution the cloud usage spread across education, healthcare, e-commerce, and supply chain industry also. The situation only slightly improves looking ahead to 2021, with 84% expecting a continued impact. And 74% of respondents expect a second wave of COVID-19 impact, with 51% planning to move more applications to the cloud to prepare for it. According to the recent trends in the adoption of cloud with the availability of the internet and high bandwidth ensures revenue despite the remote login but the cons in that sudden shifting to cloud increased the traffic and security issues cyber world along with data breaches. As a passive attack in COVID-19 pandemic, several cloud medium has got affected and the attack of cyber threat will also increase in the future. Not only cyber threats, data breaches, but network breaches are also common penetration points of attack. As the security concern is always a primary objective which needs to ensure, we must look into the problem arising due to work from home scenario. In March to June survey conducted by Verizon says that 474 data breaches cases reported across the world where 80% of the breaches are caused for hacking, stolen data, and brute force attacks [5]. The same survey also reported among the 32,012 security cases 3950 cases were confirmed data breach attack which is the double in an amount from their last survey (2013). 81 global contributors from 81 countries participated in this survey [6]. Another survey conducted by Microsoft blog reveals that from March the usage spike to 775% in Italy shortly just after declaring lockdown [7].

Generally, the rapid growth of cyber-attack when increases day by day across the world which not only affected the real-time data in the cloud, it hampers the host's personal space also [8]. As we all know cloud strategy comes with stringent security protocol with an adequate compatible structure that suites the business needs. But shifting to cloud in hurricane fashion forces the world to access real-time data from their personal workstation which is connected to the internet with the local service provider or mobile operator which is outside of enterprise zone in turn untrusted. This situation not only increases the cyber-attack, but the attacker also penetrates the host's IP address and making it the victim of Trojan horse attack, ransomware attack, spoofing of IP, MAC, etc. Now the question is the huge amount of breaches is caused only because of the use of cloud strategy is a rapid manner? The answer will be no,

where we must restructure the security policy according to the recent trends of spoofing, apart from this cloud resources have been used in several inefficient manners. Unskilled and lack of proper knowledge of individuals is another reason for cyber –attack. When the whole world is threatened by the coronavirus pandemic spoofers took the advantage and make people victimized to use this. Apart from accessing the working essential engagement of leisure activities make the cloud prone to data breaches. Overall from the above mentioned survey, it is seen that apart from the IT industry, education, healthcare sectors are affected by these scams.

Considering the current scenario this paper discusses the several cyber-attack which make the cloud resources as well as hosts vulnerable. The social impact and precautions have also discussed here.

The rest of the paper is organized in the following manner. Section II presents possible security concerns, In Section III recent security attacks are discussed and Preventive precautions have proposed in Section IV and Section V concludes with the conclusion and future work.

II. POSSIBLE SECURITY CONCERN

A. Remote Learning: Expansion of Security threats

Shifting to the digital era in this pandemic is comparatively a drastic decision worldwide. The education system followed the traditional system so far. But to confirm the social distancing over 1.2 billion students and faculties are at home and ensures distance learning [9]. This pandemic brings the offline education industry to the mainstream online model in an amplified manner. Millions of teachers, students are dependent on video lecture software, online chat messages, lesion portal to support distance learning [10]. Automatically cloud based software and storage system are in the frontline which are adopted in hurricane fashion by the education industries. But the dedicated budget, ill-equipped infrastructure, and without efficient manpower any resources become vulnerable and become prey for the cyber security attackers. The coronavirus pandemic has had major cyber-security implications around the world. Tailored phishing attacks and contact-tracing scams prey on fear and uncertainty. According to a recent survey by the Department for Digital, Culture, Media, and Sport, 80% of UK higher educational institutions, 76% of secondary schools, and 41% of primary schools have experienced a breach or attack in the previous year, compared to 46% of all UK businesses.
Causes of some of the major security breaches are discussed in following [11]:

1. **Data Breaches:** The database of any education industry is a goldmine of potential. By exploiting the university database can leads to a severe data breaches. For cyber-criminals seeking high-value targets, educational institutions are especially attractive. Essential to society and the economy, schools and universities also store reams of sensitive data. Without proper authentication and using it from dispersing a hierarchical level become the prey for attackers.

2. **Unskilled Usage:** With the fast pace of transition to the cloud system, the education industry faces a severe problem as most the persons are not aware of this cloud security as well as they don't have any proper training. Without knowing any security protocol and proper usage of online services resources become vulnerable. In maximum cases, students and parents don't have that much-dedicated knowledge of cloud services which leads to unintended exposure.

3. **Psychological Effects on Cyber Security:** Colleges and universities deal with the pupil's age group of 18-22 years. They have a psychological tendency to break any rule. By learning ethical hacking and with the help of intelligence they can break the password and disrupt the system. Scamming email is one of the major attacks in this situation. By creating duplicate id with the similar name of the authority they threaten people and by clicking unintendedly victimized by this type of attack. The following figure is an email phishing attack where someone impersonates the director of a university and send an email [12].

4. **Attacks Due to Using Dark Web**: Teenagers have a curiosity to explore new things and experiment. Cyber security and the concept of the dark web is getting popular. Many people use the same credentials with their officials which unintendedly drawn to this cybercrime world.

5. **Attacks on Video tutorial software:** In this situation to continue the learning faculties depends on video tutor or video conferencing app like Zoom, Cisco WebEx, Google Meet, Blackboard, etc. But in some recent attacks, it is seen that at the time of sharing the screen with the students gets harmful for the teachers. Hacking does not limit to stealing the credentials and contact details but it gets access to any screen which are open in the workstations simultaneously.

6. **Phishing Scams:** By creating fake websites by the name of the cloud vendor also leads to the unintended exposure of resources in the education industry. Without knowing the security protocol it is hard to find any phishing scams.

7. **Attacks on Hosts:** Besides cloud software by the name of face vector attackers forced to download materials which in turn inject Trojan horse, malware spoofing and IP stealing attacks.

8. **Ransomware Attacks:** It is easy to prey the cyber security attackers to vector the students by stalking their activity and demand money instead.

9. **Email Scams:** By phishing any institute email id or administration's email, attacks have occurred where rumours were spread about coronavirus pandemic which leads to an unperceived situation among the education sector.

B. Impact of Enterprise in the support of Work from home

Though the adoption of cloud has already captured the IT market, this health crisis gives a huge essential boost to cloud services. Collaborating with remote working enterprise have to move on the cloud without any restrictions. The use of personal workspace does not correspond with existing stringent security policies which leads to severe attacks these days. It is true that with the increment of cloud usage, cyber attackers make the prime vector by penetrating the loopholes which are discussed below [13].

1. **Without Proper Authorization and Authentication**: Remote workstation does not ensure the industry-specific authentication mechanism (i.e biometric) to use enterprise resources which is the rudimentary point of attacks.

2. **Connecting Through Home Network**: Connecting to the enterprise resources hosted in cloud server employee's use their untrusted network service provided by local service providers or mobile network which does not possess any privacy protocol. Exposing through Internet service providers (ISP) causes spoofing attacks (ARP spoofing, IP spoofing, MAC spoofing), DDoS attacks. Besides DNS Hijacking, DNS snooping, Cache spoofing are some major attacks which are can breakdown the system through network connection[14] [15].

- **Exposure of Resources:** In the present situation irrespective of the designations, enterprise resources can be available to the subordinate employees which leads the risks due to unskillful nature. Lack of proper training of security measures and restrictions of cloud services makes people ambiguous. Unintended clicks make the workforce vulnerable to security breaches.

3. **Lack of Budget for Up-Gradation**: When the security policies need a radical change to support remote working, in this situation due to lack of revenue and economic growth they decreased the dedicated budget in this fiscal year.

4. **Social Engineering Attacks**: The most common cyber-attack is the social engineering attack in this health crisis. Cyber-attack is a human problem where the attacker finds keyboards or visual screen as the weakest point to trick us into divulging sensitive information. This widely remote working situation gives a suitable opportunity to take advantage of this changed behaviour. Relevant social engineering attacks are described below [16].

5. **Phishing Scams**: Sharing the sensitive work details through email or any other social media like WhatsApp, messenger leads to severe phishing attacks in recent days. Phishing email id is a common practice, where the scammer sends some email pretending an official email, and employee's often get victimized by this type of attack. This attack is caused by any WhatsApp group or messenger also [17]. Phishing can be of several types depending on the nature of attacks. Two Email phishing instance is given below for an example (Fig. 1) [20] where the attacker impersonate an authority and make the users victim. From Fig 1ii), It is seen that a spoofed link is given for phishing.

   - **Shoulder Surfing Attacks:** In remote working, it is impossible to ensure authentication through any third party authentication device or by checking the MAC address of the workstations. When users have authenticated themselves by using keyboard stroke, shoulder surfing attacks can be one type of recent attack which can be done by any insiders with or without intention.

   - **Spear Phishing Attacks:** Gathering of interest and choice from an online chat group or any social platform is not tedious for scammers. By collecting the relevant information about any person, they target the hosts as their prime prey. Sharing of scammed email, SMS in the common attack.

   - **Scareware Attacks:** Transferring to the cloud system needs proper training and skill for all the employees. In the current situation, organizations run their business without proper knowledge or skill. Victimized can easily involve in fictitious scam or false alarm that their system might get affected. Scareware can be through email or pop up, messages [19].

   - **By changing the URL:** By altering a URL address scammers can get the credentials of the targeted victim. If 'http://www.facbook.com' is created with the same look & feel which coexist with http//www.facebook.com. Usually, people just type first two or three letters of any website which have already opened from that machine. Naturally, the targeted URL will appear before the original website. By clicking on this scammed link authentication details have easily got exposed.

- **The benefit of Interest**: utilizing ample time in peruse passion or hobby is engaging people. Most of the people are doing to follow the new trend in social media. By utilizing cloud service people uses photo, music, video editing applications. Surfing online video to engage in new gaming platform needs login credentials which can be an attacking door. By sharing the same window with the working platform with more dangerous where the attacker can easily penetrate by collecting the cookie.
- **Password Cracking Attacks**: Authentication through keyboard or mobile device identifies the MAC address of the remote workstations. Without having the third party authentication system makes the contacts more vulnerable where hackers can hijack the password by keyboard stroke random guessing.
- **Unable to Control Cloud Data Centre**: In the current scenario, every cloud datacentres are handled by a cloud service provider (CSP's) which is also a point to consider for breaches.
- **Video Conferencing Attacks**: enterprises installed different video conferencing applications in support of remote work which gives a huge spike in Zoom, Slack, Google Meet, WebEx Cisco . Some recent attacks on these apps do not possess the security of the hosts and the cloud resources at all.
- **Cross-Site Scripting, SQL Injection, Man-in-the-Middle Attack, and Reply Attacks:** These are some most common attacks of cloud security breaches that cannot be overlooked in this remote login perspective.

C. In the perspective of Healthcare, Banking, E-commerce, Entertainment in this outbreak:

1. **E-Banking and Transferring Money**: Sometimes it might happen we cannot understand if any spoofed already happens in the workstations. This situation becomes dangerous when someone transfers money even though SSH secured a website or accessing the banking portal.

2. **Unskilled Use of Banking Website**: In this restricted health outbreak cases people rely mostly on online banking. We can found a different group of users using the e-portal for emergencies without much knowledge about security protocol. Unskilled use of the banking portal remains open when customers forget to log-out. This situation becomes prey for the attackers recently.

3. **Attack through Coronavirus Safety Apps**: Spreading malware through coronavirus safety app and gaining contacts is another infected area in this pandemic. Thousands of coronavirus website have been created for this spoofing. Besides applications running in the current situation do not possess ultimate trust where some recent attacks occurred.

4. **Spikes in Online Purchase of Essential Goods**: In pursuit of purchasing online essential goods like medicines, grocery items local online e-commerce portal making money. By stealing the customers' information through mobile number or email address hackers can penetrate their login information and penetrate their banking details too.

5. **Using Dark Web**: Recent days the world is panicking and checks daily updates coming in the WhatsApp /Facebook or any other link. Unintended clicks and the tendency to know the news drive the world to the dark web. Maximum time users get exposed by an unintended click of these unauthenticated links. Google does not ensure any centralized search engine. The concept of the dark web is called onion domain where the domain of the portion is exposed to the entire world. By clicking this type of link and news people are itself creating an entry point of hackers.

6. **Intruder Attacks:** For more interest, people download the rigorous application (games, movies, personal interest apps) from anonymous links in their phone or workstations by using similar authentication details. By making this as an entry point intruders steal MAC address, IP address of potential.

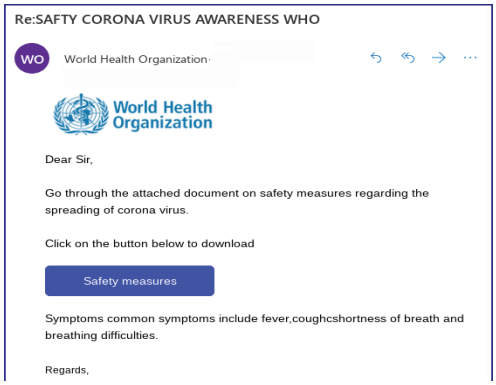

Fig 1 i): Phishing by impersonating WHO [20]

Fig 1ii): Phishing Attack by giving a link for spoofing [20]

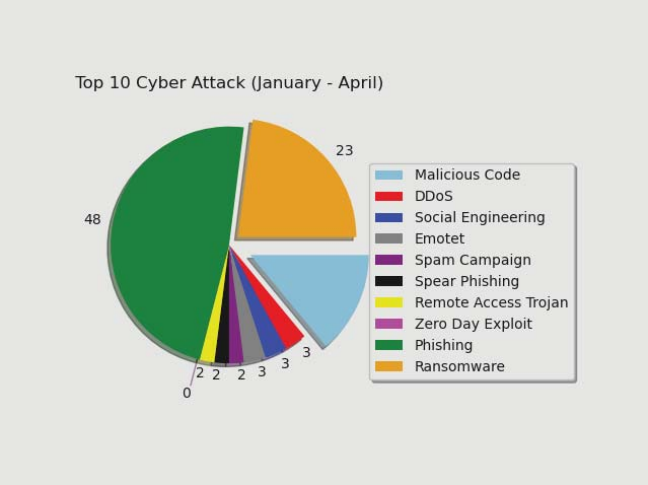

Fig 2: Top 10 Recent Attacks based on statistics of [25]

III. SOME RECENT ATTACKS

In this coronavirus spreads some of the recent worldwide occurred security breaches have been briefed.

On a report of Kaspersky, 93 COVID-19 related malware in Bangladesh, 53 in Philippines, 40 in China, 23 in Vietnam, 22 in India , 20 in Malaysia till 14th March ,2020. They have also reported email scams worldwide. A recent scam impersonating World Health Organizations (WHO) demonstrating how cybercriminals recognize and are capitalizing on the important role WHO has in providing trustworthy information about the coronavirus [21]. On a report of WHO on 23rd April, 450 Active email addresses along with passwords have been exposed in coronavirus pandemic [22]. Within a very short span of time Zoom Meeting App becomes a vector of the data breach. In the first week of April 2020, 500,000 stolen passwords were up to sale on the dark web. More than half of the millions of login credentials, host keys, meeting URLs were sold for less than a US cent each. Not only Zoom, Google, and Microsoft video conferencing apps were the lucrative victims of cyber-attack by creating fake meeting URL, my email phishing like "You have added to a Google meeting". Over the last 3 months, 192,000 coronavirus related breaches have been reported by phishing email and domain. Cyber attackers created history by hacking twitter on July 15, 2020. Among the 150 targeted account, 45 twitter account was reset and fake tweets were sent $2000 for $1000 sent to an unknown Bitcoin address. The Twitter breach well-coordinated scam made attackers swindle $121,000 in Bitcoin through nearly 300 transactions [23]. In April 2020 Magellan Health was stuck by a ransomware attack and 365,000 patients were affected in the sophisticated cyber-attack. Cybercriminals are increasingly targeting the financial services sector during the Covid-19 coronavirus pandemic, with attacks on banks and other financial institutions spiking by 38% between February and March to account for 52% of all attacks observed by VMware's Carbon Black Cloud [24]. According to the statistics of Fig. 2 shows the recent attacks in the period of January to April 2020 conducting by a survey reported in [25]. From the graph it is clear the majority of the cyber – attack is caused by phishing.

IV. SOME PREVENTIVE FOR CLOUD SERVICES

Irrespective of existing security policies cloud services face severe cyber security data breaches in coronavirus outbreak. As a preventive, some measurements can stop spreading the cyber threat [23] [26].

- To ensure the authentication of workstations or hosts, a strong password policy should be taken and a multi authentication policy should be adopted.
- Using external USB devices should be prevented when connecting with an enterprise's cloud services.
- Organizations should create any training session about security preventive and awareness to individuals.
- To stop social engineering attacks, always check the email address, URL before clicking. Unintended clicks are strictly prohibited to avoid phishing scams.
- The shared file system (Dropbox, Google drive etc.) should be used as a communication medium between employees. Sharing files through a free email address or any social media group is strict NO.
- For video conferencing, always allow the users to join after the admin joins. Beware of sharing screen.
- Back up all the files to the hard disk before sharing it to the cloud medium.
- Before download, any random application check the source of this application.
- Always maintain a sign-out pattern after using cloud services.
- Keep all your software and applications updated with the latest security patches from time to time
- Email domain security can be provided against email spoofing attacks through DMARC, SPF, and DKIM protocols.
- Incorporate phishing scam response tools in workstations.
- Always verify the spelling and grammar of any link before clicking.
- Look into the generic greetings like 'Dear Sir/Madam'. This randomness usually specify phishing attack.
- Avoid emails which insist to act immediately and emails containing any prize winning money or any serious loss (eg: Lost of ATM card).
- Avoid mixing of official work and personal interest in the same workstations.

- Avoid clicking and downloading from anonymous websites.
- Be cautious about online payment. Always verify before any payment against some cause.

V. CONCLUSION & FUTURE WORK

In this paper we have discussed the security concern irrespective of the IT industry, Education, Banking sector based on the recent perspective. We have witnessed several cyber security attacks in this healthcare emergencies in the period of March to July. This paper presented all the security concerns for causing attacks with some recent attacks description as a literature study. Though we have not find any proper article or journal regarding these in very short period of time we suggested some generic preventives which can be followed. Mainly the paper is presented by referring blogs, websites, white papers of several companies and few journals. The aim of this paper is to create an awareness among society regarding these attack and recommendation of the needfulness of security policy modification .Social engineering attack has clear elevated graph by comparing with previous year which also depicted from the survey. To counter this serious problem the overall structure of security policy should change. When the enterprise needs to modify the access control policies and firewall settings, in the same time users need to be more aware of cyber-attacks and prepare their workstations with requisite precautions. With the motivation of making security protocol, we will further propose an access control policy framework to support remote working and distance learning for ensuring security to the cloud resources against spoofing attacks.

REFERENCES

[1] H. S. Lallie et al., "Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic," arXiv:2006.11929 [cs], Jun. 2020, Accessed: Aug. 03, 2020. [Online]. Available: http://arxiv.org/abs/2006.11929.

[2] L. Zhong, L. Mu, J. Li, J. Wang, Z. Yin, and D. Liu, "Early Prediction of the 2019 Novel Coronavirus Outbreak in the Mainland China Based on Simple Mathematical Model," IEEE Access, vol. 8, pp. 51761–51769, 2020, doi: 10.1109/ACCESS.2020.2979599.

[3] "McAfee Labs COVID-19 Threats Report, July 2020," p. 40.

[4] "Operational resilience in the time of COVID-19: SaaS to the rescue." https://www.moodysanalytics.com/articles/2020/operational-resilience-in-the-time-of-covid-19 (accessed Aug. 09, 2020).

[5] U. N. Service, "Data breach incidents increases during COVID-19: Verizon Business Study," http://www.uniindia.com/data-breach-incidents-increases-during-covid-19-verizon-business-study/south/news/2099031.html. http://www.uniindia.com/data-breach-incidents-increases-during-covid-19-verizon-business-study/south/news/2099031.html (accessed Aug. 09, 2020).

[6] C. R. N. Team, "What impact has COVID-19 had on the data breach landscape?," CRN - India, Aug. 05, 2020. https://www.crn.in/columns/what-impact-has-covid-19-had-on-the-data-breach-landscape/ (accessed Aug. 09, 2020)

[7] H. Sheth, "External attacks on cloud accounts increased by over 600% during Covid-19: Report," @businessline. https://www.thehindubusinessline.com/info-tech/external-attacks-on-cloud-accounts-increased-by-over-600-during-covid-19-report/article31687423.ece (accessed Aug. 09, 2020).

[8] "How does COVID-19 impact cloud adoption?," Help Net Security, Jun. 08, 2020. https://www.helpnetsecurity.com/2020/06/08/covid-19-impact-cloud-adoption/ (accessed Aug. 09, 2020).

[9] "The COVID-19 pandemic has changed education forever. This is how," World Economic Forum. https://www.weforum.org/agenda/2020/04/coronavirus-education-global-covid19-online-digital-learning/ (accessed Aug. 04, 2020).

[10] "COVID-19 brings new cyber-security threats to universities." https://www.universityworldnews.com/post.php?story=20200607084916387 (accessed Aug. 09, 2020).

[11] L. H. Newman, "Schools Already Struggled With Cybersecurity. Then Came Covid-19," Wired. https://www.wired.com/story/schools-already-struggled-cybersecurity-then-came-covid-19/ (accessed Aug. 09, 2020).

[12] A. S. Reporter, "Hacking Attacks on Educational Portal Tripled in Covid-19 Amid Online Learning," dynamicCISO, May 11, 2020. https://www.dynamicciso.com/hacking-attacks-on-educational-portal-tripled-in-covid-19-amid-online-learning/ (accessed Aug. 09, 2020).

[13] "What COVID-19 teaches us about cybersecurity – and how to prepare for the inevitable global cyberattack," World Economic Forum. https://www.weforum.org/agenda/2020/06/covid-19-pandemic-teaches-us-about-cybersecurity-cyberattack-cyber-pandemic-risk-virus/ (accessed Aug. 09, 2020).

[14] O. A. Osanaiye, "Short Paper: IP spoofing detection for preventing DDoS attack in Cloud Computing," in 2015 18th International Conference on Intelligence in Next Generation Networks, Paris, France, 2015, pp. 139–141, doi: 10.1109/ICIN.2015.7073820

[15] "What is a DNS Hijacking | Redirection Attacks Explained | Imperva," Learning Center. https://www.imperva.com/learn/application-security/dns-hijacking-redirection/ (accessed Aug. 04, 2020).

[16] A. Alzahrani, "Coronavirus Social Engineering Attacks: Issues and Recommendations," IJACSA, vol. 11, no. 5, 2020, doi: 10.14569/IJACSA.2020.0110523.

[17] B. Feng, Q. Li, Y. Ji, D. Guo, and X. Meng, "Stopping the Cyberattack in the Early Stage: Assessing the Security Risks of Social Network Users," Security and Communication Networks, Jul. 11, 2019. https://www.hindawi.com/journals/scn/2019/3053418/ (accessed Aug. 09, 2020).

[18] "Cybercriminals are 'already taking advantage' of the COVID-19 crisis," Healthcare IT News, May 07, 2020. https://www.healthcareitnews.com/news/cyber-criminals-are-already-taking-advantage-covid-19-crisis (accessed Aug. 09, 2020).

[19] A. Mauro, "Working from home during the coronavirus pandemic creates new cybersecurity threats," The Conversation. http://theconversation.com/working-from-home-during-the-coronavirus-pandemic-creates-new-cybersecurity-threats-134954 (accessed Aug. 04, 2020).

[20] "[Updated] Top 9 coronavirus phishing scams making the rounds," Infosec. http://www.infosecinstitute.com/blog/top-7-coronavirus-phishing-scams-making-the-rounds/ (accessed Aug. 17, 2020).

[21] "Cybercriminals exploiting public fear of rising COVID-19, IT Security News, ET CISO." https://ciso.economictimes.indiatimes.com/news/cybercriminals-exploiting-public-fear-of-rising-covid-19/74621845 (accessed Aug. 04, 2020).

[22] "WHO reports fivefold increase in cyber attacks, urges vigilance." https://www.who.int/news-room/detail/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance (accessed Aug. 04, 2020).

[23] P. Dutta, "5 Biggest Data Breaches of 2020 (So Far)," Kratikal Blog, Aug. 01, 2020. https://www.kratikal.com/blog/5-biggest-data-breaches-of-2020-so-far/ (accessed Aug. 09, 2020).

[24] "Coronavirus: Cyber attacks on banks seen spiking, says Carbon Black," ComputerWeekly.com. https://www.computerweekly.com/news/252481684/Coronavirus-Cyber-attacks-on-banks-seen-spiking-says-Carbon-Black (accessed Aug. 09, 2020).

[25] "COVID-19 RELATED CYBER ATTACKS," ITC Secure | Secure IT Network Infrastructures, Apr. 01, 2020. https://itcsecure.com/covid-19-related-cyber-attacks/ (accessed Aug. 10, 2020).

[26] S. Zeadally, F. Siddiqui, Z. Baig, and A. Ibrahim, "Smart healthcare: Challenges and potential solutions using internet of things (IoT) and big data analytics," PSU research review, pp. 1–17, Oct. 2019, doi: 10.1108/prr-08-2019-0027.