International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 9 Issue: 8
***Article Received:** 25 May 2021 **Revised:** 12 June 2021 **Accepted:** 30 July 2021*

Prevent Cyber Attacks on Cloud Computing Environments Covid 19 Era

[1]Ramasankar Molleti, [2]Anirudh Khanna
[1] Independent Researcher, Illinois, USA, Email: Ramasankar.molleti@gmail.com
[2] Independent Researcher, Plano, TX, USA, Email: mailtoanirudh@gmail.com

***Abstract*:** COVID-19 Pandemic timeframe confirms that cloud computing is a useful part of an international structure that enables sharing computing facilities while working remotely. Though, the newly developed connected as well as automated cars have also amplified the susceptibility to cyber-crimes like phishing, malware, ransomware, and data breach. In this case, attention will be drawn to the new trends identified in the process of Cloud Computing during the pandemic, namely the increased level of sophistication of attacks by cybercriminals and hackers, and sometimes with the support of states. It narrates possible threats which are Sniffer attacks, DNS weaknesses, CAPTCHA cracking, Google hacking and many others, their effects on international security. This analysis shows that to secure such information for continued business, then efficient security controls like encryption of data, MFA, and monitoring should be incorporated. It also aims at new threats to be included into the system in addition to optimizing security measures with a view of improving on the protection of new complexes such as cloud environments. Therefore, the conclusion suggests that daily monitoring and the struggle for finding new approaches are critically important to safeguard cloud services in the dynamic environment and in the context of the post Covid-19 period.

***Key words**: COVID-19, Pandemic, Cloud Computing, CAPTCHA, MFA, cyber attacks*

1. Introduction

1.1. Background

In the environment of the current COVID-19 global crisis, the cloud computing model has been more crucial, which provides global access to share large computing resources. But it was the year 2000 and the subsequent decades that brought a massive increase in cybersecurity risks, especially against the background of the modern world's focus on remote work and cloud solutions [1]. Hackers including state sponsored ones have taken advantage of this situation to engage in more advanced attacks like phishing, malware and ransomware in global networks. Existence of these challenges makes it extra crucial to safeguard the cloud environments on account to the fact that cloud service providers are in charge of infrastructure and data belonging to their users. Data protection from actual and potential dangers is a complex process, which presupposes adequate protection measures, including data integrity, data reliability, and data confidentiality. This paper aims to identify current threats that COVID-19 has brought to cloud computing environments and their effects on various security systems around the world and how they can be managed.

1.2. Scope and aim

The scope entails recognizing the common cyber threats like phishing, malware, and ransomware which have risen with the applications of remote working and the use of cloud services. It will analyze how these threats affect the security architectures worldwide and compare how cloud service providers contribute to the management of infrastructures and data security [2]. This study research paper primarily aims to demonstrate certain effective strategies that could be helpful in preventing various cyber-attacks on the Cloud Computing environments that could happen in the time period of post Covid-19 era. This study will be mainly focused on the implementation of the robust securities and technologies that include various reliabilities, data integration enhancement, and confidentiality security that could ensure a continuous vigilance in order to increase safety against suspicious activities within the cloud computing environments.

1.3. Importance of cloud computing

Cloud computing is a significant phenomenon in present business environments as the provision can be rapidly deployed, and contributes to the development of technologies as hardware barriers can be evaded [3]. It provides unprecedented scalability and flexibility for operative resources and their quick change according to the flows' density, which minimizes the requirements for substantial investments in fixed assets. Managing costs occur through the pay-as-you-go approach, having no capital expenses that could demand considerable funds or be tied to a certain period ultimately allowing IT teams to focus on project-oriented exercises. Flexibility is the key in data accessibility anytime and anywhere increased security measures and management by professionals augment security. Furthermore, features such as the backup and disaster recovery in cloud providers eliminate risks of losing data and enable the business to run as usual despite catastrophes.

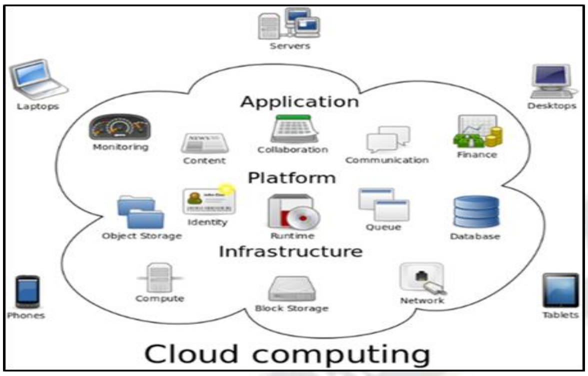

Figure 1: Importance of cloud computing
(Source: Aljumah and Ahanger 2020)

2. Threats of Cloud Computing and defense mechanism

2.1. Security concerns regarding data breaches

On the same note, in regard to threats posed by cloud computing services, 43% of the respondents specified that they considered threats such as SQL Injection & Cross site scripting as significant [4]. Research by different writers show that malware injection and in particular SQL injection is on the increase and hackers are focusing on entering SQL databases and injecting malicious code. Furthermore certain studies have shown the reasons for their selection, revealing that cyber-attacks are one of the most frequently used hacking techniques. In such attacks, the hackers get in-between the routing and transport protocols of the intended network, which results in embezzlement of sensitive data. These results prove the necessity to use proper security models to counteract such threats in cloud computing environments.

2.2. Google hacking and captcha code breaking

Captcha cracking through image based hacking is among the rising issues in cloud computing. In the survey, 38% out of the total respondent strongly agreed and 44% agreed that captcha breaking is a menacing threat for cloud computing services. Moreover, 41% admitted Google hacking as usual and it affected sound business operations and functioning. Some of the research studies also show that presently spammers can solve the captcha on sites such as Gmail and Hotmail with relative ease and use of audio systems to recite captcha for their clients. These results demonstrate the existing and emerging problems of captcha breaking and Google hacking in the field of cloud computing therefore, it is crucial to increase the security level in this area [5]. The spammers are becoming smarter in evading captcha mechanisms and attacking the weaknesses related to such problems point towards the need to effectively solve them to enhance reliability and security of cloud-based services.

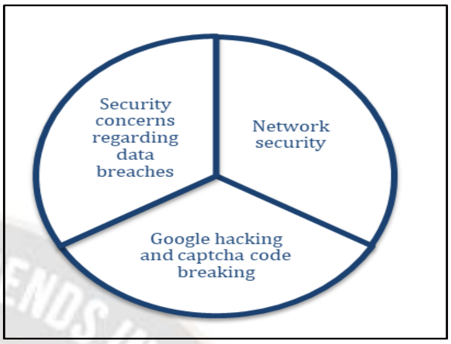
Security concerns regarding data breaches
Network security
Google hacking and captcha code breaking

Figure 2: Threats of Cloud Computing
(Source: Self-created)

2.3. Network security

Concerning the threat issues of the network, 42% of the participants considered that the sniffer attacks would be the biggest obstacle to cloud computing services. These attacks capture data using a sniffer application through the network traffic. On the other hand, about 54% of the respondents vehemently disagreed that DoS and distributed DoS were major security issues. Also, there was a strong agreement on the concern caused by domain name server (DNS) problems with 31% respondents strongly agreeing with the issue. DNS attacks are implemented when the server re-routes and captures user data as well by providing the wrong IP address [6]. This suggests the prevalence of threat from high-traffic sites, especially applications, which act as a severe threat. Although, several studies and work reveals that through DNS attacks, the risk of organizations in the cloud computing domain has been amplified by the violation of personal user information.

2.4. Defense mechanisms

As opposed to data breaches or DoS attacks, data loss is frequently caused by human error that affects the servers physically or when particular events are under attack. Regardless of the cause, the outcome is the same that include companies can lose years' worth of records pertinent to their operations. Some of the causes are the insecure APIs, inside threats, no proper security monitoring, and no disaster recovery plans. Although, new data deletion risks stem from the cloud and obscure identification of data locations, and shaky confirmation of data erasure, particularly with IaaS [7]. The respondents recommended the following defenses for the contents stored in the cloud. Concerning the aspects of data loss and breaches, their suggestions were to use two-factor

Article Received: *25 May 2021* ***Revised:*** *12 June 2021* ***Accepted:*** *30 July 2021*

authentication and strong passwords. And to prevent the misuse of insiders, they recommended employing IDSs and FAT or file allocation tables to detect the traffic and the content of the network. For DNS attacks, they recommended the use of domain system security extensions to eliminate unauthorized changes on the same.

3. Different active cyber-attacks in pandemic COVID 19

3.1. Disrupting Services

Although some research papers noted that the number of dDoS attacks increased in 2020 due to the large concentration of Internet users because of quarantine, distance learning, and teleworking. These attacks have practical consequences by making references to a reported cyber-attack on the US Health & Human Services in March this year [9]. Owing to the COVID-19 outbreak, spyware attacks were identified as one of the malware that targeted systems with the aim of infiltrating and collecting information from the system's memory without the owner's consent. For instance, COVID-19 tracker applications such as Corona Live contained spyware to track the usage made by the users. All these threats depict how the COVID-19 enhanced cyber threats in the fully digitized world.

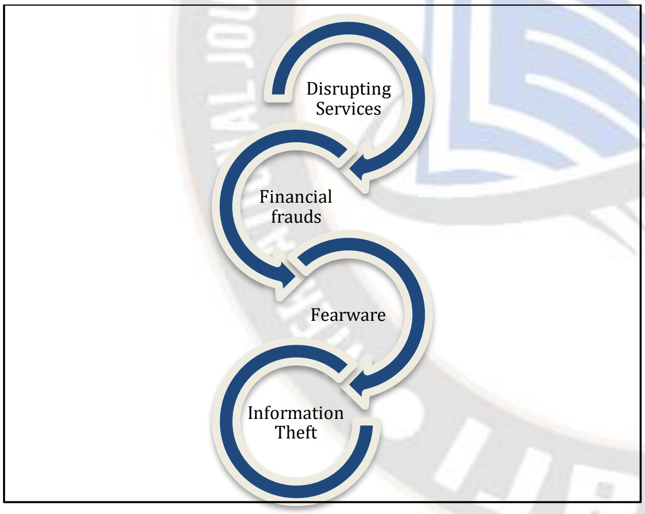

Figure 3: Cyber-attacks in pandemic COVID 19

(Source: Self-created)

3.2. Financial frauds

Cyber threats such as Ransomware attacks and levels of Digital Fraud have significantly increased due to COVID-19 pandemic which has made people panic and also due to increased use of digital services. CovidLock Android-app locks personal data and extorts monetary amounts in bitcoins, stating that it will release or delete the data if the request is not met. This has led to increased instances of COVID-19 themed digital fraud mainly regarding the gray market in PPE plus other COVID-19 related hygiene and safety instruments or products at greatly inflated prices, or in some cases the distribution of fakes and non-approved products [8]. The intelligence agencies Interpol within a week have reported that they have located nearly 2000 fake web links in March 2020, and have seized close to 13 million Euros of pharmaceuticals, 37000 illegitimate medical devices. They show the necessity of being protected from various malware and fraudulent schemes during crises at the international level.

3.3. Fearware

Some of the observed informative campaigns have also been enacted on common social media platforms such as Facebook, WhatsApp and LinkedIn where fake or misleading information was posted. This includes beliefs such as ayurvedic medicine working on COVID-19 or tea or cow urine preventing the spread of COVID-19. Although with no scientific evidence to support these statements, they formed confusion to the society and in some instances resulted in loss of lives or got some people injured. Many articles and videos of the use of social networks contain information or instructions on how to produce home-made hand sanitizers and other similar products [10]. There have also been low inhibition calls to do away with the COVID-19 virus as fake news spreads on sundry popular social media sites. Besides, articles with the title COVID-19 that include statements about violence against specific ethnic groups are also present online.

3.4. Information Theft

In the COVID-19 pandemic time and the post pandemic time period the information theft and the data breaching incidents are highly frequent. These could be happening by certain processes that include vishing calls, vulnerability exploitations, and phishing [11]. Telecommunication is crucial in flexible working while containing COVID-19 and in healthcare advisories buy cybercriminals take advantage. Telephony and internet communication has also been frauded by vishing calls, rob call scams and technical support scams. Weaknesses in online platforms such as LMS and video conferencing tools have been exploited more with the increased use, for instance, video conference sabotage. Vulnerability exploitation is very common among the existing social lives out there in the today's world. There are several such incidents that are even highly promoted or publicized and further have been reported, by which the cyber criminals got identified for the exploitation vulnerability. Also apart from these Phishing is one of the most common cybercrimes that have been observed during the COVID-19 pandemic [12]. There are over 309,000 spam and fraud emails were discovered in this time that were attacking people

***Article Received:** 25 May 2021 **Revised:** 12 June 2021 **Accepted:** 30 July 2021*

worldwide and were identified by the WHO or World Health Organization.

Table 1: Types of Information Theft

Threat Type	Examples	Impact
Vishing or voice phishing Calls	VoIP scams, technical support scams	Financial loss, personal information stolen
Vulnerability Exploitation	Video conference hijacking	Unauthorized access to vulnerable and sensitive content
Phishing	COVID-19 spam emails impersonating WHO	Suspicious and unauthenticated attachment downloads, and data breaches

(Source: Self-created)

4. Cloud Computing attacks preventing strategies in COVID-19

4.1. Cloud data encryption

Data encryption is now considered a crucial element of Business Continuity Plans as more cloud-based resources get targeted during the post-pandemic period. Unlike an organization's own data centers, cloud use involves contracting with a third party to host and manage data and applications [13]. Cloud Data Encryption is done before data gets to the cloud and most often, keys to decrypt the data are kept within your IT department. This strategy increases data security since it becomes hard for an unauthorized person to get access to the data. Nevertheless, data encryption has been around for quite some time, and while many companies at some point used only the basic encryption that can be easily cracked by brute force. Because of the increased frequency of cyber threats during the COVID-19 pandemic, encryption has become the best practice rather than the best advice for organizations. Prevent interception of data through end-to-end encryption Companies that earlier might not have applied the tactic of strong encryption tools or applied weak keys have to adopt end-to-end encryption for the safety of data. Thus, it is necessary to upgrade your data security strategy and implement more sophisticated encryption approaches.

4.2. Data backup and recovery

Specifically, as the trend for data centers moves from physical central hosts to cloud services, the backup and recovery of this information also requires changes. Previously, the organizations used the multiple copies of the company data for the restoration purposes. Today, the problem concerns end devices and Shadow IT arising when more and more employees bring their own devices to work and interact with new technologies that they have never encountered previously [14]. Thus, backup plans should consider these factors. It attributed the increased attack on such systems to cause costly downtime and loss of data when such systems are held ransom. Due to the constant selection of cloud platforms by hackers, it is recommended to implement efficient backup and data recovery solutions into cloud security policies. Although all the cloud providers possess a mechanism of automatically doing monthly backups, downloading manual, regular backups entail optimal data protection and are effective in preventing or containing break ins.

4.3. Cloud computing environment monitoring

The adoption of remote working has seen the use of many company devices connected to office networks and thus the cloud environment must be monitored on a continual basis. Generally available cloud services contain network health and status checking utilities that should be part of administrators' daily IT checklists. Uninterrupted supervision helps identify unknown gadgets, threats, and suboptimal solutions public cloud consumers watch network flows and platforms, whereas private ones have better control to counteract adversities. This way, abnormal patterns of activity can be identified and addressed before they pose a threat to the company's information systems. This is because due to remote work employees could be subjected to attacks and thus real-time monitoring should be adopted in cloud security [15]. If the current services are unsatisfactory and are unable to filter adequately the level of online threat, then they should avail of third-party services that aid in increasing security and in immediately acting upon any unusual activities that may pose a threat to the organizations' operations and stability.

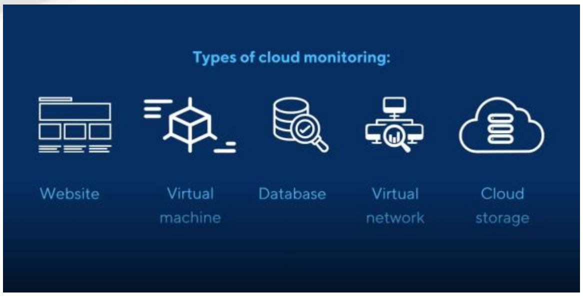

Figure 4: Cloud environment monitoring types

(Source: https://www.virtualmetric.com)

4.4. MFA or Multi-factor authentication

Multi-factor Authentication (MFA) is one of the cloud security best practices to increase the security level of data resources and become successful for both business and personal use. Besides the use of a username and password, MFA uses Cloud Access Management to check multiple factors of a user before considering them legitimate, and to help administrators identify and stop imposters [16]. To be protected from attacks that result from misused credentials, it is advisable to adopt MFA in your network's cloud security plan. Thus, it ensures that only the right people can see the cloud applications and the business' valuable information, among others. To some extent, MFA has been understudied and underused even though it is efficient and its implementation cost is low, again, especially with the consideration of the COVID-19 episodes, which have increased hacking incidents [15]. Besides enhancing security, MIN also reduces the threats of social engineering attacks, which makes it an essential component of the security model when working in cloud environments.

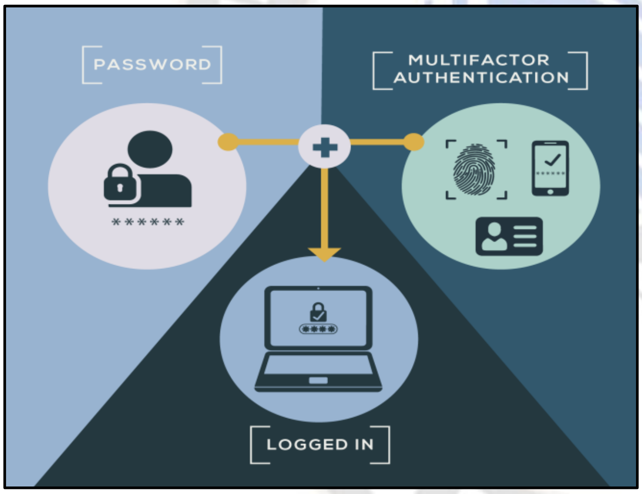

Figure 5: Multi-factor Authentication (MFA)
(Source: https://www.nist.gov)

4.5. User security

The utilization of cloud services entails giving the employees as well as the clients direct and straightforward access to a company's information and applications, which calls for the concrete specification of roles as well as controls that are given by the administrators. Security management which is essential to control the possession and alteration of cloud data is worked through identify and access management [17]. Therefore, there is a need to have a more concrete authentication system that can cater for a large number of users and thus respect the ICT devices available in organizations today in order to protect valuable applications, information, and client data.

End-user security carries PII and must have service agreements to deny anyone unauthorized access. The case of small businesses emphasizes that companies returning to work remotely after covid-19 have difficulties controlling cloud access and protection. To counter such problems, one needs to incorporate the following such as security training of the users, restricted use of the devices, appropriate usage of the cloud environments, the use of encryption and malware scans. By implementing the above measures they will assist in reducing the security threats and enhancing the protection of data that may be confidential and sensitive and therefore prone to being in the cloud.

5. Future work

The areas for future research should include the improvement of current threat detection systems relating to the constantly emerging environment of cloud computing security. Because modern cyber threats evolve, integrating machine learning and artificial intelligence into security measures might improve the identification and counteraction of security breaches on the spot.

Also, studying the efficiency of new encryption methods and the ways of their implementation in the cloud computing space will also be important. Further research on users' actions and effects of work from home on cloud security will also be useful [18]. Moreover, expanding the concerns of security to reflect the capacity of organizations of different sizes and structures will provide more information relevant to the creation of advanced and generally usable security concepts. This means that it will be vital for future research, particularly in the academic field, to cooperate with cloud system providers and other industries to address new threats and vulnerabilities.

6. Conclusion

The outbreak of the COVID-19 pandemic has brought to the realization the indispensability of protecting cloud computing systems due to emerging threats from hackers. While the COVID pandemic has forced companies to adopt an increased dependency on remote work and cloud services, so has increased deceptive techniques such as phishing, ransomware, and data breaches.

Techniques such as the use of strong encryption algorithms, constant data vigilance, and the use of several verification processes are important especially in the protection of critical information. The profound interest in cloud security measures is imperative not only to guard against the losses of data but also to continue the business in the presence of growing threats. It is critical to continuously adapt and evolve the security paradigms to effectively address the threats while maintaining cloud computing security in the post-COVID-19 world.

Reference List

Journals

[1] Aljumah, A. and Ahanger, T.A., 2020. Cyber security threats, challenges and defence mechanisms in cloud computing. IET communications, 14(7), pp.1185-1191. https://ietresearch.onlinelibrary.wiley.com/doi/abs/10.1049/iet-com.2019.0040

[2] S. Hakak, W. Z. Khan, M. Imran, K.-K. R. Choo, and M. Shoaib, “Have you been a victim of COVID-19-Related cyber incidents? Survey, Taxonomy, and Mitigation Strategies,” IEEE Access, vol. 8, pp. 124134–124144, Jan. 2020, doi: 10.1109/access.2020.3006172.

[3] P. Kumar, “Literature based study on Cloud Computing for Health and Sustainability in View of COVID19,” International Journal of Innovative Technology and Research, pp. 01–06, May 2020, [Online]. Available: http://www.ijitr.com/index.php/ojs/article/download/2566/pdf

[4] Okereafor, K. and Adelaiye, O., 2020. Randomized cyber attack simulation model: a cybersecurity mitigation proposal for post covid-19 digital era.http://34.29.95.55:8080/jspui/handle/123456789/1254

[5] Sharma, A., Gupta, P. and Noida, I., 2020. COVID 19 PANDEMIC: IMPACT ON BUSINESS AND CYBER SECURITY CHALLENGES. Journal of Emerging Technologies and Innovative Research (JETIR), 7(7).

[6] Ahmad, S., Mehfuz, S. and Beg, J., 2020, December. Securely work from home with CASB policies under COVID-19 pandemic: a short review. In 2020 9th International conference system modeling and advancement in research trends (SMART) (pp. 109-114). IEEE. https://ieeexplore.ieee.org/abstract/document/9337121/

[7] M. Milanovic and M. N. Schmitt, “Cyber Attacks and Cyber (Mis)information Operations during a Pandemic,” *Social Science Research Network*, Jan. 2020, doi: 10.2139/ssrn.3612019.

[8] F. Li, “Cloud-native database systems at Alibaba,” Proceedings of the VLDB Endowment, vol. 12, no. 12, pp. 2263–2272, Aug. 2019, doi: 10.14778/3352063.3352141.

[9] J. Moura and D. Hutchison, “Review and analysis of networking challenges in cloud computing,” Journal of Network and Computer Applications, vol. 60, pp. 113–129, Jan. 2016, doi: 10.1016/j.jnca.2015.11.015.

[10] Y. K. Dwivedi et al., “Impact of COVID-19 pandemic on information management research and practice: Transforming education, work and life,” International Journal of Information Management, vol. 55, p. 102211, Dec. 2020, doi: 10.1016/j.ijinfomgt.2020.102211.

[11] L. Tawalbeh, F. Muheidat, M. Tawalbeh, M. Quwaider, and G. Saldamli, “Predicting and Preventing Cyber Attacks During COVID-19 Time Using Data Analysis and Proposed Secure IoT layered Model,” International Journal of Innovative Technology and Exploring Engineering (IJITEE), Oct. 2020, doi: 10.1109/mcna50957.2020.9264301.

[12] G. Somani, M. S. Gaur, D. Sanghi, M. Conti, and R. Buyya, “DDoS attacks in cloud computing: Issues, taxonomy, and future directions,” Computer Communications, vol. 107, pp. 30–48, Jul. 2017, doi: 10.1016/j.comcom.2017.03.010.

[13] N. Subramanian and A. Jeyaraj, “Recent security challenges in cloud computing,” Computers & Electrical Engineering, vol. 71, pp. 28–42, Oct. 2018, doi: 10.1016/j.compeleceng.2018.06.006.

[14] S. Das, B. Wang, Z. Tingle, and L. J. Camp, “Evaluating User Perception of Multi-Factor Authentication: A Systematic review.,” HAISA, pp. 166–178, Jan. 2019, [Online]. Available: https://dblp.uni-trier.de/db/conf/haisa/haisa2019.html#DasWTC19

[15] M. M. Alshammari, A. A. Alwan, A. Nordin, and I. F. Al-Shaikhli, “Disaster recovery in single-cloud and multi-cloud environments: Issues and challenges,” IEEE, Nov. 2017, doi: 10.1109/icetas.2017.8277868.

[16] Wiggen, J., 2020. Impact of COVID-19 on cyber crime and state-sponsored cyber activities (Vol. 391, p. 2). Konrad-Adenauer-Stiftung.https://ieeexplore.ieee.org/abstract/document/9337121/

[17] S. Chowdhury, S. Mukherjee, S. N. Roy, R. Mehdi, and R. Banerjee, “An overview of cybersecurity risks during the COVID-19 pandemic period,” Scientific Voyage, vol. 1, no. 3, pp. 47–54, Sep. 2020, [Online]. Available: http://scientificvoyage.net/index.php/sv/article/download/21/17.

[18] Lai, J., Xiong, J., Wang, C., Wu, G. and Li, Y., 2017. A secure cloud backup system with deduplication and assured deletion. In Provable Security: 11th International Conference, ProvSec 2017, Xi'an, China, October 23-25, 2017, Proceedings 11 (pp. 74-83). Springer International Publishing.https://link.springer.com/chapter/10.1007/978-3-319-68637-0_5