ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3, March 2022

The Era of a Global Crisis Coronavirus Pandemic and Opportunity on Cloud Technology Migration

Bryan B. Penuliar

School of Information Technology, Mapua University, Makati City, Philippines
Corresponding Author Email: penuliarbryan@yahoo.com

Abstract*— *In this generation, Coronavirus pandemic has many various impact on company businesses. The situation has required telework from their home as a precaution and safety measure to avoid being infected with the contagious coronavirus. Although going through the coronavirus outbreak, many businesses have tried to migrate and use cloud technology to keep pace with technology change, which requires data security and safe use of the cloud in business operations. Current cloud providers that are gradually evolving are becoming an integral part of facilitating a business already in the cloud and protected by innovative tools. Many users have already adopted emerging technologies associated with cloud applications and need to protect data in a cloud security environment. Currently, cloud security still needs to secure the environment, which is one of the reasons to consider when in the cloud environment. This study describes the era of a pandemic of the coronavirus, as well as the possibility of migrating cloud technologies for data protection at working from home or even in the remote workplace.

Keywords*— *COVID-19, Security challenge, Work from home

I. INTRODUCTION

The new disease discovered and spread that has worsened around the world is the coronavirus. In December 2019, when it was found in China, the coronavirus appeared in Wuhan, where this disease shocked the whole world. Experts discovered this disease, and they classified it as SARS which also originated in china SARS-CoV-2 or COVID-19, which they named this new virus. A sick person carrying COVID-19 can be transmitted by coughing or sneezing into the air. This symptom of having an infection from the virus will be felt after 14 days. Its symptoms include cough, difficulty breathing, chest tightness, body aches, and flu-like chills. If these symptoms worsen and are not treated right away, it can lead to death.

Moreover, around the world, all countries have been affected and experienced the impact of the pandemic. Many companies were involved, others were forced to close, many people got sick with covid-19, lost loved ones, and affected their daily living. Many scientists have focused on and discovered a drug to address the worsening spread of COVID-19 disease worldwide [1] . Also, businesses of all countries around the world are will inevitably impacted. Immediate lockdown, travel restriction, and quarantines are promptly implemented by the government, resulting in economic consequences on the losses of businesses. The company and government employees cannot commute to work to the offices due to the spreading of the coronavirus. Since the operation or transaction of businesses should not stop, because of the pandemic, it became possible to work in the homes of employees where the computers and devices were necessarily connected to the internet. Working at home has become important in companies approved by all workers while the entire country is still experiencing a pandemic. The pandemic also helped see if working at home could be appropriately done effectively. It also paved the way for the lack of connections or infrastructure to improve to be more useful in the following work at home [2].

Before the pandemic came, there was no work from home, and it had not been implemented abroad by other companies. Working at home or remotely is a goal or desire of employees to fulfill. But this is unlikely to be enforced by companies for employee requests who want to work at home if they choose. Working at home requires a good place at home that is quiet, undisturbed, the internet is fast and above all working in the company is not affected. But until now, it happened and was replaced by pandemic, because working at home was allowed and it became beneficial to the employees who just wanted to work at home. It became easy for them and safe from the spreading pandemic.

The cloud service providers have become more recognizable and appeared to help in the midst of a pandemic. All of the countries affected all have employees working at home. But the company and the employee need to use a security tool to share information in data exchange securely. Thus, this search results finding out the security-related technologies or tools used while working outside the company can help further develop the transition to the cloud. The article is classified as follows: In Section 2, Opportunities of cloud computing technology. Strategies or approaches in Section 3 for secure assistance teamwork in the work environment. Section 4 is the comparison of cloud security tools. Section 5 presents the results. Then the latter for section 6 provides a conclusion and discussion related to the topic.

II. OPPORTUNITY OF CLOUD COMPUTING TECHNOLOGY

While companies worldwide are experiencing pandemics, it has become a way to recognize the cloud; the need for the cloud has also become in-demand. Above all, its importance to the industry has been realized. In addition, the cloud brings many services to its users. The cloud is represented as cloud computing with services and is called pay-as-go. Its services are storage, applications, software, and more available through the internet. One of the services delivered by the cloud is to consumers where their emails, photos, and applications are backed up via smartphones, which allows such a service to host all their data with consumer agreement.

As shown in fig.1, According to NIST, it is shown that the cloud computing model allows access to resources within the network where resources such as storage, software, servers, and others. These resources can easily be deployed instantly in real-time [3]. In this model, there are other services where the service is complete such as IaaS or Infrastructure as a Service. The same goes for other service models such as PaaS or Platform as a Service, and the latter is SaaS service or Software as a Service.

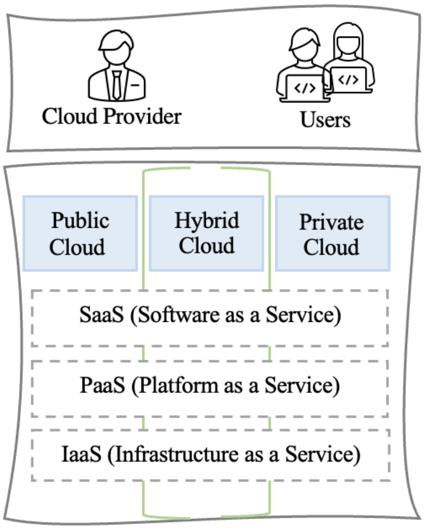
Cloud Provider
Users
Public Cloud
Hybrid Cloud
Private Cloud
SaaS (Software as a Service)
PaaS (Platform as a Service)
IaaS (Infrastructure as a Service)

Figure I : Model of Cloud Computing

Every business has clouding requirements. That is where the service has the decision and controls what happens in the cloud environment. The cloud environment has different models that will guide depending on the need, such as the public cloud. A public cloud is a public one that everyone can use. Everyone has access to a personal cloud that can instantly share applications, data information, and more with the permission and responsibility of the service. With the internet, one must consider the possibilities that may occur, such as malicious attacks, data leakage, etc. Public cloud security must be knowledgeable to the user to avoid mistakes [4].

However, a Private Cloud is generally defined as everything behind a company's walls. These systems operate in a company's local data center [4]. Additionally, large data centers are a big responsibility of the companies managed by ITs who have knowledge of data center operation where they must maintain its security such as servers, software and maintaining the freezing temperature of the facility. On the other hand, Hybrid Cloud deployment often describes a company operating both a public cloud and a private cloud. In a hybrid cloud environment, they are not together with the private and public cloud, but they are connected [5]. It is not that easy to monitor in this highly complex hybrid cloud environment. It can compromise the security of the entire cloud. The cloud service is based on the needs of the company or business users. Such as the type of storage service, what hardware, software to use or deploy, etc. They are accessed or usable through the internet and virtualization technology. That is why it has become easy for employees and has become a solution for companies while there is still a pandemic.

III. THE APPROACH FOR SECURE ASSISTANCE TEAMWORK IN THE WORK ENVIRONMENT

While the pandemic is not over and to keep employees safe, companies have temporarily laid out a cloud environment to give them the privilege or access to connect to the office network and do their jobs while at home. Due to the pandemic and lockdown in countries, some companies are not ready to telework or work from home. They implemented and deployed the cloud without proper security implementation to not affect the business transaction.

To tight control, safe and secure workplace. Protection inside and outside the network is essential for important data shared with users. VPN or Virtual Private Network provides cloud network access protection to users' company's data, applications, and files. It can be accessed using a desktop or mobile application [6]. It has strict encryption security on network traffic to the destination in the on-premises area. Active Directory (AD) is a service that allows logon authenticator and access control to objects in the directory.

An administrator can manage directory and organization data across their network using a network logon and authorized network users. With MFA or Multi-factor authentication, its process creates strict security for log-in with a further guarantee of who access [7], If the user is authorized to use and log in to a portal or a site requiring verification will be sent and will receive a code to your registered number. The primary purpose of CASB or Cloud Application Security broker is to secure, visible monitor, security policies or regulations on application uses to prevent information leakage and act as a safeguard permitted to access. It maintains strict security on insecure and registered devices [8].

IV. COMPARISON OF CLOUD SECURITY TOOLS

This section of the paper discusses cloud service tools that provide secure connectivity. This section will know the difference between security tools and those that fully offer protection, such as VPN-Virtual Private Network, MFA-Multi-Factor Authentication, AD-Active Directory. The latter is the CASB-Cloud Application Security Brokers, where they are focused and coordinate with Identity Access Management (IAM).

i. Secure Access Virtual Private Network – VPN [9]

As shown in fig. 2, a VPN is a Virtual Private Network. VPN is used to lay out the security of the company network where the location and destination are encrypted. It uses two devices configured by private IP addresses. Cloud VPN protects the company from unauthorized access from outside or not covered by the network. Companies that use VPN allow them to access their data and information secured to authorized users or employees working in their home or outside the company who know the IP address to access using smart devices [9]. The cloud VPN has the following characteristics.

- Cloud VPN helps with network infrastructure security through the company's internal and external network, where the private network is encrypted and protects against unintentional access.
- With users connected to their devices on the company's VPN, they can securely access the network entered. They can freely access files or applications to which they are allowed but limited to which they are entitled.
- Sends authentication to the user or access to applications where it is encrypted the on-premises private network and configured towards the VPN cloud.

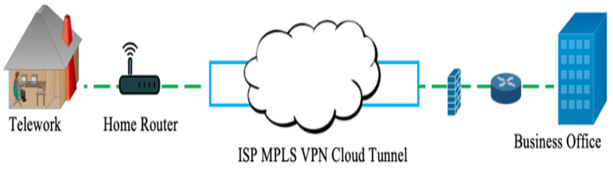

Figure 2 : VPN Cloud Conceptual View

ii. Multi-Factor Authentication – MFA [10]

As shown in fig.3, Multi-factor Authentication – MFA is extra layered for more secure and tighter security. It also acts as secondary login protection, and it will send verification to verify your identity before entering or accessing the network. It might be linked with the portal site, application, or files used while connected to the company's VPN, and it is also strict in authentication security [10]. On the other hand, MFA aims to verify your identities, such as biometrics and facial recognition and may send authentication to the registered smart device or personal number that is registered and authorized to use when you log in to the portal or application be accessed.

Characteristics of MFA:

- Multi-factor authentication further improves its security restrictions. It stands as a barrier before entering as there is a lot of authentication required [11]. Authentication may require up to three verifications, and one of the most stringent authentications is fingerprint or biometrics and facial recognition.
- Multi-factor authentication is also used in online sites or apps transaction to secure and protect consumers' security.

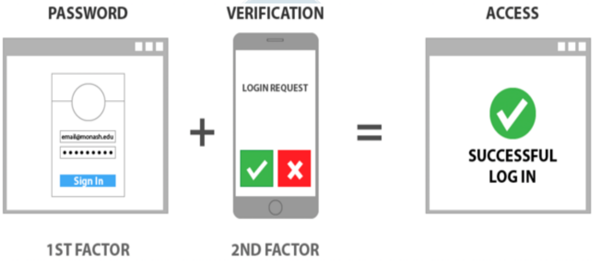

Figure 3 : MFA Conceptual View [12]

iii. Azure Active Directory – AD [13]

Microsoft Azure Active Directory is one of those that also require authorization that proves the right to enter or access the company. It is a directory of users who can only log in with personal credentials. It also lists the registered applications and can be used where the user name is written based on what the company will use. In short words, A directory of users and applications controlled within the company [13].

Characteristics of AD:

- Active Directory helps to determine and control who only has access permission. The MFA can accompany this for tighter security and to know the threats trying to enter.

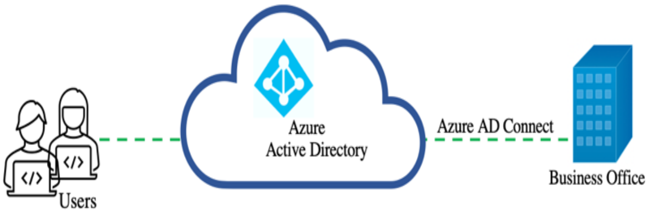

Figure 4 : AD Conceptual view

iv. Cloud Application Security Broker – CASB [14]

As shown in fig. 5, In CASB or Cloud Access Security Broker is one of the important cloud security. Its purpose is to act as an intermediary and monitor all user movements in real-time in the cloud while using personal devices. This tool controls apps and services deployed to have info about users' experiences and avoid risks of filtering and loss of information. Integrated CASB provides a robust interface and Management environment to execute the company-wide protocols and define Firewall rules.

Characteristics of CASB:

- Cloud application security is a tool that can monitor and detect all cloud activities over which cloud apps control and safeguard the security of the company's cloud environment [14].
- Cloud application security protects from downloading data or information for which use is limited. You can also control which the user can only use smart devices and apps. To prevent and protect the leakage of important information.

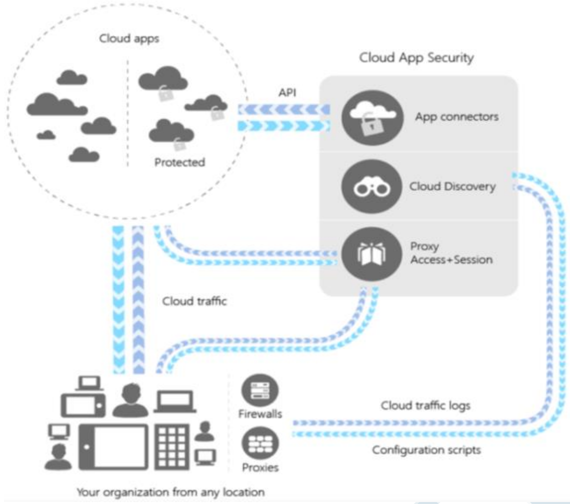

Figure 5 : CASB Conceptual view [15]

V. RESULTS

As shown in table 1, The cloud application security broker is security observing to safeguard the entire cloud. It serves as a safeguard to those who want to enter and get information. It compares according to their usage and service concerning visibility or monitoring, threat detection to those attempting to access, and the latter to compliance management.

TABLE 1 : Cloud Security Tools Functionality

Component	Terms	VPN	MFA	AD	CASB
Visibility	Detect device and location info and can block the apps that have been currently used.	X	X	X	✓
Compliance	Protects data stored on the cloud against data breaches. Ensure that the data stored outside the organization meets all compliance as per the regulatory requirements.	✓	✓	✓	✓
Data Security	Encryption, Tokenization and access control.	✓	✓	✓	✓
Threat Protection	Has a malware analysis and threat intelligence to block malware.	X	X	X	✓

As shown in fig. 6, The user or employee connects to the internet to access the cloud through VPN, but the applications will first go through their validations before accessing work accounts. After thorough verification in Azure Active Directory and Multi-Factor Authentication, it will go to the cloud app security (CASB) to check the information and access the applications assigned to the user. The user admin is the one who manages the environment of the applications, which also needs to connect to the internet to access it. The researcher used this system architecture with an ongoing request between the client and the applications used in the hosted cloud.

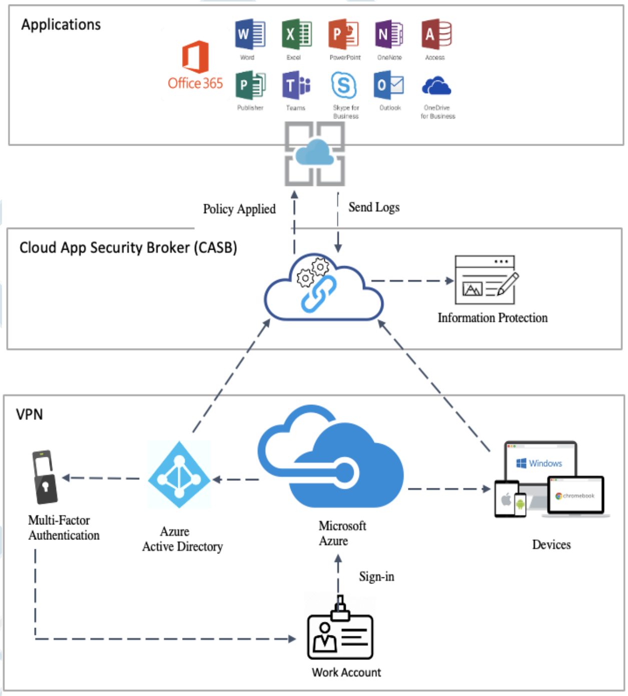

Figure 6 : Implemented Cloud Security Tools

VI. CONCLUSION AND DISCUSSION

This pandemic COVID-19 crisis is unexpected resulting to lack or preparedness to face the situation in businesses operation. It restructured the shape of working setup of employees which is working outside the companies and work in a full time telework or a work from home setup. Cloud technology tools are now being become known and useful that enable to securely share and handle sensitive information. Identity and access management plays vital role to define the access control and secured authorization to avoid attackers that easily steal copy of large data. VPN, MFA, AD and CASB are the security tools can help the company employees when they are working from home using their connected device in the internet. Each tools has different functions providing organization with encryption capabilities, visibility, evaluate the performance and discovering security issues in a real time data protection.

REFERENCES

[1] X. Yao, F. Farha, R. Li, I. Psychoula, L. Chen, and H. Ning, "Security and privacy issues of physical objects in the IoT: Challenges and opportunities," *Digital Communications and Networks*, vol. 7, no. 3. Chongqing University of Posts and Telecommunications, pp. 373–384, Aug. 01, 2021, doi: 10.1016/j.dcan.2020.09.001.

[2] H. Suo, J. Wan, C. Zou, J. L.-2012 international conference on, and undefined 2012, "Security in the internet of things: a review," *ieeexplore.ieee.org*, 2012, doi: 10.1109/ICCSEE.2012.373.

[3] D. Kozlov, J. Veijalainen, Y. A.- BODYNETS, and undefined 2012, "Security and privacy threats in IoT architectures.," *researchgate.net*, 2012, doi: 10.4108/icst.bodynets.2012.250550.

[4] X. X.-2013 I. conference on computational and undefined 2013, "Study on security problems and key technologies of the internet of things," *ieeexplore.ieee.org*, Accessed: Feb. 17, 2022.

[5] M. Bharathi, … R. T.-2012 I., and undefined 2012, "Node capture attack in Wireless Sensor Network: A survey," *ieeexplore.ieee.org*, Accessed: Feb. 17, 2022. [Online].

[6] D. Puthal, S. Nepal, R. Ranjan, J. C.-I. C. Computing, and undefined 2016, "Threats to networking cloud and edge datacenters in the Internet of Things," *ieeexplore.ieee.org*, Accessed: Feb. 17, 2022.

[7] D. Brumley, D. B.-C. Networks, and undefined 2005, "Remote timing attacks are practical," *Elsevier*, Accessed: Feb. 17, 2022. [Online].

[8] "Prabhakar: Network security in digitalization: attacks... - Google Scholar."

[9] M. Conti, N. Dragoni, & V. L.-I. C. S., and undefined 2016, "A survey of man in the middle attacks," *ieeexplore.ieee.org*, Accessed: Feb. 17, 2022. [Online].

[10] "What is computer exploit? - Definition from WhatIs.com."

[11] B. Ali and A. I. Awad, "Cyber and physical security vulnerability assessment for IoT-based smart homes," *Sensors (Switzerland)*, vol. 18, no. 3, pp. 1–17, 2018, doi: 10.3390/s18030817.

[12] S. Gupta, … B. G.-J. of S. A. E. and, and undefined 2017, "Cross-Site Scripting (XSS) attacks and defense mechanisms: classification and state-of-the-art," *Springer*, Accessed: Feb. 17, 2022. [Online].

[13] D. Bastos, M. Shackleton, and F. El-Moussa, "Internet of Things: A Survey of Technologies and Security Risks in Smart Home and City Environments," 2018.

[14] "Smart Home: Threats and Countermeasures - Rambus."

[15] Y. Lu and L. Da Xu, "Internet of things (IoT) cybersecurity research: A review of current research topics," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2103–2115, 2019, doi: 10.1109/JIOT.2018.2869847.

[16] D. E. Kouicem, A. Bouabdallah, H. Lakhlef, D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, "Internet of things security : A top-down survey To cite this version : HAL Id : hal-01780365 Internet of Things Security : a top-down survey," 2018.

[17] A. M. Lonzetta, P. Cope, J. Campbell, B. J. Mohd, and T. Hayajneh, "Security vulnerabilities in bluetooth technology as used in IoT," *J. Sens. Actuator Networks*, vol. 7, no. 3, pp. 1–26, 2018, doi: 10.3390/jsan7030028.

[18] "How Encryption is Powering the Future of IoT." https://www.iotforall.com/future-iot-encryption (accessed Feb. 24, 2022).

[19] P. Sethi and S. R. Sarangi, "Internet of Things: Architectures, Protocols, and Applications," *J. Electr. Comput. Eng.*, vol. 2017, 2017, doi: 10.1155/2017/9324035.

[20] S. Milivojevic, "'The Internet of Everything,'" *Crime Punishm. Futur. Internet*, vol. 7, no. 1, pp. 60–79, 2021, doi: 10.4324/9781003031215-4-4.

[21] C. Perera, C. McCormick, A. K. Bandara, B. A. Price, and B. Nuseibeh, "Privacy-by-design framework for assessing internet of things applications and platforms," *ACM Int. Conf. Proceeding Ser.*, vol. 07-09-Nove, pp. 83–92, 2016, doi: 10.1145/2991561.2991566.

[22] "(PDF) Internet Of Things (Iot) Security Best Practices. IEEE Community-led White Paper | Jared Bielby, rajesh nighot, and Sukanya Mandal - Academia.edu." https://www.academia.edu/32053241/Internet_Of_Things_Iot_Security_Best_Practices._IEEE_Community-led_White_Paper (accessed Feb. 24, 2022).

[23] "Cisco 2017 Annual Cybersecurity Report | The Network.".

[24] "(PDF) A risk analysis of a smart home automation system | Ramakrishna Bhat - Academia.edu." https://www.academia.edu/29318863/A_risk_analysis_of_a_smart_home_automation_system (accessed Feb. 24, 2022).

[25] A. A. Ahmed and W. A. Ahmed, "An effective multifactor authentication mechanism based on combiners of hash function over internet of things," *Sensors (Switzerland)*, vol. 19, no. 17, 2019, doi: 10.3390/s19173663.

[26] D. Geneiatakis, I. Kounelis, R. Neisse, I. Nai-Fovino, G. Steri, and G. Baldini, "Security and privacy issues for an IoT based smart home," *2017 40th Int. Conv. Inf. Commun. Technol. Electron. Microelectron. MIPRO 2017 - Proc.*, no. 1, pp. 1292–1297, 2017, doi: 10.23919/MIPRO.2017.7973622.

[27] J. M. Hatfield, "Social engineering in cybersecurity: The evolution of a concept," *Comput. Secur.*, vol. 73, pp. 102–113, 2018, doi: 10.1016/j.cose.2017.10.008.

[28] I. G. Seissa, J. Ibrahim, and N. Yahaya, "Cyberterrorism Definition Patterns and Mitigation Strategies: A Literature Review," *Int. J. Sci. Res.*, vol. 6, no. 1, pp. 180–186, 2017, doi: 10.21275/art20163936.

[29] H. Rahmani, N. Sahli, and F. Kamoun, "Distributed denial-of-service attack detection scheme-based joint-entropy," *Secur. Commun. Networks*, vol. 5, no. 9, pp. 1049–1061, 2012, doi: 10.1002/sec.392.

[30] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of Things security and forensics: Challenges and opportunities," *Futur. Gener. Comput. Syst.*, vol. 78, pp. 544–546, 2018, doi: 10.1016/j.future.2017.07.060.

[31] N. Apthorpe, D. Reisman, S. Sundaresan, A. Narayanan, and N. Feamster, "Spying on the Smart Home: Privacy Attacks and Defenses on Encrypted IoT Traffic," 2017

[32] S. Ur Rehman and V. Gruhn, "An approach to secure smart homes in cyber-physical systems/Internet-of-Things," *2018 5th Int. Conf. Softw. Defin. Syst. SDS 2018*, pp. 126–129, 2018, doi: 10.1109/SDS.2018.8370433.

[33] "Best Practices for Security within the Internet of Things."