Since January 2020 Elsevier has created a COVID-19 resource centre with free information in English and Mandarin on the novel coronavirus COVID-19. The COVID-19 resource centre is hosted on Elsevier Connect, the company's public news and information website.

Elsevier hereby grants permission to make all its COVID-19-related research that is available on the COVID-19 resource centre - including this research content - immediately available in PubMed Central and other publicly funded repositories, such as the WHO COVID database with rights for unrestricted research re-use and analyses in any form or by any means with acknowledgement of the original source. These permissions are granted for free by Elsevier for as long as the COVID-19 resource centre remains active.
Impact of coronavirus pandemic crisis on technologies and cloud computing applications

Ziyad R. Alashhab a, Mohammed Anbar a,*, Manmeet Mahinderjit Singh b, Yu-Beng Leau c, Zaher Ali Al-Sai b, Sami Abu Alhayja’a a

a National Advanced IPv6 Centre, Universiti Sains Malaysia, Penang, 11800, Malaysia
b School of Computer Sciences, Universiti Sains Malaysia, Penang, 11800, Malaysia
c Faculty of Computing and Informatics, Universiti Malaysia Sabah, Malaysia

ARTICLE INFO

Keywords:
Big data privacy
Cloud computing (CC) applications
COVID-19
Digital transformation
Security challenge
Work from home

ABSTRACT

In light of the COVID-19 outbreak caused by the novel coronavirus, companies and institutions have instructed their employees to work from home as a precautionary measure to reduce the risk of contagion. Employees, however, have been exposed to different security risks because of working from home. Moreover, the rapid global spread of COVID-19 has increased the volume of data generated from various sources. Working from home depends mainly on cloud computing (CC) applications that help employees to efficiently accomplish their tasks. The cloud computing environment (CCE) is an unsung hero in the COVID-19 pandemic crisis. It consists of the fast-paced practices for services that reflect the trend of rapidly deployable applications for maintaining data. Despite the increase in the use of CC applications, there is an ongoing research challenge in the domains of CCE concerning data, guaranteeing security, and the availability of CC applications. This paper, to the best of our knowledge, is the first paper that thoroughly explains the impact of the COVID-19 pandemic on CCE. Additionally, this paper also highlights the security risks of working from home during the COVID-19 pandemic.

1. Introduction

Coronavirus, formerly known as 2019-nCoV, has caused disruption around the globe. It was discovered in December 2019, with a report stating that people were suffering from fever and breathing problems after doing their shopping in a seafood marketplace in Wuhan, Hubei, China. In less than a month, the cases of 2019-nCoV infection spread to several countries (Thailand, Japan, Vietnam, and Singapore) and districts (Hong Kong, Taiwan, and Macau).

The latest statistics have recorded that more than 120 countries’ people have been affected. With an increasing number of infected people and deaths daily, most countries in the world have started to take this outbreak seriously. Many of them began their investigations into the spread of the disease by monitoring contact and gathering epidemiological and clinical data from patients to find treatments. Meanwhile, the suspected and confirmed cases were isolated and the public was instructed to adopt strict hygiene practices. Moreover, governments announced strict lockdowns across their countries to minimize the possibility of spreading the disease. Schools have been closed and the medium of learning has been converted to distance learning. Companies suspended employees from working.
in offices and implemented a work-from-home policy. The airline industry has enforced limitations in both international and domestic flights.

According to the United Nations Educational, Scientific and Cultural Organization (UNESCO) monitoring, the total number of 39 countries affected with many cases of 421388462 [1]. Twenty-nine countries have closed their schools, affecting 391 million children and youth. With the probability of this event becoming even more international, hundreds of millions of learners will stay at home [2]. According to the Federal Student Aid [3], an office of the US Department of Education, students can be affected either directly because of the outbreak itself, the lockdown, overseas travelling, or the indirect effects of remote learning. That is, university students or graduates are no longer able to participate in internships or attend classes on campus. Online education is the only viable option left to teach students. Similarly, in California, schools are facing inevitable closures because of this disease [4]. They are looking for other ways to keep education going as students are forced to stay home. One of the ways to teach students is remotely using online learning. In light of the coronavirus crisis, the role of the cloud computing environment (CCE) has emerged as an unsung hero. During this pandemic, Universiti Sains Malaysia (USM) has taken proactive measures to protect students, faculty, and staff from being infected with the virus, such as working from home and teaching through e-learning (distance learning) [5]. The same proactive measures were followed by other universities and companies throughout the world, such as Microsoft, Cisco, Twitter, Facebook, The University of Jordan, Stanford University, and Harvard University. Due to these measures, the usage or demand for cloud service providers (CSPs) has been increasing. As such, these CSPs face a difficult set of challenges to provide quality services as a result of the explosive growth of the demand because of the coronavirus [6].

Almost all sectors, such as small and large companies, healthcare, and education, have been forced to electronically convert their services. All these businesses, such as Facebook, The University of Jordan, and more, have become extremely dependent on cyberspace for their day-to-day activities. Because this disease has spread widely and rapidly throughout the world, the request for online services has been growing accordingly with this crisis. The service demands being requested are much greater than before. With the increasing sophistication of technologies, more can be achieved more easily online through these services, such as merchandise purchases, bill payments, education, medical consultations, purchases of airline tickets, sea and land transport, and hotel reservations. The competition between enterprises has increased tremendously during this pandemic to gain customers' satisfaction, given the lack of in-person options. Customer trust occurs by providing better online services.

The use of cloud computing (CC) applications has increased the volume, velocity, and/or variety in data being generated every minute around the world from various services and applications. The generated data could be in the form of structured, semi-structured, or unstructured data. It is stored in different formats that cannot be easily integrated due to large data flow at high speeds [7,8]. While data on a large scale has grown from various fields, organizations face challenges and pressure to keep their positions in the competitive market [8]. A new era of digital transformation requires compatible technologies, while the existing capabilities might be not able to handle them well. Organizations will need to handle the challenges related to big data to survive in the new digital market [7]. To do so, they should investigate their customers' demands and desires and move their capturing, collection, and analyses to a future-oriented platform. Organizations should also have the ability to identify their critical data sources, structures, and architecture, as well as to define the infrastructure that supports the big data analysis. Additionally, they would need to measure the applications and technologies that support the needs of the organization [7]. Big data is supporting organizations in making decisions based on analyzing high volumes of data from various sources [9], such as the Internet of things (IoT) [10]. Benefitting from big data requires high levels of preparation in terms of applications, tools, and resources selected and used. Organizations also need to formulate new regulations and policies to ensure data security, privacy, accuracy, quality, and control. The growing volume, variety, and velocity of data present critical risks and call for more preparations [7].

These factors have required enterprises to change their ways of presenting services to customers, from the "old era" services to the "new era" services. The term, online services (application services), came into the picture due to enterprises' awareness towards technology services. This development needs the procedures for these services to be done remotely. From this point, more people have started to look at such services because they help with working remotely and do not take much time to implement. Additionally, these huge services need a technological environment that can accommodate them. Those application services developers with innovative ideas, however, need not being worried about application services' limited resources.

One critical trend is evident in CCE services, which seems like it will change the world. CCE is made up of a pool of computing resources that can be configured, offering the uniqueness of quick setup and minimal service interaction (US National Institute of Standards and Technology (NIST)) [11]. CCE can accommodate the high demands for services in this unprecedented crisis, and the adoption of CCE services reduces the cost and setup complexity. There are a lot of benefits for cloud users, such as not having to invest in hardware, network infrastructure, or software licenses. CCE has low up-front costs, quick deployment, customizable features, and flexibility, while also being a solution with room for innovation. These CCE features are effective and attractive. One of its most valuable features is that it is accessible to all users and enables them to interact with online application services. For example, in 2014 there were more than 900 social media sites available on the Internet [12]. Nowadays, their numbers continue to increase. This, in turn, creates rapid growth in the number of Internet users. Today, around 90% of companies' services are on CCE [13]. For instance, to boost its business, IBM has announced two new services for enterprises to move their applications and data to CCE. These two services are called IBM CCE Migration Services and IBM CCE Deployment Services. These help enterprises make their existing workloads available to the public CCE, adding ease to the deployment of services and the cost-effectiveness of creation. This means the demand for CCE is expected to be driven by flexibility, agility, security, and above all, lower costs [14].

Amazon’s “Greatest Hits” is its cloud service, Amazon Web Service (AWS) [11]. It accounted for 55% of the company’s operating profit in the second quarter (Q2), 2018. The migration of applications services to CCE is anticipated to increase at a significant compound annual growth rate (CAGR) of 22.59% during the years of 2019 to 2022. This statistic may change due to the current coronavirus
outbreak, with a possible increase in this percentage. In this case, the adoption of CCE will help enterprises to bridge the gap between the information technology (IT) capacity and business demand [15]. The increasing adoption of CCE solutions that deliver both advanced and basic application services [16,17] supports the rapid growth of e-commerce applications and by ensuring access to almost unlimited resources when they are needed. This aims at eliminating application developers’ worries of overcoming these challenges. This shows the extent to which CC is efficient in supporting services, even in a crisis. According to Fremont Rider (1944) [18], the American University Library may double in size every 16 years. He predicted that by 2040, this library will hold more than 200 million volumes of books which will occupy 9656.064 km of shelves. According to Cisco, by 2021, CCE data centers will process 94% of workloads and compute instances; only 6% will be handled by traditional data centers. Further estimates show those data center workloads and compute instances will increase 2.3-fold from 2016 to 2021. For OC, it will most likely reach 2.7-fold over the same period. By 2021, total cloud workloads and computing services will be accessible to 75% of people. Based on this estimate, the cloud will be the fastest-growing application [19].

In light of this projected growth, the application’s traffic will be between 80% and 90% of total Internet protocol (IP) address traffic. Global traffic will account for 82% by 2022 [20]. According to Cisco, Internet gaming is gaining traction and may grow 9-fold between 2017 and 2022. Researchers suspect, however, that the current crisis may cause a higher percentage of growth. While gaming on-demand and streaming gaming platforms have been around, many new releases in recent times could boost gaming to become one of the biggest Internet traffic consumers [20]. Unlike traditional data centers, CCE will offer faster services and data delivery, improve the operational efficiency, and increase the application performance [17,21]. Currently, because of the coronavirus crisis, all scales of recent statistical analyses have changed due to massive increases in demand. In light of the COVID-19 pandemic caused by the novel coronavirus, human life and working culture have radically changed. As such, this paper shows the effects of COVID-19 on CCE. The research presents a high demand for CCE, especially on the application layer, due to the increased demand for applications used in those of education, work, entertainment, and other sectors. Moreover, the pandemic crisis exposes CCE to different types of attacks.

COVID-19 has undeniably changed human life and working culture. The demand for applications from CC in various sectors, such as education, entertainment, and business, has increased exponentially. These rapid changes have triggered enthusiastic researchers to move their focus towards the pandemic and how industries are coping with these changes. Hence, this paper seeks to address the following questions:

a) How has the COVID-19 outbreak affected CCE?

b) From a security perspective, what are the issues that might arise when working from home?

To our best knowledge, the COVID-19 related research to date has tended to focus on socioeconomic impacts rather than on computing technologies. As such, this paper critically examines the impact on CCE and highlights some security concerns in using CC applications at home. The findings of this study have several important implications for future practices, particularly living in this “new normal” life due to the COVID-19 pandemic.

The rest of the paper is organized as follows: In Section 2, the impact of the pandemic outbreak crisis on CCE is discussed. Section 3 describes the security risks present in working from home. Section 4 is the discussion. Section 5 presents the limitations of the research. Section 6 provides the conclusion.

2. Impact of the COVID-19 outbreak on CCE

Even with COVID-19, the relationship to CCE is a continuity relationship, unless a new technology comes after CCE. CCE is a system configured from applications, IT infrastructure, and network services. It uses the resources of a data center (DC), which can be shared through the virtualization technology. This use of services is on-demand, elastic, or instant services and rates. They are also charged as a utility bill [22,23]. CCE characteristics can be visualized in a graphical form, as illustrated in Fig. 1.

With this concept of “computing as a utility”, there is a lot of potential in CCE, just as that in electricity, gas, and water. With options like plug and play, or even a “pay as you go” system, the potential is huge. Customers are free to choose their software, platform, and infrastructure needs. With this potential, users do not need to plan for IT growth in the near future. As a utility, there is scalability and

---

Fig. 1. Schematic definition of CCE.
instant access. However, like any computing feature, there will be security gaps in threats, trust, and risks. CCE needs more work in the area of security to minimize or close all these gaps [24,25]. The cloud model comprises two parts: 1) CSP that delivers cloud services and 2) cloud users represented in organizations or individuals that access the provided cloud services. Other potential components are the cloud auditor and the cloud broker [26]. With the rise of new applications over the Internet, more security is required.

The CC model includes the platform, hardware, software, and infrastructure as a service and is now a complete package [27], with these service models now described as a type of service offered [28]. The three categories are: Infrastructure as a service (IaaS), software as a service (SaaS), and platform as a service (PaaS) [29]. In cloud deployment, there are four models: a) Private cloud, b) public cloud, c) community cloud, and d) hybrid cloud [30,31]. Each model describes how the cloud is deployed or what is available to users. Clouds can be based on the size, type of services, location, type of users, and security. CCE is deployed through the virtualization technology. This virtualization is an abstraction called the virtual machine monitor (VMM) or hypervisor layer between the operating system, hardware, and applications [32]. VMM is similar to a controller. This controller governs hardware resources and enables multi-tenancy. To share resources, multi-tenancy allows multiple operating systems to reside on the same physical hardware at the same time [33].

3. Security risks of working from home

There are many types of business models in markets, such as business-to-consumer (B2C), business-to-business (B2B), and business-to-government (B2G). These types of business models were rarely in demand in many countries until online consumer businesses became heavily saturated. Now, COVID-19 has unexpectedly given life to home-to-X terminology, like home-to-business (H2B), home-to-government (H2G), or home-to-consumer (H2C). This technology involves virtual meetings, digital healthcare, online education, cybersecurity, logistics to smart cities, and telecommunications [39]. Office and education centers have been closed, and stay-at-home orders have resulted in a massive and sustained surge in users’ collaboration, learning, and entertainment solutions into virtual-only ones. This “stay-at-home” situation to limit the spread of this disease is not for a short period, and may extend over months, as announced in many countries across the world. Therefore, moving work to home is necessary for maintaining the continuity of work. In other words, the work environment is transferred to home, both individually and virtual-collectively (virtual-together) remotely. On the
other hand, it will result in unexpected damage and security issues. These can be classified into five new taxonomies based on the issues of security of home-to-X: Data privacy, applications, personal devices [40], the Internet, and CCE, as shown in Fig. 3.

3.1. Data privacy issues

Nowadays the COVID-19 crisis has generated huge amounts of data through the different sectors’ transactions. One place that shows promise is big data [7]. Data is collected for healthcare, whether from patients, the virus genome, pharmaceutical to clinical trials, social media, and even facial recognition data. Researchers can be resourceful and apply all of these data to help curb the disease or discover a cure [41]. Therefore, data must be stored and processed correctly.

Current concerns about this massive amount of data are the circumstances related to this crisis. Because it has led people to work from home, they are also forced to transfer, use, and withdraw data from the Internet, removable hard disks, or flash memory cards. All these methods may not be secure to transfer data because they may change data or duplicate it, or it could be hacked. At home, there is no backup solution to track changes in data or new data. The data quality includes four aspects: Accuracy, redundancy, completeness, and consistency [42]. Regulatory requirements must be followed to avoid legal issues as much as possible. There is also the question of data being exchanged across the globe with each country having different laws and regulations concerning privacy laws of data protection and data integrity. There will be risks associated with the jurisdiction and loss of data. Even more, the business could be interrupted if the traffic network is congested. Questions as to where data is stored need to be addressed, as do other such legal requirements. Whenever data protection is deployed and all security solutions are provided, data owners should have full control over who has the right to access and has proper authorization to use the data. All institutional security policies must be adhered to.

One of the basic needs of securing data transmission is the need to ensure the existence of a virtual private network (VPN); however, many VPNs are considered fake and can be malicious. Therefore, employers and employees should limit their use of the binder only. It will secure and encode the communications channel with the Internet protocol security (IPSec) technology for the data to be exchanged safely. The data that is handled must be via easy transport systems so that there is no overload on the power of the communications channel that is passed through.

3.2. Internet quality issues

COVID-19 in 2020 is one of the biggest drives for tremendous and extraordinary digital transformation worldwide [43]. It suddenly turned ordinary working life into a virtual one [44]. It also has affected the use of the Internet and applications, even so much as causing fears of the Internet and social media collapse [45].

The coronavirus pandemic has a huge impact on the Internet, and this unexpected urgency and demand have caused some problems for Internet service providers (ISPs). This, in turn, is reflected in users when using applications from home. These applications usually need a good Internet speed to work properly for audio, video quality, and transfer of data. Vodafone reported that the Internet usage has surged up to 50% in some European countries [46] and in the UK it is expected to experience a 30% rise [38]. TalkTalk revealed an increased demand of around 20% on Tuesday, March 17 following Boris Johnson’s guidance for millions to work from home. As shown in Fig. 4, data is provided from the same period from Open Reach; however, it is still far below the normal evening peaks. It is defined as 10 times the typical daytime (working hours) demand and can be up to 17 Tb/s [38,46].

While these are important, it is even more crucial to maintain a high-quality experience once the sessions are established. To ensure Internet stability, PlayStation-Sony lowered the bandwidth for download speeds in the US and Europe [47] to preserve the Internet availability for the whole community [48]. In the UK, mobile networks and Internet providers are being urged to relax data limits as online traffic reaches a peak of 30%. There are millions of Britons working or learning from home during this pandemic, resulting in companies cutting down the quality of their streaming services [46]. Netflix, which was at the forefront in terms of use, cut down the quality of its streaming during the period of the pandemic because of overloads. The move followed the calls by the European Union for
online media platforms to stream movies and entertainment in standard rather than high definition to relieve the pressure on Internet providers during this crisis [38].

Zeus Kerravala (ZK), the founder and principal analyst with ZK Research, asked Cisco to implement a 20% packet loss to reduce network congestion [49]. The test data from the packet loss caused periodic outages on both platforms. For Zoom, they used the extra bandwidth to recover faster, as its rate shifted down to 360 pixels. Following the test, Cisco downgraded its rate to 360 pixels.

Once the packet loss was achieved at 20%, Webex’s algorithms kicked in to restore video resolution to 720 pixels, while Zoom took a little longer to eventually recover to 720 pixels, but it was outside the testing window. Fig. 5 shows the bandwidth utilization between Zoom and Webex.

3.3. Applications issues

Another change which the COVID-19 pandemic crisis has initiated is social distancing. This makes working or learning from home necessary. As such, this now encompasses virtual work, virtual meetings, and distance learning. The rapid spread of COVID-19 accompanied high volumes of data in different formats such as structured, semi-structured, or unstructured data, requiring these applications and large processing abilities [50]. Performing this level of data without sufficient technology infrastructure and applications is difficult, so the use of various kinds of applications pressure organizations to realize the new technology [7,18]. An analysis from an investment firm Yunqi Partners stated that there are opportunities for remote collaboration tools for people to work collectively even when they are not physically together. Among the popular downloads of work apps are WeChat Work, DingTalk, and TikTok’s sister, Lark. America’s Zoom jumped exponentially from No. 180 at the end of January to No. 28 at the end of February 2020 in terms of downloads and installs, as shown in Fig. 6. The downside to this rapid growth has been hacked and pirated due to the security faults in the application.

In the UK, ISPs are offering customers unlimited access and increased data to the National Health Services (NHS) sites during this time of self-quarantine [46]. Vodafone, which offers both broadband and mobile Internet, has stated it will give customers unlimited access to NHS of UK online websites [46]. MailOnline understands Everything Everywhere Limited (EE), Three UK mobile (Three), and
Telefonica O2 UK Limited (O2) will also offer free access to NHS websites [46]. As mentioned before, Netflix also announced it would cut down the quality of its streaming services by 25% [38]. The Pokemon Go application game has been reinventing itself to cope with the current circumstances and the increased demand to play from home [51].

Apps from other parts of the world helping people nationwide to work from home are Alibaba’s DingTalk, ByteDance’s Lark, and Tencent’s WeChat Work. Sensor Tower compiled these app rankings, and all three apps have year-over-year growth in downloads from January to February 2020, i.e., Lark: 6085%; DingTalk: 1446%; and WeChat Work: 572%. DingTalk, an app developed by an Alibaba team, launched in 2014. It became the most-downloaded free iOS app in China [52].

3.4. Personal devices issues

Because the coronavirus pandemic crisis has forced people to work remotely from home, it has also led to the re-use of older devices. Many people working from home have little or no knowledge about the information technology and the security issues related to it. This makes security matters worse, after re-using personal devices such as personal computers, laptops, and tablets. These devices may have not been in use for a long time, requiring updates for the operating system, anti-virus software, previously installed programs, and so on. Cybercriminals have seen an opportunity to exploit people, as they have already developed malicious software to infect devices [53]. All of these devices might get infected with malware (Botnets) when connecting to the Internet to use web applications and get updates from the servers that are located on CCE, which will cause great damage if these devices are infected once they are connected to the Internet. Malware may cause an increase in Internet traffic, leading to distributed denial of service (DDoS) attacks.

3.5. CCE

As the viral outbreak continues to spread, many people around the world are now experiencing social distancing, work-from-home environments, and other changes to their daily lives, making CCE an unsung hero in terms of work-from-home solutions. While systems should have the ability to control and manage the changing velocity of capturing and analyzing large volumes of data, scalability is a critical characteristic of storage and analytical systems, meaning that the availability of IT infrastructure is required [7]. The public cloud and its enabling technologies are supporting the massive shift to remote work and learning. Several CCE stocks, like Zoom, will increase in value over the next few quarters. RingCentral, Inc. offers a cloud-based suite of communications tools, and the sales increased 34% to clock in at $902 million [54]. AWS has committed $20 million in CCE credits for researchers working on tracking and studying the disease, looking to accelerate the development of tests by allowing researchers to run workloads at no cost on its CCE. The launch has 35 labs and businesses participating [55]. Alibaba has pledged support to fight against this disease, since its cloud revenue is more than 10 billion yuan for the first time. It has grown 62% to hit 10.72 billion yuan for its third quarter (Q3) [56].

The COVID-19 crisis has impacted almost all sectors, including tourism, health, education, CSPs, and others. In education, many institutions, such as Western Michigan University [57], Washington’s Office of the Superintendent of Public Instruction [58], and Zhejiang University (ZJU) [59], have had to shift traditional learning to distance learning in response to this pandemic. Students have stopped going to the campus to receive lectures and instructions at schools and universities. Online services for distance learning are important to continue the interactions between lecturers and students during closures [36]. The online tools that are provided by software developers are critical in helping all those sectors running businesses during the difficult and complex time like these. As the situation evolves, potentially even more work will be migrated to online applications’ services. This means that they must move fast to meet business needs and avoid financial losses, particularly for education.

Therefore, the education sector needs to purchase software to continue teaching remotely and ensure it runs without interruption.

Fig. 6. Usage of the Zoom application.
CCE offers various types of services, such as website hosting. It also provides online software and a platform for developing applications [60]. A website hosted in CC allowing day-to-day access enables mobile devices like personal desktops and smart devices to connect. At this time, CCE has various security issues, as evidenced by cyberattacks [61]. These attacks, according to the Cloud Security Alliance (CSA), show how DDoS attacks are dangerous to CCE security [62]. The DDoS attack is a very large threat [16]. Therefore, providing security to CCE secures the website it hosts, and vice versa [63]. Some characteristics of CCE may be harmful if exploited by smart attackers, especially since availability is the main requirement for web application services on CCE. One of the most important things is to preserve the rights between the two parties as CSP and as a consumer. For example, a service level agreement (SLA) is made to ensure the quality of service. SLA describes how the provider will deliver and how the consumer will use, a set of services. All responsibilities and remedies for each party are clearly stated.

CCE has vast infrastructure as a distributed service-oriented paradigm consisting of multi-domain, multi-operating, and multi-user systems. It tends to have more security against threats and vulnerabilities, such as DDoS and EDoS attacks. One of the risks is out of control for the over-provisioning of resources. Over-provisioning can lead to the lack of availability of resources, thereby creating a denial of the service scenario. When this happens, those who work from home are critically affected. Because CCE provides virtual infrastructure through virtual machines (VMs), different CCE VM users may have the same or different physical hosts at the CCE center. This makes CCE vulnerable to denial-of-service (DoS) attack/DDoS. If one VM is infected and initiates a service denial attack on the physical host, then the other VMs on the same host will also be affected. The DDoS attack makes use of a network of many resources compared with a DoS attack, which comes from a single source. Table 1 shows the advantages and disadvantages of CCE characteristics within the COVID-19 pandemic crisis.

### 4. Discussion

China utilized data and digital technologies to help fight the disease by using robotics and drones [64,65]. The former is used to prepare meals at hospitals, perform diagnoses, conduct thermal imaging, and transport medical samples. The latter is used to spray disinfectants to try to prevent the spread of the virus. Applications are also using the big data technology with artificial intelligence (AI) for face recognition and infrared temperature detection. AI is further playing a heroic role in healthcare with COVID-19, such as helping in predictive and data analytics. Consequently, there has been the collaboration between the Chinese government and Alibaba and Tencent to develop an application, such as the health system. The health rating system quick response (QR) codes were used to track millions of people daily, while blockchain was utilized to help sectors during this crisis to deal with potential financial constraints. This is another way in which the COVID-19 crisis has unexpectedly increased the Internet use, not only by forcing people to do their work from home, but also to transfer, use, and withdraw data. People have been using applications for virtual work, virtual meetings, and distance education, among others, while also re-using their old devices to move the applications onto CCE. The previous research has not reported that the number of services on CCE would reach this limit in a very short period. The increase in the data volume requires additional data storage systems, services, storage mechanisms, new environments, and technology infrastructure that meet the demands for massive amounts of data [9].

The effect of the coronavirus on CCE came from moving a lot of application services onto it, which might increase certain types of attacks, such as an EDoS attack [66]. This attack targets the CCE billing system rather than the physical resource itself. In addition, EDoS targets the auto-scaling feature of CCE and prompts more and more resources to be added by CSP to meet the availability of the service based on SLA. Extra resources add extra billing costs, which leads to more financial burdens on the CCE consumer [67,68].

Moreover, “stay-at-home” may support DDoS and EDoS attacks and make matters worse. Workers and students are likely to re-use outdated personal devices and these devices, whether infected or not with malware, will reconnect to the Internet to use web applications while taking updates from the servers located on CCE. In addition, software developers will be trying to work fast to meet market demands, which could cause security holes that may lead to an increase in DDoS/EDoS attacks on CCE. Under all these, there is a persistent need to develop an efficient approach to detect the presence of EDoS attacks, especially in the current situation of the COVID-19 pandemic crisis.

### Table 1

| CCE characteristics | Advantage | Disadvantage |
|---------------------|-----------|--------------|
| On-demand self-service | Any time | – |
| Security | 50% secure | 50% not secure |
| Time to run service | Real time | – |
| Service availability | 99.99% | Unexpected issues with X attacks |
| Resources expandable of VM | Elastic | Issues elastic with X attacks |
| Resources expandable of CCE | Scalability | – |
| Resources type | Heterogeneous | – |
| Environment work | Virtualization | – |
| Services cost | Low pay-as-you-use | High with X attacks |
| CCE down time | 99.99% running | Unexpected issues down (electricity outages, X attacks) |
5. Limitations of the research

There are not yet enough resources about attack cases on CCE that have occurred during this period, because the COVID-19 pandemic crisis is ongoing.

6. Conclusion

The dependency on CC applications and other technologies has dramatically increased due to the current situation of the COVID-19 pandemic. Undoubtedly, this pandemic crisis has impacted almost all sectors, such as tourism, healthcare, education, CSPs, and others. Furthermore, the COVID-19 crisis could cause a permanent shift towards working from home as precautionary measures for containing the virus. The global rapid spread of COVID-19 has also increased the volume of data generated from various sources. The increase in the data volume needs additional data storage systems, storage mechanisms, new environments, and novel technologies, all of which create a critical challenge. In this paper, we have tried to clearly show the actual and potential impacts of the COVID-19 crisis on CCE and other technologies due to the sudden increase in working from home. Additionally, this paper analyzes the security risks for working from home. From a security perspective, the current situation might expose both CCE and its users to different types of attacks due to the lack of preparedness to face such a sudden situation. For CCE, attacks, such as DoS, might be prominent during the period of COVID-19. Users might be vulnerable to different types of attacks as they operate untrustworthy Internet applications on their own home devices, which might not be updated or patched with the latest security policies. Therefore, at-home workers might become the target of attackers to easily steal (copy) large amounts of data. As a result, there is a need to address the security risks that CCE and users face, as well as to raise the awareness of users about the threats of using unsecured devices to access the Internet when they are working from home.

References

[1] UNESCO, School closures caused by coronavirus (COVID-19) [Online]. Available, https://en.unesco.org/covid19/educationresponse, April 2020.

[2] British Broadcasting Corporation, Coronavirus: School closures and travel curbs in UK plans [Online]. Available, https://www.simhospital73.com/2020/03/coronavirus-school-closures-and-travel.html, April 2020.

[3] Office of Postsecondary Education, Guidance for interruptions of study related to coronavirus (COVID-19) [Online]. Available, https://www2.ed.gov/coronavirus/files/2020/03/COVID-19/EA-Guidance for-interruptions-of-study-related-to-coronavirus-COVID-19.pdf, April 2020.

[4] Edsource, How learning will change across California’s K-12 schools amid coronavirus closures [Online]. Available, https://edsource.org/2020/how-learning-will-look-very-different-across-californias-k-12-schools-amid-coronavirus-closures/625623, April 2020.

[5] Universiti Sains Malaysia (USM), COVID-19: social responsibility, preventive policy and current developments at Universiti Sains Malaysia [Online]. Available, https://www.usm.my/index.php/covid19/announcements/754-covid-19-social responsibility-preventive-policy-and-current-developments-atuniversiti-sains-malaysia, April 2020.

[6] Z.R. Al Ashhab, M. Anbar, M.M. Singh, K. Alleyan, W.I. Abu Ghazaleh, Detection of HTTP flooding DDoS attack using Hadoop with MapReduce: a survey, Int. J. Adv. Trends Comput. Sci. Eng. 8 (1) (Jan.-Feb. 2019) 71–77.

[7] Z.A. Al-Sai, R. Abdullah, M.H. Husin, Big data impacts and challenges: a review, in: Proc. of IEEE Jordan Intl. Joint Conf. on Electrical Engineering and Information Technology, 2019, pp. 150–155.

[8] R. Krishnamurthi, M. Goyal, Enabling technologies for IoT: issues, challenges and opportunities, in: B.B. Gupta (Ed.), Handbook of Research on Cloud Computing and Big Data Applications in IoT, IGI Global, Hershey, 2019, pp. 32–82.

[9] C. Stergiou, K.E. Psannis, B.B. Gupta, Y. Ishibashi, Security, privacy & efficiency of sustainable cloud computing for big data & IoT, Sustain. Comput.: Inf. Syst. 19 (Sept. 2018) 174–184.

[10] S.P. Ahuja, Architecture of fog-enabled and cloud-enhanced Internet of things applications. IGI Global [Online]. Available, https://www.igi-global.com/article/architecture-of-fog-enabled-and-cloud-enhanced-internet-of-things-applications/240691, July 2020.

[11] R.K. Sharadchandra, L.M.R.J. Lobo, Parallelization of genetic algorithm using Hadoop, Int. J. Eng. Res. Technol. 1 (9) (Nov. 2012) 1–5.

[12] StatisticBrain, Twitter statistics [Online]. Available, https://www.statisticbrain.com/twitter-statistics, April 2020.

[13] Casson Prweb, 451 research: 69% of enterprises will have multi-cloud/hybrid it environments by 2019, but greater choice brings excessive complexity [Online]. Available, http://www.prweb.com/releases/2017/11/prweb14952386.htm, April 2020.

[14] MarketsandMarkets, Cloud migration services market size, share and global market forecast to 2022 [Online]. Available, https://www.marketsandmarkets.com/Market-Reports/cloud-migration-service-market-266815130.html, April 2020.

[15] MarketWatch, Global cloud migration services market size by 2022: top players, growth factors, trends, business development [Online]. Available, https://www.marketwatch.com/press-release/global-cloud-migrationservices-market-size-by-2022-top-players-growth-factors-trends-businessdevelopment-2019-09-27, April 2020.

[16] The Next News, Hong Kong group battles huge DDoS attack [Online]. Available, https://thenextweb.com/asia/2014/06/20/cloudflarehong-kong-democracy-movement-battling-one-largest-ddos-attackshistory/#nv_N1dwMQei, April 2020.

[17] Cisco, Cisco global cloud index: forecast and methodology, 2016-2021 [Online]. Available, https://www.cisco.com/c/en/us/solutions/executive-perspectives/annual-internet-report/index.html, April 2020.

[18] K. Fischbach, U.R. Krieger, Measurement, Modelling, and Evaluation of Computing Systems and Dependability and Fault Tolerance, Springer, Cham, 2014, pp. 5–597.

[19] The Japan Times, Outbreak of SARS-like pneumonia being investigated in China [Online]. Available, https://www.criticalinfrastructurereprotectionreview.com/news-december-2018/outbreak-of-sars-like-pneumonia-being-investigated-in-china/, April 2020.

[20] Cisco, Cisco visual networking index: forecast and trends, 2017-2022 [Online]. Available, https://www.cisco.com/c/en/us/solutions/collateral/executive- perspectives/annual-internet-report/white-paper-c11-741490.html, April 2020.
Ziyad R. Alashhab is pursuing his Ph.D. degree with the National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia (USM), Penang. He received his B.S. degree in business networking and systems management from University of Philadelphia, Philadelphia in 2005 and the M.S. degree in management information systems from Arab Academy for Banking and Financial Sciences (AABFS), Jordan in 2008. His research interests are network security, the Internet security, and cloud computing and security.

Mohammed Anbar obtained his Ph.D. degree in advanced computer network from USM in 2013. He is currently a senior lecturer with NAv6, USM. His current research interests include malware detection, web security, intrusion detection system (IDS), intrusion prevention system (IPS), network monitoring, Internet of things (IoT), and Internet Protocol version 6 (IPv6) security.

Manmeet Mahinderjit Singh is a lecturer with the School of Computer Sciences, USM. She graduated from The University of Queensland, Brisbane in 2012 with the Ph.D. degree in data security. She obtained her M.Sc. and B.Sc. degrees in computer science from USM in 2006 and 2001, respectively, specialising in the field of distributed systems. Her passion and expertise are in the areas of information and cyber security, trusted system models, cybercrime prevention and detection, and mobile security. She is interested in data mining technologies and sensor networks. She is also interested in the applicability of IoT in smart home, smart city, wearable devices, and “bring your own devices” (BYOD).

Yu-Beng Leau is a senior lecturer in computer science with the Faculty of Computing and Informatics, Universiti Malaysia Sabah (UMS), Kota Kinabalu. He received his B.Sc. degree in multimedia technology from UMS in 2004, the M.Sc. degree in information security from Universiti Teknologi Malaysia, Johor in 2006, and the Ph.D. degree in Internet infrastructure security from USM in 2016. His current research interests are Internet infrastructures security (IPv6, information-centric networking (ICN), software-defined networking (SDN), and vehicular ad hoc network (VANET)) and information security management (IoT, cloud computing, and big data).
Zaher Ali Al-Sai received the B.S. degree in computer science from Al-Zaytoonah University of Jordan, Amman in 2004, and the M.Sc. degree (Honors) in e-government project management-MBA from Al-Balqa’ Applied University, Al-Balqa in 2014. She is currently pursuing her Ph.D. degree in software engineering and big data with the School of Computer Science, USM. She is currently an active researcher in the fields of empirical software engineering and big data. Her research interests include big data analytics, software process improvement, big data engineering, big data development, big data readiness and maturity assessment, and evidence-based software engineering. She is a presenter for many workshops on performing the systematic literature review and research support topics. Also, she is the founder and CEO of the non-profit organization “Big Data Minds”.

Sami Abu Alhayja’a is pursuing the Ph.D. degree with NAve6, USM. He obtained his B.S. degree in computer information systems from Zarqa Private University, Zarqa in 2008 and his M.S. degree in information technology from Universiti Utara Malaysia, Kuala Lumpur in 2011. His research interests are network security, Internet security, and IoT.