

Security Risks of Cloud and Mobile Technologies During the Pandemic and Their Opportunities

Alexis-Valentin ZAHARIA
Bucharest University of Economic Studies, Romania
alexis.zaharia@ie.ase.ro

In the current pandemic situation, social distancing is the new normal. Jobs that allow remote work are done from home and technologies for video conferencing, online shopping, online services from the state etc. are now in the foreground. Cloud and mobile technologies were already on an upward trend in popularity, but this period propelled them even more into people's preferences. However, like any technology, they can pose security risks in the context of a more intensive use by a larger audience, which must be considered. Of course, the risks must also be measured in comparison with the opportunities that have arisen in the new context.

This paper aims to analyze the potential security risks posed by a more intensive use by a larger population of the cloud and mobile technologies. At the same time, the opportunities brought by these technologies in the new pandemic context will be analyzed.

Keywords: cloud, mobile technologies, pandemic, security risks, opportunities

DOI: 10.24818/issn14531305/24.3.2020.06

1 Introduction

The current pandemic situation forces us to find ways to communicate and work respecting the rules of social distance. Companies are increasingly open to the idea of working from home. Technologies that allow working from home are increasingly sought after. Thus, the cloud is becoming an increasingly popular technology in the current situation.

More intensive use of cloud services means more opportunities for malicious actors to produce cyber-attacks. An increase in interest in the cloud can lead to a directly proportional increase in the number of attacks. In addition to more intensive use of the cloud by existing customers, new customers have emerged who have considered migrating their businesses to the cloud. These new customers can also come up with new security issues, in terms of setting up and using the accounts created for them.

The opportunities brought by the cloud, however, outweigh the risks posed by these services. Cloud technologies have matured, implementing better and better security solutions. This encourages more and more people to try these services, especially during this period.

This paper is a continuation of [1] which presented the role of the cloud for mobile

solutions in the current pandemic context. It aims to analyze the current use of the cloud and mobile technologies; this use being increasingly emphasized. Also, the potential security risks arising from the use of these technologies will be analyzed, as well as the opportunities brought by them.

2 Literature review

Mobile devices and technologies have developed a lot in recent years. They allowed people to access the computing power of a PC on the go, changing the way people retrieve the necessary information and interact with each other. Mobile technologies have been well received by the population, with more and more people leaning towards their use, which has led experts to believe that the future of information technology lies in mobile technologies with wireless networks for communication [2].

Cloud computing technologies have become increasingly popular in recent years, especially by large companies. Cloud computing allows the storage of data and applications of companies and provides very powerful computing services. A major attraction for the cloud is the fact that it reduces the cost of a company to create its own IT infrastructure. The growing network of data transmission

capacity, computers and low-cost storage media has led to a growing popularity for cloud computing [3].

Mobile technologies in the cloud computing environment are of increasing interest in the current context, the role of this binder being to bring rich computing resources to users of mobile devices. Although mobile devices are becoming increasingly powerful in terms of resources and computing power, they are still considered limited, with current technological developments leading to an increasing volume of data, and the need for increasingly powerful data analysis and processing programs for these vast volumes of data. In this case, Mobile Cloud Computing attacks the limitations of mobile devices such as limited processing capacity and limited storage capacity, delegating these requirements to other systems with better performance and rich resources [4] [5]. In addition to the increased processing and storage capacity, cloud computing also comes with a very important aspect, which is security. According to [6], 74.6% of companies

mentioned security as a major challenge. General vulnerabilities in the cloud are: unauthorized access to data and accounts of cloud service users, Internet protocols, command injection vulnerabilities (SQL injection, OS injection), API and web browser vulnerabilities. To solve these security issues, you can encrypt data transmitted over the network, scan for malicious activities, check the connected account, and secure interfaces and APIs [6] [7] [8] [9].

3 The current context of the cloud and mobile technologies

I took statistical data to see the current use of the cloud and mobile technologies. I organized this data according to a set of criteria, such as the time spent on different types of devices, the traffic consumed by different types of devices and the number of people who opted for work from home in different periods. I analyzed the data obtained, performing a quantitative analysis on these data.

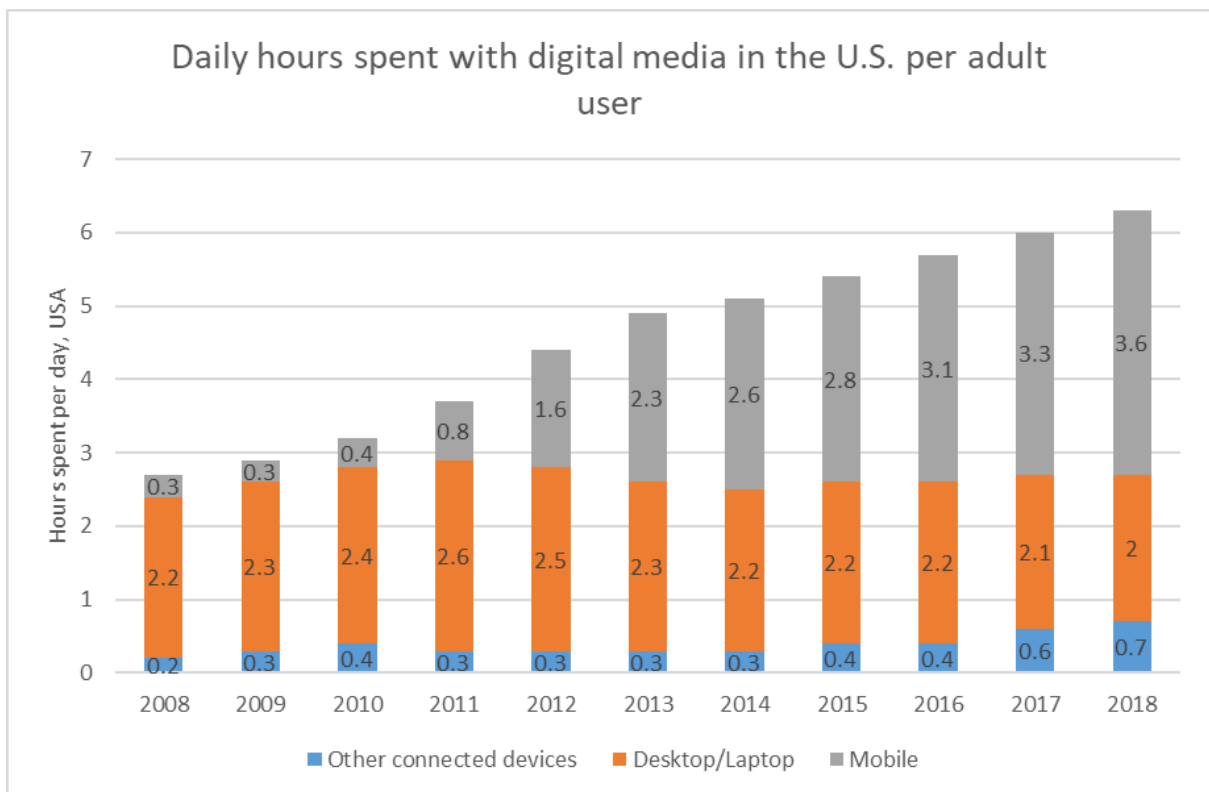


Fig. 1. Daily hours spent with digital media in the U.S. per adult user [10]

A study published in Statista last year, which presents the discoveries of Mary Meeker,

suggests that smartphones consume us for about a quarter of the day. We can see from

the graph shown in Figure 1 that in 2018 out of a total of 6.3 hours a day spent in the digital environment, people in the United States spend 4 hours in front of phones, a significantly longer time spent in front of mobile devices rather than desktop PCs or laptop devices, and this is accentuated by the increasingly powerful networks to which mobile devices connect, especially due to the latest leap in connectivity to mobile networks, 5G [10]. Mobile devices, although increasingly resource-intensive, allowing them to run increasingly demanding applications, are still limited. They are currently on the same level as processing power with some laptops, but the biggest limitation is the battery life, which does not last long. So, running demanding

applications, although possible with the current processing power of mobile devices is not recommended, as it will significantly shorten battery life.

To conserve battery and limit the calculations made by mobile devices, the "offloading" of mobile applications can be used. With the help of the offloading mechanism, applications and mobile devices become customers, entrusting a server with processing, which increases the efficiency of mobile devices and thus extends the battery life. Cloud services are perfect for such tasks, as they are already used to host applications running in the cloud. At the same time, the cloud also has a benefit for mobile devices, such as expanding storage capacity.

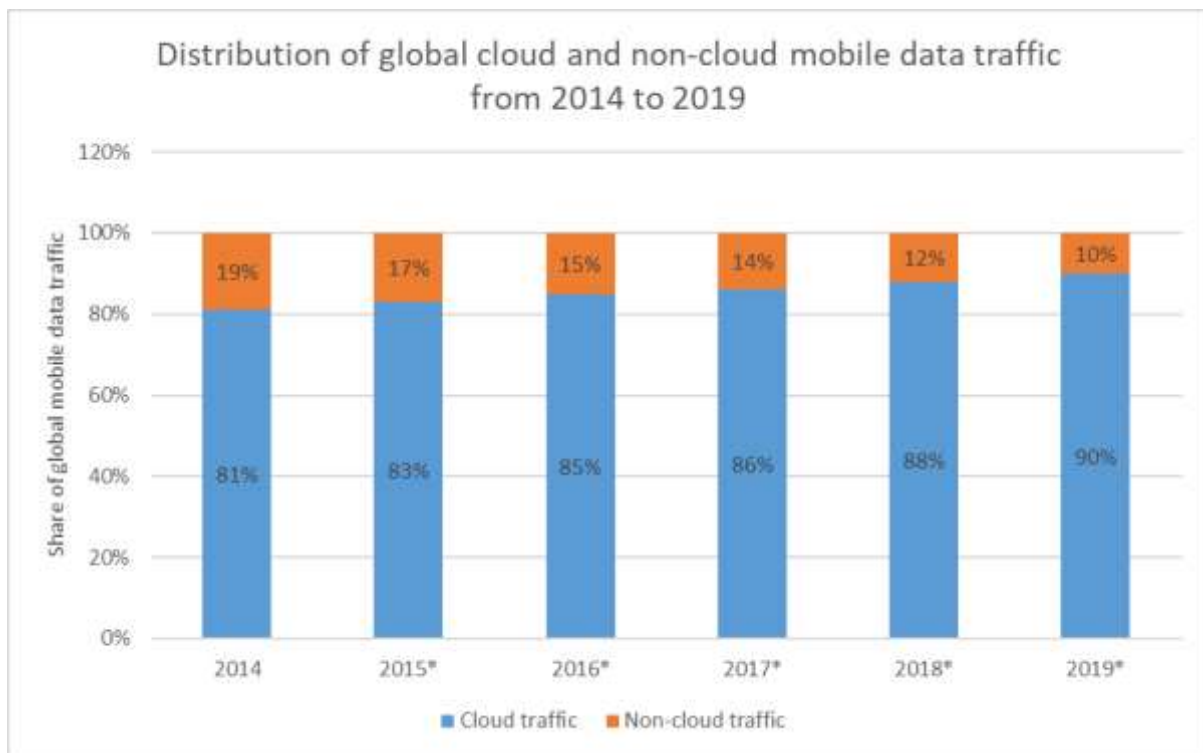


Fig. 2. Distribution of global cloud and non-cloud mobile data traffic from 2014 to 2019 [11]

Mobile devices and the cloud work well together, with the cloud being able to reduce the shortcomings of mobile devices, such as processing power draining battery and storage limitations. This is shown in a study conducted by Cisco Systems in 2014 which was written in February 2015 and published in Statista. This study indicates, as can be seen in Figure 2, that in 2014 mobile device traffic in the cloud was already 81% of total global

traffic with 19% representing non-cloud traffic. They have made a forecast for the coming years until 2019 which shows an increase in cloud traffic and a decrease in non-cloud traffic [11].

At the beginning of the pandemic, there was an increase in data traffic in the first 3 months of this year compared to last year, as can be seen in Figure 3. Data traffic for phones has increased the most. Desktop PC traffic is

declining compared to last year. It follows the trend of diseases by increasing traffic.

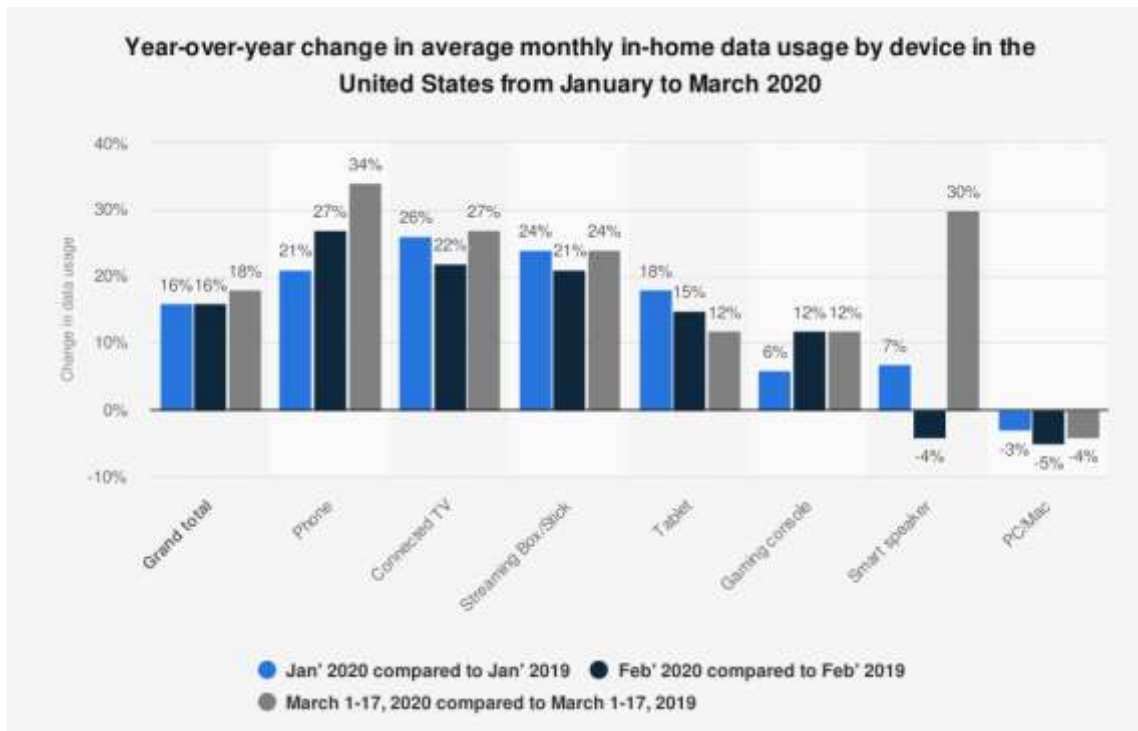


Fig. 3. Year-over-year change in average monthly in-home data usage by device in the United States from January to March 2020 [12]

Given the fact that in the context of the current pandemic, social distance is the best solution, the interest for remote work increased from

February to March. This trend has been accentuated from March 8 to 9 until now.

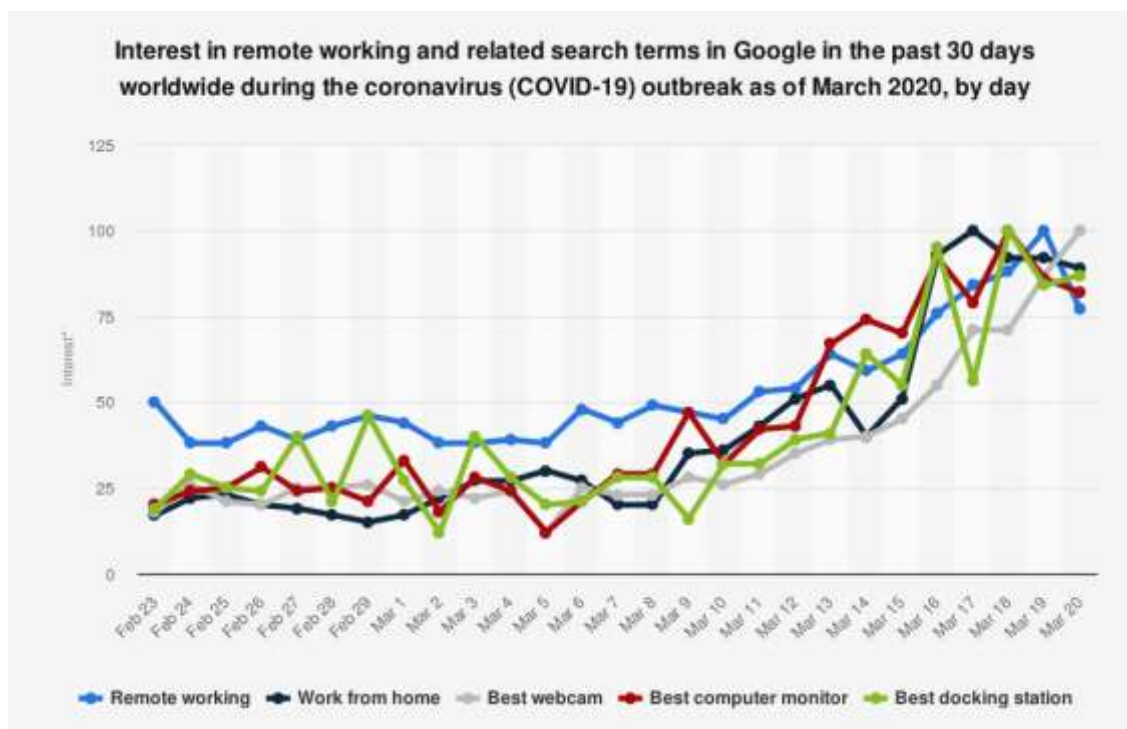


Fig. 4. Interest in remote working and related search terms in Google in the past 30 days worldwide during the coronavirus (COVID-19) outbreak as of March 2020, by day [13]

As the pandemic continues, and we are currently seeing signs of an increase in the number of positive cases of COVID, the trend of moving to work from home will also increase.

4 Cloud challenges

The cost-effectiveness of cloud computing has led to an increase in interest in the cloud, but data security remains a major concern. Organizations have adapted a low-risk approach to migrating business processes until the point where the cloud is considered secure. This is even though the cloud is more secure than most internal networks. Cloud service providers put security first, as it is the main competitive advantage and a barrier to the growth of cloud computing [14].

Mobile devices that access the Internet perform mobile cloud computing because phones need to borrow storage and computing energy from the cloud because of limited resources or because it makes more sense. Accessing cloud data from mobile devices is becoming a necessity. There are successful initiatives that use mobile cloud services, such as ING Home Bank, an M-Banking service. Other applications are in M-Health, M-Agriculture and M-Education [5] [14].

There are several barriers to cloud computing adoption, such as security, privacy, connectivity and open access, reliability, interoperability, independence from cloud service providers, economic value, IT governance, changes in IT organization, and borderline policy issues. global. The problems of developing economies when we adopt cloud computing, especially for small businesses, will be presented below [5] [14].

Security, privacy and trust

Security and privacy are crucial for mobile cloud computing environments because these characteristics determine the level of trust mobile users have when they offload some of their jobs on their mobile devices and store their personal data in the cloud environment. The dynamic and distributed nature of mobile cloud computing environments makes achieving such requirements a major challenge. In addition, privacy in mobile cloud computing

is quite different from traditional cloud computing because it involves more sensitive data such as location information from the GPS when various location-based services are used. Therefore, there is a strong need for robust, efficient and scalable techniques to ensure security and preserve the privacy of mobile users. Doing so will help mobile users to trust mobile cloud computing environments [5].

Infrastructure

Most rural communities in developing economies lack basic infrastructure, such as roads, telecommunications, electricity and water. These infrastructures are the backbone of any development initiative. This does not help the fight to reduce the digital divide. The lack of such infrastructure leads to the unavailability of internet infrastructure and to the increased costs of these services and the costs of internet access devices [14].

Bandwidth and data transfer

Mobile cloud computing brings several benefits such as longer battery life and storage for mobile devices which can be accomplished through centralized processing and storage at the cloud service's datacenter. This approach, however, may lead to more communication overhead because of the increased bandwidth consumption and data transfers. Unfortunately, the increased communication overhead can also lead to additional hidden costs for mobile users and can constitute a barrier between mobile cloud computing consumers and the mobile cloud computing service providers [5].

Data management and synchronization

Due to the hardware limitations of mobile devices, mobile cloud computing allows computation offloading where some computation tasks are transferred to the cloud datacenter. This process requires a proper data management system. In addition, cloud datacenters can synchronize mobile devices' applications and data to allow data accessibility from different devices or restoring data after a lost event. However, there is clearly a trade off

between offloading compute intensive tasks and bandwidth utilization. In other words, the same trade off takes place with frequent synchronization intervals. On the one hand, high computation offloading means more tasks can be accomplished. Moreover, more frequent synchronization intervals result in restoring the most recent lost data. On the other hand, increased bandwidth utilization means fewer tasks can be supported and restoring outdated data. As a result, it is important to understand when to offload compute intensive tasks and how frequently synchronization intervals take place. In other words, the mobile cloud computing environment requires strong data management and flexible data synchronization techniques [5].

Devices

Most households in developing countries do not have a personal computer and rely on mobile devices for internet access. Mobile service providers, in the case of less developed or developing countries, have rolled out more advanced 3G and 4G network coverage in all their access areas, with mobile networks bringing internet access to many areas outside major cities for the first time. It provides the backbone for launching a wider range of mobile services. However, services should not be limited to those available only on mobile devices, but should be extended to computers. This is true for the services provided by IaaS, for example, if the appropriate devices could

be personal computers not just mobile devices, so it is necessary to provide these devices and the ability to connect [14].

Internet coverage

Internet coverage in developing economies is still a challenge due to the lack of infrastructure, in this case, dial-up internet coverage, which does not cover most underdeveloped communities, such as rural areas. For example, Africa has 15% of the world's population, but represents 5.7% of the world's internet users. The lack of infrastructure in Africa has led to low bandwidth and high costs. On 23 July 2009, the 17,000 km SEACOM underground fiber optic cable became active, providing broadband connection to several African countries. Meanwhile, internet cafes are the main means of internet access in these developed communities and play a significant role in bridging the digital divide [14].

Romania, for example, is a developing country in Central and Eastern Europe. Internet coverage is on average 76.2% with the western and central part of the country having a wider coverage, while in the east and south-east the coverage is weaker, except for the capital Bucharest. This prevents the entire population, especially during this period, from being able to access online services, such as cloud services. Thus, the development of the infrastructure must be done quickly [15].

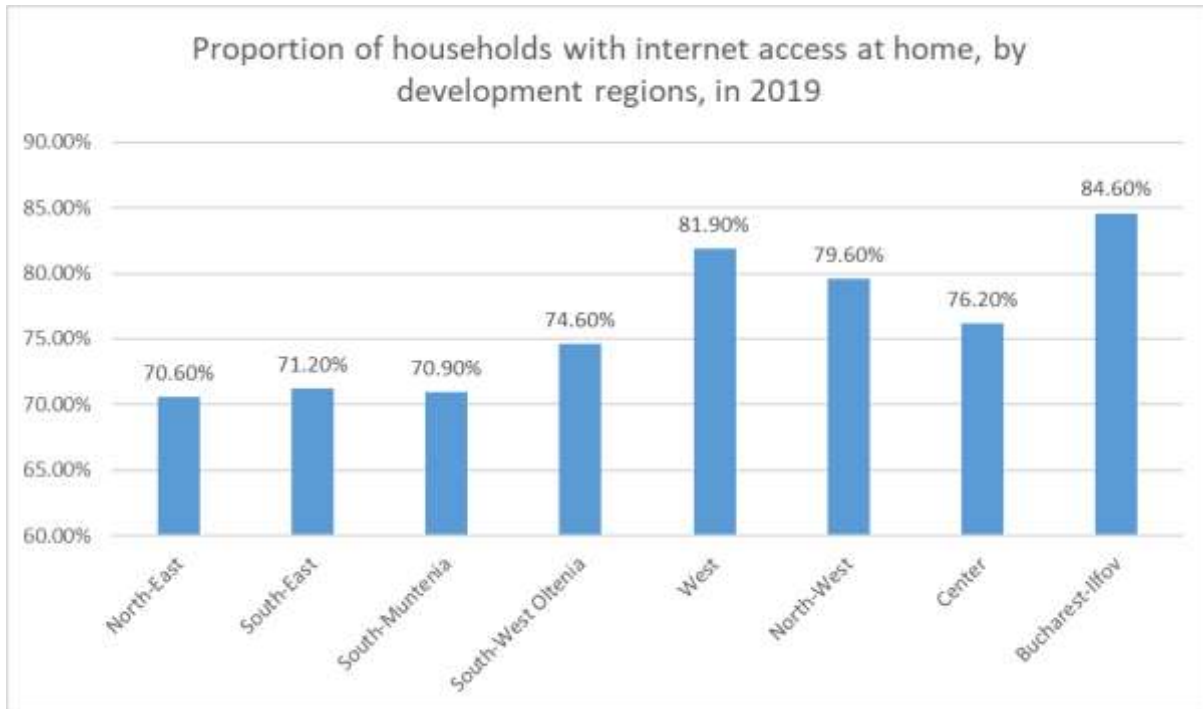


Fig. 5. Proportion of households with internet access at home, by development regions, in 2019 [15]

Physical location of data

Major cloud service providers are overseas companies such as Google, Amazon and Microsoft. Therefore, the infrastructure is usually not physically located in the consumer's premises, much less the same country, in the case of most developing economies. Therefore, there is a lack of control over an organization's assets. Cloud computing requires a higher bandwidth internet to be able to access servers in Europe or the USA [14].

5 Security risks and opportunities for cloud

The cloud has become a mature technology, accessed by more and more customers. However, although much progress has been made, it is also accompanied by security and operational issues.

Service availability

The cloud service may be unavailable for several reasons, these may include security breaches in the physical location of data centers, failure of equipment in the data center, failure of equipment on the consumer's site, failure of connectivity. This is exacerbated by

the lack of reliable internet connectivity in developing economies, as cloud computing relies heavily on network connectivity. Finally, steps must be taken to manage not only the risk of unavailability of temporary services, but also those situations where a cloud service provider abruptly and unexpectedly ceases to provide services. Therefore, the business must have alternative means to deal with such a failure if it affects business processes [6] [14].

Identity management

In addition to the smooth availability of the service, there is a need for reliable identity management to enable accurate pricing of cloud services. Identity theft is on the rise, so cloud consumers need to be sure that there are reliable verification mechanisms to check if people are who they are saying they are and to avoid the risk of payment for services accessed by intruders [6] [7] [14].

Data and application security

In cloud computing, several layers of security are needed to ensure consumer comfort. Security in the infrastructure layer (hardware, operating system and storage) must be applied.

The network layer for data transmission must ensure that all components of the final offer to the consumer do not have security holes. Testing should be done to ensure operability in different environments and scenarios, such as low-bandwidth variable networks [6] [7] [14].

Data integrity

The system should maintain security such that data can be only modified by the authorized person. In cloud-based environment, data integrity must be maintained correctly to avoid the data lost. Most of the web services face a lot of problems with the transaction management frequently as it uses HTTP services. HTTP service does not support transaction or guarantee delivery. It can be handled by implementing transaction management in the API itself [9].

Privacy

Consumer data must be protected from access by other consumers, as this could jeopardize its competitive advantages over other competitors. Safeguards are also needed to ensure that the provider will not use consumers "for unwanted purposes." When services are provided by providers in another country, there is a risk that an organization's data will be confiscated by the provider's authorities when the regulations in that country have been

breached. So, the consumer must trust the supplier to ensure a viable relationship of trust [14].

Denial of Service

Denial of service attacks can block customers' access to cloud resources. If such blockages last for a long time, customers' transactional processes can be seriously affected, interrupting the activity not only of the cloud provider, but also of all companies that rely on these services, thus causing large losses [6] [7].

Injection vulnerabilities

Cloud providers need to ensure that they do not have vulnerabilities in their services to SQL injection or OS injection, as such attacks can bring major problems to cloud customers [6].

Malicious insider

A malicious insider in the cloud provider can cause major damage to its customers. At the same time, in a cloud scenario, such an intruder can cover his tracks [6] [7].

Number of cyber-attacks in recent years

Large companies continue to experience cyber-attacks. With the increase in cloud usage, the number of attack attempts has also increased.

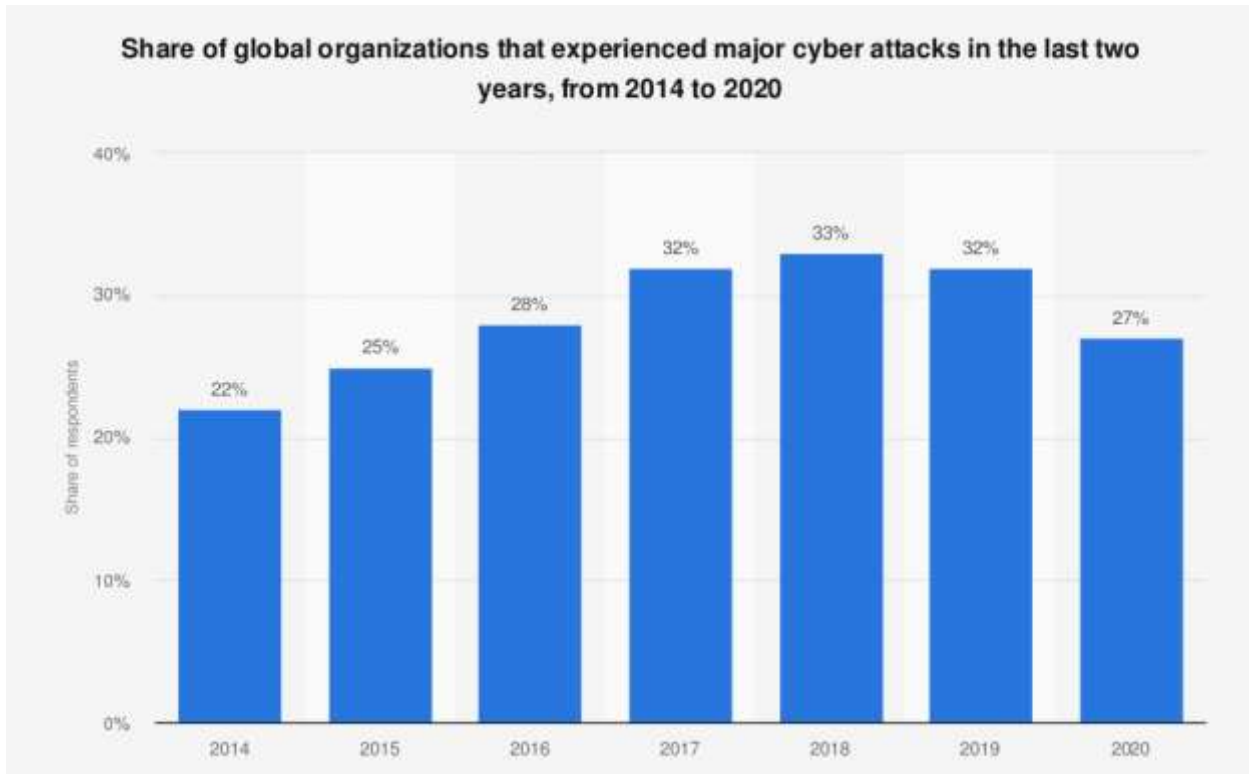


Fig. 6. Share of global organizations that experienced major cyber-attacks in the last two years, from 2014 to 2020 [16]

According to the latest statistics, the number of attacks has increased in recent years, until a maximum was reached in 2018, the last two years registering a lower number of incidents.

Opportunities for cloud and mobile devices

Due to the current pandemic context, more and more companies are looking for solutions to digitize their business. Thus, we are looking for solutions for network communication and solutions for accounting for the work of people at home. If so far, the cloud has not been of interest to some companies, the last few months have changed their perspectives, the cloud being an attractive option to meet the new requirements. Although security is still a hot topic of discussion, cloud technologies are mature, and the benefits of using the cloud are beginning to weigh more than its disadvantages. Thus, this period is a great opportunity for cloud providers to extend their services to more and more customers.

There are opportunities during this period for the development of the mobile devices market. They work well with cloud services and are easy to get. At the same time, the

flexibility they offer is a great advantage, because they can be used anywhere and anytime very easily.

6 Conclusions and future work

Due to the pandemic and the need for social distance, more and more aspects of society have been digitized. Remote work is increasingly in demand.

The cloud has a very important role in this regard, because small and medium-sized companies will turn to cloud services to adapt their business to the new context. Nowadays, communication and management in companies is done online, and the cloud through the benefits it brings is the perfect solution.

Security is still a sensitive issue and will continue to be so, but the maturity of the cloud and the need for digitization are encouraging more and more companies to migrate to it.

Given the growing interest of companies in the cloud, a future direction of research could be an analysis of the cloud services used by these companies and the benefits of these adoptions. It would be interesting to see if cloud services have significantly improved

the work processes of the companies that have chosen to transition to the cloud.

Acknowledgment

Parts of this research have been published in the Proceedings of the International Conference on Economics and Social Sciences [1].

References

- [1] A. V. Zaharia, "The role of the cloud for mobile solutions in crisis situations," in *International Conference on Economics and Social Sciences*, Bucharest, 2020.
- [2] C. Ceobanu and Ș. Boncu, "The Challenges of the Mobile Technology in the Young Adult Education," *Procedia - Social and Behavioral Sciences*, vol. 142, pp. 647 - 652, 2014.
- [3] K. E. Kushida, J. Murray and J. Zysman, "Diffusing the Cloud: Cloud Computing and Implications for Public Policy," *Journal of Industry, Competition and Trade*, vol. 11, no. 3, pp. 209 - 237, September 2011.
- [4] K. Akherfi, M. Gerndt and H. Harroud, "Mobile cloud computing for computation offloading: Issues and challenges," *Applied Computing and Informatics*, vol. 14, no. 1, pp. 1-16, 2018.
- [5] T. H. Noor, S. Zeadally, A. Alfazi and Q. Z. Sheng, "Mobile cloud computing: Challenges and future research directions," *Journal of Network and Computer Applications*, vol. 115, pp. 70-85, 2018.
- [6] G. Ramachandra, M. Iftikhar and F. A. Khan, "A Comprehensive Survey on Security in Cloud Computing," *Procedia Computer Science*, vol. 110, pp. 465-472, 2017.
- [7] N. Subramanian and A. Jeyaraj, "Recent security challenges in cloud computing," *Computers & Electrical Engineering*, vol. 71, pp. 28-42, October 2018.
- [8] P. R. Kumar, P. H. Raj and P. Jelciana, "Exploring Data Security Issues and Solutions in Cloud Computing," *Procedia Computer Science*, vol. 125, pp. 691-697, 2018.
- [9] R. V. Rao and K. Selvamani, "Data Security Challenges and Its Solutions in Cloud Computing," *Procedia Computer Science*, vol. 48, pp. 204-209, 2015.
- [10] Statista Research Department, "Smartphone Are the Bulk of Our Digital Media Diet," Statista Research Department, 12 June 2019. [Online]. Available: <https://www.statista.com/chart/18347/hours-spent-on-digital-media/>. [Accessed 26 January 2020].
- [11] "Distribution of global cloud and non-cloud mobile data traffic from 2014 to 2019," Statista Research Department, February 2015. [Online]. Available: <https://www.statista.com/statistics/292840/distribution-global-cloud-and-non-cloud-traffic/>. [Accessed 26 January 2020].
- [12] Statista, "Year-over-year change in average monthly in-home data usage by device in the United States from January to March 2020," 08 04 2020. [Online]. Available: <https://www.statista.com/statistics/1106821/covid-19-change-in-in-home-data-usage-in-us-2020/>.
- [13] Statista, "Interest in remote working and related search terms in Google in the past 30 days worldwide during the coronavirus (COVID-19) outbreak as of March 2020, by day," Statista, March 2020. [Online]. Available: <https://www.statista.com/statistics/1105696/remote-working-google-searches-worldwide-during-covid-19-outbreak/>. [Accessed 8 April 2020].
- [14] M. Mujinga and B. Chipangura, "Cloud computing concerns in developing economies," in *Australian Information Security Management Conference*, 2011.
- [15] National Institute of Statistics, "Population access to information and communication technology — Romania 2019," 12 October 2019. [Online]. Available: <https://insse.ro/cms/en/content/population-access-information-and-communication-technology-%E2%80%94-romania-2019>. [Accessed 16 November 2020].

- [16] Statista, "Share of global organizations that experienced major cyber-attacks in the last two years, from 2014 to 2020," September 2020. [Online]. Available: <https://www.statista.com/statistics/662937/worldwide-cio-survey-cyber-fears/>. [Accessed October 2020].



Alexis-Valentin ZAHARIA is a software developer enthusiast who graduated the Faculty of Cybernetics, Statistics and Economic Informatics, economic informatics specialization, in 2017. He holds a Master diploma in the research of Economic Informatics from 2019. Currently he is working as a Java software developer and is a PhD student at the Economic Informatics specialization. His current interests are in mobile technologies in the cloud computing environment.