IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 4, April 2022

DOI: 10.17148/IJARCCE.2022.11402

Potential Risk: Hosting Cloud Services Outside the Country

A.S. Hovan George[1], Dr. A. Shaji George[2]

Masters IT Solutions, Chennai, Tamil Nadu, India.[1,2]

Abstract: An object of the study is the potential risk of hosting the server outside of the country. The goal of this article is to define the risks and opportunities associated with the rapid development of cloud technologies and their penetration into almost all technological areas. The modern-day economy is evolving under the influence of information and communication technology. People are witnessing huge success in every sphere of management and economy with the use of Cloud Computing, Big Data, and Cyberphysical Systems. Modern life and work are shaped by cloud computing. It has become a part of the daily lives of people. Companies of all sizes have now turned to cloud computing for their business needs. Currently, everyone is talking about the cloud solution as a way to save money and increase the efficiency of resources. However, nothing is perfect, and this is no exception for cloud computing. The use of this technology is undoubtedly beneficial, however, there are some risks and concerns that should not be overlooked. The purpose of this article is to raise awareness about the ongoing war between Ukraine and Russia, how it impacts cloud technology when hosted outside of the country. Furthermore, this article will also look at how this war affects the IT industry if organizations depend on their operations and get support from outside countries, including hardware, software, network infrastructure, data centers, mobile device management, cloud computing, cyber security etc. Although cloud computing is developing rapidly, both conceptually and practically, legal, contractual, economic, service quality, interoperability, security, and privacy issues continue to pose significant challenges. The discussion focuses on critical challenges in cloud computing: regulatory, security, and privacy issues. A brief presentation on the future trends of cloud computing deployment is also presented, together with some solutions to mitigate these challenges.

Keywords: Cloud Computing, Bigdata, Blockchain, Cyber Security, Russia & Ukraine Cyber War, IT Army, DDos.

I. INTRODUCTION

Modern life and work are shaped by cloud computing. In fact, it has become an integral part of the daily lives of people around the world. Companies of all sizes have now turned to cloud computing for their business needs [1]. The adoption of cloud computing has been increasing rapidly in recent years due to a number of important advantages including cost savings, scalability, security, ease of deployment. Currently, everyone is talking about the cloud solution as a way to save money and increase the efficiency of resources. In the past few years, organizations have been actively migrating their infrastructure and applications to the cloud. In the field of remote work, managing critical business processes, and having access to key systems, cloud technologies play a crucial role in helping companies solve all of these challenges [2]. As companies migrate to cloud infrastructure, cloud security has become a high priority for a growing number of organisations as well as the government. While many businesses and governments are still cautious about cloud technologies, most do see the benefits and understand the strengths of cloud solutions. However, many organizations are still wary of taking the first step. To a certain extent, this may be correct, however, the cloud may not be the most suitable solution for every business or government. It depends on a set of conditions and circumstances [3]. The growth of cloud adoption also brings with it a number of challenges regarding privacy and security of data [4]. If Cloud technologies are implemented properly, used intelligently, and adopted in accordance with the correct cloud security principles, will help to drive and improve business performance. In the Government, Semi-Government and vital sectors, cloud services are usually classified as regulated approaches for data privacy and security, ever since data privacy and security has become a top concern among government bodies. A recent war illustrates the importance of choosing the location for hosting cloud solutions for businesses and governments. The new study discusses the attitudes of Russian companies towards cloud technologies and explores the main factors that prevent their adoption. In this article, the author mainly focuses on an important phenomenon the fear of the cloud and its underlying factors [4]. Due to this reason, establishing enhanced cybersecurity standards for cloud computing has become a top priority for businesses and nations around the globe, not just a need, but an essential social requirement as well. However, nothing is perfect, and this is no exception for cloud computing. The use of this technology is undoubtedly beneficial, however, there are some risks and concerns that should not be overlooked.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 4, April 2022

DOI: 10.17148/IJARCCE.2022.11402

II. OVERVIEW OF CLOUD DATA LOCALIZATION

Cloud Data localization is the method of maintaining data inside the region it came from. For instance, if the organization collects data in a country, they store it in the country instead of transferring it to a different country for further processing [6]. The Internet allows data to traverse the globe in milliseconds, so where that data goes and what is done with the data is of growing interest to regulators, privacy advocates, as well as consumers [7].

Cloud Data localization vs. Cloud data residency

Cloud Data localization and cloud data residency are two concepts that are occasionally used interchangeably, even if they have somewhat different meanings [6]. Independently, Cloud data residency means a place where Information (data)is stored. Cloud Data residency requirements could compel organizations in order to change the location where their data is stored [8]. Cloud Data localization is an action of observance of Cloud data residency requirements [6].

III.THE REQUIREMENTS OF CLOUD DATA LOCALIZATION

There are some legal norms that have cloud data residency requirements that require organizations to localize the cloud data [10]. Though, the majority of cloud data privacy frameworks do not require data localization [7]. But although jurisdictions might not require data localization by the law, heavily regulated industries such as banking as well as healthcare will be able to adopt best practice guidelines establishing more data requirements in order to be processed beyond their country of origin. In such cases, organizations might prefer to localize data instead of meeting these extra requirements. Many companies operating in regions with strict data-processing regulations can want to prevent possible violations entirely by maintaining data in those regions, even if this does not protect data any better.

IV.THE FUNCTION OF CLOUD DATA LOCALIZATION

Cloud Data localization is straightforward for organizations that rely upon one country or region and will use local infrastructure to store data [7]. If their data stays secure inside their data centers (DC), it needs to be properly localized. Cloud computing makes data localization more complex. Cloud servers are accessed through the internet and can be placed worldwide [8]. Organizations that depend on cloud computing have far less visibility into where their data are actually processed and stored, due to the fact that the cloud computing supplier is processing those decisions. Nevertheless, cloud data localization was made possible by cloud computing in the event that the cloud vendor commits to just managing and storing data inside data centers (DC) in the designated region. Not all cloud vendors have a sufficient global footprint to set it up, however many do. If a cloud vendor has the data center within the established region, then there are any number of ways in which they can secure a given customer's data stays in that data center (DC).

V. THE GOAL OF DATA LOCALIZATION

Most data localization laws apply for the creation and storage of personal data [5]. Since, People have a basic understanding of what data localization is, let us move on to some of the reasons why governments would put them in place. The primary objective of data localization is to:

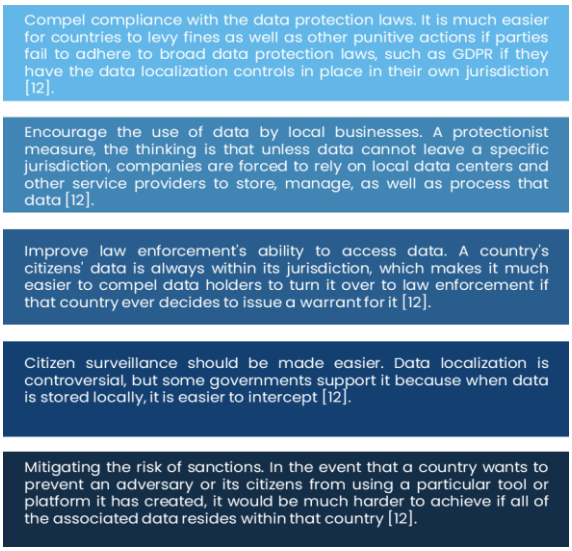

Fig -1: The Goal of Data Localization

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 4, April 2022

DOI: 10.17148/IJARCCE.2022.11402

Whether warranted or not, localization requirements are increasing and creating an enormous challenge for companies that want to remain compliant [5,6].

VI. TYPE OF CLOUD DATA LOCALIZATION

Cloud Data localisation refers to the practice of data storage on any device located within the boundaries of the country where the data is produced [13]. Currently, the vast majority of this data is stored in a cloud outside of country's [14]. Localisation decrees that companies gathering critical data regarding consumers need to store and process them within the boundaries of the relevant country. Many countries worldwide have implemented or in the process of implementing cloud data localisation laws to protect their own country's data and the privacy and data of their citizens.

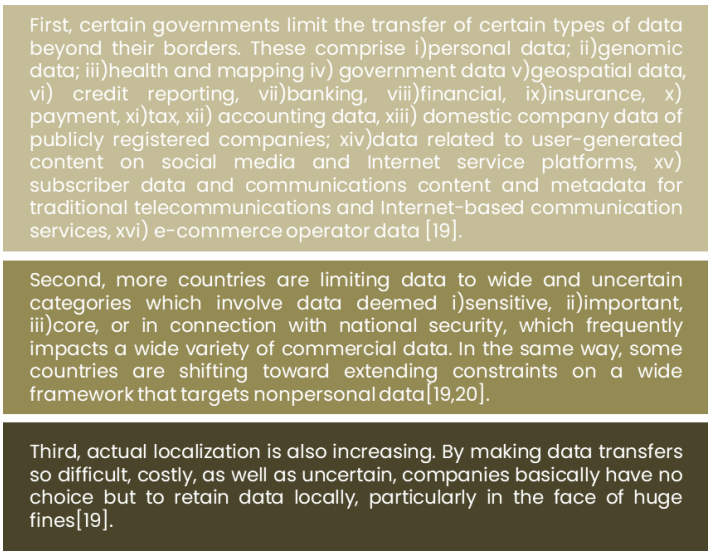

Fig -2: Types of Cloud Data Localization

VII. BENEFITS OF CLOUD DATA LOCALIZATION

- Cloud Data Localization will offer Law enforcement simple supervisory access. This helps law enforcement authorities efficiently investigate crimes and national security threats.
- Local governments and regulators are empowered to request data in case of disputes or fraud [16].
- Cloud Data localization guarantees the safety of citizens' data as well as provides data privacy protection and freedom from foreign surveillance.
- Cloud Data localization will guarantee more accountability from tech, particularly about the end-use of data gathered [17].
- Cloud Data warehousing is huge business, and it will help boost the data centre(DC) industry in the country and provide jobs.
- It will reduce conflict of authority due to cross-border data-sharing and guarantee the delivery of justice for cases that arise as a result of data violation and privacy suits.

VIII. ISSUES FACED BY THE CLOUD MARKET

Localization of Cloud data will be a hot topic in the coming years. Recently, many countries have expanded their enforcement of the cloud data localization law against the technology giants. Although this battle may be unique to the megalithic tech companies, how aggressively and in what manner the country plays its data privacy card may have inverse effects on future investments [20]. The fear of clouds, which is widespread throughout the world, is another factor. There are three major challenges associated with cloud migration, according to a recent study: the adaptation of cybersecurity controls, compliance with legal and regulatory requirements, and migration of IT systems to the cloud. Cloud services in all countries face the same issues many industries and regions have had when it comes to adopting the cloud. Even though the cloud offers vast advantages in cost optimization and scalability, basic cloud information remains elusive to the majority of people. Those who work for companies that utilize cloud technology either did not know how their company protected data in the cloud or were using it "as is" without additional cybersecurity protocols. Even worse are some of the concerns that people have regarding cloud computing. When asked about the most important risks involved with

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 4, April 2022

DOI: 10.17148/IJARCCE.2022.11402

cloud technologies, they believe accessing critical data by cloud provider staff indicates a deep mistrust of technology [20]. If so, many users do not trust the cloud, it could be a significant barrier to establishing country-wide cloud services. Even though many companies have been using the cloud, they may be reluctant to fully commit to using it. Whether the problem relates to global cloud services or country-specific cloud services is unclear, but service providers need to be transparent, otherwise, the confluence of country-specific data privacy and the general public's mentality could pose a barrier to growth and adoption.

IX. THE BEST PRACTICES FOR CLOUD SECURITY

There are six pillars to a security reference architecture that describe the minimum requirements required by organizations to place workloads securely in the cloud [18].

The best course of action is:	It should be done as follows:
Design and implement the basic security controls to create a secure landing zone in the cloud solution provider platform.	It is important to define the roles that are authorized to operate in the environment, what they are expected to do and what their responsibilities are.
Design re-usable cloud solutions provider secure PaaS templates with the integrated security controls.	Secure connectivity between on-premises data centers and utilize the "hub and spoke" model of network security
Platforms and services can be combined in order to bring together existing enterprise security tools for clients with operational processes and procedures.	Set up secure landing zone configuration policies and apply platform security controls to cloud service providers.

Table -1: Best Practices for Cloud Security

X. RUSSIA-UKRAINE CYBER CONFLICT: HOW CLOUD SERVICES ARE WEAPONS

Russia continues its invasion of Ukraine, and the Researchers have examined how cloud technology contributes to conflict at least in a virtual war [19]. When Russia invaded Ukraine, online action was triggered [19]. In the past, Ukraine has experienced numerous attacks resulting in defacement of websites, (DDoS) outages, as well as the use of destructive wiper malware. A group of anonymous hackers subsequently became engaged, and Ukraine's government sought volunteers with cybersecurity skills to help secure key infrastructure.

Ukrainian government officials have formed an IT army to defend Ukrainian networks and counter Russian threats. In the study, cloud technologies are now playing a part in the digital aspect of the conflict. There is a lot of code and tools that have been tracked by the team in public repositories, including code libraries, Docker images, as well as other software packages. In the search, they searched for guides, names, as well as tools that were promoted by either side to use in the cyberattacks. There was an effort to interfere with the network traffic of online services by utilizing these public repositories to carry out denial-of-service attacks. The team was particularly interested in the container images. Through DDoS tools that provide how-to guides, the audiences with no technical expertise are able to disrupt websites through cloud deployment. On the list of targets are financial institutions and providers of multiple services in Russia.

In addition, the container images also included attack tools that initiated DNS floods through the UDP protocol, sending a large number of DNS requests through UDP in port 53 and targeting Russian banks. Honeypots have been deployed to collect data regarding Russian and Ukrainian IP addresses. In general, network and media organizations were the most frequently attacked. The advancement of technology allows experienced threat actors to develop and distribute simple automated tools that allow individuals with limited technical expertise to participate in cyberwar. Additionally, it enables individuals and organized hacking groups to influence the conflict using their skills and resources. There is no doubt that emerging technologies are relevant to these efforts and can make a significant contribution.

XI. THE NEGATIVE IMPACT OF STOPPING SALES OF HARDWARE AND IT SUPPORT FROM THE WESTERN WORLD

The majority of companies and government agencies have relied on technology developed in the West for their own and operated IT systems for decades [22]. This includes servers, operating systems, applications, and tools. In general, these tools enable organizations to send emails, analyze data, store records, and generally manage their operations. Many of these technologies cannot be switched off remotely by vendors [22]. However, there are several ways to impede a client's

DOI: 10.17148/IJARCCE.2022.11402

system. As an example, local cloud service providers, banking, transport, telecom, and other organizations in the country may be hindered if vendors stop supplying replacement parts, security patches, software updates, and technical assistance. A halt in the supply of goods will have an adverse effect on everything. Consequently, clients may be forced to find other options, such as pen-and-paper bookkeeping, if the services go offline or degrade due to a lack of updates.

XII. CYBER WAR: THE RISK IN REMOTE MANAGED SERVICES AND CLOUD SERVICES

Managed services: Managed service operators manage services of an Organisation on their own behalf. This could include a) authentication services, b) application services, c) cloud services, d)backup services, e)desktop services, f)enterprise mobility services, g)gateway services, h)hosting services, i)network services, j)security services, k)support services, l)procurement services, and other commercial-associated services. By doing so, managed service providers can manage the services from their clients' facilities or their own premises. In taking into account the security risks related to the managed services, an organization should examine all managed service providers who have access to their systems, facilities, or data. These services may be put at risk in the event of a cyberwar.

Outsourced cloud services: Outsourcing may be a cost-efficient option for delivering cloud services, and also possibly providing a superior service. Though, outsourcing may affect an organization's security risk profile. An Organisation will still have to decide if a particular outsourced cloud-based service is equivalent to acceptable security risk and, if suitable, authorize it for its own use [5]. In the event of a cyberwar, these services may be at risk.

XIII. DATA LOCALIZATION WITHIN A COUNTRY

The country data localization law requires that at least a copy of all information about country citizens be stored locally within local data centers. With data localization and the center of country data privacy, the crucial consideration is that even though a copy or the original of the data must be held on local soil, you can trust the storage and processing of that restricted information to a third party within the country. As a result of the reality of those countries' data protection laws, local cloud services do hold a significant advantage in helping businesses store data within compliance. This is the primary reason why observers expect market growth to mainly come from national cloud providers rather than further expansion by global cloud providers.

XIV. DO DATA RESIDENCY REDUCES CLOUD RISKS

In order to protect private and classified data generated by their citizens, countries are establishing their own data residency regulations to mandate the storing of that information in that country the country of origin instead of outside of it [21]. This theory is based on the idea that the laws of the country in which the data is stored will apply to the data. Six aspects are involved in the life cycle of data. Following are the creation, use, storage, sharing, archiving as well as the destruction of the data. Data residency only deals with the aspect of storing data. Data residency requests will be based on concerns that data privacy laws may be less stringent in some jurisdictions [22]. In some jurisdictions, data residency has been adopted as a policy, however, there is some question as to whether it is effective. Is it more beneficial to store protected data in the country of origin or does the level of risk remain the same while the nature of the risk changes? Although storing data meets data residency requirements, data residency is not effective in protecting data if the owner of the cloud center, or the SaaS provider, has access and can send the data to be processed in a different jurisdiction [23]. Remember that Cloud computing is based on the layered service model that makes use of Cloud federation to achieve maximum functionality, reach, performance, and economy.

XV. THE RISE OF RISK FROM CLOUD COMPUTING

When cloud services are used, the control of data is automatically lost [12]. Even when the cloud service provider (CSP) encrypts data during both the transit and when it will be stored in the cloud, it could easily decrypt it too [12]. A crucial risk is a fact that government agencies or private organizations that use the courts could force the cloud service provider (CSP) to deliver your data or appropriate encryption keys. Many times, it may not even be known whether such a legal proceeding or court order was executed. This is termed Blind Subpoena. The problem becomes apparent when your data is being processed in various countries while it is residing in a particular country. If data resides in the data centers located in the country, it is possible to be able to count on legal protections which apply to the data.

XVI. CONCLUSIONS

Usage of the internet is becoming increasingly common as governments and business organizations move services on the internet to make processes more effective and to provide a wider reach. With the development of global enterprises and

DOI: 10.17148/IJARCCE.2022.11402

the growing digital economy, organizations must carefully review the application of cloud data localization as well as data transfer laws to their operations and those of their clients. Cloud computing certainly offers many advantages, and the future seems clearer too. Though, it also includes many risks and challenges for the enterprise. Therefore, it's important to know the problems which can come up if the organization or government intends to move the workload to the clouds. However, given its extensive reach of loose as well as light digital infrastructure, it represents a big threat to nations, and public as well as private businesses and individuals. The government must take accountability for tackling the nation's potential vulnerabilities. The biggest concern between the government and the organizations to shift their workloads or processes to the cloud is data security. Although security measures laid down in cloud computing have been evolving throughout the years, it is still a significant challenge. There are lessons to be learned from the Russian War for the rest of the world. The war demonstrated the risks associated with using the cloud. Therefore, all government and public sector organizations should be analysed before the Government and Organization transfer their data to the cloud. In today's world, cloud solutions are used more and more, making any nation susceptible to such a digital crisis. To deal with this, the government or organization must be prepared. In today's world, it is not surprising to see a digital crisis because it may happen at any time and to anyone. This research paper offers an overview of multiple threats, vulnerabilities, and the potential risk of cloud data, this is an article that can serve as a guide to policymakers in organizations to assess the security potential risk hosting cloud services outside the country.

REFERENCES

[1]. Sharma, Hemant. “Top 10 Advantages and Disadvantages of Cloud Computing [2022].” Intellipaat Blog, https://intellipaat.com/blog/tutorial/amazon-web-services-aws-tutorial/advantages-and-disadvantages-of-cloud-computing/.

[2]. Sokolova, Olga. "Russia In the Cloud: What Drives the Market?". Linxdatacenter.Com, 2020, https://www.linxdatacenter.com/press-room/news/novye-uslugi/russia-in-the-cloud-what-drives-the-market.

[3]. Dr. A. Shaji George, and A. S. Hovan George. DOI 10.17148/IJIREEICE.2021.9701 a Brief Overview of Vxlan...https://www.researchgate.net/profile/AShaji-george/publication/352999040_A_Brief_Overview_of_VXLAN_EVPN/links/60e369c2299bf1ea9ee516b1/A-Brief-Overview-of-VXLAN-EVPN.pdf.

[4]. DR.A. SHAJI GEORGE, and A.S. HOVAN GEORGE. “The Evolution of Content Delivery Network: How It Enhances Video Services, Streaming, Games, e-Commerce, and Advertising.” Http://Www.ijareeie.com/Volume-10-Issue-7, July 2021, http://www.ijareeie.com/upload/2021/july/40_The_NC.pdf.

[5]. Benjamin Vitaris. “What Is Data Localization? Meaning and Laws Explained.” Permission.io, 27 Oct. 2020, https://permission.io/blog/data-localization/.

[6]. Heather Devane. “Data Localization: A Complete Overview.” Immuta, 27 Jan. 2022, https://www.immuta.com/articles/data-localization/.

[7]. What is data localization? | data residency | cloudflare. (n.d.). Retrieved from https://www.cloudflare.com/learning/privacy/what-is-data-localization/

[8]. Review, B. S. (2021, August 18). Data localization: No panacea for cloud computing issues. Law School Policy Review & Kautilya Society. Retrieved from https://lawschoolpolicyreview.com/2021/08/18/data-localization-no-panacea-for-cloud-computing-issues/

[9]. Danielle Kaye, et al. “Explainer: Will Big Tech Cloud Companies Cut off Russia?” Reuters, Thomson Reuters, 8 Mar. 2022, https://www.reuters.com/technology/will-big-tech-cloud-companies-cut-off-russia-2022-03-08/.

[10]. Samuel Yang, AnJie Law Firm. “China: Data Localisation.” Lexology, Global Data Review, 28 Oct. 2021, https://www.lexology.com/library/detail.aspx?g=77c65f77-6292-46fd-ac3a-44ffe34aef92.

[11]. Information Security Manual - Cyber.gov.au. 10 Mar. 2022, https://www.cyber.gov.au/.

[12]. Puneet. “Microsoft Azure: Services.” Encryption Consulting | Encryption Consulting, 3 June 2021, https://encryptionconsulting.com/education-center/microsoft-azure-services/.

[13]. Nigel Cory, Luke Dascoli. “How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them.” How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them, Information Technology and Innovation Foundation, 19 July 2021, https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost.

[14]. “Data Localization – Advantages & Challenges.” Tides Academy |, 23 July 2019, https://tidesacademy.com/data-localization-advantages-challenges/.

[15]. A. Shaji George, and Bashiru Aremu. “User Revocation Using Advanced Key Generation in Cloud Architecture.” Science and Engineering Journal, Https://Www.researchgate.net/Publication/350353398_USER_REVOCATION_USING_ADVANCED_KEY_GENERATION_IN_CLOUD_ARCHITECTURE, 10 Mar. 2021, https://saejournal.com/volume-25-issue-3/.

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 4, April 2022

DOI: 10.17148/IJARCCE.2022.11402

[16]. Drishti IAS. "Data Localisation." Drishti IAS, 24 Nov. 2018, https://www.drishtiias.com/to-the-points/paper3/Data-Localisation.

[17]. "Data Privacy Rankings - Top 5 and Bottom 5 Countries - Privacy HQ." PrivacyHQ, https://privacyhq.com/news/world-data-privacy-rankings-countries/#_Toc66028355.

[18]. Daniel Mellen. "Secure Cloud." Accenture-The Importance of Cloud Security, 19 Jan. 2021, https://www.accenture.com/us-en/insights/security/secure-cloud.

[19]. Osborne, Charlie. "How Cloud Services Become Weapons in Russia-Ukraine Cyber Conflict." ZDNet, ZDNet, 15 Mar. 2022, https://www.zdnet.com/article/the-role-of-cloud-services-containers-in-the-russia-ukraine-cyber-conflict/.

[20]. Grieco, James. "Global Clouds and Cloud Providers in Russia." InCountry Global Clouds and Cloud Providers in Russia, 15 July 2021, https://incountry.com/blog/global-clouds-and-cloud-providers-in-russia/.

[21]. Aggan, Wael. "Does Data Residency Reduce Cloud Risks?" Cloudmask, https://www.cloudmask.com/blog/does-data-residency-reduce-cloud-risks.

[22]. Guseyva, Viktoriya. "Data Residency Laws by Country - Overview." InCountry, 17 Mar. 2022, https://incountry.com/blog/data-residency-laws-by-country-overview/.

[23]. Dr. A. Shaji George, and A. S. Hovan George. "Server Less Computing: The Next Stage in Cloud Computing's Evolution and an Empowerment of a New Generation of Developers." IJARESM, Apr. 2021, http://www.ijaresm.com/server-less-computing-the-next-stage-in-cloud-computing-s-evolution-and-an-empowerment-of-a-new-generation-of-developers.

