kriativ.tech

Edition No. 9 – 22-11-2021
ISSN Print: 1646-9976 | ISSN Online: 2184-223X |
http://www.kriativ-tech.com
DOI: 10.31112/kriativ-tech-2021-10-63

Security and Privacy in Cloud Computing: Simple Checklist to Virtualization

Dulce Mourato
Assistant Professor at ISTEC
dulce.mourato@my.istec.pt

Abstract: *With the COVID-19 Pandemic, Portuguese enterprises discover the crucial opportunity to make the difference worldwide with virtualization, using Cloud Computing technologies, however they are yet not fully convinced. Cloud security and privacy seems to be the main problems for organizations early adoption. It was possible to use a descriptive methodology, and an literature review approach to differentiate solutions, build on a simple checklist format and reveal essential arguments, that any small and medium-sized Portuguese company should take into account, before purchasing Cloud technologies adapted to its potential growth.*
One of the major limitations of this study, was the inability to point out at real business environment, only using observation and scientific, technological and specialized level studies, presented here as potential result. The goal was verify if the applications or services implementation for protection and security scalability - really works.

Keywords: *Security, Privacy, Cloud Computing, Virtualization, Checklist.*

I. Introduction

COVID-19 Pandemic brings new business opportunities and branches security challenges to all technologies and Cloud Computing was no exception. It seems that lack of regulations and legal uncertainty, un-authorized access by third parties, absence of control mechanisms for users, cross-border data and others vulnerabilities, still bring many doubts to Portuguese small and medium enterprises (SMEs). How safe and secure, how could Cloud Computing ensures the integrity and confidentiality of secured data, and what about storing data or service providers - can it be reliable?

Issues of lack of security and privacy were the decisive arguments of some Portuguese companies, more resistant to change, for non-technological integration in the Cloud, despite all the inherent advantages of the potential business virtualization. The objective of this study is clarify how to manage cloud transition with a scientific, technological and specialized literature review and create a simple Checklist, that synthetize, enumerate and could evaluate the results of pre and post Cloud Computing adoption.

IDC Portugal Digital Event [1] made predictions until 2024 about four majors areas that must have a massive upgrade worldwide in business (Acceleration, Repair, Extension and Ecosystem Transition). All of them are related to Cloud Computing, Machine Learning and Artificial Intelligence (AI). IDC Portugal [1] explain: “By 2022, 70% of companies will integrate cloud management – in their public and private clouds – by implementing unified multi-cloud technologies, tools and processes. By 2023, more than half of the new corporate IT infrastructures deployed will be on the ‘edge’ rather than the datacenter. What will cause the weight of infrastructure investment in the ‘edge’ to increase from the current 10% to more than 50% in 2023. In 2024, 50% of

companies will use AI for intelligent automation of the selection and contracting process with suppliers". IDC Portugal [1] claims also that more than 62% national organizations, follow recent trends of cloud adoption until 2021, however security seems to be the most fragile argument to get more followers and adopters.

II. Literature Review

Cloud services providers must deliver the answers to lack of security and privacy like IT team holistic skills for cloud architecture to better plan, design, develop, migrate and operate applications between environments and on-premises platforms in terms of cloud interoperability, compliance and complexity. How to make this happen? Manage information systems remotely and cost-effectively and access to remote cluster of servers using protection as a flag or look at complex nature of the cloud system and draw a simple path?

Aristova, Daradkeh & Korolev [2] claims "the urgent need for the development of techniques and tools for cybersecurity of clouds is noted. Among the authors of the articles are noted groups Ali, Zhang, Lee, Li; Fowley, Chen, Islam, and Sha; Chi, Luna, Awad, Cafaro, Zhang, and Xu are well known in the professional community. The various cybersecurity techniques and tools described by these research and development teams are described".

Zissis and Lekkas [3] categorize the security cloud issues into five classes as follows: data control, account control, multi-tenancy, malicious insiders and management console security.

Bhandari and Zheng [4] define 12 cloud security threats, such as data breach, insufficient identity, credential and access management, insecure interface and APIs, system vulnerabilities, account hijacking, malicious insiders, advance persistent threats, data loss, insufficient due diligence, abuse and nefarious use of cloud services, denial of services, and shared technologies issues.

Gonzalez et al. [5] suggest three groups as follow: cloud architecture security (security of networks, virtualization and interfaces); data privacy (security of data itself and the legal issues) and finally compliance (responsibilities of each party and the applied policies).

Alqahtani [6] specify that "there is a critical need to develop comprehensive and critical studies with a clear methodology that contribute to knowledge and provide a clear understanding of cloud computing security challenges. Further, there is a need to develop more studies that propose solutions/approaches for the identified security issues". Alqahtani [4] particularize that "consequently, cloud computing access control security issues and cloud computing computation and storage security issues must gain more attention from researchers and developers in both academic and industrial fields. The authentication, applied cryptographic system and storage data issues have the largest share of the identified security issues" that why Alqahtani [6] explain the importance of 16 Identified cloud computing security issues taxonomy:

- Software that include Platform (safe termination, isolation, accounting) and Frontend (open source, un-authorised access, un-guaranteed delivery, direct internet connection, VMM, Masked-code injection);
- Virtualization that contain Availability (DoS) and Management (large-encrypted image, image thieving, image access, virtual machine monitor, virtual network, sprawl, escape attack & zero-day) and Mobility (VM cloning, VM mobility) and Malware (malware-injection, roll-back function, side-channel and convert-channel attacks);
- Internet that englobes Protocols (network-based cross tenant attacks, combining HTTP, HTTPS, HTTP, HTTPS over PaaS) and Web Services (XML wrapping attack, scanning, spoofing attack) and Web Technologies (unauthenticated session management) and Connectivity (Flood attacks, DoS attacks, Bandwidth under-provision);
- Trust that combine Auditability (monitoring, third part) and Human Factor (social engineering, password attack);
- Access that integrate Physical Access (unauthenticated access, malicious attacks) and Authentication (password attack, account lock out, identity management);
- Computation and Storage that hold Data Storage (geographical distribution, loss control) and Cryptography (insecure cryptography,

algorithm failure) and Malware (syncing via data) and Sanitization (cloud recycling).

There are lots of vulnerabilities and threats amplify by clouds' infrastructure, more digital assets and proliferation of mobile access devices. Security is now connected to the crucial need of confidentiality, integrity and availability present as data, software and hardware. As resources sharing, computation outsourcing and external data warehousing increases, more accurate turns the security and privacy concerns in order to create new security challenges.

Another research Ray [7] describe other paradigm with four features and several factors that could be pursuit by enterprises in their implementation:

- Cost Adoption (Migration and Acquisition Cost, Customization, Uncertainty, Cost of Data Confidentiality and Availability Loss);
- Technical (Complexity of Current Systems, Compatibility with Current Systems, Scalability, Availability and Accessibility, Security);
- Organizational (Top Management Support, Firm Size, Skill of IT Resources, Employee Buy-in, Innovative Culture);
- Environmental (Industry Adoption, Competitor Pressure, Regulatory Concerns, Vendor Expertise/ Availability).

The insight of Nagahawatta, Warren, Lokuge and Salzman [8] made in a 2021 study, shows the importance of giving answers to refine cybersecurity strategies to address the growing sophistication of post-COVID cyber-attacks on individual and corporate cyberspace assets. Nagahawatta et al. [8] tried to elucidates "the knowledge gap in the relationship between security-related factors and the adoption of cloud computing from a social and technical perspective. Security concerns are major barriers to adoption. Studies have focused on barriers to cloud computing adoption by SMEs worldwide, yet little is known about cloud computing adoption by SMEs".

Like those authors (Nagahawatta et al. [8]) also in Gartner Group Website [9] the results of CIO survey claim "growth rate of spending on information security and risk management technology would grow 12% to $150.4 billion in 2021 showcasing continuing demand for remote worker technologies and cloud computing security issues". Gartner Group [9] also highlight security and regulatory demands of public cloud and software as a service, early market signals of growing automation and further adoption of machine learning technologies in support of AI security as top activities provide by organizations that will extend and standardize threat detection to combat all kind of attacks.

"Organizations continue to grapple with the security and regulatory demands of public cloud and software as a service," explain Lawrence Pingree, managing research vice president at Gartner Group [9]. "Looking ahead, we're seeing early market signals of growing automation and further adoption of machine learning technologies in support of AI security. To combat attacks, organizations will extend and standardize threat detection and response activities."

As Brandão and Martins [10] says about Cybersecurity - Risks of Telework in Kriativ-Tech "security is never finalized. We can never give the topic closed, as cybercriminals will also always be innovative and adaptable to new trends and technological innovations. Most of all, a computer literacy training plan is created for all those involved in the entire process and manipulate employees for the disclosure of privileged and confidential data".

III. Clarification and Application

On fundamental level or at large Web Worldwide scale, cloud computing security is a never-ending goal. Misunderstandings based in shared responsibility connection between cloud providers and cloud users, external support, level of security as well as expertise and technical holistic perspective are some of the key points followed in Checklist design.

Each item of the Checklist must respect the business goals, define if there are any security threats in virtualization, different from others information systems or ethics issues and why this happen. Verify if the potential technology choice is accurate, secure, safe and really depends of the way security contents are addressed for the users or final clients.

In first phase it was possible compile a small amount of information about how could enterprises find and manage security and privacy stepstone and use a framework quality control, that

should be used to measure the degree of achievement before and after virtualization in order to saving money and accomplish the main objectives.

In second phase it was possible verify as Dalmazo [11] mention, how computing power dynamically could provide on demands organization needs, verifying how powerful and ubiquitously available resources and software hosted in remote locations in Web-scale storages could really be used. Cloud computing seems to be a kind of Customer Relationship Management (CRM) practical options: distributed for many users as well as more possibilities to grow.

Actual organizations landscape overview in third phase, prove that Cloud security and privacy must cover at same time proper cloud migration to get more resilience, scalability and cost-efficiency in ecologic terms. In fact, according to Aristova, Daradkeh & Korolev [2] to proceed to virtualization, several problems arise: protect people and information based in a Security Policy for Cloud Computing Services, specially customized to each case; set rules for expected behavior followed by users, minimizing risks, avoid threats and help to track compliance with regulation in addition to unauthorized access to information, that can jeopardize data and make an disruption in the most elementary principles of information security.

Based on literature review presented above, one suitable way to evaluate security issues, to detect possible security or performance problems, fitting the most adequate security strategy as well as congregate several authors frameworks, that could be used in small or medium enterprises, as possible business turning point it was possible elaborate a simple checklist guidelines:

- Verify if there are skilled personnel ready to action (both at providers' mode or local employees) to pay attention to security issues;
- Cloud computing is the natural technology in terms of cost acquisition and efficiency, availability and accessibility, scalability relevance and care for business evolution and people training;
- Perceived security benefits, data security and data privacy concerns, regarding cost of data confidentiality and availability Loss;
- Portuguese SMEs agree with legal compliance, cloud security standards and trust in Cloud Services Providers (CSP);
- Cloud computing security and privacy trends customization, specially adopted to Portugal social and cultural environment.

Critical times post pandemic COVID-19, require unexpected measures, more than improving the way Portuguese companies do business, it is possible with a simple checklist generalize the implementation of cloud computing networking, increase agility and speed of data transfer, concerning security and privacy besides storage costs. Supply and demand market reveals cost reduction that could stimulate more small and medium enterprises to make the ultimate migration, moving workloads from on premises to the cloud to develop and achieve more easily their business objectives.

IV. Conclusion

Keeping in mind that is urgent simplify and answer to particular advices or to global trend for SMEs, that want to migrate to the Cloud, with security and privacy concerns, this study was made a checklist proposal, with some items to take into account for the use of all the Cloud Computing full potential (heterogeneous architectures, multiple clouds and on-premises platforms).

This checklist could indicate how to choose the service and the providers: Amazon, Alibaba, Cisco, Google, IBM, Microsoft, Oracle, VMware and others players plan distributing a puzzling assortment of Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Desktop as a Service (DaaS) an On-premisses possibilities to support organizations in developing and running their services, increase performance and found better dynamic and adaptable solutions in various aspects and situations.

The limitations of this research instrument are grounded on theoretical proposals and literature review frameworks, instead of real world based. Some themes like disaster recovery and value proposition are forgotten Maybe, future studies could prove that this simple Checklist could be feasibility and tested in the field, decreasing the needed (at first view) of technical specialized experience, reducing the operational complexity, and

improve the flexibility of the delivered service.

.

V. References

[1] IDC Portugal. Future Enterprise: Building Resiliency and Agility to Thrive in the Next Normal. IDC Futur Scape Portugal - Digital Event. Lisboa, 2021. https://idcportugal.com/solucoes/eventos/ [Accessed 2 11 2021].

[2] Aristova, S., Daradkeh Y. I. & Korolev, P. A General Systems Approach to Cloud Computing Security Issues. Intechopen, 2020. p. 4. https://www.intechopen.com/chapters/71961 [Accessed 2 11 2021].

[3] Zissis, D. and Lekkas, D. Addressing cloud computing security issues. Future Generation Computer Systems., pp. 583-592.,2012.http://www.sciencedirect.com/science/article/pii/S0167739X10002554http://dx.doi.org/10.1016/j.future.2010.12.006 [Accessed 2 11 2021].

[4] Bhandari B, Zheng J. A Preliminary Study On Emerging Cloud Computing Security Challenges., ACM, 2018. https://arxiv.org/pdf/1808.04143.pdf [Accessed 2 11 2021]

[5] Gonzalez, N., Miers, C., Redígolo, F., Simplício, M., Carvalho, T., Näslund, M. and PourzandI, M. A quantitative analysis of current security concerns and solutions for cloud computing., Journal of Cloud Computing,, pp. 1-18., 2012. https://journalofcloudcomputing.springeropen.com/articles/10.1186/2192-113X-1-11 [Accessed 2 11 2021]

[6] Alqahtani, H. A novel approach to providing secure data storage using multi cloud computing. University of Bedfordshire., London. England., 2019. [Accessed 2 10 2021]

[7] Ray, D. Cloud Adoption Decisions: Benefitting from an Integrated Perspective. The Electronic Journal Information Systems Evaluation. 2016. 19 (1), 3-21. https://academic-publishing.org/index.php/ejise/article/view/168 [Accessed 2 10 2021]

[8} Nagahawatta, R.; Warren, M.; Salzman S. and Lokuge S. Security and Privacy Factors Influencing the Adoption of Cloud Computing in Australian SMEs. PACIS 2021 Proceedings. 7., 2021.

[9] Gartner Group. Gartner Top Strategic Technology Trends for 2022. 20 10 2021. [Online]. Available: https://www.gartner.com/en/information-technology/insights/top-technology-trends. [Accessed 2 11 2021].

[10] Brandao, P. R. and Martins M. CyberSecurity - Risks of Telework. Kriativ-Tech, no. 9, p. 4, 26 October 2021. http://www.kriativ-tech.com/?p=66388

[11] Dalmazo, B. A Prediction-based Approach for Anomaly Detection in the Cloud, Coimbra: PhD Thesis, Department of Informatics Engineering Faculty of Sciences and Technology University of Coimbra, 2018. https://eg.uc.pt/bitstream/10316/81235/1/A%20Prediction-based%20Approach%20for%20Anomaly%20Detection%20in%20the%20Cloud.pdf