Secure Cloud Migration Strategy (SCMS): A Safe Journey to the Cloud

Dalal N. Alharthi
University of Arizona, Tucson, AZ, United States

dalharthi@arizona.edu

Abstract: The state of cloud security is evolving. Many organizations are migrating their on-premises data centers to cloud networks at a rapid pace due to the benefits like cost-effectiveness, scalability, reliability, and flexibility. Yet, cloud environments also raise certain security concerns that may hinder their adoption. Cloud security threats may include data breaches/leaks, data loss, access management, insecure APIs, and misconfigured cloud storage. The security challenges associated with cloud computing have been widely studied in previous literature and different research groups. This paper conducted a systematic literature review and examined the research studies published between 2010 and 2023 within popular digital libraries. The paper then proposes a comprehensive Secure Cloud Migration Strategy (SCMS) that organizations can adopt to secure their cloud environment. The proposed SCMS consists of three main repeatable phases/processes, which are preparation; readiness and adoption; and testing. Among these phases, the author addresses tasks/projects from the different perspectives of the three cybersecurity teams, which are the blue team (defenders), the red team (attackers), and the yellow team (developers). This can be used by the Cloud Center of Excellence (CCoE) as a checklist that covers defending the cloud; attacking and abusing the cloud; and applying the security shift left concepts. In addition to that, the paper addresses the necessary cloud security documents/runbooks that should be developed and automated such as incident response runbook, disaster recovery planning, risk assessment methodology, and cloud security controls. Future research venues and open cloud security problems/issues were addressed throughout the paper. The ultimate goal is to support the development of a proper security system to an efficient cloud computing system to help harden organizations' cloud infrastructures and increase the cloud security awareness level, which is significant to national security. Furthermore, practitioners and researchers can use the proposed solutions to replicate and/or extend the proposed work.

Keywords: Cloud Migration, Cloud Transformation, Cloud Security, Cloud Strategy, Attacking Public Cloud, Defending Public Cloud

1. Introduction

Cloud solutions provide a powerful computing platform that enables organizations to migrate their on-premises applications and storage space as easy, flexible, and cost-effective solutions/services over the internet. Yet, cloud environments also raise certain security concerns that may hinder their adoption. Virtualization, storage, and networks, as mentioned by Ouda et al (2022), are the most serious security concerns in cloud computing. Hence, awareness of the latest innovations in cloud security technologies is necessary in order to mitigate the risks of these security challenges and provide security solutions to remain competitive (Hassan et al, 2019). Several research efforts have been made in evaluating challenges related to security faced by cloud computing environments, and a number of solutions to such problems have also been proposed. Despite the research efforts in the cloud security field, there are still some open research problems and challenges which are discussed in this paper.

As addressed by Ahmad et al (2020), migration to cloud environments needs careful planning, strong business case, credible migration strategy, and robust migration frameworks. Hence, this paper aims to develop a Secure Cloud Migration Strategy (SCMS). The proposed strategy addresses cloud migration phases, which are 1) preparation; 2) readiness and adoption; and 3) testing. Among these phases, cloud security tasks/projects are illustrated from the different perspectives of cloud defenders, attackers, and developers. Adopting the proposed SCMS may enable both academia and practitioners in the cloud computing community to get an overarching view of the strategy of the legacy application migration to public cloud environments in a secure manner. Additionally, the author addresses cloud security documents/runbooks that need to be developed, such as incident response runbook, disaster recovery planning, risk assessment methodology, and cloud security controls. Furthermore, the paper identifies some necessary cloud security challenges that have not yet been addressed by existing approaches, developing opportunities for further research endeavors.

The main contribution of this study can be summarized as follows:

- The paper summarizes current research efforts related to securing the cloud migration journey.

- The paper categorizes tasks/projects to secure the cloud migration journey from the different perspectives of defenders, attackers, and developers.
- The paper addresses cloud security documents/runbooks that organizations may develop and automate to secure the cloud migration journey.

The remainder of this paper is structured as follows. Section 2 provides the necessary background information on cloud providers in addition to the multi-cloud migration approach. Section 3 presents the related research efforts on cloud security. Section 4 addresses the research questions this paper aims to answer and describes the author's methodology for developing the strategy and identifying cloud security documents/runbooks. The proposed Secure Cloud Migration (SCM) Strategy is presented and illustrated in Section 5. Then, Section 6 highlights the documents/runbooks that organizations may develop and automate when migrating to the cloud. Section 7 addresses threats to the validity of the proposed solutions. The paper's conclusion and future work are mentioned in section 8.

2. Background

This section provides an overview of the big three cloud providers that organizations consider migrating to, which are Amazon Web Service (AWS), Microsoft Azure, and Google Cloud Platform (GCP). Additionally, it sheds some light on the multi-cloud approach.

AWS is the first-to-market launching in 2006. It has over 200 services as of February 2023. It is considered by many organizations to be the default choice for cloud migration due to its feature set, reliability, and growth. Azure is also gaining on AWS quickly due to its competitive pricing model. It has proven itself to be a viable alternative. Although GCP lags far behind them both, it too has grown significantly in market share. GCP is also a patron of open-source technology such as Kubernetes and TensorFlow. It also acquired some popular cloud platforms including Firebase and Stackdriver.

These large-scale cloud providers allow organizations to pay for whatever resources they need, enabling customers to increase or decrease the number of resources requested as needed. Yet, the traditional use of cloud services focused on the consumption of one provider is not valid anymore due to different shortcomings being the risk of vendor lock-in a critical (Alonso et al, 2023). Hence, the use of multiple cloud providers simultaneously is increasing to achieve higher service availability and reduce damage in the case of malicious insiders on a single Cloud Service Provider (CSP) (AlZain et al, 2012). Therefore, many organizations prefer to migrate their on-premises environments to a multi-cloud approach to leverage the best of all cloud worlds. Forrester surveyed 727 cloud decision-makers globally and found that 86% of respondents identified themselves as "multi-cloud" (McLellan, 2019). Multi-cloud can be defined as utilizing numerous cloud networks and services simultaneously (Hong et al, 2019). While migrating to a multi-cloud environment can help develop a more effective disaster recovery plan, it can also produce some challenges for cloud security professionals. As addressed by Kavitha and Radha (2022), a multi-cloud environment has the possibility of greater challenges for service quality, security, and privacy attacks.

3. Literature Review

In the existing literature, an increasing amount of research works addressed the security issues in cloud computing to find efficient security solutions. On the other hand, different research groups have studied and published cloud migration security mechanisms. Gonzalez et al (2012) addressed the most remarkable ones named NIST (National Institute of Standards and Technology), CSA (Cloud Security Alliance), and ENISA (European Network and Information Security Agency). This section focuses on the related research efforts in light of this research.

Cloud computing, a new paradigm of flexible and cost-effective computing, is being explored as a possible solution to make enterprise IT sustainable. In that context, Ahmad, Naveed, and Hoda (2018) highlighted some of the procedures for cloud migration planning and execution, such as architecture recovery, dependency checks, provisioning, pilot migration, data migration, application migration, integration, and validations. Among these procedures, there are key processes concepts, as addressed by Fahmideh et al (2019), that need to be incorporated into a typical process of legacy system migration to the cloud including the following: analyze migration requirements, define a plan, recover legacy system knowledge, choose cloud platform/provider, design cloud solution, identify incompatibilities, make system stateless, decouple system components, replicate system components, make mock migration, use logging, resolve licensing issues, develop integrators, deploy

system component, enable elasticity, encrypt the database, handle transient faults, isolate tenant, encrypt/decrypt messages, obfuscate codes, reconfigure the network, synchronize/replicate system components, communicate a-synchronous, and test system.

Due to its dynamic abstraction and scalability, applications and data outsourced to the cloud have unlimited security boundaries and infrastructure. Another primary security concern surrounding the adoption of cloud computing is its multi-tenancy nature and sharing of virtualized resources (Abdulsalam and Hedabou, 2022). To secure the systems migration to the cloud environments, it is vital to be aware of crucial aspects of security. El Kafhali, El Mir, and Hanini (2022) and Masadeh, AlShrouf, and Kumar (2023) identified some of these security challenges and issues such as the lack of control over the Cloud Datacenters, weak integration of security into the service development process, data breaches, data leakage/loss, account or service traffic hijacking, insecure interfaces/APIs, Denial of Service (DoS), malicious insiders, insufficient due diligence, shared technology vulnerabilities, loss of governance, lock-in, insecure or incomplete data deletion, and the availability chain.

4. Research Questions and Methodology

This section describes the research questions this research aims to answer, followed by the research methodology to develop the strategy and identify cloud security documents/runbooks.

- RQ1: What are the main phases of migrating on-premises applications and services to the cloud?
- RQ2: What are the key tasks/projects to secure the cloud migration journey from the different perspectives of defenders, attackers, and developers?
- RQ3: What are the necessary cloud security documents/runbooks that organizations may develop and automate to secure the cloud migration journey?

To answer these questions, the author followed a Systematic Literature Review (SLR) technique as recommended by Okoli and Schabram (2010). The study conducted a literature review of the most recent journal and conference papers that contained the following keywords and strings in their titles “Cloud Migration”, “Cloud Security”, and/or “Cloud Strategy”. For each paper, the author extracted security challenges from both offensive and defensive security perspectives. This SLR examined the research studies published between 2010 and 2023 within popular digital libraries such as IEEE Xplore, Springer, ACM, Google Scholars, and Science Direct. These digital libraries are the primary source of publications on topics from both computer science and cybersecurity domains.

5. Secure Cloud Migration Strategy (SCMS)

By investigating the existing literature, the author classifies the Secure Cloud Migration Strategy (SCMS) into three main repeatable phases/processes for iterative cloud transformation, which are 1) Preparation; 2) Readiness and Adoption; and 3) Testing. Among these processes, proposed cloud security projects are addressed from the different perspectives of defenders, attackers, and developers. More details on the proposed SCMS are addressed below and illustrated in Figure 1.

5.1 Preparation

This phase includes tasks such as building the Cloud Center of Excellence (CCoE), designing the migration architecture, and developing the RACI Chart. Building the CCoE can be one of the first steps in the cloud migration journey. This should include the following teams: Infrastructure, Cloud Security, Developers, Contractors, and anyone who is working on the cloud migration project. Another task to be completed in this phase is developing the Cloud Migration Architecture, which should take into consideration Business Units, Core Accounts, Firewalls, and the Transit Gateway and/or VPC Peering. Moreover, the team should invest in building the cloud migration RACI Chart. The acronym RACI stands for responsible, accountable, consulted, and informed. It is, as described by Araújo (2021), a clear matrix chart used to attribute responsibilities and duties per each job or decision in a project by all of the team members.

5.2 Readiness and Adoption

In this phase, both defenders (blue team) and developers (yellow team) may work together to ensure the security of the cloud environment. Here are more details on what tasks/projects can be included in this phase. From the defenders’ perspectives, projects/tasks may start with preparing the security toolkits such as firewalls, Single Sign On (SSO), password management, antivirus, SIEM solution, vulnerability assessment, and compliance

tools. Integrating these tools is essential i.e., the vulnerability assessment tool may be integrated with the compliance tool to provide a better understanding of the current compliance status of the cloud environment. Other tasks/projects may include Identity and Access Management (IAM), least privileges determination, access control, secret management, data encryption, network security, defense-in-depth, continuous monitoring, and cloud compliance to the relevant industry standards and regulations. From the developers' perspective, it is vital to adopt the Security Shift Left concept to shift security to be in the early stages of the Continuous Integration and Continuous Deployment (CICD) pipeline of the software development cycle. Gonzalez, Perez, and Mirakhorli (2021) highlighted seven pain points that developers may experience as they learn to adapt their existing skills to the security tests, which are mocking security components, interacting with security services/APIs, creating security fixtures, bypassing access controls for protected resources, designing authentication flows, creating HTTP request objects, and configuring systems for test environments.

5.3 Testing

Ease of using the cloud may cause security flaws and due to this reason, security issues of cloud computing should be examined in-depth (Yurtseven and Bagriyanik, 2020). Therefore, security testing is fundamental to identifying existing security issues and is particularly powerful when carried out by means of penetration testing (pentesting) and vulnerability assessment techniques. Casola et al (2018) proposed a methodology that allows easy carrying out of a coarse-grained security evaluation of a cloud application by automating the set-up and execution of penetration tests. The methodology relies on the knowledge of the application architecture and on the availability of a catalog including security-related data collected from multiple sources and properly correlated. The methodology started with the preparation phase in which a risk assessment should be conducted, followed by the scanning phase to identify weaknesses and vulnerabilities, then the pentesting phase to configure and execute the attack. The tasks/projects identified here are the responsibility of the red team.

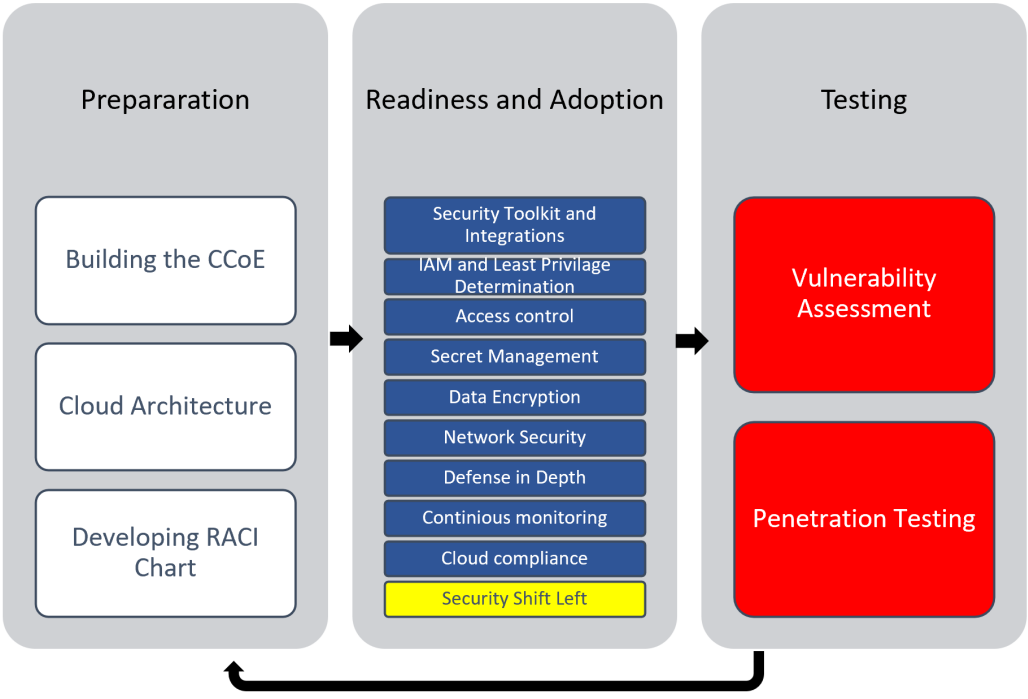

Figure 1: The proposed Secure Cloud Migration Strategy (SCMS)

6. Secure Cloud Migration Documents/Runbooks

Among the three phases addressed by the SCMS in Section 6, it is essential to develop and automate cloud security documents/runbooks to ensure a secure journey to cloud transformation. This section addresses some of these documents/runbooks, such as the Incident Response (IR) Runbook, Risk Assessment Methodology, Disaster Recovery Planning, and Cloud Security Controls.

6.1 The Incident Response (IR) Runbook

This should consider incident response steps addressed by Grobauer and Schreck (2010), which include containment, eradication, and recovery. Upon developing the document, it should be tested and automated. The IR Runbook may also contain the contact information of the teams who will be responsible for responding to cloud security incidents. Additionally, different cyberattack scenarios should be illustrated, and the appropriate response to each of the scenarios shall be addressed in detail. NIST outlined these response steps in (Cichonski et al, 2012) to be gathering evidence; containing and then eradicating the incident; recovering from the incident; and conducting post-incident activities, including post-mortem and feedback processes.

6.2 Disaster Recovery Planning

As the name implies, this document shall contain a recovery plan in place in case of data loss or breaches. The primary concern for this document is finding ways to ensure that the process of data backup and recovery is effective in providing high data availability, flexibility, and reliability at a reasonable cost. As addressed by Alshammari et al (2017), the majority of providers of cloud services enable their customers to rapidly recover from disasters with a minimum of disruption via the use of a geographically distributed data backup and redundancy model.

6.3 Risk Assessment Methodology

This document shall identify potential security risks and data privacy issues associated with migrating to the cloud. According to Ali et al (2020), unique elements of risk assessment in cloud computing may relate to the operational security and monitoring of cloud services. Security assessments are important mechanisms for risk mitigation from cloud security breaches.

6.4 Cloud Security Controls

This document can serve as guidance for developers to address cloud security controls that should be taken into consideration when migrating on-premises applications/services to the cloud. Developing this document may help the implementation of SecDevOps, which has recently appeared in the researchers and developers communities, but the management of security in a DevOps life cycle is not a straightforward task. Hence, adopting Security-by-Design through developing and implementing the Cloud Security Controls document is vital. The Security-by-Design approach, as defined by Casola et al (2020) and Santos, Tarrit, and Mirakhorli (2017), is designing the software from the foundation to be secure. At this aim, the alternate security tactics and patterns are first thought and, among them, the best are selected and enforced by the application designer, and then used as guiding principles for developers.

7. Threats to Validity

This section discusses the threats to the validity of the proposed solutions and the author's steps to minimize those threats. To develop the SCMS and the associated tasks/projects to secure cloud transformation in addition to identifying cloud security documents/runbooks, the author mainly relied on a comprehensive literature review. As with any such review, some significant references could have gone unnoticed. To minimize this threat, the author examined papers with “Cloud Migration”, “Cloud Security”, and “Cloud Transformation” keywords and strings in the title and read their abstracts, introductions, and conclusions.

8. Conclusion and Future Work

Being a relatively newer technology, cloud computing comes with its own array of security challenges and new perspectives for attacks to happen. Despite the rigorous efforts of the cloud security research community, there are still many open issues and challenges to the security of the cloud environment. Hence, this paper proposed a secure path to cloud transformation through a Secure Cloud Migration Strategy (SCMS). Additionally, necessary cloud security documents/runbooks were identified in this paper. Both contributions were developed based on a systematic literature review on the legacy of securing the cloud migration journey.

The next step is to analyze and test the effectiveness of the proposed SCMS and cloud security documents/runbooks by implementing them through an experimental study involving migrating applications/services to cloud environments. As another venue of future work, the author aims to develop a dynamic-optimizing approach for a secure and relaxed privilege management system in the cloud. The term

'secure and relaxed' refers to usable security which aims to make sure that security products and processes are usable by those who need them.

References

Abdulsalam, Y.S. and Hedabou, M., 2022. Security and privacy in cloud computing: technical review. *Future Internet, 14*(1), p.11.

Ahmad, N., Qamar, S., Khan, N., Naim, A., Hussain, M.R., Naveed, Q.N. and Mahmood, M.R., 2020. Cloud computing trends and cloud migration tuple. *Innovations in Electronics and Communication Engineering: Proceedings of the 8th ICIECE 2019,* pp.737-745.

Ahmad, N., Naveed, Q.N. and Hoda, N., 2018, November. Strategy and procedures for Migration to the Cloud Computing. In *2018 IEEE 5th international conference on engineering technologies and applied sciences (ICETAS)* (pp. 1-5). IEEE.

Ali, O., Shrestha, A., Chatfield, A. and Murray, P., 2020. Assessing information security risks in the cloud: A case study of Australian local government authorities. *Government Information Quarterly, 37*(1), p.101419.

Alonso, J., Orue-Echevarria, L., Casola, V., Torre, A.I., Huarte, M., Osaba, E. and Lobo, J.L., 2023. Understanding the challenges and novel architectural models of multi-cloud native applications–a systematic literature review. *Journal of Cloud Computing, 12*(1), pp.1-34.

Alshammari, M.M., Alwan, A.A., Nordin, A. and Al-Shaikhli, I.F., 2017, November. Disaster recovery in single-cloud and multi-cloud environments: Issues and challenges. In *2017 4th IEEE international conference on engineering technologies and applied sciences (ICETAS)* (pp. 1-7). IEEE.

AlZain, M.A., Pardede, E., Soh, B. and Thom, J.A., 2012, January. Cloud computing security: from single to multi-clouds. In *2012 45th Hawaii International Conference on System Sciences* (pp. 5490-5499). IEEE.

Araújo, T.M.R.P.D., 2021. Cloud Technology Selection: *A structured framework for decision making (Doctoral dissertation).*

Casola, V., De Benedictis, A., Rak, M. and Salzillo, G., 2020. A cloud SecDevOps methodology: from design to testing. In *Quality of Information and Communications Technology: 13th International Conference, QUATIC 2020, Faro, Portugal, September 9–11, 2020, Proceedings 13* (pp. 317-331). Springer International Publishing.

Casola, V., De Benedictis, A., Rak, M. and Villano, U., 2018, June. Towards automated penetration testing for cloud applications. In *2018 IEEE 27th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE)* (pp. 24-29). IEEE.

Cichonski, P., Millar, T., Grance, T. and Scarfone, K., 2012. Computer security incident handling guide. *NIST Special Publication, 800*(61), pp.1-147.

El Kafhali, S., El Mir, I. and Hanini, M., 2022. Security threats, defense mechanisms, challenges, and future directions in cloud computing. *Archives of Computational Methods in Engineering, 29*(1), pp.223-246.

Fahmideh, M., Daneshgar, F., Rabhi, F. and Beydoun, G., 2019. A generic cloud migration process model. *European Journal of Information Systems,* 28(3), pp.233-255.

Gonzalez, D., Perez, P.P. and Mirakhorli, M., 2021, October. Barriers to Shift-Left Security: The Unique Pain Points of Writing Automated Tests Involving Security Controls. In *Proceedings of the 15th ACM/IEEE International Symposium on Empirical Software Engineering and Measurement (ESEM)* (pp. 1-12).

Gonzalez, N., Miers, C., Redigolo, F., Simplicio, M., Carvalho, T., Näslund, M. and Pourzandi, M., 2012. A quantitative analysis of current security concerns and solutions for cloud computing. *Journal of Cloud Computing: Advances, Systems and Applications, 1*, pp.1-18.

Grobauer, B. and Schreck, T., 2010, October. Towards incident handling in the cloud: challenges and approaches. In *Proceedings of the 2010 ACM workshop on Cloud computing security workshop* (pp. 77-86).

Hassan, W., Chou, T.S., Li, X., Appiah-Kubi, P. and Tamer, O., 2019. Latest trends, challenges and solutions in security in the era of cloud computing and software defined networks. *Int J Inf & Commun Technol ISSN, 2252*(8776), p.8776.

Hong, J., Dreibholz, T., Schenkel, J.A. and Hu, J.A., 2019. An overview of multi-cloud computing. In *Web, Artificial Intelligence and Network Applications: Proceedings of the Workshops of the 33rd International Conference on Advanced Information Networking and Applications (WAINA-2019) 33* (pp. 1055-1068). Springer International Publishing.

Kavitha, M.G. and Radha, D., 2022. Quality, Security Issues, and Challenges in Multi-cloud Environment: A Comprehensive Review. *Operationalizing Multi-Cloud Environments: Technologies, Tools and Use Cases,* pp.269-285.

Masadeh, S.R., AlShrouf, F.M. and Kumar, A.S., 2023. Concerns from Cloud Security Issues: Challenges and Open Problems. *International Journal, 12*(1).

McLellan, C., 2019. Multicloud: Everything you need to know about the biggest trend in cloud computing. *ZDnet, Jul.*

Okoli, C. and Schabram, K., 2010. A guide to conducting a systematic literature review of information systems research.

Ouda, A.J., Yousif, A.N., Hasan, A.S., Ibrahim, H.M. and Shyaa, M.A., 2022. The impact of cloud computing on network security and the risk for organization behaviors. *Webology, 19(1)*, pp.195-206.

Santos, J.C., Tarrit, K. and Mirakhorli, M., 2017, April. A catalog of security architecture weaknesses. In *2017 IEEE International Conference on Software Architecture Workshops (ICSAW)* (pp. 220-223). IEEE.

Yurtseven, I. and Bagriyanik, S., 2020, October. A review of penetration testing and vulnerability assessment in cloud environment. In *2020 Turkish National Software Engineering Symposium (UYMS)* (pp. 1-6). IEEE.