

Cyber Security Experts Association of Nigeria (CSEAN)
Society for Multidisciplinary & Advanced Research Techniques (SMART)
Faculty of Computational Sciences & Informatics - Academic City University College, Accra, Ghana
SMART Scientific Projects & Research Consortium (SMART SPaRC)
Sekinah-Hope Foundation for Female STEM Education
ICT University Foundations USA

Proceedings of the Cyber Secure Nigeria Conference – 2023

A Proactive Approach to Addressing Security Challenges in Cloud Migration

Njoku, Janet

Cybersecurity Engineer

Infinion Technologies

E-mail: janetnjokuc@gmail.com

Phone: +2348100230773

ABSTRACT

In today's digital landscape, organizations are increasingly migrating their operations to the cloud. However, during this shift comes the crucial need for robust security measures. This paper explores the major security challenges organizations face during cloud migration and proposes an effective strategy to mitigate these risks. By building upon existing research, the paper identifies key security challenges and focuses on a proactive approach to address them. The paper delves into the fundamental principles of cloud security, emphasizing the shared responsibility model and the importance of encryption, access controls, identity management, and cloud governance. It highlights the specific security issues encountered during cloud migration. To address these challenges, it advocates for the application of threat modeling—a systematic approach to identify and evaluate potential threats, vulnerabilities, and risks. The benefits of threat modeling include early risk identification, risk prioritization, a security-by-design approach, alignment with standards and best practices, and ongoing security assurance. Practical guidance on implementing threat modeling for a secure cloud migration is provided particularly based on the Microsoft threat modelling approach by identifying and prioritizing potential security threats, implementing effective controls, and validating their effectiveness.

Keyword: Proactive Approach, Security Challenges, Cloud Migration, Security, Risks, Models

Proceedings Citation Format

Njoku, J. (2023): A Proactive Approach to Addressing Security Challenges in Cloud Migration. Proceedings of the Cyber Secure Nigeria Conference. Nigerian Army Resource Centre (NARC) Abuja, Nigeria.
11-12th July, 2023. Pp 89-96. <https://www.csean.org/>. dx.doi.org/10.22624/AIMS/CSEAN-SMART2023P11

1. INTRODUCTION

In today's digital landscape, organizations are increasingly recognizing the benefits of migrating their operations to the cloud. Cloud computing has received notable attention and Vendors

trumpet the Cloud model citing merits such as accessibility, flexibility and efficiency (Fisher, 2018). However, with this shift towards cloud adoption, understanding the importance of implementing robust security measures becomes eminent. Safeguarding sensitive data, mitigating risks and protecting critical systems are major concerns for organizations undergoing cloud migration.

According to the National Institute of Standards and Technology (NIST), Cloud computing has three main cloud service models. The delivery models are IaaS, PaaS and SaaS (Mell & Grance, 2011). Each with its own complexities of shared responsibility, data storage and access. The importance of security in migration projects cannot be overstated. As organizations transition their operations to the cloud, they must address a myriad of security challenges unique to this environment.

This paper aims to shed light on the major security challenges organizations face during the migration to the cloud and propose an effective strategy to mitigate these risks. By building upon existing research, I have identified key security challenges outlined in previous studies. Although these challenges will be referenced, the focus will be on proposing a proactive approach to address these concerns.

In the subsequent sections of this paper, I will delve into the fundamental principles of cloud security, discuss the specific challenges encountered during migration, explore the concept of threat modeling, and provide practical guidance on implementing this strategy effectively. The findings and proposed security strategy outlined in this article will contribute to the body of knowledge in the field of cloud security, empowering organizations to safely embrace the cloud and ensure the success of their migration endeavors.

2. CLOUD SECURITY FUNDAMENTALS

The diversity of involved elements in the cloud paradigm, i.e., network, architecture, APIs, and hardware, increases the intricacy of security issues (Pancholi & Patel, 2016). This section offers an overview of the fundamental principles of cloud security and underscores their significance in driving successful migration projects. The cornerstone of cloud security lies in the shared responsibility model. Understanding this shared responsibility model is essential for customers who are moving to the cloud. Cloud providers offer considerable advantages for security and compliance efforts, but these advantages do not absolve the customer from protecting their users, applications, and service offerings (Microsoft, 2019).

Central to maintaining the confidentiality and integrity of critical information is the deployment of encryption and robust data protection mechanisms. Data must be anonymized to enhance privacy. Anonymization indicates a privacy reservation technique to make the data valueless to unauthorized access (Sahab et al., 2020). Employing powerful encryption techniques, both at rest and in transit, shields data from unauthorized access and potential breaches. Encryption acts as a formidable defense, ensuring the security of sensitive information throughout its lifecycle.

Effective access controls and identity management are pivotal in bolstering cloud security. Organizations must implement stringent measures, such as role-based access control (RBAC), multi-factor authentication (MFA), and SSO to verify user identities and grant appropriate levels of access (Indu et al., 2018). By doing so, they prevent unauthorized access attempts and mitigate the risk of data breaches.

Cloud environments can be unruly and unpredictable without effective cloud governance. It is, therefore, very important to have strong cloud governance and management controls in place that are fully aligned with organizational goals and objectives, supportive at all levels of the cloud journey and in sync with the enterprise's existing frameworks, methodologies and ISO standards (Ahmed, 2021). Organizations must adhere to rigorous data protection regulations, such as GDPR, HIPAA, and PCI DSS, to ensure the privacy and security of customer data.

By understanding and following basic cloud security principles, organizations can safely navigate the challenges of cloud migration. Strong security measures protect data integrity, reduce risks, and prevent unauthorized access. We will examine the specific security issues that arise during cloud migration and offer workable solutions in the next sections. Organizations can begin on a secure and successful migration journey, fully utilizing the potential of the cloud while protecting their assets, by properly addressing these concerns.

3. SECURITY CONSIDERATIONS DURING CLOUD MIGRATION

When it comes to cloud migration, there are several critical security issues that organizations must address to ensure a successful and secure transition. These issues, as identified in the journal "A Study on Cloud Migration Models and Security Issues in Cloud Migration," include data breaches, hijacking of accounts, insider threat, malware injection, abuse of cloud services, insecure API, insufficient due diligence, shared vulnerabilities and data loss (Sravya & Mohammad, 2019).

Data breaches: Unauthorized access or disclosure of sensitive data can lead to devastating consequences. This can happen through a variety of ways, such as misconfiguration of cloud resources, human error, or malicious attacks. **Hijacking of accounts:** In a recent Capital One data breach, a threat actor gained access to 140000 social security numbers, 1 million Canadian Social Insurance numbers and 80,000 linked bank account numbers of credit card customer (Capital One, 2019). They were able to do this via exploit of misconfigured web application firewall according to the Justice department. Strategies such as phishing, extortion, and exploitation of software vulnerabilities are utilized to figure Account or Service Hijacking in cloud framework setup too (Tyagi, 2017). Attackers may attempt to compromise user accounts or administrative credentials, gaining unauthorized access to cloud resources.

Insider threat: Insiders can become a real threat to organizations migrating to the cloud because they do not have to breach any external security fences (ISC)². Insider threat presents a formidable risk as individuals within an organization who have authorized access to sensitive data and systems can potentially misuse or exploit their privileges. This can include actions such as stealing data, deleting data, or disrupting cloud services.

Malware injection: Malware injection is a critical security concern during cloud migration, as it can have severe repercussions on the integrity, confidentiality, and availability of data and systems. Cross-site scripting and structured query language (SQL) injection attacks are two of the most often used techniques. Once malware is injected, it can propagate throughout the cloud infrastructure, compromising the security of interconnected systems.

Abuse of cloud services: The common form of abuse is the unauthorized use of cloud resources, where individuals or groups exploit the cloud platform without proper authorization, this can include spinning up virtual machines, deploying applications, or storing data without adhering to the organization's security requirements, and misuse of cloud services for malicious purposes.

Insecure APIs: APIs play a crucial role in facilitating communication and interaction between different components of cloud services, including data storage, networking, authentication, and application functionality. At present, there are many security risks in API design, such as various attacks caused by out-of-date API, unauthorized users abusing the API, sensitive API calls, and version confusion (Sun et al., 2022). When APIs are inadequately designed and implemented, they become potential entry points for attackers to exploit.

Insufficient due diligence: It is essential for organizations to conduct comprehensive assessments of potential providers to ensure they meet the necessary security requirements and adhere to relevant compliance standards. With the increased demand and dependency on cloud computing, risk to expected service levels (e.g., availability, reliability, performance, security), potential for financial impact, and level of trustworthiness of CSPs are all important areas requiring attention (Maeser, 2020).

Shared Vulnerability: If the cloud service provider does not adequately secure the underlying infrastructure, it can create a vulnerability that affects multiple customers. Similarly, if the customer fails to properly configure access controls or implement appropriate security measures within their cloud instances, it can lead to vulnerabilities that impact their own data and potentially other customers' data as well.

Data loss: There is a possibility of a data breach during data migration if security solutions provided by the vendor are not planned, implemented, and executed correctly (Mudrakola, 2018). This can result in irretrievable loss of critical information and severe business disruptions. Several factors contribute to data loss risks, including hardware failures, human errors, and malicious activities.

4. APPLYING THREAT MODELING FOR SECURE CLOUD MIGRATION

Threat modeling is one approach that includes identifying the main assets within a system and threats to these assets (Xiong & Lagerström, 2019). It is a systematic approach used to identify and evaluate potential threats, vulnerabilities, and risks to a process, system, application, or organization. By analyzing weaknesses related to known attack techniques and providing mitigation suggestions for these attacks, stakeholders of an enterprise can assess threats to their IT environment and analyze what security settings that could be implemented to secure the system more effectively (Xiong et al., 2022) and allocate resources effectively to address the most significant risks. Threat modeling, which offers a structured method for identifying, evaluating, and mitigating security risks and vulnerabilities, is crucial in impacting a successful cloud migration. It can strengthen the cloud migration procedure in the following ways:

1. Early risk identification: Organizations can discover potential security risks and vulnerabilities using threat modeling at an early stage of the cloud migration process. Organizations can proactively find vulnerabilities that attackers might exploit by evaluating the cloud architecture, data flows, and system components. By identifying risks early on, it is possible to install security controls in a timely manner.
2. Risk prioritization: Risk assessment is an integral part of the threat modeling process. Risk is a measure of the extent to which an entity is threatened by a circumstance or event, and it is a function of the likelihood of the event and the adverse impact caused by the event (Griffioen & Sinopoli, 2021). Threat modeling aids in risk prioritization and mitigation by ranking security hazards according to their likelihood and potential impact. Organizations may deploy resources and efforts efficiently by being aware of the potential effects of each risk. In order to ensure that the most important risks are adequately handled, threat modeling directs the creation and implementation of risk mitigation measures unique to the cloud migration scenario.
3. Security by design approach: Threat modeling and security requirements provide the foundations upon which the rest of the security system is built. Threats are analyzed based on their criticality and likelihood, and a decision is made whether to mitigate the threat or accept the risk associated with it (Myagmar et al., 2005). Once infrastructure designers have decided which security mechanism the architecture must be able to use, it's incorporated right from the design phase of the migration lifecycle.
4. Alignment with standards and best practices: In the context of compliance, risk identification involves examining how a compliance requirement—an obligation or prohibition—can lead to risk. Failure to properly consider risks can lead to the selection of inappropriate compliance measures and ineffective regulatory outcomes (Esayas & Mahler, 2015). Threat modelling can assist in locating security settings and configurations compliant with established frameworks.
5. Ongoing security assurance: Threat modeling is not a one-time activity; it should be revisited and updated throughout the cloud migration process and the lifecycle of the cloud environment. As new information, technologies, or threats emerge, organizations can adapt their threat models accordingly. This ongoing security assurance helps organizations maintain a proactive and resilient security posture in the cloud.

5. PRACTICAL GUIDANCE ON IMPLEMENTING THREAT MODELLING FOR A SECURE CLOUD MIGRATION

“Threat modeling is the key to a focused defense. Without threat modeling, you can never stop playing whack-a-mole.”— Adam Shostack [20]. It is a wide concept that encompasses a broad range of techniques that can be utilized to make a system more secure. My approach is based on the Microsoft approach to threat modelling. Implementing a threat modeling strategy for a secure cloud migration must be intentional and practical steps need to be followed to ensure its effectiveness. Here's some guidance on how you can align your threat modelling goals.

Defining security requirements: To start the threat modeling process, it's crucial to define the security requirements. This involves identifying the specific security goals and objectives for the migration. Consider compliance requirements and regulatory standards that must be met. Thinking about security requirements with threat modeling can lead to proactive architectural decisions that allow for threats to be reduced from the start (Shevchenko et al., 2018). Additionally, determine the desired security controls. A set of security controls for cloud should include Access controls, Incident Response and management, System and network configuration backups, security testing, data and communication encryption, password standards and continuous monitoring (Venu et al., 2015).

Creating an architectural diagram: The next step is to create an architectural diagram that represents the cloud migration environment. This diagram provides a visual representation of the system components, services, and data flows involved in the migration. It helps identify trust boundaries and data boundaries, enabling the identification of control points and potential attack vectors. **Identifying threats:** Using the architectural diagram as a reference, it's important to identify potential threats and attack vectors. Apply threat modeling techniques, such as STRIDE, to systematically analyze the architecture for potential security weaknesses. STRIDE threat model was considered an effective technique for effective measure for safeguarding cloud systems (Morana & Uceda 2015).

Mitigating threats: This is put in place to prevent data breaches and security incidents, as well as monitoring and responding to threats (Khraisat et al., 2019). After identifying the threats, the next step is to determine appropriate mitigation strategies for each one. Align these strategies with security best practices, cloud service provider recommendations, and industry standards. Implement security controls that address the identified threats effectively. This may include access controls, encryption mechanisms, intrusion detection systems, or other relevant measures.

Validating that threats have been mitigated: Once the security controls are implemented, it's essential to validate their effectiveness in mitigating the identified threats. An essential part of an effective cybersecurity engineering process is testing the implementation of a system for vulnerabilities and validating the effectiveness of countermeasures (Wooderson & Ward, 2017). Conduct validation tests to ensure that the implemented controls work as intended. Perform security testing and vulnerability assessments to identify any remaining vulnerabilities or weaknesses.

6. CONCLUSION

In conclusion, this research paper has highlighted the major security challenges faced by organizations during cloud migration and proposed a proactive approach to mitigate these risks. By understanding the fundamental principles of cloud security and applying threat modeling techniques, organizations can address security concerns early on, prioritize risks, implement security measures, and validate their effectiveness. By adopting this approach, organizations can safely embrace the cloud, protect sensitive data, and ensure the success of their migration endeavors. Threat Modelling is an iterative process and it's important to revisit and refine the process as needed based on new information or changes in the cloud migration environment.

REFERENCES

1. Fisher, C. (2018) Cloud versus On-Premise Computing. *American Journal of Industrial and Business Management*, 8, 1991-2006. doi: 10.4236/ajibm.2018.89133.
2. Mell, P., & Grance, T. (2011). The NIST definition of cloud computing (NIST SP 800-145). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-145>
3. Pancholi, S., & Patel, N. (2016). Enhancement of cloud computing security with secure data storage using AES. *International Journal for Innovative Research in Science and Technology*, 2(12), 1-5.
4. Microsoft. (2019). Shared Responsibility for Cloud Computing (Publication No. 2019-10-25). Microsoft. Shared Responsibility for Cloud Computing-2019-10-25.pdf (microsoft.com)
5. Sahab, D. M., Abdul Monem, S. R., & Rahma Taha, M. H. (2020). Maintaining the integrity of encrypted data by using the improving hash function based on GF 28. *TEM Journal*, 9(3), 1277-1284. <https://doi.org/10.18421/TEM93-57>
6. Indu, I., Rubesh Anand, P. M., & Bhaskar, V. (2018). Identity and access management in cloud environment: Mechanisms and challenges. <https://doi.org/10.1016/j.jestch.2018.05.010>
7. Ahmed, H. S. A. (2021). Building cloud governance from the basics. ISACA. Building Cloud Governance From the Basics (isaca.org)
8. Sravya, P., & Mohammad, S. (2019). A study on cloud migration models and security issues in cloud migration. *SSRN Electronic Journal*, 6, 235-240.
9. Capital One. (2019). 2019 Capital One Cyber Incident | What Happened. Capital One. <https://www.capitalone.com/facts2019/>
10. Tyagi, R. (2017). Security aspects of cloud migration. *International Journal of Engineering Science and Computing*.
11. (ISC)². Insider threats can turn your cloud security into a storm. <https://www.isc2.org/articles/insider-threats-can-turn-your-cloud-security-into-a-storm#>
12. Sun, R., Wang, Q., Guo, L. (2022). Research Towards Key Issues of API Security. In: Lu, W., Zhang, Y., Wen, W., Yan, H., Li, C. (eds) *Cyber Security. CNCERT 2021. Communications in Computer and Information Science*, vol 1506. Springer, Singapore. https://doi.org/10.1007/978-981-16-9229-1_11

13. Maeser, R. (2020). Analyzing CSP Trustworthiness and Predicting Cloud Service Performance. *IEEE Open Journal of the Computer Society*, 1, 73-85. <https://doi.org/10.1109/OJCS.2020.2994095>.
14. Mudrakola, S. (2018). Cloud data migration: Common issues and problems you must avoid. Retrieved from <http://techgenix.com/cloud-data-migration>
15. Xiong, W., & Lagerström, R. (2019). Threat modeling–A systematic literature review. *Computers & Security*, 84, 53-69.
16. Xiong, W., Legrand, E., Åberg, O., et al. (2022). Cybersecurity threat modeling based on the MITRE Enterprise ATT&CK Matrix. *Software and Systems Modeling*, 21, 157-177. <https://doi.org/10.1007/s10270-021-00898-7>
17. Griffioen, P., & Sinopoli, B. (2021). Assessing risks and modeling threats in the Internet of Things. arXiv preprint arXiv:2110.07771.
18. Myagmar, S., Lee, A., & Yurcik, W. (2005). Threat modeling as a basis for security requirements.
19. Esayas, S., & Mahler, T. (2015). Modeling compliance risk: A structured approach. *Artificial Intelligence and Law*, 23(3), 271-300. <https://ssrn.com/abstract=2746822>
20. Shostack, A. (2014). *Threat modeling: Designing for security*. Wiley.
21. Shevchenko, N., Chick, T. A., O’Riordan, P., Scanlon, T. P., & Woody, C. (2018). *Threat modeling: A summary of available methods* (PhD thesis).
22. Venu, G., Rao, M., Madhava, V., & Selvaraj, R. (2015). Security and architectural patterns for securing the cloud architecture. *American Journal of Engineering Research*, 4, 188-191.
23. Morana, M. M., & Uceda Vélez, T. (2015). *Risk-centric threat modeling: Process for attack simulation and threat analysis*. Wiley.
24. Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: Techniques, datasets and challenges. *Cybersecurity*, 2, 1-22.
25. Wooderson, P., & Ward, D. (2017). *Cybersecurity testing and validation*. SAE Technical Paper 2017-01-1655. <https://doi.org/10.4271/2017-01-1655>