POLYTECHNIQUE
MONTRÉAL
UNIVERSITÉ
D'INGÉNIERIE

FACULTÉ DE GÉNIE

Comparative Critique of Three Scientific Papers

Auteur	*Email*	*Id*
Diab Khanafer	REDACTED	REDACTED

Présenté à :
REDACTED

November 13th 2023

Table des matières

1 Comparative Critique of Three Scientific Papers

1.1 Overview

Throughout the years, cloud infrastructures have been taking a bigger role and importance with companies favoring and promoting the usage of the cloud instead of on-premise infrastructures. This has pushed for a higher need for better services and management of cloud infrastructures, without forgetting the security aspects of having an your whole organization relying on a setup accessible by public internet (public cloud). With this massive move to the cloud, multiple researches have been made to critic multiple aspects of using the cloud, and in comparative critic we will compare three scientific papers which all have the same general topic : security or cybersecurity in a cloud environment. Two of them [2][3] focus on Amazon Cloud Services (AWS) and the third one [1] being more generic. The importance of such comparative critic is crucial, because it brings a person to develop their critical thinking, understand research methodology, validating scientific claims while also identifying weaknesses and strengths in specific papers.

1.2 Research Questions/Objectives

Here are the main research question or objective brought by each paper by their research :

— **[1]** : With the ever growing availability of Cloud computing, security has become one of the major challenge. The paper presents the state of the art in regard to cloud identity management by reviewing some literature already available and presenting the trend to provide a guide for future research.

— **[2]** : Cloud computing being a new business model and computing paradigm at the time of the article, security was becoming a big and long-term concern. The paper briefly describes some basic cloud security concerns regarding Cloud computing and Data security, as well as some cloud specific attacks.

— **[3]** : This paper, being the most recent of all three, re-examines the content of an advanced course in Cybersecurity, only from the perspective of Cloud computing. It is also used as a guide to aid "cloudifying" a Cybersecurity offering, re-examine Cybersecurity in-light of the new paradigm of Cloud computing, and acts as preparation for the Security Speciality certification from AWS.

1.3 Methodologies

The following points are the methodologies of each paper :

— **[1]** : The analysis begins by establishing and explaining the main talking points of the paper, which are the basis of the cloud, the different level of abstractions provided (IaaS, Paas, SaaS), and then diving into Cloud computing, digital identity and identity management. The next step was to further explain the layers of Identity Management System (IDM), the different classifications (Isolated, Centralized, Federated, Anonymous), then identify the various components for user authentication, and then displaying some IDM vulnerabilities. With these steps done, the authors then present the perspective of IDM in the industry, such as Identity Access Management-as-a-Service (IDaaS) to user secure IDM, the relevant involvement of cybersecurity experts in the field, and the multiple means of improving said IDM with ways more complicated than simple username and passwords.

— **[2]** : Considering the paper is the oldest among the three, we need to be lenient on the information and steps taken in the research. First, they start by taking a look at the types of Amazon Cloud storage available, then a quick introduction on Data security in S3. After that, they dive into multiple Cloud Risks and API Concerns, such as general server risks, API keys and APIs, service and account hijacking and possible defenses. After that, they discuss ideas about the future of cloud security.

— **[3]** : The paper starts by providing different approaches to Cybersecurity, or different angles, such as a Software engineer, as a business, or as an educator. This can give the reader a quick overview of how to view cybersecurity in general depending on their status. After that, they dive into the core curriculum of what Cybersecurity offers, such as it's objectives (such as the CIA and AAA fundamentals). Then, they proceed to present and explains a multitude of basic attacks that could occur against infrastructures like DDoS, social engineering, phishing and so on. After that, they detail the methods of cryptography and it's goal as a security measure. They also present some basics then two types of cryptography : symmetric and asymmetric encryption. Finally, they present AWS best practices regrouping everything that was said so far in a cloud aspect and point of view.

As we can notice, the common factor between those three papers are the fact that they aim to explore, present, discuss and improve the cybersecurity posture in the cloud. However, their methodology remains different in the steps and the main aspect they end up focusing on. Paper one [1] focusing mainly on user identification, authentication and systems associated. They detail and present popular identification management usage and compared them. The other two papers [2][3] did not stick to one specific subject like [1] did. They remained broad in their methodology and showcased more than one system of the cloud. Which is why these two [2][3] are fairly similar in their methodology, but not in their goal, since [3] focused on the educational aspect of cybersecurity in the cloud by acting as a guide and review, but [1] and [2] focus on actual structures provided in the cloud such as services and management systems.

1.4 Key Findings

— **[1]** : The key findings of the first paper are that Identity and access management (IAM) is an important and critical issue in Cloud computing, that various architectures are in place to ensure secured IDMs, but more effort is still needed to be put in place to provide robust and all-encompassing IDM for Cloud computing.

— **[2]** : In this paper, the authors implore some of the basics of terms and concepts of cloud computing, as well as discuss different aspects such as data security, API concerns, account hijacking and more. They showcase the differences between traditional and cloud services in terms of security, as well as possible defenses. Their findings are provided in a sort of guideline of research on cloud services and security issues.

— **[3]** : This article does not include "key findings" in the definition of the terms. However, what it includes is, after a deep dive into key elements of security and it's objectives, a structured AWS best practices guideline in term of security for readers to focus and rely upon.

1.5 Strengths and Limitations

Let's start by discussing the shared strengths among all three papers. They are explain really well the points they try to bring concerning cloud security, one [1] by being very specific in the subject concerning IDM security and the two others [2] [3] by providing a more generalist approach. A solid point of strengths by the first paper [1] is that the subject is applicable cross-platform and not only dependent on AWS.

On the sides of limitations, contrary to the first paper [1], both other two articles [2] [3] are very specific on AWS infrastructure and features without necessarily showcasing others. Although some points can still be translated to similar cloud providers, theirs are more specific to AWS. As well, these two same papers are

1.6 Discussions and Implications

It becomes evident that the authors of each paper interpret their results in different ways, contributing to a difference of insights. The first paper [1] focused on the understanding and the security aspects of Identity Management Systems (IDM), mainly focusing on account management, authentication, authorization, federation and auditing aspects. Their logic and research is based on already existing literature and what they targeted in said literature. The second paper [2] took a centered view on a couple AWS services such as S3, AMI, IAM, EBS storage and more, then put an emphasis on risks and concerns related to these services as well as server risks and APIs. In this paper, the authors did their own research and did not rely on parallel researches done. For the third article [3], the author took three approaches, one being to aid in "cloudifiying" cybersecurity, then to re-examine it in the new light of cloud computing, and last to provide a guide in AWS Security. To do this, they based their research on already written articles as well and guides and best practices from AWS. Compared to the other two papers, they did not take a technically stand and mainly detailed logic and provided better understanding.

1.7 Recommendations and Future Directions

From the comparative analysis of the three scientific papers on cloud security, several recommendations for future research can be pointed out. First, there is always a need for studies that integrate the insights from security experts, general users and researchers. Collaborative research that exceeds these separate individuals can enhance the efficacy of cloud security measures, albeit actual and future. Furthermore, future investigations could focus on refining the balance between security and usability, addressing the challenge of implementing robust security measures without compromising user experience and interactivity. Finally, the dynamic and ever changing nature of security calls for ongoing collaboration ensure that research findings are effectively translated into practical and scalable security solutions for all cloud environments.

2 General Observations

In comparing the three scientific papers on cloud security, several overarching patterns and insights have emerged. Firstly, a common point across the studies is the recognition of encryption as safeguarding data integrity and confidentiality within cloud environments remains an important point to all. Secondly, while the papers individually dive into different aspects of cloud security, a common point showcases the necessity for a security strategy and posture that combines these diverse aspects. The comparative analysis draws attention the relationship between encryption [3], access control and IDMs [1], cloud security best-practices [3], and illustrating the need for an adaptive approach in the face of evolving cybersecurity issues. Furthermore, the papers collectively shed light on the challenge of balancing robust security measures with the imperative for user-friendly and scalable solutions in cloud environments [1]. This perspective positions cloud security not merely as a technological challenge and a simple fix, but as a complex interplay of technical, usability, and financial strategic considerations. Overall, the comparative critique provides insights that advocate for a comprehensive and collaborative approach from users as well as researchers, for future work on the matter of cybersecurity in the cloud.

3 Conclusion

In conclusion, the comparative critique of the three scientific papers on cloud security provides a nuanced understanding of the intricacies and issues generally raised within this dynamic and ever changing field. In this critique, we compared the distinct researches done on access control mechanisms and IDM systems [1], the security aspects of cloud services including their risks [2], and an AWS guide and best practices for security provided [3]. This analysis showcases the importance of a comprehensive, integrated approach to cloud security.

The comparative critique has served as a tool in displaying the objectives of each paper, their methodologies and their key findings, the strengths and limitations of each study, as well as the discussions and implications brought up by each and future directions that could be taken. In the ever lasting pursuit of securing cloud infrastructures, lots of research still remains to be made.

Références

[1] Temidayo Abayomi-Zannu et Isaac Odun-Ayo. « Cloud Identity Management – A Critical Analysis ». en. In : *Hong Kong* (2019). url : `https://www.researchgate.net/publication/333402738_Cloud_Identity_Management_-_A_Critical_Analysis`.

[2] Patrick Mosca et al. « Cloud Security : Services, Risks, and a Case Study on Amazon Cloud Services ». en. In : *International Journal of Communications, Network and System Sciences* 07.12 (2014), p. 529-535. issn : 1913-3715, 1913-3723. doi : `10.4236/ijcns.2014.712053`. url : `https://www.scirp.org/html/4-9701936_52580.htm` (visité le 12/10/2023).

[3] Michael Soltys. *Cybersecurity in the AWS Cloud*. en. arXiv :2003.12905 [cs]. Mars 2020. url : `http://arxiv.org/abs/2003.12905` (visité le 12/10/2023).