Scientific Research Publishing

Journal of Information Security, 2023, 14, 250-263
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

Security Model for Cloud Computing: Case Report of Organizational Vulnerability

Sakharkar Shreyas

Independent Author, Stevenson Ranch, CA, USA
Email: shrey16sakharkar@gmail.com

How to cite this paper: Shreyas, S. (2023) Security Model for Cloud Computing: Case Report of Organizational Vulnerability. *Journal of Information Security*, **14**, 250-263.
https://doi.org/10.4236/jis.2023.144015

Received: May 8, 2023
Accepted: August 6, 2023
Published: August 9, 2023

Abstract

Cloud computing services have quickly become a mainstay in business, leading to success as a business model and numerous advantages from the client's point of view. Ease and amount of storage and computational services provisions were not previously accessible or affordable. However, parallel to this explosion has been significant security risk concerns. Thus, it is important to understand and define these security risks in a cybersecurity framework. This paper will take a case study approach to approach past security risks and propose a model that can be followed by organizations to eliminate the risk of Cloud-related cyberattacks. The main aims of this systematic literature review (SLR) are to (1) address security risks/vulnerabilities that can target cloud environments, (2) define tools that can be used by organizations to defend their cloud environment against those security risks/vulnerabilities, and (3) analyze case studies of significant cyberattacks and provide recommendations for organizations to mitigate such cyberattacks. This paper will propose a novel cloud cybersecurity model from a two-pronged offensive and defensive perspective for implementation by organizations to enhance their security infrastructure.

Keywords

Cloud Computing, Vulnerabilities, Security Risks

1. Introduction

Cloud computing has fundamentally changed the Information Technology (IT) landscape by making data access and resource availability more accessible than ever before. Prior to the cloud computing era, data was stored offline, limiting access, and hampering remote work and collaboration. However, the advent of cloud computing changed the landscape. This was brought about by major service providers like Amazon's AWS or Alphabet's Google Apps. Cloud computing introduced an era of seamless outsourcing of IT solutions, virtual management of software and data, and dynamic deployment of resources. This has significantly enhanced operational efficiency and cost-effectiveness for organizations and contributed to energy efficiency [1] [2].

Despite these significant benefits, the shift to cloud computing is full of challenges. Among the primary concerns is the area of cloud security, which has emerged as a significant barrier to the widespread adoption of cloud services. According to the 2021 AWS Cloud Security Report, 90% of organizations use more than two cloud providers, and while cloud platforms provide data security solutions, major challenges persist across every provider, such as Identity and Access Management (IAM), access control, security policies, network security, and Digital Forensics and Incident Response (DFIR) [3] [4].

This paper endeavors to provide a comprehensive overview of the development and application of cloud computing, with a particular emphasis on security risks. By adopting a data-centric approach to examine how cloud applications encode and relay data within the cloud to ensure secure communication, we aim to delve into the heart of cloud security issues [2].

In our analysis, we will be looking at a case study: the significant security breach experienced by Capital One in June 2022. In this instance, due to a misconfiguration on the developers' side, an ex-AWS employee managed to exploit vulnerability in Capital One's firewall, leading to the unauthorized access of the personal information of 100 million individuals [2].

Additionally, a survey of over 300 cybersecurity professionals revealed that a staggering 95% are high to moderately concerned about public cloud security, with "Misconfiguration of the cloud platform" being the top concern for 71% of the participants [3].

By presenting a thorough exploration of the security risks in cloud computing, this paper seeks to elucidate potential vulnerabilities and shed light on strategies to enhance security measures in the rapidly evolving landscape of cloud computing.

2. Objectives

1) To comprehensively identify and understand the major security risks associated with cloud computing.

2) To devise a robust model that organizations can implement to mitigate these security risks.

3) To analyze real-life case studies to demonstrate the practical implications of these risks and the effectiveness of the proposed model.

3. Research Outcome

The importance of this research lies in its potential to significantly improve the security posture of organizations utilizing cloud computing. As data continues to be a pivotal asset, ensuring its security is paramount.

The escalating sophistication of cyber-attacks, coupled with the increasing reliance on cloud-based systems, underscores the need for a robust and comprehensive security model. This research, therefore, serves as a timely resource for organizations seeking to enhance their security measures in the cloud environment.

By providing an in-depth understanding of the various security risks and proposing an actionable security model, this research can contribute to minimizing the instances of data breaches, loss of customer trust, and financial losses due to cyber-attacks. It also paves the way for further development and refinement of security strategies to match the evolving cyber threat landscape.

The practical nature of this research, demonstrated through real-life case studies, adds to its relevance and applicability across a wide range of sectors. Hence, the insights drawn from this research could help guide policy and decision-making in organizations, enhancing the overall security and integrity of cloud-based systems.

4. Methodology

To answer the research aims, this paper will follow the methodology below. A systematic literature review of recent studies was conducted. Two databases, Google Scholar and PubMed, were utilized. Keywords that were used included "Cloud Security", "Cloud Computing", "security risks in cloud computing" and "organizational use of the cloud". Each paper was analyzed for techniques used and success rates to establish and secure cloud environments in various organizations. A PRISMA 2020 model was followed, as shown in **Figure 1**. Systematic literature reviews, case studies, and meta-analyses were all included. Thirty-five of the studies were found to fit within the inclusion criteria. Of these, four were duplicative and removed. Twenty-nine studies remained to conduct our literature review with. Select case studies will be looked at in further detail below as well for the purposes of model building.

5. Literature Review

The concept of cloud computing as a distributed architecture centralizes server resources on quite a scalable platform to provide on-demand computing resources and services [5]. However, according to literature, the rapid transition towards the cloud has fueled concerns on a critical issue for the success of information systems, communication, and information security [6].

Cybersecurity experts claim that cloud platforms are not secure because of the increasing number of attacks targeting cloud platforms [7]. In addition to this, everything on the cloud is shared, which means people and organizations have to share several components such as storage space, CPU cores, and network interface, emphasizing the need for increased data-driven analyses of security risks.

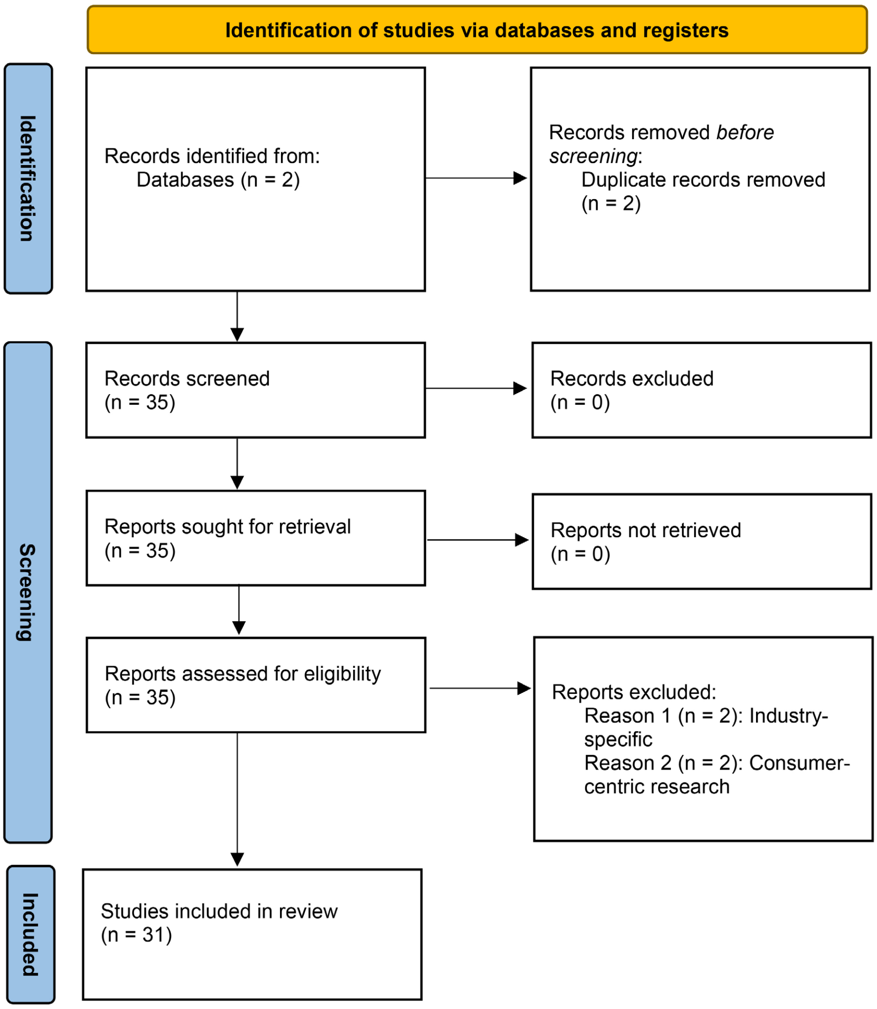
Identification of studies via databases and registers
Identification
Screening
Included
Records identified from:
Databases (n = 2)
Records removed *before screening*:
Duplicate records removed (n = 2)
Records screened (n = 35)
Records excluded (n = 0)
Reports sought for retrieval (n = 35)
Reports not retrieved (n = 0)
Reports assessed for eligibility (n = 35)
Reports excluded:
Reason 1 (n = 2): Industry-specific
Reason 2 (n = 2): Consumer-centric research
Studies included in review (n = 31)

Figure 1. PRISMA.

Three major cloud providers have recently published the shared responsibility model, where the customer is responsible for security in the cloud, and the cloud providers are responsible for the security of the cloud. Those shared responsibility models will be further illustrated here [8]. This means that security risk assumptions are placed on the consumer. However, due to the nature of the cloud computing product model, IT support and guidance are now rendered defunct in-house, leading to a cyclic nature of exploitation of security risks that are unable to be fixed by the consumer and ignored by the providers.

Thus, Mather *et al.* suggested a methodology to secure the enterprise cloud environment, including but not limited to infrastructure security, data security, and storage, identity and access management, and audit and compliance [9].

Many organizations aim to migrate their on-premise environments to the cloud to benefit from cloud features. This comes with challenges as addressed in a key survey by Fahmideh *et al.* [10]. These challenges include limited resource elasticity, multi-tenancy, and an unpredictable environment. This survey paper illustrated an evaluation framework and open challenges relevant to cloud migration. Based on that, it proposed a cloud migration evaluation framework and used it to analyze and compare existing approaches.

However, the literature also highlights security risks. Enriquez addresses that there are many security concerns regarding the following Azure services, which are Azure Defender, Azure DDoS protection, Access and Permissions, and Network Security. Therefore, the paper suggested evaluating internal policies and protocols in addition to embracing security best practices in the management and use of the Azure cloud [11]. Additionally, Statista addressed that the top cloud security concerns are data loss and leakage (69%), and data privacy/ confidentiality (66%), followed by accidental exposure of credentials (44%) [12].

Many security threats/risks target cloud environments as well as the on-premise environment, such as privacy, compliance regulations, malicious insiders, Denial of Service (DoS), Distributed Denial of Service (DDoS), vulnerable systems, and APIs, weak authentication and identity management, account hijacking, shared technology vulnerabilities, lacking due diligence, Advanced Persistent Threats (APT), abuse of cloud services, lack of responsibility, insufficient security tools, human error, ransomware, spectra and meltdown, data breaches, data loss, malicious insiders, unprotected IoT devices [13] [14].

On the other hand, other vulnerabilities/risks in cloud environments do not exist in classic IT data centers [15]. Those vulnerabilities/risks are structured in **Table 1**.

Areas organizations felt were the most important in 2019 to improve security visibility for the use of public cloud services include identifying software vulnerabilities and remediation (29%), identifying workload configurations that were out of compliance including those that didn't adhere to the industry standards benchmarks (28%), identifying misconfigured security groups (25%), discovering public cloud-resident sensitive data (24%), and third-party access to public cloud-resident data (23%) [16].

Figure 2 details the threat picture for cloud computing platforms. Threat actors target the organization's assets using attack tools.

One major case study will be explored to further identify specific vulnerabilities and craft a model for addressing these risks for mitigation.

Our research has comprehensively examined existing security risks and vulnerabilities associated with cloud computing. We present an in-depth analysis of these threats and propose viable defense strategies that organizations can adopt.

6. Data Breaches

A data breach involves the unauthorized access and extraction of sensitive information. A general breach flowchart is detailed in **Figure 3**. This is the most prevalent risk in cloud computing due to the vast volumes of data stored in the cloud. Data breaches can lead to significant financial losses and irreparable damage to an organization's reputation. Defense methods against data breaches include implementing strong data encryption, regular audits, and ensuring proper data access controls.

Table 1. Cloud environment risks, responsibility, and solutions.

Unique Threat	Responsibility	Current solutions
Lack of consumer visibility over operations	Infrastructure responsibility for assets and operations in the cloud computing world is dependent on the model of cloud service used. Security monitoring onus has paradigm shifted towards consumer self-monitoring requirements, despite this lack of control.	Re-hire onsite IT monitoring from a consumer perspective, and undo a part of the cost-effective benefits of cloud computing over past methodologies.
Unauthorized usage	The lowered barrier to creating and purchasing new cloud services, often as simple as clicking a single button, has allowed individual contractor autonomy even within the consumer organization without proper security risk analysis.	Increased surveillance and management to reduce worker autonomy in cloud services within consumer organizations.
API compromise	This data-centric issue is deathly researched. The same vulnerabilities that exist on the OS exist on the Internet through these computing platforms, exposed to widespread vulnerability exposure and potential asset compromise.	
Cross-consumer exploitation	This regards a cloud provider's infrastructure. Just as these vulnerabilities can be specific to the API, they are just as easily exploitable through an attack that is referred to as a "multi-tenant" attack, creating massive security failures and data leaks.	No attacks have currently resulted from "logical separation failure", but have been simulated successfully.
Incomplete data wiping	Especially regarding research organizations and medical organizations that require legally secure data storage options, secure data deletion is mandated. However, consumers and organizations do not have full control of the deletion protocol and are often unable to verify it as such.	Cloud services intended for these organizations that require increasing levels of security upon deletion and confirmation exist as a marketable product.
Stolen credentials	This is one of the most common ways that data leaks occur through leveraging cloud computing resources. This will be explored further in the case studies below.	Ensuring that Cloud service provider worker credentials are tightly monitored will help minimize this occurrence.
Lost data	Lost data may not occur as a result of a malicious attack, but rather a failure to retain encryption protocols or permanent accidental deletions, or improper use of the model.	

7. Insufficient Identity, Credential, and Access Management

Weak identity, credentials, and access management can allow unauthorized individuals access to sensitive data. Such breaches can lead to financial losses, intellectual property theft, and even regulatory penalties. To guard against this, organizations should enforce strict access controls, multi-factor authentication, and regular audits to track and manage data access.

8. Insecure APIs

Cloud services often provide APIs for users. If these APIs are not secure, they can be exploited by attackers to gain control of the system. Potential impacts include data loss, breach of privacy, and system failures. The defense against this involves regular vulnerability scanning, penetration testing, and ensuring APIs are designed with security in mind.

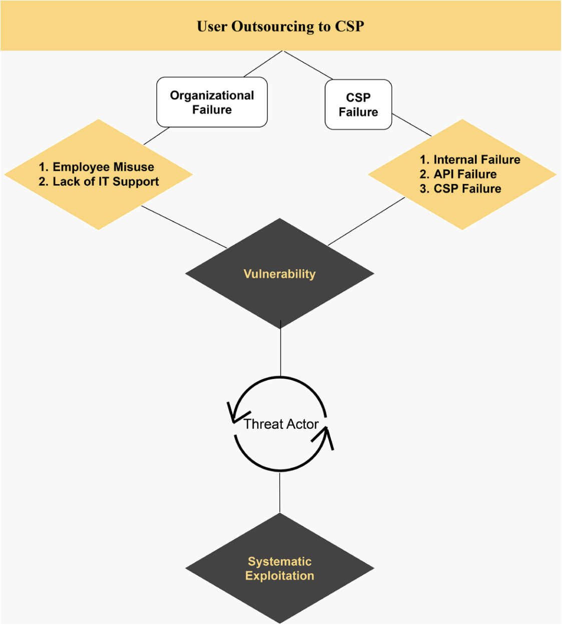

Figure 2. Organizational CSP exploitation model.

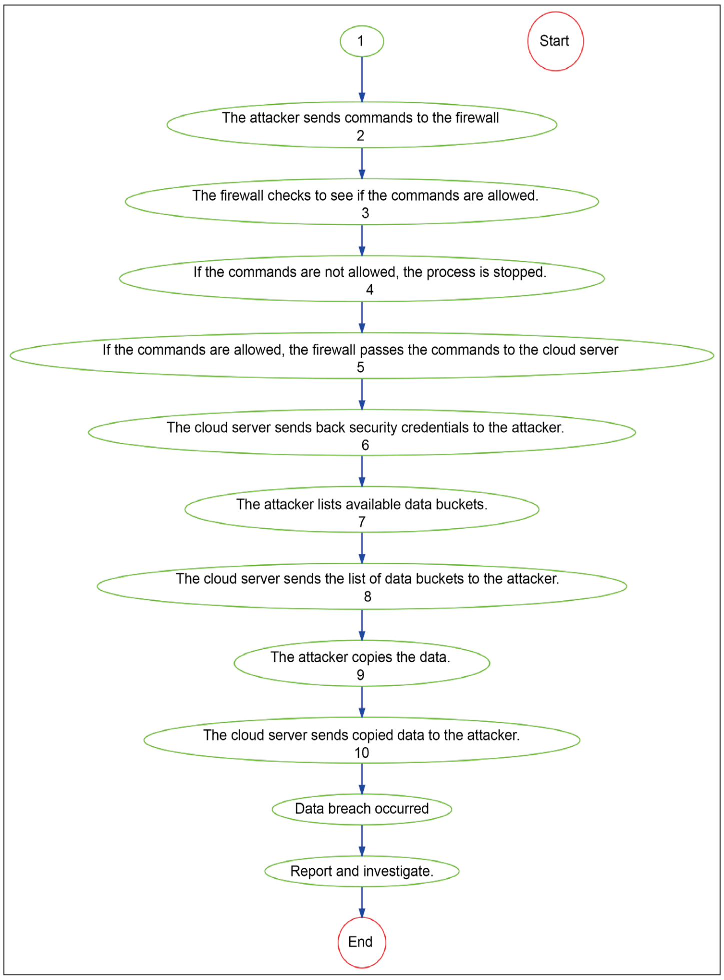
1
Start
The attacker sends commands to the firewall
2
The firewall checks to see if the commands are allowed.
3
If the commands are not allowed, the process is stopped.
4
If the commands are allowed, the firewall passes the commands to the cloud server
5
The cloud server sends back security credentials to the attacker.
6
The attacker lists available data buckets.
7
The cloud server sends the list of data buckets to the attacker.
8
The attacker copies the data.
9
The cloud server sends copied data to the attacker.
10
Data breach occurred
Report and investigate.
End

Figure 3. General data breach flowchart.

9. System Vulnerabilities

System vulnerabilities are flaws in system design that can be exploited by attackers. These vulnerabilities can lead to system failures and data breaches. A mitigation approach is the use of security configurations and patch management.

10. Account Hijacking

Account hijacking involves gaining control of a user's account. The consequences can range from unauthorized transactions to extensive data loss. Defense methods include implementing strong password policies, multi-factor authentication, and monitoring for suspicious activities.

In summary, while cloud computing brings a host of benefits, it is not without its security risks and vulnerabilities. Organizations need to be aware of these threats and take proactive measures to mitigate them, thereby ensuring their data remains secure in the cloud. The proposed model in this paper aims to serve as a guide for organizations in implementing these security measures effectively. Further case studies will elaborate on the practical application and effectiveness of this model.

11. Case Study Analysis: Capital One's Cloud Security Breach

Capital One experienced a significant cloud security breach between March and July of 2019, compromising the personal data of approximately 100 million customers. This incident underscores the dangers of managing sensitive data in the cloud and the risks associated with third-party service providers [17].

12. Cause of the Attack

The investigation revealed that the breach was due to a firewall misconfiguration as detailed in **Figure 4**. This allowed commands to be executed by a server, thereby gaining access to data in Capital One's storage space at the cloud computing company. The attacker, Paige Thompson, used a combination of four software commands to access and copy data over to her personal server, most of which were credit card applications.

13. Impact of the Attack

The Capital One breach led to significant reputational damage for the financial institution and exposed it to potential regulatory penalties. More importantly, it jeopardized the trust of millions of customers, whose personal data was compromised, thereby increasing the risk of identity theft and other forms of financial fraud.

14. Recommended Measures

From this incident, several key recommendations can be derived for improving cloud security:

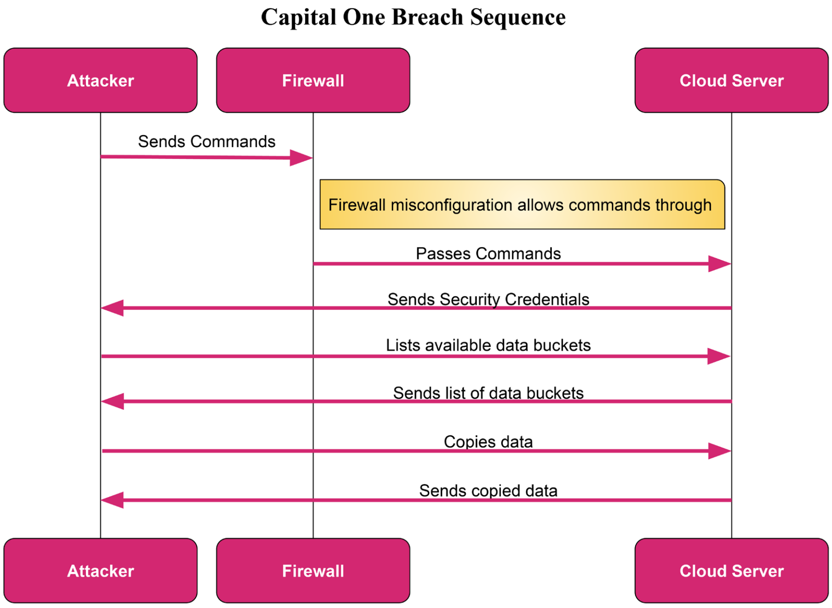
Capital One Breach Sequence
Attacker
Firewall
Cloud Server
Sends Commands
Firewall misconfiguration allows commands through
Passes Commands
Sends Security Credentials
Lists available data buckets
Sends list of data buckets
Copies data
Sends copied data
Attacker
Firewall
Cloud Server

Figure 4. Data breach Web sequence diagram.

1) Encrypt Sensitive Data: Although Capital One utilized encryption, the attacker managed to decrypt the information. This highlights the need for advanced encryption methods and techniques to protect sensitive data.

2) Implement Zero Trust Principle: The Zero Trust principle assumes that breaches are inevitable and verifies every request as though it originates from an open network. Regardless of where the request originates or what resource it accesses, Zero Trust teaches to "never trust, always verify".

3) Mitigate Server-side Request Forgery (SSRF) Attacks: Organizations should review and implement OWASP mitigation techniques for SSRF cyberattacks to ensure their servers are safe from such threats.

4) Use Code Analysis Tools: Static and/or dynamic code analysis tools can help identify vulnerabilities in the code before being sent to production, reducing the likelihood of breaches.

5) Implement Key/Secret Management Tools: Tools like KeePass or LastPass can help manage and secure digital passwords, providing an additional layer of security.

6) Establish Internal Security Boundaries: Creating security boundaries and internal firewalls can prevent a single attack from compromising an entire network by establishing different security zones.

This case study offers invaluable insights into the potential risks and security vulnerabilities associated with cloud computing, emphasizing the need for organizations to be proactive in their defense strategies. The proposed model in this paper offers a blueprint for such proactive measures.

15. Discussion

The literature review has established that the benefits of cloud computing have led to a relative lack of consumer understanding regarding personal and organizational responsibility for vulnerabilities within CSP infrastructure. Understanding the threat actors present and identifying the vulnerabilities can address the issues as well as mitigate these risks in a manner that is proactive rather than reactive. To address the vulnerabilities above, we created an organizational model to better inform choices from the consumer and CSP points. This will be split into a two-pronged approach to evenly distribute responsibility in hiring and moving forward with an organizational contract for additional cloud services, avoiding the numerous issues detailed above.

16. Model

The model will focus on two areas, which are offensive and defensive cybersecurity as follows and detailed in Figure 5.

16.1. Defensive

1) **Vulnerability Assessment and Penetration Testing.** It is essential to assess the vulnerabilities and remediate them in a timely manner. [18] Kritikos *et al.* addressed the significance of connecting vulnerability management to the application lifecycle to highlight the exact moments where application vulnerability assessment must be performed.

2) **Ethical Hacking and Risk Avoidance.** According to Chow [19], ethical hacking and penetration testing should be considered an efficient and effective means to mitigate and close security gaps and deficiencies before malicious hackers can exploit them. There are three main approaches to penetration testing, or pentesting.

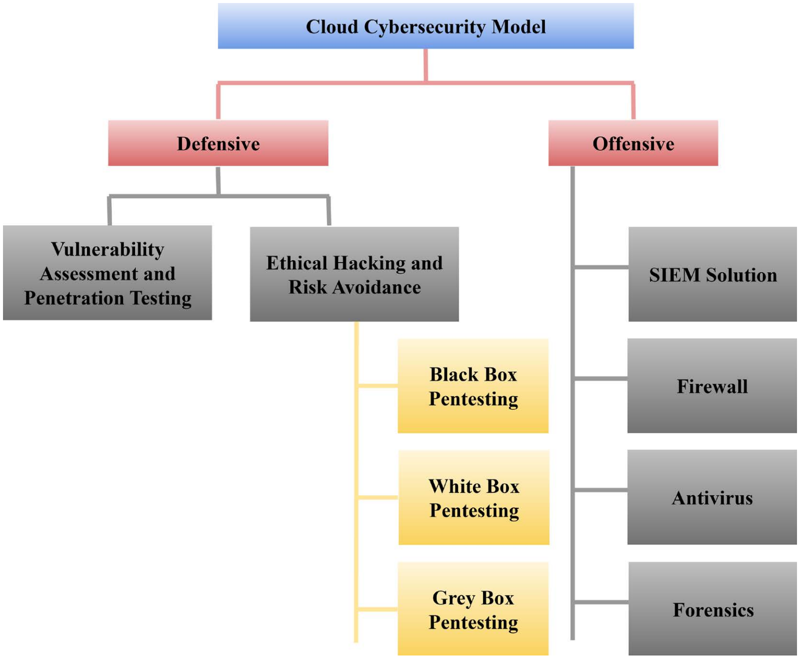

Figure 5. Cloud cybersecurity model.

- **Black Box Pentesting.** Penetration testers are given no inside information about the system (other than the information available publicly online) and are told to try to hack into the cloud. In this way, testers are placed in the same scenario as ordinary hackers.
- **White Box Pentesting.** All information about the cloud, regardless of its publicity, is given to penetration testers to try to hack into the cloud. In this way, more vulnerability can be found. However, this contrasts black box pentesting in which penetration testers may approach finding vulnerabilities differently than hackers without inside information.
- **Gray Box Pentesting.** As an intermediate between black box and white box pentesting, gray box pentesting provides penetration testers with some of the information of the cloud, but not all.

16.2. Offensive

1) SIEM solutions. According to Pourmajidi *et al.* [20], it is essential to define the health state of the cloud, create unified monitoring environments, and establish a high availability strategy.

2) Firewall Upgrade. [21] Myllykangas suggested that it is essential to integrate antivirus in the cloud production environment from the beginning to mitigate the risk of cyberattacks.

3) Forensics and Antivirus. Organizations must create an Incident Response, test the plan, and automate its implementation. This can be followed by conducting digital forensics. [22] Guo *et al.* illustrated the difference between traditional IR and cloud IR. The author addressed that cloud computing is a new battlefield of cybercrime and a new ground for novel investigative approaches.

Advantages, Application Prospects, and Future Directions of the Proposed Cloud Security Model

Advantages of the Proposed Cloud Security Model:

1) Proactive Defense: The proposed model provides a proactive approach to cloud security, helping to identify and fix vulnerabilities before they can be exploited.

2) Comprehensive Coverage: By considering various aspects such as data encryption, the Zero Trust principle, mitigation of SSRF attacks, use of code analysis tools, and internal security boundaries, the model provides a comprehensive approach to cloud security.

3) Adaptability: The model's inherent flexibility allows it to adapt to different organizational needs and cloud infrastructures.

4) Scalability: The proposed model's framework and principles can be scaled up or down based on an organization's size and requirements, making it relevant for both small and large businesses.

Application Prospects:

The proposed cloud security model can be applied in any sector that uses cloud computing services. These include but are not limited to:

- Banking and finance sector: Financial institutions that store and process vast amounts of sensitive data could benefit immensely from the proposed model.
- Healthcare industry: With increased digitization, healthcare providers are increasingly moving towards cloud solutions for storing patient data, where the model can provide robust security.
- Retail industry: E-commerce platforms can implement the model to ensure safe transactions and secure customers' personal and credit card information.

Future Research Directions:

Several avenues for future research emerge from the proposed model. These include:

1) Automation of security measures: Future research could focus on the automation of the proposed security measures, using machine learning and AI. This can improve the efficiency and effectiveness of these measures.

2) Adapting the model for specific sectors: Future research could explore adaptations of the model for specific sectors, such as healthcare, finance, or retail. Each sector has unique security requirements, and customizing the model for each could provide additional benefits.

3) Measuring the effectiveness of the model: Future studies could also consider empirical testing of the model's effectiveness across different organizations and sectors. This will help refine the model and increase its efficacy.

17. Conclusions

In this paper, we have explored the principal vulnerabilities and risks that target cloud environments and proposed a comprehensive cybersecurity model to address these challenges. Through the analysis of a case study and a review of relevant literature, we have developed a Cloud cybersecurity model that encompasses both offensive and defensive strategies. By adopting this model, organizations can enhance their ability to identify and mitigate vulnerabilities in their cloud environment, thereby improving their overall security posture.

The proposed model emphasizes the importance of proactive measures such as vulnerability assessment, penetration testing, ethical hacking, and risk avoidance. It also highlights the significance of implementing security measures like SIEM solutions, firewall upgrades, and incident response planning. Additionally, the model emphasizes the need for continuous monitoring, encryption of sensitive data, and adherence to security best practices such as the Zero Trust principle and OWASP mitigation techniques.

Limitations

While this study provides valuable insights into cloud security, there are certain limitations that should be acknowledged. Firstly, the lack of quantifiable analysis regarding the most common vulnerabilities and issues is a limitation. Future research should focus on conducting more extensive quantitative studies to identify and prioritize the most prevalent risks in cloud environments.

Furthermore, the case study analysis presented in this paper provides a specific example of a security breach but may not cover the full spectrum of potential attack scenarios. Additional case studies and real-world examples can be explored to further validate and strengthen the proposed model.

In conclusion, this paper contributes to the understanding of cloud security risks and provides a comprehensive model for organizations to enhance their cloud security posture. It highlights the importance of proactive security measures, continuous monitoring, and adherence to industry best practices. Future research should build upon these findings to develop more robust and quantifiable approaches to address cloud security challenges.

Acknowledgments

I would like to acknowledge Mitali Sakharkar for her editorial insights.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] Shaikh, F.B. and Haider, S. (2011) Security Threats in Cloud Computing. 2011 *International Conference for Internet Technology and Secured Transactions*, Abu Dhabi, 11-14 December 2011, 214-219.

[2] Dudin, E.B. and Smetanin, Y.G. (2011) A Review of Cloud Computing. *Scientific and Technical Information Processing*, **38**, 280-284. https://doi.org/10.3103/S0147688211040083

[3] The 2021 AWS Cloud Security Report. Fidelis Cybersecurity. https://fidelissecurity.com

[4] Galiveeti, S., *et al.* (2021) Cybersecurity Analysis: Investigating the Data Integrity and Privacy in AWS and Azure Cloud Platforms. In: Maleh, Y., *et al.*, Eds., *Artificial Intelligence and Blockchain for Future Cybersecurity Applications*, Springer, Cham, 329-360. https://doi.org/10.1007/978-3-030-74575-2_17

[5] Carlin, S. and Curran, K. (2013) Cloud Computing Security. In: Curran, K., Ed., *Pervasive and Ubiquitous Technology Innovations for Ambient Intelligence Environments*, IGI Global, Hershey, 12-17. https://doi.org/10.4018/978-1-4666-2041-4.ch002

[6] Zissis, D. and Lekkas, D. (2012) Addressing Cloud Computing Security Issues. *Future Generation Computer Systems*, **28**, 583-592. https://doi.org/10.1016/j.future.2010.12.006

[7] Diogenes, Y. and Ozkaya, E. (2018) Cybersecurity? Attack and Defense Strategies: Infrastructure Security with Red Team and Blue Team Tactics. Packt Publishing Ltd., Birmingham.

[8] AWS. Shared Responsibility Model—Amazon Web Services (AWS). https://aws.amazon.com/compliance/shared-responsibility-model/

[9] Mather, T., Kumaraswamy, S. and Latif, S. (2009) Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance. O'Reilly Media, Inc., Sebastopol.

[10] Fahmideh, M., *et al.* (2020) Cloud Migration Process a Survey Evaluation Framework and Open Challenges. https://arxiv.org/ftp/arxiv/papers/2004/2004.10725.pdf

[11] Loaiza Enriquez, R. (2021) Cloud Security Posture Management/CSPM in Azure. https://www.theseus.fi/handle/10024/504136

[12] Top Cloud Security Concerns Worldwide 2021. Statista, 19 June 2023. https://www.statista.com/statistics/1172265/biggest-cloud-security-concerns-in-2020

[13] Suryateja, P.S. (2018) Threats and Vulnerabilities of Cloud Computing: A Review. *International Journal of Computer Sciences and Engineering*, **6**, 297-302. https://www.researchgate.net/profile/Pericherla-Suryateja/publication/324562008_Threats_and_Vulnerabilities_of_Cloud_Computing_A_Review/links/5ad5bf9d458515c60f54c714/Threats-and-Vulnerabilities-of-Cloud-Computing-A-Review.pdf https://doi.org/10.26438/ijcse/v6i3.297302

[14] Agarwal, A. and Agarwal, A. (2011) The Security Risks Associated with Cloud Computing. *International Journal of Computer Applications in Engineering Sciences*, **1**, 257-259. https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.207.9119&rep=rep1&type=pdf

[15] Faatz, D. (2018, March 12) Best Practices for Cloud Security. SEI Blog. https://insights.sei.cmu.edu/blog/12-risks-threats-vulnerabilities-in-moving-to-the-cloud

[16] Swiss Cyber Institute (2021, November 25) 21 Cloud Security Statistics You Probably Didn't Know. https://swisscyberinstitute.com/blog/21-cloud-security-statistics-you-probably-didnt-know

[17] Cipher (2019, August 30) Analysis of a Cyber Attack: Capital One. Cipher. https://cipher.com/blog/analysis-cyber-attack-capital-one

[18] Kritikos, K., *et al.* (2019) A Survey on Vulnerability Assessment Tools and Databases for Cloud-Based Web Applications. *Array*, **3**, Article ID: 100011. https://doi.org/10.1016/j.array.2019.100011

[19] Chow, E. (2011) Ethical Hacking & Penetration Testing. No. AC 626, University of Waterloo, Waterloo.

[20] Pourmajidi, W., *et al.* (2018) On Challenges of Cloud Monitoring. https://arxiv.org/abs/1806.05914

[21] Myllykangas, T. (2016) Integrating Next-Generation Firewalls into a Private Cloud Datacenter. https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=Integrating+Next-Generation+Firewalls+into+a+Private+Cloud+Datacenter.&btnG=

[22] Guo, H., Jin, B. and Shang, T. (2012) Forensic Investigations in Cloud Environments. 2012 *IEEE International Conference on Computer Science and Information Processing* (*CSIP*), Xi'an, 24-26 August 2012, 248-251. https://doi.org/10.1109/CSIP.2012.6308841