



University of Wales
Trinity Saint David
LONDON

Case: Security Challenges in Amazon web Services & Microsoft-Azure Risks, Vulnerabilities, and Mitigation Strategies

Id:2505521

Submitted By: Shahriar Badhan

Submitted To: Suresh Shanmugasundaram

Table of Contents

List of Figures	29
-----------------------	----

List of Tables	26
----------------------	----

Abstract	4
----------------	---

1. Introduction	5
------------------------------	----------

1.1 Context and Background	5
1.2 Research Problem	6
1.3 Research Aim and Objectives	7
1.3.1 Aim	7
1.3.2 Objectives	8
1.4 Significance of the Research	10

2. Literature Review	12
-----------------------------------	-----------

2.1 Inception	12
2.2 Cloud Security Overview	13
2.3 Security Challenges in AWS	14
2.4 Security Challenges in Azure	15

2.5 Research Gaps	16
--------------------------------	-----------

2.5.1 Misconfiguration Detection Automation Gap	16
2.5.2 Shared Responsibility Model Confusion	17
2.5.3 Multi-Cloud Security Complexity	18
2.5.4 Real-Time Threat Detection Differences	19
2.5.5 Identity and Access Management (IAM) Weakness	20

2.5.6 User-Centric Security Design Gap	21
2.5.7 GDPR Compliance Challenges	22
2.6 Literature Summary	23

3. Research Design and Methodology 24

3.1 Research Design	24
3.2 Research Methods	25
3.2.1 Qualitative Methods: Case Study Analysis	25
3.2.2 Quantitative Methods: Performance Evaluation	26
3.3 Research Strategy	27
3.3.1 Comparative Analysis	27
3.3.2 Case Study Evaluation	28
3.3.3 Security Framework Assessment	28
3.4 Data Analysis	29
3.5 Materials	30
3.5.1 Data Sources	30
3.5.2 Software Tools	31
3.5.3 Hardware Requirements	31

4. Expected Outcomes 32

4.1 Identification of Key Vulnerabilities	32
4.2 Comparative Security Insights	32
4.3 Development of Mitigation Strategies	32
4.4 Contribution to Research and Practice	33

5. Timeline	34
6. Conclusion	35
7. References	36

Abstract

Cloud computing is a foundation of modern digital infrastructure; it enables organizations, and sometimes even entire economies that scale up quickly across the world with ease. Major cloud platforms like Amazon Web Services and Microsoft Azure control almost everything in the global cloud ecosystem, delivering both service portfolios as well as integrated security mechanisms. Even with these advancements, however, cloud environments are still susceptible to some of the same security issues they have always confronted -- such as misconfigurations between the development and production environment or weaknesses in identity and access management processes-- along a host of emerging threats.

Abstract: The objective of this research is to perform a complete comparative analysis between AWS and Microsoft Azure systems in terms security challenges by exploring their security architecture, vulnerabilities and current existing mechanisms needed. The study identifies important research opportunities, including automated detection of misconfiguration, uncertainty in the shared responsibility model of CSPs (Cloud service providers), complexity and risks inherent to multi-cloud environments, comparative assessment drawbacks related to real-time threat discovery capabilities among several cloud platforms and identity & access management shortcomings. The research also investigates end-user device and user-centred security design challenges, as well as those governing compatibility with GDPR requirements.

A mixed-method strategy is employed, whereby qualitative case study that relies on quantitative outcome measurement regarding business performance. Expected outcome: Provisioning mitigation strategies and contributing to the improvement of cloud security best practices across various on-premise/cloud environments.

1.Introduction:

1.1 Context and Background

Cloud computing is an ever-evolving field which has been changing the way how businesses manage IT infrastructure. Cloud-based platforms deliver on-demand access to computing resources that will continue to replace traditional, often outdated or expensive on-premise systems. This is driven by the requirement for scalability, flexibility and cost optimization.

Amazon Web Services (AWS) and Microsoft Azure, in that order are the two most popular adoption of cloud service within top providers. AWS has such a larger repertoire of services in areas like computing storage networking and analytics, whereas Azure provides strong enterprise integration hybrid cloud capability.

On the other hand, migrating to a cloud computing environment poses additional threats to security. Cloud environments follow a shared responsibility model instead of traditional systems. Having that model can confuse and cause the misconfiguration [1].

In addition to this, cloud environments are dynamic and tightly-scalable resulting in a higher potential for configuration errors. It has also been found that misconfigurations are one of the leading cause for cloud security breach [2]. The increasing sophistication of cyber attacks threatens the presence of secure clouds, such as ransomware and advanced persistent threats [3].

The growing prevalence of adopting multi-cloud strategies, where organizations will utilize a number of providers e.g. AWS and Azure does not make things less complex by any means! Persistent policies and integration is lacking across platforms for managing security [4].

1.2. Research Problem

Even though there are advanced security tools and frameworks offered by AWS, Azure et al., organizations have faced plenty of security incidents. In the majority of cases, these incidents are not because there is a flaw in the platforms themselves but rather that security controls were either improperly implemented or lost track over time.

Problem

Statement:

Organizations continue to struggle protecting cloud environments on AWS and Azure as the prevalence of misconfigurations, complex security architectures, unclear distribution of responsibility, and a shifting threat landscape rattle enterprise confidence.

This problem is made more complex when you consider a few different things. Security and expert configuration Because cloud systems require expertise to configure, issue No. Many businesses do not have the skills to configure them correctly. Second, the shared responsibility model causes confusion and leads to security gaps in implementation. Third, these days cyber threats are constantly becoming more advanced, by developing new forms of attack strategies they deprive organizations from compacting them.

Additionally, as more organizations transition into multi-cloud environments there arise challenges such as consistent policy and integration. On the other hand, previous studies mainly investigate different aspects of cloud security and are not comparative between AWS and Azure.

1.3 Research Aim and Objectives

Aim

The main objective of this study is to perform a comparative critical analysis on security threats in leading cloud computing platforms i.e., Amazon Web Services and Microsoft Azure along with proposing practical, efficient mitigation strategies that can improve the real threat levels found in some existing clouds.

The reason for this objective is the increasing adoption of cloud functions among industries which has created a new set of multifaceted security challenges like misconfiguration, identity problems and advanced cyber-attacks. However, organization witnesses breaches in the availability and confidentiality of such component due to improper implementations and lack of awareness about security mechanisms provided by both these platforms [2], [3]. Hence, this research also aims to provide practical solutions along with the challenges that it seeks to analyze and gaps in existing cloud security practices.

Objectives

1. To analyze the security architectures of AWS and Azure

This goal examines the security frameworks, models and mechanisms both AWS and Azure have put in place. This involves assessing elements like IAM, encryption methods, network security controls again and monitoring strategies.

The architecture understanding is very important since security in cloud computing actually depends upon the design and integration of these components. For example, AWS offers a shared responsibility model with fine-grain IAM controls whereas Azure has strong integration into enterprise identity systems like Active Directory [5], [9]. Through this analysis of these architectures, the research will also be able

to discern structural strengths and weaknesses that factor into overall security success.

2. To identify key vulnerabilities and threats in cloud environments

The purpose of that objective is to identify and classify the most frequent types of security vulnerabilities in AWS and Azure environments. Some of these are things like misconfigured storage systems, insecure APIs even weak authentication mechanisms and insider threats.

One common reason for data breaches [2], [7] is misconfiguration and cloud environments are more susceptible to this type of attacks. Further, the ever-growing complexity of cyber threats such as ransomware and advanced persistent attacks (APTs) continues to be an important risk in cloud system [3]. The identification of these vulnerabilities forms the basis for targeted security solutions.

3. To evaluate existing security tools and mechanisms

AWS and Azure both have a set of security tools like AWS GuardDuty, AWS IAM, Azure Defender and Azure Active Directory. The goal of this is to test how well these tools can perform security detection, prevention and response.

The assessment will take into account usability; scaling; integration capabilities and real-life utility. These tools are intended to enhance security but their usefulness depends mainly on the right configuration and operation [8], [10]. As a result, this study will examine in critical light whether these tools provide capabilities appropriate to meet the demands of contemporary security environments.

4. To compare real-time threat detection capabilities

One of the most important capabilities in computer security is real-time threat detection, which provides organizations with a way to respond quickly to attacks. This compares threat detection capabilities and accuracy, response time of the tools on AWS vs Azure as well false positive rates.

Both platforms offer a positive scoring system and advanced monitoring, but little comparative analysis work has been done to indicate performance under similar scenarios [12]. The objective of this comparison is to assess both systems and understand how either platform performs concerning improving the detection ability of methodical threats.

5. To investigate critical research gaps in cloud security

This objective is intended to systematically identify and qualitatively evaluate the literature focusing on gaps in research pertaining cloud security, particularly with reference to leading platforms such as Amazon Web Services and Microsoft Azure. Related studies usually investigate isolated matters without providing panoramic and practical solutions to the impact of cloud security issues even though a lot of research on this topic has already been done.

One of the biggest gaps that have been identified from literature, is automated misconfiguration detection systems. CLOUD SECURITY BREACHES: Misconfiguration is still the most common cause behind cloud security breaches, often a result of human error or lack of proper expertise Current tools can monitor IT assets but are mostly reactive and require a human to intervene. It should be noted that there is still little research on intelligent, automated solutions for their timely and proactive detection and rectification of ongoing misconfigurations [14].

One major gap is the misunderstandings around the shared responsibility model. Though this model articulates a clear demarcation of security duties between cloud providers and users, it is not adhered to by many organizations. This misconception

results in security holes, especially around data protection and access control. Although existing literature explains the concept theoretically, it is underexplored in terms of practical implementation.

The growing use of multi-cloud environments, on the other hand, have added another level of complexity with rather limited research in this field. Dealing with different configurations, policies and tools across multiple platforms is often problematic for security management yielding inconsistencies that can lead to increased vulnerabilities. Many existing works target to secure single-cloud environments and therefore lack unified multi-cloud security frameworks [4], [11].

Another field that sees big gaps is identity and access management (IAM). While AWS and Azure have both added comprehensive IAM systems, many organizations still face challenges such as over-provisioning permissions, weak authentication practices, and poor policy management. In addition, the number of studies about predictive & behaviour-based IAM system that detects anomalies and prevents unauthorised access before it happens is limited [13].

Furthermore, we see a distinct absence of user-centric design in cloud security tools. Most security solutions are essentially very high-tech and difficult to use which leads to greater chances of human errors. While usability is a key factor of security, it has so far been somewhat overshadowed in an essential research aspect. User experience design could lower the risk of incorrect configurations and influence general security effectiveness [14].

Lastly, current cloud environments are still lacking in scalability and able to keep with various regulatory requirements (e.g. GDPR). Cloud systems are by nature distributed, which makes them difficult to monitor and manage for compliance - an area where most organizations apply consistent standards across multi- or hybrid-cloud environments. Although the existing literature does highlight these challenges, it provides little guidance on practical implementation methods and especially encourages data residency measures as well as auditability [15].

In summary, past work has largely concentrated on measuring individual security issues instead of solutions — especially holistic and scalable ones. The aim of this research is to fill these gaps and provide an integrated view on cloud security as well

as actionable insights that both academics can build upon, but also practitioners during their day-to-day live.

6. To propose practical and scalable mitigation strategies

Finally, the goal is to establish appropriate preventive actions following these results. The purpose of these strategies is to mitigate down those vulnerabilities tracked in the cloud security.

Proposed solutions may include:

- Automated tools for misconfiguration detection
- More majority IAM tablets and least-privilege accessibility control
- Platform Security Architectures for Multi-Cloud
- Improve real time inspection examinations and hazard recognition devices

The strategies have been designed to be practical and scalable, so that organizations of any size can implement them. This goal emphasises real-world applicability so that the research meets academic as well in industry significance.

1.4 Significance of the Research

This research is significant due to its contribution in solving both theoretical and practical problems related to cloud security in contemporary computing surroundings. With organizations now relying more than ever on cloud platforms like Amazon Web Services and Microsoft Azure, maintaining strong security is a top priority. However, although such tools are much more advanced and sophisticated today than they were a decade ago or two decades previously – many

organizations still face data breaches and security incidents through misconfigurations, weak access control etc. [2], [3].

This research thus offers perspectives from the industry on the real-world security challenges confronting actors of cloud environments. It identifies the most exploited vulnerabilities and compares AWS with Azure in terms of potential effectiveness of their security mechanisms, helping organizations choose among different cloud services for effectively managing them. In addition, many of the proposed mitigations—including automated misconfiguration detection and more comprehensive identity and access management policies as well as improved threat detection systems—can help organizations strengthen their security posture. It is highly relevant in the light of rising cyber threats and compliance pressures, with cost implications due to data breaches or regulatory fines [1], [2].

This study adds value to the body of knowledge as there are many unexplored areas that this research is trying to discover. Previous research has primarily analyzed more general issues of security, with only a limited amount of comprehensive comparative work being performed on AWS and Azure relating to real-time threat detection or multi-cloud complexity, cyber-physical systems (CPS), human factors in cybersecurity, etc. The research not only fills these gaps but also paves way for future cloud security studies [4], [11].

Additionally, this paper is also valuable in addressing emerging data issues related to multicloud infrastructure, digital-decoupling etc and regulatory compliance (GDPR). With the growing adoption of multi-cloud strategies among organizations, securing multiple platforms often makes security more complex. Our work emphasizes the necessity for consolidated security frameworks and serves as a guide to how those would solve such challenges [15].

The study also underlines automation with usability in cloud security. A lot of those security blunders are actually human error; particularly when it comes to configuring cloud resources properly. This study takes the approach of identifying solutions with automation and user-friendly designs to minimize these errors and improve overall system reliability [14].

In summation, the importance of this research can be explained through both academic and industrial implications. In addition to deepening theoretical insights associated with cloud security challenges, it also presents actionable guidance applicable in practice. The results of this research will be very critical in supporting secure and efficient cloud adoption as the area of Cloud Computing continues to evolve.

Comparative Security Features Table

Feature	Amazon Web Services	Microsoft Azure
Identity Management	AWS IAM (fine-grained control)	Azure Active Directory (enterprise integration)
Threat Detection	Guard Duty (AI-based monitoring)	Azure Defender (integrated security analytics)
Data Encryption	Server-side & client-side encryption	Encryption at rest & in transit
Compliance	Wide range (ISO, GDPR, HIPAA)	Strong enterprise compliance support
Monitoring	CloudWatch	Azure Monitor
Multi-cloud Support	Limited native support	Better hybrid integration

2. Literature Review

2.1 Inception

This literature review will critically analyze the existing researched information associated with cloud security, specifically surrounding such platforms as Amazon

Web Services and Microsoft Azure. A significant number of research works focus on various aspects of addressing the security concerns in cloud computing as its facilities evolve, but these findings are often quite focused and fragmented rather than establishing comparative perspectives.

This section will summarize major themes, trends and arguments from previous research but it will also highlight gaps within the academic literature that warrant this research. The reviewed literature deals with development of basic cloud computing theories, practical security problems and recent solutions on cloud security mechanisms. They focus especially on topics like misconfiguration, identity and access management, real-time threat detection along with multi-cloud security complexities.

Moreover, this review includes an evaluation of both academic research and industry reports to provide a balanced insight on theoretical concepts as well as real-world applications. This section reviews the existing literature regarding previous studies in order to build on a solid background for what this research implements and where more work needs to be done.

2.2 Cloud Security Overview

Cloud security is a concept that includes numerous policies, technologies and control plans designed to protect cloud based systems like servers, storage and applications from potential threats, breaches or unauthorized access. Cloud computing is very different from a traditional IT environment where data and assets were all local to one physical machine, so it introduces its own unique set of security challenges that need addressing.

Mell and Grance [5] define cloud computing as a solution with on-demand self-service, resource pooling and rapid elasticity. These features not only help in flexibility and efficiency but also are a result on vulnerabilities as the infrastructure

is shared using multi-tenancy. Therefore, it becomes more difficult to preserve data privacy and integrity.

Third, one of the biggest challenges with cloud security comes from working within a shared responsibility model where protecting infrastructure falls on the cloud provider and applications/data fall on customers. Evading this model otherwise triggers the unmet need for security vulnerabilities [5], like access control and data protection.

Potential risks of the cloud environments are data breaches, insecure APIs, insider threats and account hijacking as well denial-of-service attacks [6]. Sensitive data breaches due to misconfigured storage or weak encryption. Another great worry is insecure APIs — entry point for many attackers. Because of the tools and access they have, insider threats — either malicious or inadvertent — are another big risk.

In addition, the fast-paced transactions in cloud technologies have given rise to sophisticated threats like ransomware or advanced persistent threat (APTs) as they take advantage on vulnerabilities during a long period of time[3]. These undermine the fact continuous monitoring and adaptive security mechanisms are a necessity.

Thus, a global reflection of the literature reveals that cloud security is not simply an IT problem but also one relating to management and governance challenge. Real security is never one core method, but a combination of strong tech with proper configuration and human general awareness.

2.3 Security Challenges in AWS

Amazon Web Services (AWS) is the most widely used cloud platform, with a complete technology stack and superior security. AWS provides tools in the form of Identity and Access Management (IAM), Virtual Private cloud (VPC) services, encryption services, Cloud Watch – monitoring tool, Guard Duty etc. The tools that fall in those categories only serve one purpose, and their objective is to improve security through more granular access control as well real-time monitoring.

However, even these robust security mechanisms are not enough to prevent issues in AWS environments. Among the most important problems in literature is misconfiguration especially for storage services like Amazon S3. There are multiple studies that have reported cases of accidental exposure of sensitive data on publicly accessible S3 buckets [7]. Many of these misconfigurations are caused by human mistakes, not the platform itself.

A key issue is identity and access management. Although the AWS IAM enables a high-resolution permission setting, it also comes with such extreme complexity that you can set too many permissions or simply do not apply least privilege. This means the possibility of unauthorized access and insider attacks [8].

Moreover, AWS environments are prone to API-based security concerns. Cloud services work mainly by using APIs to communicate; without the proper configurations, an insecure API can let attackers gain access to sensitive data or a service [17]. Thus, it is important to monitor and secure APIs as a part of the AWS security.

Lit review also indicates that real-time detection and response to threat is still not yet well founded. While AWS offers some built-in security tools like GuardDuty, they won't be effective if not properly configured and set up with other dedicated security groups as well. Organizations that choose not use these tools to their full potential will have delayed detection of threats.

So, to sum up, AWS does provide a robust security framework; however how good the implementation of these controls is dependent on the user.

2.4 Security Challenges in Azure

Another major player in the cloud space is Microsoft Azure, which has a big focus on enterprise environment integration and identity management systems. Azure has a wide variety of security services such as Azure Active Directory (AAD), Azure

Security Center & and AAD Defender. Those tools enable you to centrally manage identities, access and threats.

Great strength of azure is its identity management system integration with enterprise authentication systems. But this integration provides challenges as well. Unauthorized access to Azure Active Directory (AAD) can be the result of misconfigurations like weak authentication policies or improper role assignments [9].

The configuration complexity is another big challenge inside Azure environments. You have Azure providing a hundred or more services and settings spread among many different locations in the cloud, making it difficult to manage if your organization lacks experience. This complexity increases the risk for human error, a leading cause of security incidents [10].

We can also expect some problems with authentication and access control in Azure as well. Exploitable systems are caused by weak password policies, a lack of multi-factor authentication (MFA), and improper role-based access control (RBAC) settings. This usually goes back to security practices rather than any technical limitation.

Additionally, like AWS Azure environment also suffers from the issues of API security and data protection. Insecure APIs and poor data handling give rise to data breaches, compliance violations.

It also reinforces what the literature suggests -- that while Azure has fantastic security features, they are subject to proper implementation and constant monitoring. Due to the changing nature of threats, organizations are required to stay ahead in terms of managing configurations related to security.

2.5 Research Gaps

2.5.1 Misconfiguration Detection Automation Gap

It is a well-known fact that misconfiguration can be one of the top reasons for cloud security breaches. Large scale studies in the cloud also show that a considerable share of incidents, often 60% or more, can be traced back to misconfiguration [2], e.g. faulty storage services setup and inadvertent access control leakage across potentially open networks. Such misconfigurations are the result of human error, lack of expertise or simply the sheer complexity around cloud environments.

While there are monitoring and auditing tools offered by cloud service providers (CSPs) like Amazon Web Services, Microsoft Azure etc., they typically address security issues in a reactive fashion rather than a proactive one. Too often, vulnerabilities are found only after they have been exploited — and sometimes the software industry itself has no idea when a vulnerability is being used.

The lack of fully automated misconfiguration detection systems is an important research gap. However, these tools need manual fine-tuning and constant human supervision — a not practical solution in many scale cloud environments. Continuous monitoring and automated remediation of their configurations in real-time is incredibly valuable, which leads to an increasing need for intelligent systems that can find anomalies and apply fixes quickly. Approaches based on machine-learning would be highly useful in detecting patterns of misconfiguration and predicting environment exploits before they are used [14]. Bridging this gap would, in fact, lead to a drastic reduction of dependency on human involvement and an overall safe-based cloud environment.

2.5.2 Shared Responsibility Model Confusion

One of the basic concept related to cloud security is shared responsibility model, which means what all things falling under service provider side and what will be

customer side. Like the infrastructure is secured by providers, customers however should secure their applications and data as well access controls [5].

But studies have shown that this model is often misunderstood by organizations, with many believing the cloud provider has full responsibility for every aspect of security. This misunderstanding results in serious vulnerabilities, most notably concerning data protection, identity governance and configuration management.

While literature has explained the shared responsibility model in theory, there is not much pragmatic frameworks or tools that can help organizations implement it. Generally, most of the guidelines on cloud technology provided by providers are technical and may not make easy sense to non-expert users. This movement is not the disconnect of theory vs practical.

This suggests an urgent need for more intuitive frameworks, preparation models and automatic guidance architectures that can assist organizations comprehend their obligations. Fixing this would increase compliance, decrease misconfiguration and strengthen the overall security posture.

2.5.3 Multi-Cloud Security Complexity

Organizations uncomfortable with the thought of vendor lock in have flocked towards multi-cloud strategies and as much attention & implementation has gone into redundancy and robustness. Yet, securing multiple cloud platforms can pose significant challenges.

Every cloud provider (including Amazon Web Services and Microsoft Azure) has its own tools, policies and configuration for security. The absence of standardization complicates the task of uniformly implementing security policies across platforms [4], [11].

This leads to a greater complexity in monitoring, managing and securing an organization specific cloud environment. Another drawback of multi-framework

onboarding is the attack surface area, which draws more and better opportunities for attackers to exploit. Also, security tools tend to be intricately integrated across disparate platforms; therefore integration may be technically challenging and resource intensive.

Most existing research has addressed single-cloud environments, with a large gap in the multi-cloud security strategies. What is missing are governance and security frameworks that can work with many different platforms, unified management systems across multiple vendors. Bridging this gap will help enterprises implement uniform security policies and reduce complex operations.

2.5.4 Real-Time Threat Detection Differences

A core function of cloud security is the ability to detect threats in real time which can be crucial for organizations so they may mitigate them before it turns detrimental. AWS and Azure both offer features to detect threats which are not executable like AWS GuardDuty.

Still, relatively few attempts have been made to compare these tools against each other in terms of their performance when leading to real life decisions. In the literature, previous works typically investigate these systems in isolation [12] and do not compare their detection accuracy, response time or false positive rates head to head.

The absence of comparative analysis makes it difficult for organizations to make informed decisions when choosing a cloud platform or designing security strategies. This knowledge is critical for making better decisions, it also helps you understand how different platforms perform under similar circumstances.

Consequently, this provides a research gap that commands empirical studies assessing and comparing real-time threat detection capabilities. Such analysis would yield valuable information on strengths and shortcomings of single or multiple platforms, but also improvement in security practices.

2.5.5 Identity and Access Management (IAM) Weakness

The Identity and Access Management (IAM) service is an essential component of cloud security, as it governs who can access resources and in what capacity. Both AWS and Azure offer sophisticated IAM that facilitate very granular permissions over roles.

These capabilities did not remove IAM as a significant source of vulnerabilities. Studies show that privilege issues, weak authentication, and access control practices are the reasons for many security breaches [13]. One user may have more than he or she should based on the principle of least privilege which increases risks such as insider threats and unauthorized access.

Another drawback of existing IAM systems is that they are largely reactive, i.e. Rather than trying to predict future disasters, most systems are designed for policy enforcement. Limited research exists on the use of predictive analytics and behavioral monitoring to detect suspicious activity by users.

That leaves a huge gap in the research of cloud security. An intelligent IAM by this function will be able to analyze users' behavior and identify anomalies, which can significantly improve security and avoid possible breaches.

2.5.6 User-Centric Security Design Gap

Cloud security tools could be highly technical in nature, but usability plays a lesser role. As a result, these neuroimaging tools can be complicated to use and often less useful for non-expert users.

This complexity introduces random human errors which is one of the primary causes behind most cloud security incidents [14]. One of the most common factors is lack of understanding like misconfiguration of security settings or not applying best practices.

While usability is a critical consideration, little research has been conducted to make cloud security systems that reconcile the needs of users and others. More of the articles bring out technical improvements rather than user experience.

This gap can only be bridged using more user-friendly interfaces, easy workflow configurations, and automated suggestions. This reduces human error and helps improve overall security in organizations.

2.5.7 GDPR Compliance Challenges

Organizations working in cloud environments must comply with stringent data protection regulations like GDPR. The challenge though is exacerbated in cloud systems due to their distributed and dynamic nature.

Data, in cloud environments, may be dispersed into more than one geographical location [15], [16] and because of this it is also difficult to achieve compliance across all areas as space restrictions will differ with host locations. In addition, clouds can be tricky to configure correctly as both the cloud provider and user have responsibilities in meeting data protection standards under a shared responsibility model.

While previous research has established the need for compliance, it does not adequately capture organizational realities. For instance, there are no clear claims on how to manage and maintain data residency, auditability, and compliance in multi-cloud implementations.

This gap reveals the urgent requirement for pragmatic frameworks and tools that assist organizations in both achieving compliance and ensuring they maintain it over time.

2.6 Literature Summary

The literature that was reviewed shows there has been some progress in terms of addressing the security challenges for cloud computing, with greater advances made in encryption, identity management and threat detection. Leading cloud providers, including Amazon Web Services and Microsoft Azure, have rolled out sophisticated security controls to help secure their environments.

Yet, despite this progress large gaps still remain. They consist of poorly automated security mechanisms, limited usability of the available tools for protection against cybersecurity threats, difficulty in keeping a multi-cloud secure environment and insufficient comparison among performance about security. Also, human factors are still a big factor in security incidents as well due to hacking and misconfiguration that leads to data leakage.

In the literature, there is also plenty of mentions about the gap between theoretical research and practice. Though most of the studies address security issues, few provide things that can be done in practice.

Thus, this study intends to address the existing voids by furnishing an extensive comparative assessment of AWS and Azure accompanied with a set on practical mitigation strategies. This study indirectly supports secure cloud adoption by contributing to improvement in both technical and human factors in actual practices for security Cloud.

3. Research Design and Methodology

3.1 Research Design

We use a comparative design science research (DSR) methodology that integrates both the theoretical and practical layers when investigating tangible cloud security phenomena. Design science research aligns particularly well with this study as it does not simply describe the problems; instead, it develops and evaluates solutions (artefacts) to them. A design science approach provides for both analytical understanding and a means of practical improvement in light of the dynamic nature of security challenges associated with cloud computing.

Due to the comparative nature of this research, a systematic assessment of Amazon Web Services and Microsoft Azure security mechanisms can be accomplished. Research strives to enumerate similarities, differences and performance gaps of the security architectures you are on two platforms through critical comparisons. The importance of this is exacerbated by the rise in popularity and usage of multi-cloud environments, where organisations use multiple providers at a time [4], [11].

Additionally, this approach intertwines theoretical perspectives from prior research with empirical findings gleaned from case studies and historical evidence. Thus, we combine academic soundness with practical applicability. Using the design science approach also helps in producing mitigation strategies that can be deployed on real-world cloud environments through mitigating issues like misconfigurations and identity management vulnerabilities [2], [13].

The overall research workflow followed in this study is illustrated



3.2 Research Methods

A mixed-method will be used for this research that entails collecting qualitative and quantitative methods. This is relevant because cloud security itself is intersecting between a classic quantitative and qualitative domain, where the former may lead to more but unnecessary numbers in reports.

Qualitative Methods: Case Study Analysis

The second part of the research will focus on qualitative analysis which includes extensive review and presentation of real world case studies involving cloud security incidents. The case studies may sometimes involve publicly disclosed breaches, misconfigurations, and security issues with acute scope in AWS and Azure environments. By analyzing this, the aim is to train against how security vulnerabilities are introduced into systems in practice and exploited by attackers.

Through quantification it is possible to analyse the cause and contributions of security problems in a serial way, such as terrorism or civil disturbances; however case study analysis enables researchers to also take on an exploratory role where they evaluate how far certain qualitative data impacts this exploration (career path) [Maximizing academic potentials by choosing innovative paths]. For instance, analyzing the incidents related to misconfigured storage buckets or leaked credentials might show that human mistake lack of awareness and organization security policy contribute as a root cause [2], [7].

Qualitative analysis can also make a contribution towards better understanding the implementation challenges of this shared responsibility model. A number of organizations do not understand their security obligations or cannot accurately implement something for various reasons [5]. Using case studies, the research can spot trends and offer practical recommendations.

Quantitative Methods: Performance Evaluation

The second, quantitative part of the study will benchmark the performance of security mechanisms in AWS and Azure. This consists of quantitative metrics such as detection accuracy, response time and false positive rate.

A quantitative perspective offers an objective ground for appraising the efficacy of one security tool versus another. As an example, AWS GuardDuty and Azure Defender can be assessed on their speed and accuracy to detect potential attacks [12].

Moreover, as one of the key identified research gaps in this study is perform quantitative evaluation to assess real time threat detection capabilities. As per the suitable metrics, organizations can make a comparison of both platforms embedded in this research and it would be easier for them to decide.

The qualitative and quantitative complementary methods provide a wholistic analysis considering both the technical performance of acoustics in design, as well as practical portable implementation.

Proposed Multi-Cloud Security Architecture for AWS and Azure

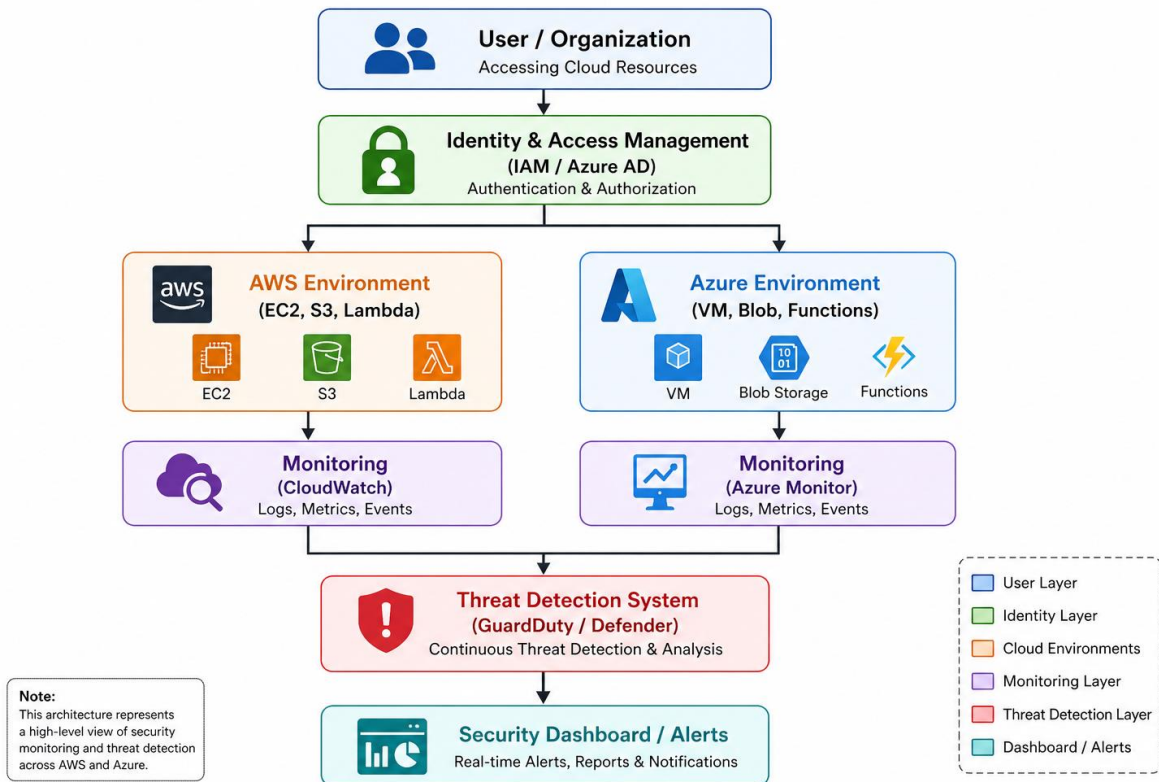


Figure: X

As shown in Figure X, the system integrates identity and access management with cloud environments and monitoring tools to enable centralized threat detection. This architecture supports comparative evaluation of AWS and Azure security mechanisms.

3.3 Research Strategy

The research strategy is structured around three key components: **comparative analysis, case study evaluation, and security framework assessment.**

Comparative Analysis

The main methodology of this research is directly comparing AWS and Azure security features. It includes methodical evaluation of multiple components of cloud security such as identity management, data protection, threat detection and compliance mechanisms.

In order to identify the strengths and weaknesses of each platform, comparative analysis is critical. AWS might provide more robust monitoring tools, for example; while Azure may better integrate with enterprise identity systems [13]. It is important to understand these differences especially for organizations running multi-cloud environments [4].

Case Study Evaluation

Study evaluation helps situate the comparative analysis within a real-world context. By surveying recorded security incidents, the research seeks to highlight vulnerabilities that commonly arise and assess how they are mitigated on various platforms.

It also serves to validate theoretical findings. For example, if the literature shows that misconfiguration is a significant threat domain then case studies can provide evidence [2].

Security Framework Assessment

The research will evaluate current security frameworks and guidelines as provided by AWS, Azure. This involves looking into their compliance standards, risk management strategies and security best practices.

Understanding the compliance of these platforms with common industry standards such as NIST and GDPR [5], [15] is important for assessing frameworks. Identify implementation gaps, especially in the areas of compliance and users' responsibilities.

3.4 Data Analysis

Data analysis in this research will focus on evaluating security performance using specific metrics. These metrics provide a structured way to compare AWS and Azure and assess their effectiveness.

Detection Accuracy

Detection of Accuracy means it helps the security system to identify threats correctly. High precision is crucial to avert attacks, as false negatives (missed threats) may pose severe and detrimental security breaches [12].

False Positive Rate

False Positive Rate: The false positive rate is an indicator of how often a system will incorrectly detect normal activity as a threat. The usefulness of system could be determined by the true positive while A high false positive rate decreases confidence in the system and increases operational demand as security teams expend resources chasing unnecessary alerts [14].

Response Time

Response time refers to how quickly a system reacts to a detected threat. In cloud environments, where attacks can spread rapidly, fast response times are critical for minimizing damage [3].

Vulnerability Frequency

This metric measures how often vulnerabilities occur within a system. It provides insight into the overall security posture of a platform and highlights areas that require improvement [1].

By analyzing these metrics, the research can provide a comprehensive evaluation of cloud security performance and identify areas for improvement.

3.5 Materials

Data Sources

The research will rely on multiple data sources to ensure a comprehensive analysis:

- Academic journals and conference papers provide theoretical insights into cloud security challenges [6], [7]
- Industry reports from organizations such as IBM, Cisco, and ENISA offer real-world data on security incidents and trends [2], [3]
- Official documentation from AWS and Azure provides detailed information on security features and best practices [8], [9]

Using diverse data sources enhances the reliability and validity of the research findings.

Software Tools

The study will utilize various software tools for data analysis and evaluation:

- **Python** will be used for data processing and analysis due to its flexibility and extensive libraries
- Security tools and monitoring platforms will be used to simulate or analyze threat detection scenarios

These tools are widely used in cybersecurity research and provide reliable results.

Hardware Requirements

The research can be conducted using standard computing systems. However, access to cloud environments (AWS or Azure free tier) may be used for testing and validation purposes. Cloud-based environments provide realistic conditions for evaluating security mechanisms.

4. Expected Outcomes

The expected outcomes of this research are both theoretical and practical in nature. The study aims to provide a comprehensive understanding of cloud security challenges while also offering actionable solutions.

Identification of Key Vulnerabilities

The research is expected to identify critical vulnerabilities in AWS and Azure environments, particularly those related to misconfiguration, identity management,

and multi-cloud complexity. These findings will be supported by both literature and case study analysis [2], [13].

Comparative Security Insights

By comparing AWS and Azure, the study will provide valuable insights into their relative strengths and weaknesses. This will help organizations choose appropriate platforms based on their security requirements.

Development of Mitigation Strategies

One of the key outcomes of this research is the development of practical mitigation strategies. These may include:

- Automated misconfiguration detection systems
- Improved IAM policies and access controls
- Unified security frameworks for multi-cloud environments
- Enhanced real-time threat detection mechanisms

These strategies aim to address the gaps identified in the literature and improve overall cloud security.

Contribution to Research and Practice

The findings of this study will contribute to the academic field by addressing underexplored areas such as automation and usability in cloud security. Additionally, the research will provide practical recommendations for organizations, helping them improve their security posture in increasingly complex cloud environments.

5. Timeline

Phase	Duration
Proposal Planning & Topic Approval	Week 1
Literature Review	Week 2 – Week 3
Research Design & Methodology	Week 4
Data Collection	Week 5
Data Analysis	Week 6 – Week 7
Writing & Draft Preparation	Week 8
Revision & Final Submission	Week 9 – Week 10

6. Conclusion

Proposed Research: Providing a comprehensive study of the security vulnerabilities with usage and adoption patterns for AWS/Azure. With the prominence of cloud computing in virtually any digital transformation, impenetrable security is a priority for every sector.

The study characterized that even with the presence of sophisticated security programs and frameworks, main drivers comprising configuration myths, identity control superiority issues as well as ever extra complex cyber threats leave cloud environments prone to severe safety lapses. But these problems are not only technical, they also have human aspects (if security practices do exist — lack of awareness or improper implementation) [2], [14].

This paper is a major work in terms of identification and expound on various important gaps that exist for cloud security research. This includes lack of automated detection systems for misconfiguration, ambiguity in the model of shared responsibility between cloud providers and customers, challenges associated with multi-cloud environments, a limited understanding about comparative evaluation methods involving real-time threat detection mechanisms. The practical challenges

are also discussed, which will trigger user-compliant responses to demand regulatory compliance as required by GDPR [15].

A mixed-methods approach and comparative design science framework were utilized to structure the proposed methodology for analyzing both theoretically- as well practically-insights related to cloud security. The mixed-method approach consisting of qualitative case studies and quantitative performance measurement allows a complete view on the problem.

The expected results of this research are identifying 15 critical weaknesses, providing comparative insights and suggesting mitigation strategies. We believe that these contributions will serve the dual purpose of informing both academic research and industry practice by providing actionable recommendations for improving cloud security.

It should be noted that the research may encounter some limitations, such as relying on secondary data sources and difficulties in reproducing actual cloud environments for testing. However, this research has several limitations and further studies could explore cloud security using different perspectives.

This research is intended to fill in some of the important gaps on cloud security and will help foster progress towards safer, more resilient cloud computing environments. Given the growth of many ICT organizations in their dependence on platforms like AWS and Azure, this study will significantly facilitate empirical decision making as practitioners perform practices to improve security.

6. References

- [1] CSA, “Top Threats to Cloud Computing,” 2020.
- [2] IBM, “Cost of a Data Breach Report,” 2023.
- [3] ENISA, “Cloud Security Threat Landscape,” 2022.
- [4] Gartner, “Multi-Cloud Adoption Trends,” 2022.
- [5] P. Mell and T. Grance, “NIST Definition of Cloud Computing,” 2011.
- [6] S. Subashini and V. Kavitha, 2011.
- [7] K. Hashizume et al., 2013.
- [8] AWS Security Whitepaper, 2022.
- [9] Microsoft Azure Security Docs, 2023.
- [10] Q. Zhang et al., 2018.
- [11] Google Cloud Multi-Cloud Study, 2021.
- [12] Palo Alto Networks Report, 2023.
- [13] NIST IAM Guidelines, 2017.
- [14] Usability in Cybersecurity Study, 2019.
- [15] GDPR EU Guidelines, 2020.
- [16] European Commission Report, 2021.
- [17] OWASP Top 10 API Security, 2023.
- [18] McKinsey Cloud Security Report, 2022.
- [19] Cisco Cloud Security Report, 2022.
- [20] Symantec Threat Report, 2023.

