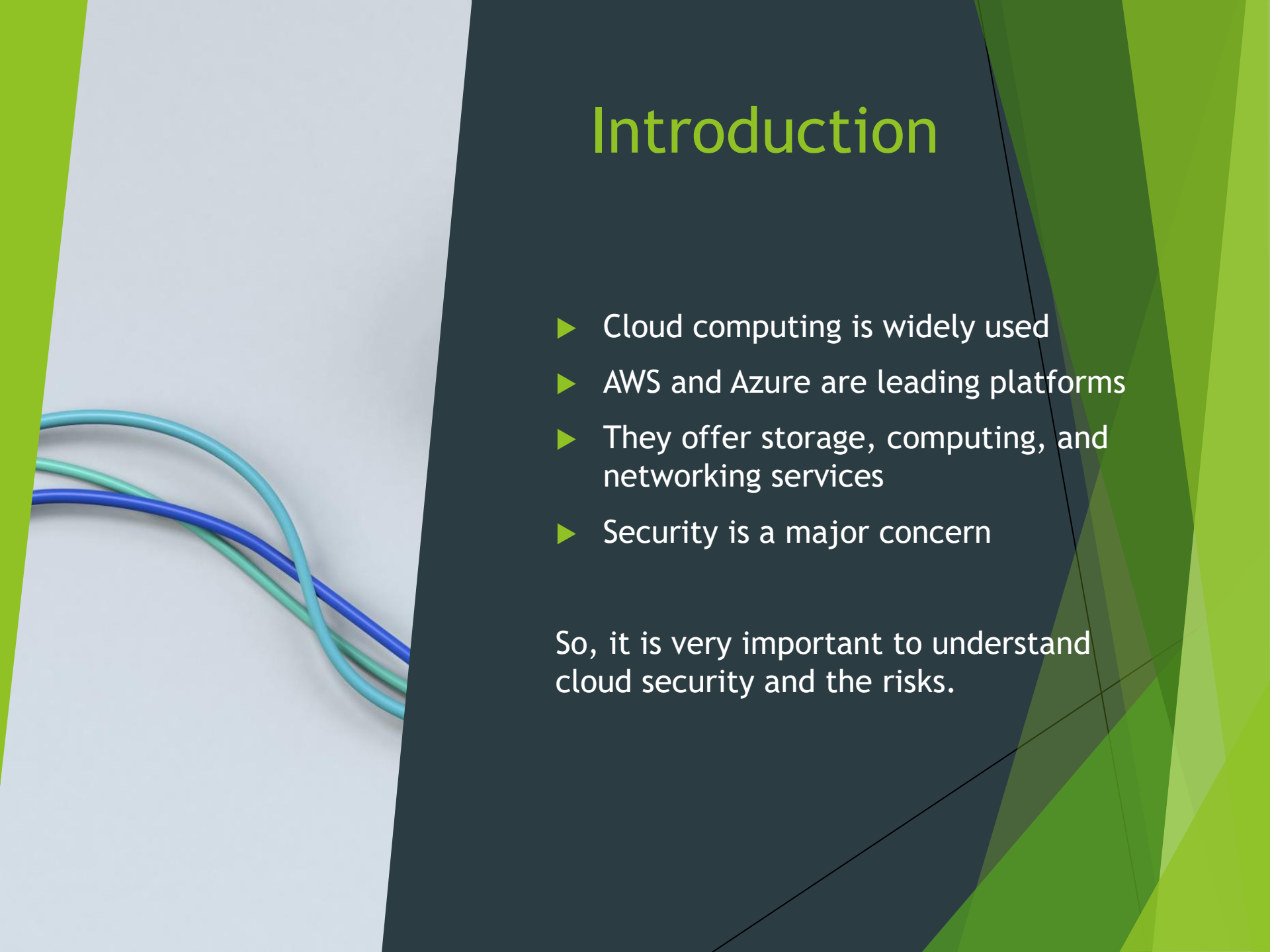


Security Challenges in Amazon web Services & Microsoft Azure

Name: Shahriar Badhan

Id:2505521

University of Wales Trinity Saint
David



Introduction

- ▶ Cloud computing is widely used
- ▶ AWS and Azure are leading platforms
- ▶ They offer storage, computing, and networking services
- ▶ Security is a major concern

So, it is very important to understand cloud security and the risks.

Problem Statement

- ▶ Cyber threats are increasing rapidly & hackers are trying to attack systems and steal information.
- ▶ Data breaches expose sensitive information (personal data or company data) can be exposed.
- ▶ Misconfiguration is a common mistake (cloud settings are not set up properly)
- ▶ Identity theft can occur due to weak access control “[5]”. This means unauthorized people can enter the system and misuse data.

So, it is important to understand these problems and find better security solutions.



Aim

- The main aim is to identify and analyze security challenges in AWS and Azure that means I want to understand what kind of security problems can happen in these platforms.
- I want to understand risks , such as data breaches and unauthorized access.
- This research will suggest some simple solutions to improve security and reduce these risks.

Objectives

Examine

study security features of AWS and Azure & how to protect data



Identify

Find out common security risks & data breaches and misconfiguration.



Compare

Compare platforms differences and which one is better in terms of security



Suggest

Suggest solutions improve security and reduce risks.

Research Questions



Main
challenges?



Differences
in security?



Causes of
breaches?



How to
improve?

- ✓ **Main challenges:** Find out the common security problems in Amazon Web Services and Microsoft Azure.
- ✓ **Differences in security:** Compare both platforms to see how their security systems are different.
- ✓ **Causes of Breaches :** Explain why security problems happen, like misconfiguration or weak access control.
- ✓ **How to Improve :** Suggest simple ways to improve security and reduce risks.

Key Security Challenges

- ❑ Data breaches → unauthorized people can access to important data
- ❑ Misconfiguration → This happens when cloud settings are not set correctly.
- ❑ IAM issues → This means weak login/permission control so wrong people can get access
- ❑ Insider threats → This happens when employees misuse their access.
- ❑ Insecure APIs → This means unsafe connections between systems .[4]



AWS vs Azure



AWS:



AZURE:

- AWS uses a system called IAM to control user access and permissions.[1]
- Azure uses Active Directory to manage users and login.[2]
- AWS is strong in global services and has a wide range of tools.[1]
- Azure is strong for companies that use Microsoft products like Windows.[2]

Methodology

- Use a qualitative research approach, which means I focus on understanding information instead of using numbers.
- Data is collected from reliable sources such as journals, articles, and official reports about Amazon Web Services and Microsoft Azure. [1], [2], [3], [4]
- Use case studies, which are real-life examples of security problems in cloud systems.
- Compare AWS and Azure to understand their differences and identify key security challenges.



Expected Outcomes

- ❑ This research will give a **better understanding of cloud security risks**, meaning we will clearly know what problems can happen in cloud systems.
- ❑ Provide a **clear comparison between Amazon Web Services and Microsoft Azure**, so we can understand their differences.
- ❑ The study will help in the **identification of common vulnerabilities**, such as misconfiguration and weak access control.
- ❑ It will give **practical security recommendations**, which can help organizations improve their cloud security.

Conclusion

- ❑ **“In conclusion, securing cloud platforms like Amazon Web Services and Microsoft Azure is not optional—it is essential for protecting data and ensuring trust.”**
- ❑ **“The future is in the cloud, but security will decide how safe that future is.”**
- ❑ **“By understanding these challenges, we can build more secure and trustworthy cloud systems.”**

That is why **security practices are very important.**

Organizations need to use proper security measures to protect their data in platforms like Amazon Web Services and Microsoft Azure.

Reference

- [1] Amazon Web Services, “AWS Security Overview,” 2024. [Online]. Available: <https://aws.amazon.com/security/> [Accessed: Apr. 20, 2026].
- [2] Microsoft, “Azure Security Documentation,” 2024. [Online]. Available: <https://learn.microsoft.com/en-us/azure/security/> [Accessed: Apr. 20, 2026].
- [3] National Institute of Standards and Technology (NIST), *Security and Privacy Controls for Information Systems and Organizations*, 2020.
- [4] Cloud Security Alliance (CSA), *Security Guidance for Critical Areas of Cloud Computing*, 2021.
- [5] IBM, *Cost of a Data Breach Report*, 2023. [Online]. Available: <https://www.ibm.com/reports/data-breach> [Accessed: Apr. 20, 2026].



Thank You

Any Questions?