RISK MANAGEMENT IN CLOUD COMPUTING ENVIRONMENTS

ITIS 6230 – ENTERPRISE AND INFRASTRUCTURE PROTECTION

Rakesh Dama - 801337628
Akshith Vuduthala - 801367175
Tharun Kumar Reddy Vattam - 801359994

INTRODUCTION

- Cloud Computing has revolutionized IT resource management, offering scalability, flexibility, and cost-effectiveness.
- Effective risk management is crucial for ensuring security, compliance, and resilience in cloud-based systems.
- This presentation explores the challenges, strategies, and best practices in risk management in cloud computing environments.

CLOUD COMPUTING OVERVIEW

- Cloud computing delivers IT resources and services over the internet.
- Benefits include scalability, flexibility, and cost-effectiveness.
- However, it also introduces risks such as data breaches, service disruptions, and compliance issues.

CHALLENGES IN CLOUD RISK MANAGEMENT

Cloud infrastructure is dynamic and distributed, posing challenges in management.

The shared responsibility model between providers and customers complicates risk management.

Multi-cloud and hybrid architectures add complexity due to integration challenges.

KEY RISK FACTORS

Data breaches : Security incidents leading to data compromise.

Service disruptions: Interruptions affecting business operations.

Compliance issues: Violations of regulatory requirements.

Vendor lock-in: Dependency on a single provider.

EXISTING FRAMEWORKS AND STANDARDS :

- ✓ NIST, ISO, CSA provide guidance for risk management.
- ✓ These frameworks help organizations identify and address risks effectively.

RISK ASSESSMENT METHODOLOGIES :

- ✓ Risk matrices, threat modeling, vulnerability scanning prioritize vulnerabilities.
- ✓ These methodologies are essential for effective risk assessment and mitigation.

SECURITY MECHANISMS AND CONTROLS :

- ✓ Encryption, access controls, intrusion detection systems safeguard data and resources.
- ✓ Compliance with industry standards such as GDPR, HIPAA, and PCI DSS is crucial.

EMERGING TECHNOLOGIES AND TRENDS :

- ✓ Edge computing, serverless computing, containerization offer new opportunities but also pose challenges.
- ✓ Organizations must adapt risk management strategies to incorporate these technologies effectively.

REGULATORY REQUIREMENTS :

- ✓ GDPR, HIPAA, CCPA set standards for data protection and privacy.
- ✓ Compliance with these regulations is essential to mitigate legal and regulatory risks.

METHODOLOGY :

- ✓ Literature review, data collection, analysis inform the development of risk management frameworks.
- ✓ Validation through industry experts and peers ensures the effectiveness of the framework.

RESULTS AND DISCUSSION :

- ✓ Comprehensive risk catalog identifies various risks in cloud computing.
- ✓ Evaluation of existing mitigation strategies highlights the need for adaptive security measures.
- ✓ Proposed risk management framework emphasizes holistic approaches to enhance resilience.

CONCLUSION :

- ✓ Effective risk management is essential for capitalizing on the benefits of cloud computing while safeguarding assets and data.
- ✓ Continuous innovation and collaboration are necessary to address evolving risks and challenges.

REFERENCES :

- Rittinghouse, J. W., & Ransome, J. F. (2016). Cloud Computing: Implementation, Management, and Security.
- Mell, P., & Grance, T. (2011). The NIST Definition of Cloud Computing (NIST Special Publication 800-145).
- Khan, M. A., Salah, K., Alzahrani, A. I., & Alelaiwi, A. (2019). A Systematic Review of Risk Assessment Techniques in Cloud Computing.
- Alshammari, G., Jiang, J., Alowibdi, J. S., & Hammoudi, S. (2017). Cloud Computing Security Risk Assessment Using Fuzzy Analytic Hierarchy Process.
- Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing.