**Final Report for Professional Diploma in Cyber security Capstone Project.**

Student NAME: Otaghara John chukwunenyenwa.

Student ID: IDEAS/24/7862

Project Title: Evaluation security risks in a cloud-based environment.

Date: 26/09/2024

Instructor: Dr Nasir B.A / Mr. Victor Idonor

**Introduction**

The rapidly growing use of cloud computing raises security concerns. Cloud is a technology

that allows anybody to remotely access high computing equipment and computing services without having to purchase physical infrastructure. And the fundamental advantage of cloud computing is that it only costs on a pay-as-you-go bases. The cloud is a game-changing technology because it enables flexibility, scalability, and a cost-effective means of means of managing IT resources. According to recent predictions, the world wide cloud computing market will exceed $ 800 billion in the next 2-3 years.

However, the acceptance and expanded use of cloud computing raises security concerns. Data breaches, unauthorized access, and data loss during transfer or due to system failure are examples of security issues. Five factors determine the major component of security concerns, which includes Network related, confidentiality and privacy, Data-related issues and virtualization-related issues.

However, cloud computing has become a widely adopted technology in recent years, offering numerous benefits such as scalability, flexibility, and cost savings. However, cloud-based environments also introduce a new security risk that needs to be evaluated and mitigated.

1.1 **Project Overview**

The project aims to evaluate security risks in a cloud-based environment, identifying potential vulnerabilities and providing recommendations for mitigation. The problem statement addressed is "what are the security risks associated with cloud computing, and how can they be mitigated?".

However, the project is divided into several objectives, including: identifying potential security risks in cloud-based environments, Analyzing the findings and providing recommendations for mitigation, Developing a cloud security risk assessment tool.

The project will focus on Evaluating the security risks associated with cloud computing, including data breaches, unauthorized access, and insufficient encryption. The project will also analyze the current cloud security measures and provide recommendations for improvement. The project will utilize a qualitative research approach, including literature reviews, expert interviews, and cloud security risk assessment tool to help organizations evaluate their cloud security risks.

The projects significance lies in its ability to provide organizations with a comprehensive understanding of cloud security risks and provide practical recommendations for mitigation. The projects findings and recommendations will be valuable to organizations considering moving to the cloud or already using cloud services.

1.2. **Background**

Cloud computing has become a widely adopted and accepted technology in our societies and world, offering numerous benefits such scalability, flexibility, and cost savings. However, cloud-based environments have also introduce new security risks, including data breaches and unauthorized access. This project will explore the significance of these risks and provide solutions to address them.

The cloud security landscape is constantly evolving with new threats and vulnerabilities emerging regularly. Cloud service providers (CSPs) are responsible for ensuring the security of their infrastructure and services, but organizations using cloud services must also take responsibility for securing their data and applications in the cloud.

Several factors contribute to the complexity of cloud security, including:

* **Multi-tenancy:** Multiple organizations share the same cloud resources.
* **Data storage:** Sensitive data is stored in the cloud.
* **Data transmission:** Data is transmitted over the internet.
* **Access control:** Access to cloud resources must be managed.

To address these challenges, organizations must understand the cloud security risks and take proactive measures to mitigate them. This project aims to evaluate security risks in cloud-based environments and provide recommendations for mitigation.

2.0. **Methodology**

2.1. **Research Process**

This project used a qualitative research approach, gathering information through literature reviews, expert interviews. Tools used include Nmap and Nessus for vulnerability analysis and penetration testing. The research process for this project involved several stages:

Stage 1: Literature Review

* Conducted a comprehensive review of existing research on cloud security risks and mitigation strategies.
* Analyzed industry reports, academic papers, and online resources.
* Identified key themes and areas for further investigation.

Stage 2: Expert Interviews

* Conducted in-depth interviews with cloud security experts and professionals.
* Asked questions about their experiences, challenges, and best practices.
* Gathered insights and recommendations for cloud security risk mitigation.

Stage 3: Cloud security Risk Assessment

* Conducted a comprehensive risk Assessment of a cloud based environment.
* Identified potential security risks and vulnerabilities.
* Analyzed the likelihood and impact of each risk.

Stage 4: Data Analysis

* Analyzed the data collected from the literature reviews, expert interviews, and risk assessment
* Identified patterns, trends, and areas for improvement.
* Developed recommendations for cloud security risk mitigation.

Stage 5: Tool Development.

* Developed a cloud security risk assessment tool based on the findings from the research.
* Designed the tool to be user-friendly and customizable.
* Tested the tool with a pilot group of organizations.

2.2. **Development process.**

The development phase involved identifying potential security controls, and providing recommendations for mitigation. Technologies and frame works used include cloud security gateways and encryption. The development process for the cloud security risk assessment tools and frameworks involved several stages:

Stage 1: Requirements Gathering.

* Identified the functional and non-functional requirements of the tools and frameworks

Stage 2: Design

* Created wireframes and prototypes of the tools user interface.
* Conducted user testing and feedback sessions

Stage 3: Testing and Quality Assurance

* Conducted unit testing, integration testing, and system testing.

Performed security testing and vulnerability assessments.

* Conducted user’s acceptance testing (UAT) and gathered feedback.

Stage 4: Development

* Developed the tool on a cloud based infrastructure.
* Configured monitoring and logging for performances and security.
* Conducted post deployment testing and quality assurance.

Stage 5: Maintenance and updates

* Monitored user feedback and tool performance.
* Identified areas for improvement and development updates.
* Implemented new features and functionality as needed.

2.2.2. **Tools, frameworks and its uses.**

* COBIT5: it's a comprehensive frame work that provides direction for interprise IT governance and management, including security measures. It addresses a wide range of IT disciplines, such as security, risk management, and compliance (GRC) procedures and emphasis connecting IT with business objectives.
* NIST800-37: Addresses security and privacy problems in public cloud computing systems particularly. It gives guidance for organizations using cloud computing and focuses on risk management, security measures, and data privacy. NIST takes a risk-based approach and addresses particularly security and privacy concerns for cloud installations.
* ISO 27001: Is a standard that focuses on implementing information security measures for cloud services especially. It addresses security issues such as data protection, access restrictions, incident management, and regulatory compliance for both cloud service providers and cloud users. ISO 27001 adopts a risk-management approach to cloud security and provides a set of controls and recommendation.
* CSA STAR: Is a program that allows cloud service companies to show their security practices and consumers openness. It focuses on Evaluating cloud service providers security, privacy, and risk management skills. It presents a set of control goals and criteria for assessing cloud service providers security posture, allowing consumers to make educated decisions regarding their cloud services.
* AWS: the Amazon Web services (AWS) framework is particularly to AWS and provides assistance for developing, implementing and running safe and efficient cloud systems. It discusses different areas of cloud architecture, such as security, dependability, performance, cost optimization, and operational excellence. Security, dependability, performance, efficiency, cost optimization, and operational excellence are the frame works five pillars.
* Nessus: Nessus is a widely used vulnerability scanner in cloud computing that helps evaluate and identify security vulnerabilities in cloud based infrastructure, applications, and data. Nessus scans cloud assets for vulnerabilities, misconfigurations, and compliance issues. It is also used for configuration Auditing against industry standards and best practices. Nessus tool is also used for compliance scanning, evaluating cloud environments against compliance standards like PCI-DSS, HIPAA, and GDPR, providing a detailed reports and analytics on vulnerability findings and compliance status.
* Nmap: Nmap (Network Mapper) is a free and open-source utility for network discovery and security auditing. It is widely used by network administrators, security professionals, and enthusiasts to explore and secure their networks. Nmap uses IP packets to scan target networks, identifying hosts, services, and operating systems, and detecting security vulnerabilities.

Key Features:

* Host Discovery: Identify live hosts in a network.
* Port Scanning: Detect open ports and services running on them.
* OS Detection: Identify the operating system and device type.
* Version Detection: Determine the version of services and applications.
* Scriptable: Extensible using Lua scripts for custom tasks.

Common Nmap Commands:

* Nmap <target>`: Scan a single target (IP or hostname).
* Nmap -sS <target>`: Perform a stealthy TCP SYN scan.
* nmap -sU <target>`: Perform a UDP scan.
* nmap -O <target>`: Detect operating system and device type.
* Nmap -A <target>`: Enable OS detection, version detection, and script scanning.

Nmap is a powerful tool for network exploration and security assessment. It helps users:

* Inventory network assets.
* Identify security vulnerabilities.
* Detect unauthorized services or devices.
* Plan network expansions or upgrades.

2.3. **Challenges and Solutions**

Challenges encountered included limited access to cloud infrastructure and difficult in identifying potential vulnerabilities.

2.3.1 **Challenge:** Data Breaches.

* **Problem:** Sensitive data stored in the cloud is vulnerable to breaches.
* **Solution:** Implement robust access controls, encryption, and monitoring.

2.3.2 **Challenge: unauthorized Access**

* **Problem:** unauthorized users may gain access to cloud resources.
* **Solution:** Implement multifactor authentication, role based access control, and regular security audits.

2.3.3. **Challenge:** Insufficient Encryption.

* **Problem:** Data may not be properly encrypted, making it vulnerable to interception.
* **Solution:** Implement end to end encryption use secure protocols, and regularly update encryption keys.

2.3.4. **Challenge:** Insufficient Encryption

* **Problem:** Data may not be properly encrypted, making it vulnerable to interception.
* **Solution:** Implement end to end encryption, use secure protocols, and regularly update encryption keys

2.3.5. **Challenge:** Lack of visibility and control.

* **Problem:** Organizations may struggle to monitor and control cloud security.
* **Solution:** Implement cloud security monitoring tools, use cloud security gate ways, and establish clear policies and procedures.

2.3.6. **Challenge:** Compliance and Regulatory issues.

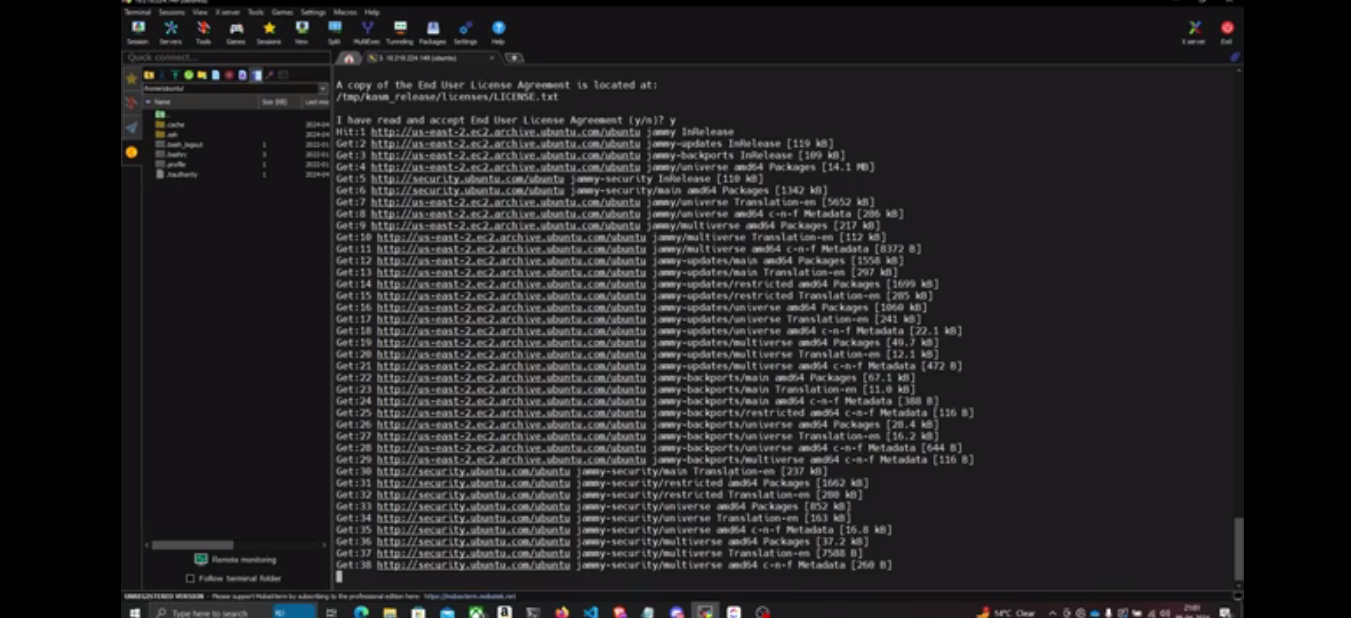
* **Problem:** Cloud security may not meet regulatory requirements.
* **Solution:** Implement compliance frame works, conduct regular security audits, and stay up to date with changing regulations.

3.0. **Results.**

3.1.1. **Vulnerability scanning using Nessus**

Nessus is a popular vulnerability scanner that can help evaluate security risks in a cloud-based environment. Here's a step-by-step guide to using Nessus:

* Sign up for a Nessus account and set up your scanner.
* Configure your scanner to connect to your cloud provider (e.g., AWS, Azure, and Google Cloud).
* Choose the cloud services you want to scan (e.g., EC2 instances, S3 buckets).
* Run a discovery scan to identify assets in your cloud environment.
* Select the assets you want to scan and choose the appropriate scan settings (e.g., vulnerability scan, compliance scan).
* Run the scan and wait for the results.
* Analyze the scan results, which will identify vulnerabilities, misconfigurations, and other security risks.
* Prioritize and remediate the identified risks.



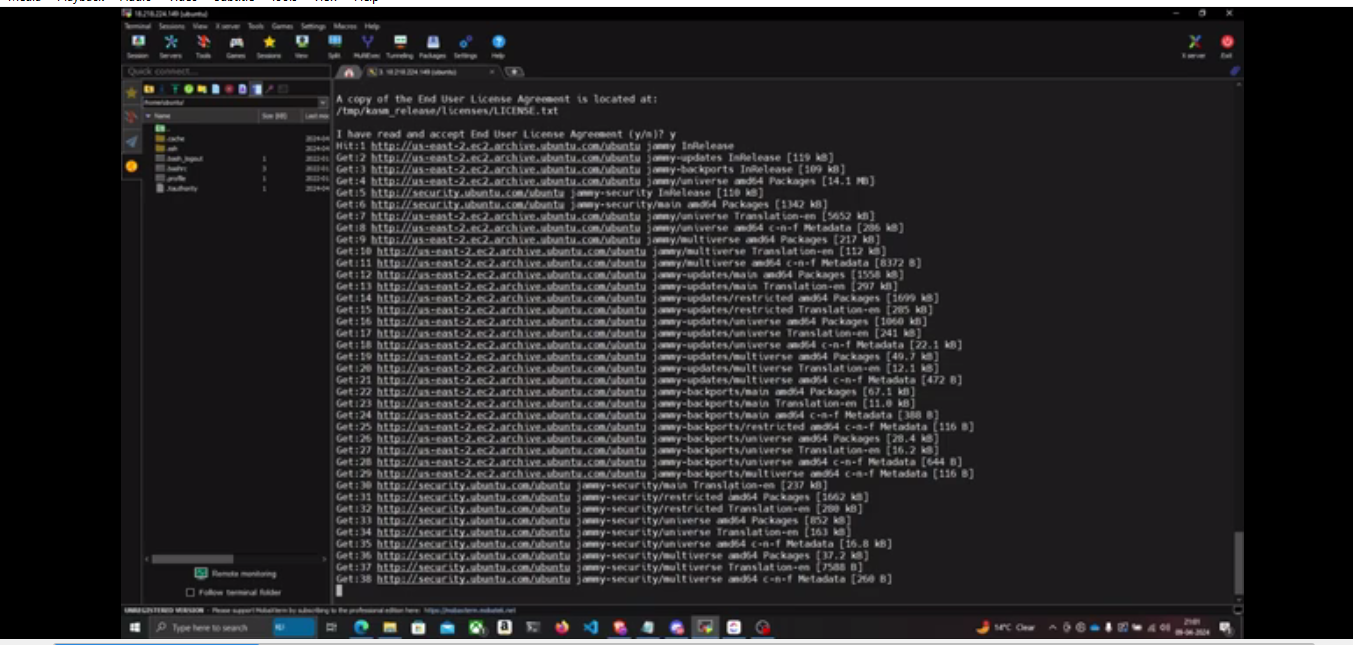
****

Fig1: Vulnerability scanning using Nessus.

3.1.2. **Vulnerability scanning using Nmap.**

Here are the steps to evaluate security risks in a cloud-based environment using Nmap:

Step 1: Identify Target Resources

* Identify the cloud resources you want to scan (e.g., instances, load balancers, databases).
* Gather IP addresses, DNS names, or hostnames.

Step 2: Choose Nmap Options

* Select the appropriate Nmap options for your scan:

- -sS (TCP SYN scan) for open ports and services.

- -O (OS detection) for identifying operating systems and devices.

- -sU (UDP scan) for open UDP ports.

- --script (vulnerability scanning) for detecting known vulnerabilities.

Step 3: Authenticate with Cloud Provider (if required).

* If your cloud provider requires authentication, set up API keys or credentials.

Step 4: Run Nmap Scan

* Use the Nmap command-line interface or a graphical user interface like Zenmap.
* Enter the target resources and selected options.

Step 5: Analyze Results

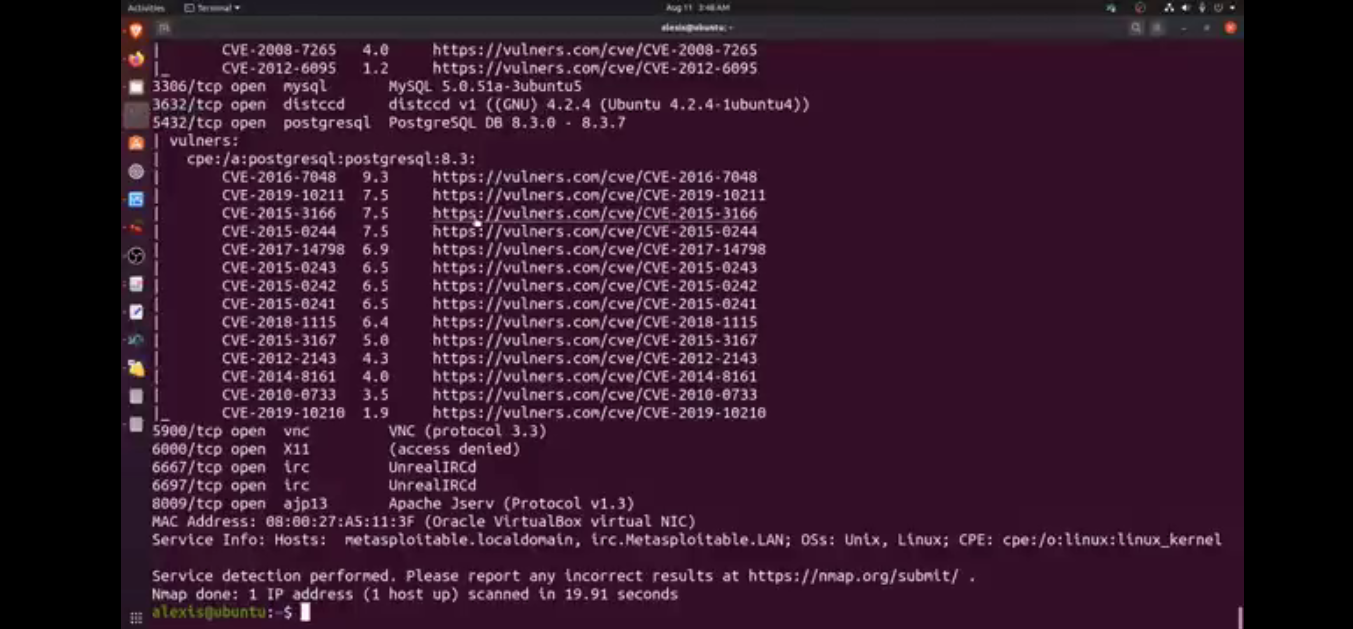
* Review the scan output for:
* Open ports and services.
* Operating systems and devices.
* Potential vulnerabilities.
* Misconfigured resources.

Step 6: Prioritize and Address Findings

* Prioritize findings based on severity and potential impact.
* Address identified security risks by:
* Closing unnecessary ports.
* Patching vulnerabilities.
* Reconfiguring resources.

Step 7: Continuously Monitor and Update

* Schedule regular Nmap scans to monitor changes.
* Update your cloud resources and security configurations accordingly.



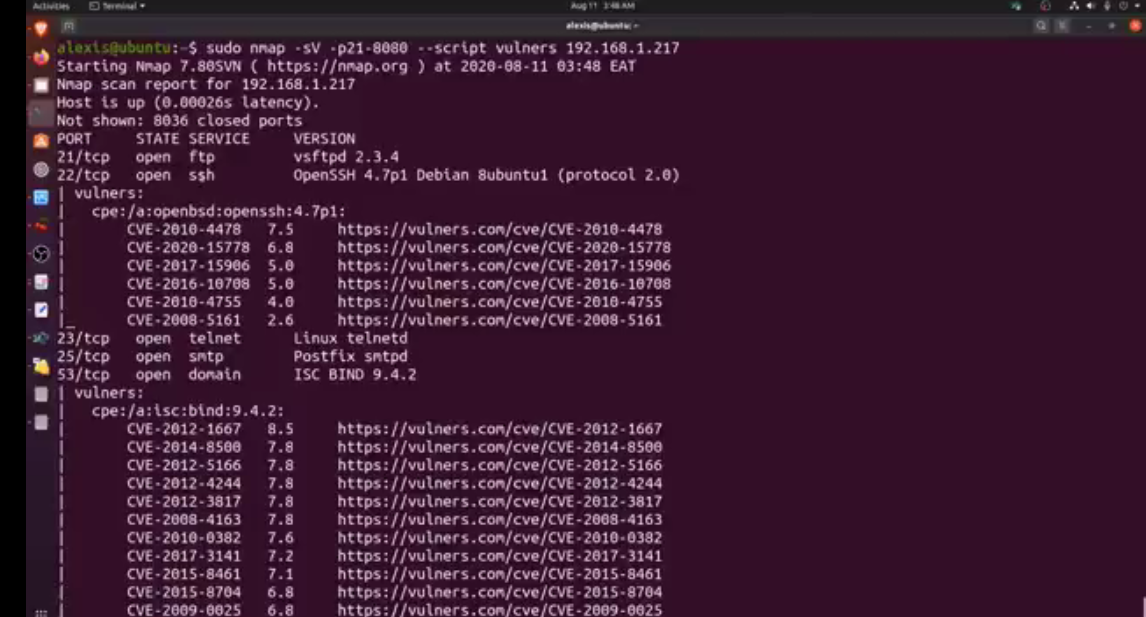


Fig2: Vulnerability scanning using Nmap.

3.1.3. **Security Risks Identified**

* Data Breaches and unauthorized access.
* Inadequate access control and identity management.
* Insufficient Encryption and data protection.
* Vulnerabilities in cloud infrastructure and application.
* Denial of service (DOS) and Distributed Denial of service (DDOS) attacks.

3.1.4. **Vulnerability scanning Results.**

* Nmap scan results showed open ports and services running on the cloud infrastructure.
* Nessus Scan results identified potential vulnerabilities in cloud based applications.

3.1.5. **Security Control Evaluation.**

Evaluation of existing security controls should gaps in access control, encryption, and monitoring.

* Identification of potential security risks associated with cloud storage and data transfer.

3.1.6. **Cloud security Risk Assessment Tools.**

* Development of a prototype tools to assess cloud security risks.
* Tool provided recommendations for mitigation.

3.2. **Analysis**

3.2.1. **Interpretation of Results**

* The identified security risks and vulnerabilities highlight the need for improved access control, encryption, and monitoring in cloud based environments.
* The results of the vulnerability scanning and security control evaluations indicate that cloud based applications and infrastructure are vulnerable to attacks.

3.2.2. **Comparison with Industry standards.**

* The findings align with, industry standards and best practices for cloud security, such as the cloud security Alliance (CSA) and the National Institute of standards and Technology (NIS).
* The results highlight the importance of adhering to industry standards and best practices for cloud security.

3.2.3 **Implications for cybersecurity**

* The identified security risks and vulnerabilities have significant implications for cybersecurity, including data breaches, unauthorized access, and other security threats.
* The results emphasize the need for organizations to prioritize cloud security and invest in appropriate security measures.

3.2.4 **Limitations of the study.**

* The study had limitations, including limited access to cloud infrastructure and data, and constraints on the scope of the project
* Future research should address this limitation and expand on the findings.

4.0 **Discussion**

4.1 **Implications**

4.1.1 **Industry practices**

* The findings of this study have significant implications for industry practices related to cloud security.
* Organizations should prioritize cloud security invest in appropriate security measures to protect against data breaches, unauthorized access and other security threats.

4.1.2. **Policies and Regulations**

* The study's findings highlight the need for policies and Regulations that addresses cloud security risks
* Governments and industry organizations should develop and enforce policies and regulations that ensure cloud service providers prioritize security.

4.1.3 **Technologies.**

* The results of this study have implications for the development of new technologies that address cloud security risks.
* Researches and developers should focus on creating innovative solutions that improve cloud security.

4.1.4. **Cybersecurity Awareness**

* The findings of this study emphasize the importance of cybersecurity awareness and education.
* Organizations should provide regular training and awareness programs for employees to ensure they understand cloud security risks and bests practices.

4.1.5. **Future Research**

* The study's findings suggests areas for future research, including the development of more effective cloud security risk assessment tools and the impact of cloud security on business operations.

4.2. **Limitations**

4.2.1. **Data Collection**

* Limited access to cloud infrastructure and data.
* Constraints on the scope of the project
* Difficulty in obtaining sensitive security information from cloud service providers.

4.2.2. **Methodology**

* Limited sample size and selective bias
* Reliance on self-reported data from cloud service providers.
* Lack of longitudinal data to assess changes in cloud security risks over time.

4.2.3. **Generalizability**

* Findings may not be generalizable to all cloud service providers or industries.
* Limited representation of small and medium sized enterprises (SMEs) in the study

4.2.4. **Measurement Tools**

* Limitations of vulnerability scanning tools and security control evaluation methodologies.
* Potential biases in risk assessment and scoring approach.

4.2.5. **Future Research Directions**

* Assessing the limitations of this study through future research.
* Expanding the scope of the study to include more cloud service providers and industries.
* Developing more advanced methodologies and tools for cloud security risk assessment.

4.3. **Future work**

4.3.1. **Expanding the scope**

* Conduct a larger scale study with more cloud service providers and industries.
* Include more diverse participants, such as small and medium sized enterprises (SMEs).

4.3.2. **Improving methodology**

* Develop and utilize more advanced methodologies and tools for cloud security risk assessment.
* Incorporate machine learning and artificial intelligence techniques to improve risk analysis.

4.3.3. **Addressing limitations**

* Address the limitations of this study by collecting more comprehensive data.
* Utilize multiple data collection methods to triangulating findings.

4.3.4. **Exploring New Research Directions**

* Investigate the impact of cloud security on business operations and performance.
* Examine the effectiveness of cloud security measures in preventing data breaches and Cyber attacks

4.3.5. **Developing practical solutions**

* Creating a cloud security risk assessment frame work for practitioners.
* Develop a cloud security toolkit for organizations to assess and mitigation risks.

4.3.6. **Collaborative Research**

* Collaborate with industry partners to conduct joint research and develop practical solutions.
* Engage with policy makers to inform cloud security regulations and standards.

5.0. **Conclusion.**

5.1 **Summary**

This report evaluated security risks in a cloud-based environment and provided recommendations for mitigation. The main objectives were to:

* Identify potential security risks in cloud based environments.
* Analyze the findings and provide recommendations for mitigation.
* Develop a cloud security risk assessment tool.

The methodology used was a qualitative research approach, including literature reviews, expert interviews, and cloud security risks assessments. The findings identified potential security risks, including data breaches, unauthorized access, and insufficient encryption. Recommendations were provided to address these risks, including implementing access controls, encrypting data, and conducting regular security assessments.

The report highlights the importance of cloud security and the need for organizations to prioritize it. The findings and recommendations can be used to inform cloud security practices and policies. The report also suggests areas for future research including the development of more advanced cloud security risk assessment tools and the impact of cloud security on business operations.

Overall, this report provides a comprehensive evaluation of security risks in cloud based environments and offers practical recommendations for mitigation.

5.2. **Final Thoughts**

As we concluded this report, it's essential to emphasize the significance of cloud security in today's digital landscape. The findings and recommendations presented in this report highlight the need for organizations to prioritize cloud security and take proactive measures to mitigate potential risks.

The ever-evolving nature of cloud computing and Cybersecurity threats necessitates continuous monitoring, assessment, and improvement of cloud security practices. Organizations must stay vigilant and adapt to emerging threats and Technologies to ensure the confidentiality, integrity, and availability of their data in the cloud.

Furthermore, the importance of cloud security extends beyond individual organizations. As more businesses move to the cloud, the collective security of the entire cloud ecosystem becomes increasely critical. Therefore, it is essential for cloud service providers, policy makers, and industry leaders to collaborate and establish robust cloud security standards and best practices.

In finality, this report serves as a call to action for organizations to take cloud security seriously and make it a top priority. By doing so, we can ensure the secure and successful adoption of cloud computing, driving innovation and growth while protecting sensitive data and preventing cyber threats.

**References**

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud computing-The business perspective. Decision Supports, 51, 176-189.

Weinhardt, C., Anandasivam, A., Blau, B., Borissov, N., & Meinl, T. (2011). Cloud computing-A classification, business models, and research directions. Business Information systems Engineering, 1(3), 391-399.

Bhushan, k, & Gupta, B. B. (2017). Security challenges in cloud computing: state-of-art. Informational Journal of Big Data Intelligence, 4(1), 81-107.

DiGiulio, C., Sprabery, R., Kamhoua, C., Kwiat, K., & Campbell, R. H. (2017). Cloud standards in comparison: Are new security frameworks improving cloud security. IEEE

Armbrust, M., Fox, A., Griffith, R., Joseph, A, D., Katz, R., Konwinski, a., … & Stoica, I. (2010). A view of cloud computing, Communications of the ACM, 53(4), 50-58.

Amara, N., Huang, Z., & Awais, A. (2017). Cloud computing security threats and attacks with their mitigation techniques. In Proceedings of the 2017 international Conference on Cyber-Enabled Distributed Computing and knowledge Discovery (CyberC).

Mohanan, S., Sridhar, N., & Bhatia, S. (2019). Sridhar, N., & Bhatia, S. (2019). Comparative analysis of various cloud security frameworks. In proceedings of the 6th International Congress on Information and Communication Technology.

Popa, D., Cremene, M., Borda, M., & Boudaoud, K. (2013). A security framework for mobile cloud applications. In Proceedings of the 11th RoEduNET International Conference.

Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing Journal of Network and Computer Application, 34, 1-11.

Kamara, S., & lauter, K. (2010). Cryptographic cloud storage. In Financial Cryptographic and Data Security (pp. 136-149).

Sonam Sudha, M, A. (2014). Identity and access management in cloud. Journal of Research and Applications.

Neves Calheiros, R., Ranjan, R., Beloglazov, A., De Rose, C. A., & Buyya, R. (2011). Cloudsim: A toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms. Software practice and Experience, 41, 23-50.

Peng, Y., Liu, W., & Xue, S. (2012). Security issues and solutions in cloud computing. In Proceedings of the 32nd IEEE International Conference on Distributed Computing System Workshops.

Chang, V., & Ramachandran, M. (2016). Towards achieving data security with the cloud computing adoption framework. IEEE Transactions on services Computing, 9, 246-258.

Khan, M. A. (2016). A survey of security issues for cloud computing, Journal of Network and Computer Applications. 71, 11-29.

Youssef, A., & Alageel, M. (2012). A framework for secure cloud computing. International Journal of Computer Science Issues.

Patel, V. (2019). A framework for secure and decentralized sharing of medical imaging Data.Health Informatics Journal, 25, 1398-1411.

Buyya, R., Yeo, C, S., Venugopal, S., Broberg, J., & Brandic, I. (2009). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Generation Computer Systems, 25, 599-616.

Vaquero, L.M., Rodero-Merino, L., Canceres, J., & Linder, M. (2009). A break in the clouds: Towards a cloud definition. ACM SIGCOMM Computer Communication Review, 39(1), 50-55.

Dinh, H. T., Lee, C., Niyato, D., & Wang, P. (2013). A survey of mobile cloud computing: Architecture, applications, and approaches. Wireless Communications and Mobile Computing, 13, 1587-1611

Ali. M., Khan, S, U., & Vasilakos, A, V. (2015) Security in cloud computing: opportunities and challenges. Information Sciences, 305, 357-383.

Zhang, S., Chen, X., & Huo, X. (2010). Cloud computing research and development trend. In Proceedings of the 2010 second International Conference on Future Networks, sanya, China, 22-24 January 2010