DOI: http://dx.doi.org/10.26483/ijarcs.v16i5.7347

Volume 16, No. 5, September-October 2025

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

MANAGING THREATS IN CLOUD COMPUTING: A CYBERSECURITY RISK MITIGATION FRAMEWORK

Md Imran Khan
College of Graduate and Professional Studies
Master of Science in Information Studies, Trine University,
Angola, Indiana, USA

Abstract: Data processing, management, and storage have all been changed by the internet of things, which offers companies scalable and reasonably priced solutions. There is serious cybersecurity concerns connected to using cloud services, such as service outages, unauthorized access, and data breaches. Investigating these security threats and developing defenses to enhance cloud security are the goals of this study. This study reviews current security mechanisms including encryption, authentication, and access control and highlights critical vulnerabilities in cloud systems through methodical literature analysis and risk assessment. To assist enterprises in evaluating and prioritizing cloud security concerns, the study suggests a risk assessment methodology. To strengthen cloud computing's overall security posture, best practices and security solutions are also advised. The results of this study will help create cloud infrastructures that are more secure, guaranteeing data availability, confidentiality, and integrity in the rapidly changing digital environment.

Keywords: Cloud computing, cybersecurity, risk mitigation, data security, access control, Encryption

INTRODUCTION

Since the introduction of computing in the cloud and the numerous advantages it provides to businesses, technology for communication and information, or ICT, has grown significantly. However, the shift from the traditional company structure to this new paradigm can be more difficult due to cloud tenants' security and privacy concerns inadequate underlying architecture transparency Because the underlying cloud architecture is opaque, security officials have been emphasizing the need to protect servers in the cloud, ICT systems, and applications regarding cyberattacks. The basic cloud telecommunication systems that are linked and categorized as tools used in ICT activities are referred to as cloud infrastructure. The use of information technology is growing significantly. It encourages the exponential growth of security incidents in a variety of ways, including Internet phishing efforts, interruption of service (DoS), unauthorized access, virus attacks, breaches of data, and social engineering. Infrastructure as a Service (IaaS) is one way to provide cloud services. offers on-demand computing resources that pose serious dangers to the cloud computing ecosystem, among other things Cybersecurity risk is the potential loss that on by an organization's technology infrastructure, is what these security events are known. According to (Oludele Awodele et,al 2024) Preventing cyberattacks, cyberthreats, and unauthorized access to business applications, information, programs, groups, and systems are known as cybersecurity on the other hand, hostile actions Computer viruses and security breaches are designed to steal or corrupt data or to disrupt the digital health and safety of an organization.

1.1 Background of the Study

A major component of contemporary IT, Businesses can make money with cloud computing in a few ways, as affordability and scalability, and flexibility. Businesses must now ensure that their data, apps, and networks in the cloud to leverage cloud services effectively. The goal of this systematic literature review is to locate the most recent data on internet computing safety with a focus on dangers and mitigation techniques. Furthermore, it enumerates some prevalent risks associated with cloud computing protection, including malware assaults, distributed enemy disruptions (DDoS) attacks, account theft, and data breaches. The present research also looks at a few mitigating techniques, such as events, login and managing passwords (IAM), security data, and leadership team security.

1.2 Problem Statement

Cybersecurity issues have grown increasingly complex and pervasive in today's rapidly evolving digital economy, posing serious risks to people, businesses, and governments everywhere .The importance of cybersecurity in safeguarding private data and ensuring the integrity of digital systems has been brought to light by the growth of networked devices, the rise of sophisticated cyberthreats and the exponential expansion of data .The sheer volume and variety of cyberattacks, however, is one of the biggest problems facing cybersecurity today. Cybercriminals are always coming up with new tactics to take advantage of

© 2023-2025, IJARCS All Rights Reserved

vulnerabilities in networks, software, and human behavior. Cyber threats are varied and constantly evolving, ranging from ransomware and data breaches to malware and phishing attacks. These assaults can have catastrophic consequences, from monetary losses and damage to one's reputation to disruption.

1.3 Research Objectives

To Identify Key Cybersecurity Threats in Cloud Computing Environments Analyze common vulnerabilities, attack vectors, and threat actors targeting public, private, and Cloud infrastructures that are hybrid To Assess the Performance of Present Cloud Security Procedures and Guidelines Assess industry-standard frameworks, encryption methods, and access control measures used to secure cloud systems To Investigate Risk Assessment Models for Cloud-Based Systems Examine existing methodologies for quantifying and prioritizing cybersecurity risks in cloud platforms. To analyze the Role of Compliance and Regulatory Requirements in Cloud Security Explore how frameworks like GDPR, HIPAA, and ISO/IEC 27001 influence cloud security strategies and risk management.

1.4 Research Questions

To guide the investigation into cybersecurity issues in cloud computing and the development of effective mitigation strategies, the following research questions are proposed:

What are the most common cybersecurity threats facing cloud computing environments today?

How effective are current cloud security measures in preventing data breaches and unauthorized access?

What methodologies can be used to assess and quantify cybersecurity risks in cloud systems?

How do legal and regulatory compliance requirements influence cloud security practices?

What are the most effective strategies for mitigating cybersecurity risks in cloud computing?

In what ways do human factors and user behavior contribute to cloud security vulnerabilities?

How can cloud service providers and organizations implement effective monitoring and incident response systems?

1.5 Significance of the Study

Cybersecurity is now a major worry for both consumers and enterprises due to the growing reliance upon online computing for data processing, storage, and service delivery. Because it tackles the increasing difficulties and intricacies of protecting cloud-based infrastructures from a changing threat landscape, this work is noteworthy. Through the identification of critical cybersecurity threats and the assessment of successful mitigation techniques, this study seeks to improve cloud systems' overall security posture.

The study will benefit the following stakeholders:

Cloud Service Providers (CSPs): The findings can support CSPs in strengthening their security frameworks and aligning them with best practices and compliance requirements. Organizations and Enterprises: By understanding the risks and mitigation strategies, businesses can make informed decisions regarding cloud adoption and implement stronger security controls 1.6 Scope and Limitations

Scope:

This study focuses on identifying cybersecurity risks associated with cloud computing and evaluating practical strategies for mitigating these risks. It covers risks including data breaches, illegal access, malicious activity, and misconfigurations across a variety of computing environments, including private, public, and hybrid clouds. The research considers both technical and human factors contributing to cloud security vulnerabilities. In addition, it reviews existing risk assessment models, industry best practices, and compliance frameworks (e.g., ISO 27001, GDPR, and NIST).

The study will primarily focus on:

Platform as a Service (PaaS), Infrastructure as a Service (IaaS), and Software as a Service

(SaaS) models all have security concerns. Typical attack methods include denial-of-service (DoS) attacks, malware injection, and phishing. Identity and access management (IAM), encryption, access control, and incident response planning are examples of risk mitigation techniques. The function of user awareness, governance, and policy in cloud security.

Limitations:

Scope of Technologies: The study will not delve into highly specialized technologies (e.g., quantum cryptography or advanced AI-based threat detection) due to the project's practical and academic constraints.

Vendor-Specific Analysis: While general cloud security practices will be discussed, detailed evaluations of specific vendor platforms (e.g., AWS, Azure, Google Cloud) will be limited to widely accepted practices due to proprietary restrictions.

Geographical Context: Regulatory and legal aspects will primarily focus on international standards and may not fully explore country-specific laws unless broadly applicable.

Data Availability: The study relies on existing literature, case studies, and expert analysis; access to real-time threat data or proprietary incident reports may be limited.

Time Constraints: Given the academic timeline, longitudinal analysis or implementation of full-scale security solutions will not be conducted.

2.1 Review of Related Literature

Cloud computing has transformed the way firms keep, analyses, & manage information because it offers

© 2023-2025, IJARCS All Rights Reserved

economical, adaptable, and scalable solutions. To ensure cloud-based data and services 'availability, confidentiality, and integrity, new security risks and challenges have emerged.by this quick adoption must be addressed. This capstone project's goal is to examine the cybersecurity risks associated with cloud computing. and propose a set of strategies to mitigate these risks. According to (Sun, P. J. et, al 2019) The data that can be used on the platform is not under the owners' control in the cloud. For instance, the owner is unaware of whether the task is completed or not and whether the data is safeguarded. To enable businesses and organizations to use cloud computing technology and send their own data to a cloud service provider (CSP), issues with privacy and security, encryption, access control, and trust must be examined and resolved.

A major component of contemporary IT, cloud computing offers businesses several benefits, including affordability, expandability, and adaptability. To properly use cloud services, businesses must now protect information, apps, and cloud-based networks. The main objective of this thorough literature review is to be located to the most up to date data on security for cloud computing, with a focus on hazards and mitigation techniques. Additionally, it lists several prevalent risks associated with cloud computing security, including data breaches, distributed denial-of-service (DDoS) assaults, account theft, and virus attacks. According to (Alouffi, B et, al 2021) Distributed software architecture gave rise to the concept of "cloud computing" and its associated technologies, which aims to deliver hosted services via the internet. In the field of technological innovation, cloud computing has recently led to the emergence of numerous new user groups and sectors years. Two instances of distributed computing capabilities that are offered from data centers dispersed throughout the globe are Google apps and Microsoft SharePoint.

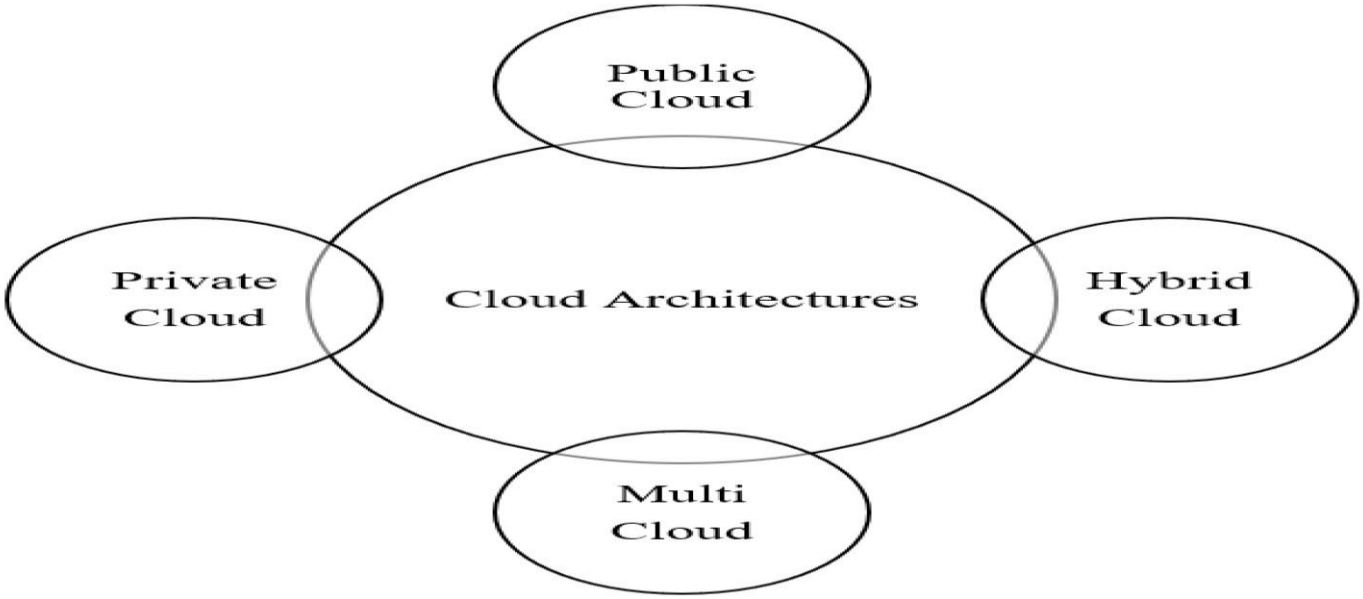

Fig. 2 .1 Architecture of Cloud Computing

2.2 Cloud Computing Overview

We give a summary of the development, advantages, and difficulties of cloud computing. Then, by contrasting We examine the risk factors identified in the auditing and accounting literature using a hand-selected sample of cloud-based firms and a matching group of non-cloud computing companies. The study uses a variety of attributes from auditing and accounting literature to characterize client-company risk, audit risk, including auditor related risk. greater leverage, a longer audit period, and a greater chance of a significant flaw. The dangers posed by cloud providers are not statistically significantly captured by the parameters included in the analysis. The study contributes to the corpus of knowledge about IT outsourcing throughout and cloud computing. The study also responds to the increasing need for insightful cloud research.

2.3 Cybersecurity Challenges in Cloud Environments

Resources and data can be dispersed over multiple sites and accessed from a range of industrial settings thanks to the adaptable framework provided by cloud computing. For industrial applications, cloud computing has transformed how resources like data, services, and apps are used, stored, and shared. Over the past ten years, many industries have swiftly moved to cloud computing because of its improved performance, reduced cost, and more extensive availability. Furthermore, the worldwide web of things (IoT) has advanced significantly because of the utilization of cloud computing. However, this rapid cloud migration raised several security issues and concerns. Traditional security procedures may not necessarily be applicable or even effective for cloud-based systems.

© 2023-2025, IJARCS All Rights Reserved

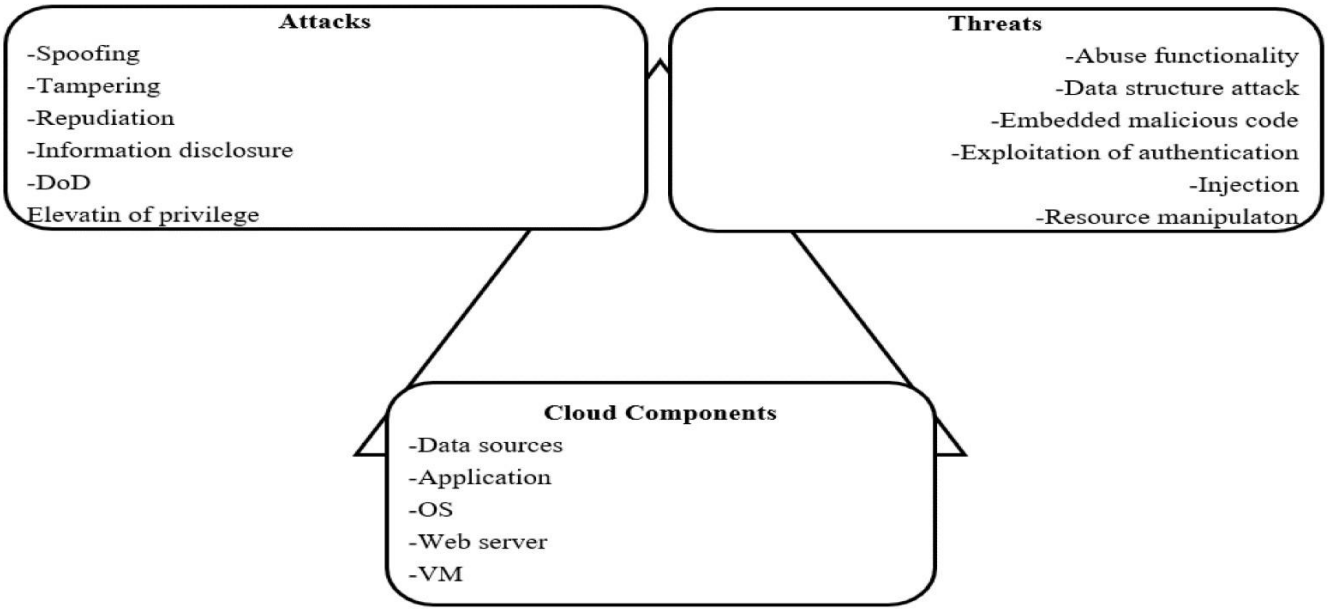

Fig. 02 .3: Attacks, threads, and components on cloud

2.4 Risk Management and Mitigation Strategies

An essential component of supply chain management, reverse logistics (RL) recycles goods used to recovery facilities to cut down on waste production. However, organizations appear hesitant to implement RL because of a variety of dangers that are seen as a threat to their bottom line. This study synthesizes the supply chain & risk management literature to identify and categorize RL risk variables and propose risk mitigation strategies to reduce the negative impacts of risks on RL deployment.

Methodology

A well-structured methodology for managing cloud computing security can be developed using the Goal Question Metric (GQM) approach. This involves creating a security metrics hierarchy aimed at producing a security index that reflects the security level of the cloud environment. This index helps in setting management priorities with a security focus.

2.5 Justification for a Structured Methodology

Complexity of Cloud Environments: Cloud infrastructures involve various every approach to deployment (public, private, and hybrid) and service models (IaaS, PaaS, and SaaS) have unique security considerations. A structured methodology provides a comprehensive framework to address these complexities. One of the newest and latest growing technologies in the IT industry is cloud computing. Among the services offered by Internet-based computing are network, storage, application, and software sharing. Dynamic Threat Landscape: Cyber threats are tremendously evolving. A systematic approach enables organizations to proactively recognize new risks and modify their security plans appropriately. Regulatory Compliance: Following guidelines like ISO/IEC 27001 require formalized risk management processes enforcing a structured methodology ensure compliance and demonstrate due effort.

2.6 Research Design: Qualitative Case Study Approach

A quantitative case study methodology is especially well-suited for investigating intricate, context dependent issues like cloud security. This design permitted an in-depth understanding of security challenges within real-world cloud settings. Researchers can obtain detailed insights into the particular security issues that firms implementing cloud technologies meet by concentrating on cases.

3.1 Analysis Techniques

The analysis techniques selected for this study are aligned with the qualitative and exploratory nature of the research. These techniques will help interpret data collected through literature review, case studies, and expert interviews, allowing for meaningful insights into the cybersecurity risks and mitigation strategies associated with cloud computing.

3.2 Risk Assessment Model Evaluation

The effectiveness of existing risk assessment models (such as the NIST Cybersecurity Framework or the ISO 27001 risk management standard) will be evaluated through qualitative content analysis. The goal is to determine how these models can be applied or adapted for cloud-specific risks. The

© 2023-2025, IJARCS All Rights Reserved

analysis will include evaluating the risk identification, assessment, and mitigation components of each model.

3.3 Surveys and Interviews

IT managers, cloud service providers, and cybersecurity experts may participate in surveys or semi-structured interviews. Primary information about how businesses evaluate and reduce cybersecurity threats in their data centers will be obtained from these interviews. To find patterns and examples of excellence in cloud security management, the qualitative data comprising interviews will be analyzed using thematic coding.

3.4 Statistical Analysis

If quantitative data is collected through surveys or publicly available reports (such as statistics on cloud breaches), statistical methods will be used to analyze the prevalence of certain types of attacks and the effectiveness of mitigation strategies. Descriptive statistics, correlation analysis, and trend analysis will be employed to draw insights from this data.

Project Plan and Execution

Work Breakdown Structure (WBS)

This hierarchical decomposition outlines the major deliverables and activities of your project.

Cybersecurity for Cloud Computing Project

Project Initiation

Define project objectives and scope

Identify stakeholders and team members

Conduct preliminary risk assessment Approve project proposal

Requirements Gathering & Research

Review existing literature and case studies

Identify key cloud security risks (e.g., data breaches, misconfigurations)

Analyze current mitigation techniques

Define security requirements and compliance standards (e.g., ISO 27001, NIST)

Risk Identification & Analysis

Classify risks (technical, legal, operational)

Prioritize risks based on impact and likelihood

Create risk register

Mitigation Strategy Development

Propose cloud security architecture enhancements

Recommend policies (e.g., IAM, encryption, logging)

Identify security tools/technologies (e.g., firewalls, SIEM, MFA)

Total Project Duration: Approx. 11 weeks (April 15 – June 30)

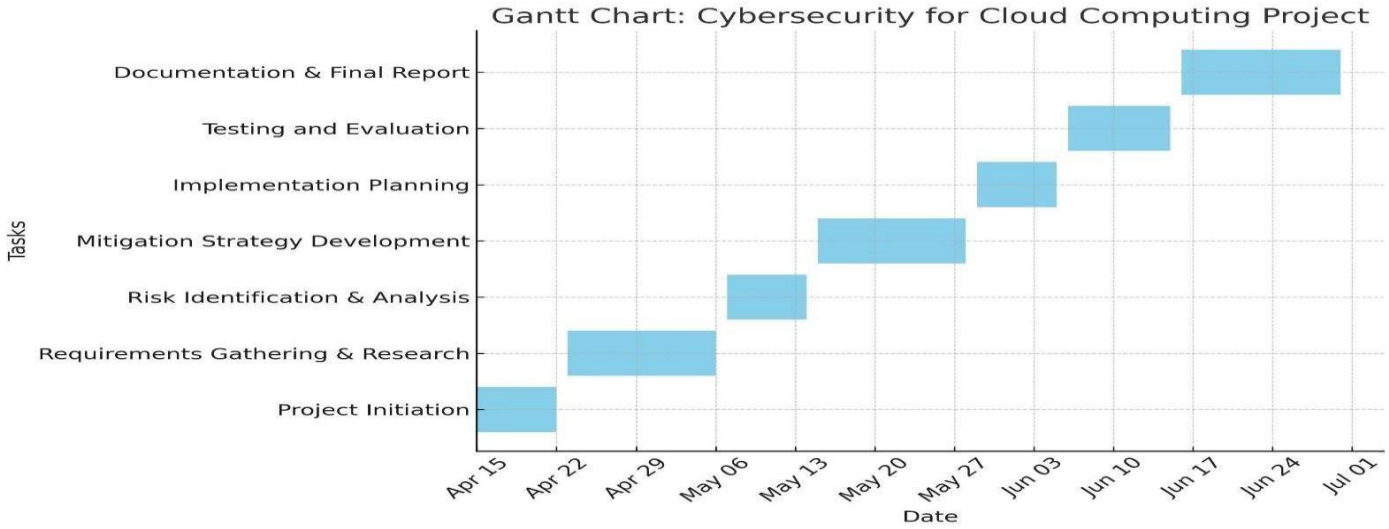

Fig 03.4: Gantt chart for internet of things project cybersecurity.

DISCUSSION

Problems and Difficulties with Security in Cloud Computing

Businesses face a range of cybersecurity challenges unique to the cloud environment as cloud usage keeps increasing. Some of the most urgent problems and difficulties are as follows Data Breaches and Data Loss:

Large volumes of sensitive data are stored on cloud platforms, which makes them appealing targets for hackers. Unauthorized access brought on by inadequate authentication, improperly designed storage, or software flaws can result in serious data spills or irreversible loss.

Insecure APIs and Interfaces

APIs are made available by cloud services so that users can communicate with the system. These APIs can act as entry points for attackers to intensify privileges and take advantage of services or obtain unauthorized data if they are not well secured.

© 2023-2025, IJARCS All Rights Reserved

Misconfiguration of Cloud Services
Among the most frequent causes of cloud vulnerabilities are improperly configured databases, storage buckets, or security groups. This shortcoming is randomly exacerbated by human errors and a lack of visibility across services.

Shared Responsibility Model Confusion
The shared responsibility paradigm of cloud computing, which requires customers to secure their own data, identities, and configurations while the provider oversees infrastructure security, is misunderstood by many enterprises.

Cybersecurity Risks in Cloud Computing
The study's initial goal was to determine the primary cybersecurity risks that organizations face when using cloud computing platforms. Based on the survey responses and interview insights, several key risks were highlighted, including

Findings and Analysis
The results of polls and discussions with IT specialists, security specialists, and decisionmakers in businesses utilizing cloud computing services are shown in this section. The investigation will concentrate on determining the main cybersecurity threats connected to cloud computers and the tactics used by businesses to reduce those threats.

4.1 Data Breaches
Organizations were found to be most concerned about data breaches utilizing cloud services. Nearly 60% of survey respondents highlighted data breaches as a primary threat. Interviewees also expressed concerns about the growing number of cyberattacks targeting cloud infrastructures. For instance, a respondent from a large financial institution noted that data breaches have a direct impact on customer trust and regulatory compliance.
Analysis:
Data breaches are a result of both external and internal threats, such as hacking and unauthorized access by insiders. This finding aligns with industry reports suggesting that cloud platforms are often targeted due to the vast amount of sensitive data stored on them. Mitigation strategies like encryption and advanced access controls are essential to reduce these risks.

4.2 Insider Threats
Another significant risk mentioned by 45% of survey participants was insider threats. These threats include malevolent acts taken by workers or subcontractors with proper permission to cloud systems. Because patient data is sensitive, insider threats are especially problematic, according to one of the respondents from the healthcare industry.
Analysis:
Internal threats are often difficult to detain because they involve individuals with legitimate access to systems. Implementing proper access controls, monitoring user behavior, and conducting regular security audits are vital to minimizing these risks.

4.3 Compliance and Regulatory Issues
According to a healthcare interviewee, cloud providers must have idea to specific standards to protect patient data, and 40% of survey participants mentioned difficulties in guaranteeing that they adhere to industry rules. Organizations that employ cloud services are particularly concerned about complying to rules and regulations like GDPR and HIPAA.
Analysis:
To guarantee data security and privacy, cloud companies are required to comply to several rules and frameworks. When choosing cloud service providers, organizations need to do their research to make sure they comply with industry regulations. Compliance distances are sometimes caused by a lack of ideas about the shared responsibility paradigm between providers of cloud services and consumers.

4.4 Inadequate Data Encryption
Inadequate encryption was highlighted by 30% of respondents as a cybersecurity risk. Many organizations store delicate information in the cloud but fail to encrypt it adequately. One respondent from a technology firm stated that while encryption at rest is commonly used, data in transit is often left unprotected.
Analysis:
Encryption is one of the better strategies to protect data in the cloud. Ensuring end-to-end encryption both at rest and in transit should be a priority for organizations assisting keep private data safe from unwanted access.

4.5 Mitigation Strategies Implemented by Organizations
The second motive of the study was to understand the strategies employed by organizations to mitigate cybersecurity risks accreditation with cloud computing. The findings serval a variety of practices and tools used to safeguard cloud environments.

4.6 Multi-Factor Authentication (MFA)
Multi-Factor Authentication (MFA) is recently the most used method of implemented security measures, with 75% of respondents indicating that their organization need MFA for access to cloud platforms. One respondent from a retail company explained that MFA has significantly reduced the possibility of unaware access to virtual resources.
Analysis:
MFA is an outstanding security measure, as it adds an extra degree of security by mandating that users use more than simply a password to confirm their identity. This tactic

© 2023-2025, IJARCS All Rights Reserved

successfully decreased the chances of credential theft, a frequent point of entry for attackers.

4.7 Data Encryption

Another popular mitigating technique was to encrypt data both in transmission and at rest. with 65% of survey respondents indicating its use. Organizations use different encryption measurements such as AES-256, to confirm safeguarding private information.

Analysis:

Encryption remains Among the best strategies to protect data from unwanted access, especially in multi-tenant cloud environments. The use of strong encryption protocols is important in safeguarding data, even if a hacker manages to access the system.

CONCLUSION:

The purpose of the study is to further the field of security in the cloud by determining the hazards unique to cloud technology settings and offer a wide range of risk-reduction tactics. With an increasing number of organizations migrating to the clouds, ensuring the security of these environments has never been more important. The proposed research could lead to improved security practices, a stronger understanding of cloud vulnerabilities, and practical Tools for securing cloud infrastructures. Scalability, which is flexibility, and cost effectiveness are just a few of the groundbreaking advantages that cloud computing provides for businesses. These benefits do, however, come with a few cybersecurity threats that, if left unchecked, might jeopardize the availability, confidentiality, and integrity of data. Finding the primary cybersecurity threats that cloud settings encounter and looking at workable mitigation strategies to strengthen cloud security were the goals of this study.

REFERENCES:

[1] Awodele, O., Ogbonna, C., Ogu, E. O., Hinmikaiye, J. O., & Akinsola, J. E. T. (2024). Characterization and risk assessment of cybersecurity threats in cloud computing: A comparative evaluation of mitigation techniques. Acadlore Trans. Mach. Learn, 3(2), 106118.

[2] Sun, P. J. (2019). Privacy protection and data security in cloud computing: a survey, challenges, and solutions. Ieee Access, 7, 147420-147452.

[3] Alouffi, B., Hasnain, M., Alharbi, A., Alosaimi, W., Alyami, H., & Ayaz, M. (2021). A systematic literature review on cloud computing security: threats and mitigation strategies. Ieee Access, 9, 57792-57807.

[4] Zhang, X., Wuwong, N., Li, H., & Zhang, X. (2010, June). Information security risk management framework for the cloud computing environments. In 2010 10th IEEE international conference on computer and information technology (pp. 1328-1334). IEEE.

[5] Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 34(1), 1–11. https://doi.org/10.1016/j.jnca.2010.07.006

[6] Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. Future Generation Computer Systems, 28(3), 583–592. https://doi.org/10.1016/j.future.2010.12.006

[7] Rittinghouse, J. W., & Ransome, J. F. (2016). Cloud computing: Implementation, management, and security (2nd ed.). CRC Press. ISBN: 978-1498782152

[8] Tissir, N., El Kafhali, S. & Aboutabit, N. Cybersecurity management in cloud computing: semantic literature review and conceptual framework proposal. J Reliable Intell Environ 7, 69–84 (2021). https://doi.org/10.1007/s40860-020-00115-0

[9] Senouci, O., & Benaouda, N. (2025). Enhancing Phishing Detection in Cloud Environments Using RNN-LSTM in a Deep Learning Framework. Journal of Telecommunications and Information Technology, (1), 1-9.

[10] Ankalaki, S., Rajesh, A. A., Pallavi, M., Hukkeri, G. S., Jan, T., & Naik, G. R. (2025). Cyber-attack prediction: From traditional machine learning to generative artificial intelligence. IEEE Access.

[11] Rakibuzzaman, M., Khan, M. I., & Hasan, M. M. (2024). Cybersecurity Investment Prioritization Using Business Analytics: A Decision Support Framework. American Journal of Business, 1(1).

[12] Asad, K., & Farooqui, M. F. (2025). A Study of Cyber Threats and Security Frameworks in Cloud Computing. In Cyberology (pp. 120-134). Chapman and Hall/CRC.

© 2023-2025, IJARCS All Rights Reserved