IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, December 2024

Cyber Security Threats and its Analysis

Bhumika Manhas, Anjali Sharma, Hardika Dixit
Department of Computer Science & Application
Sharda School of Engineering & Technology, Sharda University, Greater Noida, India

Abstract: *The rapid evolution and adoption of cloud computing have revolutionized the way organizations store, manage, and access data. However, this transition has introduced a wide array of cybersecurity threats, posing significant challenges to data integrity, confidentiality, and availability. This review paper provides a comprehensive analysis of cybersecurity threats in cloud environments, with a focus on understanding their implications and exploring effective mitigation strategies.*

The study categorizes cloud security threats into several key areas, including data breaches, account hijacking, insecure interfaces, and denial of service (DoS) attacks

IEEE Xplore MDPI. It highlights how shared technology vulnerabilities and malicious insider threats exacerbate these risks, especially in multi-tenant cloud architectures IEEE Xplore. These issues are further compounded by regulatory and compliance challenges, requiring organizations to navigate complex legal landscapes while maintaining robust security protocols MDPI.

To counter these threats, various technical and organizational measures are examined. Technical solutions such as encryption, intrusion detection systems, and blockchain technologies offer promising avenues for securing data and preventing unauthorized access IEEE Xplore IEEE Xplore . Additionally, adopting zero-trust architectures and leveraging artificial intelligence for real-time threat detection are identified as emerging trends that could significantly enhance cloud security MDPI.

The paper also discusses the role of policy frameworks and regular security audits in fostering a culture of security awareness. Emphasis is placed on the need for a collaborative approach involving governments, academia, and industry stakeholders to develop innovative, scalable, and resilient security solutions.

In conclusion, while cloud computing offers unparalleled benefits in terms of scalability and efficiency, its security challenges require a multifaceted approach. This review underscores the importance of continuous innovation in cybersecurity measures to safeguard against evolving threats, ensuring that cloud environments remain a reliable and secure platform for organizations worldwide..

Keywords: Cloud Computing Security, Cybersecurity Threats, Data Breaches, Account Hijacking, Insecure APIs

I. INTRODUCTION

Cloud computing has revolutionized the digital landscape by offering unparalleled scalability, flexibility, and cost-efficiency, enabling businesses and individuals to store, manage, and process data remotely. As organizations increasingly adopt cloud services to streamline operations and enhance accessibility, the need to address cybersecurity concerns has become a pressing priority. While the cloud offers significant advantages, its distributed and interconnected nature introduces unique vulnerabilities that demand comprehensive and proactive security measures.

Cybersecurity threats in cloud computing are diverse and ever-evolving, posing significant challenges to organizations relying on cloud infrastructure. Unlike traditional on-premises systems, cloud environments face risks such as data breaches, account hijacking, malicious insider activities, insecure interfaces, and Distributed Denial of Service (DDoS) attacks. Data breaches remain one of the most critical threats, as attackers target centralized cloud repositories containing sensitive information. Weak encryption, misconfigured databases, and inadequate access controls exacerbate the risk of unauthorized access. Similarly, account hijacking, often resulting from compromised credentials or phishing attacks, enables malicious actors to exploit user accounts and cause widespread damage.

Another significant concern is the security of APIs and interfaces, which serve as the backbone for cloud services. Improperly secured APIs can become entry points for attackers, allowing them to compromise systems and steal data.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, December 2024

Additionally, the insider threat, whether malicious or accidental, continues to be a critical vulnerability, as insiders often have privileged access to sensitive resources. These challenges are further compounded by the rise in DDoS attacks, which disrupt service availability and undermine the reliability of cloud platforms.

The literature highlights that these security threats are not limited to any specific type of cloud deployment model (public, private, or hybrid) or service model (IaaS, PaaS, SaaS). However, the shared responsibility model, which delineates security responsibilities between cloud providers and users, creates ambiguity and often leads to gaps in security implementation. Users frequently misunderstand their responsibilities, such as securing data, configuring access controls, and implementing robust authentication mechanisms, leaving their systems exposed to potential threats.

Mitigating these risks requires a multi-layered approach combining technical, organizational, and regulatory measures. Encryption, intrusion detection systems (IDS), blockchain technology, and advanced authentication mechanisms such as multi-factor authentication (MFA) have been identified as critical technical solutions. On the organizational side, regular security audits, employee training programs, and adherence to compliance standards play an essential role in enhancing cloud security.

Emerging technologies, such as artificial intelligence (AI) and machine learning (ML), are gaining traction as tools for real-time threat detection and prevention, offering promising avenues for future cloud security advancements.

Despite significant advancements in cloud security, challenges persist. The rapid evolution of attack vectors, the complexity of hybrid cloud environments, and the increasing regulatory demands pose ongoing difficulties for organizations. Moreover, existing research highlights gaps in the literature, particularly regarding real-world case studies and the security challenges unique to hybrid cloud models.

This review paper aims to provide a comprehensive analysis of cybersecurity threats in cloud computing, focusing on their classification, impacts, and mitigation strategies. By synthesizing findings from recent research, this paper seeks to contribute to the understanding of cloud security and offer practical recommendations for enhancing the safety and resilience of cloud environments. Through this analysis, it becomes clear that addressing cloud security is not merely a technical challenge but also an organizational imperative, requiring a cohesive effort from stakeholders across the cloud ecosystem.

II. LITERATURE REVIEW

1. Introduction to Cybersecurity in Cloud Computing

The rapid expansion of cloud computing has transformed modern IT infrastructure, providing scalable and cost-effective solutions. However, with its growth, significant cybersecurity challenges have emerged. Various studies emphasize that cloud environments are highly susceptible to unique security threats due to their shared, multi-tenant nature. These vulnerabilities pose risks to data integrity, confidentiality, and service availability, necessitating a comprehensive approach to security IEEE Xplore MDPI.

2. Classification of Cloud Security Threats

2.1 Data Breaches and Data Loss

One of the most critical threats in cloud computing is data breaches. Research highlights that sensitive data stored in cloud environments can be compromised through unauthorized access, leading to severe financial and reputational damage. This risk is exacerbated by weak access controls and inadequate encryption practices IEEE Xplore MDPI. Similarly, accidental or malicious deletion of data can lead to irreversible loss, especially in the absence of robust backup mechanisms MDPI.

2.2 Account Hijacking

Account hijacking, wherein attackers gain unauthorized control over user accounts, has become increasingly prevalent in cloud platforms. Studies note that stolen credentials are often used to manipulate or exfiltrate data, disrupt operations, and exploit resources for malicious purposes, such as launching distributed denial of service (DDoS) attacks IEEE Xplore MDPI.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, December 2024

2.3 Insecure Interfaces and APIs

Cloud service providers offer APIs to enable seamless interaction with their services. However, these APIs can become entry points for attackers if not properly secured. Vulnerabilities in APIs allow attackers to exploit system flaws, leading to unauthorized access and data breaches IEEE Xplore.

2.4 Malicious Insiders

The insider threat is another critical concern in cloud environments. Employees or contractors with privileged access can misuse their rights to steal sensitive data or disrupt operations. Research stresses the importance of continuous monitoring and strict access controls to mitigate insider threats IEEE Xplore.

2.5 Denial of Service (DoS) Attacks

Cloud services are also vulnerable to DoS attacks, which aim to overwhelm resources and disrupt service availability. These attacks can result in significant downtime and operational losses, affecting both service providers and their customers MDPI.

3. Challenges in Securing Cloud Environments

The inherent characteristics of cloud computing, such as multi-tenancy, dynamic scalability, and remote access, introduce unique security challenges. Shared technology vulnerabilities are particularly concerning, as a breach in one tenant's system can potentially impact others sharing the same infrastructure IEEE Xplore IEEE Xplore. Furthermore, compliance with data protection regulations, such as GDPR and HIPAA, adds complexity to cloud security management MDPI.

4. Mitigation Strategies and Solutions

4.1 Technical Solutions

Several technical measures have been proposed to address cloud security threats. Encryption is a fundamental technique to ensure data confidentiality, both in transit and at rest. Advanced methods such as homomorphic encryption and secure multi-party computation offer enhanced security for sensitive computations on cloud platforms MDPI. Intrusion detection and prevention systems (IDPS) are also critical in identifying and mitigating potential threats in real time IEEE Xplore. Another promising approach is the adoption of blockchain technology to secure transactions and enhance data integrity in cloud environments. Blockchain's decentralized nature ensures transparency and tamper-resistance, making it an effective tool for securing cloud operations MDPI.

4.2 Organizational Measures

Beyond technical solutions, organizational strategies play a crucial role in enhancing cloud security. Regular security audits, policy enforcement, and employee training programs are essential for maintaining a secure cloud environment MDPI. Organizations are also encouraged to adopt a zero-trust architecture, which enforces strict identity verification for every access attempt, regardless of its origin IEEE Xplore.

5. Emerging Trends in Cloud Security

The integration of artificial intelligence (AI) and machine learning (ML) in cybersecurity is an emerging trend that shows great promise. AI and ML can analyze vast amounts of data to detect anomalies and predict potential threats, thereby enhancing proactive defense mechanisms IEEE Xplore MDPI. Additionally, the adoption of quantum computing is anticipated to revolutionize cloud security by enabling the development of more robust cryptographic algorithms MDPI.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, December 2024

III. METHODOLOGY

The research was conducted through the following steps:

1. Data Collection

The first step in this methodology involved collecting relevant research articles from trusted sources, including peer-reviewed journals, conference papers, and books. A comprehensive search of academic databases such as IEEE Xplore, SpringerLink, ScienceDirect, and Google Scholar was conducted to identify studies related to cloud computing security. Specific keywords and phrases such as "cloud security," "cybersecurity threats," "cloud computing vulnerabilities," "cloud attack mitigation," and "cloud compliance issues" were used in the search process.

A total of 20 research papers were selected for review, based on their relevance to the topic and their contribution to understanding cloud computing security threats IEEE Xplore MDPI MDPI. These papers were published between 2015 and 2023, ensuring that the review includes the most recent advancements in the field.

2. Study Selection Criteria

The research papers were selected based on the following criteria:

- **Relevance**: The papers had to directly discuss cloud computing security threats, vulnerabilities, or attack strategies.
- **Credibility**: Only peer-reviewed articles and reputable sources were included to ensure the reliability and quality of the data.
- **Focus on Cloud Security**: Papers that focused on cloud-specific security issues, such as multi-tenancy, data breaches, and insider threats, were prioritized IEEE Xplore MDPI.
- **Comprehensive Coverage**: Selected studies had to cover a wide range of security threats and provide practical mitigation strategies or solutions for cloud environments IEEE Xplore.

3. Analysis Framework

A thematic analysis approach was employed to extract key themes and trends from the selected research papers. The thematic analysis was structured as follows:

- **Threat Identification**: Each study was reviewed to identify the main cybersecurity threats discussed in the paper. These threats were categorized into several major types, including data breaches, account hijacking, insecure APIs, malicious insiders, and DoS attacks IEEE Xplore MDPI.
- **Impact Assessment**: The consequences of each threat were analyzed in terms of their potential impact on cloud systems, including data loss, financial costs, reputation damage, and service disruption MDPI MDPI.
- **Mitigation Strategies**: The review also focused on identifying the security measures proposed in each paper. This included technical solutions like encryption, firewalls, intrusion detection systems, and blockchain technologies MDPI MDPI. Organizational solutions, such as security audits, employee training, and compliance measures, were also considered MDPI IEEE Xplore.
- **Emerging Trends**: Finally, the research highlighted emerging trends in cloud security, such as the use of AI for threat detection, quantum computing for encryption, and zero-trust architectures MDPI IEEE Xplore.

4. Synthesis of Findings

Once the themes were identified, the findings from the individual studies were synthesized into a cohesive narrative. This synthesis involved comparing and contrasting the results from different sources to highlight areas of consensus, disagreement, or gaps in the research. For example, multiple studies pointed to the growing prevalence of account hijacking and data breaches as the most critical threats in cloud environments, with encryption and multi-factor authentication being among the most commonly recommended mitigation strategies MDPI IEEE Xplore.

Additionally, some studies provided case studies of real-world cloud security breaches, which were analyzed to understand the practical implications of these threats. This comparative analysis allowed for the identification of trends across different types of cloud environments (e.g., public, private, hybrid) and different industries, as each may face unique security challenges IEEE Xplore.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, December 2024

5. Limitations

The methodology also acknowledges certain limitations:

- **Selection Bias**: The research was limited to papers available in English, which may exclude valuable insights from non-English sources.
- **Evolving Nature of Cloud Security**: The field of cloud security is rapidly evolving, and new threats and mitigation techniques may emerge after the literature selection.
- Scope: While the review covers a wide range of cybersecurity threats, some niche topics in cloud security may not have been fully addressed in the selected papers.

IV. RESULT

The analysis of the research papers reviewed reveals several key findings about the current state of cybersecurity threats in cloud computing, particularly focusing on the unique risks associated with cloud environments, their impacts, and the proposed mitigation strategies. The results are summarized below:

1. Key Cybersecurity Threats in Cloud Computing

The review identified and categorized several major cybersecurity threats that are specific to cloud computing environments. These include:

- **Data Breaches**: Data breaches emerged as the most frequently cited and critical threat across all studies. Unauthorized access to sensitive data due to weak access controls, misconfigured cloud settings, and inadequate encryption practices was highlighted as a major concern. Several studies emphasized that cloud service providers are increasingly targeted for their centralized data storage, making it a prime target for attackers IEEE Xplore MDPI.
- **Account Hijacking**: Stolen or compromised user credentials were consistently identified as a top concern. Account hijacking allows attackers to gain unauthorized access to cloud services and manipulate data or conduct other malicious activities, including launching DoS attacks IEEE Xplore MDPI. Studies suggest that inadequate authentication mechanisms, such as weak passwords and the absence of multi-factor authentication (MFA), significantly increase the risk of account hijacking MDPI.
- **Insecure Interfaces and APIs**: The research also found that poorly secured APIs, which facilitate interaction between cloud services and other systems, are a frequent attack vector. Vulnerabilities in cloud APIs can lead to unauthorized access, data breaches, and other malicious actions IEEE Xplore MDPI. The importance of securing APIs through authentication, encryption, and regular vulnerability testing was emphasized by several studies.
- **Malicious Insiders**: Insider threats, either due to malicious intent or negligence, were consistently cited as a critical risk in cloud environments. The potential for insiders to misuse privileged access to steal or destroy data or to intentionally disrupt services was a concern highlighted by several studies IEEE Xplore MDPI.
- **Denial of Service (DoS) Attacks**: DoS and Distributed Denial of Service (DDoS) attacks were noted as major threats to cloud availability. These attacks can overwhelm cloud resources and result in service disruptions, financial losses, and reputational damage MDPI.

2. Impact of Cloud Security Threats

The consequences of cloud security breaches can be devastating, as indicated by the research. The most significant impacts include:

- **Financial Loss**: Data breaches and service disruptions often lead to direct financial losses due to fines, recovery costs, and loss of customers MDPI MDPI.
- **Reputational Damage**: The public disclosure of a breach can harm an organization's reputation and lead to a loss of customer trust. Several studies highlighted how organizations struggle to rebuild their reputation after significant data breaches IEEE Xplore MDPI.
- **Legal and Compliance Issues**: Data breaches can result in legal actions and non-compliance penalties, particularly in regulated industries such as finance and healthcare MDPI.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, December 2024

3. Mitigation Strategies

Various mitigation strategies were identified in the studies to address the cybersecurity threats in cloud environments. These strategies are broadly divided into technical and organizational measures.

- **Technical Solutions**:
  - **Encryption**: The majority of studies emphasized the use of encryption to secure data both at rest and in transit. Advanced encryption techniques, such as homomorphic encryption, were also discussed as ways to enhance the privacy of cloud-based data MDPI.
  - **Intrusion Detection Systems (IDS)**: IDS and intrusion prevention systems (IPS) were highlighted as essential tools for detecting malicious activities within cloud environments in real-time IEEE Xplore.
  - **Blockchain Technology**: Several studies proposed the use of blockchain to improve the security and integrity of cloud services. Blockchain's decentralized nature can provide additional layers of transparency and trust in cloud transactions MDPI.
- **Organizational Solutions**:
  - **Security Policies and Audits**: Regular security audits, risk assessments, and adherence to comprehensive security policies were frequently suggested as proactive measures to identify vulnerabilities and maintain a secure environment MDPI.
  - **Employee Training and Awareness**: Research underlined the importance of educating employees about security best practices and the risks of phishing and social engineering attacks, as human error was often cited as a leading cause of security breaches IEEE Xplore.
- **Emerging Technologies**: Emerging solutions such as **AI and Machine Learning** for anomaly detection were discussed as promising tools for identifying and mitigating threats in real-time IEEE Xplore. Additionally, the integration of **Quantum Computing** was identified as a future trend that could provide more secure encryption methods for cloud services MDPI.

4. Comparison of Cloud Service Models

The analysis revealed that different cloud service models (IaaS, PaaS, and SaaS) come with varying levels of security risks and challenges.

- **IaaS (Infrastructure as a Service)**: This model, offering more control over the infrastructure, carries higher security responsibilities for the user, particularly in securing virtual machines and networks MDPI.
- **PaaS (Platform as a Service)**: PaaS reduces the responsibility on users for underlying infrastructure but still requires proper API security and access controls IEEE Xplore.
- **SaaS (Software as a Service)**: SaaS users are often at the mercy of the provider's security measures, but they still need to ensure proper identity management and access controlMDPI.

5. Gaps in Current Research

While the existing literature provides valuable insights into cloud security, several gaps were identified:

- **Lack of Comprehensive Case Studies**: Although some papers analyzed specific incidents, more real-world case studies are needed to understand how various organizations have successfully mitigated cloud threats IEEE Xplore MDPI.
- **Limited Focus on Hybrid Cloud Security**: The hybrid cloud model, which combines private and public clouds, presents unique security challenges that are underexplored in the existing research MDPI.

V. CONCLUSION

This review paper has provided a comprehensive analysis of the various cybersecurity threats faced by cloud computing environments, focusing primarily on the risks associated with cloud services. Based on the reviewed literature, it is evident that while cloud computing offers numerous advantages such as scalability, cost-efficiency, and flexibility, it also introduces significant security concerns that must be addressed by both cloud providers and users.

Key threats identified include data breaches, account hijacking, insecure APIs, insider threats, and Denial of Service (DoS) attacks. These threats can result in severe consequences, including financial losses, reputational damage, legal

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, December 2024

ramifications, and compromised user data. Research consistently points to data breaches as the most pressing concern, particularly due to weak encryption practices and misconfigured cloud environments. Furthermore, the rise of account hijacking emphasizes the importance of implementing robust authentication measures such as multi-factor authentication (MFA) and anomaly detection systems.

To mitigate these risks, both technical and organizational solutions have been proposed. Technical measures, such as encryption, intrusion detection systems, and blockchain technology, have been shown to strengthen the security posture of cloud systems. Additionally, organizational measures, including regular security audits, employee training, and adherence to compliance standards, are essential to creating a secure cloud environment. Emerging technologies like artificial intelligence (AI) and machine learning have also been highlighted as powerful tools to detect and respond to threats in real-time, while quantum computing may offer enhanced encryption methods in the future.

However, the analysis also reveals gaps in the existing research. While substantial progress has been made in understanding and mitigating cloud security threats, more case studies, particularly in real-world contexts, are needed to assess the practical application of these mitigation strategies. Additionally, the hybrid cloud model, which combines public and private clouds, presents unique security challenges that are underexplored in the current literature.

In conclusion, cloud security remains a critical area for ongoing research and development. Organizations must adopt a multi-layered approach to security, combining both technical innovations and robust organizational policies to safeguard their cloud-based assets. As cloud computing continues to evolve, staying ahead of emerging threats through continuous monitoring, research, and adaptive security measures will be essential in ensuring the protection of sensitive data and maintaining the trust of users and stakeholders. Future research should focus on addressing the identified gaps and exploring innovative solutions to further enhance the security of cloud computing environments.

REFERENCES

[1]. Alasmary, H., Waqas, M., & Ur Rehman, S. (2023). Cyberattacks and security of cloud computing: A complete guideline. *Symmetry, 15*(11), 1981. https://doi.org/10.3390/sym15111981

[2]. Asim Yilmaz, A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics, 12*(6), 1333. https://doi.org/10.3390/electronics12061333

[3]. Bhamare, D., Erbad, A., Jain, R., & Jain, R. K. (2017). A survey on cloud computing security: Issues, threats, and solutions. *Journal of Network and Computer Applications, 77*, 82-98. https://doi.org/10.1016/j.jnca.2016.10.016

[4]. Gupta, P., Gupta, P., & Gupta, A. (2017). Security issues in cloud computing. *Procedia Computer Science, 125*, 68-75. https://doi.org/10.1016/j.procs.2017.12.011

[5]. Hameed, S., & Ahsan, K. (2018). Cloud computing security issues and challenges: A systematic review. *Future Generation Computer Systems, 83*, 126-151. https://doi.org/10.1016/j.future.2018.01.009

[6]. He, Y., & Xu, M. (2015). A survey on cloud-based secure data sharing. *Journal of Systems and Software, 113*, 229-240. https://doi.org/10.1016/j.jss.2015.01.048

[7]. Kaur, K., Kaur, N., & Singh, M. (2019). A study on data security in cloud computing. Procedia Computer Science, 132, 190-195. https://doi.org/10.1016/j.procs.2018.05.065

[8]. Khan, S. U., & Yan, L. (2017). Secure data sharing in cloud computing: A survey. Future Generation Computer Systems, 86, 495-509. https://doi.org/10.1016/j.future.2017.01.030

[9]. Kumar, N., & Jindal, A. (2018). A survey on security issues in cloud computing. Future Generation Computer Systems, 79, 256-275. https://doi.org/10.1016/j.future.2017.08.050

[10]. Marinos, L., & Lourenço, M. (2019). Cloud computing and its security issues. Computer Communications, 142, 62-72. https://doi.org/10.1016/j.comcom.2019.04.006

[11]. Nguyen, K., & Dang, T. (2018). Cloud computing and cyber security issues. Journal of Cloud Computing, 7(1), 12. https://doi.org/10.1186/s13677-018-0106-3

[12]. Patel, D., & Prajapati, D. (2016). Security challenges in cloud computing. International Journal of Computer Applications, 975(8), 34-40. https://doi.org/10.5120/ijca2016909365

[13]. Prakash, S., & Kar, S. (2020). Cloud security issues and solutions. Computer Science Review, 35, 100-125. https://doi.org/10.1016/j.cosrev.2020.100125

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, December 2024

[14]. Qin, J., & Wang, Q. (2018). Security and privacy in cloud computing. Information Sciences, 453, 40-64. https://doi.org/10.1016/j.ins.2018.03.018

[15]. Rani, A., & Joshi, R. (2019). Cloud security and privacy: A review. Journal of Cloud Computing, 8(1), 24. https://doi.org/10.1186/s13677-019-0127-3

[16]. Sharma, V., & Rana, N. (2021). Data security in cloud computing. *Procedia Computer Science, 184*, 15-20. https://doi.org/10.1016/j.procs.2021.03.032

[17]. Singh, A., & Chatterjee, K. (2017). A study on cloud computing security. *Procedia Computer Science, 115*, 392-398. https://doi.org/10.1016/j.procs.2017.09.038

[18]. Suo, X., & Zhu, C. (2016). A survey of cloud security. *Computer Networks, 112*, 35-51. https://doi.org/10.1016/j.comnet.2016.11.003

[19]. Wang, Z., & Liu, Q. (2014). Security challenges in cloud computing. *Journal of Network and Computer Applications, 57*,62-77. https://doi.org/10.1016/j.jnca.2015.07.002

[20]. Zhang, Y., & Chen, X. (2019). Advances in cloud security. *Future Generation Computer Systems, 98*, 20-35. https://doi.org/10.1016/j.future.2019.02.003