International Journal of Computational and Experimental Science and ENgineering (IJCESEN)

Vol. 12-No.1 (2026) pp. 823-830
http://www.ijcesen.com

ISSN: 2149-9144

Research Article

Investigating the Security and Privacy Implications of Cloud-Based Disaster Recovery

Somaning Turwale *

Shivaji University, India
* **Corresponding Author Email:** turwales@gmail.com - **ORCID:** 0000-0002-5247-9060

Article Info:

DOI: 10.22399/ijcesen.4921
Received : 05 February 2026
Revised : 15 February 2026
Accepted : 20 February 2026

Keywords

Cloud Computing Security,
Disaster Recovery,
Data Privacy,
Access Control,
Encryption Mechanisms,
Security Frameworks

Abstract:

The article explores security weaknesses in cloud disaster recovery setups. One of the major concerns is that confidential information may be exposed unintentionally during replication. The article also highlights that if the recovery environment's access control is not robust, it can be a great exploit for hackers to gain unauthorized access. Furthermore, the privacy aspect is affected due to data residency and multi-tenant isolation issues. In the same article, it is pointed out that protection such as encryption, identity management, and network security controls is are way in which the system can be shielded against threats. The next paragraph talks about the need for having proper governance in place as a prerequisite for deploying security recovery architectures. Apart from that, regular reviews of the system, execution of data handling measures, and preparation for the response team in the event of an incident are also part of the organization's playbook. The last sentence states that companies should not forget the challenge of striking a balance between the need to recover operations and protect data so as not to lose their resilience, and at the same time not break the rules.

1. Introduction

Disaster recovery constitutes a fundamental operational requirement for organizations dependent on digital infrastructure. Traditional recovery strategies relied on secondary physical data centers. Although such methods were feasible, they came at a high price due to the need for a sizeable capital outlay and continuous maintenance of the system. Cloud-computing disaster recovery redefines the way the system works by making it possible for resources to be provisioned on demand. The National Institute of Standards and Technology describes cloud computing as a model that facilitates ubiquitous, convenient, and on-demand network access to a shared pool of configurable computing resources [1]. Some of the resources are the networks, servers, storage, applications, and services. Cloud infrastructure can be rapidly provisioned and released with minimal management effort or service provider interaction [1].

The essential characteristics of cloud computing directly support disaster recovery objectives. On-demand self-service allows organizations to provision computing capabilities automatically without requiring human interaction with service providers [1]. Rapid elasticity enables resources to scale outward and inward commensurate with demand [1]. Resource pooling permits provider computing resources to serve multiple consumers using a multi-tenant model [1]. These characteristics eliminate the need for dedicated standby infrastructure. Recovery environments can remain dormant until activation becomes necessary.

The migration of disaster recovery functions to cloud environments introduces distinct security challenges. Information system security requires a comprehensive evaluation of risks associated with data replication and storage across a distributed infrastructure. Federal information security standards establish requirements for protecting information systems through appropriate security controls [2]. The Federal Information Security Management Act mandates that organizations implement security programs addressing confidentiality, integrity, and availability objectives [2]. Compliance with such standards necessitates continuous assessment of security postures across all operational environments, including disaster recovery sites.Cloud-based disaster recovery architectures must address security control

implementation across trust boundaries. Data traversing network segments between production and recovery environments faces exposure risks during transmission. Multi-tenant cloud infrastructure introduces shared responsibility considerations. The service delivery models defined by NIST include Software as a Service, Platform as a Service, and Infrastructure as a Service [1]. Each model distributes security responsibilities differently between providers and consumers. Infrastructure as a Service deployments place greater security obligations on consuming organizations.

Security compliance frameworks require organizations to demonstrate effective control implementation through documented evidence and testing. FISMA compliance demands that information systems undergo security categorization, control selection, and continuous monitoring [2]. Disaster recovery environments must satisfy identical compliance requirements as production systems. An article analyzes the security and privacy implications of cloud-based disaster recovery. The examination is focused on vulnerabilities arising from cloud replication methods, access control issues, and data residency challenges related to jurisdiction. Protective frameworks and technical controls receive detailed evaluation. Implementation guidelines establish pathways for secure recovery architecture deployment.

2. Related Work

Security issues with cloud computing have been the focus of available research, and this has paved the way for a thorough understanding of the threats that have an impact on distributed infrastructures. The earlier research has identified the challenges in virtualization exploitation, difficulties in ensuring the isolation of the multi-tenant environment, and the creation of secure data mechanisms in cloud environments. However, limited attention has been directed toward security implications specific to disaster recovery implementations. The intersection of business continuity requirements and cloud security controls presents unique challenges requiring dedicated examination.

The article builds upon established cloud security frameworks while extending focus to disaster recovery contexts. A systematic evaluation of vulnerability categories identifies data exposure risks during replication processes and access control weaknesses in recovery environments. Privacy implications arising from cross-border data transfers and jurisdictional regulatory variations receive detailed treatment. The contribution establishes connections between general cloud security principles and specific disaster recovery operational requirements.

The technical framework integrates layered defensive architectures addressing multiple threat vectors simultaneously. Encryption mechanisms, identity management controls, and network isolation strategies form interconnected protective layers. Implementation guidelines translate theoretical security requirements into practical governance structures. The framework emphasizes security control persistence throughout failover operations. Recovery testing procedures incorporate security validation activities, ensuring protection mechanisms remain effective during actual disaster events. The contribution bridges gaps between cloud security theory and disaster recovery operational practice.

3. Security Vulnerabilities in Cloud Disaster Recovery

Cloud disaster recovery architectures present distinct security vulnerabilities requiring systematic examination. The migration of critical organizational data to cloud environments expands potential attack vectors. Understanding vulnerability categories enables appropriate control implementation.

3.1 Data Exposure During Replication

Continuous replication of production data to cloud recovery environments creates persistent exposure windows. Data packets traverse multiple network segments during transmission. Cloud computing environments introduce security challenges related to data transmission across shared infrastructure [3]. The lack of direct control over network paths increases interception risks. Encryption mechanisms must protect data throughout. On the one hand, emergency escape routes have to maintain a certain level of security, while on the other hand, they should not impair regular operations in any way. The utilization of privileged access management ensures that the administrative functionalities are limited to a certain extent, i.e., only those capabilities that are necessary are allowed.

Storage-level vulnerabilities compound transmission concerns significantly. Replicated data in cloud storage faces exposure through multiple vectors. Misconfigured access policies represent a common vulnerability category in cloud deployments [3]. The multi-tenant nature of cloud infrastructure raises data isolation concerns. Physical storage resources remain shared among

multiple consumers. Logical separation mechanisms must prevent cross-tenant data leakage [3]. Inadequate cryptographic key management creates unauthorized access opportunities.

Cloud service providers abstract storage locations from consumer visibility. This abstraction complicates data locality verification efforts. Trust relationships between consumers and providers become critical security considerations [3]. Organizations must evaluate provider security practices before entrusting sensitive data. The distributed architecture of cloud storage introduces data remnant risks. Information may persist on storage media following deletion requests. Verification of complete data removal becomes challenging across distributed systems.

3.2 Access Control Weaknesses

Cloud disaster recovery environments frequently operate with elevated privilege configurations. Rapid failover operations demand broad permissions across infrastructure components. Information security risk assessment identifies access control failures as significant vulnerability sources [4]. Threat actors exploit misconfigured identity policies to gain unauthorized system entry. Compromised credentials enable lateral movement across recovery infrastructure.

Risk assessment frameworks emphasize the identification of threats targeting authentication mechanisms [4]. Password-based authentication remains vulnerable to credential theft attacks. Multi-factor authentication requirements strengthen identity verification processes. However, recovery scenarios may bypass standard authentication workflows. Emergency access provisions create potential exploitation pathways.

The separation between production and recovery environments introduces governance challenges. Security controls applied to primary systems may not extend to recovery infrastructure [4]. Recovery environments remain dormant for extended periods between tests. Security configurations become stale without regular validation. Access control policies require synchronization across operational boundaries.

Vulnerability assessment processes must encompass disaster recovery infrastructure within scope [4]. Periodic security evaluations identify configuration drift and emerging weaknesses. Privileged access management solutions should monitor recovery system access patterns. The activation of dormant infrastructure during disasters may reveal unaddressed vulnerabilities. Organizations must maintain security parity between production and recovery environments. The neglect of access control issues can lead to the failure of the entire system of resilience, even if other protective measures are in place.

4. Privacy Implications and Data Residency Concerns

Cloud disaster recovery architecture involves the duplication of data across infrastructures that are geographically distributed. This distribution introduces significant privacy implications for organizations managing sensitive information. Regulatory compliance becomes complex when recovery data crosses jurisdictional boundaries.

4.1 Cross-Border Data Transfer Challenges

Personal information replicated to recovery sites in different jurisdictions faces varying legal requirements. Cloud computing arrangements often involve data transfers across national borders [5]. The physical location of data determines which privacy laws apply. Data protection regulations differ substantially between countries and regions. Organizations may face conflicting legal obligations regarding data handling and disclosure [5].

Government access provisions create additional compliance complexity. Law enforcement authorities possess varying powers to compel data disclosure. Cloud providers may receive governmental requests without consumer notification [5]. The jurisdictional location of recovery infrastructure determines applicable legal authority. Organizations must evaluate governmental access risks when selecting recovery site locations.

Breach notification requirements vary across regulatory frameworks. Security incidents affecting recovery environments trigger notification obligations. Different jurisdictions impose distinct timelines and reporting procedures [5]. Organizations operating across multiple regions face complex notification coordination requirements. Contractual agreements with cloud providers should address breach response responsibilities. Clear delineation of notification duties prevents compliance gaps during incident response.

4.2 Multi-Tenant Architecture Privacy Risks

Multi-tenant architecture characterizes most cloud platform deployments. Multiple organizations share underlying physical infrastructure resources. Cloud computing relies on virtualization to provide logical separation between tenants [6]. Virtual machines

from different organizations may execute on shared physical hosts. This resource sharing introduces potential privacy exposure pathways.

One of the biggest issues when talking about virtualization is security in the multi-tenant environment. The hypervisor layer is responsible for the isolation of virtual machines and for the distribution of resources. If there are any holes in the virtualization software, this can be exploited to break the tenant separation [6]. Virtual machine escape attacks are designed to get through the isolation boundaries. When they're successful, it opens up the door for hackers to access the tenant environment that they're in the same physical machine with. The cloud provider should always be on top of their game by making sure that the hypervisor is up to date and that their patching and configuration management are all taken care of. Side-channel attacks rely on components that are common to the target hardware in order to glean confidential information.

Side-channel attacks exploit shared hardware resources to infer sensitive information. Processor caches, memory controllers, and network interfaces serve multiple tenants simultaneously [6]. Attackers may analyze resource usage patterns to extract confidential data. Cache-based timing attacks represent a documented threat category. Cloud providers implement countermeasures, including resource isolation and noise injection.

Companies that deal with regulated data have no choice but to be on the lookout for potential dangers that come with the multi-tenant set-up. Medical records, financial data, and personally identifiable information are good examples of things that need to be guarded in an enhanced manner. Privacy impact assessments should evaluate cloud recovery architecture suitability [6]. The assessment process identifies exposure risks and control requirements. Regulatory compliance demands documentation of data protection mechanisms.

Data minimization principles should guide recovery replication strategies. Organizations should replicate only the information necessary for recovery objectives. Excessive replication expands privacy exposure without operational benefit. Retention policies must govern recovery data lifecycle management. Secure deletion procedures should remove expired data from recovery environments.

5. Security Frameworks and Protective Mechanisms

Effective cloud disaster recovery security requires layered defensive architectures. Multiple threat vectors demand corresponding protective controls. Comprehensive security frameworks integrate encryption, access management, and network isolation mechanisms.

5.1 Encryption and Cryptographic Controls

Encryption serves as the foundational protective mechanism for cloud disaster recovery. Data security represents a primary concern in cloud computing environments [7]. Transport Layer Security protects data during replication between production and recovery sites. Storage-level encryption safeguards persisted recovery images against unauthorized access.

Cryptographic controls must address data protection throughout the entire lifecycle. Cloud environments face unique challenges regarding data confidentiality and integrity [7]. Encryption mechanisms should protect data during transmission across network boundaries. Data at rest requires equivalent cryptographic protection in storage systems. Key management practices determine overall encryption effectiveness.

Recovery site infrastructure must have access to decryption capabilities during failover events. Key distribution methods that are central to the system need to be secured in such a way that they are safeguarded from being intercepted and exposed to unauthorized individuals. In order to provide a secure environment free from any meddling, hardware security modules come with the necessary features for storing keys. Key rotation policies reduce exposure windows following potential compromises. Separation of key management from encrypted data strengthens protection postures.

5.2 Identity and Access Management

Identity and access management frameworks provide critical controls for recovery environments. Cloud security frameworks emphasize authentication and authorization as fundamental requirements [8]. Role-based access policies restrict interactions to authorized personnel only. Access control mechanisms prevent unauthorized entry to the recovery infrastructure.

Multi-factor authentication strengthens identity verification processes significantly. Password-based authentication alone provides insufficient protection. Additional authentication factors include hardware tokens and mobile verification applications [8]. Recovery environment access should mandate multiple authentication factors. On the one hand, emergency escape routes have to maintain a certain level of security, while on the other hand, they should not impair regular

operations in any way. The utilization of privileged access management ensures that the administrative functionalities are limited to a certain extent, i.e., only those capabilities that are necessary are allowed. Administrative accounts possess elevated permissions enabling system modifications. Privilege escalation attacks target administrative credential acquisition [7]. Just-in-time access provisioning limits privilege duration to operational necessity. Session monitoring provides accountability for privileged activities.

5.3 Network Security and Monitoring

Network security measures serve to keep the recovery infrastructure safe from malicious or unauthorized intrusions by isolating it internally. Moreover, cloud security frameworks can handle network-level risks with the aid of several cooperating mechanisms [8]. For instance, virtual private cloud setups are used to create logical networks that have their own boundaries. Besides, security group policies are used as a traffic-filtering tool that performs its task based on pre-established rules. Micro-segmentation levels make a strong barrier against intruders who want to move laterally from one environment to another. Security information and event management platforms aggregate log data centrally. Intrusion detection systems identify malicious activity patterns [7]. Real-time alerting notifies security personnel of detected anomalies. Log analysis supports forensic investigation following security incidents.

Cloud security frameworks recommend defense-in-depth approaches combining multiple controls [8]. Beyond doubt, continuous monitoring is indispensable in order to enable and support timely threat detection that can occur anywhere throughout the recovery infrastructure.

6. Implementation Guidelines for Secure Recovery Architectures

Any organization that wants to implement a cloud-based disaster recovery plan has to put in place a thorough framework for the governance of security. Technical and operational measures on their own cannot guarantee security; hence, they need to be integrated systematically. Implementation success depends on structured approaches addressing security throughout the recovery lifecycle.

6.1 Security Governance and Assessment

Security governance frameworks establish accountability for recovery environment protection. Cloud computing introduces specific security considerations requiring organizational attention [9]. Governance structures should define roles and responsibilities for disaster recovery security. Clear delineation of security obligations between providers and consumers remains essential.

Security assessments evaluate recovery infrastructure configurations against established benchmarks. Cloud environments face threats, including unauthorized access and data breaches [9]. Vulnerability assessments identify weaknesses in recovery system deployments before exploitation occurs. Configuration audits are performed to check for any departure from security baselines, and these are followed up with actions that are corrective in nature. Continuous compliance monitoring is a practice that is aimed at ensuring that security requirements set forth are constantly adhered to. When it comes to cloud computing, security requirements refer to the three main goals of confidentiality, integrity, and availability [9]. It is also possible for assessment tools that operate automatically to recognize, without delay, that a change in the configuration of a system has occurred and that such a change is unauthorized. Regular assessment cycles identify emerging vulnerabilities requiring organizational attention. Documentation of assessment activities supports audit and regulatory compliance requirements.

6.2 Data Classification and Protection Alignment

Data classification protocols must extend to disaster recovery environments. Sensitive data in cloud computing requires appropriate protection mechanisms aligned with classification levels [10]. Information sensitivity determines encryption requirements and access restrictions. Classification schemes enable proportionate security investment across data categories.

Protection mechanisms must maintain consistency between production and recovery environments. Privacy-preserving techniques protect sensitive information during cloud storage and processing [10]. Security controls applied in production require equivalent implementation at recovery sites. Data handling procedures should specify recovery environment requirements explicitly. Automatically implemented policy measures can guarantee that the same level of security is maintained in all the situations, environments, or instances that are subject to the policy. There are a number of aspects that should be taken into account in the process of protecting sensitive information, one of which is the consideration of data lifecycle stages. Data confidentiality mechanisms must address storage, transmission, and processing phases [10]. Retention

and disposal requirements apply equally to recovery data stores. Classified information requires secure deletion upon retention period expiration. Verification procedures confirm complete removal following disposal requests.

6.3 Recovery Testing and Incident Response

Recovery testing procedures should incorporate security validation activities. Failover operations must maintain protective controls throughout the recovery process. Security testing during recovery exercises validates control persistence after activation. Authentication mechanisms require verification following infrastructure failover. Access control policies need confirmation after recovery completion.

Test scenarios should address security incident simulations affecting recovery infrastructure. Cloud security threats require proactive detection and response capabilities [9]. Tabletop exercises evaluate response procedures for recovery environment compromises. Technical testing validates detection and containment capabilities under realistic conditions.

Incident response planning must address recovery environment compromise scenarios. Security incident detection mechanisms should monitor recovery infrastructure continuously. Response procedures establish containment actions for identified threats [10]. Communication protocols define notification requirements during security incidents. Post-incident analysis identifies improvement opportunities for future response effectiveness. Recovery environment security requires equivalent attention to production system protection.

***Table 1**. Security Vulnerabilities in Cloud Disaster Recovery [3, 4]*

Vulnerability Category	Description
Data Exposure During Transmission	Data packets traverse multiple network segments during replication, facing interception risks without encryption protection
Storage-Level Vulnerabilities	Misconfigured access policies and inadequate key management create unauthorized access opportunities in cloud storage
Multi-Tenant Data Isolation	Logical separation mechanisms may fail to prevent cross-tenant data leakage in shared infrastructure
Access Control Misconfigurations	Elevated privilege configurations for failover operations create exploitation pathways for compromised credentials
Governance Gaps	Security controls applied to production systems may not extend to dormant recovery infrastructure
Configuration Drift	Recovery environments remaining inactive for extended periods develop stale security configurations

***Table 2.** Privacy Implications and Data Residency Challenges [5, 6]*

Privacy Concern	Impact on Disaster Recovery
Cross-Border Data Transfers	Personal information replicated across jurisdictions becomes subject to varying legal frameworks
Government Access Provisions	Law enforcement authorities in recovery site jurisdictions may compel data disclosure
Breach Notification Variations	Security incidents trigger different notification obligations across regulatory frameworks
Hypervisor Vulnerabilities	Virtualization software flaws could compromise tenant isolation boundaries
Side-Channel Attacks	Shared processor caches and memory resources enable inference of sensitive information
Data Remnant Risks	Information may persist on shared storage media following deletion requests

***Table 3.** Security Frameworks and Protective Mechanisms [7, 8].*

Security Control	Protective Function
Transport Layer Encryption	Protects data during replication between production and recovery environments
Storage-Level Encryption	Safeguards persisted in recovery images against unauthorized access
Role-Based Access Control	Restricts recovery environment interactions to authorized personnel
Multi-Factor Authentication	Strengthens identity verification beyond password-based mechanisms

Privileged Access Management	Constrains administrative capabilities to defined operational contexts
Network Micro-Segmentation	Restricts lateral movement within recovery environments
Security Information and Event Management	Aggregates log data and identifies suspicious activity patterns
Intrusion Detection Systems	Identifies malicious activity patterns in the recovery infrastructure

Table 4. *Implementation Guidelines for Secure Recovery Architectures [9, 10].*

Implementation Component	Security Objective
Security Governance Frameworks	Establish accountability and define roles for disaster recovery protection
Vulnerability Assessments	Identify weaknesses in recovery system deployments before exploitation
Continuous Compliance Monitoring	Ensure ongoing adherence to security requirements through automated tools
Data Classification Protocols	Align protection mechanisms with information sensitivity levels
Privacy-Preserving Techniques	Protect sensitive information during cloud storage and processing
Recovery Security Testing	Validate control persistence throughout failover operations
Incident Response Planning	Establish containment procedures for recovery environment compromises
Post-Incident Analysis	Identify improvement opportunities for future response effectiveness

7. Conclusions

Cloud-based disaster recovery solutions indeed open up a wide range of possibilities in terms of carrying out day-to-day operations for businesses that are willing to build up their resistance to service interruptions. For example, cloud infrastructures are designed to be elastic, which means that they allow resources to be provisioned as and when they are needed without the need for any upfront investments in dedicated hardware. Moreover, recovery efforts can be scaled up and down in a very flexible way depending on what is the real and not the estimated maximum demand at a given time. However, the architectural shift toward cloud recovery environments necessitates careful attention to security and privacy considerations. Data traversing network boundaries faces interception risks without adequate encryption protection. When it comes to the storage that is used in multi-tenant environments, the necessary isolation mechanisms should be very robust and powerful enough to keep cross-tenant data exposure at bay permanently. Attempts to access control configurations should be made with the aim of achieving operational flexibility on the one hand, and, on the other hand, following the least privilege principles. What is more, multi-factor authentication and privileged access management solutions should be used in order to provide privileged credentials with additional layers and thus protection. The requirement for data about the location of the jurisdiction makes the decision of where to place the recovery site that much harder. There are quite a few differences between one region and the other in terms of the regulatory frameworks that govern personal information. When positioning their recovery infrastructure, organizations need to assess not only what governments will do in terms of accessing their data but also what they will do regarding notifying them about security breaches. Security governance frameworks establish accountability structures and assessment protocols for recovery environment protection. Data classification schemes ensure protection mechanisms align with information sensitivity requirements. Recovery testing procedures should validate security control persistence throughout failover operations. Incident response capabilities must extend to recovery infrastructure compromise scenarios. Among the various endeavours of integrating security controls into disaster recovery operations, the most prominent one is perhaps managing to strike the right balance with recovery time objectives. Further enhancements in terms of protection capabilities may be achieved by the use of confidential computing and zero-trust architectures that are still in development. Enterprises should not stop performing a risk evaluation for new security tech and threat scenarios to be able to optimize the effectiveness and safety of their DR postures across cloud environments.

Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.

- **Conflict of interest:** The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper
- **Acknowledgement:** The authors declare that they have nobody or no-company to acknowledge.
- **Author contributions:** The authors declare that they have equal right on this paper.
- **Funding information:** The authors declare that there is no funding to be acknowledged.
- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.
- **Use of AI Tools:** The author(s) declare that no generative AI or AI-assisted technologies were used in the writing process of this manuscript.

References

[1] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," National Institute of Standards and Technology, Special Publication 800-145, Sep. 2011. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-145/final

[2] Elaine Hulitt and Rayford B. Vaughn, "Information System Security Compliance to FISMA Standard: A Quantitative Measure," Proceedings of the International Multiconference on Computer Science and Information Technology, 2008. [Online]. Available: https://annals-csis.org/proceedings/2008/pliks/99.pdf

[3] Debabrata Nayak, "Understanding the Security, Privacy and Trust Challenges of Cloud Computing," Journal of Cyber Security and Mobility, 2012. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=11059777

[4] Ievgeniia Kuzminykh et al., "Information Security Risk Assessment," MDPI, 2021. [Online]. Available: https://www.mdpi.com/2673-8392/1/3/50

[5] Lisa J. Sotto et al., "Privacy and Data Security Risks in Cloud Computing," Electronic Commerce & Law Report, 2010. [Online]. Available: https://www.hunton.com/media/publication/3733_Privacy-Data_Security_Risks_in_Cloud_Computing_2.10.pdf

[6] Keiko Hashizume et al., "An analysis of security issues for cloud computing," Journal of Internet Services and Applications, 2013. [Online]. Available: https://link.springer.com/content/pdf/10.1186/1869-0238-4-5.pdf

[7] Muhammad Faheem Mushtaq, "Cloud Computing Environment and Security Challenges: A Review," (IJACSA) International Journal of Advanced Computer Science and Applications, 2017. [Online]. Available: https://www.researchgate.net/profile/Muhammad-Mushtaq-20/publication/320802850

[8] Milan Chauhan and Stavros Shiaeles, "An Analysis of Cloud Security Frameworks, Problems and Proposed Solutions," MDPI, 2023. [Online]. Available: https://www.mdpi.com/2673-8732/3/3/18

[9] Fariba Ghaffari et al., "Security Considerations and Requirements for Cloud Computing," 8th International Symposium on Telecommunications, 2016. [Online]. Available: https://www.researchgate.net/profile/Fariba-Ghaffari/publication/315468942

[10] Ali Gholami and Erwin Laure, "SECURITY AND PRIVACY OF SENSITIVE DATA IN CLOUD COMPUTING: A SURVEY OF RECENT DEVELOPMENTS," arXiv, 2015. [Online]. Available: https://arxiv.org/pdf/1601.01498