Does the Cloud Computing Environment Provide Security Guarantees for Sensitive Data?

Thais Marciano
School of Engineering and Management
São Paulo, Brasil

Ana Carolina Russo
School of Engineering and Management
São Paulo, Brasil

ABSTRACT
The text discusses a thematic approach to ensuring security for sensitive data in the cloud computing environment. The research methodology involves a bibliographic review using qualitative sources like books, magazines, and articles to analyze security concerns in this context. The main goal is a comprehensive examination of sensitive data security in cloud computing, addressing challenges from its increased use. The article explores existing security mechanisms, strategies, and best practices for safeguarding data, identifying risks, proposing solutions, and suggesting future research directions. The analysis aims to enhance understanding of cloud computing security for businesses, IT professionals, and users to protect sensitive cloud-stored data. The research suggests further contextual studies and a future case study to supplement the findings.

Keywords
Cloud computing; Security; Cloud; Sensitive data.

1. INTRODUCTION
Cloud computing's rapid popularity raises concerns about securing sensitive data stored in it, despite its efficiency (SILVA NETO and BONACELLI, 2021). Data protection is vital due to potential threats like leaks and cyberattacks, and adherence to data laws is crucial (RODRIGUES, GALDINO, and NETO, 2019). Encryption, authentication, and access controls offer security, but users must adopt best practices and reliable providers (PEREIRA and SACILOTTI, 2019).

Cloud computing's benefits need data protection for user trust and compliance. Security measures mitigate risks, ensuring safe usage. The article analyzes sensitive data security in the cloud, exploring challenges, mechanisms, and best practices to ensure protection. It considers rising cloud adoption, addressing risks to data integrity and proposing solutions and future research. This aids users, professionals, and companies in securing cloud-stored sensitive data.

2. REFERENCE FRAMEWORK

2.1 Definition and characteristics of Cloud Computing
Cloud computing offers remote access to computational resources through the internet, eliminating local infrastructure needs. It provides on-demand services with scalability for adjusting resource capacity based on real-time needs, leading to cost savings and agility (PEREIRA and SACILOTTI, 2019). Virtualization creates efficient resource utilization through virtual machines (VMs) (SILVA NETO and BONACELLI, 2021). Service models include IaaS, PaaS, and SaaS, with shared security responsibility between providers and customers (SILVA NETO and BONACELLI, 2021).

Cloud's popularity is driven by flexibility, scalability, and cost-effectiveness, though sensitive data security remains a concern (PEREIRA and SACILOTTI, 2019). Understanding cloud components forms the basis for analyzing their impact on sensitive data security. The article explores security challenges, threats, and solutions in the cloud computing landscape (RODRIGUES, GALDINO, and NETO, 2019).

Please use a 9-point Times Roman font, or other Roman font with serifs, as close as possible in appearance to Times Roman in which these guidelines have been set. The goal is to have a 9-point text, as you see here. Please use sans-serif or non-proportional fonts only for special purposes, such as distinguishing source code text. If Times Roman is not available, try the font named Computer Modern Roman. On a Macintosh, use the font named Times. Right margins should be justified, not ragged.

2.2 Sensitive Data and security challenges
Sensitive data, including personally identifiable information, demands strict protection in cloud computing due to potential harm from unauthorized access. Unique challenges in securing sensitive data in the cloud must be addressed (CAMARA et al., 2021). Primary concern is confidentiality, given shared servers' risk. Robust encryption ensures data confidentiality during storage and transmission (NETO, SILVA, and NOGAROLI, 2020). Data integrity, preventing unauthorized alterations, requires integrity control mechanisms (DE FLÔRES and DA SILVA, 2020).

Data availability needs redundancy, backup, and disaster recovery (SARLET and RUARO, 2021). GDPR and LGPD compliance presents challenges (CAMARA et al., 2021). Complex cloud demands security controls at various layers (NETO, SILVA, and NOGAROLI, 2020). Cryptographic key management is vital, covering secure generation, storage, rotation, and access (DE FLÔRES and DA SILVA, 2020). Effective communication, training, and audits uphold security policies. Limited control over third-party cloud requires strong contracts (SARLET and RUARO, 2021).

Lack of cloud security awareness necessitates investment in training (DE FLÔRES and DA SILVA, 2020). Sector-specific regulations, like healthcare and finance, demand tailored security (NETO, SILVA, and NOGAROLI, 2020). Rapid tech evolution introduces security challenges, requiring continuous adaptation (CAMARA et al., 2021).Please use a 9-point Times Roman font, or other Roman font with serifs, as close as possible in appearance to Times Roman in which these guidelines have been set. The goal is to have a 9-point text, as you see here. Please use sans-serif or non-proportional fonts only for special purposes, such as distinguishing source code text. If Times Roman is not available, try the font named Computer Modern Roman. On a Macintosh, use the font named Times. Right margins should be justified, not ragged.

2.3 Risks and Threats to sensitive data security in the Cloud

Cloud computing introduces significant risks and threats to the security of sensitive data, necessitating awareness and appropriate countermeasures (ALVES et al., 2021). Unauthorized access poses a primary threat, achieved through breaches, authentication flaws, or compromised accounts, enabling data manipulation or extraction (DA SILVA, 2023).

Data leakage is a considerable risk due to configuration errors, improper sharing, or vulnerabilities, potentially harming reputation and trust (BÉRGAMO and DE OLIVEIRA, 2019). Distributed Denial of Service (DDoS) attacks disrupt services and data access (BÉRGAMO and DE OLIVEIRA, 2019). Malware, including phishing, exploits users to disclose sensitive information, while system vulnerabilities allow unauthorized data access (ALVES et al., 2021).

Inadequate disaster recovery planning may lead to data loss, especially during crises (DA SILVA, 2023). Lack of transparency and control over cloud infrastructure reduces confidence in data security (BÉRGAMO and DE OLIVEIRA, 2019). Non-compliance with regulations like GDPR has legal and privacy implications (ALVES et al., 2021). Organizations must comprehend these risks, implementing robust measures for safeguarding sensitive cloud data.

3. METHODOLOGY

This article employs a qualitative literature review methodology to comprehensively explore sensitive data security in the cloud computing environment. This approach involves collecting information from reputable sources like scientific studies, books, articles, and technical reports. Qualitative data collection is crucial for a contextualized understanding of the topic, incorporating diverse perspectives and trends.

To perform the literature review, databases like PubMed, IEEE Xplore, ACM Digital Library, and Google Scholar will be used. Relevant keywords will guide the search, with a focus on terms like "sensitive data security" and "encryption in cloud computing." Article selection will adhere to established criteria, considering content relevance, source credibility, and timeliness.

Qualitative analysis of collected data follows, categorizing studies based on themes, concepts, and conclusions. This analysis identifies trends and insights regarding sensitive data security in cloud computing. It's important to note that this approach doesn't involve primary data collection through experiments or interviews, but rather critically interprets existing studies to provide an informed view of the subject.

Subsequently, results are analyzed and interpreted, addressing research objectives and collected data. This step's subjectivity varies among studies based on data type. Lastly, an analytical reading is conducted to summarize researched information, ensuring alignment with research objectives and problem-solving..

4. RESULTS AND DISCUSSION

This article employs a qualitative literature review methodology to comprehensively explore sensitive data security in the cloud computing environment. This approach involves collecting information from reputable sources like scientific studies, books, articles, and technical reports. Qualitative data collection is crucial for a contextualized understanding of the topic, incorporating diverse perspectives and trends.

Cloud computing security is vital due to sensitive data stored and processed. Encryption converts data into unreadable format, applied during transmission and storage. Authentication verifies user/system identity via passwords, tokens, or multi-factor methods to prevent unauthorized access.

Network security is crucial, using firewalls, intrusion detection/prevention to thwart cyberattacks. Backups and disaster recovery policies maintain data availability/integrity during failures. Regular updates for systems/apps mitigate vulnerabilities, reducing exploitation risk.

Data encryption at rest/in transit safeguards data, while web app firewalls detect/block attacks. Penetration testing simulates attacks to find flaws. Intrusion detection systems monitor user activity, alerting to potential threats. Security governance policies ensure compliance and best practices.

User education and awareness on security best practices are vital. Compliance policies, security certifications (ISO 27001, PCI DSS, etc.) assure security measures. Security audits evaluate policies and recommend improvements.

Mitigating DDoS attacks is vital for service availability. Privacy policies, data protection compliance (LGPD), and sandboxing/virtualization enhance data security. Role-based access control (RBAC) manages access, while malware detection and antivirus systems block threats.

Security Information and Event Management (SIEM) systems monitor cloud security events. Regular cyber hygiene practices like updates and patches are crucial. Encrypted backups add security. Data retention policies reduce unnecessary exposure and maintain privacy.

5. CLOSING REMARKS

In summary, this literature review delves into the critical issue of securing sensitive data in cloud computing. The article covers various facets, from defining cloud computing to strategies for safeguarding sensitive information within this framework. Cloud computing provides advantages like scalability and cost savings, but it also poses security challenges. Risks range from unauthorized access to data leaks, malware, and system vulnerabilities. Mitigating these risks demands a comprehensive security approach, involving provider assessment, encryption, authentication, monitoring, backup, education, and testing.

Cloud security is a continuous effort, requiring adherence to evolving best practices and collaboration among providers, users, and regulators. While cloud computing offers great benefits, ensuring sensitive data security necessitates.

6. REFERENCES

[1] ALVES, Andrio de Andrade et al. Cloud computing risks: a study from the perspective of managers of federal public agencies in Brazil. Navus: Journal of Management and Technology, n. 11, p. 1-18, 2021.

[2] BÉRGAMO, Luciano; DE OLIVEIRA, Vitor Coimbra. BIG DATA IN CLOUD. SITEFA-Sertãozinho Fatec Technology Symposium, v. 2, n. 1, p. 404-411, 2019.

[3] CAMARA, Maria Amália Arruda et al. Internet of Things and blockchain in the Unified Health System: protection of sensitive data under the General Data Protection Law. Cadernos Ibero-Americanos de Direito Sanitário, v. 10, n. 1, p. 93-112, 2021.

[4] DA SILVA, Anildo Joaquim. Information security in the cloud computing environment. Primeira Evolução Journal, v. 1, n. 38, p. 13-25, 2023.

[5] DE FLÔRES, Mariana Rocha; DA SILVA, Rosane Leal. Challenges and perspectives of sensitive personal data protection in the public administration: between the public duty to inform and the citizen's right to be protected. Law Journal, v. 12, n. 2, p. 1-34, 2020.

[6] NETO, Miguel Kfouri; SILVA, RODRIGO DA GUIA; NOGAROLI, RAFAELLA. Artificial Intelligence and Big Data in the Diagnosis and Treatment of COVID-19 in Latin America: New Challenges to Personal Data Protection. Brazilian Journal of Fundamental Rights & Justice, v. 14, n. 1, p. 149-178, 2020.

[7] PEREIRA, Thiago Martins; SACILOTTI, Adani Cusin; JÚNIOR, José Roberto Madureira. Cloud computing: platform as a service. In MARTINS, Ernane Rosa. Fundamentals of Computer Science, v. 2, p. 116-125, 2019.

[8] RODRIGUES, Grazieli Cristina; GALDINO, Lilian Rosa; NETO, Joaquim Maria Ferreira Antunes. Application of cloud computing in small and medium-sized enterprises: systematic review. Prospectus (ISSN: 2674-8576), v. 1, n. 1, 2019.

[9] SARLET, Gabrielle Bezerra Sales; RUARO, Regina Linden. Protection of sensitive data in the Brazilian normative system under the General Data Protection Law (LGPD)–L. 13.709/2018. Fundamental Rights & Democracy Journal, v. 26, n. 2, p. 81-106, 2021.

[10] SILVA NETO, Victo José da; BONACELLI, Maria Beatriz Machado; PACHECO, Carlos Américo. The digital technological system: artificial intelligence, cloud computing, and Big Data. Brazilian Innovation Journal, v. 19, 2021.