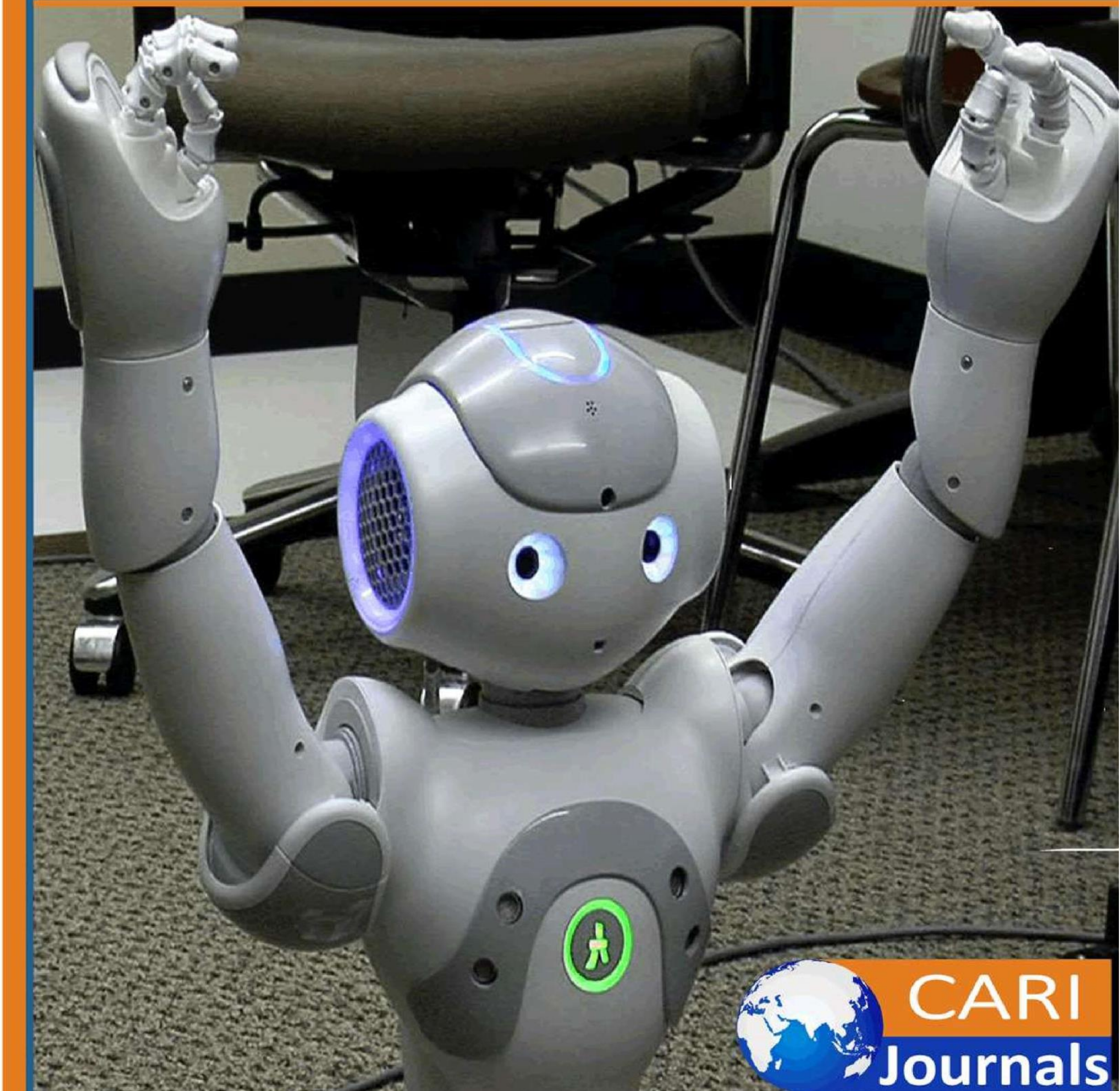
International Journal of
Computing and Engineering
(IJCE)

Enhancing Big Data Security through Comprehensive Data Protection Measures: A Focus on Securing Data at Rest and In-Transit.



CARI Journals

Enhancing Big Data Security through Comprehensive Data Protection Measures: A Focus on Securing Data at Rest and In-Transit

Preyaa Atri

Accepted: 24th Mar, 2024 Received in Revised Form: 24th Apr, 2024 Published: 24th May, 2024

Abstract

Purpose: This research paper aims to enhance Big Data security by implementing comprehensive data protection measures, focusing on securing data at rest and in transit. In the era of Big Data, organizations handle vast quantities of data characterized by high velocity, volume, and variety, which complicates management and increases security risks.

Methodology: The study examines various data protection strategies, including encryption, access control, data masking, immutable storage, tokenization, and physical security for data at rest. For data in transit, it explores encryption protocols, secure transfer methods like SSH and TLS, VPNs, Zero Trust architecture, and secure APIs. These methods are crucial for safeguarding sensitive information and preventing unauthorized access.

Findings: The findings highlight common security challenges in Big Data, such as data breaches, unauthorized access, and integrity issues. The study emphasizes the need for robust protection measures and offers a comprehensive view of the data security landscape. Implementing these strategies helps organizations safeguard sensitive information and ensure compliance with international data protection regulations, enhancing their overall security posture.

Unique contribution to theory policy and practice: This paper contributes to theory, policy, and practice by advocating comprehensive data protection strategies. It stresses the importance of continuous monitoring and regulatory compliance, providing practical insights into best practices and technologies that protect Big Data. The research supports developing robust data protection policies and practices, advancing knowledge in Big Data security.

Keywords: *Big Data Security, Data Protection, Secure Data Transfer, Data at Rest, Data in Tra nsit*

Introduction

In the era of Big Data, where vast amounts of information are generated and processed at an unprecedented rate, the security of this data has become a paramount concern for organizations across various industries [32] [33]. As the title suggests, this research paper focuses on enhancing Big Data security through comprehensive data protection measures, with a specific emphasis on securing data at rest and in transit. To begin, a thorough understanding of Big Data and its security challenges is essential. Big Data, characterized by the volume, velocity, and variety of data, poses unique security risks due to its sheer size and complexity [34]. Common security challenges in Big Data include data breaches, unauthorized access, and data integrity issues [35]. Addressing these challenges requires effective strategies for securing data at rest, which involves safeguarding data stored in databases, servers, and other repositories. Encryption techniques and access control measures play crucial roles in enhancing the security of data at rest by protecting it from unauthorized access and tampering [36]. Similarly, securing data in transit, as it travels across networks and communication channels, is vital to prevent interception and manipulation by malicious actors [37]. Encryption and network security practices are key components in ensuring the confidentiality and integrity of data during transit [38]. By implementing comprehensive data protection measures, organizations can develop holistic strategies that encompass encryption, access controls, network security, and continuous monitoring to safeguard their Big Data assets effectively. This paper aims to explore the best practices for implementing data security policies and highlight the importance of continuous monitoring in improving Big Data security posture.

Understanding Big Data and Its Security Challenges

What is Big Data?

Big data, by its very nature, encompasses vast and intricate datasets that are continuously generated from a multitude of sources such as social media platforms, Internet of Things (IoT) devices, and various digital transactions [1]. This complexity and the rapid speed at which this data is produced pose unique challenges, particularly in terms of storage, analysis, and security. Traditional data processing tools are often found wanting in their capacity to manage this deluge effectively, leading to the recognition that big data is fundamentally unmanageable by conventional means [1]. Consequently, this has necessitated the development and adoption of innovative big data technologies and analytics tools. These tools are not just pivotal in harnessing the power of big data for strategic business insights, market predictions, and operational improvements, but they also play a critical role in ensuring that the data is processed and stored securely [2][1]. The importance of these technologies cannot be overstated, especially when considering the diverse nature and the significant volume of data involved.

Why is Big Data security critical?

Given the inherent vulnerabilities in big data architecture as highlighted by the increased use of big data analytics tools, the criticality of big data security cannot be overstated. As the volume, complexity, and speed of data generation continue to soar, so does the attractiveness of this data to malicious actors, underscoring the urgent need for robust protection measures [3]. This urgency is further magnified by the realization that the integrity and accuracy of data are paramount; any compromise due to unauthorized access could lead to significant issues in decision-making and analysis, thereby emphasizing the critical nature of security measures [4]. Moreover, the growing integration of artificial intelligence (AI) into big data analytics amplifies these security concerns. AI's ability to process and analyze big data at unprecedented speeds means that any security lapse can have far-reaching consequences, making the safeguarding of these data sets not just a matter of protecting information, but also of ensuring the reliability of AI-driven decisions [3]. Thus, the interplay between the volumes of data generated, its attractiveness to attackers, and the integration of AI technologies elevates the importance of big data security to an essential component of modern data management and analytics strategies.

Problem Statement

The era of big data brings forth a multitude of challenges related to data security. Organizations grapple with securing vast datasets that encompass diverse formats and reside in complex, distributed environments. Sensitive information, such as personally identifiable information (PII), financial records, and intellectual property, becomes vulnerable to unauthorized access, data breaches, and malicious attacks. The consequences of such security incidents can be severe, leading to reputational damage, financial losses, and legal repercussions.

Common security challenges in Big Data?

Given the complexity inherent in big data frameworks and the critical nature of ensuring data privacy, integrity, and compliance, understanding the common security challenges becomes paramount. Among these challenges, data protection, access control, monitoring and detection, compliance, and governance stand out as core areas of concern [5]. These challenges are exacerbated by the continuously evolving landscape of practices and tools designed to safeguard big data, which necessitates an ongoing commitment to adapt and refine security measures [5]. Furthermore, the shared responsibility model underscores the complexity of big data security, requiring a collaborative effort among tech security professionals, database administrators, programmers, quality testers, InfoSec and compliance officers, business units, and end-users [5]. This model highlights the multifaceted approach needed to address big data security challenges effectively, ensuring that every stakeholder plays a role in safeguarding the data ecosystem.

Solution

There are various strategies and technologies to securing data at rest and in-transit. This research paper provides a comprehensive framework describing various such strategies, including the best practices that companies can use to build their future data policies.

Securing Data at Rest: Approaches and Solutions

A. Key vulnerabilities of data at rest and solutions to ensure its security

One of the most pressing concerns for modern enterprises is the security of data at rest, which encompasses all data in digital storage not actively moving from device to device or across networks. The inherent vulnerabilities of data at rest stem from various factors, including its stationary nature and the valuable information it often contains. Data at rest is at a heightened risk of loss, leakage, or theft, primarily because it can become invisible or improperly managed within an organization [6]. This invisibility makes it an attractive target for insider attacks, where unauthorized employees might store or access sensitive data without proper clearance [6]. Moreover, sensitive information stored on devices or backup mediums is easily susceptible to attacks, further amplified by the fact that unprotected data leaves enterprises exceedingly vulnerable to both insider and outsider threats [6][7]. The reality that data at rest can be considered more enticing to malicious hackers due to its perceived sensitivity and the volume of information that could potentially be stolen underscores the critical need for robust protection measures [8][6]. Thus, it is imperative for organizations to adopt effective security strategies to safeguard this valuable asset from the myriad of threats it faces.

Some of the major data security strategies for securing data at rest are:

1**. Data Encryption:** This cornerstone technique transforms data into an unreadable format using algorithms and encryption keys. AES (Advanced Encryption Standard) and RSA (Rivest-Shamir-Adleman) are popular choices, with AES suitable for bulk data encryption and RSA for secure key exchange [22]. This method of encryption not only complies with various industry and governmental regulations—such as GDPR, HIPAA, and PCI DSS—but also becomes a mandatory component of an organization's data security protocols [6]. Furthermore, major cloud service providers, recognizing the importance of securing data at rest, now offer automated encryption solutions. This advancement simplifies the encryption process for organizations of all sizes, ensuring that data, regardless of its volume or the speed of its generation, remains secure and inaccessible to unauthorized parties [8].

2. **Access Controls:** Implementing stringent access control mechanisms like Role-Based Access Control (RBAC) limits data access to authorized personnel based on their roles and responsibilities within the organization. This prevents unauthorized users from accessing sensitive information [23]. This holistic approach to data security not only addresses the immediate challenges of securing sensitive information but also aligns with the broader goal of maintaining data privacy and integrity within big data frameworks.

3. **Data Masking:** By obscuring sensitive data elements with modified content (e.g., replacing credit card numbers with asterisks), data masking ensures privacy while maintaining data usability for testing and development purposes [24].

4. **Immutable Storage:** This technique utilizes storage solutions where data, once written, cannot be modified or deleted. Immutable storage ensures data integrity and protects against ransomware attacks or accidental deletions [25].

5. **Tokenization:** Sensitive data is replaced with non-sensitive placeholders (tokens) while the original data is securely stored elsewhere. Tokenization reduces the risk of exposure and facilitates secure data processing [26].

6**. Physical Security:** Protecting physical storage devices and infrastructure from unauthorized access through measures like surveillance systems, access controls, and environmental safeguards adds an essential layer of defense against data breaches [27].

Securing Data In-Transit: Approaches and Solutions

B. Key vulnerabilities of data in-transit and solutions to ensure its security

The inherent vulnerabilities of data in transit significantly heighten its susceptibility to security threats, primarily because it traverses various networks outside the protective confines of an organization's immediate control. This movement beyond traditional security guardrails exposes data to a range of potential threats and weaknesses, notably when it is transmitted outside the company's network perimeter, thereby placing it directly in the path of opportunistic attackers, [9]. The exposure is aggravated by the fact that attackers continuously seek innovative methods to exploit these vulnerabilities, aiming to gain unauthorized access to valuable data regardless of its state [7], [10], [7]. Consequently, the vulnerability of data in transit not only underscores the necessity for robust security measures to safeguard sensitive information but also emphasizes the critical role of the various measures mentioned below that ensures the confidentiality, integrity, and authenticity of data as it moves across networks, thereby mitigating the risks associated with its exposure during transit,[10], [7].

Some of the strategies for securing data in transit include:

1. Encryption: Similar to data at rest encryption, this technique safeguards data during transmissi on. However, it often utilizes protocols like TLS (Transport Layer Security) and SSL (Secure Soc kets Layer) to secure communication channels and ensure data confidentiality and integrity [28]. These protocols leverage asymmetric or public key encryption, wherein a public key is used for encryption and a private key for decryption, ensuring that data remains secure during its transfer [10], This method addresses the issue of secure key storage, often cited as a challenge with private key encryption, by facilitating a system where the decryption key remains private, thereby enhancing the security of the data in transit [9].

2. Secure Transfer Protocols: SSH (Secure Shell) enables secure remote access and file transfer , while TLS/SSL protocols establish encrypted connections for web browsing, email, and other ap plications, protecting data from man-in-the-middle attacks [29].

3. VPN (Virtual Private Network): By creating an encrypted tunnel over public networks, VPN s ensure secure communication between devices and networks, shielding data from prying eyes a nd unauthorized access [30].

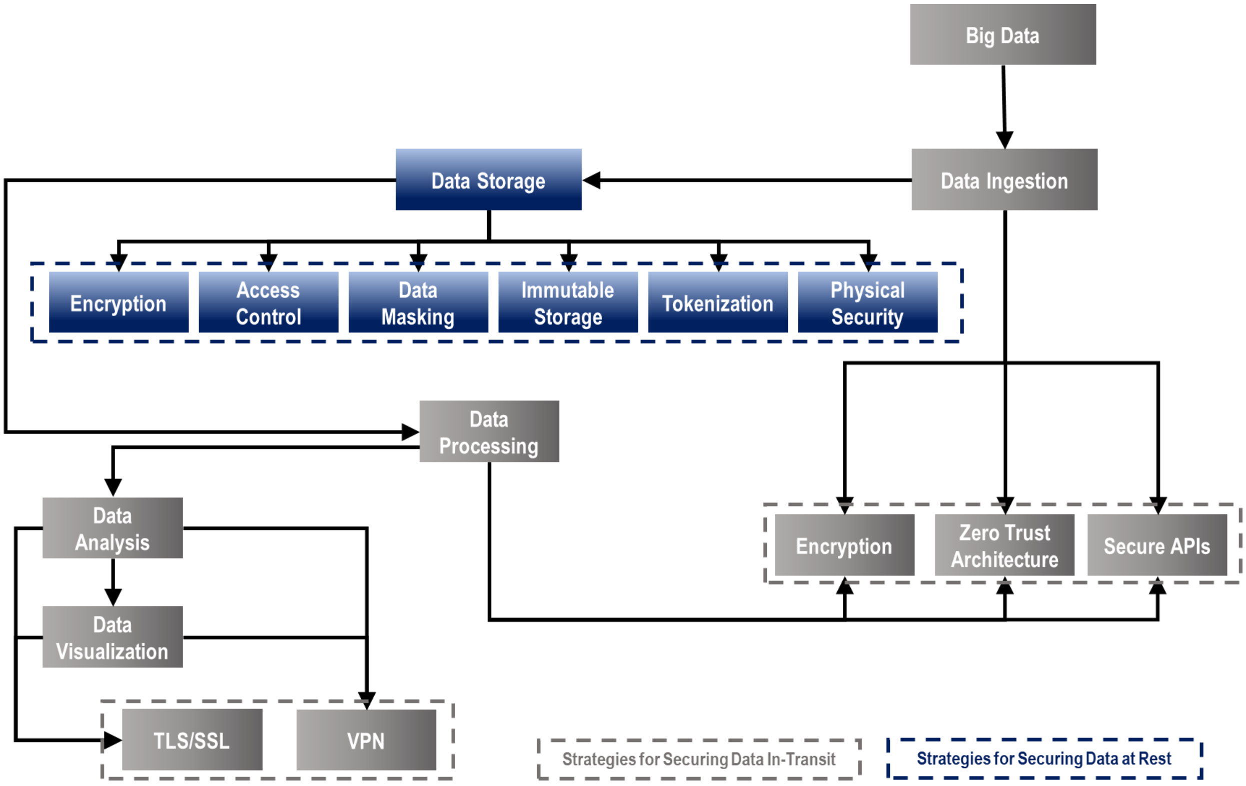
4. Zero Trust Architecture: This security model operates on the principle of "never trust, alway s verify," continuously authenticating and authorizing users and devices before granting access to data, thereby minimizing the attack surface [31].

5. Secure APIs (Application Programming Interfaces): Implementing security measures like a uthentication, authorization, and encryption within APIs safeguards data exchanged between appl ications and services, preventing unauthorized access and data leakage.

Network security practices for protecting data in-transit?

In the realm of Big Data, where security is paramount, the protection of data in-transit represents a critical challenge that demands rigorous and effective network security practices. Among these practices, Network Data Loss Prevention (DLP) emerges as a highly effective strategy, focusing on the safeguarding of sensitive information such as personally identifiable information, intellectual property, and proprietary data [9]. The essence of Network DLP lies in its ability to disrupt and prevent the unauthorized exfiltration of sensitive data, thereby ensuring that information remains secure as it moves across networks [9]. Moreover, the implementation of secure tunneling technologies further fortifies the security of data in transit, providing an additional layer of protection against potential breaches [10]. This approach is complemented by the adherence to stringent regulatory requirements, including HIPAA, PIPEDA, GDPR, and PCI DSS, which set the standard for data protection and underscore the importance of compliance in network security practices [10]. Together, these measures form a comprehensive defense mechanism against the vulnerabilities associated with data in transit, reflecting a proactive stance towards safeguarding data integrity and privacy in the dynamic landscape of Big Data.

Exhibit 1: Comprehensive Overview of Data Protection Solutions for Securing Data at Rest and In-Transit



Recommendations

How can organizations develop a holistic data protection strategy?

Developing a holistic data protection strategy requires a multi-faceted approach that encompasses not only the implementation of stringent policies but also the integration of robust technical measures to safeguard personal data across all fronts. At the core of this approach is the establishment of comprehensive data protection policies that explicitly outline the security measures to be employed for the defense of personal data, ensuring its confidentiality, integrity, and availability [11]. These policies must be detailed and encompassing, guiding the organization in deploying comprehensive security protocols and maintaining stringent information security policies, which are crucial for the protection of digital assets. Moreover, to address the evolving threats and vulnerabilities in the digital landscape, organizations must ensure that these policies cover the entire data lifecycle, from creation and storage to transmission and disposal [13]. This comprehensive coverage is essential not just for safeguarding against potential breaches but also for ensuring the organization's compliance with legal standards such as the General Data Protection Regulation (GDPR), thereby reinforcing its commitment to data privacy and protection.

Comprehensive Data Protection Framework

To effectively safeguard their data, organizations should adopt a comprehensive data protection framework that includes the following elements:

First, data classification is essential. This involves categorizing data based on its sensitivity and value to determine the appropriate levels of protection needed. Next, conducting a thorough risk assessment helps identify potential threats and vulnerabilities to data security, allowing organizations to prioritize their mitigation efforts.

Clear policies and procedures are crucial for data access, handling, and protection. Establishing these guidelines ensures that everyone in the organization understands the rules and practices for maintaining data security. Alongside this, security awareness training is vital. Educating employees on data security best practices and their role in protecting sensitive information helps create a culture of security within the organization.

Continuous monitoring and auditing of systems and networks are necessary to detect suspicious activities. Regular audits ensure compliance with security policies and help identify areas for improvement. In the event of a data breach or security incident, having a well-developed incident response plan is critical. This plan outlines the steps to respond effectively and minimize the impact of such incidents.

Implementing the right technologies and tools based on the risk assessment and data classification is also important. These technologies provide the necessary defenses to protect against identified threats. Finally, regular review and updates of the framework are essential. As new threats emerge and security requirements evolve, the framework must be continuously evaluated and improved to remain effective.

By implementing this comprehensive framework, organizations can establish a robust defense against data breaches, ensuring the confidentiality, integrity, and availability of their valuable information assets.

What are the best practices for implementing data security policies?

Given the vulnerabilities inherent in big data architectures, as highlighted by the increasing reliance on big data analytics tools, the implementation of robust data security policies becomes paramount. To mitigate these vulnerabilities, regular reviews and updates of existing policies are crucial [14]. This is because as technology evolves, so too do the tactics employed by cybercriminals, making it imperative that policies keep pace with the rapid development of both data analytics tools and potential threats. Furthermore, the adoption of best practices for data security, such as the implementation of comprehensive encryption standards, cannot be overstated [14]. Encryption acts as a critical barrier, safeguarding data even in the event of unauthorized access, thereby maintaining the integrity and confidentiality of sensitive information. This approach not only addresses the vulnerabilities associated with the complexity and volume of big data but also aligns with the proactive steps recommended for safeguarding digital assets against cyber threats [15]. Hence, in the context of big data, where the stakes are significantly raised due to the volume and sensitivity of the data involved, the implementation of rigorous, up-to-date data security policies is not just beneficial but essential for maintaining data integrity and protecting against cyberattacks. Below we list some of the best policies for safeguarding data both at rest and in transit.

Best Practices for Securing Data at Rest and In-Transit

In the realm of data security, securing data at rest and in transit is of paramount importance. For data at rest, Format-Preserving Encryption (FPE) emerges as a powerful tool, enabling encryption without altering the data's format, thus facilitating seamless cloud migration and legacy application development. FPE's versatility in supporting the encryption of numeric, string, and combined data types makes it a robust solution for safeguarding data in cloud environments [16]. Additionally, a defense-in-depth approach that combines RSA for confidentiality, ECC for key exchange, and hashing for data integrity, along with digital certificates for non-repudiation, is crucial for protecting data across diverse IT environments [17].

When it comes to securing data in transit, a formal data security policy that outlines expectations for data confidentiality, integrity, and availability is fundamental. This policy should be reinforced by standards, guidelines, and procedures for implementation, ensuring consistent security processes and compliance across the organization [18]. Adopting best practices is a practical way to adhere to data security and privacy standards, especially in the context of international data flows and outsourcing, with industry associations playing a key role in promoting and enforcing these standards [19].

For Service-Oriented Architectures (SOAs), a layered security approach incorporating integrated key management, identity management, and policy-based enforcement is essential to protect data at rest and in transit across enterprise systems [20]. Moreover, innovative architectures like DiTD, designed to protect data in transit, offer high-performance cloud computing-based security frameworks that leverage both symmetric and public-key cryptography for efficient key strength and exchange, thereby enhancing cloud communication security [21].

These best practices encompass a range of strategies, from employing advanced encryption methods and developing comprehensive security policies to leveraging cloud-specific architectures for protecting data in transit. By implementing these practices, organizations can significantly enhance the security of their data throughout its lifecycle.

Continuous monitoring to improve big data security?

Building on the foundation that big data security is of paramount importance, continuous monitoring emerges as a key strategy to enhance the security posture of these complex data frameworks. By implementing continuous monitoring, organizations can adopt a proactive approach to data security management, which is crucial for identifying and responding to potential security breaches as they occur [14]. This approach includes the deployment of machine learning (ML) algorithms that scrutinize network traffic, system logs, and user behavior in real-time, providing an advanced method for detecting unusual patterns or behaviors that could signify a security breach [14]. Furthermore, continuous monitoring facilitates the immediate response to suspicious activities, significantly reducing the time between the detection of a potential security threat and the response to it [14]. This capability is essential for maintaining the integrity, privacy, and compliance of big data, ensuring that organizations can protect themselves against both internal and external security risks. By integrating continuous monitoring into their data security strategies, organizations can create a more resilient and responsive defense mechanism against the evolving threats that target big data systems.

Conclusion

In this research paper, the focus on enhancing big data security through comprehensive data protection measures, specifically securing data at rest and in-transit, sheds light on the critical importance of safeguarding the vast and intricate datasets characteristic of big data frameworks. The complexities of managing and securing such massive volumes of data, sourced from various sources like social media platforms and IoT devices, underscore the necessity for innovative technologies and analytics tools to mitigate inherent vulnerabilities. The integration of continuous monitoring as a proactive strategy for identifying and responding to security breaches in real-time is highlighted as a key component in fortifying data security postures. Moreover, the growing integration of AI technologies into big data analytics amplifies security concerns, emphasizing the need for robust protection measures against both internal and external threats. Encryption techniques, such as asymmetric key encryption and SSL/TLS protocols, play a crucial role in securing data at rest and in-transit, bolstering data privacy, integrity, and compliance. Access control measures, advanced encryption protocols, and secure data analytics platforms collectively form a comprehensive strategy for organizations to safeguard sensitive information and maintain a resilient defense against evolving security threats. The discussion underscores the urgent need for organizations to adapt and refine security measures continuously in response to the evolving landscape of practices and tools designed to protect big data. By acknowledging the critical role of data security in modern data management and analytics strategies, this research paper contributes to the ongoing advancement of knowledge in the field of big data security and underscores the imperative of upholding data integrity and privacy in an era of escalating cyber threats.

References

[1] Intetics, "Big Data: Security Issues and Challenges," Intetics Blog, Apr. 2023. [Online]. Available: https://intetics.com/blog/big-data-security-issues-and-challenges/

[2] Cprime, "Big Data Security: Biggest Challenges and Best Practices," Cprime. [Online]. Available: https://www.cprime.com/

[3] Sertainty, "Understanding the Challenges and Solutions of Big Data Security," Sertainty. [Online]. Available: https://www.sertainty.com/

[4] New Softwares, "Big Data Explained: Security Challenges and Solutions in Presentations," New Softwares. [Online]. Available: https://www.newsoftwares.net/

[5] M. Devs, "Big Data Security: Best Practices," Mad Devs Blog, Sep. 2023. [Online]. Available: https://maddevs.io/blog/big-data-security-best-practices/

[6] A. Coos, "How to Protect Your Data at Rest," Endpoint Protector, June 2021. [Online]. Available: https://www.endpointprotector.com/

[7] N. Lord, "Data Protection: Data In Transit vs. Data At Rest," Digital Guardian Blog, May 2023. [Online]. Available: https://www.digitalguardian.com/blog/data-protection-data-in-transit-vs-data-at-rest/

[8] Teradata, "Data Security: Data At Rest," Teradata Insights. [Online]. Available: https://www.teradata.com/insights/data-security/data-at-rest

[9] C. Brook, "Data In Transit & How to Protect It," Digital Guardian, July 2023. [Online]. Available: https://www.digitalguardian.com/blog/data-in-transit-and-how-to-protect-it

[10] TitanFile, "Securing Data in Transit With Encryption: The Ultimate Guide," TitanFile Blog. [Online]. Available: https://www.titanfile.com/blog/data-in-transit-encryption/

[11] Cloudian, "Data Protection Policy: Key Elements to Include and 3 Best Practices," Cloudian. [Online]. Available: https://cloudian.com/

[12] Perisai Cybersecurity, "Essential Data Protection Measures for Security," LinkedIn, [Online]. Available: https://www.linkedin.com/pulse/essential-data-protection-measures-security-perisai-cybersecurity-ua7qc/

[13] S. Nayak and B. Lal, "Implementing a comprehensive information protection strategy," Tata Consultancy Services. [Online]. Available: https://www.tcs.com/

[14] SurveyCTO, "A Comprehensive Approach to Data Security Management," SurveyCTO. [Online]. Available: https://www.surveycto.com/resources/guides/data-security-guide/

[15] Flexential, "How to Build & Maintain Data Security Strategy," Flexential. [Online]. Available: https://www.flexential.com/

[16] N. Chaudhari, "A Cloud Security Approach for Data at Rest Using FPE," IJCCSA, vol. 5, pp. 11-16, 2015.

[17] S. Chaudhari, A. Thakur, and A. Rajan, "Securing Digital Information Using Cryptography Techniques to Enhance IT Security," Research Reports on Computer Science, 2023.

[18] Photopoulos, "Data Security Policy," 2008.

[19] K. Bajaj, "Promoting Data Protection Standards through Contracts: The Case of the Data Security Council of India," Review of Policy Research, vol. 29, pp. 131-139, 2012.

[20] U. T. Mattsson, "Securing Data Beyond PCI in a SOA Environment: Best Practices for Advanced Data Protection," 2008.

[21] K. Nandakumar et al., "Securing data in transit using data-in-transit defender architecture for cloud communication," Soft Computing, vol. 25, pp. 12343-12356, 2021.

[22] W. Stallings, Cryptography and Network Security: Principles and Practice, 7th ed. Pearson Education, 2017.

[23] F. Ferraiolo, R. Sandhu, S. Gavrila, D. R. Kuhn, and R. Chandramouli, "Proposed NIST standard for role-based access control," ACM Transactions on Information and System Security (TISSEC), vol. 4, no. 3, pp. 224-274, 2001.

[24] C. Clifton and T. Tassa, "Dynamic data masking: Maintaining the utility of data while ensuring privacy," Proceedings of the 2008 ACM SIGMOD International Conference on Management of Data, pp. 837-848, 2008.

[25] A. Haq, "Immutable storage: Ensuring data integrity in the cloud," IEEE Cloud Computing, vol. 5, no. 2, pp. 76-80, 2018.

[26] J. Zhou, D. P. Pezaros, and M. M. Theoharidou, "Tokenization as a service: A case study of PCI DSS compliance," Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, pp. 1217-1228, 2014.

[27] National Institute of Standards and Technology (NIST), "Security and Privacy Controls for Information Systems and Organizations," NIST Special Publication 800-53 Rev. 5, Apr. 2020.

[28] E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.3," RFC 8446, Aug. 2018.

[29] T. Ylonen and C. Lonvick, "The Secure Shell (SSH) Transport Layer Protocol," RFC 4253, Jan. 2006.

[30] S. Kent and R. Atkinson, "Security architecture for the internet protocol," RFC 2401, Nov. 1998.

[31] J. Kindervag, Zero Trust Networks: Building Secure Systems in Untrusted Networks, O'Reilly Media, 2019.

[32] P. C. Zikopoulos and C. Eaton, *Understanding Big Data: Analytics for Enterprise Class Hadoop and Streaming Data*. McGraw-Hill Osborne Media, 2011.

[33] B. Marr, *Big Data: Using SMART Big Data, Analytics and Metrics to Make Better Decisions and Improve Performance*. Wiley, 2015.

[34] M. Chen, S. Mao, and Y. Liu, "Big Data: A Survey," *Mobile Networks and Applications*, vol. 19, no. 2, pp. 171-209, 2014.

[35] A. Katal, M. Wazid, and R. H. Goudar, "Big Data: Issues, Challenges, Tools and Good Practices," in *2013 Sixth International Conference on Contemporary Computing (IC3)*, 2013, pp. 404-409.

[36] B. Grobauer, T. Walloschek, and E. Stocker, "Understanding Cloud Computing Vulnerabilities," *IEEE Security & Privacy*, vol. 9, no. 2, pp. 50-57, 2011.

[37] K. Sood, S. E. Sarma, and T. Karygiannis, "Intrusion Detection Framework for Smart Grid," *IEEE Communications Magazine*, vol. 50, no. 5, pp. 102-108, 2012.

[38] S. A. Ahson and M. Ilyas, *Cloud Computing and Software Services: Theory and Techniques*. CRC Press, 2012.