iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** XI **Month of publication:** November 2024

DOI: https://doi.org/10.22214/ijraset.2024.65610

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue XI Nov 2024- Available at www.ijraset.com

A Review on Data Security in Information Management Using Digitized Technology

S. Saira Banu[1], S. M. Sasi Rekha[2]
[1]*Assistant Professor, EASA College of Engineering and Technology, Coimbatore*
[2]*Assistant Professor & Head,, EASA College of Engineering and Technology, Coimbatore*

Abstract: ***This Paper provides a review on Data Security in information management. In information management systems, ensuring data integrity, confidentiality, and availability is crucial. Data security involves safeguarding information against unauthorized access, loss, confidentiality and availability throughout the cycle. This paper also focuses on the impact of latest technologies such as Cloud Computing, Big data and IoT that are reshaping the landscape of data integrity. The integration of digitized technology in information management offers transformative benefits but necessitates robust data security mechanism. As threats evolve, a proactive approach combining technology, policy, and user education is critical for safeguarding digital assets.***

Keywords: Data Security, Data Integrity, Security Threats, Security Goals, Encryption, Digitized Technology

I. INTRODUCTION

In today's digital era, databases play a crucial role in numerous sectors, including finance, healthcare, government, and e-commerce, acting as repositories for valuable data such as personal information, financial records, intellectual property, and confidential business data. The importance of database security stems from the potential ramifications of security breaches. Unauthorized access, data breaches, or malicious activities targeting databases can result in severe consequences such as identity theft, financial loss, privacy breaches, damage to reputation, and legal consequences. Additionally, the evolving nature of cyber threats and the continually changing regulatory landscape necessitate the implementation of robust security measures to protect sensitive data effectively. Ensuring database security is paramount due to the potentially severe outcomes of breaches, such as identity theft, financial fraud, privacy violations, reputational harm, and legal liabilities. Furthermore, the dynamic nature of cyber threats and evolving regulatory requirements demand the adoption of comprehensive security strategies to safeguard valuable data effectively. Encryption techniques are employed to safeguard data from unauthorized disclosure, both during storage and transmission. Rapid reaction to security incidents is facilitated by auditing and monitoring methods[1].Upholding data integrity is imperative for maintaining the consistency, accuracy, and reliability of information across the enterprise. It serves as a safeguard against significant setbacks, preserving both the organization's operational efficacy and its credibility in the market.

A. Security Threats

1) Human Errors: Data may become unavailable due to accidental deletion, compromised in accuracy due to typographical errors or incorrect data entry, or rendered incomplete due to employee oversight. While such issues are often the result of unintentional mistakes, there are instances where they stem from deliberate malicious actions, highlighting the need for robust data governance and security measures

2) Transfer Errors: Transfer errors can occur when data is sent to an incorrect destination or becomes compromised during transmission between devices. Such incidents can render the data unreliable or unusable, undermining its value to the organization and potentially leading to significant operational disruptions.

3) Cyber Threats: These include vulnerabilities such as bugs, spam, malware, and other malicious activities specifically aimed at compromising your organization’s data integrity, exposing sensitive information, and disrupting operations.

4) Security Issues: These encompass vulnerabilities or security gaps that can be exploited by cybercriminals to infiltrate your systems, jeopardizing data integrity and exposing sensitive information to unauthorized access.

5) Hardware or Infrastructure Vulnerabilities: These include outdated hardware, physical damage to devices, or poorly secured infrastructure that lacks adequate attention to security. While data security measures can mitigate some of these threats, many challenges to data integrity require a comprehensive strategy. Without a robust approach to preserving data integrity within your organization, addressing these vulnerabilities and safeguarding your data will become increasingly difficult.

B. Security Goals

1) Confidentiality: It confirms the ability to the concealment of messages from a passive attacker so that any message communicated remains confidential.

2) Integrity: It confirms the reliability of the data and refers to the ability to confirm a message has not been tampered with, altered or changed

3) Authentication: It confirms the reliability of the message by identifying its origin. Data authentication verifies the identity of senders.

4) Availability: It confirms the ability to use the resources and whether the communication link is available for the messages to communicate.

II. RELATED WORK

Smith et al. examine traditional encryption methods like Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA) encryption, highlighting their strengths in securing digital information against threats. [2]

Zhou & Li (2021) explore the emerging field of post-quantum cryptography, presenting new algorithms designed to withstand potential quantum computing attacks. [3]

Early work by Morris & Thompson (1979) identified the vulnerabilities of simple password systems, especially regarding brute-force and dictionary attacks. [4]

More recent research by Gupta et al. (2020) combines CAPTCHA with password-based systems to enhance authentication security. [References [5]

Jain et al. (2016) provide a detailed review of various biometric systems, including fingerprint, facial, and iris recognition, focusing on their security benefits and challenges such as spoofing. [6]

Saeed et al. (2022) explore behavioral biometrics like keystroke dynamics, analyzing how user behavior can serve as an additional layer of authentication. [7]

Kim & Park (2020) highlight the use of blockchain technology in ensuring data integrity, with its decentralized, immutable ledger system offering an effective way to safeguard digital records[8]

Lee et al. (2017) discuss the application of cryptographic hash functions like SHA-256 in ensuring data integrity across distributed systems.[9]

Miller et al. (2021) discuss the rise of Advanced Persistent Threats (APTs) and ransomware attacks, stressing the importance of adaptive security measures. [10]

Huang et al. (2023) explore the role of Artificial Intelligence (AI) in identifying and mitigating threats in real-time, presenting promising solutions for intelligent threat detection.[11]

III.METHODOLOGY

Figure :1 Approaches to Safeguard Data Security in Organizations

A. *Data Eraser in Information Management*

Data erasure is a critical data security control in information management, ensuring that sensitive data is completely and irretrievably destroyed from storage devices. This prevents unauthorized access to confidential information, particularly during the disposal or repurposing of old hardware. Techniques such as secure erasure software, physical destruction, and cryptographic wiping are commonly employed to ensure that data cannot be recovered once it is deleted.

B. *Data Resilience*

Data resilience is a vital aspect of data security controls, ensuring that an organization's information systems can recover quickly and continue operating in the face of disruptions such as cyber attacks, hardware failures, or natural disasters. Key strategies include implementing robust backup solutions, employing redundancy across storage systems, leveraging disaster recovery plans, and utilizing secure cloud infrastructures. These measures help maintain data availability, integrity, and continuity, safeguarding critical information and minimizing downtime in information management systems.

C. *Backups and Disaster Recovery*

Backups and disaster recovery are essential components of a comprehensive data security strategy, ensuring the protection and restoration of critical data during unexpected disruptions.

1) *Backups:* Regularly creating copies of data and storing them in secure locations (safeguards against data loss due to hardware failures, accidental deletions, or cyber attacks. Effective backup strategies include full, incremental, and differential backups, tailored to organizational needs and recovery objectives.
2) *Disaster Recovery:* Disaster recovery involves a structured plan to restore systems, data, and operations following catastrophic events such as natural disasters, or system failures. Disaster Recovery plans often incorporate failover mechanisms, Recovery Time Objectives (RTO), And Recovery Point Objectives (RPO) to minimize downtime and ensure business continuity.

Together, backups and disaster recovery ensure that organizations can maintain resilience, protect data integrity, and recover quickly in the face of disruptions.

D. *Data Security Controls - Encryption in Information Management*

Encryption is a fundamental data security control used in information management to protect sensitive data by converting it into an unreadable format, accessible only to authorized parties with a decryption key. Common encryption methods include symmetric encryption (e.g., AES) for faster processing and asymmetric encryption for secure key exchanges. It ensures confidentiality, protects against unauthorized access, and mitigates risks of data breaches even if the data is intercepted or stolen. Encryption is essential for regulatory compliance, safeguarding intellectual property, and maintaining trust in information management systems.

E. *Access control*

Access control is a critical data security measure in information management that regulates who can view, use, or modify information based on predefined permissions. It ensures that only authorized users have access to sensitive data, reducing the risk of breaches and unauthorized activities.

IV. COMPARISION OF EFFICIENCY AND CHARACTERISTICS IN DATA SECURITY CONTROLS

Table: 1 Comparative Analysis of the Efficiency And Characteristics of Data Eraser, Data Resilience, Backups and Disaster Recovery, Encryption, and Access Control in Data Security

Control	Purpose	Efficiency
Data Eraser	Ensures permanent deletion of data to prevent unauthorized recovery.	High efficiency in preventing data breaches after hardware disposal or repurposing.
Data Resilience	Maintains availability and integrity of data during disruptions.	Critical for sustaining operations in the face of failures or attacks.
Backups and Disaster Recovery	Safeguards data by creating copies and enabling system restoration post-disaster.	High efficiency in data recovery after breaches or physical damage.
Encryption	Protects data by converting it into an unreadable format for unauthorized users.	Highly efficient for ensuring confidentiality and security during data transmission and storage.
Access Control	Regulates user permissions to prevent unauthorized access.	Essential for real-time security and preventing breaches.

A. *Efficiency Levels (%) for Data Security Controls*

The efficiency of data security controls varies depending on the use case, implementation quality, and specific organizational requirements. Below is an estimated percentage efficiency level for each control, based on typical effectiveness in its designated function:

Table: 2 Comparative Analysis of the Efficiency Levels of Data Eraser, Data Resilience, Backups and Disaster Recovery, Encryption, and Access Control in Data Security.

Control	Efficiency Level (%)	Explanation
Data Eraser	99%	Highly effective in ensuring data cannot be recovered if proper methods (e.g., cryptographic wiping) are used.
Data Resilience	95%	Very efficient in maintaining data availability during disruptions, but effectiveness depends on infrastructure robustness and redundancy measures.
Backups and Disaster Recovery	95%	Strong for data recovery; efficiency depends on the frequency of backups, recovery plans, and testing procedures.
Encryption	98%	Exceptionally effective in protecting data during storage and transmission but relies on secure key management.
Access Control	90%	Effective for restricting access, but can be compromised by poor configuration, insider threats, or social engineering.

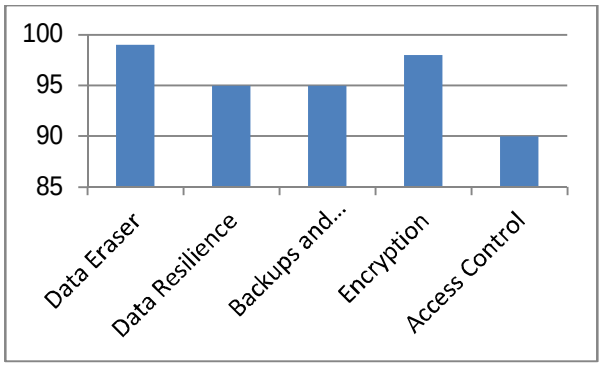


Figure 2: Efficiency Levels of Data Eraser, Data Resilience, Backups and Disaster Recovery, Encryption, and Access Control in data security.

V. OBSERVATIONS

1) Data Eraser is optimal for end-of-life data security but does not contribute to ongoing protection or recovery.
2) Data Resilience ensures operational continuity but relies on robust infrastructure and resource investment.
3) Backups and Disaster Recovery are crucial for post-incident recovery but require planning and regular validation.
4) Encryption offers universal protection against unauthorized access but needs effective key management for efficiency.
5) Access Control is a foundational security layer that complements all other methods by restricting data access to authorized users only.

Each technique addresses specific aspects of data security, and an integrated approach combining these controls is essential for comprehensive protection. Data Eraser has near-perfect efficiency when implemented correctly, but gaps may arise if methods are outdated or improperly executed. Data Resilience heavily relies on proactive design and infrastructure investments, such as redundancy and fault tolerance. Backups and Disaster Recovery efficiency is lower due to the reliance on human intervention, regular testing, and potential delays in restoration. Encryption achieves high efficiency but can fail if encryption keys are mishandled or if quantum-resistant algorithms are not used when necessary. Access Control is highly effective for real-time protection but requires integration with robust authentication mechanisms and vigilant monitoring. While Data Eraser and Encryption can achieve very high efficiency (approaching 99%) under optimal conditions, no control can guarantee 100% efficiency due to external variables and the dynamic nature of cyber security challenges. A layered, defense-in-depth strategy is the best approach to achieve maximum security.

VI. USAGE OF DIGITIZED TECHNOLOGIES

Block chain technology can be used for Data integrity, transparency, and decentralization. Offers strong authentication through cryptographic identities and secure transaction verification.
IoT is for Connecting and managing devices, especially in real-time data exchange.
AI tool can be used for Anomaly detection, enhancing encryption methods, and improving real-time decision-making.
Quantum Computing is b**est** for Future-proof encryption, addressing vulnerabilities in traditional cryptographic systems.
The Big Data Analytics is best for extracting actionable insights from vast amounts of data while detecting patterns for security threats.
This comparison examines how Block chain**,** IoT (Internet of Things)**,** AI (Artificial Intelligence)**,** Quantum Computing**,** and Big Data Analytics contribute to Data Security And Authentication, highlighting their characteristics and efficiency in these contexts.

Table: 3 Comparative Analysis of the Efficiency Levels of Data Eraser, Data Resilience, Backups and Disaster Recovery, Encryption, and Access Control in Data Security.

Technology	Characteristics	Data Security Characteristics	Capability
Block chain	Decentralized ledger system that stores data in an immutable, transparent manner.	Enhances Data Integrity and protects data from unauthorized modifications.	Highly secure and resilient, especially for identity management and secure transactions.
IoT (Internet of Things)	Network of interconnected devices that communicate and exchange data. Often uses cloud computing for data storage and processing.	Vulnerable to data breaches, as many IoT devices lack robust security.	IoT is efficient in enabling real-time data access but often lacks strong security controls.
AI (Artificial Intelligence)	Uses machine learning and deep learning to process large datasets and make predictions. AI algorithms improve over time.	Detects anomalies, potential threats, and malicious activity through pattern recognition.	Highly efficient in identifying patterns and detecting security threats in real-time.
Quantum Computing	Uses quantum mechanics principles to solve complex problems far faster than classical computers.	Quantum computing can break traditional cryptographic algorithms.	While still in development, quantum computing has the potential to disrupt traditional data security.
Big Data Analytics	Uses large, complex datasets to derive insights and make decisions. Real-time data processing and analytics.	Secures large volumes of data by detecting threats through pattern recognition.	Efficient at processing and analysing massive datasets. Security can be weak if data quality is flawed.

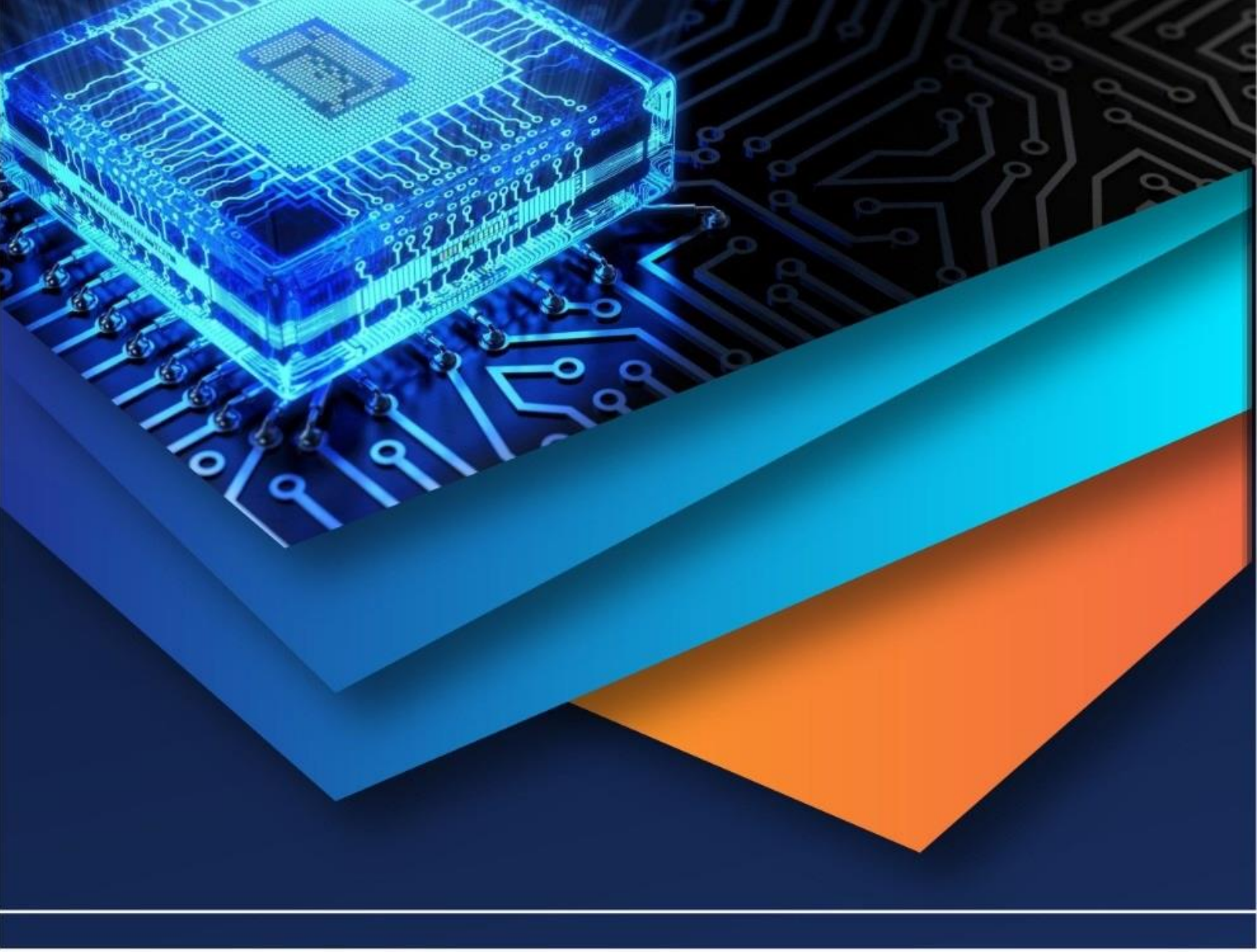
VII. CONCLUSION

The integration of digitized technology in information management offers benefits but necessitates robust data security mechanism. As threats evolve, a proactive approach combining technology, policy, and user education is essential for safeguarding digital assets. Collaboration between researchers, policymakers, and industry stakeholders will ensure that the innovations in data security remain a step ahead of potential adversaries. Data Eraser and Encryption can achieve very high efficiency under optimal conditions. no control can guarantee 100% efficiency due to external variables and nature of cyber security challenges. A layered, defense-in-depth strategy is the best approach to achieve maximum security. To achieve maximum data security, organizations should aim for a layered approach that combines these controls. This synergy ensures that weaknesses in one area are mitigated by the strengths of another.

REFERENCES

[1] K. Abouelmehdi, A. Beni-Hssane, H. Khaloufi, and M. J. P. C. S. Saadi, “Big data security and privacy in healthcare: A Review,” vol. 113, pp. 73-80, 2017.
[2] Smith, R., Zhang, X., & Gupta, M. *Advancements in Cryptographic Systems for Information Security*. International Journal of Information Security, 18(2), 55-71.2019
[3] Zhou, W., & Li, X.. *Post-Quantum Cryptography: Techniques and Challenges*. Journal of Cybersecurity, 27(4), 199-212.2021.
[4] Morris, R., & Thompson, K. (1979). *Password Security: A Case History*. Communications of the ACM, 22(11), 594-597.
[5] Gupta, S., Rajput, R., & Sharma, A.. *Enhanced Password Authentication with CAPTCHA for Security*. Journal of Information Security, 32(3), 77-88.202

[6] Jain, A.K., Ross, A., & Nandakumar, K. (2016). *Introduction to Biometrics*. Springer Science & Business Media.]
[7] Saeed, M., Iqbal, T., & Shahid, A. (2022). *Behavioral Biometrics for Authentication: A Review*. Security and Privacy, 5(1), 1-12.2016
[8] [Kim, H., & Park, H. *Blockchain for Data Integrity in Digital Information Systems*. Journal of Blockchain Technology, 5(2), 22-36,2020.
[9] Lee, Y., Lee, K., & Chang, W. *Data Integrity and Hashing Algorithms: A Survey*. International Journal of Computer Science and Security, 12(1), 63-77.2017
[10] Miller, P., Wang, T., & Stone, J. Emerging Cyber Threats and Adaptive Security. Journal of Cybersecurity and Information Protection, 28(3), 45-56.2021
[11] Huang, Z., Chen, Y., & Liu, B., AI-Based Cyber Threat Detection and Prevention. AI & Security, 9(1), 34-48, 2023



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY