Review and Prospect of Research on the Application of VR Technology in Education and Teaching Analysis based on citespace knowledge graphs

Nanda Ari Wahyu Widagdo [1]*, Afiat Lintang Winasis[2], Fanisa Halya Putri[3], Fhatoni Nur Wardana [4], Bondan Wahyu Pamekas[5]

[1,2,3,4,5] *Duta Bangsa University, Indonesia*

Article Information

Received: 21-11-2024

Revised: 28-11-2024

Published: 05-12-2024

Keywords

Data Protection; Information Systems; Security

Correspondence Email:

nandaari@gmail.com

Abstract

Management information system (MIS) data protection is critical and cannot be ignored, especially considering the increasing number of cyber threats and data leaks that can harm organizations. This journal discusses various data protection methods that can be used in MIS, with special emphasis on risk analysis and good implementation. In this research, we conducted a comprehensive analysis of the various threats faced by management information systems, including threats from cyberattacks, human error, and technological vulnerabilities. We also identify the components that contribute to those risks and how they impact data integrity and confidentiality. We do this using a case study approach and qualitative data collection. Additionally, the journal offers various solutions for mitigation, such as implementing strict access controls, data encryption, and security training for users. We also emphasize how important it is to have a clear information security policy and disaster recovery procedures to ensure continued operations. This research aims to assist organizations in strengthening their management information systems by providing practical, evidence-based recommendations for implementing data protection strategies. It is hoped that the results will serve as a guide for stakeholders in designing and implementing effective data protection strategies, which will increase trust and security in data management in the digital era.

1. Introduction

Management information systems (MIS) play an important role in the increasingly digital era to assist decision making, more efficient operations and management of organizational data. MIS not only serves as a tool for collecting and processing data, but is also the basis for broader business strategies. However, with increasing reliance on information technology, data protection issues are becoming increasingly complex. Cyberattacks, human error, and system failures are some sources of data security risks. Recent reports indicate that many organizations are experiencing significant data leaks, which can result in financial losses and reduce customer trust. Therefore, it is important for organizations to identify these threats and create a useful data protection plan.

The aim of this journal is to examine various approaches to data protection in management information systems, with an emphasis on risk analysis and implementation of appropriate solutions. We will analyze the various types of risks faced by MIS and how implementing appropriate policies and technology can manage these risks. In the next section, we will discuss research techniques used to identify and analyze risks as well as successful mitigation methods. It is hoped that this journal can assist in the development of information security policies in various organizations by providing in-depth information about MIS data protection. It is also hoped that this study can help stakeholders create better and more sustainable data protection measures in today's digital era.

1.1 Literature Review

As threats to data security increase, data protection in Management Information Systems (MIS) becomes increasingly important. Organizations rely heavily on the management and protection of their data, as data is a valuable asset. According to Wijoyo et al. (2023), MIS data security includes protection of the confidentiality, integrity and availability of stored information. Therefore, dangers such as data theft and system damage must be considered comprehensively. Data protection policies are an important component of a data protection strategy. Indonesian regulations such as Minister of Communication and Information Technology Regulation Number 20 of 2016 concerning Personal Data Protection help manage personal data. However, there are still problems implementing these policies, especially related to organizational compliance and personal data protection in the ever-changing digital era.

2. Research Methods

By focusing on risk analysis and implementation, this research aims to investigate methods for protecting data in management information systems. To gain a comprehensive understanding of problems and solutions in data protection, both qualitative and quantitative approaches will be used. Various stakeholders, including IT managers, users, and cybersecurity experts, participated in this research to gain an in-depth understanding of data protection. Data can be collected through interviews and questionnaires distributed online to selected individuals. Data Analysis: For qualitative data, content analysis techniques were used to determine major themes from interviews and discussions; for quantitative data, survey results are analyzed using statistical software and presented in the form of graphs or tables.

3. Results and Discussion

In the digital era that continues to develop rapidly, data security is very important. Data not only functions as a supporting tool, but is also a strategic asset that determines a company's sustainability and competitiveness in a world that is increasingly dependent on technology. As reliance on modern technologies such as cloud computing, Internet of Things (IoT), and artificial intelligence (AI) increases, management information systems face increasingly complex challenges. Although these technologies provide high operational efficiency, they also pose significant security risks.

If data is not secure, there are significant consequences, such as financial losses from data theft or hacking, damage to the organization's reputation, and legal consequences from breaches of personal data protection. Additionally, organizations that fail to maintain data security can lose the trust of partners, customers, and other stakeholders. As a result, an effective data security strategy must be proactive and holistic. This method requires the use of advanced technology, structured policies, and an organizational culture that supports data security. Additionally, implementing a strong security strategy involves comprehensive prevention, detection, response, and remediation measures.

Data Security Threat Ecosystem

1. Technological Threats Technology-based threats include Distributed Denial of Service (DDoS) attacks, malware, ransomware, and exploitation of system weaknesses. This is increasingly complex as attacks that use artificial intelligence to disguise patterns and create zero-day threats—that is, previously undetected exploits—are emerging.

2. Human Threats Data leaks often occur due to human error, such as system misconfiguration or use of poor passwords. This vulnerability is enhanced by insider actions, whether intentional or not. Hackers can access an organization's systems if employees click on phishing links without realizing it.

3. Structural Threats It is possible that weaknesses in the system architecture design, such as a lack of data redundancy or poor access control, increase the risk of data corruption or loss. Systems that lack a regular audit or evaluation process also make it difficult to identify and remediate potential threats early.

Multilayer Approach In Data Protection

In data protection, a multilayer approach combines multiple layers of protection to make a system resistant to various types of threats.

1. Integrated Security Architecture

a. Role-Based Access Control: Manage access based on user roles to ensure only authorized parties can access sensitive data.

b. Multi-Factor Authentication: This is a combination of various authentication techniques, such as passwords, biometrics, or tokens, used to increase security.

c. End-to-End Encryption: Protects data as it is stored and transmitted so that only authorized people can view it.

2. Advanced Protection Technology:

a. Advanced Encryption Methods: Protects data from unauthorized access by using algorithms such as High Encryption Standard (AES) or RSA.

b. Redundant Array of Independent Disks (RAID): Provides data redundancy to prevent information loss due to hardware failure.

c. Backup and Recovery: To reduce operational downtime, use an automated backup system with a measured recovery point of interest (RPO).

3. Dynamic Access Control

a. Access restrictions tailored to user behavior, such as restricting access when suspicious activity is discovered;

b. Automatic revocation of access permissions after users complete tasks to prevent unauthorized use of data.
4. Security Incident Handling Protocol

Planned procedures are required to handle security incidents from detection to recovery. Training Stage: a. Establish

a special security group trained to handle security accidents.

b. Develop standard operational guidelines with emergency response scenarios.

c. Incident simulation is carried out to evaluate system readiness.

Identification Stage:

a. Detect anomalous activity using AI.

b. Conduct a thorough examination of incoming attack patterns.

Restriction Stage:

a. Protect systems that are indicated to be infected from spreading.

b. Stop operations on affected parts while ensuring that the system is operating properly.

Eradication Stage:

a. Removes malware and other system threats.

b. Fix weaknesses in use

Recovery rate:

a. Restore the system to normal condition with safe data.

b. Test system reliability post-recovery to ensure that no threats remain.

Follow-up Stage:

a. Conduct a thorough analysis to determine the main source of the incident.

b. Incorporate lessons learned into new security approaches.

Human Factors in Data Security The human component is an important part of a security system. Even the best technology can fail if users do not know and are able to use it. Therefore, users should be trained regularly to ensure that they understand the importance of data security. To gauge user readiness, training programs may include simulated attacks such as phishing or ransomware. promote a culture of information security in the company by providing incentives to employees who follow good security protocols. Future Challenges and Projections 1. Increasing Complexity of Threats: Organizations must face new challenges that require more innovative security approaches due to the adoption of technologies such as the Internet of Things and AI. 2. Incorporation of Modern Technology: AI to quickly detect attacks Machine learning to use historical patterns to predict potential threats. 3. Global Standardization: To ensure that organizations around the world receive the same protection, security procedures must be adapted globally.

4. Conclusions

In the connected digital era, data security is increasingly important. Organizations and individuals must be prepared to face increasingly sophisticated and diverse data threats. More and more companies, government agencies and individual users are realizing how important it is to maintain data integrity, confidentiality and accessibility. Strict regulations and advanced technology will be critical to keeping data secure and creating a safer digital environment. With the emergence of new technologies such as 5G, Internet of Things, and AI in the future, data security issues will become increasingly complicated. To overcome this problem, a broad and multi-layered approach is needed. Therefore, data protection must be a joint effort involving governments, organizations, technology developers and the general public. We can create a safer digital ecosystem with cooperation, strong regulations and technological advances. For data to remain a useful resource without compromising the privacy and security of people and organizations, it is important to continually adapt to evolving cyber threats.

5. References

Abdullah, M. S., & Ikasari, I. H. (2023). Perkembangan Terbaru Dalam Keamanan Siber, Ancaman Yang Diidentifikasi Dan Upaya Pencegahan. JRIIN: Jurnal Riset Informatika dan Inovasi, 1(1), 96-98.

Muhajirin, M., & Panorama, M. (2017). PENDEKATAN PRAKTIS; Metode Penelitian Kualitatif dan Kuantitatif.

Nurul, S., Anggrainy, S., & Aprelyani, S. (2022). Faktor-Faktor Yang Mempengaruhi Keamanan Sistem Informasi: Keamanan Informasi, Teknologi Informasi Dan Network (Literature Review Sim). Jurnal Ekonomi Manajemen Sistem Informasi, 3(5), 564-573.

Octaria, M., & Nasution, M. I. P. (2024). Peluang dan Tantangan Penerapan Internet of Things (IoT) dalam Sistem Informasi Manajemen. Switch: Jurnal Sains dan Teknologi Informasi, 2(3), 56-62.

Ramadhana, R. Z., & Nasution, M. I. P. (2024). Analisis Dampak Penerapan Teknologi AI pada Pengambilan Keputusan Strategis dalam Sistem Informasi Manajemen. Jurnal Ilmiah Research and Development Student, 2(1), 161-168.

Romlah, S. (2021). Penelitian Kualitatif dan Kuantitatif (Pendekatan Penelitian Kualitatif dan Kuantitatif). Pancawahana: Jurnal Studi Islam, 16(1), 1-13.

Syahputra, R. A., Maliza, N. O., Kasmawati, K., & Putri, C. W. A. (2024). Strategi Peningkatan Kesadaran Data dan Informasi Masyarakat di Era Digital. Jurnal Pengabdian kepada Masyarakat Nusantara, 5(3), 3164- 3171.

Wijoyo, A., Fatimah, S., & Widianti, Y. (2023). Keamanan Data dalam Sistem Informasi Manajemen: Risiko dan Strategi Perlindungan. TEKNOBIS: Jurnal Teknologi, Bisnis dan Pendidikan, 1(2)