Journal of Artificial Intelligence and Engineering Applications

Website: https://ioinformatic.org/

15th June 2025. Vol. 4. No. 3; e-ISSN: 2808-4519

Data Security Analysis in Information Management in Digital Food Sovereignty Systems

Ida Ayu Dara Putri Amaranggani[1]*, Lilik Widyawati[2], Dadang Priyanto[3], Galih Hendro Martono[4]

[1,2,3,4]Universitas Bumigora
idaayuputry18@gmail.com[1*], lilikwidya@universitasbumigora.ac.id[2], dadang.priyanto@universitasbumigora.ac.id[3], galih.hendro@universitasbumigora.ac.id[4]

Abstract

The digital food sovereignty system represents an innovation in food information management, enhancing efficiency, transparency, and food security across various sectors. However, during its implementation, data security remains one of the most significant challenges that must be addressed to ensure the system's continuity and reliability. This study aims to analyze data security aspects within the digital food sovereignty system, focusing on potential risks, vulnerabilities, and applicable mitigation strategies. A descriptive qualitative approach was employed, involving data collection through direct observation, stakeholder interviews, and literature reviews from relevant sources. The findings indicate that key challenges in data security include threats from cyberattacks, data breaches, and insufficient user awareness regarding the importance of information protection. To address these issues, strict security measures such as data encryption, multi-layered authentication, and regular system monitoring are essential. The analysis highlights that strengthening data security in digital food sovereignty systems requires a comprehensive approach that integrates technical solutions, policy development, and user education. This research is expected to contribute to the formulation of more effective security strategies that support the advancement of digital-based food sovereignty.

Keywords: *Data Security, Food Sovereignty, Information Management, Security Risk, Digital Systems.*

1. Introduction

The development of information technology has transformed various sectors, including the food sector. The digitalization of food sovereignty enables more efficient data management in production, distribution, and consumption. Data such as harvest yields, stock levels, and supply chains are now processed digitally to support decision-making. However, this advancement also brings data security risks, such as hacking, data theft, and information manipulation, which can disrupt the food supply chain [1].

Data security has become a critical issue, as vulnerabilities in the system may significantly impact food security. Therefore, policies that ensure data confidentiality, integrity, and availability are essential through the implementation of encryption, strict access control, and regular audits [2]. Raising awareness of the importance of data security among stakeholders is also necessary.

The implementation of data protection standards such as ISO/IEC 27001 is a strategic step in building a reliable system. This standard provides guidelines for data management, security incident response, and personal data protection [3]. With these measures, digital food sovereignty systems can operate optimally without neglecting security risks.

Digital transformation has changed food system management, enabling real-time monitoring of productivity, distribution, and consumption. However, the rising number of cyber threats adds complexity to data security challenges. The Global Food Security Index (2023) highlights cyberattacks as a factor influencing global food security [5].

This study discusses the impact of digitalization on food sovereignty systems, particularly regarding data security risks. Rachmayani [4] emphasized that digital systems can enhance the effectiveness of food production and distribution management, but also face serious threats. Therefore, this study aims to analyze data security in digital food sovereignty systems, identify vulnerabilities, and propose strategic data protection recommendations to support the sustainability of food systems.

2. Research Methodology

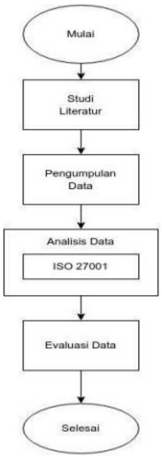

Fig. 1: Research Methodology

2.1. Literature Review

The literature review was conducted to understand the concepts, theories, and practices related to data security and digital food information systems. The researcher examined various sources, including scientific journals, reference books, research reports, and policy documents, with a focus on the ISO 27001 information security standard. This review centered on three main aspects of information security: confidentiality, integrity, and data availability.

In terms of confidentiality, the study explored the importance of restricting access to food data so that only authorized parties can access it. The reviewed literature covered access policies based on authorization, user account management, and access control mechanisms tailored to the needs of information systems in village environments.

For integrity, the researcher investigated the importance of maintaining data accuracy and consistency. The review included data validation policies, proper documentation, and audit procedures to ensure that data is not altered without proper authorization.

Regarding availability, the study reviewed strategies to ensure that digital food information systems remain accessible to authorized parties. The literature analyzed policies on data backup, continuous system maintenance, and risk mitigation strategies to ensure operational continuity.

2.2. Data Collection

The data collected served as the foundation for analysis based on the ISO 27001 framework. Data collection was conducted through observation. Observations took place by directly examining the food data management processes in Tagawiti Village. The researcher focused on the following: data security mechanisms implemented in the food information system, potential vulnerabilities that threaten data confidentiality, integrity, and availability, the condition of the information technology infrastructure, including hardware and software, user behavior in maintaining data security and compliance with existing security policies.

2.3. Data Analysis

The purpose of data analysis in this study was to evaluate the level of information security in the management of digital food data in Tagawiti Village based on ISO 27001 standards. The analysis focused on three key aspects of information security: confidentiality, integrity, and availability.

Regarding confidentiality, the analysis identified potential vulnerabilities such as inadequate authentication systems and the absence of data encryption. These findings indicate a risk of unauthorized access to food data. To address this, the researcher recommends implementing multi-layered authentication and role-based access policies.

For integrity, the analysis found that Tagawiti Village lacks a systematic data validation mechanism, potentially leading to data errors or manipulation. The researcher recommends developing data validation procedures prior to storage and implementing change logs to monitor any data modifications.

In terms of availability, the analysis revealed that the village does not yet have a structured data backup policy, increasing the risk of data loss due to technical disruptions or disasters. The researcher suggests implementing a regular data backup system and establishing clear data recovery procedures.

2.4. ISO 27001

The ISO 27001 is an international standard for information security management designed to help organizations protect data from various risks. This study adopts ISO 27001 as a framework to analyze data security in the digital food sovereignty system in Tagawiti Village. The analysis focuses on three key aspects:

Confidentiality: Securing access to information so that only authorized personnel can retrieve data, Evaluation revealed weaknesses in user authentication, It is recommended to apply data encryption and conduct security training for village staff.

Integrity: Ensuring that data remains accurate and unchanged without authorization, The implementation of input validation, audit logs, and data redundancy is advised to maintain information reliability.

Availability: Ensuring the system is accessible whenever needed, Regular backups, system maintenance, and emergency response procedures are recommended.

2.5. Evaluation

This study evaluates data security aspects in managing digital food sovereignty systems using the ISO 27001 approach. The evaluation includes several key areas. Security policies must be formally developed and implemented to serve as clear operational guidelines. In risk management, threat identification has been conducted, but a more detailed approach is required to mitigate potential risks to data security. From a technical control perspective, the system has begun to implement input validation and data protection measures; however, it still requires additional protection mechanisms. Access management is not yet optimal and must be aligned with appropriate user authorizations. System monitoring also remains unstructured, necessitating the development of better security monitoring mechanisms. Finally, security training for system administrators is essential to ensure their understanding of information security standards and enhance implementation effectiveness.

3. Results and Discussion

The research began with a literature review. This review aimed to understand the theoretical foundations of data management and information security in digital food sovereignty systems. The literature included references from books, academic journals, and international standards such as ISO 27001. This review highlighted the importance of protecting sensitive data and implementing security protocols to minimize the risk of information leakage.

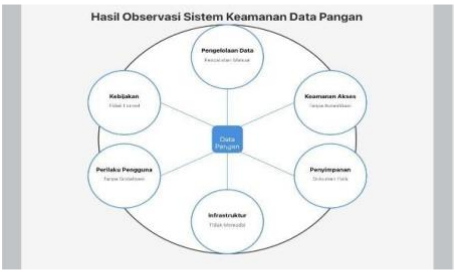

Fig. 2: Observation Results on Food Data Security System

During the documentation review phase, the following documents were examined:

1. Food production records: including the quantity and types of food commodities produced.
2. Data recording and management processes: whether using manual or digital systems.
3. Data security policies: regulations concerning the management, access, and storage of information.
4. Technological infrastructure: devices or systems used for food information management.

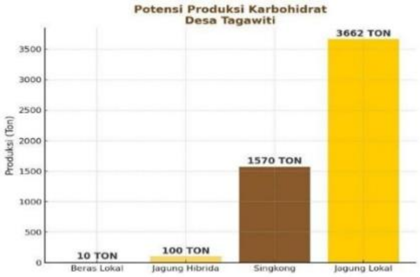

Fig. 3: Food Production in Tagawiti Village

The diagram above indicates that the village heavily depends on corn and cassava as the main drought-resistant crops, reflecting the significant influence of environmental factors on farming patterns. The low rice production increases vulnerability to food crises if corn production is disrupted, particularly in the absence of alternative carbohydrate sources. Therefore, a digital food sovereignty system must be designed to accurately record, monitor, and analyze the production of these two commodities to support food resilience.

Moreover, based on document analysis related to the food production recording system, several weaknesses in data security were identified, especially when compared to ISO 27001 standards.

The current data storage system still relies on physical records without digital support, posing a high risk of data loss or damage due to disasters, negligence, or document deterioration. Furthermore, access security lacks clear regulations regarding who is authorized to access or modify data, increasing the potential for manipulation or information leakage. The absence of backup procedures also heightens the risk of permanent data loss, which could hinder planning and decision-making. Data accuracy is another concern, as records are manually entered without a verification system, making them prone to errors that could affect the analysis of food production and distribution. Additionally, data integrity is not guaranteed due to the absence of audit systems or verification mechanisms, allowing undetected input errors or data manipulation.

In the data security analysis, risk identification was conducted to map potential threats to data availability, integrity, and confidentiality. Key identified risks include data breaches caused by system vulnerabilities or cyberattacks, and data tampering that could result in information manipulation or deletion, thus disrupting system operations. Malware threats such as ransomware or spyware also pose serious risks to the system. Other threats include denial-of-service (DDoS) attacks that may hinder system access, data loss due to system failure or lack of backups, and unauthorized access by unapproved parties.

Following risk identification, a security evaluation was conducted by comparing the current system with ISO 27001 standards. The evaluation revealed several areas in need of improvement. First, regarding confidentiality, the system lacks strong authentication mechanisms and has not yet implemented role-based access control, increasing the risk of unauthorized access. Second, in terms of integrity, the system does not yet feature audit logs to systematically record user activity, nor does it implement sufficient data validation to prevent manipulation. Third, in terms of availability, the system lacks a routine data backup procedure, risking information loss in the event of system failure. These findings indicate the need for multiple improvements to align the system with ISO 27001 standards.

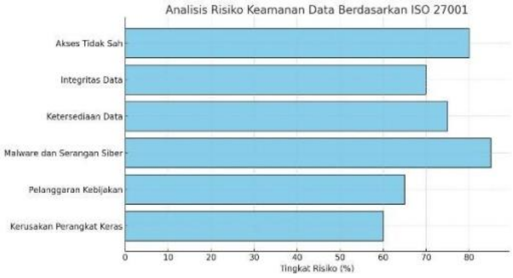

Fig. 4: Data Security Risk Analysis Based on ISO 27001

Based on the prior evaluation, the most significant threats to the system stem from malware and cyberattacks, which can severely damage or steal large amounts of data. Additionally, unauthorized access by third parties remains a critical concern, as it can lead to the misuse of confidential information. The lack of backup and data replication systems also increases the risk of information loss, which could impact service availability. Several mitigation measures should be implemented to address these issues.

One recommendation is to regularly update firewalls and implement intrusion detection and prevention systems (IDS/IPS) to identify and block potential attacks before they damage the system. Furthermore, the implementation of two-factor authentication (2FA) would strengthen access security and minimize the risk of unauthorized entry. In terms of availability, automatic data backups and off-site data replication are strongly recommended to ensure data safety in the event of technical disruptions.

As part of the effort to improve data security, various security controls have been applied to the system. One key measure includes regular system maintenance through periodic security audits aimed at identifying and correcting potential vulnerabilities before they are exploited. Additionally, the system now features real-time security monitoring, allowing for the swift detection of suspicious activities.

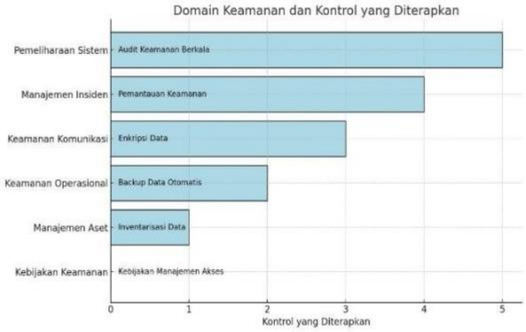

Fig. 5: Security Controls Applied in the Digital Food Sovereignty System

In terms of communication security, the system employs data encryption during transmission, ensuring better protection against eavesdropping. Operational security has been strengthened through automatic data backups, guaranteeing that information can be recovered in case of system failure. From an asset management perspective, periodic data inventory is conducted to ensure proper handling of sensitive information. Lastly, in the area of security policy, the system has implemented role-based access controls to limit users' access only to information relevant to their responsibilities.

Based on the evaluation of implemented security controls, the measures taken have improved data protection, especially in access control and data backup. The implementation of data encryption and automatic backup has provided additional protection against potential data loss or theft. However, several aspects still require improvement. One notable weakness is the lack of real-time threat detection mechanisms, which means the system is not yet capable of promptly responding to attacks. Additionally, the data recovery capability after an incident needs enhancement to ensure a more efficient restoration process. Therefore, to improve the effectiveness of security controls, it is necessary to strengthen monitoring and incident response mechanisms so the system can be more resilient to evolving threats.

4. Conclusion

This study highlights that the digital food sovereignty system in Tagawiti Village still faces significant data security challenges. The implementation of ISO 27001 standards is not yet optimal, with major weaknesses in authentication, access control, and the absence of comprehensive security policies. In terms of confidentiality, the lack of clear encryption and authentication increases the risk of data breaches. Regarding integrity, data recording remains manual and lacks sufficient validation, making it prone to errors and manipulation.

Furthermore, availability is a concern due to the absence of a structured data backup policy, increasing the risk of information loss. The low level of user awareness about data security further exacerbates the potential threats. To address these issues, stricter security policies are essential, including role-based access control, regular data backups, and user security training.

This study contributes by identifying security vulnerabilities and recommending improvements to enhance data protection in the digital food sovereignty system. By aligning security controls with international standards, the system is expected to become more secure, efficient, and reliable in the future.

References

[1] Rachmayani, A. N. (2015). Kesiapan daerah mendukung pertanian modern. Jurnal Agribisnis Indonesia, 3(1), 45–60.

[2] Popon, R. Y. (2023). Building a cyber security system in the archipelago capital (IKN) to support it. Kemhan RI.

[3] Swajati, W. G. (2019). Strategi implementasi regulasi perlindungan data pribadi di Indonesia. Indonesiana, 1–26. https://www.indonesiana.id/read/6877/urgensi-regulasi-perlindungan-data-pribadi-di-indonesia.

[4] Timisela, N. R., Dwidjono, H. D., & Hartono, S. (2014). Supply chain management and performance of local food sago agroindustry in Maluku Province: A structural equation models approach. Agritech, 34(2), 184–193. https://doi.org/10.22146/agritech.29676

[5] Ummah, M. S. (2019). Pilar-pilar hukum progresif menyelami pemikiran Satjipto Rahardjo. Sustainability, 11(1), 1–14. https://doi.org/10.3390/su11010001