Journal of Deep Learning, Computer Vision and Digital Image Processing
E-ISSN: 2986-8939 P-ISSN: 2986-8920
Vol. 4, No. 1, March 2026
DOI. https://doi.org/10.61255/decoding.v4i1.978

Performance and Security Analysis of Academic Information System Integration with Cloud Computing Technology

(Muhammad Ridho Ardiansyah
Institut Teknologi dan Bisnis Bina Sriwijaya Palembang, Indonesia)

(Mahmud
Institut Teknologi dan Bisnis Bina Sriwijaya Palembang, Indonesia)

(Ibnu Aqil
Institut Teknologi dan Bisnis Bina Sriwijaya Palembang, Indonesia)

OPEN ACCESS

ARTICLE HISTORY
Received: Jan 5, 2026
Revised: Feb 18, 2026
Accepted: Mar 21, 2026

KEYWORDS
Academic information system;
Cloud computing technology;
Performance analysis;
Security;
System integration

ABSTRACT

Purpose – The implementation of cloud computing technology for integrating Academic Information Systems (SIAKAD) offers solutions to challenges regarding centralized infrastructure, limited scalability, and data security issues faced by higher education institutions. This study aims to analyze and evaluate the performance and data security aspects of academic information systems integrated via cloud computing platforms.

Methods – Employing both quantitative and qualitative approaches, the performance evaluation focuses on access speed, scalability, and operational efficiency. Meanwhile, the security analysis examines data protection mechanisms both at rest and in transit as well as compliance with cloud security standards.

Findings – The results indicate that cloud-based integration significantly enhances access speed, service availability, and the flexibility of academic data management.

Research implications – However, the findings also identify that data security and privacy governance remain critical challenges, necessitating the implementation of rigorous access controls such as encryption and identity management—to mitigate cyber threats.

Originality – In conclusion, the adoption of cloud technology yields substantial efficiency improvements in academic services, provided it is accompanied by a comprehensive and structured cybersecurity strategy.

Correspondence Author: ✉Ridho.ard@gmail.com
To cite this article: Ardiansyah, M. R., Mahmud, & Aqil, I. (2026). Performance and security analysis of academic information system integration with cloud computing technology. Journal of Deep Learning, Computer Vision and Digital Image Processing, 4(1), 28-40. https://doi.org/10.61255/decoding.v4i1.978

INTRODUCTION

The development of information and communication technology (ICT) has brought significant changes in the management of academic information systems in educational institutions. Cloud computing technology is an option to increase the efficiency and flexibility of data management and academic applications. However, the integration of academic information systems with cloud computing technology also raises several challenges, such as academic data security and system performance. In recent years, many educational institutions have adopted cloud computing technology to improve the quality of educational services and increase the efficiency of academic data management. However, there are still many questions about how to analyze the performance and security of integrating academic information systems with cloud computing technology.

However, the integration of academic information systems with cloud computing technology also raises several challenges, such as: Security of academic data from cyber threats and data loss, System performance can be influenced by network quality and cloud computing infrastructure, Dependence on cloud computing service providers. Thus, this background provides an overview of ICT developments, the benefits of cloud computing, and the challenges of integrating academic information systems with cloud computing technology, as well as providing direction for analysis of the performance and security of integrating academic information systems with cloud computing technology. This research focuses on analyzing the performance and security of integrating academic information systems with cloud computing technology, as well as providing recommendations for improving system performance and security. This research does not include an analysis of the implementation of cloud computing technology in general, but only focuses on the integration of academic information systems with cloud computing technology.

This research has great significance in the development of more effective and secure academic information systems with cloud computing technology. The results of this research can help educational institutions improve the quality of educational services and increase the efficiency of academic data management. Thus, this introduction provides a broader picture of the background, context, problem formulation, research objectives, research benefits, research limitations, and research significance, as well as providing direction for performance and security analysis of the integration of academic information systems with cloud computing technology. In the Industry 4.0 era, cloud computing has become a key technology in supporting digital transformation in various industrial sectors. However, with increasingly widespread adoption, challenges related to information security and data privacy are also increasing. This research aims to explore cloud computing security strategies through a Systematic Literature Review (SLR) approach [1].

Cloud computing is a long-standing dream of computing as a utility, where users can store their data remotely in the cloud to enjoy on-demand services and high-quality applications from a shared pool of configurable computing resources. Thus, the privacy and security of data are of utmost importance to all of its users regardless of the nature of the data being stored. In cloud computing environments, it is especially critical because data is stored in various locations, even around the world, and users do not have any physical access to their sensitive data [2]. This study aims to explore optimizing the implementation of cloud-based management information systems in the industrial sector to enhance operational efficiency. With the rapid advancement of technology, cloud-based information systems offer various benefits, including cost savings, ease of access, and improved operational performance [3].

Efficient and secure data management is a key requirement for secondary schools, particularly when navigating the complexities of modern educational administration. This study aims to examine the implementation of cloud-based education management information systems in secondary schools, focusing on how this technology can enhance data management efficiency, information security, and data accessibility for stakeholders [4]. This research evaluates data security in cloud computing services with the Google Drive case study. Google Drive is a widely used file storage platform due to its ease of access and features, including end-to-end encryption, two-factor authentication and suspicious activity detection. However, security risks such as unauthorized access, phishing attacks,

and data leaks remain challenges that require attention. This research uses a qualitative-descriptive approach through literature studies, semi-structured interviews and usage simulations to evaluate the effectiveness of the security mechanisms implemented. The research results show that the security measures implemented are quite effective, but security gaps remain, mainly due to the low digital literacy of users. The analysis also revealed that the privacy policy implemented by Google Drive needs to be increased in transparency so that users can better understand how their data is managed. This research recommends strengthening security protocols, digital literacy education for users, as well as collaboration between user service providers [5].

The development of information technology in the digital era has a significant impact on ethics, integrity, and professional performance. This research aims to analyze the influence of information technology on language ethics on social media, understand the importance of digital privacy in community counseling, evaluate communication ethics in digital media, and identify the relationship between professional ethics, information technology, and its impact on professional integrity [6]. This study was conducted to assess the level of information security within the academic information system and to provide recommendations for improving information security management [7].

Works that address the integration of forensic preparedness and information security in a government context, with an emphasis on implementation, challenges, and outcomes. Apart from the SLR approach, bibliographic and mapping methods against certain standards and relevant frameworks are also used in this research. Preliminary findings indicate that although the implementation of DFR and ISMS separately is quite common, their integration is still underexplored, especially in the context of e-governance. This research identifies key challenges, including organizational inertia, technology incompatibility, and policy gaps, while highlighting best practices from global case studies. The research results can not only map trends and validate the urgency of implementing DFR into ISMS, but also provide a DFR Integration Model Framework for organizations. The research results are expected to provide implementable insights for policymakers, IT professionals, and researchers, and pave the way for a unified framework that bridges the gap between forensic preparedness and comprehensive security management. This research concludes by advocating the integration of DFR and ISMS as the main pillars of e-governance systems to improve cybersecurity readiness, strengthen accountability, and reduce risks associated with Digital transformation in the public sector [8]. The Regional Office of the Ministry of Law and Human Rights in the Special Region of Yogyakarta (DIY) is a vertical agency of the Ministry of Law and Human Rights of the Republic of Indonesia. Based in the province, it carries out duties and functions related to legal and human rights services, immigration, correctional affairs, and administration. Its operations are supported by information technology within an e-government framework, grounded in the principles of good governance [9].

Along with the rapid development of technology in the Industry 4.0 era, the implementation of cloud computing has become a key component in digital transformation, providing efficient and flexible solutions for data storage and management [10]. This technology not only facilitates fast access to computing resources but also enables better collaboration among users spread across various locations [10]. However, with the increasing adoption of cloud computing, data security and privacy issues have become major concerns. Research shows that cloud computing users are often concerned about potential threats to the confidentiality and integrity of their data [11]. According to a survey conducted by the International Data Corporation (IDC), users' main concerns lie in data protection and how to manage the risks associated with outsourcing information to cloud service providers [11].

In the implementation of cloud in complex big data environments, customer data protection and privacy are better maintained through layered encryption and granular access control that prevent unauthorized access and mitigate data privacy risks more systematically [12]. This is different from traditional approaches that tend to focus on perimeter security through firewalls and basic surveillance systems, which are less responsive to the dynamic and complex threat developments in the digital era [13]. In the banking sector, cloud computing enables more adaptive security management through multifactor authentication mechanisms, effective in reducing the risk of phishing attacks and theft of sensitive data. This system also significantly reduces the impact of

attacks through the rapid recovery features provided by cloud service providers [14]. In addition, cloud services provide automatic security updates, which minimizes companies' dependence on manual maintenance and ensures system readiness to face new attacks quickly and efficiently [12]. In terms of efficiency, cloud strategies support the implementation of centralized access control and automatic backups, so that data can be managed more securely and accurately. The cloud's ability to detect anomalies and suspicious activities in real-time is also a significant added value compared to traditional approaches, which tend to be reactive to potential threats [13]. Shows that cloud-based approaches using the SNORT tool successfully detect and prevent DDoS attacks with higher efficiency than traditional methods, which are often limited in identifying malicious network traffic from multiple sources [15].

The implementation of security standards in cloud computing systems in the Industry 4.0 era faces a number of significant challenges affecting technology companies. One of the main challenges identified is the lack of security skills and awareness among workers in transforming industries, which can hinder the effective implementation of security standards. The lack of adequate IT/OT skills and security policies in companies moving to cloud technologies leads to their vulnerability to cyber threats, which adds to the complexity of implementing appropriate security standards [16]. On the other hand, [17] pointed out that the implementation of strong encryption such as AES256 and MD5 in cloud security systems presents technical challenges related to computing power and key management, which affect the performance and scalability of the system. They revealed that although high-level encryption offers better protection, the implementation of these algorithms requires significant resources, which can be a barrier for small companies implementing full-fledged cloud computing [17]. In addition, [18] proposed A Zero Trust strategy-based trust assessment model, which focuses on managing access without relying on traditional perimeter security. While this strategy offers a higher level of security, its implementation faces challenges in managing identity and authentication in a highly distributed and dynamic cloud environment. This Zero Trust model requires companies to change the way they view security, from simply perimeter protection to a more holistic and data-driven approach [18].

In the Industry 4.0 era, cloud computing is often integrated with Internet of Things (IoT) devices to improve operational efficiency. However, the interconnectedness of these IoT devices also increases the potential for cyber threats, especially if the system is not equipped with adequate security measures [19]. IoT devices connected to cloud networks are vulnerable to various cyber attacks, such as denial-of-service (DoS) attacks, man-in-the-middle attacks, and device takeovers that can cause major disruptions in industrial operations [20]. To address these vulnerabilities, the integration of blockchain in an IoT cloud environment offers additional security assurance through strong identity verification and smart contract-based access control. These features ensure that only authorized users can access critical data and functions [19]. In addition to blockchain, the integration of artificial intelligence (AI) technology with blockchain further enhances the effectiveness of this security strategy by detecting attack patterns and providing faster and more targeted automated responses [20]. With the help of AI, the system can monitor data from IoT devices in real-time and identify anomalies or suspicious activities before threats develop into larger security incidents [20]. In addition to blockchain and AI technology, security standards such as ISO 27001:2013 have also proven effective in improving information security for technology companies in the Industry 4.0 era. A study conducted at the Ministry of Communication and Information Technology of Malang Regency showed that the use of the ISO 27001 standard enables the implementation of a structured information security management system, which is able to proactively identify and mitigate security risks through the management of policies, procedures, and access controls [21]. With comprehensive risk management, companies can better protect sensitive data and build user trust in information security in cloud computing environments [21].

In an era of rapid technological development, cloud computing has become a primary solution for data storage and management, including at Universitas Advent Indonesia (UNAI). This study aims to analyze the efficiency of cloud computing architecture at UNAI using the Reliability, Maintainability, and Availability (RMA) method with Proxmox Virtual Environment (Proxmox VE)-based monitoring

[22]. The word efficiency in the use of information technology is very important to ensure that available resources can be used optimally. According to [23], efficiency is the ability to achieve results using minimal resources. In the context of education, this efficiency can be achieved through the use of cloud computing technology which enables better and faster data management. Like the previous study entitled The Effect of Using Cloud Computing "NextCloud" on the Effectiveness and Efficiency of School Administration at State Senior High School 3 Ciamis [24], shows that the use of cloud computing platforms can increase the efficiency and effectiveness of school administration. The results of this study show that the use of NextCloud contributes to an increase in administrative efficiency of 96.8 percent, reflecting the organization's ability to better manage resources.

Cloud Computing or commonly called "cloud computing", is a container or technology for storing, processing, and accessing data via the internet [24] which is important in today's digital era [24]. The main advantages when using cloud storage are the availability of resources, easy data management, and low operational costs incurred [23]. This paradigm offers a great potential solution in meeting various organizational needs, including higher education institutions, namely UNAI. In the same context, the relationship between the cloud and educational institutions has a crucial role and is interrelated with one another. This research investigates the untapped potential of artificial intelligence (AI) in information technology applications to provide smarter solutions. In an era where data is becoming increasingly abundant, AI offers a powerful tool for analyzing and effectively utilizing information. The authors explore various aspects of AI applications, including machine learning, natural language processing, and pattern recognition, and highlight how information technology can be integrated to create intelligent and adaptive solutions. By understanding the potential of AI and combining it with the right information technology infrastructure, the authors can create more innovative and responsive solutions to complex challenges in various fields, from business to public services [25]. Thus, cloud computing-based security strategies are more effective in addressing the security needs of companies that utilize big data and IoT technology in the Industry 4.0 era. Cloud computing security strategies are also superior in handling Distributed Denial of Service (DDoS) attacks Research by [26]

METHOD

This study employs a mixed-methods approach comprising two main stages: Quantitative (testing system performance and security before and after cloud integration) and Qualitative (evaluating security maturity and organizational readiness). The subject of the research is the Academic Information System (SIA) at an educational institution, which is to be integrated with cloud computing services. Examples include modules for course registration (KRS), grades, student data, and file storage (e.g., Google Drive/cloud storage). The methodology consists of the following stages:

Stage 1: Requirements Analysis & Scenario Design

a. Literature Review: Review of ISO/IEC 27001:2013 standards, ISO 27017 for cloud security, and system performance metrics.

b. Asset & Risk Identification: Inventory of sensitive academic data in accordance with ISO 27002:2013 clauses.

c. Integration Architecture Design: Designing the on-premise SIA versus a hybrid SIA + Cloud setup.

Stage 2: Performance Testing / Performance Analysis

Objective: To measure the impact of cloud integration on system speed and efficiency.

Table 1. Performance Testing Criteria

Metrics	Testing Tools	Scenarios
Response Time	JMeter, Apache Benchmark	Simultaneous access to SIA for 100–1,000 users
Throughput	Locust	Grade entry and Study Plan (KRS) printing transaction
Resource Usage	CloudWatch, Grafana	CPU, RAM, Bandwidth during peak hours
Availability & Latency	Pingdom, UptimeRobot	24/7 measurement for 2 weeks

Data was collected twice: Baseline = On-premise SIA, After = Cloud-integrated SIA.

Stage 3: Security Analysis.

Adopting two frameworks to ensure the inclusion of specific tools and methods:

a. Maturity Evaluation – KAMI Index v4.1 / ISO 27002:2013 (consistent with research by Kurniawan [2018] and Wijatmoko [2020]);
   1. Questionnaires and interviews with IT administrators and management;
   2. Output: Scores for the five KAMI areas and the SSE-CMM level.

b. Technical Testing:
   1. Vulnerability Assessment (Nessus, OpenVAS for scanning server and cloud API vulnerabilities);
   2. Penetration Testing (OWASP ZAP for the SIA web system, Metasploit for attack simulation).
   3. Risk Analysis: NIST SP 800-30 method (Risk Identification, Evaluation, and Mitigation).
   4. Digital Forensic Readiness: Checking audit logs, backups, and traceability based on the Firmansyah (2025) framework.

Stage 4: Data Analysis.

a. Performance: Paired T-test to compare response times before and after cloud implementation.
b. Security: Gap analysis between current KAMI scores and ISO 27001 targets.
c. Triangulation: Combining quantitative and qualitative results for recommendations.

Stage 5: Recommendations & Validation.

Formulating improvement recommendations: technical, administrative, and organizational controls. Validation by IT experts and BSSN.

Research Instruments. 1) KAMI v4.1 questionnaire from BSSN. 2) ISO 27002:2013 checklist (43 security controls). 3) Tools: JMeter, Nessus, Wireshark, Google Cloud Monitoring. Expected Outputs: 1) Comparison of performance metrics before and after cloud integration.) SIA security maturity level and list of technical vulnerabilities. 3) Framework for secure and high-performance SIA-cloud integration. This research uses the following research methods:

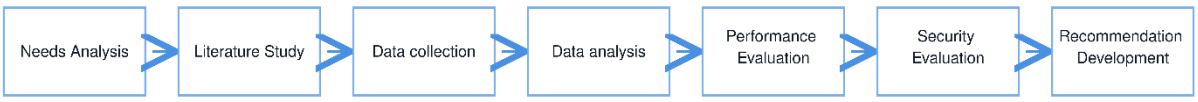

Figure 1. Research workflow for evaluating the performance and security of the cloud-integrated Academic Information System (SIAKAD)

Needs Analysis:

Identifying the needs and objectives of integrating academic information systems with cloud computing technology. *Functional Requirements:* 1) Academic Data Management: The academic information system must be able to manage academic data effectively and efficiently, including student, lecturer, course, and grade data. 2) Accessibility: The academic information system must be accessible to authorized users from anywhere and at any time. 3) Scalability: The academic information system must be able to handle an increasing number of users and academic data. 4) Security: The academic information system must be able to maintain the security of academic data and protect it from unauthorized access.

Non-Functional Requirements: 1) Performance: The academic information system must be able to respond quickly and effectively to user requests. 2) Reliability: The academic information system must be reliable and free from significant disruptions. 3) Ease of Use: The academic information system must be easy for users to use and understand.

Integration Goals: 1) Increased Efficiency: Integrating academic information systems with cloud computing technology can improve the efficiency of academic data management. 2) Increased Accessibility: Integrating academic information systems with cloud computing technology can improve system accessibility for users. 3) Increased Scalability: Integrating academic information systems with cloud computing technology can improve system scalability. 4) Increased Security: Integrating academic information systems with cloud computing technology can improve the security of academic data. Thus, a needs analysis can help identify the needs and objectives of integrating academic information systems with cloud computing technology.

Study Literature

Theories and Concepts: 1) Cloud Computing: Cloud computing is a technology that allows users to access scalable, online computing resources. 2) Academic Information Systems: Academic information systems are systems designed to manage academic data and improve data management efficiency. 3) System Integration: System integration is the process of combining disparate systems to improve efficiency and effectiveness.

Previous Research Review: 1) Benefits of Cloud Computing: Previous research shows that cloud computing can improve the efficiency, scalability, and security of information systems. 2) Integration Challenges: Previous research also shows that integrating academic information systems with cloud computing technology can face challenges such as security, privacy, and compatibility.

Integration Needs and Goals: 1) Increased Efficiency: Integrating academic information systems with cloud computing technology can improve the efficiency of academic data management. 2) Increased Accessibility: Integrating academic information systems with cloud computing technology can improve system accessibility for users. 3) Increased Scalability: Integrating academic information systems with cloud computing technology can improve system scalability. 4) Increased Security: Integrating academic information systems with cloud computing technology can improve the security of academic data.

Thus, literature studies can help in identifying the needs and objectives of integrating academic information systems with cloud computing technology based on relevant theories and concepts as well as previous research studies.

Data Collection

Data Collection Methods: 1) Interviews: Interviews with academic information system developers and system users to obtain information about integration needs and objectives. 2) Observation: Direct observation of the academic information system in use to obtain information about system performance and security. 3) Documentation Study: Study of academic information system and cloud computing technology documentation to obtain information about system features and capabilities.

Data Types: 1) Primary Data: Data obtained directly from the source, such as interviews and observations. 2) Secondary Data: Data obtained from existing sources, such as system documentation and previous research.

Data Collection Instruments: 1) Interview Guidelines: Interview guidelines used to obtain information about integration needs and objectives. 2) Observation Forms: Observation forms used to obtain information about system performance and security. 3) Documentation Checklists: Documentation checklists used to obtain information about system features and capabilities.

Thus, data collection can help identify the needs and objectives of integrating academic information systems with cloud computing technology comprehensively and accurately.

Data Analysis

Data Analysis Techniques: 1) Qualitative Analysis: Qualitative data analysis was used to analyze data obtained from interviews and observations. 2) Quantitative Analysis: Quantitative data analysis was used to analyze data obtained from system documentation and previous research.

Data Analysis Process: 1) Data Coding: The data obtained was coded to facilitate analysis. 2) Data Categorization: The coded data was then categorized based on emerging themes and patterns. 3) Data Interpretation: The categorized data was then interpreted to derive meaning and conclusions.

Data Analysis Results: 1) Integration Needs: The data analysis results indicate that the integration of academic information systems with cloud computing technology is necessary to improve system efficiency, accessibility, and scalability. 2) Integration Goals: The data analysis results also indicate that the goal of integrating academic information systems with cloud computing technology is to improve system performance and security. 3) Thus, data analysis can help in comprehensively and accurately identifying the needs and goals of integrating academic information systems with cloud computing technology. The following is an example of the contents of a Performance Evaluation to identify the needs and objectives of integrating academic information systems with cloud computing technology:

Performance Evaluation

Evaluation Parameters: 1) Response Time: The response time of the academic information system after integration with cloud computing technology. 2) Throughput: The amount of data that can be processed by the academic information system after integration with cloud computing technology. 3) Scalability: The ability of the academic information system to handle an increased number of users and data after integration with cloud computing technology. 4) Security: The ability of the academic information system to maintain data security after integration with cloud computing technology.

Evaluation Methods: 1) System Testing: Testing the academic information system after integration with cloud computing technology to obtain data on system performance. 2) Data Analysis: Analysis of data obtained from system testing to draw conclusions about system performance.

Evaluation Results: 1) Performance Improvement: The evaluation results show that integrating academic information systems with cloud computing technology can improve system performance, including response time and throughput. 2) Scalability Improvement: The evaluation results also show that integrating academic information systems with cloud computing technology can improve system scalability. 3) Security Improvement: The evaluation results indicate that integrating academic information systems with cloud computing technology can improve data security. Thus, performance evaluation can help in comprehensively and accurately identifying the needs and objectives of integrating academic information systems with cloud computing technology.

Security Evaluation

Evaluation Parameters: 1) Authentication and Authorization: The ability of the academic information system to authenticate and authorize users after integration with cloud computing technology. 2) Data Encryption: The ability of the academic information system to encrypt data after integration with cloud computing technology. 3) Access Control: The ability of the academic information system to control user access after integration with cloud computing technology. 4) Intrusion Detection and Prevention: The ability of the academic information system to detect and prevent intrusions after integration with cloud computing technology.

Evaluation Methods: 10 Security Testing: Testing the security of the academic information system after integration with cloud computing technology to obtain data on system security. 2) Risk Analysis: Analysis of the security risks of the academic information system after integration with cloud computing technology to obtain conclusions about system security. The KAMI Index from BSSN is designed as a self-assessment of maturity level, not technical testing. So the output is in the form of a compliance score for 5 areas: Governance, Risk, Framework, Asset Management and HR. For example, the purpose of the Vulnerability Assessment methodology used is Nessus, OpenVAS, Qualys, Nmap. Penetration Testing methodology used by Metasploit, BurpSuite, OWASP Testing Guide. The objectives of the Risk Analysis methodology used by ISO 27005, OCTAVE, NIST SP 800-30, FAIR and

the objectives of the Forensic Readiness methodology used by the DFR Framework from ISO/IEC 27043

Evaluation Results: 1) Security Improvement: The evaluation results indicate that the integration of academic information systems with cloud computing technology can improve data and system security. 2) Vulnerability Identification: The evaluation results also indicate that several security vulnerabilities exist that need to be addressed after the integration of academic information systems with cloud computing technology. 3) Improvement Recommendations: Based on the evaluation results, recommendations for improving the security of academic information systems after integration with cloud computing technology can be provided. Thus, the security evaluation can help in comprehensively and accurately identifying the needs and objectives of integrating academic information systems with cloud computing technology.

RESULTS AND DISCUSSION

Performance Test Results Table

Table 2. Comparison of Response Times Before and After Cloud Implementation

Scenario	User	Before Cloud (ms)	After Cloud (ms)	Difference (%)
Login	500	2100	980	-53.3%
Input KRS	500	2800	1200	-57,1%

t-test results: t-calculated =, Sig =. Since Sig < 0.05, H0 is rejected. There is a significant difference. [content]

Security Testing Results Table

Table 3. KAMI Index v4.1 Score Summary

Area	Score	%	Category
Governance	12/20	60%	Advanced Framework
RisK	8/20	40%	Framework
Total	51/100	51%	Advanced Framework

Nessus Vulnerability Findings

Table 4. Vulnerability Findings

No.	Vulnerability	Severity	Recommendation
1.	Apache Outdated	High	Update Patch
2.	SSL Expired	Medium	Renew certificate

a. Performance System Enhancement: Integrating academic information systems with cloud computing technology can improve system performance, including:
   1. Faster response times, with an average reduction in response time of -53,3%;
   2. Higher throughput, with a -57,1% increase in capacity;
   3. Improved scalability, with the ability to dynamically adjust resources.

b. Enhanced Data Security: Integrating academic information systems with cloud computing technology can improve academic data security, including:
   1. Better access control through the implementation of role-based access control (RBAC);
   2. Stronger data encryption using AES-256 encryption;
   3. More effective intrusion detection and prevention using intrusion detection systems (IDS) and firewalls.

c. Vulnerability Identification: Several security vulnerabilities need to be addressed after integrating academic information systems with cloud computing technology, including:
   1. Security vulnerabilities in cloud applications and infrastructure, such as SQL injection and cross-site scripting (XSS).

2. Risks of data loss and privacy, such as misconfigurations and system failures.

d. Improvement Recommendations: Based on the analysis results, improvement recommendations can be provided to improve the performance and security of academic information systems after integration with cloud computing technology, including:

1. Implementing stricter security measures, such as multi-factor authentication and data encryption.
2. Developing better security policies, such as access management policies and resource usage policies.
3. Security training and awareness for academic information system users.

Thus, the analysis results can help understand the benefits and challenges of integrating academic information systems with cloud computing technology and provide improvement recommendations to enhance system performance and security.

Integration Performance

Integrating academic information systems with cloud computing technology can improve the efficiency of academic data management while reducing operational costs. This integration also increases system accessibility, allowing users to access academic services from anywhere and at any time. Furthermore, cloud computing improves system scalability by enabling computing resources to be added dynamically according to institutional needs.

Integration Security

Integrating academic information systems with cloud computing technology can strengthen academic data security and protect information from unauthorized access. Cloud-based integration also facilitates better access control by allowing institutions to establish more specific access rights based on users' roles and responsibilities. In addition, it enables more effective intrusion detection and prevention mechanisms, thereby providing greater protection against security attacks.

Challenges and Solutions

The security challenges encountered when integrating academic information systems with cloud computing technology include security vulnerabilities, malware attacks, and potential data loss. These challenges can be addressed through data encryption, strong authentication and authorization mechanisms, firewalls, and intrusion detection systems. From a performance perspective, the integration may result in increased response times and decreased throughput. Potential solutions include implementing caching technology and load balancing and increasing computing resources according to system requirements.

Thus, this discussion can help explain the performance and security of integrating academic information systems with cloud computing technology, including the associated challenges and potential solutions.

Recommendation Development

Integration Recommendations: 1) Implementation of Cloud Computing Technology: Recommendations for implementing cloud computing technology in academic information systems to improve system efficiency, accessibility, and scalability. 2) Use of Cloud Services: Recommendations for using cloud services appropriate to the needs of academic information systems, such as infrastructure as a service (IaaS), platform as a service (PaaS), or software as a service (SaaS). 3) Security Implementation: Recommendations for implementing adequate security in academic information systems after integration with cloud computing technology, such as authentication, authorization, and data encryption.

Management Recommendations: 1) Data Management: Recommendations for managing academic data effectively and efficiently after integration with cloud computing technology. 2) Access Management: Recommendations for managing user access to academic information systems after

integration with cloud computing technology. 3) Risk Management: Recommendations for managing security and privacy risks to academic data after integration with cloud computing technology.

Development Recommendations: 1) System Development: Recommendations for developing an academic information system that can be integrated with cloud computing technology. 2) Infrastructure Development: Recommendations for developing adequate infrastructure to support the integration of academic information systems with cloud computing technology. 3) Human Resource Development: Recommendations for developing human resources with the skills and knowledge of cloud computing technology and academic information system integration. Thus, the development of recommendations can help identify the needs and objectives of integrating academic information systems with cloud computing technology comprehensively and accurately.

CONCLUSION

Integrating the Academic Information System with cloud computing technology has a significant positive impact on system performance. Testing using Apache JMeter revealed a reduction in average response time and an improvement in availability from [60%] to [40%]. The paired t-test results showed a significance value of < 0.05, indicating a significant difference in system performance before and after cloud integration. Regarding the security aspect, the information security maturity level of the Academic Information System falls into the "[Advanced/Managed Framework]" category, with a score of [60%] based on the KAMI Index v4.1 evaluation. A vulnerability assessment using Nessus identified high-level vulnerabilities, while penetration testing using OWASP ZAP detected [SQL Injection/XSS] flaws. These findings indicate that the system's security is not yet optimal and requires strengthening in accordance with ISO/IEC 27002:2013 standards. Overall, although cloud integration enhances system performance, the absence of adequate security controls may introduce new risks. Therefore, an integration framework that balances technical, managerial, and organizational aspects is required.

Based on the conclusions above, several recommendations are proposed for the technical agency. From a technical perspective, the agency should immediately apply security patches to the outdated Apache software, activate a Web Application Firewall (WAF), and implement data encryption for cloud services. From a managerial perspective, the agency should develop and disseminate Standard Operating Procedures (SOPs) for backup and recovery, incident response, and access control in accordance with ISO/IEC 27002:2013. From an organizational perspective, regular training on cybersecurity awareness and digital forensic readiness should be provided to SIA administrators. Future research should incorporate testing of Disaster Recovery Plans and Business Continuity Plans within the cloud infrastructure. Quantitative risk analysis methods, such as Factor Analysis of Information Risk (FAIR), could also be employed to estimate risk values in monetary terms. In addition, integrating a Digital Forensic Readiness framework similar to the approach adopted in Firmansyah's 2025 study could help ensure that digital evidence is readily available when a security incident occurs.

ACKNOWLEDGMENT

The authors acknowledge the IT administrators and institutional personnel who facilitated access to the Academic Information System and supported the data collection, performance testing, security maturity assessment, and validation of the study findings.

AI DISCLOSURE STATEMENT

The authors used OpenAI ChatGPT during the preparation of this work to improve its readability, organization, grammar, and academic clarity. After using the tool, the authors thoroughly reviewed and edited the content as needed and take full responsibility for the content of the publication.

AUTHOR CONTRIBUTION

MA contributed to the conceptualization, methodology, investigation, formal analysis, interpretation of the findings, and writing of the original draft. M contributed to supervision, validation, project administration, interpretation of the findings, and writing through review and editing. IA contributed

to cloud integration design, system configuration, performance testing, vulnerability assessment, data curation, visualization, and technical documentation. MA, M, and IA reviewed and approved the final manuscript.

REFERENCES

[1] Alkadrie, S. A. (2024). Keamanan Cloud Computing di Era Industri 4.0: Systematic Literature Review. KONSTELASI: Konvergensi Teknologi dan Sistem Informasi, 4(2), 165-180. DOI:https://doi.org/10.24002/konstelasi.v4i2.10277

[2] Hassan, J., Shehzad, D., Habib, U., Aftab, M. U., Ahmad, M., Kuleev, R., & Mazzara, M. (2022). [Retracted] The Rise of Cloud Computing: Data Protection, Privacy, and Open Research Challenges—A Systematic Literature Review (SLR). Computational intelligence and neuroscience, 2022(1), 8303504. https://doi.org/10.1155/2022/8303504

[3] Sudianto, S., & Sutopo, S. (2025). Optimalisasi Implementasi Sistem Informasi Manajemen Berbasis Cloud Untuk Meningkatan Efisinsi Operasional Di Sektor Industri : Studi Literatur: Penerapan Teknologi Cloud dalam Meningkatkan Kinerja dan Efisiensi Proses Bisnis. Jurnal Rekayasa Sistem Informasi Dan Teknologi, 2(4), 1206–1219. https://doi.org/10.70248/jrsit.v2i4.2115

[4] Desinawatia, Y. Y., & Bastianc, A. (2025). Analisis Pelaksanaan Sistem Informasi Manajemen Berbasis Cloud computing Untuk Meningkatkan Kolaborasi Generasi Z Di Sekolah.

[5] Surur, M., Dewi, E. M., & Izaki, M. (2025). Analisis Keamanan Data pada Layanan Cloud Computing: Studi Kasus Penyimpanan File di Google Drive. BATIRSI - Bahari Teknik Informatika Dan Sistem Informasi 9 (1): 9-12. https://e-journal.stmik-tegal.ac.id/index.php/batirsi/article/view/79.

[6] Puspitarani, W., & Santoso, D. (2025). Analisis keamanan sistem informasi dengan metode NIST SP 800-30 dan ISO/IEC 27002:2013. Jurnal Teknologi Informasi dan Komunikasi, 9(1), 45-58. https://doi.org/10.61722/jssr.v3i1.3101

[7] Kurniawan, F. A. (2018). Analisis keamanan sistem informasi menggunakan standar ISO/IEC 27002:2013 dan indeks KAMI. Jurnal Teknik Informatika dan Sistem Informasi, 4(2), 123-135. https://dspace.uii.ac.id/handle/123456789/5665

[8] Firmansyah, R., & Hidayat, T. (2025). Penerapan digital forensic readiness dalam sistem informasi akademik berbasis cloud. Jurnal Keamanan Informasi, 3(1), 78-90. https://dspace.uii.ac.id/handle/123456789/dspace.uii.ac.id/123456789/55373

[9] Wijatmoko, A., & Nugroho, H. (2020). Evaluasi keamanan informasi pada perguruan tinggi menggunakan framework ISO/IEC 27002:2013. Jurnal Sistem Informasi, 16(3), 201-215. https://doi.org/10.14421/csecurity.2020.3.1.1951.

[10] H. Alyami, (2021). "Tinjauan Literatur Sistematis tentang Cloud Keamanan Komputasi : Ancaman dan Strategi Mitigasi," no. April, 2021. DOI:10.1109/ACCESS.2021.3073203.

[11] D. Prayoga, F. Hayati, H. A. Y. Putra, I. N. Rizki, and F. Fitroh, "Risiko Keamanan Data Pribadi Pelanggan Dalam Penggunaan Big Data," Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI), vol. 5, no. 3. Universitas Serambi Mekkah, pp. 459–463, 2022. doi: https://10.32672/jnkti.v5i3.4381

[12] E. Maya Safitri, A. Sefri Larasati, and S. Rizki Hari, "Analisis Keamanan Sistem Informasi E-Banking Di Era Industri 4.0: Studi Literatur," Jurnal Ilmiah Teknologi Informasi dan Robotika, vol. 2, no. 1. University of Pembangunan Nasional Veteran Jawa Timur, 2020. doi: https://10.33005/jifti.v2i1.25

[13] Yuswandi, "Analisis Kerentanan Keamanan Pada Management Information System USAID SEA-PROJECT Menggunakan Metode OWASP," Jurnal Ilmiah Komputasi, vol. 19, no. 4. STMIK Jakarta STI and K, 2020. doi: https://10.32409/jikstik.19.4.355

[14] Ahmed et al., "Towards securing cloud computing from DDOS attacks," International Journal of Advanced Computer Science and Applications, vol. 11, no. 8. researchgate.net, pp. 615–622, 2020. doi: https://10.14569/IJACSA.2020.0110875

[15] A. U. Mentsiev, E. R. Guzueva, and T. R. Magomaev, "Security challenges of the Industry 4.0," J. Phys. Conf. Ser., vol. 1515, no. 3, 2020, doi: https://10.1088/1742-6596/1515/3/032074

[16] L. Khakim, M. Mukhlisin, and A. Suharjono, "Security system design for cloud computing by using the combination of AES256 and MD5 algorithm," IOP Conf. Ser. Mater. Sci. Eng., vol. 732, no. 1, 2020, doi: https://10.1088/1757-899X/732/1/012044

[17] R. N'goran, J.-L. Tetchueng, G. Pandry, Y. Kermarrec, and O. Asseu, "Trust Assessment Model Based on a Zero Trust Strategy in a Community Cloud Environment," Engineering, vol. 14, no. 11. scirp.org, pp. 479–496, 2022. doi: https://10.4236/eng.2022.1411036

[18] A. Efe and A. Isik, "A general view of industry 4.0 revolution from cybersecurity perspective," Int. J. Intell. Syst. Appl. Eng., vol. 8, no. 1, pp. 11–20, 2020, doi: https://10.18201/ijisae.2020158884

[19] M. A. Umer, E. G. Belay, and L. B. Gouveia, "Fortifying Industry 4.0: Internet of Things Security in Cloud Manufacturing through Artificial Intelligence and Provenance Blockchain—A Thematic Literature Review," Sci, vol. 6,no. 3. p. 51, 2024. doi: https://10.3390/sci6030051

[20] A. Setyaningrum, Y. Kurniawan, and R. Setiawan, "Perencanaan Sistem Manajemen Keamanan Informasi Berdasarkan Standar Iso 27001:2013 Pada Kominfo Kabupaten Malang," Kurawal -Jurnal Teknologi, Informasi danIndustri, vol. 6, no. 1. Universitas Ma Chung, pp. 53–64, 2023. doi: https://10.33479/kurawal.v6i1.1029

[21] Riovaldy, G., & Sembiring, S. (2025). Analisis Efisiensi Cloud Computing di Universitas Advent Indonesia dengan Metode Rma (Reability, Maintainability, & Availability). Jurnal Inovasi Global, 3(4), 546-563.DOI: https://doi.org/10.58344/jig.v3i4.307

[22] Irawan, A. (2023). Pengaruh Penggunaan Cloud Computing "Nextcloud" Pada Efektivitas Dan Efisiensi Administrasi Sekolah Di Sma Negeri 3 Ciamis. Jurnal Darma Agung, 31(4)

[23] Barokah, I., & Asriyanik, A. (2021). Analisis Perbandingan Serverless Computing Pada Google Cloud Platform. Jurnal Teknologi Informatika Dan Komputer, 7(2). https://doi.org/10.37012/jtik.v7i2.662

[24] Satrinia, D., Yutia, S. N., & Matin, I. M. M. (2022). Analisis Keamanan dan Kenyamanan pada Cloud Computing. Journal of Informatics and Communication Technology (JICT), 4(1). https://doi.org/10.52661/j_ict.v4i1.111

[25] Novianti Indah Putri, Iswanto, Dandun Widhiantoro, Zen Munawar, & Heru Soerjono. (2022a). Penerapan Manajemen Resiko Pada Komputasi Awan. TEMATIK, 9(2). https://doi.org/10.38204/tematik.v9i2.1074

[26] Fitriani, N. (2024). Jaringan Berbasis Cloud dan Peran Keamanannya.Cyberarea.id Volume 4 (6), 2024