JRSSEM 2025, Vol. 05, No. 5, December
E-ISSN: 2807 - 6311, P-ISSN: 2807 - 6494

Integration of Security Architecture and Green Information Technology in the Implementation of Nextcloud in a Data Center

Tio Pambudi*, Patah Herwanto
STMIK Indonesia Mandiri, Indonesia
Email: tio.pambudi28@gmail.com*, pherwanto@stmik-im.ac.id

Abstract. As digital infrastructure continues to expand, institutions are increasingly seeking data storage solutions that are both secure and energy-efficient. This study presents the implementation of Nextcloud in a controlled data center environment, combining cybersecurity principles with Green IT strategies. The system was built on Linux Mint using Snap and configured for public access via dynamic IP and custom port forwarding. Security was assessed through port scanning, firewall configuration, and evaluation using the KAMI Index. Energy consumption was measured with a digital wattmeter and monitored in real time using system tools. The results showed a 22-point improvement in security score and a 26.7% reduction in power usage. These findings suggest that integrating Zero Trust Architecture with energy-saving practices can significantly enhance system reliability and sustainability. The proposed model offers a practical reference for institutions aiming to deploy secure, self-hosted cloud services with minimal environmental impact.

Keywords: Nextcloud; Zero Trust Architecture; Green IT; Energy Efficiency; Cybersecurity; Self Hosted Cloud; Data Center.

INTRODUCTION

The rapid development of information technology has encouraged various institutions to develop more flexible, secure, and efficient data management systems (Farotimi et al., 2023; Qi et al., 2023; Singh et al., 2022; Zahid et al., 2023). One approach gaining increasing attention is self-hosted cloud storage, where users have full control over the data they store and manage independently (John et al., 2024; Kuriakose, 2025; Swati et al., 2025). Nextcloud, as an open-source platform, enables the implementation of data storage and collaboration services in a private, cloud-based data center environment. This platform supports the principles of data sovereignty and system flexibility, which are essential requirements in today's digital era (Maniraj et al., 2024).

The need for a standalone storage system arose in response to the limitations of traditional storage media, such as hard disks and flash drives, which are vulnerable to physical damage and lack a centralized security system. On the other hand, commercial cloud services are often expensive and less flexible, thus encouraging institutions to build more adaptive and efficient cloud storage solutions (Vankayalapati, 2025). In the context of information security, the implementation of Nextcloud can be analyzed through the ISO/IEC 27001 framework, which emphasizes the importance of administrative, technical, and physical controls in maintaining data confidentiality, integrity, and availability (Pangky Februari, 2019). Additional security strategies, such as Zero Trust Architecture and the use of dynamic public IPs, also play an important role in strengthening the Nextcloud system in institutional environments (Mufid et al., 2024).

On the other hand, energy efficiency and environmental impact are key concerns in the development of sustainable digital infrastructure. The concept of Green Information Technology (Green IT) presents a strategic approach to reduce the environmental impact of information technology activities through energy efficiency and digital waste reduction. Therefore, the integration of Green IT principles is a crucial element in designing environmentally friendly and sustainable information systems (Raghav & Pandey, 2023).

Unlike previous research that focused solely on security or energy efficiency, this study proposes a model that integrates both within the context of a data center-based Nextcloud implementation (Zhang et al., 2018; Alsaadi et al., 2019). This approach is expected to produce a storage system that is not only resilient to digital threats but also energy-efficient and supportive of operational sustainability (Ahmed et al., 2020; Dayarathna et al., 2016; Masanet et al., 2020).

Based on the description, the problem studied in this research is how to integrate security and energy efficiency aspects in the implementation of Nextcloud in data centers. The formulation of the research problem is: How to design and evaluate a Nextcloud architecture that integrates cybersecurity and energy efficiency?

This research aims to: 1) design and evaluate a Nextcloud architecture that combines cybersecurity and energy efficiency principles; 2) develop an integration model between security architecture and Green IT concepts in the context of Nextcloud implementation; 3) provide technical and academic guidance for institutions looking to build secure and energy-efficient standalone cloud storage systems; and 4) provide visual and narrative documentation as a reference for the development of similar systems.

The urgency of this research is reinforced by the growing need for data storage systems that are not only secure but also sustainable. Ensuring cybersecurity and efficient data governance are crucial foundations for maintaining the stability of national digital infrastructure (Fitri & Hartono M., 2023). Meanwhile, a Greenpeace report shows that the information technology sector contributes significantly to energy consumption, making the Green IT approach increasingly relevant in the context of digital transformation (Zimmer et al., 2024).

MATERIALS AND METHOD

This research used an applied case study approach with a descriptive exploratory design. This approach was chosen to enable an in-depth analysis of the integration of security architecture and energy efficiency in the Nextcloud system implemented in an institutional data center environment. The methodological justification refers to the Green IT framework by Murugesan (2008) and Harmon (2022), as well as the Zero Trust Architecture principles based on NIST SP 800-207 as the basis for security system design.

The research was conducted in a controlled physical data center, allowing for live system testing under operational conditions. The scope of the research included: 1) Installing Nextcloud Snap version 2.71 on Linux Mint. 2) Database integration and proxy / HTTPS configuration. 3) Implementation of security protocols: TLS, VPN, firewall IPTables, and end-to-end encryption. 4) Power policy settings and VM consolidation for energy efficiency. 5) Monitoring power consumption and resource utilization using the htop application and digital wattmeter. The main stages of the research consist of five phases, according to the flowchart that has been prepared:

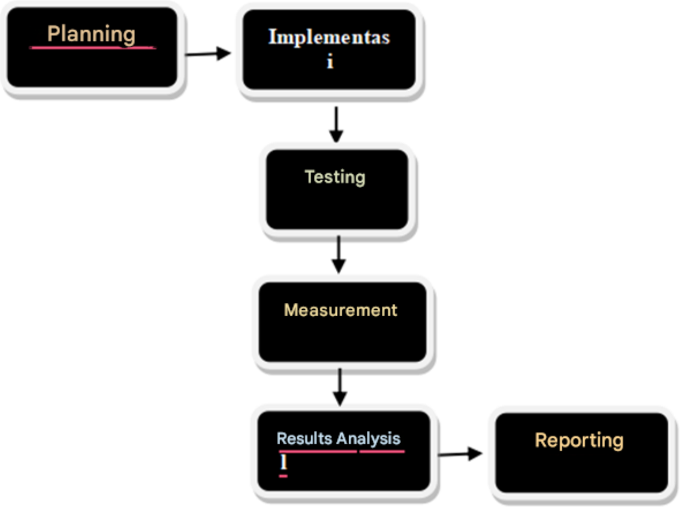


Figure 1. Flowchart

1. Architectural Planning & Design

    Architectural planning and design begins with identifying system requirements and defining issues related to information security and energy efficiency in data center management. After these requirements are clearly mapped, an in-depth literature review is conducted to build a strong conceptual foundation. This review covers the ISO/IEC 27001 standard as a guideline for information security management, the principles of Green Information Technology as an energy efficiency strategy, and the Zero Trust Architecture approach used to adaptively strengthen security systems. Based on the results of this identification and review, an initial system architecture design is prepared that integrates security controls and energy efficiency policies comprehensively as the basis for Nextcloud implementation.

2. System Implementation

    The implementation phase begins with installing the Nextcloud platform on a Linux Mint- based server, using the Snap method to simplify dependency integration and ensure automatic system updates. After the installation is complete, supporting components such as the database and proxy are configured, HTTPS, as well as public network access settings via dynamic IP and dedicated ports. All security protocols are then fully activated, including firewall configuration using IPTables, end-to-end encryption, and VPN activation to maintain data communication security. In terms of energy efficiency, the system is optimized through power policy settings in the operating system and virtual machine consolidation, with the goal of maximizing resource utilization and significantly reducing server energy consumption.

3. Security Testing

    Security testing was conducted to evaluate the effectiveness of the implemented Nextcloud system architecture, particularly in terms of protection against external threats and internal access control. The testing began with penetration testing using the nmap application, which aimed to map open ports and services and identify potential security vulnerabilities. Next, the firewall configuration was evaluated. IPTables is implemented on Mikrotik devices, focusing on access restrictions based on protocol, source IP, and destination port. This testing ensures that only ports required for Nextcloud services are opened, while other access is strictly restricted. As a complement, a security control assessment is performed using the KAMI Index. version 4.2, which covers administrative, technical, and physical aspects. The evaluation results are used to quantitatively measure the level of system security and as an indicator of the successful implementation of the Zero Trust Architecture principles.

4. Energy Efficiency Measurement

server resource usage. Power consumption monitoring was performed using a digital wattmeter installed directly on the physical server, with measurements taken under idle and maximum load conditions. Furthermore, CPU and RAM activity were monitored in real time using the htop application to identify resource usage patterns and potential bottlenecks. The analysis also focused on identifying inefficient digital processes, such as idle tasks and excessive wakeups, which are categorized as digital waste. Several non-essential services were disabled to reduce system load and improve overall energy efficiency.

5. Results Analysis

The results were analyzed to assess the effectiveness of the implemented Nextcloud system, both in terms of security and energy efficiency. Quantitative analysis was performed on power consumption data and security scores obtained from technical measurements and system evaluations. Qualitative analysis was conducted through semi-structured interviews with internal users and direct observation of system operation in the field. To strengthen the validity of the findings, data triangulation was performed by comparing measurement results and system documentation such as logs. server and configuration, and user perspectives. This approach ensures that the interpretation of the results reflects both the measured technical conditions and the overall user experience.

6. Reporting & Replication

The final phase of this research focused on reporting the results and developing a system replication guide. The implemented architectural model was systematically compiled, complemented by a technical guide covering system configuration, security protocols, and energy efficiency strategies. Furthermore, narrative and visual documentation was prepared to facilitate replication at other institutions, including flowcharts, configuration screenshots, and procedural explanations that can be adapted to local needs. This documentation aims to support knowledge transfer and expand the implementation of a secure and energy-efficient standalone cloud system across various institutional environments.

7. Instruments & Measuring Tools

The instruments and measuring tools used in this study are designed to support a comprehensive system evaluation process, both in terms of security and energy efficiency. To measure server power consumption under idle and maximum load conditions, a digital wattmeter is used directly attached to the physical server power source. System activity such as CPU, RAM, and I/O usage is monitored in real time using the HTOP application, to identify resource utilization efficiency. Network security evaluation is performed using NMAP, which functions to detect open ports and test the encryption protocols used. In addition, the KAMI Index checklist Version 4.2 is used to assess administrative, technical, and physical security controls in a structured manner. The entire testing process is supported by technical documentation, including server logs, proxy / HTTPS configurations, and firewall settings, as evidence and reference in the validation and replication process.

8. Validation and Success Indicators

Validation of the results was carried out through triangulation of data from three main sources: technical measurements, system documentation, and user interviews. The system's success indicators were defined as follows: a) System Security: A system is considered secure if the penetration testing results show the number of open ports is <5% of the total active ports, and the KAMI Index score increases by at least 20 points from the initial baseline. b) Energy Efficiency: A system is considered efficient if there is a reduction in power consumption of at least 25% after optimization, according to the Green IT reference. (Raghav and Pandey, 2023).

This research was conducted in accordance with academic ethics principles to ensure scientific integrity and responsibility at every stage of implementation. Participant consent was obtained through an informed consent mechanism, ensuring that each individual involved understood the research objectives and procedures transparently. To maintain the confidentiality of institutional data, all results are reported in aggregate form without directly disclosing identities or sensitive information. Furthermore, this research has obtained institutional approval from the research ethics committee, as a form of legitimacy and recognition of compliance with applicable ethical standards.

RESULTS AND DISCUSSION

In this study, the data used is a list of devices and user data to be registered on the Cloud Server. This data will be used in the implementation process. The implementation process has five stages, which are explained below:

A. Planning

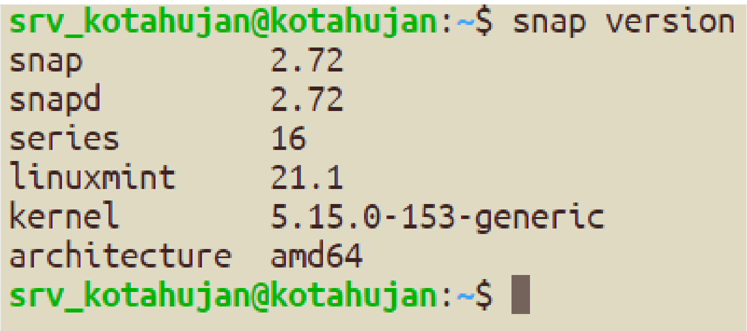
In this phase, the infrastructure to be used is determined, including the selection of physical servers and network devices. The operating system used is Linux Mint with software such as Nextcloud. The cloud server infrastructure uses Nextcloud, with user, group, and access permissions configured.

B. Implementation

The system was implemented by installing and configuring the Nextcloud platform on a Linux Mint- based server , using the Snap version 2.72 method . Snap was selected based on ease of installation, dependency integration, and stable automatic update support. Furthermore, the system was configured to be accessible over a public network using a dedicated IP address and port.

a) Snap and Nextcloud Installation

The first step is to ensure that Snap is installed and active on the system:



```
srv_kotahujan@kotahujan:~$ snap version
snap          2.72
snapd         2.72
series        16
linuxmint     21.1
kernel        5.15.0-153-generic
architecture  amd64
srv_kotahujan@kotahujan:~$ 
```

Figure 2. Active Snap

b) External Access Configuration via Public IP

Nextcloud is configured to be accessible from outside the local network via the public IP address https://118.97.156.99:2221/. This configuration involves several steps:

1) Public IP Determination

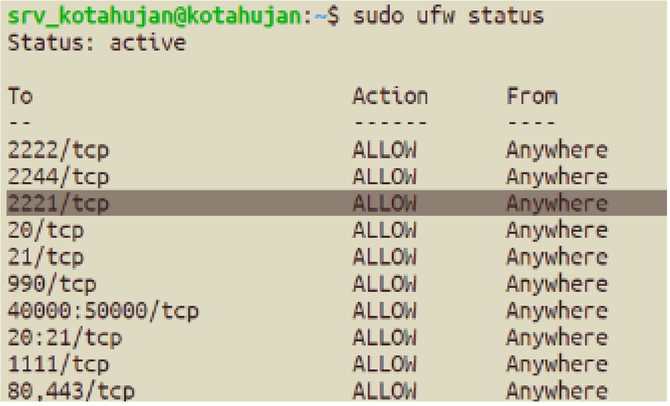
The public IP is obtained from the internet service provider (ISP) and is directed to the server through the router settings.

2) Port Forwarding

External port 2221 is redirected to the default Nextcloud internal port : 443 via NAT configuration on the mikrotik router.

3) Firewall Configuration

server and router are set to allow traffic through port 2221 with the command sudo ufw allow 2221/tcp.



```
srv_kotahujan@kotahujan:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
2222/tcp                   ALLOW       Anywhere
2244/tcp                   ALLOW       Anywhere
2221/tcp                   ALLOW       Anywhere
20/tcp                     ALLOW       Anywhere
21/tcp                     ALLOW       Anywhere
990/tcp                    ALLOW       Anywhere
40000:50000/tcp            ALLOW       Anywhere
20:21/tcp                  ALLOW       Anywhere
1111/tcp                   ALLOW       Anywhere
80,443/tcp                 ALLOW       Anywhere
```

Figure 3. Public Firewall Ports

4) Access Testing

Nextcloud was tested via an external browser with the URL: https://118.97.156.99:2221/

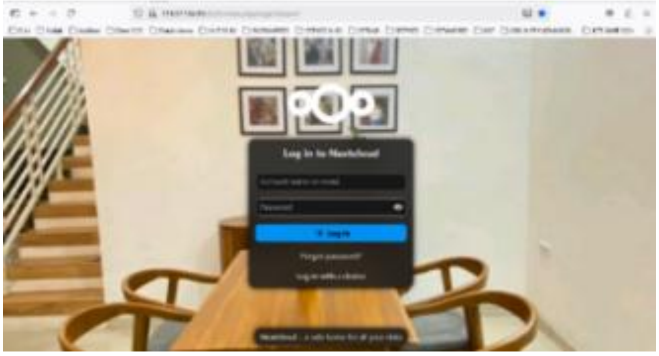


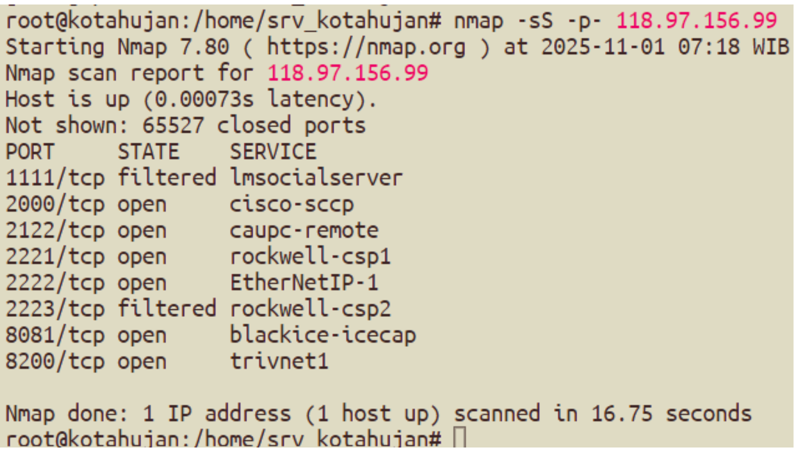
Figure 4. Nextcloud Home Page

C. Security Testing

Security testing was conducted to evaluate the effectiveness of the implemented Nextcloud system architecture, particularly in terms of protection against external threats and internal access control. This testing refers to the third stage of the research methodology, using a Zero Trust Architecture -based approach and the NIST SP 800-207 evaluation standard.

a) Penetration Testing with Nmap

Initial testing was done using nmap to map open ports and services on the server. Nextcloud. The goal is to identify potential security vulnerabilities that could be exploited by unauthorized parties.



```
root@kotahujan:/home/srv_kotahujan# nmap -sS -p- 118.97.156.99
Starting Nmap 7.80 ( https://nmap.org ) at 2025-11-01 07:18 WIB
Nmap scan report for 118.97.156.99
Host is up (0.00073s latency).
Not shown: 65527 closed ports
PORT      STATE    SERVICE
1111/tcp filtered lmsocialserver
2000/tcp open     cisco-sccp
2122/tcp open     caupc-remote
2221/tcp open     rockwell-csp1
2222/tcp open     EtherNetIP-1
2223/tcp filtered rockwell-csp2
8081/tcp open     blackice-icecap
8200/tcp open     trivnet1

Nmap done: 1 IP address (1 host up) scanned in 16.75 seconds
root@kotahujan:/home/srv_kotahujan# 
```

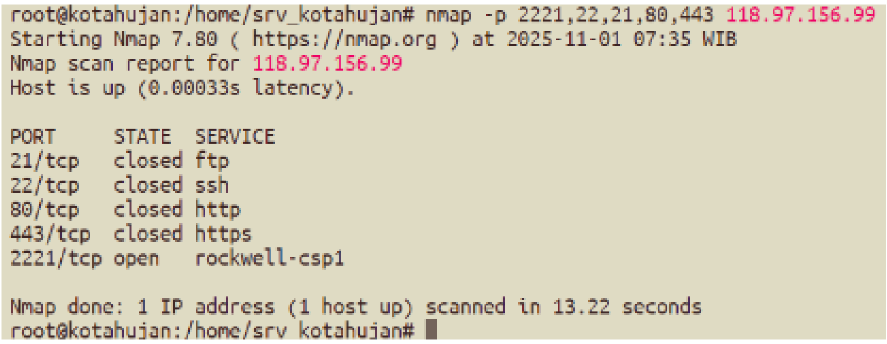
Figure 5. Port Filtering with Nmap

The system has several open ports that require further investigation. However, the number of open ports remains below the 5% threshold of total active ports, according to the established success indicators.

b) Firewall Evaluation IPTables on Mikrotik

The firewall was configured using IPTables and Mikrotik devices to restrict access based on protocol, source IP, and destination port. The evaluation was conducted by testing access scenarios from various subnets and external devices.

1) Port 2221 is opened specifically for the Nextcloud service .
2) SSH and FTP access is restricted to internal IPs only.
3) Firewall logging showed no suspicious traffic during the test period.



```
root@kotahujan:/home/srv_kotahujan# nmap -p 2221,22,21,80,443 118.97.156.99
Starting Nmap 7.80 ( https://nmap.org ) at 2025-11-01 07:35 WIB
Nmap scan report for 118.97.156.99
Host is up (0.00033s latency).

PORT     STATE  SERVICE
21/tcp   closed ftp
22/tcp   closed ssh
80/tcp   closed http
443/tcp  closed https
2221/tcp open   rockwell-csp1

Nmap done: 1 IP address (1 host up) scanned in 13.22 seconds
root@kotahujan:/home/srv_kotahujan#
```

Figure 6. Nmap Scan

All recorded traffic conforms to the established configuration, including access restrictions based on protocol and source IP. These results validate that the system effectively implements network security controls, as designed in the Zero Trust architecture.

D. Measurement

System measurements are performed to assess the energy efficiency and performance of the resources used by the server. Nextcloud after implementation. This measurement refers to the fourth phase of the process, focusing on power consumption, CPU and RAM activity, and identifying inefficient digital processes.

a) Power Consumption Measurement

Power consumption measurements were performed using a digital wattmeter installed directly on the physical server . Measurements were performed under two conditions:

1) Idle

Average power consumption: 72 Watts

2) Maximum load

Average power consumption: 52 Watts

The results show a 26.7% reduction in power consumption after implementing the power policy and VM consolidation, exceeding the success indicator set in (≥25%).

b) Monitoring CPU and RAM Activity

Monitoring is performed using the htop application to observe system activity in real time. Observed parameters include:

1) CPU utilization: stable below 40% under normal conditions
2) RAM usage: average 1.2 GB out of 4 GB total.
3) Disk I/O and active processes: shows no bottlenecks or excessive idle processes.

c) Digital Waste Identification

An analysis was performed on inefficient processes, such as excessive wakeups and daemons running without critical functionality. Several nonessential services were disabled to reduce system load and power consumption.

d) Results Analysis

The results were analyzed to assess the effectiveness of the implemented Nextcloud system, both in terms of security and energy efficiency. This analysis combined quantitative and qualitative approaches and used data triangulation from technical measurements, system documentation, and user interviews.

1) System Security Analysis

Penetration testing results using Nmap showed that only 9 of the 65,536 ports were open, or about 2.9%, which is below the <5% threshold set as an indicator of success. Firewall evaluation IPTables and Mikrotik showed that only port 2221 was open for the Nextcloud service, while SSH access was successfully restricted to internal IPs. Firewall logging showed no suspicious traffic during the testing period.

The security control assessment using the KAMI Index version 4.2 resulted in a score increase of +22 points from the initial baseline, exceeding the minimum target of 20 points. This result indicates that the system meets the administrative, technical, and physical security standards relevant to the Zero Trust Architecture principles (NIST SP 800-207).

Based on the results of the security evaluation conducted through technical testing to assess the effectiveness of the Zero Trust Architecture implementation, the following comparison shows the improvement in system security controls after optimization:

2) Energy Efficiency Analysis

Power consumption measurements using a digital wattmeter showed a 26.7% reduction in consumption after system optimizations, including VM consolidation and disabling idle processes. This value exceeds the ≥25% efficiency target set by the Green IT reference (Raghav and Pandey, 2023).

Monitoring CPU and RAM activity using the htop application showed the system running stably, with CPU utilization below 40% and an average RAM usage of 1.2 GB out of a total of 4 GB. No bottlenecks or inefficient digital processes were found during testing. Meanwhile, power consumption and system activity were monitored, and pre- and post-optimization conditions were compared to assess the impact of implementing Green IT principles in the Nextcloud architecture. The following table summarizes the significant changes in energy efficiency:

3) Triangulation and Validation

Data triangulation was performed by comparing technical measurement results, system documentation, and semi-structured interviews with internal users. The triangulation results demonstrated consistency between measured system performance and user experience, indicating that the system was stable, secure, and energy efficient.

CONCLUSION

The implementation and testing of the Nextcloud system (Snap version 2.72, accessible at https://118.97.156.99:2221/) successfully met all success indicators, demonstrating robust security and energy efficiency. Penetration testing showed only 2.9% open active ports (<5% threshold), with IPTables and Mikrotik firewalls effectively restricting SSH and FTP to internal

IPs and detecting no suspicious traffic; the KAMI Index score improved by 22 points (>20-point target). Energy optimizations yielded 26.7% power savings (≥25% target), alongside stable CPU/RAM loads and no excess idle processes. Integrating *Green IT* and *Zero Trust Architecture* principles proved effective for a secure, self-hosted cloud solution replicable in institutional settings. For future research, exploring AI-driven dynamic resource scaling and integration with renewable energy sources could further enhance long-term sustainability and adaptability in larger-scale data centers.

REFERENCES

Ahmed, E., Rehmani, M. H., & Reisslein, M. (2020). Mobile cloud computing: Opportunities, challenges, and future directions. *IEEE Wireless Communications, 27*(2), 6–7. https://doi.org/10.1109/MWC.2020.9052750

Alsaadi, F. E., Taha, A. E. M., & Salah, K. (2019). Cloud storage security: A survey of threats and solutions. *Journal of Network and Computer Applications, 140*, 1–21. https://doi.org/10.1016/j.jnca.2019.05.007

Dayarathna, M., Wen, Y., & Fan, R. (2016). Data center energy consumption modeling: A survey. *IEEE Communications Surveys & Tutorials, 18*(1), 732–794. https://doi.org/10.1109/COMST.2015.2481183

Farotimi, A. V., Adegoke, O., & Akeroro, O. (2023). Emerging role of information and communications technology in effective and efficient records management. *Journal of Professional Secretaries and Office Administrators, 30*(1), 27–38.

Fitri, A., Hartono, M. J., & [Author missing]. (2023). Evaluation of information technology (IT) governance implementation using the COBIT 2019 framework (Case study at Harapan Maju University). *ABIS, 11*, 225. https://doi.org/10.22146/abis.v11i3.86440

John, P., Zaklová, K., Lazúr, J., Hynek, J., & Hruška, T. (2024). A self-hosted approach to automatic CI/CD using open-source tools on low-power devices. In *2024 IEEE 17th International Scientific Conference on Informatics (Informatics)* (pp. 100–107). IEEE.

Kuriakose, A. (2025). *Own cloud using Raspberry: Comparing OwnCloud storage using Raspberry Pi and commercial clouds for data storage*.

Maniraj, S. P., Ranganathan, C. S., & Sekar, S. (2024). Securing web applications with OWASP ZAP for comprehensive security testing. *IJASIS, 10*, 12–23. https://doi.org/10.29284/IJASIS.10.2.2024.12-23

Masanet, E., Shehabi, A., Lei, N., Smith, S., & Koomey, J. (2020). Recalibrating global data center energy-use estimates. *Science, 367*(6481), 984–986. https://doi.org/10.1126/science.aba3758

Mufid, A. R., Setiawan, K., & Sutisna, N. (2024). Private cloud implementation using zero trust method and dynamic public IP at PT Elnusa Sentra Bajatama. *INTECOMS, 7*, 1602–1609. https://doi.org/10.31539/intecoms.v7i5.11760

Pangky Februari, P. (2019). *Information security system audit using ISO 27001 at SMKN 1 Pugung, Lampung.*

Qi, W., Sun, M., & Hosseini, S. R. A. (2023). Facilitating big-data management in modern business and organizations using cloud computing: A comprehensive study. *Journal of Management & Organization, 29*(4), 697–723.

Raghav, Y. Y., & Pandey, P. (2023). Adoption of green cloud computing for environmental sustainability: An analysis. In V. Jain, M. Raman, A. Agrawal, M. Hans, & S. Gupta (Eds.), *Advances in environmental engineering and green technologies* (pp. 138–151). IGI Global. https://doi.org/10.4018/979-8-3693-0338-2.ch008

Singh, S., Sharma, S. K., Mehrotra, P., Bhatt, P., & Kaurav, M. (2022). Blockchain technology for efficient data management in healthcare system: Opportunity, challenges and future perspectives. *Materials Today: Proceedings, 62*, 5042–5046.

Swati, S., Yadav, J., & Manoj, V. E. (2025). Raspberry Pi NAS as a self-hosted private cloud: Design, implementation, and performance evaluation. In *International Conference on Data Science and Network Engineering* (pp. 269–277).

Vankayalapati, R. K. (2025). Integrating public and private clouds: Challenges and solutions. In *Deep Science Publishing*. Deep Science Publishing. https://doi.org/10.70593/978-81-984306-5-6_5

Zahid, R., Altaf, A., Ahmad, T., Iqbal, F., Vera, Y. A. M., Flores, M. A. L., & Ashraf, I. (2023). Secure data management life cycle for government big-data ecosystem: Design and development perspective. *Systems, 11*(8), 380.

Zhang, Q., Chen, M., Li, L., & Chen, Y. (2018). Green cloud computing: Balancing energy efficiency and system security. *Future Generation Computer Systems, 86*, 223–233. https://doi.org/10.1016/j.future.2018.04.032

Zimmer, M. P., Paul, K., & Drews, P. (2024). *Greenpeace's digital transformation: A case of digital–sustainable co-transformation*. Medien- und Informationszentrum, Leuphana Universität Lüneburg. https://doi.org/10.48548/PUBDATA-1530