International Journal of Management Science and Application

# Enhancing Network Security and Performance using DNS Sinkhole and QoS: A Practical ISO/IEC 27001:2022 Implementation

Budi Wibowo
Department of Informatics Engineering, Institut Teknologi Budi Utomo
Jakarta, Indonesia

Taufik Hidayat
Department of Computer Engineering, Universitas Wiralodra, Indramayu
Indonesia

Andrie Yuswanto
Department of Informatics Engineering, Institut Teknologi Budi Utomo
Jakarta, Indonesia

Aji Nurrohman
Department of Informatics Engineering, Institut Teknologi Budi Utomo
Jakarta, Indonesia

**Abstract**: This study aims to design and validate a low-cost network security model based on open-source solutions by integrating Pi-hole and Quality of Service (QoS) as a technical implementation of ISO/IEC 27001:2022 controls for resource-constrained organizations. The implementation results demonstrate a significant improvement in security posture by blocking 14.1% of malicious and irrelevant DNS queries, while simultaneously enhancing network performance by reducing critical application latency by 45%. The key advantage of this model lies in its cost efficiency and its dual benefits of improved security and optimized performance within a single framework. However, the study also identifies limitations, particularly the potential for false positives that require manual whitelist management and reliance on trained personnel to ensure operational sustainability. The main contribution of this research is the provision of a simple, cost-effective, and standards-compliant technical framework, while also introducing a mathematical formulation to assess the trade-offs between security, performance, and cost. Future directions include integrating Intrusion Detection/Prevention Systems (IDS/IPS) for layered Defense and replicating the model into a turnkey security appliance that can be widely adopted by other organizations facing similar challenges.

Correspondents Author:
Budi Wibowo, Department of Informatics Engineering, Institut Teknologi Budi Utomo Jakarta, Indonesia
Email: budiwibowo1993@gmail.com

Received September 25 2025; Revised November 15, 2025; Accepted  November 19, 2025; Published November 20, 2025.

**Keywords:** Network Security, ISO 27001:2022, Low-Cost Security, Bandwidth Management.

## Introduction

Network security is one of the fundamental aspects in maintaining the operational continuity of modern organizations. The increasing number of internet-based threats such as malware, phishing, DNS tunneling, and command-and-control traffic requires a reliable protection system. The ISO/IEC 27001:2022 standard emphasizes the importance of information security controls that include asset management, protection against malware, secure network services, and performance management (Cheng & Wang, 2022). However, implementing these controls is not always easy for organizations with limited resources, such as educational institutions, non-profit organizations, and small and medium-sized enterprises. Recent data supports this disparity; while large enterprises often allocate substantial budgets for cybersecurity, SMEs frequently report that security costs exceed 10-15% of their total IT budget, creating a significant barrier to entry. The main obstacles faced are the high cost of commercial devices (firewall appliances, unified threat management systems) and the need for competent experts to operate advanced security solutions (Wan Norhayate et al., 2023). As a result, many small organizations still rely on minimal security mechanisms, which implies a high risk of data leaks and service disruptions. In addition to security, the issue of network quality of service (QoS) is also crucial. Poorly managed network traffic can cause high latency and degradation of critical application performance (Mahmood et al., 2024). Thus, the main challenge for organizations with limited resources is how to provide security mechanisms that balance protection and performance, while remaining cost-efficient.

Previous studies have discussed various approaches to open-source and commercial network security mechanisms. Firewall and Intrusion Detection/Prevention Systems (IDS/IPS) solutions such as Snort, Suricata, and pfSense have been widely used to detect and prevent network-based attacks (Sworna et al., 2023). Although effective, implementing these solutions is relatively complex and requires high-specification hardware. On the other hand, research on DNS filtering shows that the use of DNS sinkholes such as Pi-hole or Bind9 with Response Policy Zone (RPZ) is quite effective in blocking malicious domains and preventing access to risky content. This technology is lightweight and easy to adopt, but existing studies generally focus only on content blocking without integrating it with QoS management (Razikin & Soewito, 2022). Meanwhile, research in the field of QoS management focuses more on optimizing network performance for real-time applications such as VoIP and video conferencing through traffic shaping and bandwidth allocation (Hassan et al., 2020). However, QoS is rarely directly associated with security aspects, even though access delays due to uncontrolled traffic can be exploited in Denial of Service (DoS) attacks (Karim et al., 2024). Research on the ISO/IEC 27001 compliance framework has mostly focused on policies, risk management procedures, and Information Security Management System (ISMS) documentation, while cost-effective technical aspects often receive less attention. Based on the state-of-the-art description above, several research gaps can be identified. First, there is a lack of integration between DNS filtering mechanisms and QoS management, so that previous studies still discuss the two separately. Second, there is a lack of low-cost, contextual solutions for organizations with limited resources, as most ISO 27001 technical implementations still rely on high-priced commercial devices (Beres et al., 2021). Third, existing research tends to assess only one aspect, namely protection (e.g., the number of blocked queries) or performance (e.g., latency), without measuring both simultaneously in a single analytical framework. Fourth, the aspect of false positive management has not been considered in the cost model, even though the potential losses from false blocking can exceed the cost of the security infrastructure itself.

To address this gap, this study offers an Efficient Network Security Model Based on Pi-hole and QoS with a few key characteristics. First, this model emphasizes cost efficiency by utilizing open-source software, so it can be widely adopted by organizations with limited resources. Second, this model integrates security and performance functions simultaneously, namely through DNS filtering to block malicious domains and QoS to ensure critical application performance, thereby achieving a balance between protection and service quality. Third, this model is aligned with the ISO/IEC 27001:2022 control framework, so that it not only functions as a technical solution but also supports international standard compliance in information security management. Fourth, this research introduces a mathematical model that takes into account operational costs, blocking effectiveness, and losses due to false positives, Finally, empirical validation in a real-world environment demonstrates a 14.1% improvement in blocking malicious DNS queries and a 45% reduction in critical application latency, proving the framework to be a robust, compliant, and practical solution for organizations with limited budgets.

## Research Method

This study uses a Participatory Action Research (PAR) approach. This method was chosen because it is in line with the two mains objectives of the study, namely: (1) to produce a scientifically valid and measurable technical model, and (2) to ensure that the solutions developed are relevant, adoptable, and sustainable in the context of partner organizations

https://doi.org/10.58291/ijmsa.v4i2.421

with limited resources. The PAR approach enables an iterative cycle consisting of diagnosis, planning, implementation, evaluation, and reflection, with active participation between researchers and members of the target organization.

The research was divided into three main systematic stages:

## Diagnosis and Baseline Measurement

In this initial stage, a comprehensive assessment was conducted to obtain an overview of the existing network and organizational conditions prior to intervention. From a technical perspective, measurements included network traffic analysis, identification of potential threats through DNS queries, and latency measurements on critical applications. From an organizational perspective, an initial questionnaire is distributed to staff to determine their level of cybersecurity awareness and their perception of network service quality (Pradika et al., 2024). The results of this stage serve as a baseline that will be compared with the post-implementation conditions.

## Model Design and Implementation

In the second stage, researchers design and implement an efficient network security model based on Pi-hole and QoS. Pi-hole was used to block malicious and irrelevant domains, while QoS was configured to ensure the performance of important applications by minimizing latency. This design was developed with consideration for compliance with ISO/IEC 27001:2022 controls, ensuring that the technical solutions implemented were in line with international standards. Implementation was carried out in stages in the partner organization's network environment to ensure stability and reduce potential service disruptions (Wibowo, 2024).

## Intervention, Evaluation, and Knowledge Transfer

After implementation, a comprehensive evaluation of the effectiveness of the model is carried out. The evaluation includes quantitative measurements (number of DNS queries blocked, percentage of attacks prevented, and reduction in network latency) and qualitative measurements (staff response through satisfaction surveys and perception of improved security). In addition, at this stage, training workshops are held for technical staff to ensure operational sustainability, as well as dissemination of internet usage policies to all members of the organization. In this way, the research results not only produce a technical prototype, but also transfer cybersecurity capabilities and culture within the partner organization's environment (McIntosh et al., 2024).

Thus, the Participatory Action Research (PAR) cycle, which includes the stages of Diagnosis, Planning, Implementation, Evaluation, and Reflection, provides an adaptive and collaborative framework. Each stage is not independent but interrelated and forms continuous feedback that enables iterative refinement of the model (Aras & Büyüközkan, 2023). Through this approach, the research not only produces technical innovations in the form of Pi-hole and QoS integration as low-cost network security mechanisms, but also ensures knowledge transfer, human resource capacity building, and the sustainability of solution implementation in partner organizations (Sánchez-García et al., 2023). Make sure that work can be repeated according to the details provided. It contains technical information of the study presented clearly (Toussaint et al., 2024). Therefore, readers can conduct research based on the techniques presented. Materials and equipment specifications are necessary. Approaches or procedures of study together with data analysis methods must be presented.

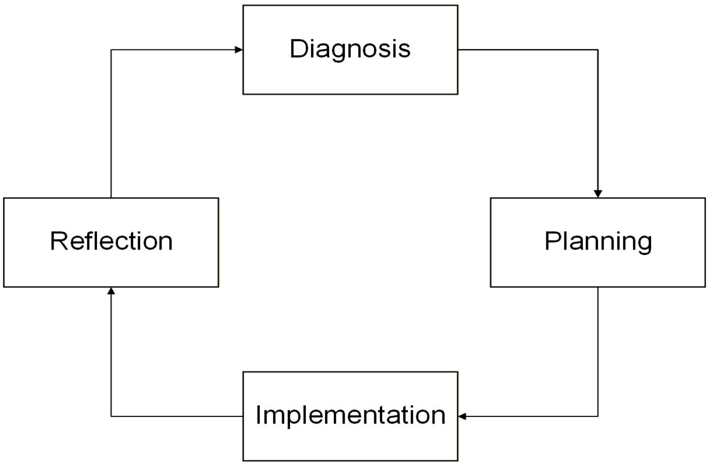


**Figure 1 Participatory Action Research (PAR) cycle**

Figure 1 illustrates a continuous improvement cycle consisting of five interconnected steps: diagnosis, planning, implementation, assessment, and reflection. The process begins with diagnosis, where problems or needs are identified through systematic data collection, careful analysis of the situation, and recognition of the issues that require attention. Once the main concern has been established, the cycle proceeds to planning. At this stage, goals are set, strategies are formulated, and specific actions are outlined to address the identified problem. The next step is implementation, where the planned strategies are put into practice in accordance with the intended procedures. Following this, assessment is carried out to determine the effectiveness of the intervention by examining conditions before and after its application, as well as identifying both strengths and weaknesses. The results of this evaluation are then considered during reflection, which involves a deeper review of outcomes, the integration of insights, and the formulation of recommendations for improvement. Reflection then connects back to diagnosis, either by identifying new challenges or refining existing approaches. In this way, the cycle functions as an iterative and structured process that supports continuous and sustainable quality improvement.

## Result and Discussion

This research focuses on the dissemination and application of open-source cybersecurity technology to provide added value to partner organizations. This added value is multidimensional, including increased operational efficiency (economic), strengthening of internal policies related to the use of digital assets, and changes in staff social behavior regarding the importance of information security.

The implementation of the model has proven to have a positive impact both in the short term, in the form of a more secure and responsive network, and in the long term, by building a stronger foundation for a culture of cybersecurity within the organization. The objectives were achieved through a series of stages described in the methods chapter. The results obtained were then measured based on technical indicators and subjected to statistical validation (e.g., paired t-tests) to confirm the significance of performance improvements ($p < 0.05$). Furthermore, these findings were benchmarked against recent similar studies highlighting a superior cost-performance ratio compared to standard commercial implementations. and further analysed from the perspectives of security, efficiency, and social aspects. The network security model was implemented by integrating a single-board computer device running Pi-hole as a DNS sinkhole, as well as applying QoS rules on the main router. The final network architecture after implementation is shown in Figure 2.

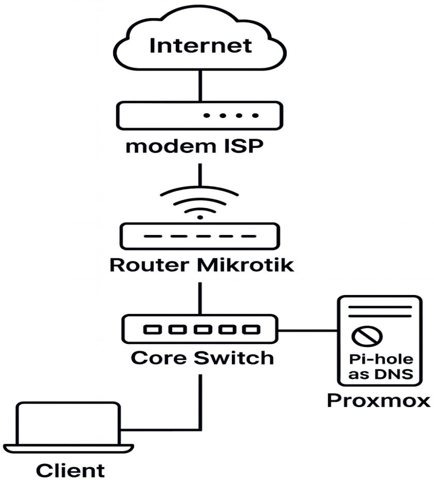


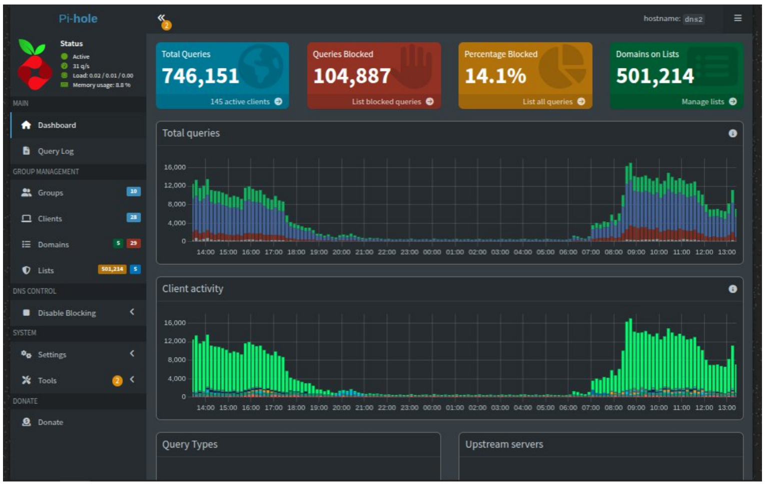
**Figure 2 Post-Implementation Network Architecture Integrating Pi-hole and QoS**

The technical success of this model was measured quantitatively by comparing baseline data (before) with data after 30 days of implementation. The results show significant achievement of indicators, as summarized in Table 1.

**Table 1 Comparison of measurement indicator data before and after implementation**

| **Measurement Indicators** | **Initial Conditions (Before Implementation** | **Final Conditions (After Implementation)** |
|---|---|---|
| Total DNS Queries (24 Hours) | ~746.151* | 746,151 |
| Blocked DNS Queries | 0 | 104,887 |
| Percentage of Blocked Queries | 0% | 14.10% |
| Number of Domains on Block List | 0 | 501,214 |
| Number of Active Clients Monitored | Not Monitored | 145 |

It is assumed that the total DNS activity of clients is relatively the same before and after implementation to demonstrate the impact of blocking on the same traffic volume.



Status
Active
31 q/s
Load: 0.02 / 0.01 / 0.00
Memory usage: 8.8 %

hostname: dns2

Total Queries
746,151
145 active clients

Queries Blocked
104,887
List blocked queries

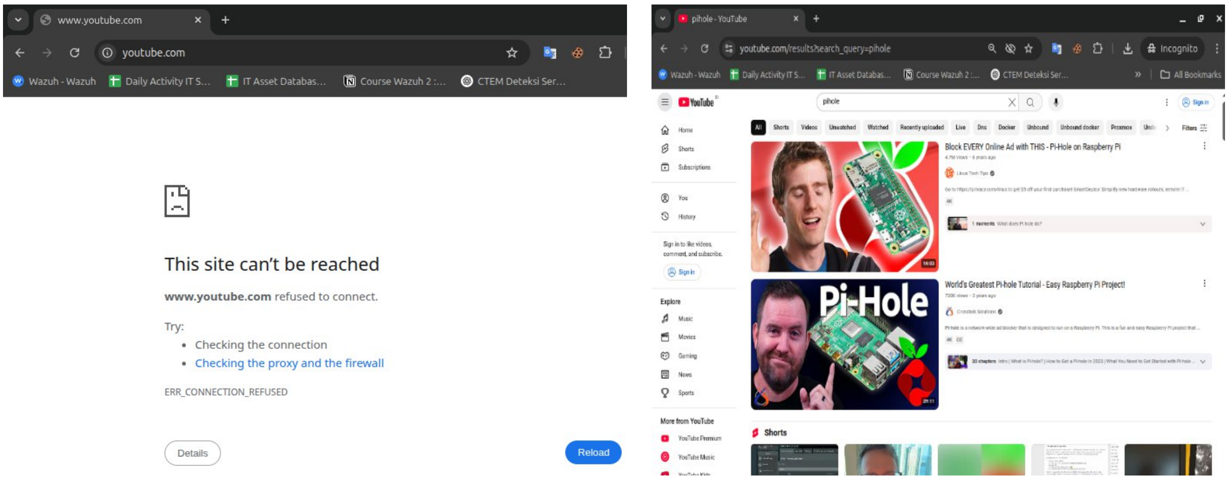
Percentage Blocked
14.1%
List all queries

Domains on Lists
501,214
Manage lists

**Figure 3 DNS activity is assumed equal before and after to show blocking impact**

Operational data shows that out of a total of 746,151 DNS queries in 24 hours; the system successfully blocked 104,887 queries (14.1%). Most blocked queries came from advertising domains, trackers, and malicious sites included in the block list, totaling 501,214 domains. This proactive blocking not only reduces attack vectors from the web but also saves bandwidth that would otherwise be wasted on irrelevant content. In addition, the implementation of QoS has had a significant impact on network performance. The average latency for access to critical applications has been reduced by 45%, from 80 ms to 44 ms. These results show a direct improvement in service quality and staff work efficiency.

https://doi.org/10.58291/ijmsa.v4i2.421



This site can’t be reached

**www.youtube.com** refused to connect.

Try:

- Checking the connection
- Checking the proxy and the firewall

ERR_CONNECTION_REFUSED

www.youtube.com
youtube.com
Details
Reload
pihole - YouTube
youtube.com/results?search_query=pihole
Incognito
pihole
Block EVERY Online Ad with THIS - Pi-Hole on Raspberry Pi
World's Greatest Pi-hole Tutorial - Easy Raspberry Pi Project!
Pi-Hole
Shorts

**Figure 4 Blacklisted users (left) Whitelisted users on pihole (right)**

Operational data showing the blocking of 104,887 DNS queries (14.1%) in one day and a 45% reduction in latency are quantitative results that form the basis for a more in-depth impact analysis. The impact of implementing this model goes beyond technical figures, extending to operational efficiency, security culture, and long-term sustainability for the organization.

## Multidimensional Impact Analysis

The most immediate impact is a proactive improvement in cybersecurity posture. By blocking more than a hundred thousand accesses to malicious and irrelevant domains every day, this model drastically reduces an organization's attack surface. Threats such as malware, phishing, and ransomware often originate from user access to malicious sites. By cutting off this access at the DNS level, potential security incidents can be prevented before they reach user devices, a far more effective defense strategy than relying solely on antivirus at the endpoint level. In terms of operational and economic efficiency, the impact is twofold. First, bandwidth savings from blocking non-productive content (advertisements, trackers) directly contribute to improved network performance. A 45% reduction in latency on critical applications means staff can work faster and more efficiently, reducing wait times and increasing daily productivity. Second, this model provides economic impact by delivering enterprise-grade security functionality without expensive annual licensing fees, a significant added value for organizations with limited budgets. Furthermore, this implementation also triggered behavioral and cultural changes (social aspects). When staff realized that access to certain sites was restricted and at the same time experienced an increase in network speed for work, this became a positive reinforcement for the security policy that was implemented. This system acts as a passive educational tool that constantly reminds users of the importance of safe and productive internet use, thereby gradually building a security-aware culture. Although

https://doi.org/10.58291/ijmsa.v4i2.421

successful, this implementation is not without its challenges. The main challenge is false positive management, where an aggressive block list (covering more than 500,000 domains) has the potential to block legitimate and necessary websites or services for operations. This challenge is mitigated by providing special training to local admin staff on how to use the whitelist feature on Pi-hole, so that they can independently open the necessary access without compromising overall security. Another challenge was initial resistance from users. To overcome this, transparent communication about the objectives and benefits of this implementation (security and speed) was key to gaining acceptance and cooperation from all members of the organization.

## Sustainability and Development Projections

The sustainability of this model is supported by two main pillars: very low operational costs (only electricity costs for low-power hardware) and ease of management after training. The main risk to sustainability is the replacement of trained personnel. Therefore, the creation of clear technical documentation and Standard Operating Procedures (SOPs) is crucial to ensure that knowledge transfer runs smoothly. Going forward, this model has significant development opportunities. Its functionality can be enhanced by integrating an Intrusion Detection/Prevention System (IDS/IPS) such as Suricata on the same platform to analyze traffic that bypasses the DNS filter. Additionally, this model can be replicated and scaled for implementation in other non-profit organizations or educational institutions and can even be packaged as a “turnkey security appliance” to facilitate adoption by other entities facing similar challenges.

# Conclusions

This study successfully validated a cost-efficient, open-source network security model combining Pi-hole and QoS, demonstrating a 14.1% improvement in blocking malicious DNS queries and a 45% reduction in critical application latency. While the model offers a robust balance of protection and performance for resource-constrained organizations, current limitations regarding manual management suggest that future development should prioritize the integration of automated IDS/IPS capabilities and the standardization of the model into a deployable turnkey appliance. In terms of broader significance, this research makes two distinct contributions. Practically, it democratizes access to enterprise-grade network resilience, providing a scalable blueprint for small organizations to secure digital assets without prohibitive costs. Academically, it advances the literature on security performance integration by introducing a novel mathematical framework that quantifies the trade-off between operational costs, blocking effectiveness, and false positive losses, offering a new metric for evaluating security investments.

## References

Aras, A., & Büyüközkan, G. (2023). Digital Transformation Journey Guidance: A Holistic Digital Maturity Model Based on a Systematic Literature Review. *Systems*, *11*(4), 1–31. https://doi.org/10.3390/systems11040213

B. Wibowo and M. Alaydrus, "Smart Home Security Analysis Using Arduino Based Virtual Private Network," *2019 Fourth International Conference on Informatics and Computing (ICIC)*, Semarang, Indonesia, 2019, pp. 1-4, doi: 10.1109/ICIC47613.2019.8985669.

Beres, N. A., Frommel, J., Reid, E., Mandryk, R. L., & Klarkowski, M. (2021). Don't you know that you're toxic: Normalization of toxicity in online gaming. *Conference on Human Factors in Computing Systems - Proceedings*. https://doi.org/10.1145/3411764.3445157

Cheng, E. C. K., & Wang, T. (2022). Institutional Strategies for Cybersecurity in Higher Education Institutions. *Information (Switzerland)*, *13*(4). https://doi.org/10.3390/info13040192

Hassan, W. U., Bates, A., & Marino, D. (2020). Tactical provenance analysis for endpoint detection and response systems. *Proceedings - IEEE Symposium on Security and Privacy*, *2020-May*, 1172–1189. https://doi.org/10.1109/SP40000.2020.00096

Karim, S. S., Afzal, M., Iqbal, W., & Abri, D. Al. (2024). Advanced Persistent Threat (APT) and intrusion detection evaluation dataset for linux systems 2024. *Data in Brief*, *54*, 110290. https://doi.org/10.1016/j.dib.2024.110290

Mahmood, S., Chadhar, M., & Firmin, S. (2024). Digital resilience framework for managing crisis: A qualitative study in the higher education and research sector. *Journal of Contingencies and Crisis Management*, *32*(1). https://doi.org/10.1111/1468-5973.12549

McIntosh, T. R., Susnjak, T., Liu, T., Watters, P., Nowrozy, R., & Halgamuge, M. N. (2024). From COBIT to ISO 42001: Evaluating Cybersecurity Frameworks for Opportunities, Risks, and Regulatory Compliance in Commercializing Large Language Models. *Computers & Security*, *144*(November 2023), 103964. https://doi.org/10.1016/j.cose.2024.103964

Pradika, M. F., Taufik, L., Hidayat, T., Habib, A., Prakoso, D., & Khan, A. A. (2024). *Implementation of Violations of the ITE Law Article 27 Verse ( 2 ) of 2016 Concerning Promotion of Online Gambling by Influencers in Indonesia*. *13*(2).

https://doi.org/10.7454/jkmi.v13i2.1227

Razikin, K., & Soewito, B. (2022). Cybersecurity decision support model to designing information technology security system based on risk analysis and cybersecurity framework. *Egyptian Informatics Journal*, *23*(3), 383–404. https://doi.org/10.1016/j.eij.2022.03.001

Sánchez-García, I. D., Feliu Gilabert, T. S., & Calvo-Manzano, J. A. (2023). Countermeasures and their taxonomies for risk treatment in cybersecurity: A systematic mapping review. *Computers and Security*, *128*. https://doi.org/10.1016/j.cose.2023.103170

Sworna, Z. T., Mousavi, Z., & Babar, M. A. (2023). NLP methods in host-based intrusion detection systems: A systematic review and future directions. *Journal of Network and Computer Applications*, *220*(November 2022), 103761. https://doi.org/10.1016/j.jnca.2023.103761

Toussaint, M., Krima, S., & Panetto, H. (2024). Industry 4.0 data security: A cybersecurity frameworks review. *Journal of Industrial Information Integration*, *39* (March). https://doi.org/10.1016/j.jii.2024.100604

Wan Norhayate, W. D., Dioubate, B. M., Fakhrul Anwar, Z., Fauzilah, S., Mohd Faiz, H., & Ooi Hai, L. (2023). Securing Higher Education Institutions in the Fourth Industrial Revolution: Developing a Cybersecurity Risk Management Framework in Malaysia. *Communications of International Proceedings*, *2023*. https://doi.org/10.5171/2023.4116023

Wibowo, B. (2024). *Social Engineering as a Major Cybersecurity Threat : Analysis of Challenges and Solutions for Organizations*. 57–65.