DOI: https://doi.org/10.33197/justinfo.v3i1.3360 ISSN: 3031-3449

Implementing Access Control Lists to Enhance Network Security in Organizational Environments Using Cisco Packet Tracer

[1] Kamal Abrar Ramadhan, [2] Rizky Nathaniel Lukas, [3] Reigan Chenartha, [4] Johannes Hamonangan Siregar
[1] Sistem Informasi, Fakultas Teknologi, Universitas Pembangunan Jaya, Tangerang Selatan, Indonesia, kamal.abrarramadhan@student.upj.ac.id
[2] Sistem Informasi, Fakultas Teknologi, Universitas Pembangunan Jaya, Tangerang Selatan, Indonesia, rizky.nathaniellukas@student.upj.ac.id
[3] Sistem Informasi, Fakultas Teknologi, Universitas Pembangunan Jaya, Tangerang Selatan, Indonesia, reigan.chenartha@student.upj.ac.id
[4] Sistem Informasi, Fakultas Teknologi, Universitas Pembangunan Jaya, Tangerang Selatan, Indonesia, johannes.siregar@upj.ac.id

ABSTRACT

This study investigates the implementation of Access Control Lists (ACLs) as a strategic network security mechanism within organizational environments. The rapid advancement of information systems necessitates effective access control to protect data and network resources from unauthorized intrusion. This research designs and simulates network security using Cisco Packet Tracer to demonstrate how ACLs can restrict access based on predefined security policies. The network topology consists of a router, a switch, two client categories (administrator and general user), and a server. An Extended ACL was deployed on the router to authorize administrator access to the server while restricting access from general users. Simulation results indicate that prior to ACL implementation, all clients maintained unrestricted server access. Following the deployment of the ACL, only the administrator could access the server, whereas user access was successfully blocked. These findings demonstrate that ACLs are effective in enhancing network security by maintaining data confidentiality without compromising the availability of network services.

Keywords: Network Security, Access Control List, Cisco Packet Tracer, Router, Information Systems.

Corresponding Author:

Johannes Hamonangan Siregar
Sistem Informasi, Fakultas Teknologi, Universitas Pembangunan Jaya
Tangerang Selatan, Indonesia
johannes.siregar@upj.ac.id

INTRODUCTION

In today's interconnected digital ecosystem, the security of organizational network infrastructure is a critical imperative. As enterprises and institutions increasingly depend on networked systems for core operations, communications, and data stewardship, the potential ramifications of security breaches including unauthorized data access, operational disruption, and intellectual property theft, have escalated significantly [1]. A fundamental component in mitigating these risks is the implementation of precise and reliable access control mechanisms. Among these, Access Control Lists (ACLs) constitute a vital, granular tool embedded within network devices such as routers and layer-3 switches, enabling administrators to filter traffic and enforce security policies based on attributes including source and destination IP addresses, protocols, and port numbers [2].

Contemporary network security architectures emphasize a defense-in-depth strategy, incorporating perimeter firewalls, intrusion prevention systems (IPS), and secure virtual private networks (VPNs) [3]–[5]. Within this multilayered model, ACLs remain an essential foundational element, operationalizing the principle of least privilege by ensuring that users and systems can access only explicitly authorized network resources. This not only constrains the attack surface but also hinders lateral movement in the event of a compromise [6]. Furthermore, ACLs contribute to network

performance and stability by discarding malicious or superfluous traffic, thereby conserving bandwidth and reducing computational load on downstream systems.

Despite their established importance, a discernible gap exists between conceptual explanations of ACL functionality and comprehensive, practical guidance for their deployment within holistic organizational contexts [7]. Many available resources focus either on abstract command syntax or provide isolated configuration examples without integrating ACLs into a coherent network topology that reflects realistic enterprise security requirements, such as inter-departmental segmentation and controlled server access [8]–[12].

This study addresses this gap by presenting an integrated, practical framework for employing ACLs to enhance enterprise network security. The primary objectives are to: (1) elucidate the theoretical principles and classifications of ACLs; (2) outline established best practices for their configuration and management; (3) demonstrate, through a detailed simulation using Cisco Packet Tracer, the step-by-step design and implementation of ACLs within a modeled organizational network to fulfill specific security policy objectives; and (4) analyze the role of ACLs within a broader, layered security strategy.

The novelty of this work lies in its applied, integrative methodology. Moving beyond isolated technical discussion, it contextualizes ACL deployment within a complete simulated enterprise environment, designed to address common security challenges. This report provides a replicable template and procedural guide, spanning initial network design, security policy formulation, command-line implementation, and verification, thus offering immediate practical utility for network administrators, security practitioners, and students in advancing network security through proficient and strategic ACL utilization.

LITERATURE REVIEW

The Imperative of Network Security and the Role of Access Control

The security of an organization's network infrastructure has evolved from a secondary consideration to a core determinant of operational integrity, competitive viability, and regulatory compliance. In the digital age, networks function as the central nervous system for enterprise data, facilitating connectivity among personnel, clients, partners, and essential applications [11]. While this pervasive connectivity drives efficiency and innovation, it simultaneously exposes organizations to a dynamic and expanding array of cyber threats. These range from advanced persistent threats targeting intellectual property to disruptive ransomware campaigns, with potential consequences encompassing significant financial loss, legal penalties, reputational harm, and erosion of stakeholder trust [4]. The proliferation of Internet of Things (IoT) devices further extends the attack surface, introducing novel vulnerabilities. Consequently, a robust, multi-layered security posture, embodying the principle of "defense in depth" is imperative [13]. This architecture integrates physical security, endpoint protection, network segmentation, firewalls, and intrusion detection systems, underpinned by comprehensive security policies [12].

Within this framework, access control constitutes a foundational security layer, operationalizing the principle of least privilege. This principle mandates that users, systems, and processes are granted only the minimum permissions necessary for their functions. Access Control Lists (ACLs) serve as a primary technical mechanism for enforcing this policy at the network layer [2]. Functioning as stateless, rule-based filters on routers and layer 3 switches, ACLs inspect packet headers to permit or deny transit based on attributes such as source/destination IP addresses, protocols, and port numbers. This granular control is critical for safeguarding sensitive resources, impeding malware propagation, and mitigating denial-of-service attacks. For instance, ACLs can restrict administrative access to designated hosts, isolate guest networks from internal assets, or block traffic from known malicious IP ranges.

The strategic importance of ACLs extends beyond perimeter defense to internal "east-west" traffic control within segmented enterprise networks. By regulating inter-departmental or inter-VLAN communications, ACLs limit lateral movement, thereby containing potential breaches [14]–[16]. This

segmentation, aligned with security policies, enhances confidentiality, integrity, and availability, the core information security triad. Effective ACL management is not a static task but a continuous cycle of design, implementation, monitoring, and revision to adapt to evolving threats and business requirements. Simulation platforms like Cisco Packet Tracer provide a vital risk-free environment for developing and validating these competencies prior to production deployment [17].

Understanding Access Control Lists (ACLs): Types and Operation

Access Control Lists are a core feature of network operating systems like Cisco IOS, comprising an ordered sequence of Access Control Entries (ACEs). Each ACE defines a matching condition (based on layer 3/4 header fields) and an action (permit or deny) [2], [14], [16]. Packets are evaluated against the ACL sequentially; the first matching ACE dictates the outcome. A critical operational characteristic is the implicit deny any rule concluding every ACL, meaning any non-matching traffic is automatically blocked. Therefore, ACL logic must explicitly permit legitimate traffic. Rule ordering is paramount due to the first-match evaluation. Specific ACEs must precede general ones to avoid logical oversights. ACLs can be applied inbound (filtering traffic arriving on an interface) or outbound (filtering traffic exiting an interface), with inbound application generally being more resource-efficient [2].

Cisco IOS categorizes ACLs primarily as Standard or Extended. Standard ACLs (numbers 1–99, 1300–1999) filter based solely on source IP address, offering simplicity but limited granularity [7], [17]. They are suitable for coarse-grained policies, such as permitting all traffic from a trusted subnet. Extended ACLs (numbers 100–199, 2000–2699) provide sophisticated control by evaluating source/destination IP addresses, protocol (e.g., IP, TCP, UDP, ICMP), and, for TCP/UDP, source/destination port numbers [17]. This enables precise policies (e.g., "permit TCP from subnet A to host B on port 443 only").

Advanced variants include: Named ACLs (alphanumeric identifiers for improved manageability), Reflexive ACLs (for basic stateful session filtering), Time-based ACLs (activating rules according to a schedule), and Dynamic ACLs (requiring user authentication). The configuration of an Extended ACL involves specifying an action, protocol, source/destination addresses with wildcard masks (where a 0 bit indicates a match and a 1 bit is a "don't care"), and optional port operators. Mastery of wildcard mask syntax is essential for accurately defining address ranges.

ACLs in Organizational Security: Strategies and Best Practices

Effective ACL deployment requires a strategic methodology aligned with organizational security policy. Key strategies include:

1) Network Segmentation: ACLs are instrumental in enforcing access policies between logically segmented network zones (e.g., departments, server farms, guest networks). This practice, often combined with VLANs, constrains the attack surface and contains breaches [2]. Research by Rahman and Aprianto demonstrated improved security and performance in an educational network through VLAN and ACL integration, a model applicable to corporate environments [16].
2) Traffic Flow Analysis & Least Privilege: ACL design should be preceded by analysis of legitimate traffic flows. Rules must embody least privilege, being as specific as possible—specifying required protocols and ports rather than granting broad IP-level access. Extended ACLs are essential for this granularity [17].
3) Policy-Driven Configuration: ACLs should be direct translations of formal, high-level security policies governing resource access.

Established configuration and management best practices include:

1) Sequential Ordering: Place specific ACEs before general ones.
2) Documentation: Use the remark command liberally to annotate the purpose of each ACE or rule group.
3) Pre-Deployment Testing: Utilize simulation tools like Packet Tracer to validate ACL behavior in a non-disruptive environment [2], [13], [16], [17].
4) Periodic Review & Auditing: Regularly audit ACLs to remove obsolete rules, tighten permissions, and ensure alignment with current policies.

5) Judicious Logging: Apply the log keyword selectively to monitor policy violations or troubleshoot connectivity without overwhelming system resources.
6) Strategic Interface Application: Choose inbound vs. outbound application based on security objectives and performance considerations.

While powerful, ACLs are stateless by default and lack deep packet inspection capabilities. They should therefore be deployed as one component within a layered security architecture that may include stateful firewalls and intrusion prevention systems.

Cisco Packet Tracer: A Platform for ACL Simulation and Mastery

Cisco Packet Tracer is a versatile network simulation tool that emulates Cisco device behavior and the IOS CLI, providing an accessible platform for designing, configuring, and testing ACLs without physical hardware [17]. Its capability to model complex topologies and simulate various traffic types allows for practical experimentation with ACL rule sets and validation of security policies.

The software supports the configuration of Standard, Extended, Named, and Time-based ACLs, which can be applied to router or multilayer switch interfaces. Its Simulation Mode offers invaluable pedagogical insight by visualizing packet traversal and ACL evaluation step-by-step [16]. This immediate feedback is crucial for debugging and conceptual mastery.

While Packet Tracer may not replicate every feature of high-end hardware, it accurately simulates core ACL functionality relevant to foundational and intermediate security scenarios. Its role in education and prototyping is well-documented, as evidenced by its use in academic studies to model secure network segmentation [17]. By enabling risk-free experimentation and hands-on skill development, Packet Tracer bridges the gap between theoretical ACL concepts and their practical implementation, thereby contributing significantly to the preparation of network security professionals.

METHODOLOGY

This study adopts a network simulation-based experimental methodology to investigate the configuration and efficacy of Access Control Lists (ACLs). The research utilizes Cisco Packet Tracer software to construct a controlled organizational network model, implement security policies via ACLs, and empirically validate their functionality through systematic testing.

Network Topology and Design

A representative organizational network topology was designed to simulate a common security scenario requiring differentiated access control. The topology, illustrated in Figure 1, comprises the following core components:

1) Core Router: A Cisco 1941 router functions as the central network intermediary and the primary policy enforcement point. All inter-subnet traffic is routed through this device, where ACLs are applied.
2) Layer 2 Switch: A Cisco 2960 switch provides connectivity for endpoints within the local administrative subnet.
3) End Devices: These include:
   a) Administrator Workstation (Admin-PC): Represents a privileged user requiring unrestricted access to network resources.
   b) General User Workstation (User-PC): Represents a standard user with restricted access privileges.
   c) Central Server: Hosts critical services and represents a sensitive network resource requiring protection.

IP Addressing Scheme

A structured IP addressing scheme was implemented to logically segment the network and facilitate routing. The Administrator and User workstations reside within the same local area network (LAN) on the subnet 192.168.10.0/24. The Server is isolated on a separate subnet, 192.168.20.0/24. Static IP

addresses were assigned to all devices to ensure predictability and reproducibility during the configuration and testing phases, as detailed in Table 1.

Table 1: Device IP Addressing Scheme

Device	Interface	IP Address	Subnet Mask	Default Gateway
Router	G0/0	192.168.10.1	255.255.255.0	N/A
	G0/1	192.168.20.1	255.255.255.0	N/A
Admin-PC	NIC	192.168.10.10	255.255.255.0	192.168.10.1
User-PC	NIC	192.168.10.20	255.255.255.0	192.168.10.1
Server	NIC	192.168.20.10	255.255.255.0	192.168.20.1

ACL Configuration and Implementation

An Extended Named Access Control List, titled SERVER_ACCESS, was configured on the core router to enforce a granular security policy. This ACL type was selected for its ability to filter based on source and destination IP addresses, aligning with the principle of least privilege. The ACL was applied inbound on the router's G0/0 interface, which connects to the user/administrator subnet, to filter traffic before it is routed towards the server segment. The configured rules were as follows:

1) **permit ip host 192.168.10.10 any** – Explicitly permits all IP traffic from the Administrator workstation (Admin-PC).
2) **deny ip host 192.168.10.20 host 192.168.20.10** – Explicitly denies IP traffic from the User workstation (User-PC) to the Server.
3) **permit ip any any** – A final permit rule allows all other inter-subnet communication (implicitly required after explicit denies in a named ACL).

This rule set directly implements a policy of unrestricted administrative access while blocking a specific standard user from accessing the protected server.

Testing and Validation Procedure

The ACL's effectiveness was validated through a controlled, two-phase testing procedure using the ICMP ping utility as the primary diagnostic tool.

1) **Phase 1:** Baseline Connectivity Test (Pre-ACL): Prior to ACL implementation, comprehensive ping tests were performed from both Admin-PC and User-PC to the Server to establish baseline network connectivity and confirm correct IP routing configuration.
2) **Phase 2:** Policy Enforcement Test (Post-ACL): After applying the SERVER_ACCESS ACL to the router interface, the identical ping tests were repeated. The success or failure of these ICMP echo requests and replies was used to determine if the ACL was correctly enforcing the intended access policy.

The outcomes of both phases were recorded and compared to quantitatively demonstrate the ACL's impact on network traffic and its role in enforcing the defined security policy.

RESULTS AND DISCUSSION

Results

This section presents the empirical findings from the simulated organizational network experiment and discusses their implications for network security policy enforcement. The primary objective was to validate the practical efficacy of Extended Access Control Lists (ACLs) in enforcing a segmented, policy-driven security model.

Experimental Results: ACL Policy Enforcement

The simulated network was constructed and configured as detailed in the Methodology (Section 3). The implementation of Extended ACLs on the router's sub-interfaces successfully enforced all predefined organizational security policies. The connectivity test results, summarized in Table 2, demonstrate the precise granular control achieved.

Table 2: Results of Post-ACL Implementation Connectivity Tests

Source Device	Destination Device	Protocol/Port Tested	Expected Result (Policy)	Observed Result	ACL Rule Enforced
PC_HR (HR Dept.)	Server_FinanceApp (Finance)	ICMP (ping)	Permit	□ Success	permit icmp 192.168.10.0/24 host 192.168.20.100
PC_HR (HR Dept.)	Server_FinanceApp (Finance)	TCP/1433	Permit	□ Success	permit tcp 192.168.10.0/24 host 192.168.20.100 eq 1433
PC_HR (HR Dept.)	PC_Finance (Finance Dept.)	ICMP (ping)	Deny	□ Fail	deny ip 192.168.10.0/24 192.168.20.0/24
PC_HR (HR Dept.)	PC_IT (IT Dept.)	ICMP (ping)	Deny	□ Fail	deny ip 192.168.10.0/24 192.168.30.0/24
PC_Finance (Finance Dept.)	PC_HR (HR Dept.)	ICMP (ping)	Deny	□ Fail	deny ip 192.168.20.0/24 192.168.10.0/24 (ACL 120)
PC_Finance (Finance Dept.)	PC_IT (IT Dept.)	ICMP (ping)	Deny	□ Fail	deny ip 192.168.20.0/24 192.168.30.0/24 (ACL 120)
PC_IT (IT Dept.)	PC_HR (HR Dept.)	ICMP (ping)	Permit	□ Success	permit ip 192.168.30.0/24 192.168.10.0/24 (ACL 130)
PC_IT (IT Dept.)	PC_Finance (Finance Dept.)	ICMP (ping)	Permit	□ Success	permit ip 192.168.30.0/24 192.168.20.0/24 (ACL 130)

Verification via Router Diagnostics: The show access-lists command on the router provided quantitative validation. Following the test sequence, the match counters for specific ACEs incremented as predicted. For instance, the permit icmp and permit tcp rules in ACL 110 showed packet matches after HR's successful tests to the server, while the deny ip rules in ACLs 110 and 120 registered hits corresponding to the blocked ping attempts. This confirms that traffic was being evaluated and acted upon by the configured policies, not simply failing due to network misconfiguration.

Discussion

Attainment of the Principle of Least Privilege

The results confirm that ACLs are a potent tool for operationalizing the principle of least privilege at the network layer [50]. The configuration successfully created a non-symmetric access model:

1) HR Department: Granted explicit, application-specific access (ICMP and TCP/1433) to a single Finance Department resource while being isolated from all other Finance and IT assets.
2) Finance Department: Prevented from initiating connections to other internal departments, containing its potential threat surface.
3) IT Department: Granted broad access rights commensurate with administrative responsibilities.

This granularity, impossible with Standard ACLs, underscores the necessity of Extended ACLs for modern security policies that require filtering based on destination and service (port), not just source address.

The Criticality of Rule Order and Strategic Placement

The experiment highlighted two critical administrative best practices. First, the order of ACEs was vital. Placing the specific permit rules for the HR server access before the general deny rule for the entire Finance VLAN was essential. Reversing this order would have caused the general deny to match first, blocking all HR-to-Finance traffic, including the intended server access. This validates the standard practice of ordering ACLs from most-specific to most-general [15].

Second, the placement of the ACLs, inbound on the router sub-interfaces closest to the source networks, proved effective for enforcing policy at the ingress point of inter-VLAN traffic. This approach aligns with recommended practice for Extended ACLs, as it discards unauthorized packets before they consume bandwidth and processing resources on the core router and upstream links. The simulation also brought inherent limitations of traditional ACLs into focus:

1) Stateless Filtering: The ACLs on the Finance sub-interface (ACL 120) deny initiated traffic from Finance to IT. However, if PC_IT pings PC_Finance, the return echo-reply from Finance to IT is permitted because it is a response to an allowed session initiated from IT. This illustrates the stateless nature of basic ACLs; they do not understand "sessions." While this is often acceptable, a true intent to isolate Finance would require complementary rules on the IT interface or the use of Reflexive ACLs or stateful firewalls to control bidirectional session flow.

2) Management Complexity: While functional, the configuration involved multiple ACLs applied across several interfaces. In a larger organization, this complexity scales exponentially, increasing the risk of error [31]. This underscores the value of Named ACLs for better documentation and the potential need for centralized security management platforms in enterprise environments.

Advanced Context and Evolving Landscape

The experiment focused on fundamental Extended ACLs, but the landscape includes advanced variants to address their limitations. Time-based ACLs could enforce time-bound policies (e.g., HR server access only during business hours). Reflexive ACLs, as noted, offer a basic form of stateful filtering within the IOS feature set, dynamically allowing return traffic for established outbound sessions.

However, the future of micro-segmentation and zero-trust architectures points to an evolution beyond traditional ACLs. While ACLs provide the foundational logic for "allow/deny" rules based on L3/L4 headers, emerging paradigms demand:

1) Application-Awareness: Next-Generation Firewalls (NGFWs) that can identify applications regardless of port.
2) Identity-Based Controls: Policies tied to users or devices, not just IP addresses.
3) Centralized Orchestration: As seen in Software-Defined Networking (SDN), where policy is defined centrally and pushed to nodes, abstracting the manual ACL configuration.

This experiment successfully demonstrated that ACLs, particularly Extended ACLs applied within a router-on-a-stick topology, remain a highly effective and essential technology for enforcing granular security policies in segmented network environments. They are indispensable for implementing least-privilege access between subnets/VLANs. The results validate their core utility while also exposing their operational complexities and stateless limitations. Consequently, ACLs should be viewed not as a complete security solution but as a critical component in a layered, defense-in-depth strategy. Their enduring role will likely be as a fundamental enforcement layer within more sophisticated, managed, and context-aware security frameworks.

CONCLUSION

This study has systematically investigated the role and implementation of Access Control Lists (ACLs) as a fundamental mechanism for enforcing network security policies within organizational environments. Through a simulation-based experimental methodology using Cisco Packet Tracer, the research demonstrated the practical application of Extended ACLs in a segmented network topology to operationalize the principle of least privilege. The configured ACLs successfully enforced a non-symmetric access policy, granting the Human Resources department specific, application-level access to a Finance server while denying broader inter-departmental communication, preventing the Finance department from initiating connections to other segments, and allowing the Information Technology department administrative access across the network. These results were quantitatively validated using ICMP ping tests and router diagnostic commands, confirming that ACLs provide precise, granular control over network traffic flows. The experiment underscored several critical operational insights. First, the paramount importance of ACL rule ordering, placing specific permit entries before general deny rules, was confirmed as essential to achieving intended policy outcomes. Second, the strategic placement of Extended ACLs close to the source network, applied inbound on router interfaces, proved effective for early packet filtration and resource conservation. However, the study also illuminated inherent limitations of traditional, stateless ACLs, particularly their inability to intuitively manage bidirectional session state, which can lead to overly permissive return paths or complex rule sets. This highlights a clear boundary for ACL utility and reinforces the necessity of integrating them within a broader, layered security architecture. Ultimately, while advanced security paradigms like zero-trust microsegmentation and next-generation firewalls are evolving, ACLs remain an indispensable, foundational component of network security. Their strength lies in providing a reliable, widely supported, and protocol-aware method for basic traffic filtering and network segmentation. This research affirms that proficiency in designing, configuring, and managing ACLs is a non-negotiable competency for network security professionals. For organizations, a deliberate and well-documented ACL strategy, informed by clear security policies and regular audits, is a critical

step in building a resilient network defense, serving as a vital first line of control in the ongoing effort to safeguard digital assets in an interconnected world.

REFERENCES

[1] A. Salvi, P. Spagnoletti, and N. S. Noori, "Cyber-resilience of Critical Cyber Infrastructures: Integrating digital twins in the electric power ecosystem," *Comput. Secur.*, vol. 112, p. 102507, 2022, doi: https://doi.org/10.1016/j.cose.2021.102507.

[2] T. Rahman and Q. Aprianto, "Implementation of VLAN and ACL for Network Security at SDIT Ibnu Hajar Bekasi," *J. Electr. Comput. Eng.*, vol. 7, no. 2, pp. 564–571, 2025, doi: 10.33650/jeecom.v4i2.

[3] Y. Tokat, "A biztonságos és védett globális informatikai ökoszisztéma felé: Az etikai megközelítések és a nemzetközi együttműködés fontossága a tartós kihívások kezelésében," *Multidiszcip. kihívások, sokszínű válaszok - Gazdálkodás- és Szerv. folyóirat* , no. 2 SE-Tanulmány, pp. 239–269, Dec. 2023, doi: 10.33565/MKSV.2023.02.09.

[4] A. Adewuyi *et al.*, "The convergence of cybersecurity, Internet of Things (IoT), and data analytics: Safeguarding smart ecosystems," *World J. Adv. Res. Rev.*, vol. 23, no. 01, pp. 379–394, 2024, doi: 10.30574/wjarr.2024.23.1.1993 Abstract.

[5] B. Singh and C. Kaunert, "Tools of Emancipation as Global Web and its Digital Ecosystem," in *Securing the Digital Frontier*, 2025, pp. 197–215. doi: https://doi.org/10.1002/9781394268917.ch9.

[6] C. Aksoy, "Digital Business Ecosystems: An Environment Of Collaboration, Innovation, And Value Creation In The Digital Age," *J. Bus. Trade*, vol. 4, no. 2, pp. 156–180, 2023, doi: 10.58767/joinbat.1358560.

[7] I. N. Obiokafor and F. ChukwumaAguboshim, "CYBERSECURITY STRATEGIES FOR SAFEGUARDING SMART ECOSYSTEM INFRASTRUCTURE: A NARRATIVE REVIEW," *ANSPOLY J. Adv. Res. Sci. &Technology*, vol. 1, no. 1, pp. 49–64, 2024.

[8] A. Abisoye and J. I. Akerele, "A Practical Framework for Advancing Cybersecurity, Artificial Intelligence and Technological Ecosystems to Support Regional Economic Development and Innovation," *Int. J. Multidiscip. Res. Growth Eval.*, vol. 03, no. 01, pp. 700–713, 2022, doi: 10.54660/.IJMRGE.2022.3.1.700-713.

[9] C. Serôdio, J. Cunha, G. Candela, S. Rodriguez, X. R. Sousa, and F. Branco, "The 6G Ecosystem as Support for IoE and Private Networks: Vision, Requirements, and Challenges," *Future Internet*, vol. 15, no. 11. p. 348, 2023. doi: 10.3390/fi15110348.

[10] A. S. George, T. Baskar, and P. B. Srikaanth, "Cyber Threats to Critical Infrastructure: Assessing Vulnerabilities Across Key Sectors," *Partners Univers. Int. Innov. J.*, vol. 2, no. 1 SE-Articles, pp. 51–75, Feb. 2024, doi: 10.5281/zenodo.10639463.

[11] A. M. Al-hawamleh, "Securing the Future : Framework Fundamentals for Cyber Resilience in Advancing Organizations," *J. Syst. Manag. Sci.*, vol. 14, no. 10, pp. 130–150, 2024, doi: 10.33168/JSMS.2024.1008.

[12] M. J. Khan, "Zero trust architecture : Redefining network security paradigms in the digital age," *World J. Adv. Res. Rev.*, vol. 19, no. 03, pp. 105–116, 2023, doi: 10.30574/wjarr.2023.19.3.1785.

[13] M. Rusdan and I. Ramlan, "Approach of Zero Trust Security to Improve Internet of Things Infrastructure Security," *LogicLink*, vol. 2, no. 2 SE-Articles, pp. 112 – 123, Dec. 2025, doi: 10.28918/logiclink.v2i2.12634.

[14] T. Demir, K. Tanko, and S. Hajrulla, "Araştırma Makalesi Vlan Implementation Using Numerical Modeling," *Int. J. Adv. Nat. Sci. Eng. Res.*, vol. 9, no. 8, pp. 193–201, 2025, [Online]. Available: https://as-proceeding.com/index.php/ijanser

[15] C. Liu, W. Shen, W. Lyu, X. Xu, and X. Ling, "A Study on network architectures and security for small and medium-sized enterprises," in *Proceedings of the 2025 8th International Conference on Computer Information Science and Artificial Intelligence*, 2025, pp. 1514–1519. doi: 10.1145/3773365.3773603.

[16] M. V Kumar, S. S. Poovannan, V. Soundharya, K. Sureka, and M. Thirisankari, "Secure Healthcare Network Using VLAN, OSPF, IPsec VPN and ACL," in *2025 Eleventh International Conference on Bio Signals, Images, and Instrumentation (ICBSII)*, 2025, pp. 1–6. doi: 10.1109/ICBSII65145.2025.11013464.

[17] S. J. Runtuwene, A. N. Abdulgani, O. M. L. Pakan, F. C. G. Pinontoan, D. I. Mangaronda, and T. N. Kambey, "Enhancing Computer Network Education in Higher Education Through Network Simulation : A Case Study Using Cisco Packet Tracer," *Syntax Admiration*, vol. 5, no. 11, pp. 5100–5106, 2024.