SIngh

by jowua paper

Submission date: 07-Jul-2025 11:13AM (UTC+0700)
Submission ID: 2711217325
File name: 10329-28915-1-RV.docx (1.16M)
Word count: 4556
Character count: 27824

JIKO (Jurnal Informatika dan Komputer)
Vol. x, No. x, April 2024, pp. x-x
DOI: 10.33387/jiko

Accredited KEMENDIKBUD RISTEK, No.105/E/KPT/2022
p-ISSN: 2614-8897
e-ISSN: 2656-1948

ENHANCED NETWORK SECURITY USING ZERO TRUST IN SMART HOME NETWORKS AGAINST MAN-IN-THE-MIDDLE ATTACKS

Bewitraj Singh[1], Raka Yusuf[2]

[1]Universitas Mercu Buana
[2]Universitas Mercu Buana
Email: [1]bewitraj12@gmail.com

(Received: dd mmm yyyy, Revised: dd mmm yyyy, Accepted: dd mmm yyyy)

Abstract

This study aims to enhance network security by implementing a Zero Trust architecture in the context of a Smart Home network and to analyze its effectiveness in protecting the network from Man-in-the-Middle (MitM) attacks. With the increasing use of Internet of Things (IoT) devices in Smart Home environments, the risk of MitM attacks has become a major concern, as attackers can eavesdrop and manipulate communications between devices. This research adopts a comparative method to evaluate the vulnerability levels to MitM attacks between networks using Zero Trust principles and those following traditional security approaches. Testing was conducted through virtual environment simulations representing both security approaches. The results show that implementing the Zero Trust architecture significantly reduces vulnerabilities to MitM attacks compared to conventional security methods. Furthermore, this study identifies various technical and implementation challenges in deploying Zero Trust in Smart Home environments, including limited device resources and complex identity management. This research provides strategic recommendations for developing more effective Smart Home security systems and is expected to serve as a reference for developers, researchers, and users in designing adaptive and sustainable security solutions.

Keywords: *Internet Of Things, Man-in-the-Middle, Smart Home, Zero Trust, Network Security*

Corresponding Author: Bewitraj Singh

1. INTRODUCTION

The The advancement of Internet of Things (IoT) technology has brought significant transformations in various aspects of human life[1]. One of the most prominent applications is in Smart Home systems, where devices such as security cameras, smart thermostats, digital door locks, and automatic lights are interconnected via the internet and can be controlled remotely[2]. With the increasing adoption of this technology, network security has become an increasingly important and complex issue[3].

Smart Home networks generally still rely on traditional security approaches, such as the use of firewalls, Network Address Translation (NAT) systems, and basic authentication[4], [5]. Although these approaches are effective in certain conditions, they have fundamental weaknesses in dealing with internal network threats, such as Man-in-the-Middle (MitM) attacks[6], [7]. In such attacks, perpetrators can infiltrate the local network and monitor or even modify communication between devices without being detected[8], [9]. This threat is exacerbated by the open nature of household networks, where connected devices often have weak security, lack network segmentation, and minimal control over who can access these devices. Therefore, a new approach is needed that can provide more comprehensive and adaptive protection[10].

The Zero Trust architecture emerges as an innovative solution that no longer relies on implicit trust in entities within the network. Its main principle is "never trust, always verify," meaning that every access request must be strictly verified, regardless of the origin of the request[11], [12]. With this approach, the network is built on the assumption that every connection is a potential threat, and access is granted based on strict policies and multi-layered

authentication[13], [14]. In the context of Smart Homes, the implementation of Zero Trust offers great potential for strengthening security, but it also presents its own challenges, such as limited device resources, complexity in identity management, and the need for systems that can operate efficiently and lightly[15], [16].

This study aims to fill this gap by comparing the effectiveness of traditional and Zero Trust security approaches in handling MitM attacks on Smart Home networks[17], [18]. By conducting simulations in a virtual environment, this research is expected to provide empirical evidence regarding the benefits and challenges of each approach, as well as offer more targeted implementation recommendations. This research aims to:

1. Design and simulate Smart Home network topologies with traditional and Zero Trust security approaches;
2. Test and compare the vulnerability levels of both approaches to MitM attacks;
3. Analyze the test results to provide recommendations for more adaptive and effective security implementations.

2. RESEARCH METHOD

Describe This research article adopts a comparative experimental approach, utilizing a virtual network simulation environment to compare the effectiveness of two security strategies: conventional and Zero Trust. The simulation environment is realized through the integration of GNS3 software for network orchestration and Oracle VirtualBox for virtual machine hosts, which collectively replicate realistic household network conditions. The research process is structured into a series of methodical steps, as illustrated in Figure 1

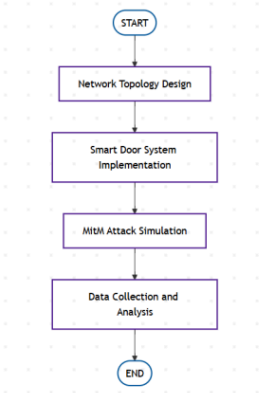

Figure 1. Research Methodology Flowchart

2.1 Network Topology Design

Two distinct network configurations were meticulously designed to represent different security scenarios: traditional and Zero Trust. The choice of these designs is based on common characteristics of home networks and the security principles of each model.

Traditional Network Topology: This topology was designed to mirror a common and conventional household network architecture, where implicit internal trust still prevails. This configuration consists of a router (simulating a generic home router), a switch, and three main entities: a user device (represented by a Lubuntu virtual machine), an IoT device (represented by an Ubuntu Server running the Smart Door application), and an attacker device (represented by a Kali Linux virtual machine). All these devices are placed within a single, flat network segment without significant segmentation or isolation, using the 192.168.10.0/24 subnet. This design reflects the inherent vulnerabilities in traditional networks, where once an attacker successfully breaches the perimeter (e.g., through physical access or compromise of a weak device), they have implicit access to all devices within the network. This openness significantly increases the attack surface for lateral movement and MitM attacks. This topology is illustrated in detail in Figure 2

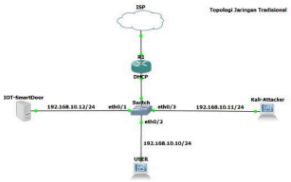

Figure 2. Traditional Network Topology

Zero Trust Network Topology: In contrast to the traditional approach, the Zero Trust topology is built upon the principles of "never trust, always verify" and "least privilege access"[19], [20]. This architecture leverages a multilayer router configured to provide strict network segmentation through the use of Virtual LANs (VLANs). Each device is placed within a separate and logically isolated subnet: the IoT device (Smart Door) is on 192.168.10.0/24, the user device (Lubuntu) on 192.168.20.0/24, and the attacker device (Kali Linux) on 192.168.30.0/24. Communication between subnets is strictly controlled using Access Control Lists (ACLs) applied to the multilayer router. These ACLs function as microsegmentation policies, explicitly defining allowed traffic and implicitly denying all other traffic by default. For example, only specific traffic from the user's subnet to certain ports on the IoT device is permitted. This drastically reduces the attack surface and prevents lateral movement by

attackers. The architectural details can be seen in Figure 3.

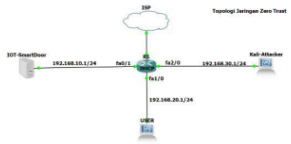

Figure 3. Zero Trust Network Topology

2.2 Smart Door System Implementation

To replicate a realistic Smart Home interaction scenario, a Smart Door application was developed on the IoT device (Ubuntu Server) using the Python-based Flask framework. Flask was chosen for its lightweight and flexible nature, suitable for simulating resource-constrained IoT devices. This application simulates the function of a smart door lock that can be operated via a web interface, allowing users to virtually "lock" or "unlock" the door. The application interface was designed to be simple and intuitive, as shown in Figure 4.

In the traditional network scenario, interaction between the user device and the Smart Door application occurred via the standard HTTP (Hypertext Transfer Protocol) protocol, running on port 8080. The choice of HTTP is based on the fact that many IoT devices, especially older or less secure models, still use unencrypted communication, which is inherently vulnerable to eavesdropping. Conversely, in the Zero Trust topology, communication between the user and the Smart Door was encrypted using HTTPS (Hypertext Transfer Protocol Secure), running on port 8443. The implementation of HTTPS involved configuring SSL/TLS (Secure Sockets Layer/Transport Layer Security) certificates on the Flask server, ensuring the confidentiality, integrity, and authentication of transmitted data. This fundamental difference in communication protocols serves as a key variable in evaluating the effectiveness of both security approaches.

Figure 4. Illustration of Smart Door Application Interface

2.3 MitM Attack Simulation

Man-in-the-Middle (MitM) attack simulation phase is the core of this comparative testing. The Kali Linux device was utilized as a comprehensive primary platform for launching various types of cyberattacks, thanks to its extensive collection of security tools. The main focus of this simulation was on exploiting network protocol vulnerabilities through ARP Spoofing[21], [22]. ARP Spoofing is a technique where an attacker sends forged ARP (Address Resolution Protocol) messages to a local network, manipulating the ARP tables on target devices (user and Smart Door). Consequently, network traffic that should flow directly between the user and the Smart Door is redirected through the attacker's device, placing the attacker in the "middle" of the communication. The arpspoof tool was used to execute this attack, continuously sending fake ARP packets.

During this ARP Spoofing attack, packet sniffing tools like Wireshark were simultaneously implemented on the attacker device. Wireshark functions to intercept, capture, and then thoroughly analyze all data traffic transmitted between the user device (Lubuntu) and the Smart Door IoT device. This analysis is crucial for identifying whether sensitive credentials (username and password) or other important information were successfully intercepted and read by the attacker in plaintext format. Additionally, the nmap tool was used to perform port scanning from the attacker's device to the target devices (Smart Door and Lubuntu). Port scanning aims to map open ports and running services on target devices, providing an overview of the exploitable attack surface. The results of packet sniffing and port scanning will then be used to verify the effectiveness of the implemented security measures in both different network topologies.

2.4 Data Collection and Analysis

Equations Primary data collection was performed by capturing network traffic using Wireshark software on the attacker device during the MitM attack simulations. The main focus of quantitative data analysis was to assess the attacker's success in stealing user credentials (username and password) in each network topology. Credentials were considered successfully stolen if they were visible in plaintext format in the Wireshark capture results. Furthermore, several additional quantitative metrics were also measured and evaluated to understand the impact of the security architecture on network performance and security more comprehensively:

1. Credential Interception Success: Judged as binary (successful/failed) based on the visibility of credentials in Wireshark.
2. Network Latency: Measured using the ping command between the user device and the Smart Door, both under normal conditions and during an attack, to monitor the potential

performance impact of security implementation.

3. Data Packet Volume: Observed from Wireshark to note differences in the number and types of packets transmitted and intercepted in both topologies.
4. Port Scanning Results: Recorded from nmap output to identify open/closed/filtered ports, indicating the level of access restriction.
5. Packet Loss (%): Measured during ping to indicate whether there was effective traffic blocking by ACLs.

Specific details regarding the parameters and configurations used in this simulation, including IP addresses, subnets, communication protocols, and ACL configurations, can be found in Table 1, providing a complete overview of the experimental environment and enabling replication.

Table 1. Simulation Parameters and Configuration

Parameters	Traditional Topology	Zero Trust Topology
Main Network Devices	IoT Device (Ubuntu Flask Smart Door), User (Lubuntu), Attacker (Kali Linux)	IoT Device (Ubuntu Flask Smart Door), User (Lubuntu), Attacker (Kali Linux)
Network Segmentation	None, all in subnet 192.168.10.0/24	IoT:192.168.10.0/24 User:192.168.20.0/24 Attacker:192.168.30.0/24
Communication Protocol	HTTP (Port 8080	HTTPS (Port 8443)
Router Specific Configuration	Basic routing configuration	DHCP: Three pools for each subnet ACL: • access-list 100 permit tcp 192.168.20.0 0.0.0.255 host 192.168.10.10 eq 8080 • access-list 100 permit udp any any eq bootps • access-list 100 permit udp any any eq bootpc • access-list 100 permit ip 192.168.10.0 0.0.0.255 any • access-list 100 deny ip any host 192.168.10.10 Implementation of ACL: ip access-group 100 in on interface fa0/1
Attack Tools Used	arpspoof, wireshark, nmap	arpspoof, wireshark, nmap
Attack Objective	Getting credentials, port mapping	Getting credentials, port mapping
Credential Interception	Success (Credentials read in plaintext	Failed (Data encrypted / Traffic blocked)
Average Latency (ms)	12 ms	17 ms
Package Lost (%)	0%	100% (Due to ACL blocking)
PortScanning	Port 8080 is open	Port 8443 (HTTPS) is filtered/restricted access

3. RESULT AND DISCUSSION

In This section presents the detailed results of the simulations performed on both network topologies (traditional and Zero Trust) against Man-in-the-Middle (MitM) attacks, followed by an in-depth discussion regarding the effectiveness of each approach in the context of IoT-based Smart Home security. The discussion will integrate the findings with relevant cybersecurity principles, highlighting the practical and theoretical implications of the obtained results

3. 1 Comparison of Network Vulnerability to ARP Spoofing and Packet Sniffing Attacks

The simulation of Man-in-the-Middle (MitM) attacks through ARP Spoofing and Packet Sniffing techniques forms the core of the comparative vulnerability assessment of the two topologies. The results obtained from these tests reveal significant differences in the security posture between traditional and Zero Trust networks.

Vulnerability in Traditional Network Topology In the traditional network topology, the ARP Spoofing attack simulation, conducted using the arpspoof tool on the Kali Linux device, successfully manipulated the ARP tables on both the user device (Lubuntu) and the IoT device (Ubuntu Server Smart Door). This success strategically positioned the attacker's device in the communication path between the two devices, effectively creating a "man-in-the-middle" scenario. The implications were severe: when the user accessed the Smart Door application via the HTTP protocol, all data traffic, including highly sensitive authentication credentials (username and password), was transmitted in plaintext.

Packet capture using Wireshark on the attacker's device clearly and unambiguously showed that these credentials could be intercepted and read without encryption. This indicates a serious vulnerability to sensitive data interception, which can lead to account compromise, unauthorized access to IoT devices, and severe privacy breaches. This vulnerability is exacerbated by the inherent characteristics of household networks: frequent use of devices with weak default security (e.g., Wi-Fi with weak or widely shared passwords), insufficient network segmentation (allowing an attacker already on the local network to easily move laterally), and weak inherent security in many IoT devices manufactured with a focus on functionality over security. Figure 5 displays an example Wireshark screenshot illustrating the credentials successfully intercepted in the traditional

topology, confirming the real threat of MitM attacks on network architectures relying on implicit trust.

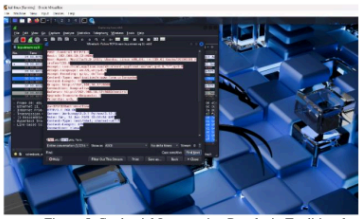

Figure 5. Credential Interception Results in Traditional Network Topology

3.1.1. Strict Subnet Segmentation and Microsegmentation via ACLs

implementation of strict subnet segmentation, where the IoT device (192.168.10.0/24), the user device (192.168.20.0/24), and the attacker device (192.168.30.0/24) reside in separate, logically isolated subnets, fundamentally alters the attack landscape. Communication between these subnets is rigorously controlled by Access Control Lists (ACLs) applied to multilayer router. Specifically, ACL rules such as access-list 100 deny any host 192.168.10.10 applied to interface fa0/1 of the router (the interface connected to the Smart Door's subnet) effectively blocked unauthorized access from the attacker's subnet to the Smart Door device (192.168.10.10). This is a manifestation of the "least privilege" and "explicit verify" principles of Zero Trust, where only traffic explicitly permitted by strict policies is allowed. Consequently, even if the attacker attempted to redirect traffic, the ACLs would deny those packets before they reached their intended destination.

3.1.2. Encrypted Communication using HTTPS

Furthermore, communication between the user and the Smart Door application was encrypted end-to-end using HTTPS (running on https://192.168.10.10:8443/). This constitutes a crucial defense layer at the application level. Even if traffic was successfully intercepted by the attacker (e.g., if the attacker managed to bypass other security layers or if there was a misconfiguration), its content would be ciphertext that could not be read or understood without the appropriate decryption key. Thus, attempts to intercept credentials by Wireshark on the attacker's device would only display encrypted data lacking informative value, as shown in Figure 6. These results empirically prove the Zero Trust principle of rejecting implicit trust and verifying every access at every layer (network and application), significantly reducing the risk of sensitive data interception.

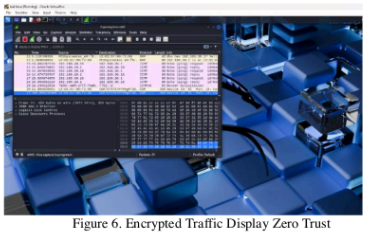

Figure 6. Encrypted Traffic Display Zero Trust

3. 2 Analysis of Port Security and Access

Beyond credential interception, port scanning is a common method used by attackers to identify potential vulnerabilities within a network. The analysis of port scanning results reveals a striking difference between the two topologies.

Open Vulnerabilities in Traditional Topology In the traditional topology, port scanning tests using the nmap tool from the attacker's device (Kali Linux) clearly showed that various ports on both the IoT device (Smart Door) and the user device were open and identifiable. These ports included, but were not limited to, those used for the Smart Door application services (HTTP port 8080) as well as potential other services that might be running by default on the operating system (e.g., SSH, FTP, or other network services). The absence of specific filters or access restrictions configured on the traditional network allowed the attacker to easily map running services and discover potential security loopholes. The attacker's ability to access services like curl or obtain credentials unhindered, as demonstrated in the previous section, provides evidence that this network is vulnerable to further exploitation and possesses a broad attack surface. Every open port represents a potential entry point for attackers. Figure 7 presents an example of nmap output showing the open ports detected in the traditional topology.

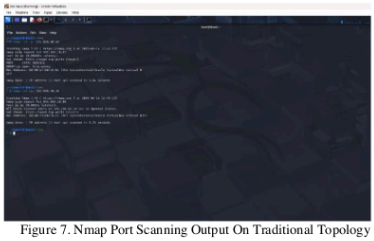

Figure 7. Nmap Port Scanning Output On Traditional Topology

Effective Access Restriction in Zero Trust Topology On the other hand, the Zero Trust topology demonstrated a significant improvement in security regarding access restriction and port protection. With network segmentation via VLANs and strict ACL

implementation, port scanning from the attacker's subnet to the Smart Door IoT device (192.168.10.10) largely failed or showed irrelevant/filtered ports. The ACL rule access-list 100 permit tcp 192.168.20.0 0.0.0.255 host 192.168.10.10 eq 8443 selectively permitted only TCP traffic from the user's subnet (192.168.20.0/24) to the Smart Door device on port 8443 (HTTPS). Other traffic from the attacker's subnet was implicitly denied by the ACL (implicit deny), or explicitly denied by a more specific rule access-list 100 deny ip any host 192.168.10.10.

This ensures that only authorized and verified traffic can reach the IoT device, significantly minimizing the attack surface and preventing attackers from freely exploring ports. When an attacker attempts port scanning, they will find that most ports are closed or filtered, providing very limited information about the target network's configuration. This is a direct demonstration of the principles of least privilege and microsegmentation within the Zero Trust architecture, where every connection and access must be explicitly authorized. Figure 8 displays the nmap output indicating closed or inaccessible ports in the Zero Trust topology, proving the effectiveness of this approach in reducing the exploitable footprint for attackers.

Figure 8. Nmap Port Scanning Output on Zero Trust Topology

3.3. Implications of HTTPS Encryption in the Context of Zero Trust and Smart Home

The implementation of the Hypertext Transfer Protocol Secure (HTTPS) protocol for the Smart Door application in the Zero Trust topology is a crucial factor that directly contributes to the overall enhancement of the security posture. Unlike Hypertext Transfer Protocol (HTTP) communication in the traditional topology, which is inherently vulnerable to plaintext interception, HTTPS ensures that all communication between the user and the Smart Door, including requests, data responses, and highly sensitive authentication credentials, is encrypted end-to-end.

This encryption process fundamentally alters the nature of data traffic; it transforms information that was previously easily readable into ciphertext that cannot be deciphered without the appropriate decryption key. Thus, packet sniffing attempts by attackers become ineffective for obtaining meaningful information, as intercepted data remains protected in encrypted form. HTTPS utilizes the SSL/TLS protocol, which provides three core security services: encryption (protecting data confidentiality), data integrity (ensuring data is not modified in transit), and authentication (verifying the identity of the server, and optionally the client, to prevent impersonation). The effectiveness of HTTPS in protecting data privacy and integrity is a fundamental difference that separates the security of the Zero Trust topology from the weaknesses of conventional topologies.

Although strict network segmentation and the implementation of Access Control Lists (ACLs) have provided strong layers of isolation and access control at the network level (OSI Layer 3 and 4), HTTPS encryption acts as a vital additional defense layer at the application level (OSI Layer 7). The presence of this encryption layer effectively addresses potential weaknesses that might arise if an attacker somehow manages to breach network defenses (e.g., through zero-day vulnerabilities or undetected misconfigurations) or if they are already within a "permitted" network segment but not the direct target (lateral movement). In such scenarios, even if an attacker manages to intercept packets, they still cannot extract useful data due to the encryption protection applied by HTTPS. This is a perfect illustration of the "Assume Breach" principle in Zero Trust, where every layer must be secured as if a breach has already occurred at another layer.

In the context of Smart Home environments, where Internet of Things (IoT) devices often have limited computational resources, slow patching cycles, and potential inherent vulnerabilities in firmware or hardware, the use of HTTPS becomes a critically important last-line defense mechanism to protect user privacy and security. Resource limitations on IoT devices can complicate the implementation of complex security controls at the device level itself, such as advanced Intrusion Prevention Systems (IPS) or endpoint security solutions. Therefore, ensuring that core data communication is encrypted becomes paramount as a primary line of defense. This evidence significantly strengthens the argument that the Zero Trust architecture, with its emphasis on "always verifying" every access and securing communication individually without assuming trust, is highly suitable for inherently vulnerable and often targeted IoT environments. HTTPS encryption not only fulfills the "explicit verification" principle of Zero Trust but also strengthens the overall security posture, even in the face of internal or lateral threats within segmented networks.

4. CONCLUSION

In This study has successfully demonstrated the comparative effectiveness of the Zero Trust architecture in enhancing Smart Home network security against Man-in-the-Middle (MitM) attacks compared to traditional security approaches. Through

virtual environment simulations, it was found that traditional topologies, which rely on perimeter-based security and HTTP communication, are highly vulnerable to attacks such as ARP Spoofing and Packet Sniffing, allowing for free credential interception and port mapping. This vulnerability is exacerbated by the lack of adequate segmentation and access restrictions.

Conversely, the implementation of Zero Trust, involving strict network segmentation, selective Access Control List (ACL) enforcement, and the use of HTTPS encryption, significantly reduces the attack surface and mitigates the risk of data interception. Testing results show that credential interception attempts on the Zero Trust topology failed due to encrypted data and unauthorized traffic being blocked by ACLs. Port access restrictions also proved effective, limiting attackers from performing network exploration. The advantage of Zero Trust lies in its rejection of implicit trust assumptions and its reinforcement of the "never trust, always verify" and least privilege principles, which are realized through communication segmentation and encryption.

The implications of this research highlight that the application of the Zero Trust architecture, supported by encryption at the application layer, is an adaptive and effective strategy for securing IoT devices in increasingly complex and vulnerable Smart Home environments. Although implementation challenges such as limited device resources and identity management complexity may exist, the security benefits offered by Zero Trust far outweigh these risks.

This study recommends the adoption of Zero Trust principles as a security foundation for future Smart Home systems, aiming to create a more resilient and protected environment against evolving cyber threats. For future research, it is suggested to explore Zero Trust implementation on physical IoT hardware to validate findings in real-world scenarios, as well as to investigate the impact of Zero Trust on the performance of larger and more diverse Smart Home networks. Furthermore, the development of lighter and more automated identity and authentication mechanisms for low-power IoT devices within a Zero Trust framework also represents a promising area for future research.

Acknowledgment

The authors express deep appreciation for the availability of scientific literature and journals that have served as a fundamental basis for developing the understanding and simulation design of this research. The academic environment at Mercubuana University has also provided a conducive atmosphere for the conduct of this research

5. REFERENCE

[1] A. Roy, A. Dhar, and S. S. Tinny, "Strengthening IoT Cybersecurity with Zero Trust Architecture: A Comprehensive Review," 2024, doi: 10.61424/jcsit.

[2] A. Johanes, N. Filzah, M. Radzuan, and Z. H. Abdullah, "Implementation of A Zero-Trust Approach in Smart Home Among the Houseowners in Kota Kinabalu, Sabah."

[3] "Evaluasi Pengujian Keamanan Arsitektur Zero Trust Network Pada Jaringan Smart Home Untuk Mengatasi Serangan Data Sniffing." [Online]. Available: https://lib.mercubuana.ac.id

[4] S. Supiyandi, C. Rizal, M. Iqbal, M. N. H. Siregar, and M. Eka, "Smart Home Berbasis Internet of Things (IoT) Dalam Mengendalikan dan Monitoring Keamanan Rumah," *Journal of Information System Research (JOSH)*, vol. 4, no. 4, pp. 1302–1307, Jul. 2023, doi: 10.47065/josh.v4i4.3822.

[5] Y. Kusnanto, M. A. Nugroho, and R. Kartadie, "JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika) Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi IMPLEMENTASI ZERO TRUST ARCHITECTURE UNTUK MENINGKATKAN KEAMANAN JARINGAN: PENDEKATAN BERBASIS SIMULASI," vol. 9, no. 4, pp. 2357–2364, 2024, doi: 10.29100/jipi.v4i1.6943.

[6] P. Srinivasan, "Zero Trust Network Architecture."

[7] H. Zhang, Q. Wang, X. Zhang, Y. He, B. Tang, and Q. Li, "Toward Zero-Trust IoT Networks via Per-Packet Authorization," *IEEE Communications Magazine*, 2024, doi: 10.1109/MCOM.001.2300390.

[8] Z. Adahman, "ZERO-TRUST ARCHITECTURE AND ITS COST-

EFFECTIVENESS ON NETWORK SECURITY A Paper."

[9] A. Talan, "Zero Trust Network Access with Cybersecurity Challenges and Potential Solutions MSc Research Project M.Sc. in Cybersecurity."

[10] A. Z. Alalmaie, P. Nanda, and T. X. He, "ZT-NIDS: Zero Trust-Network Intrusion Detection System Validation based on Attack Simulations." [Online]. Available: https://orcid.org/0000-0001-8962-540X

[11] M. Andreou and R. Project, "Zero Trust Network Security Model in containerized environments," 2020.

[12] N. I. Roslan, N. T. Mazman, and N. F. A. Johari, "Zero Trust Architecture: A Paradigm Shift in Network Security," Jul. 22, 2024. doi: 10.36227/techrxiv.172165641.12548858/v1.

[13] A. Gokhale and S. Kulkarni, "Enhanced Zero Trust Implementation -- a novel approach for effective network policy management and compliance tracking," May 27, 2023. doi: 10.22541/au.168517996.68474374/v1.

[14] M. A. Allouzi and J. Khan, "Enabling Zero Trust Security in IoMT Edge Network."

[15] P. Dhiman *et al*., "A Review and Comparative Analysis of Relevant Approaches of Zero Trust Network Model," Feb. 01, 2024, *Multidisciplinary Digital Publishing Institute (MDPI)*. doi: 10.3390/s24041328.

[16] N. Faizah Rozy, I. Muhamad Malik Matin, T. Informatika, F. Sains dan Teknologi, and U. Syarif Hidayatullah Jakarta, "UJI KERENTANAN SMART HOME MENGGUNAKAN METODE SQUARE UNTUK MENDUKUNG SMART CAMPUS," 2021.

[17] H. Fereidouni, O. Fadeitcheva, and M. Zalai, "IoT and Man-in-the-Middle Attacks," Aug. 2023, doi: 10.1002/spy2.70016.

[18] R. Rahman, A. F. Rahman, and S. Artikel, "Technology Sciences Insights Journal Penerapan Zero Trust Network Access (ZTNA) dengan penggunaan CAPTCHA pada website umum INFORMASI ARTIKEL ABSTRAK," 2024.

[19] W. R. Simpson and K. E. Foltz, "Resolving Network Defense Conflicts with Zero Trust Architectures and Other End-to-End Paradigms," *International Journal of Network Security & Its Applications*, vol. 13, no. 1, pp. 1–20, Jan. 2021, doi: 10.5121/ijnsa.2021.13101.

[20] R. Syrotynskyi, I. Tyshyk, O. Kochan, V. Sokolov, and P. Skladannyi, "Methodology of network infrastructure analysis as part of migration to zero-trust architecture ⋆," 2024.

[21] N. F. Syed, S. W. Shah, A. Shaghaghi, A. Anwar, Z. Baig, and R. Doss, "Zero Trust Architecture (ZTA): A Comprehensive Survey," 2022, *Institute of Electrical and Electronics Engineers Inc*. doi: 10.1109/ACCESS.2022.3174679.

[22] P. Phiayura and S. Teerakanok, "A Comprehensive Framework for Migrating to Zero Trust Architecture," *IEEE Access*, vol. 11, pp. 19487–19511, 2023, doi: 10.1109/ACCESS.2023.3248622.

SIngh

ORIGINALITY REPORT

9%	7%	5%	4%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Universitas Khairun Student Paper	1%
2	Submitted to University of Western Sydney Student Paper	1%
3	jurnal.stkippgritulungagung.ac.id Internet Source	1%
4	Ahmed A. Abd El-Latif, Mohammed A ElAffendi, Mohamed Ali AlShara, Yassine Maleh. "Cybersecurity, Cybercrimes, and Smart Emerging Technologies", CRC Press, 2025 Publication	<1%
5	community.spiceworks.com Internet Source	<1%
6	blog.ccna.com.br Internet Source	<1%
7	Submitted to Uxbridge College, Middlesex Student Paper	<1%
8	Yongjun Ren, Zhiming Wang, Pradip Kumar Sharma, Fayez Alqahtani, Amr Tolba, Jin Wang. "Zero Trust Networks: Evolution and Application from Concept to Practice", Computers, Materials & Continua, 2025 Publication	<1%
9	ejournal.ikado.ac.id Internet Source	<1%

10	h-o-m-e.org Internet Source	<1 %
11	Partha Pratim Ray. "Web3: A comprehensive review on background, technologies, applications, zero-trust architectures, challenges and future directions", Internet of Things and Cyber-Physical Systems, 2023 Publication	<1 %
12	Submitted to Sheffield Hallam University Student Paper	<1 %
13	www.grandviewresearch.com Internet Source	<1 %
14	Submitted to Whitecliffe College of Art & Design Student Paper	<1 %
15	ccnaclass.blogfa.com Internet Source	<1 %
16	files.eric.ed.gov Internet Source	<1 %
17	www.globalsign.com Internet Source	<1 %
18	ebin.pub Internet Source	<1 %
19	su.diva-portal.org Internet Source	<1 %
20	"Artificial Intelligence Based Smart and Secured Applications", Springer Science and Business Media LLC, 2025 Publication	<1 %
21	Nicola d'Ambrosio, Giulio Capodagli, Gaetano Perrone, Simon Pietro Romano. "SCASS:	<1 %

	Breaking into SCADA Systems Security", Computers & Security, 2025 Publication	
22	ejournals.itda.ac.id Internet Source	<1 %
23	insights2techinfo.com Internet Source	<1 %
24	www.coursehero.com Internet Source	<1 %
25	www.diva-portal.org Internet Source	<1 %
26	Peter T. Davis. "Securing and Controlling Cisco Routers", Auerbach Publications, 2019 Publication	<1 %
27	Gururaj H L, Spoorthi M, Vinayakumar Ravi, Shreyas J, Kumar Sekhar Roy. "Securing the Future", Springer Science and Business Media LLC, 2024 Publication	<1 %
28	William J. Buchanan. "Introduction to Security and Network Forensics", Auerbach Publications, 2019 Publication	<1 %

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	On		