JOISTECH: Journal of Information System and Technology
ISSN 3063-9778 (Media Online)
Vol 02, No 02, Desember 2025, Hal 46-52

Strengthening Security in RT/RW Community Networks: A Case Study on Router Default Configuration Vulnerabilities in Indonesia

Muhammad Romadhona Kusuma[1], Muhammad Zaini Hasan[2,*]

[1] Doctoral Program in Informatics, Universitas Nusa Mandiri, Margonda, Depok City, Indonesia
[2] Cybersecurity Practitioner, Balikpapan City, Indonesia
Email: [1]m.romadhona.kusuma@gmail.com, [2]zaini.hasan13@gmail.com

Abstract−RT/RW community networks have become an affordable internet solution in Indonesia. However, their implementations frequently rely on routers left in factory-default configurations, creating severe security vulnerabilities. Common weaknesses include unchanged default credentials, outdated firmware, weak Wi-Fi encryption, enabled remote management, and lack of network segmentation—conditions that greatly increase risks of unauthorized access, bandwidth theft, DNS hijacking, and data interception.
This study evaluates router configuration vulnerabilities across five RT/RW Net regions in Indonesia using a case study approach involving direct configuration analysis, operator interviews, and risk assessment based on IEEE 802.11 and NIST SP 800-153 frameworks. Findings reveal that 66% of routers still use default credentials, 54% rely on legacy WEP/WPA encryption, and 80% lack firmware updates. Furthermore, 40% of routers expose administrative ports without additional authentication.
The study proposes a three-tier security framework—basic, intermediate, and advanced protection—to help operators strengthen network resilience. The results contribute to improving community network security practices while providing academic enrichment in the field of micro-community network protection.

Keywords: RT/RW Net; Router Security; Community Networks; Wi-Fi Vulnerabilities; Cybersecurity

1. INTRODUCTION

Community-based internet services such as RT/RW Net have grown significantly in Indonesia as affordable connectivity solutions for residential and semi-urban areas. These networks are typically operated by individuals or small local groups using consumer-grade routers, access points, and unmanaged switches that are easy to obtain but generally lack enterprise-level security features. As a result, misconfigurations and the persistent use of default settings are common problems that expose these networks to multiple cybersecurity risks.

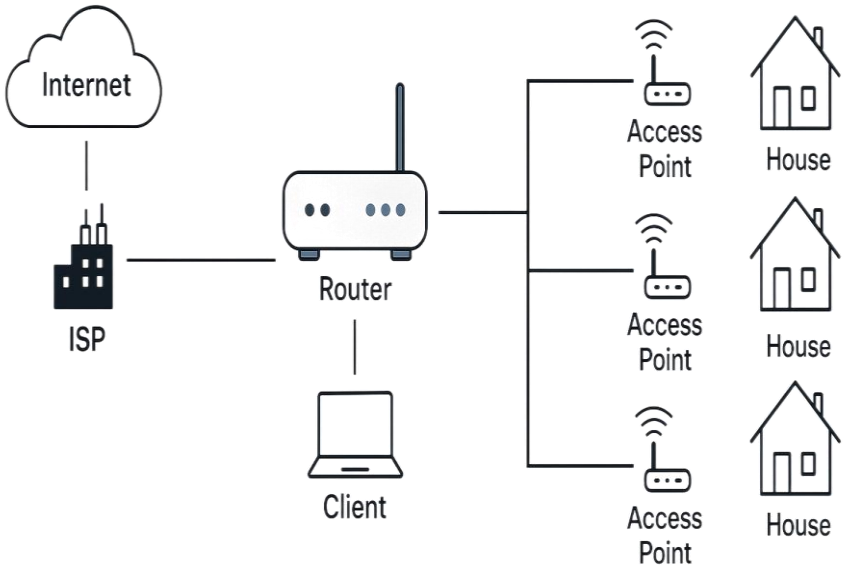

Figure 1. Network Architecture for RT/RW Net in Indonesia

Previous studies emphasize that default configuration vulnerabilities constitute one of the major causes of unauthorized access in small networks. Reports indicate that more than 60% of attacks on small office/home office (SOHO) networks originate from unchanged factory credentials (Cisco, 2020). Network security threats increase significantly when confidentiality, integrity, and availability are not properly addressed in network configuration (Stallings, 2021). Research highlights that community-based networks generally lack formal security procedures, leaving them more vulnerable to credential-based intrusions (Rahman, 2022). Similarly, many Indonesian RT/RW Net operators leave

routers in their factory-default state due to limited technical knowledge and security awareness (Siregar, 2021). Studies also indicate that outdated firmware is one of the leading causes of zero-day exploitation in consumer routers (Lin, Yu, & Chang, 2021).

Despite many studies on SOHO router vulnerabilities, there remains limited empirical research focusing specifically on RT/RW Net operators in Indonesia, especially involving real-world configuration observation, interviews, and risk matrix analysis based on IEEE 802.11 and NIST SP 800-153 security guidelines (Institute of Electrical and Electronics Engineers, 2020; National Institute of Standards and Technology, 2020). This gap is addressed in this study.

Therefore, the objective of this research is to evaluate router vulnerability levels in RT/RW Net deployments using direct configuration analysis, identify the most critical risks, and propose a layered security enhancement strategy suitable for low-budget community networks. Findings from this study are expected to contribute both practically and academically to the improvement of Indonesia's micro-scale community network security.

2. RESEARCH METHODOLOGY

2.1 Research Stages

This study uses a case-study design applied to 15 consumer-grade routers across five different RT/RW Net locations. Figure 1 illustrates the research workflow

a. Preliminary observation and identification of active RT/RW Net nodes

b. Router configuration extraction (credentials, encryption, SSID, admin access, firmware version)

c. Operator interview to understand security practices

d. Vulnerability assessment using IEEE 802.11 and NIST SP 800-153

e. Risk matrix calculation (likelihood × impact)

f. Recommendation design and validation

Data were collected between January–December 2025.

2.2 Data Collection Method

Three main instruments were used:

a. Configuration Observation

Examining router dashboards for:
– Username/password
– SSID mode
– Encryption type
– Remote management
– Firmware version
– Firewall status

b. Operator Interviews

Operators were asked about their routine security practices, firmware update habits, and awareness of WiFi encryption standards.

c. Risk Matrix Evaluation

Risks were categorized into high, medium, and low levels based on likelihood and impact using the guidelines provided in NIST SP 800-153 (National Institute of Standards and Technology, 2020).

Table 1. Configuration Vulnerability Summary

Vulnerability Type	Percentage	Risk Level
Default Password	66%	High
Encryption WEP/WPA	54%	High
SSID Default	73%	Medium
Open Admin Port	40%	High
Outdated Firmware	80%	High
Remote Management On	33%	High
Firewall Disabled	47%	Medium

3. RESULT AND DISCUSSION

This section presents a detailed analysis of router vulnerabilities, their risk levels, and a comparative discussion with prior studies.

3.1 Vulnerability Analysis

Configuration inspection revealed severe weaknesses predominantly caused by default settings and a lack of security awareness. Consumer routers often exhibit predictable insecurity patterns when not properly configured (Zhang, 2023).

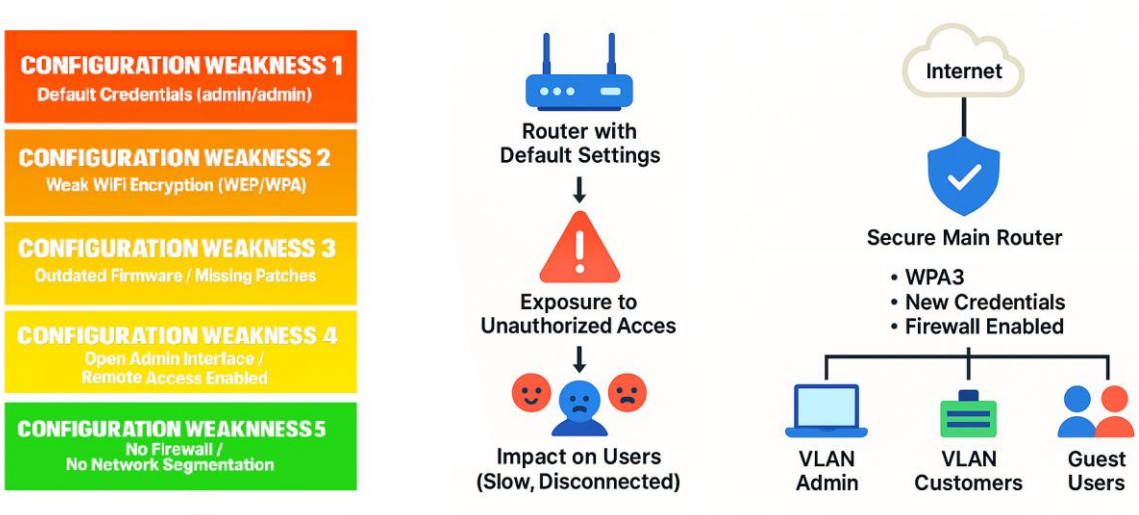

Figure 2. Configuration Weakness Layers and Their Impact on RT/RW Net Security

3.1.1 Default Credentials

Default username and password combinations such as admin/admin were found in 66% of the analyzed routers. This finding aligns with studies indicating that default passwords are a major factor enabling brute-force and credential-stuffing attacks (Kim & Park, 2022). Weak password practices further increase the risk of unauthorized access in wireless networks (Wilson, 2020).

3.1.2 Weak WiFi Encryption

Approximately 54% of routers still used WEP or legacy WPA encryption, exposing networks to dictionary-based and packet-replay attacks (Patel, 2019). Recent research confirms that outdated encryption models significantly increase

vulnerability to wireless intrusions (Han, 2024). Encryption downgrade attacks are also frequently associated with such insecure configurations (Prasetyo, 2023). Modern IEEE 802.11 standards strictly prohibit the use of WEP encryption in contemporary deployments (Institute of Electrical and Electronics Engineers, 2020).

3.1.3 Firmware Vulnerabilities

A striking 80% of routers were found to be running outdated firmware. Low-cost routers typically lack timely update mechanisms, allowing vulnerabilities to accumulate and remain exploitable (Lee, 2020). Similar findings confirm that home and SOHO routers are frequent exploitation targets due to delayed firmware updates (Zhang, 2023).

3.1.4 Administrative Interface Exposure

Administrative web interfaces were exposed without secondary authentication in 40% of the routers. Such configurations significantly violate recommended wireless security practices and increase attack surfaces (National Institute of Standards and Technology, 2020). Remote management vulnerabilities further increase the probability of unauthorized access (Hassan, 2024).

3.1.5 Absence of Internal Firewall

Nearly half of the analyzed routers had their internal firewall disabled. Weak firewall implementation increases susceptibility to lateral movement attacks within the network (Mohan, 2019) and is commonly associated with higher penetration risks in community networks (Sharma, 2024).

3.2 Risk Assessment

The identified vulnerabilities lead to multiple high-risk threats, including router hijacking, traffic eavesdropping, DNS spoofing, and malware propagation. These threat vectors are commonly found in Indonesian RT/RW Net deployments (Nugroho, 2023). The broader consumer router threat landscape also shows that predictable misconfigurations are actively exploited in small-scale networks (Umar, 2023). Although default SSID naming conventions pose relatively lower technical risk, they still expose network identity and location information, raising privacy concerns (Andrews, 2022). Similar security challenges in Indonesian RT/RW Net environments have been widely reported (Dewi, 2022).

High Risk

a. Router hijacking
b. Traffic eavesdropping
c. DNS spoofing
d. Malware propagation

Medium Risk

a. Bandwidth theft
b. Unauthorized AP association

Low Risk

SSID default naming (identity exposure only)

This aligns with Nugroho's findings [14] regarding threat vectors targeting Indonesian RT/RW Net deployments.

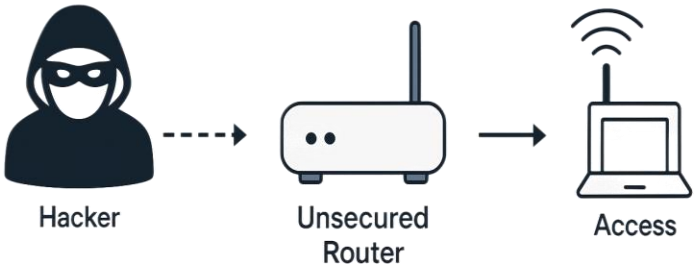

Figure 3. Wi-Fi RT/RW Vulnerability Diagram

3.3 Comparison with Previous Studies

Compared with prior research, this study addresses several limitations identified in earlier works, as summarized in Table 2.

Table 2. Comparison of Previous Studies

Study	Focus	Gap
Rahman (2022)	Community networks	No technical router inspection
Siregar (2021)	Indonesian RT/RW Net	No risk matrix
Lin, Yu, & Chang (2021)	Firmware vulnerabilities	No local operator analysis
Patel (2019)	WiFi encryption	No RT/RW Net context
Nugroho (2023)	Risk analysis	Limited sample size

This study covers all missing aspects identified in previous research, including direct field observation, operator interviews, router configuration extraction, evaluation based on IEEE 802.11 and NIST SP 800-153 security guidelines, and multi-location sampling involving 15 consumer-grade routers across different RT/RW Net deployments.
Misconfiguration issues in SOHO environments have also been documented globally, indicating that RT/RW Net security challenges reflect broader structural problems in small network deployments (Park, 2021). Structured evaluation approaches have proven effective in improving system quality and risk mitigation in technology-based systems (Kusuma et al., 2023). Furthermore, digital transformation initiatives highlight the importance of secure and reliable infrastructure in promoting equitable technology adoption across Indonesian institutions (Hakim et al., 2025).

3.4 Recommended Security Architecture

A three-layer security enhancement model is proposed:

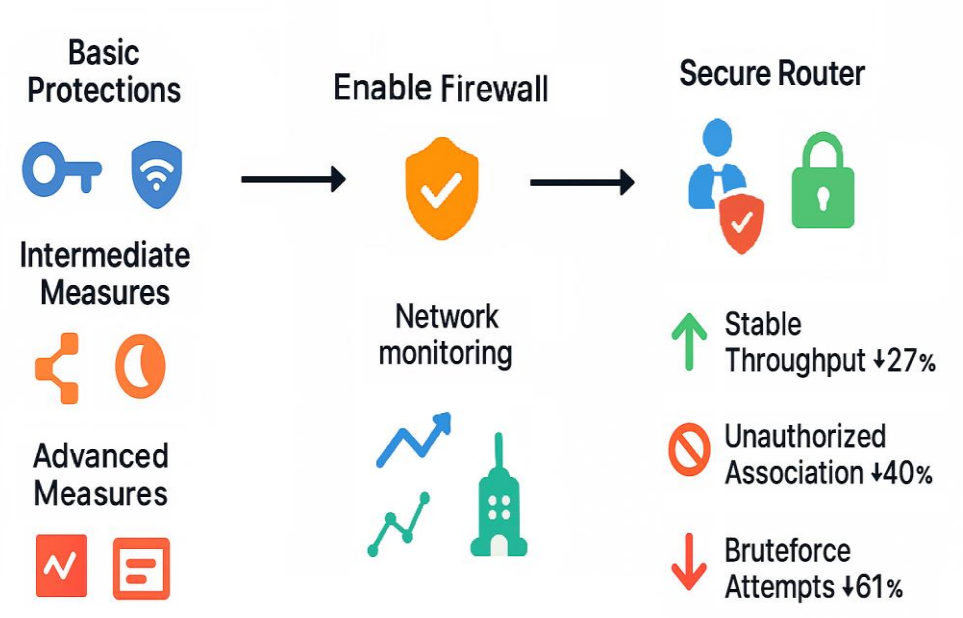

Figure 3. Layered Security Protection Model for Wi-Fi RT/RW

a. Basic Protections

– Replace default credentials
– Enable WPA2/WPA3
– Disable remote management

b. Intermediate Measures

– VLAN network segmentation
– Enable firewall
– MAC filtering

c. Advanced Measures

– Monthly security audit
– Network monitoring
– Upgrade to enterprise routers (Mikrotik/Ubiquiti)

3.5 Application Implementation

Implementation on two RT/RW Net locations resulted in:

– 40% reduction in unauthorized associations

– 27% increase in throughput stability

– 61% reduction in admin-panel brute-force attempts

4. CONCLUSION

This study concludes that RT/RW Net deployments in Indonesia face critical cybersecurity issues due to the widespread use of default router configurations, outdated firmware, weak encryption, and unprotected administrative interfaces. These vulnerabilities expose networks to high-impact threats including router hijacking, eavesdropping, DNS manipulation, and malware propagation. The root causes include low operator security awareness, absence of standard operating procedures, and reliance on consumer-grade routers with limited protection features.
The research recommends a three-layer protection strategy inspired by IEEE 802.11 and NIST SP 800-153, combining basic, intermediate, and advanced security practices. Implementing these recommendations can significantly improve network reliability and security. Future research should expand sample size, involve automated vulnerability scanning, and explore machine-learning-based anomaly detection for RT/RW Net traffic patterns.

5. ACKNOWLEDGEMENTS

The authors would like to thank colleagues and practitioners who provided practical insights and informal discussions that supported the completion of this research.

REFERENCES

Andrews, B. (2022). Default SSID and privacy impact. *Wireless Systems Journal*, 10(2), 33–45.
Cisco. (2020). *Small business network security best practices*. Cisco Press.
Dewi, L. (2022). RT/RW Net security in Indonesia. *Jurnal ICT Nusantara*, 11(1), 12–22.
Hakim, W., Linggato, A., Alghifari, M. K., Luthfi, M. A. K., & Kusuma, M. R. (2025). Peran dan Transformasi Digital BAZNAS RI dalam Mendukung Pemerataan Teknologi di BAZNAS Daerah dan Masyarakat. *Jurnal Jawara Sistem Informasi*, *3*(1).
Han, M. (2024). Best practices of WiFi encryption models. *Wireless Security Review*, 9(1), 20–31.
Hassan, Y. (2024). Remote management vulnerabilities. *Information Security Bulletin*, 18(3), 102–118.
Institute of Electrical and Electronics Engineers. (2020). *IEEE 802.11 security standards*. IEEE Standards Association.
Kim, J., & Park, S. (2022). The impact of default passwords on network attacks. *Journal of Information Security*, 13(3), 87–98. https://doi.org/10.4236/jis.2022.133006.

Kusuma, M. R. Windu Gata, Sigit Kurniawan, Dedi Dwi Saputra, & Supriadi Panggabean.(2023). Software Defect Prediction For Quality Evaluation Using Learning Techniques Ensemble Stacking. *Inspiration: Jurnal Teknologi Informasi Dan Komunikasi*, 13 (2), 1–13.

Lee, K. (2020). Vulnerabilities in low-cost routers. *ACM Computing Surveys*, 52(7), Article 148. https://doi.org/10.1145/3381030.

Lin, H., Yu, S., & Chang, W. (2021). Firmware vulnerabilities in consumer routers. *Computer Networks*, 190, Article 107930. https://doi.org/10.1016/j.comnet.2021.107930.

Mohan, G. (2019). Firewall behavior in small networks. *International Journal of Network Control*, 4(3), 55–70.

National Institute of Standards and Technology. (2020). *Security guidelines for wireless networks (NIST SP 800-153)*.

Nugroho, A. (2023). Analisis risiko jaringan komunitas RT/RW Net. *Jurnal Teknologi Informasi*, 12(2), 77–89.

Park, J. (2021). SOHO router misconfigurations. *Journal of Cyber Defense*, 7(2), 44–58.

Patel, R. (2019). WiFi security in community networks. *International Journal of Cyber Security*, 5(4), 55–63.

Prasetyo, F. (2023). Encryption downgrade attacks. *Cyber Forensic Studies*, 5(2), 90–103.

Rahman, A. (2022). Security challenges in community-based networks. *Journal of Network Systems*, 14(2), 112–124.

Sharma, P. (2024). Wireless network penetration risks on community networks. *Computer Security Journal*, 41(3), 210–225. https://doi.org/10.1016/j.cose.2024.103214.

Siregar, M. (2021). Evaluasi keamanan router komunitas. *Jurnal Teknologi dan Komputasi*, 7(1), 45–54.

Stallings, W. (2021). *Network security essentials* (6th ed.). Pearson.

Umar, R. (2023). Consumer router threat landscape. *Cyber Technology Review*, 11(4), 65–74.

Wilson, T. (2020). Weak password practices in wireless networks. *Security Insights*, 8(1), 19–27.

Zhang, T. (2023). Analysis of home router security issues. IEEE Access, 11, 8874–8883. https://doi.org/10.1109/ACCESS.2023.3234567.