Equivalent: Jurnal Ilmiah Sosial Teknik
Volume 8, Issue 4, 2094-2110
e_ISSN: 2775-0833
https://jurnalequivalent.id/index.php/jequi/index
DOI: doi.org/10.59261/jequi.v8i4.413

Sniffing Risk Assessment in Campus Wi-Fi Infrastructure Using ISO/IEC 27001 and the KAMI Index

Rut Ramayanti Hutomo*
Institut Teknologi Dan Bisnis STIKOM Bali, Indonesia

Roy Rudolf Huizen
Institut Teknologi Dan Bisnis STIKOM Bali, Indonesia

Dandy Pramana Hostiadi
Institut Teknologi Dan Bisnis STIKOM Bali, Indonesia

***Corresponding author:**
Rut Ramayanti Hutomo, Institut Teknologi Dan Bisnis STIKOM Bali, Indonesia.
✉232012020@stikom-bali.ac.id

Article Info:

Article history:
Received: July 10, 2026
Revised: August 24, 2026
Accepted: August 28, 2026
Available Online: November 03, 2026

Keywords:
Information Security Governance;
ISO/IEC 27001;
KAMI Index;
Sniffing Attack;
Wi-Fi Security;

This is an open access article under the CC BY-SA license.

Copyright © 2026 by Author. Published by Cerdika International Cyber Polytechnic

Abstract

Background: Campus Wi-Fi networks are vulnerable to sniffing attacks because of their open-access patterns, diverse user devices, and limited security monitoring.
Objective: This study assesses sniffing risks in a campus Wi-Fi infrastructure by integrating ISO/IEC 27001 control domains and the Indonesian Information Security Index (KAMI).
Methods: A quantitative assessment was conducted using questionnaires administered to five network security experts and 158 students who use the Wi-Fi network. Expert responses were analyzed using Failure Mode and Effects Analysis (FMEA) to identify and prioritize security risks. User responses were assessed through a maturity-level evaluation of various Wi-Fi security aspects using a questionnaire mapped to the relevant ISO/IEC 27001 and KAMI Index domains.
Results: The FMEA identified Network Risk Management and Log Recording as having the highest risk priority, with a Risk Priority Number (RPN) of 576, followed by Communications Security, with an RPN of 360. The maturity assessment of Wi-Fi security aspects indicates that all aspects have reached the Defined stage; however, aspects such as Wi-Fi Technology, Performance, Overload, and Stability remain at the Repeatable stage, with an average score of 2.82.
Conclusion: The combined expert-judgment and maturity assessments indicate that network risk management, log recording, and communications security should receive priority attention. The findings support regular log review, centralized logging, formal incident-response and escalation procedures, and improved capacity and performance monitoring as risk-mitigation priorities. However, these findings should be interpreted as assessment-based recommendations rather than as evidence that the technical controls were directly tested.

To cite this article: Hutomo, R. R., Huizen, R. R., & Hostiadi, D. P. (2026). Sniffing Risk Assessment in Campus Wi-Fi Infrastructure Using ISO/IEC 27001 and the KAMI Index. *Equivalent: Jurnal Ilmiah Sosial Teknik*, 8 (4), 2094-2110. https://doi.org/10.59261/jequi.v8i4.413

INTRODUCTION

The increasingly widespread use of Wi-Fi allows people to access the internet in many places, such as cafes, airports, shopping centers, and educational institutions (Lin et al., 2022; Pahlavan & Krishnamurthy, 2021). Despite this convenience, Wi-Fi use carries considerable security risks. In many cases, Wi-Fi networks do not provide adequate protection, thereby creating opportunities for malicious actors to intercept data transmitted over the network (Palamà et al., 2023; Sinthuja & Sridevi, 2024).

One of the main threats is sniffing. Sniffing is a technique used to intercept network traffic, allowing attackers to steal sensitive information (Tan et al., 2022). Attackers could use artificial intelligence-based algorithms, such as clustering, to detect devices and observe network activities, even though MAC address randomization technology has been implemented to protect user

privacy (Moamin et al., 2025; Sinthuja & Sridevi, 2024; Waqas et al., 2022). This condition could facilitate sniffing to extract personal data, such as usernames and passwords (Brierley et al., 2021; Jin et al., 2024).

The sniffing method can be used for tracking users' locations and for collecting other relevant information, which can be used for other attacks (Kampourakis et al., 2022; Pietraru et al., 2021). Through sniffing, a lot of information can be collected, such as IP addresses, login credentials, session information, users' internet activity, and information about users' devices. Collected information can later be used for different types of attacks, such as unauthorized access, session hijacking, user profiling, and targeted cyberattacks. (El-Taj & Miralam, 2024; Jagannath & Jain, 2024; Kampourakis et al., 2022)

Higher education institutions have increasingly become appealing targets for cyber threats because of the extensive amounts of sensitive data they handle, including academic transcripts, personal information, research findings, and institutional data systems (Alexei, 2021; Bwiino et al., 2026). The open configurations of campus networks, widespread Wi-Fi utilization, high levels of device mobility, and a varied user demographic heighten vulnerability to security risks, especially sniffing attacks that can result in data exposure, theft of credentials, unauthorized access, and interruptions in service (Afolalu & Tsoeu, 2025; Riggs et al., 2023; Zheng et al., 2021). These dangers are exacerbated by varying levels of cybersecurity awareness among users, including poor credential management, insecure application use, and limited capacity to identify cyber threats (Ahmead et al., 2024; Khan et al., 2023). While earlier research has thoroughly investigated sniffing attacks from a technical standpoint, including aspects like packet interception, weaknesses in authentication, detection of attacks, and methods for mitigation (Alamleh et al., 2025; Chatzisofroniou & Kotzanikolaou, 2025; Kampourakis et al., 2022; Pietraru et al., 2021; Vukšić et al., 2025; Rahman et al., 2026). There has been little exploration of these dangers in the context of information security governance. Similarly, studies that reference ISO/IEC 27001 tend to focus on the broader spectrum of information security management, whereas the KAMI is primarily used to assess the maturity level of organizational security without specifically addressing Wi-Fi sniffing risks (Folorunso et al., 2024; Gichubi et al., 2024; Hasibuan, 2024; Jevelin & Faza, 2023; Pratiwi & Wulandari, 2021; Savitri et al., 2024). An analysis of potential risks of sniffing attacks on the Wi-Fi infrastructure in higher education is conducted using the above-mentioned method, through a technical risk assessment based on the KAMI Index and ISO/IEC 27001. This work assesses an organization's information security maturity and provides a detailed analysis of the campus' preparation for information security. Based on this analysis, this work presents a detailed list of possible improvements to information security governance to mitigate risks in the campus' Wi-Fi networks. For the campus examined in this study, no packet-capture experiment, verified sniffing incident log, or penetration-test evidence was used as baseline evidence. Accordingly, the campus-specific urgency is framed as an assessment of potential exposure, risk prioritization, and governance readiness rather than as proof that sniffing attacks have already occurred.

Table 1
Research Gap

Previous Research	Research Gap	How This Study Closes the Gap
Kampourakis et al. (2022); Pietraru et al. (2021); Alamleh et al. (2025); Chatzisofroniou & Kotzanikolaou (2025); Vukšić et al. (2025)	Previous studies have mainly examined sniffing attacks from a technical perspective, including packet data theft, authentication weaknesses, protocol exploitation, detection, and mitigation. However, they have not sufficiently examined sniffing within information security governance and risk management. And no parameter standard measurement.	This study extends the analysis of sniffing threats from a technical issue to a governance-based security risk by integrating technical findings with ISO 27001 controls and the KAMI Index domains.

Folorunso et al. (2024); Gichubi et al. (2024); Jevelin & Faza (2023)	These studies use ISO/IEC standards to assess cybersecurity readiness and information security governance in general, but they do not specifically focus on sniffing risks in Wi-Fi infrastructure.	This study applies selected ISO 27001 controls specifically to Wi-Fi sniffing risks, including A.9 Access Control, A.12 Operations Security, A.13 Communications Security, and A.16 Information Security Incident Management.
Hasibuan (2024); Pratiwi & Wulandari (2021); Savitri et al. (2024)	Previous studies using Index KAMI generally measure information security maturity at the organizational level but rarely connect maturity assessments to specific technical risks, such as sniffing attacks on Wi-Fi networks.	This study links selected Index KAMI domains, namely Technology and Security, Security Framework, and Information Security Risk Management, with the assessment of sniffing risks in campus Wi-Fi infrastructure. The contribution is the explicit linkage of risk priority (FMEA), control relevance (ISO/IEC 27001), and implementation maturity (KAMI Index), enabling mitigation priorities to be derived from both risk criticality and governance readiness rather than from any single framework alone.

The methodological contribution of this study lies in a three-stage risk-to-governance linkage rather than in the mere combination of frameworks. FMEA first prioritizes potential sniffing-related failure modes through severity, occurrence, and detectability; ISO/IEC 27001 then maps those prioritized risks to relevant control domains; and the KAMI Index evaluates the maturity of the corresponding governance practices. Used separately, FMEA cannot indicate organizational control maturity, ISO/IEC 27001 does not prioritize campus-specific failure modes, and the KAMI Index does not identify which sniffing-related risks should be addressed first. Their sequential use therefore produces a risk-prioritized maturity assessment that connects technical threat characteristics with governance controls and actionable institutional priorities.

Based on these issues, this research aims to assess potential sniffing risks in campus Wi-Fi infrastructure, prioritize the most critical security dimensions through expert-based FMEA, and evaluate the maturity of related security practices by mapping ISO/IEC 27001 control domains to the KAMI Index. This research offers a structured basis for linking technical risk priority with information-security governance maturity. In practical terms, the findings are expected to help campus IT managers prioritize logging and monitoring, communications security, incident response, and Wi-Fi capacity management according to the areas where assessed risk and maturity gaps converge.

METHOD

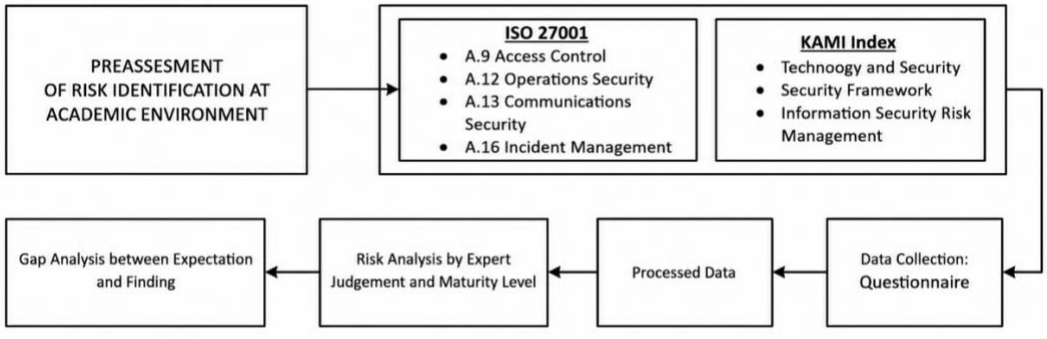


Figure 1. Research Flowchart

This study used a quantitative descriptive risk-assessment design that combined expert

judgment through Failure Mode and Effects Analysis (FMEA) with a questionnaire-based maturity assessment. It did not employ experimental or control groups, treatments, variable manipulation, or pre- and post-test measurements. The assessment mapped potential sniffing-related risks to relevant ISO/IEC 27001 control domains and KAMI Index domains, prioritized the risks through expert ratings, and evaluated users' perceptions of the maturity of related security practices. The resulting gap analysis compared prioritized risk areas with the assessed maturity of current governance practices.

The two frameworks are combined, with ISO/IEC 27001 serving as a control-oriented reference framework for information security. Relevant security requirements are determined using this framework. The KAMI Index is used as a maturity-oriented instrument in organizational contexts to assess the extent to which security controls are implemented consistently and systematically. The integration process is divided into three stages.

1) Characteristics of sniffing threats in campus Wi-Fi infrastructure include unauthorized access to a wireless network, capture of data in transit, stealing of authentication credentials, lack of sufficient logs and monitoring to detect a threat, and insufficient risk identification and incident response.
2) These threat characteristics were mapped to the most relevant ISO/IEC 27001 domains. Access-related risks were mapped to A.9 Access Control. Data interception and transmission protection were mapped to A.13 Communications Security. Network logging and monitoring were mapped to A.12 Operations Security. Incident handling requirements were mapped to A.16 Information Security Incident Management.
3) Each ISO/IEC 27001 domain was linked to the corresponding KAMI Index domain to evaluate the maturity of implementation. For example, access control and password management were linked to the Security Framework domain; logging and monitoring were linked to the Security Framework and Information Security Risk Management domains; and encryption and network protection were linked to the Technology and Security domain. The mapping results for the intersection between ISO27001 and KAMI are shown in Table 2.

Table 2
Domains of ISO 27001 and KAMI Index Dataset

Sniffing Risk Aspect	Threat Characteristic	ISO/IEC 27001 Domain	KAMI Index Domain
Wi-Fi network access control	Unauthorized users or devices may gain access to the wireless network.	A.9: Access Control	Security Framework
Wi-Fi communication protection	Network traffic may be intercepted during data transmission.	A.13: Communications Security	Technology and Security
Data encryption and credential protection	Sensitive data, login credentials, or session information may be captured by attackers.	A.13: Communications Security	Technology and Security
Network logging and monitoring	Sniffing activities may remain undetected due to limited monitoring capability.	A.12: Operations Security	Security Framework
Sniffing risk identification and assessment	Sniffing risks may not be formally identified, assessed, or prioritized.	Integrated across A.9, A.12, A.13, and A.16	Information Security Risk Management
Incident response to sniffing attempts	Security incidents may not be handled quickly or systematically.	A.16: Information Security Incident Management	Information Security Risk Management

The population in this study consists of 5 network security experts in the academic environment and 260 IT users, namely all students in the academic environment in 2024. For the network security experts, this study uses a census, meaning that all members of the population are included in the sample. Therefore, the sample for the network security experts consists of 5 respondents.

For IT users, respondents were recruited purposively from the student population because the maturity questionnaire required active campus Wi-Fi users who were familiar with routine use of the network. Eligibility required current student status, experience using the campus Wi-Fi, and sufficient familiarity with its access and service conditions to provide an informed assessment. A total of 158 eligible IT users participated. Because recruitment was non-probability purposive sampling, the sample is not interpreted as providing a probability-based margin of error.

$$n = \frac{260}{1+260\,(0{,}05)^2}$$

The previously calculated figure was retained only as an initial recruitment target and not as a basis for claiming a 5% sampling margin of error.

The final IT-user sample therefore comprised 158 purposively selected respondents. This sample size was used to provide a sufficiently broad descriptive view of user-perceived Wi-Fi security maturity within the study setting, while the interpretation remains limited to the participating users and does not assume probability-sampling generalizability.

The data for this research were collected by distributing questionnaires to network security experts in an academic environment and to IT users on the campus network. The analysis of the research data started with the assessment of the assets according to the CIA principles – confidentiality, integrity, and availability of information. For each asset, it was assessed whether it contained sensitive or authentication data, whether an unauthorized change to the asset could affect academic or administrative processes, and whether a failure or disruption of the asset would affect access to campus services and network operations. The CIA classification of the assets is shown in Table 3.

Table 3
CIA Criteria

Level	Description
High	Directly affects core systems, sensitive data, or user access.
Medium	Creates moderate or indirect security risk.
Low	Causes only minor impact if compromised.
Very Low	Has negligible impact on security and operations.

The risk analysis of the failure modes was performed by five experts, each using the Five-Expert judgment and the Failure Modes and Effects Analysis (FMEA). For each failure mode, the three parameters Severity (S) (impact on Wi-Fi security), occurrence (O) (of the failure), and detectability (D) (of the failure by existing control mechanisms) were rated by each expert on a scale of 1 to 10. The average ratings for each failure mode of the five experts were calculated. Afterward, the average scores for all failure modes within each dimension were calculated to obtain the dimension-level S, O, and D values. These values were rounded to the nearest whole number and multiplied to obtain the Risk Priority Number (RPN), using the formula:

$$RPN = Severity \times Occurrence \times Detection \quad (2)$$

Description:
Severity (S): The worst impact caused by a failure.
Occurrence (O): How often a failure may occur.
Detection (D): The ability of control measures to detect or manage the failure that occurs.

The expert judgment assessment by FMEA criteria is classified as shown in Table 4.

Table 4
FMEA Criteria

Score	Severity	Occurrence	Detection
1	Very low impact	Very rarely occurs	Very easy to detect
5	Moderate impact	Occasionally occurs	Moderately difficult to detect
10	Very high impact	Very frequently occurs	Very difficult to detect

Before conducting the maturity level assessment, this study first tested the validity and reliability of the questionnaire instrument to ensure that the measurement items were appropriate and internally consistent. The validity test was performed using the Pearson product-moment correlation, correlating each item score with the questionnaire's total score. The formula used in the validity test is presented as follows:

$$r = \frac{n(\Sigma X1X1tot)-(\Sigma X1)(\Sigma X1tot)}{\sqrt{((n\Sigma xi^2-(\Sigma xi)^2)(n\Sigma xtot^2)-(\Sigma x1tot)^2))}} \quad (3)$$

Description:
r = Product-moment correlation
∑Xi = Total score of an item
∑Xtot = Total score of all responses
$\sum xi^2$ = Sum of squared scores of an item
$\sum xtot^2$ = Sum of squared total response scores
∑XiXtot = Sum of the product of an item score and the total score

After the validity test was completed, the reliability test was conducted using Cronbach's Alpha to measure the internal consistency of the questionnaire items. The Cronbach's Alpha formula is presented as follows:

$$r = \frac{n(\Sigma AB)-(\Sigma A)(\Sigma B)}{\sqrt{((n\Sigma A^2)-(\Sigma A)^2)(n(\Sigma B^2)-(\Sigma B)^2))}} \quad (4)$$

Description
r = Correlation coefficient
n = Number of respondents
A = Score of odd-numbered question items
B = Score of even-numbered question items

Maturity tests were employed for data collected from IT users. This study uses the maturity level approach to evaluate how well the processes are designed, implemented, controlled, evaluated, and improved. The maturity test assessment criteria are classified as presented in Table 5.

Table 5
Maturity Test Criteria

Skor	Level
0 – 0,9	Nonexistent
1 – 1,9	Initial/Ad hoc
2 – 2,9	Repeatable
3 – 3,9	Defined
4 – 4,9	Managed
5	Optimized

The analytical flow in this study begins with asset identification and classification based on the confidentiality, integrity, and availability (CIA) principles to determine the value and sensitivity of information assets exposed to sniffing threats. The potential for critical assets is analyzed below to assess the extent to which existing security measures adequately protect them, based on expert judgment. A maturity test from the perspective of IT users is added to this analysis to assess the degree of implementation of the respective security measures in a consistent and

systematic way. The thus-determined parameters of asset criticality, the degree of fulfillment of measures' adequacy, and the maturity of security governance are used in a risk analysis of the resilience of campus Wi-Fi networks against sniffing attacks.

RESULTS AND DISCUSSION

Result

Risk Analysis of Sniffing Attacks on Wi-Fi Networks

The information asset identification phase involves identifying all information resources that could be affected by sniffing attacks on the Wi-Fi network. Information assets are data or system components that are valuable to an organization and are used to support academic and administrative activities. To analyze the threat and the vulnerability in relation to potential risk, information assets affected by sniffing on Wi-Fi networks must first be identified. In the risk analysis, the asset value is assessed using the CIA principles (Confidentiality, Integrity, Availability) as shown in Table 6.

Table 6
Asset Value based on CIA Principle

No	Information Asset	Asset Value	ISO/IEC 27001 Domain	KAMI Index Domain	Reason
1	Student login credentials	High	A.9: Access Control; A.16: Incident Management	Security Framework; Information Security Risk Management	It has been used to log in to the users' academic systems; the logins could then be captured by the sniffer and abused
2	Institutional email	High	A.9: Access Control; A.13: Communications Security	Security Framework; Technology and Security	Contains official communications, academic data, and personal information
3	Student academic data	High	A.9: Access Control; A.12: Operations Security	Security Framework	Sensitive in nature and affects the integrity of academic information
4	Campus application traffic	Medium	A.13: Communications Security	Technology and Security	Information about user activities while the user is transmitting information
5	User IP address	Medium	A.12: Operations Security; A.13: Communications Security	Technology and Security	The communication on the wire can be used to track the activities of users doing network profiling
6	Session cookies	High	A.9: Access Control; A.13: Communications Security; A.16: Incident Management	Security Framework; Technology and Security; Information Security Risk Management	This can be exploited for session hijacking and account takeover
7	System authentication data	High	A.9: Access Control; A.16: Incident Management	Security Framework; Information Security Risk	Primary target of sniffing to gain unauthorized access.

No	Information Asset	Asset Value	ISO/IEC 27001 Domain	KAMI Index Domain	Reason
8	User browsing activity	Medium	A.12: Operations Security; A.13: Communications Security	Management Technology and Security	Reflects internet usage patterns and potential privacy leakage
9	E-learning application data	High	A.9: Access Control; A.12: Operations Security; A.13: Communications Security	Security Framework; Technology and Security	Supports the learning process and contains academic interactions
10	Connected device information	Medium	A.12: Operations Security; A.13: Communications Security	Technology and Security	This can be used to identify targets for further attacks

Assessing the Security Level of Wi-Fi Networks Against Sniffing Activities Using ISO 27001 and KAMI Index

From the perspective of a network security expert, the results of a security assessment of Wi-Fi networks are based on expert judgment. In the context of this work, expert judgment refers to the evaluations of five network security experts with the required knowledge and experience, and a broad view of possible problems. The security assessment criteria have been derived from the domains of ISO 27001 and the KAMI Index dataset. For clarity and brevity, the aggregated results by dimension are presented in Table 7. A detailed description of the scores of all individual items, the average item scores per dimension, the average dimension scores per domain as well as the RPN values per item are not presented in this article. In Table 7, the rounded average scores for S, O, and D per dimension, as well as the corresponding RPN values, are presented.

Table 7
FMEA Assessment Recapitulation

No.	Dimension	S	O	D	RPN
1	Description and Scope of the Wi-Fi System	8	5	5	200
2	Access Point Password Distribution and Access Policy	9	4	4	144
3	Network Risk Management and Log Recording	9	8	8	576
4	Wi-Fi Technology (Performance, Overload, and Stability)	7	5	5	175
5	Access Control (Access Rights and Login Procedures)	9	5	5	225
6	Risk Management and Harmful Content Control	9	5	5	225
7	Personal Data Protection and Log Access Rights	9	5	5	225
8	Communications Security	10	6	6	360

The main problem IT is currently facing with respect to internet access via the campus Wi-Fi network is that the IT department lacks the capacity to monitor, detect, and resolve issues on the network. This problem can be framed within the scope of Network Risk Management and Log Recording. The campus-wide RPN for log use, risk monitoring, and anomaly detection is 576. The main problem for internet access via the Wi-Fi network on campus is the sniffing attack. A sniffing attack is typically silent (i.e., does not cause problems on the network) and can therefore persist for a long time before it is detected by the IT department. This means that, for instance, a data leak or theft of login credentials can persist for months before it is detected through log analysis.

A Maturity Test has been executed to assess the security quality of the IT department's Wi-Fi network from the perspective of its users. A Validity Test and a Reliability Test have also been executed on the Maturity Test. The results are presented in Table 8.

Table 8
Validity Result

Question Items	Pearson Value	Status	Question Items	Pearson Value	Status
1	0.796	Valid	17	0.777	Valid
2	0.813	Valid	18	0.795	Valid
3	0.795	Valid	19	0.802	Valid
4	0.792	Valid	20	0.855	Valid
5	0.849	Valid	21	0.809	Valid
6	0.809	Valid	22	0.836	Valid
7	0.795	Valid	23	0.868	Valid
8	0.854	Valid	24	0.825	Valid
9	0.833	Valid	25	0.865	Valid
10	0.812	Valid	26	0.851	Valid
11	0.838	Valid	27	0.800	Valid
12	0.823	Valid	28	0.839	Valid
13	0.428	Valid	29	0.861	Valid
14	0.432	Valid	30	0.851	Valid
15	0.819	Valid	31	0.823	Valid
16	0.410	Valid	32	0.850	Valid

The validity test results for all questions in this study were highly valid. Pearson correlations for all questions on the research instrument assessing risks to the campus Wi-Fi network from sniffing ranged from .410 to .868. In every instance, the calculated value for each of the questions was greater than the corresponding r-table value of .300, thereby supporting the use of the research instrument for the study's purposes and indicating that use of the research instrument is highly feasible.

Table 9
Reliability Result

Cronbach's Alpha	N of Items
0.760	32

The reliability test for this study's instrument yielded a Cronbach's alpha of 0.760. This score far exceeds the reliability threshold of 0.70, indicating that this instrument has good internal consistency across the dimensions it measures. The maturity of each dimension in this study was assessed against the ISO 27001 framework for information security management and the KAMI Index.

Table 10
Maturity Test Result Per Indicator

Dimension	Indicator No.	Item Score
Description and Scope of the Wi-Fi System	1	3.53
	2	3.60
	3	3.51
	4	3.54
Access Point Password Distribution and Access Policy	5	3.79
	6	3.58
	7	3.60
	8	3.61
Network Risk Management and Log Recording	9	3.51
	10	2.86
	11	3.61
	12	3.51
Wi-Fi Technology, Performance, Overload, and Stability	13	2.85
	14	2.86

	15	2.81
	16	2.77
Access Control, Access Rights, and Login Procedures	17	3.73
	18	3.64
	19	3.48
	20	3.57
Risk Management and Harmful Content Control	21	3.72
	22	3.64
	23	3.52
	24	3.51
Personal Data Protection and Log Access Rights	25	3.59
	26	3.67
	27	3.64
	28	3.53
Communications Security	29	3.50
	30	3.69
	31	3.64
	32	3.57

For the average indicator score of all items on a dimension:

$$Mj = \frac{\sum M_i}{m} \quad (4)$$

Description:
Mj is the maturity score of dimension j,
m is the number of items in that dimension.
For Example:

$$\text{Wi} - \text{Fi Technology} = \frac{2.85 + 2.86 + 2.81 + 2.77}{4} = 2.82$$

Recapitulation of maturity assessment presented in Table 11.

Table 11
Maturity Test Assessment

No	Statement	Score	Category
1	Maturity Test Results for the Aspect of Measurement Description and Scope of the Wi-Fi System	3.55	Defined
2	Maturity Test Results for the Aspect of Access Point Password Distribution and Access Policy	3.6	Defined
3	Maturity Test Results for the Aspect of Network Risk Management and Log Recording	3.38	Defined
4	Maturity Test Results for the Aspect of Wi-Fi Technology (Performance, Overload, and Stability)	2.82	Repeatable
5	Maturity Test Results for the Aspect of Access Control (Access Rights and Login Procedures)	3.61	Defined
6	Maturity Test Results for the Aspect of Risk Management and Harmful Content Control	3.6	Defined
7	Maturity Test Results for the Aspect of Personal Data Protection and Log Access Rights	3.61	Defined
8	Maturity Test Results for the Communications Security Aspect	3.6	Defined

The maturity questionnaire indicates that most assessed Wi-Fi security dimensions were perceived at the Defined level (scores of 3.0-3.9). This finding suggests that respondents perceived formalized policies and recurring practices across most dimensions; it does not by itself verify the technical effectiveness or consistent enforcement of those controls. Reaching the Defined level should therefore be interpreted as evidence of perceived process formalization rather than proof

of fully managed or optimized security performance.

However, the lowest score in our assessment was in the Wi-Fi Technology, Performance, Overload, and Stability dimension, with a score of 2.82, corresponding to the Repeatable level of 2. On the one hand, it can be concluded that there are likely practices on campus for managing Wi-Fi technology. On the other hand, however, these practices are probably mostly based on routines, experiences, or practices that have been repeatedly and informally implemented. In other words, the implementation of existing Wi-Fi management practices has not yet reached the level of controlled, well-managed practices that are defined and consistently implemented. In the context of security, these aspects have serious implications, especially as Overload and/or Stability problems reduce services' availability, decrease users' trust in the network, and make abnormal behavior on the network harder to detect; for example, as sniffing activity will look like normal traffic on an unstable network and thus will be detected later.

The radar chart summarizes maturity scores across the eight assessed dimensions, which ranged from 2.82 to 3.61. Seven dimensions were categorized as Defined, whereas Wi-Fi Technology, Performance, Overload, and Stability remained at the Repeatable level. The pattern suggests comparatively stronger perceived formalization in access policy, access control, personal-data protection, communications security, and risk-related practices, while technical performance and capacity management require more systematic standardization and monitoring (Standardization & Commission, 2022).

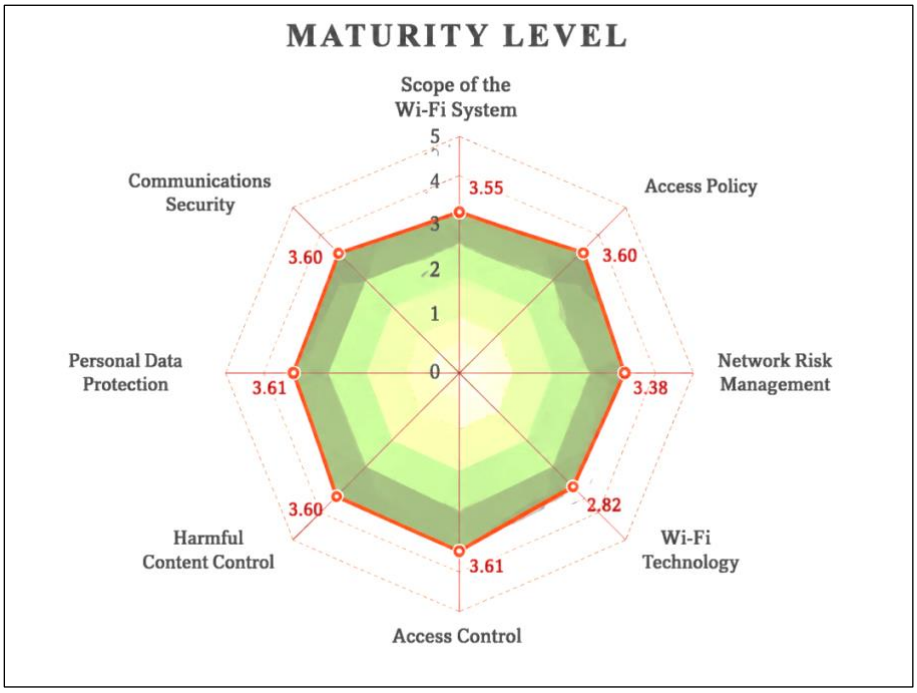


Figure 2. Maturity Level Chart

Recommendations for Sniffing Prevention Mitigation Based on the ISO 27001 Framework and the KAMI Index

The FMEA results indicate that the network risk management dimension represents the area with the highest level of security risk. Meanwhile, the ISO and KAMI assessment results show that Wi-Fi Technology (performance, overload, and stability) in academic institutions is the weakest area of governance. Therefore, this study proposes a set of recommendations, which are further evaluated through gap-closure analysis.

Table 12
Recommendation for Sniffing Prevention

Dimension	Main Gap	Risk Impact	Main Recommendation	Expected Improvement Impact
Network Risk Management and Log Recording	Logs are not reviewed regularly and have not been optimally utilized.	Sniffing activities, MITM attacks, unauthorized access, or network anomalies may be detected late due to the absence of consistent log monitoring.	Periodic log review, centralized logging, and log audit checklist. Moamin et al. (2025); Waqas et al. (2022) ISO/IEC 27001:2022 Control 8.15 Monitoring Activities	Sniffing, MITM attacks, and unauthorized access can be detected more quickly.
Network Risk Management and Log Recording	There is no strong log-based response mechanism.	Suspicious activities are not promptly followed up on, allowing incidents to escalate and recur due to a lack of clear procedures for handling them.	Incident response SOP and escalation flow. Prastowo & Sudiana (2024)	Incidents can be addressed more quickly and documented systematically.
Wi-Fi Technology (Performance, Overload, and Stability)	Network overload during peak hours.	Wi-Fi connections may become slow or unstable, while traffic anomalies become difficult to distinguish from normal user congestion.	Addition of access points, load balancing, and capacity monitoring. Zheng et al. (2021); Riggs et al. (2023); Batista et al. (2024)	Network stability improves, and disruptions decrease.
Wi-Fi Technology (Performance, Overload, and Stability)	Performance monitoring has not been optimized.	Administrators face difficulties in objectively identifying bandwidth conditions, latency, uptime, packet loss, and user load.	Dashboard for bandwidth, latency, uptime, and packet loss monitoring. Chourasiya et al. (2025); Wong & Tan (2025); ISO/IEC 27001:2022 Control 8.16 Monitoring Activities (2022)	Administrators have an objective basis for network improvement.

The gap-closure analysis prioritizes recommendations where high expert-rated risk coincides with lower or less mature governance capability. In particular, the high RPN for Network Risk Management and Log Recording and the lower maturity of Wi-Fi Technology provide a defensible basis for prioritizing monitoring, incident handling, capacity management, and performance visibility. These recommendations are proposed as risk-based improvements; their effectiveness should be verified through subsequent technical testing and operational monitoring.

Accordingly, the study recommends systematic log review, centralized logging, a documented incident-response and escalation process, capacity planning, load balancing, and objective performance dashboards. These measures are expected to improve visibility and response readiness, but the present study does not directly test whether their implementation reduces actual sniffing incidents.

Discussion

Previous studies on Wi-Fi sniffing attacks have mostly focused on the technical details of attacks that can be performed using Wi-Fi sniffing. Those studies describe packet capture, authentication weaknesses, and misuse of wireless protocols, as well as detection methods and ways to combat attacks. Most research studies on Wi-Fi sniffing attacks lack information on managing campus security in general, the information security maturity level of an organization, and handling the risks of an organization's campus Wi-Fi systems. Other related domains, such as physical security, suppliers, and business continuity, have not been studied in this context, since they are not relevant to the technical and governance problems caused by Wi-Fi sniffing attacks. Information security governance using ISO/IEC 27001 and security maturity index using KAMI Index have been studied in a wide organizational context (Folorunso et al., 2024; Gichubi et al., 2024; Hasibuan, 2024; Jevelin & Faza, 2023; Pratiwi & Wulandari, 2021; Savitri et al., 2024). Those studies are not specific to vulnerabilities caused by Wi-Fi sniffing attacks and instead relate to organizational readiness to handle such attacks.

An assessment of information assets at risk from packet sniffing on campus Wi-Fi identified multiple areas susceptible to such attacks. The assessment also conducted a Failure Modes and Effects Analysis (FMEA) to identify the major areas of risk, including Network Risk Management, Log Recording, and Communications Security. While many areas of information security have reached the Defined level of information security maturity for this campus, dimensions regarding campus Wi-Fi Technology, information security system and process performance, the ability of information security staff to manage information security overload, and information security stability have only reached the Repeatable level and therefore have not yet been fully improved. While the technical management of information networks at this campus is not yet standardized and therefore not fully optimized, governance and risk management can be strengthened through improved monitoring and logging of security information and enhanced detection and response to unusual activity. The dominance of Network Risk Management and Log Recording is plausible because sniffing is typically passive and may not create obvious service disruption; consequently, weak telemetry and infrequent log review increase detectability scores in FMEA and elevate the resulting RPN. This interpretation is consistent with studies emphasizing continuous network monitoring and anomaly detection as essential for identifying wireless attacks that otherwise blend into legitimate traffic (Jin et al., 2024; Waqas et al., 2022). The practical implication is that control visibility is as important as preventive access controls: a campus may have authentication and password rules while still lacking timely evidence for identifying suspicious traffic.

This study addressed a knowledge gap by integrating the technical study on the sniffing attacks with corresponding information security governance aspects. Therefore, it is not enough to reduce the technical vulnerabilities of sniffing attacks by relying solely on technical solutions. There are corresponding information security governance systems, risk management frameworks, monitoring systems and organizational readiness to cope with information security incidents that must exist. This study contributes to the body of knowledge by linking information security risks of Wi-Fi networks to information security maturity of organizations. Conceptually, the integration mechanism creates a decision chain that a single framework cannot provide. FMEA identifies where risk is most critical, ISO/IEC 27001 identifies which control domains are relevant to those risks, and the KAMI Index indicates how mature the associated organizational practices are. The theoretical contribution is therefore a risk-prioritized governance assessment in which technical threat characteristics and organizational maturity are interpreted together, rather than as separate security measurements.

The main contribution is not that ISO/IEC 27001, the KAMI Index, and FMEA are individually new, but that their sequential use converts potential sniffing threats into an institutionally actionable priority structure. A high RPN without maturity information would identify risk but not organizational readiness; a maturity score without risk prioritization could encourage equal attention to dimensions with unequal threat consequences. Combining both perspectives helps direct limited campus security resources toward controls where the assessed exposure and governance gap are simultaneously meaningful.

This study makes a local contribution by demonstrating how the integration of ISO/IEC

27001 and the KAMI Index to measure sniffing risks on the Wi-Fi network of campuses in Indonesian higher education was the main objective of this research. This research also provides several viewpoints for improving log monitoring, anomaly detection, communication security, and incident response, thereby enhancing campus information security and overall information security governance. This research can be beneficial to information security researchers in higher education worldwide. This research was based on a campus in a developing country. The resources required to set up information security on campus were limited. The campus network was open and had a heterogeneous user base. The implementation of part of ISO/IEC 27001 controls and the KAMI Index developed in this research were intended for specific situations within given contexts. For higher education institutions with constrained security staffing, this means that improvement programs can be sequenced rather than implemented uniformly: high-priority logging and communications-security gaps can be addressed first, while already-defined access-control practices can be maintained and periodically reviewed. This is a practical implication of the integrated model rather than a claim that the same priorities will apply to every campus.

The current study explores information security practices within higher education institutions. The information security resources available within an organization often depend on the organization's size. As the current study focuses on campus-managed Wi-Fi networks that are open and serve a heterogeneous user base, the results and recommendations obtained in this study will not be fully applicable to very large corporations and government institutions. The current study focuses on the partial implementation of ISO/IEC 27001 controls and the application of the KAMI Index across four domains or perspectives: Technology and Security, Security Framework, Information Security Practices, and Information Security Risk Management. The results and findings of the current study will only be relevant and/or applicable to assessing sniffing risks in campus-managed Wi-Fi networks operated by higher education institutions.

Future studies could include more campuses and organizations and compare them based on, for example, size, network structure, security, and organizational culture. Also, the expert judgment could be strengthened by involving more experts in the study, from different levels and departments within an organization, e.g., network engineers, security officers, system administrators, etc. In a follow-up study, the questionnaire-based maturity assessment could be integrated with a technical verification of information security implementation in real-life cases. For example, to assess sniffing risks on a network, a sniffing attack simulation could be run, and the captured traffic analyzed for interesting information. Also, possible rogue access points could be searched for, and the currently used wireless encryption methods (WPA2/WPA3), as well as other security measures like using VLANs, client isolation, 802.1X, etc., could be verified.

CONCLUSION

In response to the research objective, the combined assessment identifies Network Risk Management and Log Recording as the highest-priority potential risk dimension (RPN = 576), followed by Communications Security (RPN = 360), while the maturity questionnaire places most assessed dimensions at the Defined level and Wi-Fi Technology, Performance, Overload, and Stability at the Repeatable level (2.82). These findings indicate where potential sniffing-related governance weaknesses should be prioritized; they do not demonstrate that sniffing attacks were actually present on the campus network. The study therefore contributes a risk-prioritized governance assessment that links expert-rated threat criticality with perceived maturity of security practices.

Practically, the assessment supports prioritizing centralized logging, periodic log review, formal incident-response and escalation procedures, and stronger capacity and performance monitoring. Future research should validate the framework with direct technical evidence, including controlled sniffing simulations, packet-capture analysis, rogue access-point detection, and verification of WPA2/WPA3 configuration, VLAN segmentation, client isolation, and 802.1X. Multi-campus studies and a larger, more diverse expert panel would also help test the transferability and robustness of the proposed assessment approach.

ACKNOWLEDGEMENT

The authors thank the staff of Institution ABC who supported the expert-judgment process and provided access to relevant documentation required for the campus Wi-Fi sniffing risk assessment.

AUTHOR CONTRIBUTION STATEMENT

The first author conceptualized the study, coordinated the research process, analyzed the data, and prepared the initial manuscript. The second and third authors contributed to validation, supervision, interpretation, and critical revision of the manuscript. All authors reviewed and approved the final version and accept responsibility for the integrity of the work.

REFERENCES

Afolalu, O., & Tsoeu, M. S. (2025). Cybersecurity In Higher Education Institutions: A Systematic Review Of Emerging Trends, Challenges And Solutions. *Future Internet*, *17*(12), 575.

Ahmead, M., El Sharif, N., & Abuiram, I. (2024). Risky Online Behaviors And Cybercrime Awareness Among Undergraduate Students At Al Quds University: A Cross Sectional Study. *Crime Science*, *13*(1), 29.

Alamleh, H., Estremera, L., Arnob, S. S., & Alqahtani, A. A. S. (2025). Advanced Persistent Threats And Wireless Local Area Network Security: An In-Depth Exploration Of Attack Surfaces And Mitigation Techniques. *Journal Of Cybersecurity And Privacy*, *5*(2), 27.

Alexei, L. A. (2021). Cyber Security Strategies For Higher Education Institutions. *Journal Of Engineering Science*, *4*, 74–92. Https://Doi.Org/Https://Doi.Org/10.52326/Jes.Utm.2021.28(4).07

Batista, L. M., Gomes, H., & Almeida, J. R. (2024). A Study Of Security Issues Of Eduroam Networks In Portugal. *13th Symposium On Languages, Applications And Technologies (SLATE 2024)*, 11–14.

Brierley, C., Arief, B., Barnes, D., & Hernandez-Castro, J. (2021). Industrialising Blackmail: Privacy Invasion Based Iot Ransomware. *Nordic Conference On Secure IT Systems*, 72–92.

Bwiino, K., Mayoka, G. K., Nkamwesiga, L., & Nyamadi, M. (2026). A Systematic Literature Review Of Information Security Practices In Higher Education Contexts. *IET Information Security*, *2026*(1), 6324508.

Chatzisofroniou, G., & Kotzanikolaou, P. (2025). Security Analysis Of The Wi-Fi Easy Connect: G. Chatzisofroniou, P. Kotzanikolaou. *International Journal Of Information Security*, *24*(2), 74.

Chourasiya, L., Khatri, S., Lilhore, U. K., Simaiya, S., Alroobaea, R., Baqasah, A. M., Alsafyani, M., & Khan, M. (2025). Advanced System Log Analyzer For Anomaly Detection And Cyber Forensic Investigations Using LSTM And Transformer Networks. *Journal Of Cloud Computing*, *14*(1), 60.

El-Taj, H., & Miralam, L. (2024). Network Sniffing And Its Consequences: A Comprehensive Survey. *International Journal Of Computer Science And Information Security (IJCSIS)*, *22*(3).

Folorunso, A., Mohammed, V., Wada, I., & Samuel, B. (2024). The Impact Of ISO Security Standards On Enhancing Cybersecurity Posture In Organizations. *World Journal Of Advanced Research And Reviews*, *24*(1), 2582–2595.

Gichubi, P. M., Maake, B., & Chweya, R. (2024). Cybersecurity Framework For Kenyan Universities In Conformity With ISO/IEC 27001: 2022 Standard. *Open Access Library Journal*, *11*(8), 1–16.

Hasibuan, M. S. (2024). Analisis Tingkat Kematangan Keamanan Informasi Menggunakan Indeks KAMI Pada Tiyuh Pulung Kencana. *Journal Of Digital Literacy And Volunteering*, *2*(1), 31–37. Https://Doi.Org/10.47747/Jpsii.V2i2.548

Jagannath, R. O., & Jain, A. K. (2024). Browser-In-The-Middle Attacks: A Comprehensive Analysis And Countermeasures. *Security And Privacy*, *7*(5), E410.

Jevelin, J., & Faza, A. (2023). Evaluation The Information Security Management System: A Path Towards ISO 27001 Certification. *Journal Of Information Systems And Informatics*, *5*(4), 1240–1256.

Jin, H. J., Ghashghaei, F. R., Elmrabit, N., Ahmed, Y., & Yousefi, M. (2024). Enhancing Sniffing Detection In Iot Home Wi-Fi Networks: An Ensemble Learning Approach With Network

Monitoring System (Nms). *IEEE Access*, *12*, 86840–86853.

Kampourakis, V., Chatzoglou, E., Kambourakis, G., Dolmes, A., & Zaroliagis, C. (2022). Wpaxfuzz: Sniffing Out Vulnerabilities In Wi-Fi Implementations. *Cryptography*, *6*(4), 53. Https://Doi.Org/Https://Doi.Org/10.3390/Cryptography6040053

Khan, N. F., Ikram, N., Murtaza, H., & Javed, M. (2023). Evaluating Protection Motivation Based Cybersecurity Awareness Training On Kirkpatrick's Model. *Computers & Security*, *125*, 103049.

Lin, Y., Li, Q., Lyu, D., & Wang, X. (2022). A Review Of Wi-Fi-Based Traffic Detection Technology In The Field Of Intelligent Transportation Systems. *Buildings*, *12*(4), 428.

Moamin, S. A. H., Abdulhameed, M. K., Al-Amri, R. M., Radhi, A. D., Naser, R. K., & Pheng, L. G. (2025). Artificial Intelligence In Malware And Network Intrusion Detection: A Comprehensive Survey Of Techniques, Datasets, Challenges, And Future Directions. *Babylonian Journal Of Artificial Intelligence*, *2025*, 77–98.

Pahlavan, K., & Krishnamurthy, P. (2021). Evolution And Impact Of Wi-Fi Technology And Applications: A Historical Perspective. *International Journal Of Wireless Information Networks*, *28*(1), 3–19. Https://Doi.Org/K. Pahlavan And P. Krishnamurthy, "Evolution And Impact Of Wi-Fi Technology And Applications: A Historical Perspective," Int. J. Wirel. Inf. Networks, Vol. 28, No. 1, Pp. 3–19, 2021.

Palamà, I., Amici, A., Bellicini, G., Gringoli, F., Pedretti, F., & Bianchi, G. (2023). Attacks And Vulnerabilities Of Wi-Fi Enterprise Networks: User Security Awareness Assessment Through Credential Stealing Attack Experiments. *Computer Communications*, *212*, 129–140.

Pietraru, R. N., Andrei, Ş., Nicolae, M., & Merezeanu, D. M. (2021). A Wifi Sniffing Solution For Safe Return To Classes. *2021 12th International Symposium On Advanced Topics In Electrical Engineering (ATEE)*, 1–5. Https://Doi.Org/10.1109/ATEE52255.2021.9425125

Prastowo, S. L., & Sudiana, D. (2024). Recommendations For A Framework For Handling Security Incidents Of Electronic-Based Government Systems (SPBE) Using The ISO/IEC 27035: 2023 Standard. *JINAV: Journal Of Information And Visualization*, *5*(1), 107–114.

Pratiwi, H. A., & Wulandari, L. (2021). Evaluasi Tingkat Kesiapan Keamanan Informasi Menggunakan Indeks Keamanan Informasi (Indeks KAMI) Versi 4.0 Pada Dinas Komunikasi Dan Informatika Kota Bogor. *Journal Of Industrial Engineering & Management Research*, *2*(5), 146–163. Https://Doi.Org/Https://Doi.Org/10.7777/Jiemar.V2i5.196

Rahman, R., Ramli, N., & Rahmadani, A. P. (2026). Analisis Keamanan Jaringan Wi-Fi Publik Terhadap Serangan Evil Twin. *Jurnal Riset Sistem Informasi*, *3*(2), 35–38.

Riggs, H., Tufail, S., Parvez, I., Tariq, M., Khan, M. A., Amir, A., Vuda, K. V., & Sarwat, A. I. (2023). Impact, Vulnerabilities, And Mitigation Strategies For Cyber-Secure Critical Infrastructure. *Sensors*, *23*(8), 4060.

Savitri, R., Firmansyah, F., Dworo, D., & Hasibuan, M. S. (2024). Information Security Measurement Using INDEX KAMI At Metro City. *Journal Of Applied Data Sciences*, *5*(1), 33–45. Https://Doi.Org/Https://Doi.Org/10.47738/Jads.V5i1.152

Sinthuja, U., & Sridevi, R. (2024). Selfish Carrier Monitoring In Wifi Using Distributed Sniffers. *Arxiv Preprint Arxiv:2407.10997*. Https://Doi.Org/Https://Doi.Org/10.48550/Arxiv.2407.10997

Standardization, I. O. For, & Commission, I. E. (2022). *ISO/IEC 27001:2022 Information Security, Cybersecurity And Privacy Protection — Information Security Management Systems — Requirements* (3rd Ed.). International Organization For Standardization. Https://Www.Iso.Org/Standard/27001

Tan, S., Ren, Y., Yang, J., & Chen, Y. (2022). Commodity Wifi Sensing In Ten Years: Status, Challenges, And Opportunities. *IEEE Internet Of Things Journal*, *9*(18), 17832–17843. Https://Doi.Org/10.1109/JIOT.2022.3164569

Vukšić, M., Ćelić, J., Panić, I., & Cuculić, A. (2025). Exploiting Maritime Wi-Fi: Practical Assessment Of Onboard Network Vulnerabilities. *Journal Of Marine Science And Engineering*, *13*(8), 1576.

Waqas, M., Tu, S., Halim, Z., Rehman, S. U., Abbas, G., & Abbas, Z. H. (2022). The Role Of Artificial Intelligence And Machine Learning In Wireless Networks Security: Principle, Practice And

Challenges. *Artificial Intelligence Review*, *55*(7), 5215–5261.

Wong, D. Q. S., & Tan, C. E. (2025). Enhanced Load-Aware Handover Algorithm For High-Density IEEE 802.11 ESS Networks. *ECTI Transactions On Computer And Information Technology (ECTI-CIT)*, *19*(4), 635–644.

Zheng, R., Ma, H., Wang, Q., Fu, J., & Jiang, Z. (2021). Assessing The Security Of Campus Networks: The Case Of Seven Universities. *Sensors*, *21*(1), 306. Https://Doi.Org/Https://Doi.Org/10.3390/S21010306