ABDI MASYARAKAT
Vol. 8 No 1 Juni 2026
***P-ISSN**: 2715-8799;**E-ISSN**: 2715-9108*
Link : *http://ejournal.mandalanursa.org/index.php/PB/issue/archive*

Training on the Role of Artificial Intelligence in Network Security for Vocational High School Students at SMK St. Louis Surabaya

Kharisma Monika Dian Pertiwi[1], Emmanuel Satria Anugrah Dewangga[2], Pandu Rafa Panatagama[3], Akbar Muhammad Sadat[4], Alisina Mutirazin Ghazalah Muslimin[5]
[1,2,3,4,5] Informatics, Telkom University, Surabaya, Indonesia

Article Info
Article history:
Accepted: 09 Maret 2026
Publish: 04 Juni 2026

Keywords:
artificial intelligence (AI);
network security;
LSTM autoencoder;
cyber threats;
anomaly detection.

Abstract
A training on the role of artificial intelligence (AI) in network security was conducted for 12th-grade students of the Computer and Network Engineering program at SMK St. Louis Surabaya. The material combined an introduction to cyber threats, AI concepts, the role of AI in network security, a demonstration and hands-on practice of anomaly detection using an LSTM Autoencoder model on a network log dataset via Google Colab. Participant satisfaction evaluation showed a positive response with an average score of 4.265 (scale 1–5). However, the training duration still requires adjustment. Recommendations include adjusting the training duration, implementing quantitative competency assessments, and conducting field tests to measure the model's performance on real network traffic.

Corresponding Author:
Kharisma Monika Dian Pertiwi
Universitas Telkom
Email Coresspoden: kharismamonikadp@telkomuniversity.ac.id

1. INTRODUCTION

Computer networks have become a fundamental infrastructure for information exchange in modern society, supporting communication, learning, and digital services across various sectors, including education. The rapid growth of internet-based technologies has significantly enhanced accessibility and efficiency in educational environments, enabling institutions to adopt digital learning platforms, cloud services, and network-based administrative systems [1], [2]. However, this increasing reliance on network connectivity simultaneously expands the attack surface, making educational networks more vulnerable to cyber threats [3].

Along with the expansion of network utilization, cyber threats have evolved in both scale and complexity. Recent studies report that network-based attacks such as malware propagation, distributed denial-of-service (DDoS), phishing, and unauthorized access continue to increase globally, targeting not only commercial organizations but also academic institutions [4], [5]. Schools and vocational institutions are particularly exposed due to open network architectures, diverse user behavior, and limited cybersecurity awareness among users [6]. These conditions highlight the urgent need for effective network security strategies capable of addressing modern threat patterns.

Conventional network security mechanisms, including firewalls, intrusion detection systems (IDS), and signature-based detection, have long been employed to protect network infrastructures. While these approaches are effective against known attack patterns, they exhibit significant limitations when confronting new or previously unseen threats [7]. Signature-based systems rely heavily on predefined rules and historical attack databases, resulting in reduced detection capability for zero-day attacks and sophisticated intrusion techniques that deviate from

known signatures [8]. Consequently, network administrators face challenges in maintaining proactive and adaptive security defenses.

To overcome these limitations, Artificial Intelligence (AI) has been increasingly adopted in the field of network security. AI-based systems enable automated analysis of large-scale network traffic data and facilitate the identification of abnormal patterns that may indicate malicious activities [9], [10]. Among various AI techniques, anomaly detection has emerged as a critical approach, as it focuses on identifying deviations from normal network behavior rather than relying solely on predefined attack signatures [11]. This paradigm allows security systems to detect unknown or evolving threats more effectively.

Previous studies have demonstrated the effectiveness of deep learning models, particularly Autoencoder and Long Short-Term Memory (LSTM) architectures, in network traffic anomaly detection [12], [13]. Autoencoders are designed to learn compact representations of normal data patterns, while LSTM networks are well-suited for sequential data due to their ability to capture long-term temporal dependencies [14]. Despite promising results in research and industry applications, the integration of AI-based network security concepts into vocational education curricula remains limited. Most students in vocational high schools, especially those in Computer and Network Engineering programs, are still predominantly exposed to conventional network security techniques, creating a gap between academic knowledge, industry practices, and emerging technological demands [15].

In response to this gap, this community service activity focuses on introducing the role and practical application of Artificial Intelligence in network security to students of SMK St. Louis Surabaya through a structured training program. The activity emphasizes conceptual understanding of AI-based network security and hands-on exposure to anomaly detection using an Autoencoder–LSTM model as a representative approach. By presenting AI as a tool for analyzing network traffic behavior and identifying abnormal patterns, the program aims to enhance students' awareness of modern cybersecurity challenges and improve their digital literacy in applying machine learning concepts to real-world network security contexts [16].

2. IMPLEMENTATION METHOD

1.1. Program Target

This community service program was conducted in the form of a structured training for twelfth-grade students of the Computer and Network Engineering (TKJ) program at SMK St. Louis Surabaya who were preparing for graduation. The training aimed to introduce fundamental concepts of network security and highlight the emerging role of Artificial Intelligence (AI) as a supporting tool in modern cybersecurity practices. The learning activities emphasized practical understanding of how AI can be utilized to analyze network traffic behavior and assist technicians in identifying abnormal patterns that may indicate security threats. As a representative case, anomaly detection using an Autoencoder Long Short-Term Memory (LSTM) model was introduced to illustrate how machine learning techniques can be applied to sequential network data. Through this training, students were expected to gain additional insights into AI-driven network security approaches, enhance their digital literacy, and develop relevant competencies that align with current industry demands, particularly as they transition from vocational education to professional or higher education pathways.

Table 1 Attendance List

Class	Attendance
12 TKJ 1	25 Students
12 TKJ 2	15 Students
Total	40 Students

Table 1 presents the attendance distribution of participants involved in the community service training program. The training was attended by students from two twelfth-grade Computer and Network Engineering (TKJ) classes at SMK St. Louis Surabaya. A total of 25 students participated from class XII TKJ 1, while class XII TKJ 2 contributed 15 students. Overall, the program involved 40 students, indicating strong participation from final-year TKJ students who were preparing for graduation. This level of attendance reflects students' interest in enhancing their knowledge and skills in network security and Artificial Intelligence as part of their readiness to enter higher education or the professional workforce.

1.2. Activity Method

The implementation method of the community service program is illustrated in Figure 1. The activity plan was designed by considering the allocated training duration and the instructional approach used to deliver the material effectively. The training was conducted through two face-to-face and interactive sessions held in the Computer and Network Engineering (TKJ) laboratory. These sessions were carried out under the supervision of the head of curriculum coordination and an academic supervisor. In general, the training was delivered by the authors' team, beginning with material presentation and guided discussions to build conceptual understanding, followed by demonstrations and hands-on practice to reinforce learning outcomes. The program concluded with an interactive quiz-based activity aimed at evaluating participants' comprehension while maintaining engagement. The overall sequence and flow of the community service activities are depicted in Image 1.

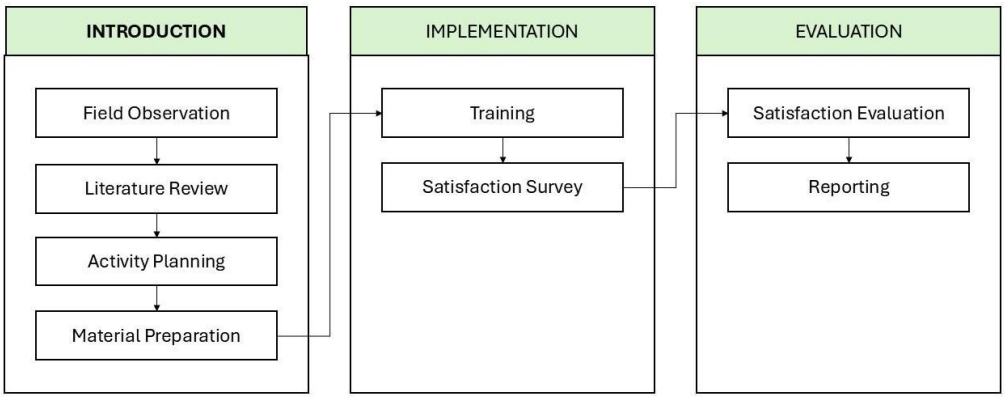

Image 1. Social Service Activity Roadmap

As an evaluation of the training activities, the participants were asked to complete a satisfaction survey to assess their perceptions of the program. The survey was administered in paper-based form and consisted of five statements evaluated using a five-point Likert scale. Response options ranged from 1 to 5, representing *Strongly Disagree (STS)*, *Disagree (TS)*, *Neutral (N)*, *Agree (S)*, and *Strongly Agree (SS)*, respectively. The evaluation statements covered key aspects of the training implementation, including the relevance of the materials to participants' needs, the adequacy of the training duration, the clarity of material delivery, the quality of services provided by the organizing team, and participants' expectations for the continuation of similar activities in the future. This survey instrument was used to capture participants' overall satisfaction and to provide feedback for improving the effectiveness and sustainability of future community service programs as depicted in Table 2.

Table 2 Survey Instrument for Training Evaluation

No.	Statement	Scale
1	The training materials were relevant to the needs of the participants.	1-5
2	The duration and scheduling of the training were appropriate and sufficient.	1-5

3	The training materials were delivered clearly and were easy to understand.	1-5
4	The organizing team provided good services throughout the training activities.	1-5
5	The participants accepted the program and expect similar activities in the future.	1-5

1.3. Training Material

The training materials were developed in accordance with the programming proficiency level of vocational high school students majoring in Computer and Network Engineering (TKJ), using an interactive approach combined with hands-on practice. The training sessions and instructional content were organized as follows:

1. Introduction to hacking types and real-world cases in Indonesia: Students were introduced to several common forms of cyberattacks, including data breaches, system intrusions, and service disruptions. In addition, a real case study of a cyber incident—the ransomware attack on the National Data Center (PDNS) that occurred in 2024—was discussed to raise students' awareness of the severe consequences of cyberattacks on government institutions, which resulted in the disruption of multiple public services.
2. Explanation of the role of AI in network security: This session covered an overview of different types of artificial intelligence, such as Narrow AI and General AI, fundamental concepts of AI and machine learning, and examples of AI applications in the context of network security.
3. Demonstration of anomaly detection using an LSTM Autoencoder model: Students were guided through the execution of an anomaly detection model to identify anomalies within a dataset consisting of 10,000 rows of pre-prepared network log data. The technical workflow—from log data preprocessing and model training to the evaluation of anomaly detection results—was explained in detail to help students understand the underlying processes behind the model's detection mechanism. Google Colab was selected as the implementation platform to facilitate model execution and to introduce students to the practical use of cloud-based development environments.
4. Emphasis on the role of AI: A discussion was conducted to highlight AI as an assistive tool rather than a replacement for network technicians or humans in general, along with an emphasis on the importance of digital literacy and ethical considerations in AI usage.
5. Screening of an awareness campaign video on AI misuse: An educational video addressing the growing risks of deepfake technology was presented, particularly those arising from the careless sharing of facial images and personal information on social media platforms. The session concluded with a discussion and summary of key takeaways from the video content.
6. Quiz-based interactive game session: Students' understanding and awareness of AI ethics and bias were evaluated through an interactive quiz designed to increase engagement and enthusiasm at the conclusion of the training program.

Table 3. Sequential Training Session

No	Session	Duration
1	Introduction to types of hacking and real-world case studies in Indonesia	10 Minutes
2	Explanation of the role of AI in network security	20 Minutes
3	Demonstration of anomaly detection using an LSTM Autoencoder model	60 Minutes
4	Emphasis on the role of AI	5 Minutes

5	Screening of a campaign video on the increasing misuse of AI	10 Minutes
6	Quiz-based game session	15 Minutes

The training was conducted over a total duration of 120 minutes, equivalent to two hours. Prior to the commencement of the game-based session and the conclusion of the training, students were invited to complete a satisfaction survey evaluating the training activities, which they were allowed to submit at any time before the session officially ended.

3. RESULTS AND DISCUSSION

1.4. Face-to-Face Trainning

The training was conducted in an in-person format at the computer laboratory of SMK St. Louis Surabaya and targeted Grade 12 students enrolled in the Teknik Komputer Jaringan (TKJ) program. Each training session was scheduled from 09:40 to 11:40 and was delivered twice over two different weeks to accommodate two separate classes, namely TKJ 1 and TKJ 2. The decision to hold the training in two sessions was made because each participant required access to an individual computer, while the laboratory facilities were not sufficient to serve both classes simultaneously. To ensure the smooth implementation of the activity, the head of the curriculum coordination team assisted at the beginning of each session by introducing the facilitators and briefly overseeing the initial proceedings. Visual documentation of the training opening session is presented in Image 2.

Image 2. Opening of Training Session

In the first week, the training was attended by students from the TKJ 1 class, with a total of 25 participants involved in the activity. A high level of enthusiasm was demonstrated by this group throughout the session, as reflected in their active engagement during discussions and their excitement during the quiz-based game segment. Questions regarding the potential applications of the anomaly detection model were raised by several students, indicating that interest in the demonstrated anomaly detection approach had been generated during the training.

During the second week, students from the TKJ 2 class were assigned as training participants, with 15 students taking part in the activity. In contrast to the first session, most of the questions raised were technical and were primarily focused on the use of the Google Colab platform. Despite this difference, increased enthusiasm was observed during the quiz-based game session, where student participation became more pronounced. Photographs of the students who achieved the highest scores in the quiz activity are shown in Image 3.

Image 3. Awarding Session

The face-to-face training conducted in the laboratory provided an opportunity for students to ask questions and receive immediate responses directly from the facilitators. The training sessions were carried out smoothly and were met with positive attention and feedback from the students as training participants. A photograph of one of the classes, namely the TKJ 2 class after the completion of the training activities, is shown in Image 4.

Image 4. Documentation

1.5. Evaluation

For the evaluation of the training on the role of AI in network security, the satisfaction survey data were processed to obtain statistical information. The survey employed five questions, and each question was assessed using a five-point Likert scale, where the response options ranged from 1 “Strongly Disagree” to 5 “Strongly Agree”.

Table 4. Average Score From Survey

Qn	Question	Average Score
Q1	The activity materials were aligned with the needs of the partners/participants	4.150
Q2	The implementation time was relatively appropriate and sufficient	4.075
Q3	The activity materials presented were clear and easy to understand	4.175
Q4	The organizing committee provided good service throughout the activity	4.500
Q5	The community accepted the activity and hopes that similar activities will be continued in the future	4.425

As described at Table 2, agreement with all five survey statements was demonstrated by the majority of respondents. An overall mean score of 4.265 on a five-point scale indicates a strong positive tendency in participants' responses. The highest levels of agreement were recorded for Q4 and Q5. In contrast, Q2 received the lowest score and the largest proportion of neutral responses, suggesting that greater attention should be given to the scheduling and duration of the activity.

1.6. Discussion

The survey results indicate a high level of participant satisfaction, with an average score of 4.265, particularly regarding the quality of the organizing committee's support and the participants' desire for the continuation of similar activities. In contrast, the timing of the training was identified as an aspect requiring further adjustment. The training approach, which combined conceptual explanations with hands-on practice—specifically the demonstration of an LSTM Autoencoder using Google Colab—was found to be effective in increasing students' interest and initial understanding of AI applications in network security, and it shows strong potential for further development or future implementation. These findings indicate that the applied training approach was effective in introducing AI-based network security concepts. However, further validation is required to assess long-term learning outcomes.

The LSTM Autoencoder demonstration provided students with an end-to-end overview of the AI workflow, covering preprocessing, model training, and evaluation stages, thereby positioning AI not merely as an abstract concept but as a practical tool for anomaly detection. However, since the demonstration relied on a controlled dataset, the model's performance on real network traffic and the students' ability to independently apply the technical procedures have not yet been verified. In addition, a key limitation of the program lies in the evaluation method, which focused solely on participant satisfaction without directly measuring technical competency. These identified implementation limitations offer a broader contextual understanding of the results, and the proposed considerations may be applied to deepen or expand future findings.

4. CONCLUSIONS

Interest and satisfaction among vocational high school students in the TKJ program regarding the role of AI in network security were successfully increased through the training, and a practical application of the LSTM Autoencoder for anomaly detection was introduced to the participants. However, the technical learning impact has not yet been quantitatively assessed, and implementation under real-world conditions remains untested. To enhance the overall effectiveness of the program, adjustments to the training schedule should be made, measurable competency-based evaluations should be incorporated, and field testing using real network traffic

should be conducted. With these recommendations implemented, the program may be developed into a more effective and sustainable model for fostering applied AI literacy and improving the workforce readiness of vocational high school graduates. Future programs may integrate real-time network traffic analysis and structured competency assessments to strengthen both technical and practical learning outcomes.

5. ACKNOWLEDGMENTS

The authors would like to express their sincere appreciation to SMK St. Louis Surabaya for granting permission and providing laboratory facilities that enabled the training program to be carried out effectively. Special thanks are extended to the Head of Curriculum Coordination and the teachers of the Computer and Network Engineering Department for their valuable support in coordinating the activities, introducing participants, and accompanying students throughout the program. The authors also acknowledge the guidance and contributions of the academic supervisor, course lecturers, and the implementation team from the Faculty of Informatics, Telkom University Surabaya, particularly in preparing the training materials, technical arrangements, and academic supervision. Appreciation is further conveyed to the twelfth-grade TKJ students for their active participation as training partners, whose enthusiasm and feedback served as both data sources and motivation for this work. Finally, the authors gratefully recognize all individuals and parties who provided direct and indirect support, including laboratory staff, discussion facilitators, and administrative personnel, whose assistance ensured the smooth execution of the entire program.

6. BIOGRAFFY

[1] S. H. Rafique, A. Abdallah, N. S. Musa, and T. Murugan, "Machine learning and deep learning techniques for Internet of Things network anomaly detection—Current research trends," Sensors, vol. 24, no. 6, p. 1968, 2024. [Online]. Available: https://www.mdpi.com/1424-8220/24/6/1968

[2] M. M. Saeed, "An AI-driven cybersecurity framework for IoT: Integrating LSTM-based anomaly detection, reinforcement learning, and post-quantum encryption," Expert Systems with Applications, 2025. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/11023579/

[3] A. K. S. Ali, A. Raza, and A. A. Hussain, "Machine learning algorithms for threat prediction and anomaly detection in cyber and information security," Scientific Engineering Systems Journal, vol. 4, no. 2, pp. 45–57, 2024. [Online]. Available: https://sesjournal.com/index.php/1/article/view/308

[4] O. O. Adeola and B. K. Alese, "Detection of real-time anomalies in network environment using deep learning," Journal of Current Research, vol. 2, no. 4, 2025, https://journalcurrentresearch.com/pub/jcr/article/download/49/42

[5] S. AR and J. Katiravan, "Enhancing anomaly detection and prevention in Internet of Things (IoT) using deep neural networks and blockchain-based cybersecurity," Scientific Reports, vol. 15, no. 1, pp. 1–18, 2025, doi: 10.1038/s41598-025-04164-4

[6] P. V. Sivarambabu, R. Agrawal, and A. Tirumala, "Enhancing cloud security through AI-driven intrusion detection utilizing deep learning methods and autoencoder technology," in AI and Cloud Security Frameworks, Wiley, 2025, pp. 299–317, doi: 10.1002/9781394209835.ch15

[7] S. Kumari, C. Prabha, and A. Karim, "A comprehensive investigation of anomaly detection methods in deep learning and machine learning: 2019–2023," IET Research Journal, 2024, doi: 10.1049/2024/8821891

[8] M. Puzhakkalaveettil and M. Praveena, "Enhancing security features in wireless sensor networks using AI-based deep learning methods," IEEE Access, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10939339/

[9] K. DeMedeiros, A. Hendawi, and M. Alvarez, "A survey of AI-based anomaly detection in IoT and sensor networks," Sensors, vol. 23, no. 3, p. 1352, 2023. [Online]. Available: https://www.mdpi.com/1424-8220/23/3/1352

[10] M. J. C. S. Reis, "AI-driven anomaly detection for securing IoT devices in 5G-enabled smart cities," Electronics, vol. 14, no. 12, p. 2492, 2025. [Online]. Available: https://www.mdpi.com/2079-9292/14/12/2492

[11] A. R. Tripathi, P. K. Upadhyay, and P. K. Goel, "Deep learning for anomaly detection in industrial networks," in Handbook of AI Applications, IGI Global, 2025. [Online]. Available: https://www.igi-global.com/chapter/deep-learning-for-anomaly-detection-in-industrial-networks/379622

[12] G. Ali, A. Samuel, and M. M. Mijwil, "Enhancing cybersecurity in smart education with deep learning and computer vision: A survey," Mesopotamian Journal of Computer Science and Communication, 2025, doi: 10.58496/MJCSC/2025/008

[13] G. Abdiyeva-Aliyeva and M. Hematyar, "AI-based network security anomaly prediction and detection in future networks," in Advances in Intelligent Systems and Computing, Springer, 2022. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-031-31956-3_13

[14] Y. Wei, "Applying AI-based techniques for DDoS anomaly detection and classification using large-scale datasets," Ph.D. dissertation, Massey Univ., New Zealand, 2024. [Online]. Available: https://mro.massey.ac.nz/handle/10179/69316

[15] N. Nizam, A. A. Rahman, and M. A. Hasan, "Comparative analysis of deep learning models for intrusion detection systems," Journal of Network and Computer Applications, vol. 214, 2025. [Online]. Available: https://www.mdpi.com/2073-431X/14/7/283

[16] M. T. Hasan and I. Ahmed, "AI-driven anomaly detection for data loss prevention and security assurance in electronic health records," RAST Journal, vol. 5, no. 2, pp. 112–125, 2025, doi: 10.63125/dzyr0648