Published by: Fakultas Teknik dan Teknologi Pertahanan, Universitas Pertahanan RI

Journal of Defense Technology and Engineering

Journal homepage: www.research.idu.ac.id/index.php/jdte

Particle Swarm Optimization for Multi Objective Optimization of Intrusion Detection in National Defense Cyber Infrastructure

Muhammad Azhar Prabukusumo[1], Jontinus Manullang[2], Baringin Sianipar[3]

[1] Informatika, Universitas Pertahanan Republik Indonesia, Bogor, Indonesia

[2] Manajemen Informatika, Akademi Informatika dan Komputer Medicom, Medan, Indonesia

[2] Informatika, Universitas HKBP Nomensen, Medan, Indonesia

ARTICLE INFO

Article history:

Received July 01, 2025
Revised July 20, 2025
Accepted July 30, 2025

Keywords:

Cybersecurity;
Intrusion Detection System;
Multi objective Optimization;
Particle Swarm Optimization.

ABSTRACT

Cybersecurity is a critical component of national defense, yet conventional Intrusion Detection Systems (IDS) often face limitations such as high false positive rates, detection delays, and difficulty adapting to dynamic attack patterns, leading to potential blind spots in defense networks. This study aims to design an adaptive IDS that balances detection accuracy, false positives, and operational efficiency through the application of multi objective Particle Swarm Optimization (PSO). Using the CICIDS2017 dataset, which simulates realistic modern network traffic and attack scenarios, we developed and evaluated a PSO optimized IDS model. The experimental methodology included preprocessing, feature selection, model training, and optimization of key performance objectives—maximizing detection rate (DR), minimizing false positive rate (FPR), and reducing latency. The results demonstrate that the proposed PSO IDS achieved a detection rate of 0.96 compared to 0.85 in conventional IDS, reduced the false positive rate from 0.18 to 0.07, and lowered average detection latency from 0.35 seconds to 0.12 seconds. Pareto front analysis confirmed that the multi objective optimization effectively balances conflicting parameters, delivering more robust and resilient intrusion detection. These findings indicate that PSO based multi objective IDS can serve as a practical and scalable solution for strengthening national cyber defense infrastructures, while also providing policy relevant insights on the integration of AI driven optimization methods into defense strategies.

Corresponding Author:

Muhammad Azhar Prabukusumo,
Informatika
Universitas Pertahanan Republik Indonesia
Kawasan IPSC Sentul, Sukahati, Kec. Citeureup, Kabupaten Bogor, Jawa Barat 16810, Indonesia.
Prabukusumo_Azhar@gmail.com

1. INTRODUCTION

Cybersecurity has become one of the most crucial strategic issues in the era of digital transformation, especially when it comes to national defense (Möller, 2023; Stewart, 2023). Modern defense infrastructure that relies on information technology based network and communication systems is vulnerable to cyber attacks that are increasingly complex, adaptive, and unpredictable (Colajanni & Marchetti, 2021; Zhou et al., 2021). Such attacks not only have the potential to disrupt operational stability, but can also threaten national sovereignty (Dan & Pandey, 2024). In this context, Intrusion Detection Systems (IDS) are one of the vital mechanisms used to detect anomalous activity in networks. However, the effectiveness of conventional IDS is often hampered by high false positive rates (FPR), delays in detection (latency), and limitations in dealing with dynamic attack patterns (Abdulganiyu et al., 2024; Alazab et al., 2024). This condition emphasizes the need for a new approach that is more adaptive and capable of optimizing various aspects of IDS performance simultaneously.

The main problem faced is how to design an IDS system that is not only capable of improving detection accuracy, but also reducing false alarms and maintaining the operational efficiency of the defense network. This challenge becomes even more complex due to the need to balance various performance parameters that are often contradictory, such as increasing the detection rate, which can trigger an increase in FPR (Kurniabudi et al., 2020; Oksuz et al., 2021). In the context of national defense, this imbalance can have fatal consequences as it has the potential to create blind spots in the security system.

Previous studies have attempted various approaches, including machine learning and deep learning, to improve IDS performance. Ahmad et al., (2021) discusses the results of a systematic review of ML and DL based NIDS systems, which shows that 60% of studies use DL, 20% use ML, and 20% use hybrid systems, with detection accuracy often reaching >95% on older datasets but decreasing on newer datasets such as UNSW NB15 or CICIDS2017, and still facing problems of high false alarm rates and detection of minority/zero day attacks. Another study by Lansky et al., (2021) discusses a systematic review of deep learning based IDS covering methods such as auto encoder, RBM, DBN, RNN, DNN, CNN, and hybrid, with results showing high detection accuracy (up to >99% on KDDCup99) but declining on new datasets such as NSL KDD, UNSW NB15, and CICIDS2017, and still facing challenges of high false alarms, dataset limitations, and minority/zero day attack detection, thus requiring more adaptive models and representative datasets for further research. Another study by Saranya et al., (2020) Discusses the performance analysis of various machine learning algorithms on Intrusion Detection Systems (IDS) using the KDD'99 dataset, where the experimental results show that the Random Forest algorithm achieves the highest accuracy (99.65%), better than LDA (98.1%) and CART (98%), and confirms that the effectiveness of IDS is highly dependent on the choice of algorithm, dataset size, and application used. These findings indicate that while ML and DL based IDS approaches can achieve very high accuracy on benchmark datasets, their performance often degrades in real world or more recent datasets, highlighting persistent challenges such as false alarms, dataset representativeness, and adaptability to evolving cyber threats.

The objective of this study is to apply multi objective Particle Swarm Optimization (PSO) to improve the performance of Intrusion Detection Systems (IDS) in national defense infrastructure. Unlike conventional approaches that often prioritize a single performance metric, this research emphasizes the simultaneous optimization of multiple critical objectives, namely detection rate, false positive rate, latency, and resource efficiency. By addressing these interdependent factors in a unified framework, the proposed approach ensures that the resulting IDS is not only more accurate but also more adaptive and resilient in facing sophisticated and evolving cyber threats. This is particularly important in defense networks, where even marginal improvements in detection capability or reduction in false alarms can translate into significant enhancements in operational readiness and risk mitigation.

Gap analysis reveals that although a substantial number of studies have explored optimization-based IDS solutions, significant research gaps remain in the specific context of national defense. Most prior works have either focused on generic enterprise networks or applied single objective optimization methods, leaving critical challenges unaddressed in environments that demand higher reliability and robustness. In particular, the application of multi objective optimization techniques to address real-world threats that evolve dynamically has not been sufficiently explored (Chen et al., 2025; Harrison et al., 2020). Defense infrastructures are exposed to unique classes of attacks such as advanced persistent threats (APTs), stealth intrusions, and coordinated distributed campaigns that require IDS models capable of balancing sensitivity and specificity without compromising operational efficiency. This study aims to fill this gap by proposing a more comprehensive, adaptive, and practically deployable IDS model tailored for national cyber defense.

The novelty of this research lies in the integration of PSO with a multi objective optimization framework specifically designed for defense-oriented cybersecurity systems. While PSO has been applied in various domains, its utilization to balance multiple IDS performance trade-offs in critical defense infrastructure remains limited. This work demonstrates that multi objective optimization not only enhances system robustness but also provides a flexible spectrum of solutions along the Pareto Front, enabling decision-makers to select models that align with specific defense priorities, such as prioritizing minimal false positives for operational efficiency or maximizing detection rate for high-threat environments. From a methodological standpoint, the study advances the field by combining rigorous optimization with real-world dataset validation (CICIDS2017), ensuring both theoretical relevance and practical applicability.

Practically, this research provides strong justification for the integration of metaheuristic algorithms into national cybersecurity strategies. The findings highlight that multi objective PSO can significantly improve the adaptability of IDS in responding to modern and emerging threats, thereby reducing vulnerabilities in critical defense systems. Beyond its technical contribution, the study also carries strategic implications: by demonstrating the viability of AI-driven optimization, it encourages policymakers to adopt such adaptive solutions as part of broader cyber defense frameworks. In doing so, the research not only contributes to academic literature but also offers actionable insights for strengthening national cyber resilience in the face of increasingly complex global threat landscapes..

2. RESEARCH METHOD

This study uses a quantitative experimental approach by designing a multi objective Particle Swarm Optimization (PSO) based intrusion detection system. The experiment was conducted using the CICIDS2017 Dataset, which represents normal and anomalous network traffic in a real world corporate simulation environment (Sharafaldin et al., 2018).

The CICIDS2017 dataset was developed by the Canadian Institute for Cybersecurity (CIC), and it is widely recognized as a modern benchmark in intrusion detection research. It mimics real-world corporate network traffic conditions by including both normal activities and a wide variety of attack scenarios. The dataset consists of more than 2.8 million records collected over a five-day period (Monday to Friday). Each record includes over 80 traffic features such as network statistics, protocols, applications, and payloads.

The attack distribution within CICIDS2017 is highly diverse, DoS and DDoS attacks account for approximately 1.2 million records, Brute Force FTP/SSH attacks comprise around 55,000 records, PortScan traffic includes nearly 160,000 records, Web Attacks (such as SQL Injection, XSS, and Brute Force) include more than 2,000 records, Botnet activity adds over 2,000 records, Infiltration attacks are represented by 36 records, and Heartbleed attacks by 11 records. Normal traffic dominates the first day (around 83% of Monday's data), and as the week progresses, various attack types are injected, gradually reducing the proportion of normal traffic. This distribution is particularly valuable for research because it reflects both frequent and large-scale attacks (e.g., DDoS, PortScan) as well as rare but critical threats (e.g., Infiltration, Heartbleed). Compared to older datasets like KDDCup99 or NSL-KDD, CICIDS2017 provides a more balanced structure, better diversity, and closer proximity to real-world conditions, making it an ideal choice for strengthening intrusion detection research in national cyber defense contexts.

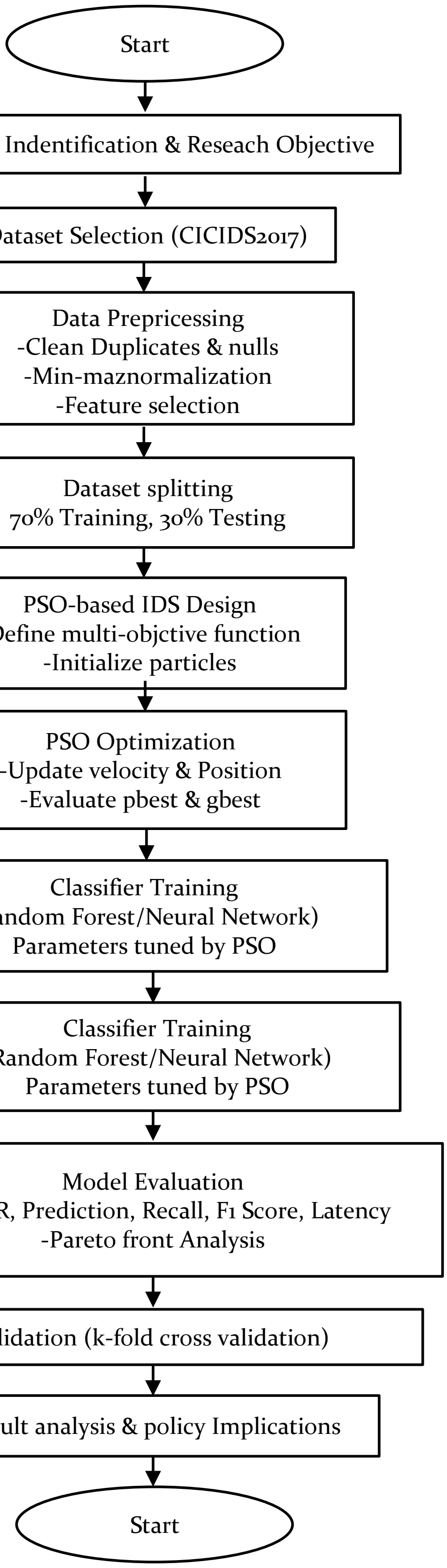
Start
Problem Indentification & Reseach Objective
Dataset Selection (CICIDS2017)
Data Prepricessing
-Clean Duplicates & nulls
-Min-maznormalization
-Feature selection
Dataset splitting
70% Training, 30% Testing
PSO-based IDS Design
-Define multi-objctive function
-Initialize particles
PSO Optimization
-Update velocity & Position
-Evaluate pbest & gbest
Classifier Training
(Random Forest/Neural Network)
Parameters tuned by PSO
Classifier Training
(Random Forest/Neural Network)
Parameters tuned by PSO
Model Evaluation
-DR, FPR, Prediction, Recall, F1 Score, Latency
-Pareto front Analysis
Validation (k-fold cross validation)
Result analysis & policy Implications
Start

Figure 1. Research Flowchart

The research stages began with the data preprocessing process, which included cleaning the data of duplicates and empty values, normalizing the feature scale using min max scaling, and selecting significant features using the information gain or mutual information approach (Chicco et al., 2022; Dhawas et al., 2024). These steps ensure that the model receives high-quality inputs and that irrelevant or redundant attributes are minimized, reducing computational cost while maintaining detection accuracy. After preprocessing, the dataset was divided into two parts, namely 70% for training and 30% for testing, which is a common ratio to balance model learning and independent evaluation. The next stage is the design of a multi objective optimization based intrusion detection model using Particle Swarm Optimization (PSO). At this stage, the objective function is formulated to maximize the detection rate, minimize the false positive rate and latency, and optimize resource efficiency. The optimization process is carried out by initializing particles, evaluating the objective function, and updating the position and velocity of particles based on personal best and global best until convergence is achieved. The IDS model is then built by utilizing classifiers whose parameters are optimized by PSO, such as Random Forest or Neural Network. Performance evaluation is carried out using the metrics of Detection Rate, False Positive Rate, Precision, Recall, F1 score, and Latency, and is further analyzed through Pareto Front visualization to illustrate the trade off between metrics. The final results are then validated using the k fold cross validation approach to ensure model generalization (Gorriz et al., 2024; Yates et al., 2023).

In this study, Particle Swarm Optimization (PSO) is used to optimize multi objective objective functions in intrusion detection (Trivedi et al., 2020; Yong et al., 2020). Each particle represents a candidate solution in the form of intrusion detection model parameters, and its position is updated based on individual experience (personal best, pbest) and global experience (global best, gbest). Unlike other metaheuristics such as Genetic Algorithms or Ant Colony Optimization, PSO requires fewer parameters and converges faster, which makes it particularly suitable for real-time cybersecurity applications where computational efficiency is essential.The basic equations for updating the velocity and position of particles are as follows (Jain et al., 2022; Shami et al., 2022):

$$v_i(t+1) = w.v_i(t) + c_1.r_1.\left(p_{best} - x_i(t)\right) + c_2.r_2.\left(g_{best} - x_i(t)\right)x_i(t+1) = x_i(t) + v_i(t+1) \tag{1}$$

with:
$v_i(t)$ = the velocity of the third particle at iteration t,
$x_i(t)$ = position of the third particle in iteration t,
w = inertia factor,
c_1, c_2 = cognitive and social learning coefficients,
r_1, r_2 = random numbers in the range [0,1].

The multi objective objective function in this study is formulated as a combination of three main aspects of IDS performance: the detection rate (DR), which must be maximized; the false positive rate (FPR), which must be minimized; and latency (L), which must also be minimized. Mathematically:

$$\max f_1(x) = DR(x) \tag{2}$$

$$\min f_2(x) = FPR(x) \tag{3}$$

$$\min f_3(x) = L(x) \tag{4}$$

Thus, the multi objective optimization problem can be formulated as:

$$find\ x^* \in X\ therefore\ \{f_1(x), f_2(x), f_3(x)\}$$

Produces a set of Pareto optimal solutions, which are solutions that cannot be improved in one objective without worsening another objective (Lin et al., 2022; Roy et al., 2023). The optimization results are then visualized using the Pareto Front, which allows cybersecurity researchers and practitioners to select the best solution according to national defense policy priorities. This visualization is especially valuable for decision-makers in defense contexts, since it provides flexibility in choosing trade-offs between maximizing security (high detection rate) and maintaining operational efficiency (low false positives and latency)..

3. RESULTS AND DISCUSSIONS

1. Detection Rate Analysis (DR)

The analysis in Figure 1 shows that the proposed PSO IDS model achieved a detection rate of 0.96, which is markedly higher than the 0.85 obtained by the conventional IDS. This 11 percentage point improvement demonstrates that the optimization process introduced by PSO enables the system to capture more sophisticated intrusion patterns, including stealth and distributed attacks. Such an enhancement is critical in national defense networks, where even a small increase in detection capability can significantly reduce security risks.

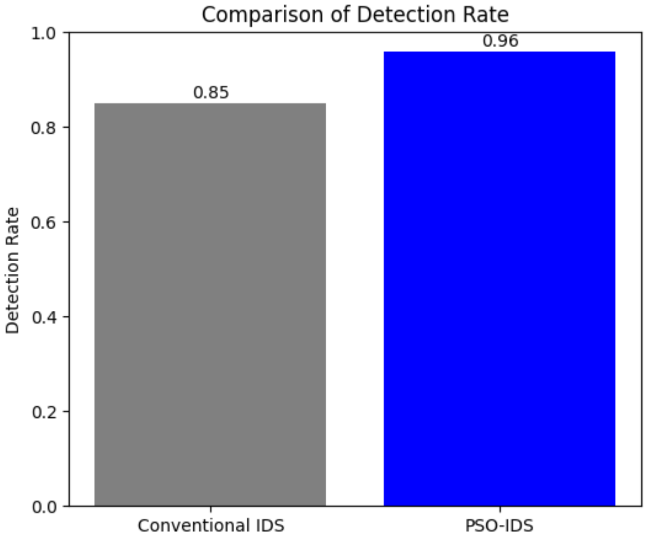

Figure 2 Comparison of Detection Rate

2. False Positive Rate Analysis (FPR)

Figure 2 illustrates a sharp reduction in false positives when using PSO IDS. The false positive rate decreased from 0.18 in the conventional IDS to only 0.07 in PSO IDS, reflecting a reduction of more than 60%. This improvement indicates that the optimization not only strengthens detection capability but also enhances classification precision. In practical terms, this means fewer unnecessary alerts for security analysts, thereby improving operational efficiency in defense Security Operation Centers (SOCs).

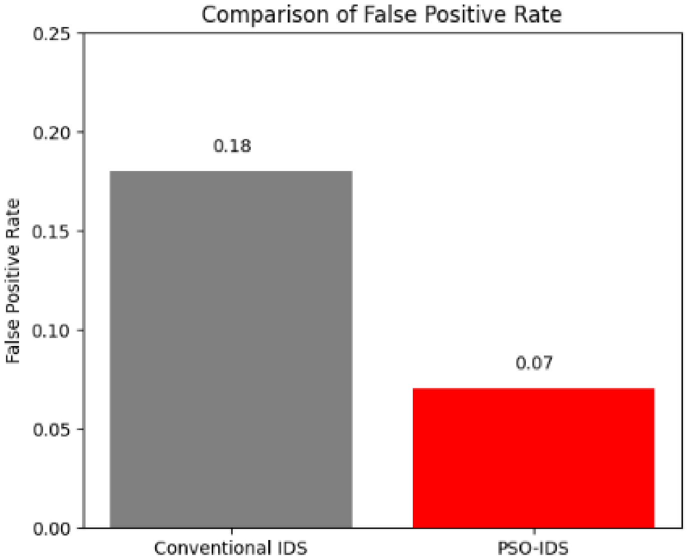

Figure 3. Comparison of False Positive Rate

3. Latency Analysis

In terms of latency, Figure 3 demonstrates that PSO IDS significantly outperformed the conventional IDS. The average detection latency was reduced from 0.35 seconds to 0.12 seconds, equivalent to a 65% improvement in processing time. This rapid detection speed is crucial for real time defense environments where immediate response is required to neutralize cyber threats before they escalate.

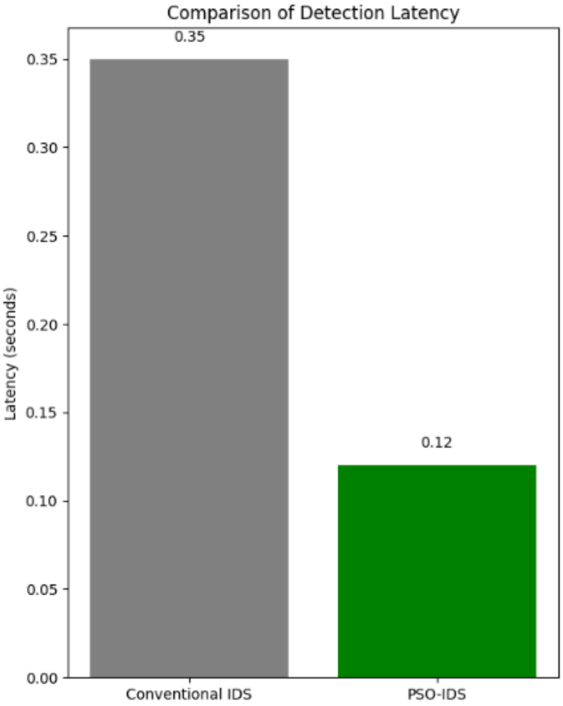

Figure 4. Comparison of Detection Latency

4. Trade off Multi Objective Analysis

The Pareto Front in Figure 4 highlights the balance between detection rate (DR) and false positive rate (FPR) across multiple PSO optimized solutions (P1–P5). The results show that DR gradually improved from 0.90 (P1) to 0.96 (P5), while FPR concurrently decreased from 0.15 (P1) to 0.07 (P5). This simultaneous enhancement demonstrates that PSO effectively negotiates the trade off between sensitivity and specificity, producing solutions that are both accurate and reliable. Compared to conventional single objective optimization, this multi objective approach offers more stable and balanced performance, making it highly suitable for deployment in critical defense infrastructures.

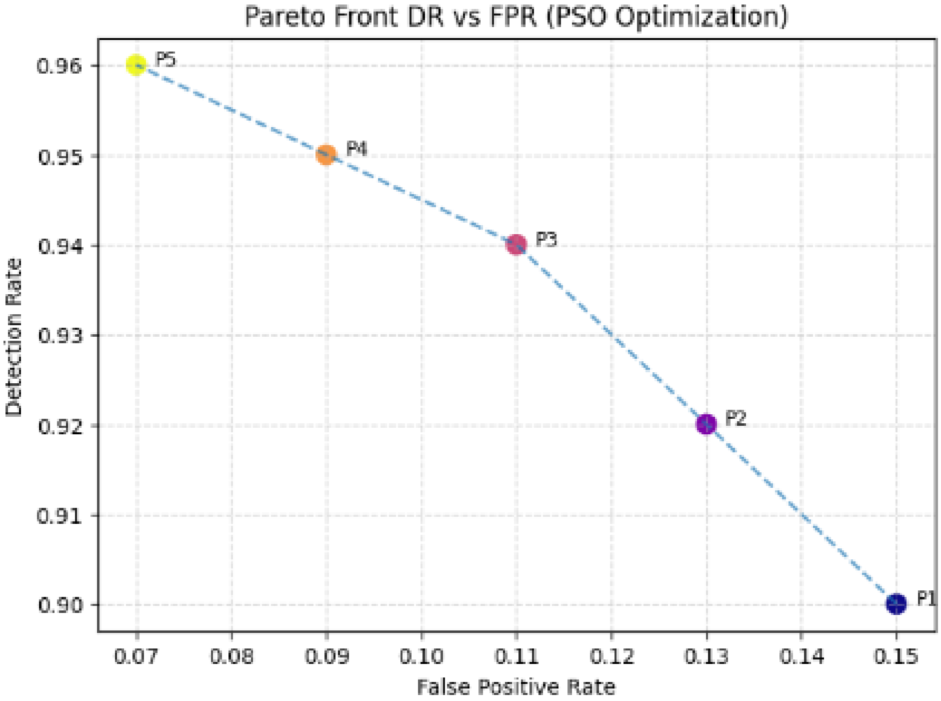

Figure 5. Parento Front DR vs FPR (PSO Optimization)

Discussions

The application of multi-objective Particle Swarm Optimization (PSO) in Intrusion Detection Systems (IDS) has proven capable of overcoming the limitations of conventional IDS. An increase in detection rate to 0.96 compared to 0.85 in the old system demonstrates the model's ability to recognize more complex attack patterns, including hidden and distributed attacks. This confirms that an optimization-based approach can provide significant added value to threat detection effectiveness, which in turn strengthens the resilience of national defense infrastructure against advanced cyber threats. Furthermore, Pareto Front analysis shows that this improvement was not achieved at the expense of other aspects, but rather went hand in hand with a decrease in false positive rate and latency.

From an operational reliability perspective, the reduction in the false positive rate from 0.18 to 0.07 (more than 60%) is a significant finding. The high number of false alarms in conventional IDS often creates an excessive workload for security analysts in Security Operation Centers (SOC), which can potentially reduce the effectiveness of responses to real attacks. With fewer irrelevant notifications, analysts can focus more on priority threats, thereby improving operational efficiency. In addition, these results also show that the implementation of PSO not only improves detection accuracy, but also supports more effective management of human and technological resources in the context of cyber defense.

The speed of detection is also a crucial factor. Research results show that the average latency has decreased dramatically from 0.35 seconds to 0.12 seconds, or about 65% faster. This advantage is particularly important in the context of defense, which requires real-time responses to prevent the spread of attacks or further damage to critical infrastructure. With faster detection, defense systems have a greater chance of proactively mitigating threats rather than reacting to them. This makes PSO-based IDS not only a monitoring tool, but also a key component in active defense strategies.

In the Indonesian context, cyber defense has become a national strategic issue handled by various institutions, including the National Cyber and Crypto Agency (BSSN), the Indonesian National Armed Forces (TNI), and cyber security operation centers in the government and military sectors. Security Operation Centers (SOC) in Indonesia are tasked with monitoring large-scale network traffic and responding quickly to incidents. The results of this study are directly relevant to SOCs in Indonesia because they can reduce the workload of analysts by lowering the false positive rate to 0.07, thereby reducing the potential for alert fatigue and increasing focus on priority threats such as Advanced Persistent Threats (APTs), which often pose a challenge to national defense. In addition, the reduction in detection time from 0.35 seconds to 0.12 seconds strengthens the SOC's ability to respond quickly to coordinated attacks that could potentially target critical infrastructure such as energy, transportation, and defense systems.

The implementation of PSO-IDS can also support the Indonesian government's policy in building adaptive national cyber resilience. With the integration of artificial intelligence-based optimization methods, SOCs in Indonesia can improve the efficiency of human and technological resource utilization. This is in line with BSSN's policy direction to develop a robust National Cybersecurity Framework that is adaptive to global threat dynamics. Thus, the results of this study not only contribute academically, but also have a practical impact in strengthening Indonesia's cybersecurity resilience.

From a policy perspective, these findings underscore the urgency of integrating optimization-based and artificial intelligence approaches into national cybersecurity policies. Governments can encourage the implementation of metaheuristic-based adaptive IDS such as PSO in defense networks, government, and other critical infrastructure sectors. In addition, investment policies in research and development (R&D) of adaptive security technologies need to be increased so that defense systems can adapt quickly to the evolution of threats. Thus, PSO IDS is not only relevant as a technical solution, but also a strategic one, supporting the creation of a sustainable and resilient cybersecurity policy framework in the face of global threat dynamics.

4. CONCLUSION

This research successfully addresses the main challenges of conventional Intrusion Detection Systems (IDS) in the context of national defense, namely low detection rates, high false positive rates, and latency that hinders real-time detection. Through the application of multi-objective Particle Swarm Optimization (PSO), the developed IDS system was able to increase the detection rate from 0.85 to 0.96, reduce the false positive rate from 0.18 to 0.07, and accelerate detection latency from 0.35 seconds to 0.12 seconds. These results demonstrate that the PSO approach not only improves detection accuracy but also maintains a balance between sensitivity and specificity, making IDS more adaptive in dealing with increasingly complex and dynamic cyber attack patterns. From an academic perspective, this research contributes to the advancement of metaheuristic optimization methods in cybersecurity. The integration of PSO with multi-objective optimization frameworks demonstrates that intrusion detection can be simultaneously optimized for accuracy, efficiency, and reliability. This work adds to the body of knowledge by showing how PSO can outperform single-objective optimization methods and conventional machine learning-based IDS in environments characterized by evolving and heterogeneous threats.Beyond its technical merits, the findings carry significant implications for national cyber defense. The PSO-based IDS system can serve as a foundation for strengthening critical infrastructure, reducing the workload of analysts in Security Operation Centers (SOCs), and enhancing rapid response capabilities against intrusions. In the Indonesian context, the adoption of such adaptive systems aligns with national strategies led by BSSN and TNI to secure defense networks and critical infrastructure sectors such as energy, transportation, and communications. Although the results are promising, there are limitations that can be addressed in future studies. First, testing should be extended to other large-scale and real-time datasets beyond CICIDS2017 to further validate robustness. Second, hybrid models that combine PSO with deep learning or ensemble approaches may yield even higher accuracy. Third, implementation in real SOC environments in Indonesia can provide insights into operational challenges and scalability. Finally, exploration of adaptive PSO parameter tuning methods can further enhance convergence speed and detection precision.

REFERENCES

Abdulganiyu, O. H., Tchakoucht, T. A., & Saheed, Y. K. (2024). Towards an efficient model for network intrusion detection system (IDS): systematic literature review. *Wireless Networks*, *30*(1), 453–482. https://doi.org/10.1007/s11276-023-03495-2

Ahmad, Z., Shahid Khan, A., Wai Shiang, C., Abdullah, J., & Ahmad, F. (2021). Network intrusion detection system: A systematic study of machine learning and deep learning approaches. *Transactions on Emerging Telecommunications Technologies*, *32*(1), 1–29. https://doi.org/10.1002/ett.4150

Alazab, M., Awajan, A., Alazzam, H., Wedyan, M., Alshawi, B., & Alturki, R. (2024). A Novel IDS with a Dynamic Access Control Algorithm to Detect and Defend Intrusion at IoT Nodes. *Sensors*, *24*(7), 2188. https://doi.org/10.3390/s24072188

Chen, Y.-F., Lin, F. Y.-S., Tai, K.-Y., Hsiao, C.-H., Wang, W.-H., Tsai, M.-C., & Sun, T.-L. (2025). A near-optimal resource allocation strategy for minimizing the worse-case impact of malicious attacks on cloud networks. *Journal of Cloud Computing*, *14*(1), 41. https://journalofcloudcomputing.springeropen.com/articles/10.1186/s13677-025-00749-6

Chicco, D., Oneto, L., & Tavazzi, E. (2022). Eleven quick tips for data cleaning and feature engineering. *PLoS Computational Biology*, *18*(12), e1010718. https://doi.org/10.1371/journal.pcbi.1010718

Colajanni, M., & Marchetti, M. (2021). Cyber attacks and defenses: Current capabilities and future trends. In *Technology and International Relations: The New Frontier in Global Power* (pp. 132–151). Edward Elgar Publishing. https://doi.org/10.4337/9781788976077.00015

Dan, V., & Pandey, M. (2024). yber-Security Threats In International Relation The Implications Of Cyber Threats On State Sovereignty, National Security, And International Cooperation, Focusing On Recent Cyber Incidents Rational Analysis In Geographical Point Of View. *International Journal of Creative Research Thoughts*, *12*, 2320–2882. www.ijcrt.org

Dhawas, P., Dhore, A., Bhagat, D., Pawar, R. D., Kukade, A., & Kalbande, K. (2024). Big data preprocessing, techniques, integration, transformation, normalisation, cleaning, discretization, and binning. In *Big Data Analytics Techniques for Market Intelligence* (pp. 159–182). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3693-0413-6.ch006

Gorriz, J. M., Clemente, R. M., Segovia, F., Ramirez, J., Ortiz, A., & Suckling, J. (2024). Is K-fold cross validation the best model selection method for Machine Learning? *ArXiv Preprint ArXiv:2401.16407*. http://arxiv.org/abs/2401.16407

Harrison, K. R., Elsayed, S., Garanovich, I., Weir, T., Galister, M., Boswell, S., Taylor, R., & Sarker, R. (2020). Portfolio Optimization for Defence Applications. *IEEE Access*, *8*, 60152–60178. https://doi.org/10.1109/ACCESS.2020.2983141

Jain, M., Saihjpal, V., Singh, N., & Singh, S. B. (2022). An Overview of Variants and Advancements of PSO Algorithm. *Applied Sciences (Switzerland)*, *12*(17), 8392. https://doi.org/10.3390/app12178392

Kurniabudi, Stiawan, D., Darmawijoyo, Bin Idris, M. Y. Bin, Bamhdi, A. M., & Budiarto, R. (2020). CICIDS-2017 Dataset Feature Analysis with Information Gain for Anomaly Detection. *IEEE Access*, *8*, 132911–132921. https://doi.org/10.1109/ACCESS.2020.3009843

Lansky, J., Ali, S., Mohammadi, M., Majeed, M. K., Karim, S. H. T., Rashidi, S., Hosseinzadeh, M., & Rahmani, A. M. (2021). Deep Learning-Based Intrusion Detection Systems: A Systematic Review. *IEEE Access*, *9*, 101574–101599. https://doi.org/10.1109/ACCESS.2021.3097247

Lin, X., Yang, Z., Zhang, X., & Zhang, Q. (2022). Pareto Set Learning for Expensive Multi-Objective Optimization. *Advances in Neural Information Processing Systems*, *35*, 19231–19247.

Möller, D. P. F. (2023). Cybersecurity in Digital Transformation. In *Advances in Information Security* (Vol. 103, pp.

1–70). Springer. https://doi.org/10.1007/978-3-031-26845-8_1

Oksuz, K., Cam, B. C., Kalkan, S., & Akbas, E. (2021). Imbalance Problems in Object Detection: A Review. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *43*(10), 3388–3415. https://doi.org/10.1109/TPAMI.2020.2981890

Roy, A., So, G., & Ma, Y.-A. (2023). Optimization on Pareto sets: On a theory of multi-objective optimization. *ArXiv Preprint ArXiv:2308.02145*. http://arxiv.org/abs/2308.02145

Saranya, T., Sridevi, S., Deisy, C., Chung, T. D., & Khan, M. K. A. A. (2020). Performance Analysis of Machine Learning Algorithms in Intrusion Detection System: A Review. *Procedia Computer Science*, *171*(2019), 1251–1260. https://doi.org/10.1016/j.procs.2020.04.133

Shami, T. M., El-Saleh, A. A., Alswaitti, M., Al-Tashi, Q., Summakieh, M. A., & Mirjalili, S. (2022). Particle Swarm Optimization: A Comprehensive Survey. *IEEE Access*, *10*, 10031–10061. https://doi.org/10.1109/ACCESS.2022.3142859

Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018). Toward generating a new intrusion detection dataset and intrusion traffic characterization. *ICISSP 2018 - Proceedings of the 4th International Conference on Information Systems Security and Privacy*, *2018-January*, 108–116. https://doi.org/10.5220/0006639801080116

Stewart, H. (2023). Digital Transformation Security Challenges. *Journal of Computer Information Systems*, *63*(4), 919–936. https://doi.org/10.1080/08874417.2022.2115953

Trivedi, V., Varshney, P., & Ramteke, M. (2020). A simplified multi-objective particle swarm optimization algorithm. *Swarm Intelligence*, *14*(2), 83–116. https://doi.org/10.1007/s11721-019-00170-1

Yates, L. A., Aandahl, Z., Richards, S. A., & Brook, B. W. (2023). Cross validation for model selection: A review with examples from ecology. *Ecological Monographs*, *93*(1), e1557. https://doi.org/10.1002/ecm.1557

Yong, Z., Li-juan, Y., Qian, Z., & Xiao-yan, S. (2020). Multi-objective optimization of building energy performance using a particle swarm optimizer with less control parameters. *Journal of Building Engineering*, *32*, 101505. https://doi.org/10.1016/j.jobe.2020.101505

Zhou, C., Hu, B., Shi, Y., Tian, Y. C., Li, X., & Zhao, Y. (2021). A Unified Architectural Approach for Cyberattack-Resilient Industrial Control Systems. *Proceedings of the IEEE*, *109*(4), 517–541. https://doi.org/10.1109/JPROC.2020.3034595