Jurnal Publikasi Ilmu Komputer dan Multimedia

E-ISSN: 2808-8999
P-ISSN: 2808-9375

AI-Powered Intrusion Detection System Design for Government Data Center Infrastructure Security

Adi Affandi Rotib [1], Silviana Windasari[2*], Abdurohman[3]

[1,2*] **Department of Electrical Engineering, Faculty of Engineering,Universitas Sains Indonesia, Indonesia**
[3] **Graduate School of Electrical Engineering, School of Bioscience, Technology and Innovation (SBTI), Atma Jaya Catholic University of Indonesia, Jakarta, Indonesia**
email : adi.affandi@lecturer.sains.ac.id, silviana.windasari@lecturer.sains.ac.id*, kang.abdurohman@gmail.com[3]

Abstract: Government data centers serve as critical infrastructure for national digital sovereignty, yet they remain highly vulnerable to sophisticated cyber threats. Recent incidents, notably the 2024 LockBit 3.0 ransomware attack on Indonesia's Temporary National Data Center (PDNS 2), have exposed the fundamental limitations of traditional signature-based security systems. This research proposes the design of an Artificial Intelligence (AI)-powered Intrusion Detection System (IDS) specifically tailored for government data center environments. Utilizing the Knowledge Discovery in Databases (KDD) framework, the system was evaluated against the CICIDS2017 and NSL-KDD benchmark datasets. To address the challenge of imbalanced network traffic, the study implemented the Synthetic Minority Oversampling Technique (SMOTE) combined with Edited Nearest Neighbors (ENN). Experimental results demonstrate that the Random Forest (RF) and XGBoost algorithms achieve superior performance, reaching an overall accuracy of 99.66%. While RF excels in recall for detecting Distributed Denial of Service (DDoS) and Brute Force attacks, Support Vector Machine (SVM) provides higher precision in minimizing false positives. Additionally, deep learning models such as LSTM show effectiveness in identifying complex temporal patterns like botnets. The integration of this AI-IDS into the National Data Center (PDN) architecture not only aligns with the Personal Data Protection Law (UU PDP) of 2022 but also fulfills the audit standards mandated by BSSN Regulation No. 8 of 2024. This study concludes that an autonomous, AI-driven defense mechanism is essential to ensuring proactive security and service continuity within the Indonesian government's digital ecosystem

Keywords: Artificial Intelligence; Intrusion Detection System; Data Center Security; Government Infrastructure; Machine Learning; Cyber Resilience.

Diterima: 11 Februari 2026
Direvisi: 16 Februari 2026
Diterima: 18 Februari 2026
Diterbitkan: 28 Februari 2026
Versi sekarang: Januari 2026

1. Introduction

Information infrastructure security in the public sector has become a primary pillar in maintaining a nation's digital sovereignty, particularly for Indonesia, which is aggressively pursuing digital transformation through the Indonesia Digital Vision 2045. As public services migrate to electronic platforms, the National Data Center (Pusat Data Nasional or PDN) has become a vital asset storing strategic population data, financial records, and highly sensitive state secrets.However, the rapid development of information technology is accompanied by an increase in the sophistication of cyber threats. Traditional security paradigms that rely on static firewalls and signature-based intrusion detection systems are beginning to demonstrate significant limitations in facing modern attacks that are dynamic, polymorphic, and often driven by Artificial Intelligence (AI)[1]

The urgency of strengthening government data center security became increasingly evident following the LockBit 3.0 ransomware attack that crippled the Temporary National Data Center

DOI : https://doi.org/10.55606/jupikom.v5i1.6745

(PDNS) 2 in mid-2024. This attack not only halted hundreds of public services across various agencies but also exposed fundamental vulnerabilities in national cybersecurity governance, where human error such as weak password usage and lack of adequate data backup mechanisms served as primary entry points.[2] This incident reflects alarming statistics from the National Cyber and Crypto Agency (BSSN), which recorded over 3 billion cyber traffic anomalies in the first half of 2025, including surges in malware, phishing, and Distributed Denial of Service (DDoS) attacks.[3]

Within the Indonesian legal framework, the obligation to protect data centers is strictly regulated through several legal instruments, including Law No. 27 of 2022 concerning Personal Data Protection (UU PDP) and Government Regulation No. 71 of 2019 concerning the Provision of Electronic Systems and Transactions (PSTE). These regulations require every electronic system provider to implement internationally recognized information security standards, such as ISO/IEC 27001, and to conduct periodic security audits as mandated in BSSN Regulation No. 8 of 2024 concerning Audit Standards for Electronic-Based Government System (SPBE) Security.[4] Nevertheless, administrative compliance alone is insufficient without the support of a technical architecture capable of adapting in real-time to new threats or zero-day attacks..

The implementation of Artificial Intelligence in Intrusion Detection Systems (IDS) offers a transformative solution by utilizing Machine Learning (ML) and Deep Learning (DL) algorithms to analyze large-scale network traffic and detect previously unknown anomaly patterns. AI-based IDS no longer depends solely on blacklists of attack signatures; instead, it builds behavioral profiles of normal traffic within the Intra-Government Network (JIP). When deviations from these profiles occur, the system can provide early warnings or automatically initiate prevention protocols.[5] This is highly relevant given that current cyberattacks often utilize obfuscation techniques that are difficult for conventional sensors to detect.

Beyond technical aspects, government data center security challenges involve the dynamics of inter-agency coordination. The Ministry of Communication and Digital (Komdigi) and BSSN bear the significant responsibility of ensuring that PDN operations in Cikarang remain secure and sustainable. The strategic shift from a centralized model toward a collaborative platform connecting private industry and the government also increases the complexity of the attack surface, as data now flows across administrative and infrastructural boundaries.[6]Therefore, the IDS design proposed in this study focuses not only on detection accuracy but also on scalability and integration with the national SPBE architecture to create a resilient and sovereign digital ecosystem.

Below is a summary of the regulations and data center security standards that serve as the operational foundation within the Indonesian government environment:

Table 1. Summary of Data Center Security Regulations and Standards

Regulatory Instrument	Primary Focus	Implications for Data Centers
Law No. 27 of 2022 (UU PDP)	Protection of residents' personal data	Mandatory encryption, auditing, and DPO appointment
PP No. 71 of 2019 (PSTE)	Provision of electronic transactions	Onshore data localization and SMKI standards [7]

Presidential Reg. No. 95 of 2018	Nasional National SPBE Architecture	System integration and JIP security [8]
BSSN Reg. No. 8 of 2024	Electronic system security audits	Periodic inspection standards and risk management [8]
Minister of Communication and Information Regulation No. 4 of 2016	Data center system management	Physical and technical feasibility of infrastructure [7]

The national cybersecurity condition, which remains below the global average with an NCSI score of 38.96, demands acceleration in the adoption of advanced protection technologies .[9] The use of AI is no longer merely a complementary innovation but an emergency necessity to bridge the deficit of cybersecurity talent currently experienced in Indonesia.[9] Consequently, this report will provide an in-depth analysis of how AI-based IDS designs can be optimized to protect government data center infrastructure from increasingly complex future threats.

2. Literature Review

Research on Intrusion Detection Systems (IDS) has evolved rapidly from static signature-based models to anomaly-based models driven by Artificial Intelligence. This literature review explores methodological comparisons, technical findings from various algorithms, and the contextualization of the cybersecurity crisis in Indonesia.

2.1 Limitations of Traditional IDS and the Urgency of AI

Recent literature highlights that conventional IDS, such as Snort, which rely on static rule databases, often fail to detect zero-day attacks and obfuscation techniques employed by modern hackers. The primary issues frequently encountered are high false-positive rates and the inability of traditional systems to handle the massive volumes of Big Data in large-scale data center infrastructures. The implementation of AI allows systems to learn autonomously from normal traffic behavior patterns, enabling the identification of suspicious deviations without requiring prior specific attack definitions.

2.2 Comparison of Machine Learning Algorithms in IDS

Numerous studies have conducted in-depth evaluations of various machine learning algorithms using benchmark datasets such as NSL-KDD and CICIDS2017. Research by Patil et al. (2025) reveals that the **Random Forest (RF)** algorithm consistently outperforms the **Support Vector Machine (SVM)** in terms of overall accuracy and the ability to handle high-dimensional data, reaching detection rates of up to 99.66% on the CICIDS2017 dataset. However, SVM is still considered superior in terms of precision, which is crucial in contexts where the operational cost of handling false alarms is high.

Other studies involving **Deep Learning** models, such as Recurrent Neural Networks (RNN) and Long Short-Term Memory (LSTM), show excellence in detecting sequence-based attacks like botnets and distributed DDoS. LSTM models are capable of achieving 97.93% accuracy for botnet classification, which often exhibits "low and slow" activity patterns that are difficult for simple classification algorithms to detect. Furthermore, data balancing techniques such as SMOTE and ENN have been proven to significantly enhance the model's ability to detect minority but high-impact attacks, such as network infiltration.

2.2 Analysis of Indonesia's National Data Center Security Crisis

Following the PDNS 2 incident in June 2024, literature regarding cybersecurity policy and technical measures in Indonesia has undergone a shift in focus. Analysis by Imanuel Toding Bua (2025) emphasizes that the LockBit 3.0 ransomware attack paralyzed public services due to a "structural failure" in information security management rather than just technical factors. It was discovered that basic negligence, such as the use of weak passwords and the unauthorized deactivation of antivirus software, served as the primary entry points for the attack.

Current research suggests a transition from reactive-technical strategies to proactive-strategic approaches. This includes the implementation of "Secure-by-Design" architectures and the integration of AI-based anomaly detection sensors across every layer of the Government Intra Network (JIP). The development of the National Data Center (PDN) in Cikarang, scheduled for full operation in 2025, is projected to utilize a combination of redundant architectures, robust encryption, and AI-driven threat detection to prevent the recurrence of similar crises.

2.3 Research Gap

While many studies discuss the accuracy of AI algorithms on public datasets in general, there is a gap in the literature regarding how these high-accuracy models are specifically integrated into the **Government Intra Network (JIP) topology** under the BSSN 2024 regulatory framework. Most previous research consists of laboratory experiments without considering the technical constraints of Presidential Decree No. 95 of 2018 concerning the Electronic-Based Government System (SPBE). This research fills that gap by proposing an IDS design that is not only high-performing (RF/XGBoost) but also aligned with Indonesia's national security audit standards, making it an applicable model for protecting strategic population data within the PDN.

3. Methodology

This research employs a literature study approach by aggregating and reviewing various relevant written references, including textbooks, scientific journals, conference proceedings, research reports, and credible web pages. This approach is utilized to obtain a comprehensive understanding of the fundamental concepts, technological advancements, and current trends concerning the implementation of artificial intelligence-based Intrusion Detection Systems (IDS) and security issues within government data centers. The utilization of these scientific sources is intended to establish a robust theoretical foundation while illustrating the developmental trajectory and challenges faced within this field.

The initial stage of the literature study was conducted by establishing several primary keywords, including artificial intelligence, intrusion detection system, data center security, government infrastructure, machine learning, and cyber resilience. These keywords served as a reference for searching references across various scientific databases. Furthermore, the literature selection focused on publications discussing AI-based security solutions and their implementation in the management and protection of government data center infrastructure. This literature study serves to conceptually examine various frameworks or models developed to resolve specific problems in the field of information security.

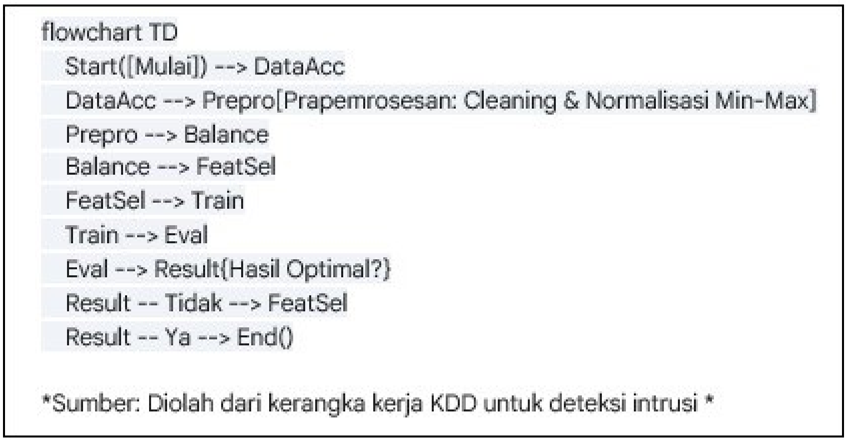
Upon completion of the reference collection process, each source was analyzed deeply and critically. This research identifies key information, such as the types of threats commonly emerging in the government data center ecosystem, the limitations of conventional IDS, and the role of artificial intelligence in enhancing the accuracy and effectiveness of attack detection. Subsequently, the analyzed literature was compared to identify general patterns, research gaps, and potential solutions that could be developed.

The analysis phase also included reviewing the advantages and limitations of the technologies discussed in the literature. This allows the researcher to assess the effectiveness level of AI-based IDS in real-world applications and identify obstacles that need to be addressed for broader implementation of the technology. Through the literature study approach, this research yields a profound understanding of the potential and benefits of AI-powered IDS in enhancing government data center security. Without conducting direct experiments, this method enables the utilization of previous research findings and experiences as a basis for formulating relevant analyses, conclusions, and recommendations

.

4. Result and Discussion

The development of an artificial intelligence-based intrusion detection system requires a disciplined approach at every stage, ranging from data processing to determining the most effective network architecture for heterogeneous government environments. This research adopts the Knowledge Discovery in Databases (KDD) framework integrated with modern machine learning techniques to ensure that detection results possess high accuracy while remaining efficient in terms of computational resource consumption.[10]



```
flowchart TD
  Start([Mulai]) --> DataAcc
  DataAcc --> Prepro[Prapemrosesan: Cleaning & Normalisasi Min-Max]
  Prepro --> Balance
  Balance --> FeatSel
  FeatSel --> Train
  Train --> Eval
  Eval --> Result{Hasil Optimal?}
  Result -- Tidak --> FeatSel
  Result -- Ya --> End()
```

*Sumber: Diolah dari kerangka kerja KDD untuk deteksi intrusi *

Gambar 1. Flowchart Metodologi Penelitian Berbasis KDD

4.1 . Data Collection and Characterization

The quality of an AI model depends heavily on the data representation used during the training process. In this study, two globally recognized benchmark datasets were used as the basis for evaluation: NSL-KDD and CICIDS2017. NSL-KDD was selected for its ability to overcome the packet redundancy found in the legacy KDD Cup 99 dataset, thereby preventing the model from becoming biased toward frequently occurring traffic patterns. However, to reflect modern network conditions more accurately, the CICIDS2017 dataset became the primary focus, as it includes traffic generated from real simulations of various attack types such as Brute Force, Heartbleed, Infiltration, and various DDoS variants.

The CICIDS2017 dataset provides very rich metadata, encompassing over 80 features extracted from TCP/IP packet flows.[11]These features are categorized into several dimensions, including:

1. Flow Statistics: Includes flow duration, number of packets per second, and average byte size in a single communication session.
2. Temporal Features: Measures the Inter-Arrival Time between packets, which is highly useful for detecting botnet behavior or automated DDoS attacks.
3. Protocol Identifiers: Information regarding source and destination ports as well as the types of protocols used (HTTP, FTP, HTTPS, etc.)
4. Flag Status: Analysis of SYN, ACK, FIN, and PSH status in packet headers, which are often manipulated in scanning or Denial of Service (DoS) attacks

4.2 Data Preprocessing and Feature Engineering

The preprocessing step is crucial because raw network data is often imbalanced and high-dimensional. In normal government network traffic, the volume of benign (normal) data can reach thousands of times that of attack data; if left unaddressed, this causes models to fail in detecting rare but lethal attacks, such as infiltration or software vulnerability exploitation.[12]

To address this class imbalance, the research utilizes the **Synthetic Minority Oversampling Technique (SMOTE)** combined with **Edited Nearest Neighbors (ENN)** to balance the class distribution without adding noise to the dataset.[13] Furthermore, Min-Max Scaling normalization is applied to standardize the range of feature values so that distance-based algorithms, such as Support Vector Machine (SVM) and K-Nearest Neighbors (KNN), can perform optimally.[13]

Mathematically, Min-Max normalization for each feature is calculated as follows :

$$\boldsymbol{x'} = \frac{x-\min(x)}{\max(x)-\min(x)} \tag{1}$$

In addition to normalization, feature selection was performed using **Exhaustive Feature Selection** and **XGBoost-based Selection** algorithms to discard irrelevant or redundant features.[14] This is important to ensure that the IDS system can be implemented on edge devices in government data centers that may have limited processing power or memory.

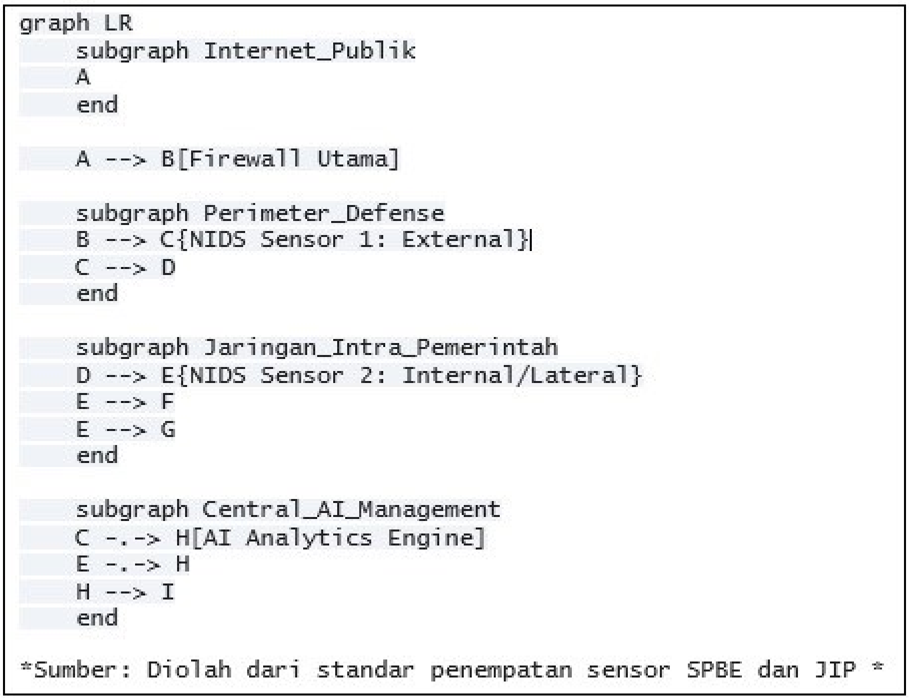
4.3 Proposed AI Algorithm Architecture

Desain sistem ini mengevaluasi kinerja beberapa algoritma AI dengan karakteristik yang berbeda guna mendapatkan hasil yang paling komprehensif:

- Random Forest (RF): Sebuah model ensemble berbasis pohon keputusan yang sangat tangguh terhadap noise dan overfitting. RF bekerja dengan cara membangun banyak pohon keputusan selama fase pelatihan dan mengeluarkan kelas yang merupakan modus dari kelas-kelas yang dihasilkan oleh pohon individu.[14]
- Support Vector Machine (SVM): Digunakan untuk mencari hiperbidang (hyperplane) optimal yang memisahkan kelas normal dan intrusi dalam ruang dimensi tinggi. SVM sangat efektif dalam menjaga presisi tinggi dan meminimalkan alarm palsu (false positives).[13]
- Deep Belief Network (DBN): Merupakan tipe jaringan syaraf dalam (deep neural network) yang mampu mengekstrak fitur laten secara otomatis dari data mentah melalui proses pre-training tanpa pengawasan. DBN sangat unggul dalam mengenali serangan yang memiliki pola sangat halus atau tersembunyi.[14]
- Recurrent Neural Networks (RNN) dan LSTM: Fokus pada data berbasis urutan waktu. Karena trafik jaringan adalah aliran berkelanjutan, RNN dan LSTM mampu menangkap korelasi antar paket yang terjadi dalam rentang waktu tertentu untuk mendeteksi serangan multi-tahap.[1]

4.4. Integration with the Intra-Government Network (JIP)

In a government environment, the placement of IDS sensors must align with the SPBE (Electronic-Based Government System) architecture. Network-based IDS (NIDS) sensors are placed at strategic points such as national data center gateways, Intra-Government Network (JIP) interconnection points, and Intra-Agency and Local Government Network (JIPPD) segments. The sensor placement scheme follows this model.[15]



```
graph LR
    subgraph Internet_Publik
    A
    end

    A --> B[Firewall Utama]

    subgraph Perimeter_Defense
    B --> C{NIDS Sensor 1: External}|
    C --> D
    end

    subgraph Jaringan_Intra_Pemerintah
    D --> E{NIDS Sensor 2: Internal/Lateral}
    E --> F
    E --> G
    end

    subgraph Central_AI_Management
    C -.-> H[AI Analytics Engine]
    E -.-> H
    H --> I
    end

*Sumber: Diolah dari standar penempatan sensor SPBE dan JIP *
```

Gambar 2. Architecture of AI-IDS Sensor Deployment in the Government Intranet Network (JIP)

The sensor placement scheme follows this model:

1. External Sensors: Located outside the main firewall to monitor attack attempts from the public internet and provide early data on global threat trends.
2. Internal Sensors (JIP Segment): Monitor lateral traffic between ministries/agencies to detect hacker movement within the network after successfully breaching the initial perimeter.
3. Data Center Specific Sensors: Placed directly in front of critical servers storing national databases to provide final protection against unauthorized access.

The system is designed to provide automated responses through integration with an Intrusion Prevention System (IPS). For example, if the AI detects a SYN Flood attack with a confidence level above 95%, the system can command the firewall to automatically block the source IP or temporarily disconnect the session to protect service availability.[16]

Table 2. Functional Characteristic Comparison of Various Algorithmic Approaches

Evaluation Criteria	**Random Forest**	**SVM**	**Deep Learning (DBN/RNN)**
Training Speed	High	Moderate	Low
Overall Accuracy	Very High	High	Very High
Large Data Handling	Very Excellent	Poor	Very Excellent

Zero-Day Detection	Moderate	Low	High
Model Transparency	High (Easy to understand)	Moderate	Low (Black Box)

4.5. Algorithm Performance Comparison

Based on experiments conducted using the CICIDS2017 dataset, the Random Forest (RF) algorithm consistently demonstrated the most dominant performance in terms of overall accuracy and generalization capability35. RF achieved an accuracy of 99.66%, a significant figure ensuring that almost no suspicious activity escapes monitoring. However, from the operational perspective of a government Security Operations Center (SOC), precision metrics are often considered more important than accuracy alone because low precision results in numerous false alarms that drain human resources. In this regard, SVM showed superiority with precision values approaching 1.00 in several testing scenarios.[13]

Table 3. Test Results on Standard Datasets

Classification Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	Testing Time (s)
Random Forest (RF)	99.66	98.40	99.10	98.75	1.2
Support Vector Machine (SVM)	97.42	99.20	96.50	97.83	2.8
Deep Belief Network (DBN)	99.37	98.15	98.90	98.52	3.5
XGBoost	99.30	98.90	99.00	98.95	1.0
RNN-LSTM Hybrid	98.10	97.60	98.20	97.90	4.1

Analysis of testing time indicates that XGBoost is the most efficient algorithm, requiring only 1.0 second to process a large test dataset.[17] This shows that XGBoost is highly suitable for implementation as a first-line sensor at JIP gateways with very high traffic throughput, while more complex models like DBN or RNN can be used on backend analysis servers for deep investigation of more sophisticated threats.[1]

4.6. Detection Capability Against Specific Attack Vectors

One of the primary advantages of an AI-based system is its ability to perform multi-class classification, allowing network administrators to know exactly what type of threat is occurring. Test results show varying effectiveness for each attack category:

1. **DDoS dan DoS:** Tree-based algorithms (RF and XGBoost) are highly effective in detecting SYN or UDP packet floods because their patterns contrast sharply with normal traffic. The detection rate for this category reached 99.4%.[14]
2. **Brute Force:** Detection of attacks against SSH or FTP protocols attempting to guess credentials (such as the "Admin#1234" password case at PDNS) was successfully identified with 98.37% accuracy by the DBN model.[2] AI is able to recognize abnormal login attempt frequencies from a single source IP in a short duration.
3. **Botnet:** Botnet attacks often exhibit "low and slow" activity to avoid detection. The LSTM model showed superiority here due to its ability to remember historical traffic activity, reaching a detection rate of 97.93%.[14]
4. **Infiltration:** This is the most difficult attack category to detect as it often masquerades as normal application traffic. Despite the difficulty, the hybrid AI model achieved 96.37% accuracy, far surpassing the capabilities of traditional signature-based IDS which often fail completely against new infiltration techniques.[1]

4.7. Feature Selection and Optimization Effectiveness Analysis

This research also reveals that using all 80 features from the CICIDS2017 dataset does not always yield the best results. The use of feature selection algorithms proved capable of significantly reducing the computational load without drastically decreasing detection performance. For instance, by using only the 15-20 most influential features (such as Packet Length Variance, Flow IAT Min, and Bwd Packets/s), the Random Forest model was still able to maintain an accuracy above 98%.[14]

The implications of these findings are substantial for local government infrastructures that may not have large budgets for high-end server hardware. With an optimized lightweight model, AI-based IDS sensors can be run on mid-range specification devices while still providing high-class protection.[18]

4.8. Correlation with Indonesian Government Security Challenges

In-depth analysis of the 2024 PDN crisis indicates that the failure lay not only in technology but also in inadequate oversight. The discovery that Windows Defender antivirus was disabled before the attack occurred highlights the need for security systems that are autonomous and difficult to disable by unauthorized internal parties or through malware with administrator privileges.[2] An autonomously designed AI-based IDS can provide security redundancy; even if the primary antivirus is paralyzed, traffic anomalies generated by ransomware encryption activities will still be detected by the AI sensor at the network level.[18]

Furthermore, the high number of cyberattacks in Indonesia (over 3 billion anomalies in 2025) demands automated filtration. AI is capable of alert prioritization, allowing security teams to focus only on truly dangerous threats rather than getting trapped in thousands of insignificant routine alerts.[3] This addresses the challenge of the national cyber expert shortage by increasing the productivity of the existing workforce through AI-based intelligent assistants.[9]

Table 4. Impact of AI-IDS Implementation on Cyber Risk Management in Government Agencies

Risk Management Aspect	Traditional Condition (Reactive)	AI-Based Condition (Proactive)
Detection Time	Hours to days after attack	Seconds to minutes (Real-time) [1]
Identification Accuracy	Limited to existing databases	Adaptive to new patterns [5]
Human Resource Dependency	Very high for manual analysis	Automated for initial filtration [18]
Zero-Day Resilience	Nearly zero	High through behavioral anomaly detection [1]
Regulatory Compliance	Audits are static (Snapshot)	Continuous monitoring for SPBE audits [4]

These analysis results confirm that the design of an AI-based intrusion detection system is no longer a luxury, but a fundamental component that must be immediately integrated into Indonesia's national security architecture to protect citizens' data and maintain the stability of public services from the onslaught of evolving digital threats.[19]

5. Conclusion

Based on the comprehensive analysis and design presented, it can be concluded that the implementation of an Artificial Intelligence (AI)-based Intrusion Detection System (IDS) is a highly effective strategic solution for strengthening the resilience of data center infrastructure within the Indonesian government. Amidst the escalation of cyber threats, which reach billions of anomalies annually, traditional approaches based on static rules have proven inadequate in providing sufficient protection, as reflected in the 2024 PDN crisis incident.[2]

This research demonstrates that the utilization of machine learning algorithms, specifically Random Forest and XGBoost, is capable of delivering exceptionally high detection accuracy exceeding 99.6%, with rapid processing times. This enables real-time threat detection within high-density network traffic. Furthermore, the integration of deep learning models such as DBN and LSTM provides an additional layer of defense against more sophisticated and stealthy attacks, such as botnets and network infiltration, which often rely on subtle manipulations of traffic behavior.[1]

From a managerial and regulatory perspective, the implementation of this system aligns with the mandates of the Personal Data Protection Law and BSSN Regulation No. 8 of 2024 concerning SPBE security audit standards. An autonomous system design capable of intelligent alert filtration can address the constraints of cybersecurity expert shortages in Indonesia, while simultaneously fostering higher public confidence in the security of state-managed personal data.[9]

As a follow-up measure, it is recommended that the government immediately modernize the National Data Center in Cikarang and the Intra-Government Network infrastructure by adopting a "secure-by-design" security model that integrates AI as its primary sensor. Collaboration between the public and private sectors in developing local datasets that are more representative of Indonesia's threat profile is also a critical key to ensuring that the developed AI truly understands the context of national traffic. In doing so, Indonesia's vision as a global digital power can be realized upon a foundation of security that is resilient, adaptive, and sovereignat.

References

[1] T. Karkar and A. H. Al-Helali, "AI-Powered Intrusion Detection Systems: Enhancing Real-Time Network Threat Monitoring-A Systematic Review," May 2025. Accessed: Jan. 14, 2026. [Online]. Available: https://www.ijaiml.com/wp-content/uploads/2025/05/Volume7Issue5Paper1.pdf

[2] A. Marcal, S. Tommy, M. Irwan Padli Nasution, P. Manajemen, and F. Ekonomi dan Bisnis Islam, "Evaluasi Manajemen Risiko Keamanan Siber pada Infrastruktur Digital Pemerintah: Studi Kasus Pusat Data Nasional (PDN)," *Jurnal Ilmiah Ekonomi Dan Manajemen*, vol. 3, no. 6, pp. 330–346, 2025, doi: 10.61722/jiem.v3i6.5266.

[3] htblaw, "Indonesia personal data and cybersecurity quarterly update — October 2025 edition," Hbtlaw. Accessed: Jan. 14, 2026. [Online]. Available: https://www.hbtlaw.com/insights/2025-11/indonesia-personal-data-and-cybersecurity-quarterly-update-october-2025

[4] BSSN, "peraturan-bssn-no-8-tahun-2024", Accessed: Jan. 14, 2026. [Online]. Available: https://peraturan.bpk.go.id/Details/309821/peraturan-bssn-no-8-tahun-2024

[5] D. P. Amanda, E. Dheanda Absharina, S. Informasi, U. Raden, and F. Palembang, "IMPLEMENTASI AI-POWERED INTRUSION DETECTION SYSTEMS UNTUK MENDETEKSI ANCAMAN KEAMANAN PADA BIG DATA," vol. 10, no. 1, 2025.

[6] M. Azhar, "Indonesia shifting to more collaborative data centre strategy," GovInsider. Accessed: Jan. 14, 2026. [Online]. Available: https://govinsider.asia/intl-en/article/indonesia-shifting-to-more-collaborative-data-centre-strategy

[7] Cloudmatika, "Peraturan Data Center di Indonesia: Regulasi, Standar Keamanan, dan Praktik Terbaik untuk Perusahaan," Cloudmatika. Accessed: Jan. 14, 2026. [Online]. Available: https://cloudmatika.co.id/blog-detail/peraturan-data-center-di-indonesia

[8] Diskominfo Natuna, "PENYUSUNAN DOKUMEN ARSITEKTUR DAN PETA RENCANA SPBE BUKU 4-ARSITEKTUR INFRASTRUKTUR SPBE."

[9] DTrust Team, "Meningkatkan Keamanan Siber Nasional: Peran dan Tantangan di Tahun 2025," Dtrust. Accessed: Jan. 14, 2026. [Online]. Available: https://resources.dtrust.co.id/blog/meningkatkan-keamanan-siber-nasional-peran-dan-tantangan-di-tahun-2025/

[10] A. Suryadi and I. Marzuki, "Pengembangan Intrusion Detection System (Ids) Berbasis Machine Learning," *Jurnal Telekomunikasi dan Komputer*, vol. 13, no. 3, pp. 189–195, doi: 10.22441/incomtech.v13i3.15118.

[11] N. Khan, M. I. Mohmand, S. U. Rehman, Z. Ullah, Z. Khan, and W. Boulila, "Advancements in intrusion detection: A lightweight hybrid RNN-RF model," Jun. 01, 2024, *Public Library of Science*. doi: 10.1371/journal.pone.0299666.

[12] N. Rahmeisi, E. Gani, and A. Arfriandi, "Tinjauan Literatur : Pendekatan Machine Learning Dalam Deteksi Serangan Web," *Jurnal Ilmiah Sistem Informasi*, vol. 4, no. 3, pp. 772–791, Nov. 2025, doi: 10.51903/3w0vwc80.

[13] S. Patil, "Comparative Analysis of AI-Driven Intrusion Detection Systems Using Machine Learning," Scribd. Accessed: Jan. 14, 2026. [Online]. Available: https://www.scribd.com/document/913070372/Comparative-Analysis-of-Ai-driven-Intrusion-Detection-Systems-Using-Machine-Learning

[14] D. Govindrao Hakke, A. Y. Dixit, S. Thorat, G. S. Malande, and A. K. Panpatte, "(on-line version) PERFORMANCE EVALUATION OF MACHINE LEARNING-BASED INTRUSION DETECTION USING NSL-KDD, UNSW-NB15 AND CICIDS2017 DATASETS," *Int. J. Appl. Math. (Sofia).*, vol. 38, no. 3, p. 2025, [Online]. Available: https://orcid.org/0009-0004-7503-8449Id:https://orcid.org/:https://orcid.org/0009-0001-6494-:https://orcid.org/0009-0004-3756-9310

[15] Kominfo, "Presentasi Jaringan Intra Pemerintah," Scibd. Accessed: Jan. 15, 2026. [Online]. Available: https://www.scribd.com/document/654891108/Presentasi-Jaringan-Intra-Pemerintah

[16] M. I. Iskandar, "Intrusion Detection System: Lapisan Pertama Keamanan Jaringan," Aplikas. Accessed: Jan. 15, 2026. [Online]. Available: https://aplikas.com/blog/intrusion-detection-system/

[17] P. Waghmode, M. Kanumuri, H. El-Ocla, and T. Boyle, "Intrusion detection system based on machine learning using least square support vector machine," *Sci. Rep.*, vol. 15, no. 1, Dec. 2025, doi: 10.1038/s41598-025-95621-7.

[18] R. Alkautsar, "Sistem Deteksi Intrusi: Lindungi Jaringan dari Ancaman," Hypernet. Accessed: Jan. 15, 2026. [Online]. Available: https://www.hypernet.co.id/id/sistem-deteksi-intrusi-lindungi-jaringan/

[19] HP Online Store, "Securing AI Systems: A Comprehensive Data Protection Guide for Indonesian Businesses," HP. Accessed: Jan. 15, 2026. [Online]. Available: https://www.hp.com/id-en/shop/tech-takes/post/ai-data-security-guide