PENGEMBANGAN SISTEM DETEKSI INTRUSI UNTUK JARINGAN KOMPUTER BERBASIS MACHINE LEARNING DI KANTOR CAMAT SENDANA KOTA PALOPO

Sealtiel[1], Siaulhak[2], Nuur Insan Tangkelangi[3]
sealtiellp29@gmail.com[1], siaulhak@uncp.ac.id[2], nuurinsan@uncp.ac.id[3]
Universitas Cokroaminoto Palopo

ABSTRAK

Tujuan penelitian ini yaitu untuk mengembangkan sistem deteksi intrusi untuk jaringan komputer berbasis machine learning di Kantor Camat Sendana Kota Palopo. Jenis penelitian yang digunakan yaitu penelitian Research and Development (R&D) yang sudah dikembangkan berdasarkan kebutuhan. Sedangkan model atau tahapan penelitian yang digunakan dalam penelitian ini model pengembangan yang digunakan adalah model pengembangan ADDIE (Analysis, Design, Development, Implementation, Evaluation) yang merupakan suatu model yang di dalamnya merepresentasikan tahapan-tahapan secara sistematika (tertata) dan sistemis dalam penggunaan bertujuan untuk tercapainya hasil yang di inginkan. Berdasarkan hasil dari rumusan masalah yang telah dikemukakan oleh penulis, maka dapat ditarik Kesimpulan bahwa sistem deteksi intrusi yang dikembangkan menggunakan algoritma SVM memberikan performa yang sangat baik dengan akurasi sebesar 99.20%. Dengan hasil confusion matrix dan classification report, dapat disimpulkan bahwa sistem ini sangat efektif dalam membedakan antara aktivitas jaringan normal dan serangan. Kemudian setelah dilakukan pengembangan sistem deteksi intrusi dengan menambahkan teknik GridSearchCV untuk mengoptimalkan hyperparameter model SVM. Hasil menunjukkan peningkatan akurasi dari 99.20% menjadi 99.46% setelah tuning, dengan kombinasi parameter terbaik: {'C': 10, 'gamma': 'scale', 'kernel': 'rbf'}. Meskipun peningkatan metrik terlihat kecil, hal ini penting dalam sistem keamanan karena berkaitan dengan kemampuan mendeteksi serangan (anomaly) secara akurat dan konsisten.
Kata Kunci: Machine Learning, Sistem Deteksi Intrusi, Kantor Camat Sendana Kota Palopo.

ABSTRACT

he purpose of this study is to develop an intrusion detection system for a computer network based on machine learning at the Sendana District Office in Palopo City. The type of research used is Research and Development (R&D) research that has been developed based on needs. While the model or stages of research used in this study, the development model used is the ADDIE development model (Analysis, Design, Development, Implementation, Evaluation) which is a model that represents the stages systematically (organized) and systematically in use aimed at achieving the desired results. Based on the results of the problem formulation that has been put forward by the author, it can be concluded that the intrusion detection system developed using the SVM algorithm provides very good performance with an accuracy of 99.20%. With the results of the confusion matrix and classification report, it can be concluded that this system is very effective in distinguishing between normal network activity and attacks. Then after the development of the intrusion detection system by adding the GridSearchCV technique to optimize the hyperparameters of the SVM model. The results show an increase in accuracy from 99.20% to 99.46% after tuning, with the best parameter combination: {'C': 10, 'gamma': 'scale', 'kernel': 'rbf'}. Although the improvement in the metric seems small, it is important in a security system because it relates to the ability to detect attacks (anomalies) accurately and consistently.
Keywords: *Machine Learning, Intrusion Detection System, Sendana District Office Palopo City.*

PENDAHULUAN

Banyaknya kejadian penyerangan jaringan dan berbagai kemungkinan cara menyerang, dibutuhkan tindakan yang harus dilakukan untuk mencegah serangan terjadi.

Salah satu infrastuktur yang terdapat pada suatu sistem komputer atau pada jaringan komputer adalah Intrusion Detection System (IDS). IDS adalah salah satu cara bagaimana mendeteksi sebuah serangan yang terjadi pada sebuah komputer atau server pada jaringan komputer. IDS akan bekerja dengan prinsip mendeteksi serangan-serangan atau percobaan intrusi dari luar sistem pada umumnya internet ke dalam suatu internal sistem. IDS akan memonitor lalu lintas jaringan, namun pada IDS dibutuhkan tindakan lebih lanjut untuk memberitahu serangan dengan karakteristik tersendiri. Dalam beberapa tahun terakhir, banyak penelitian yang mengembangkan IDS berbasis machine learning (ML) untuk meningkatkan akurasi dan efisiensi deteksi serangan (Cinderatama, Alhamri and Yunhasnawa, 2022).

Machine Learning adalah cabang aplikasi dari Artificial Intelligence (kecerdasan buatan) yang fokus pada pengembangan sebuah sistem yang mampu belajar sendiri tanpa harus berulang kali program oleh manusia (Setyawan, Firizkiansah and Nuryanto, 2021). Machine learning menawarkan potensi besar dalam mendeteksi pola serangan yang sulit dikenali oleh sistem keamanan tradisional. Teknik-teknik seperti klasifikasi dan clustering pada machine learning mampu memproses data dalam jumlah besar dan mendeteksi anomali yang mungkin menunjukkan adanya intrusi. Selain itu, penggunaan algoritma ML memungkinkan IDS untuk belajar dan berkembang dari data yang ada, sehingga dapat terus meningkatkan kemampuan deteksinya seiring waktu.

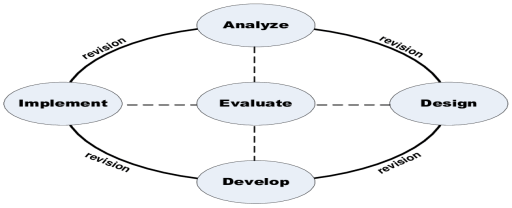
Di Kantor Camat Sendana Kota Palopo, masalah keamanan jaringan komputer masih menjadi perhatian utama. Meskipun jaringan komputer di kantor ini sudah terhubung dengan berbagai fasilitas pendukung administrasi dan pelayanan publik, banyak pegawai yang masih kurang memperhatikan pentingnya aspek keamanan jaringan. Hal ini menyebabkan kantor tersebut rentan terhadap berbagai jenis serangan yang dapat mengancam integritas data dan operasional sistem. Banyak pegawai yang belum sepenuhnya memahami risiko yang dapat timbul akibat kurangnya kesadaran dan tindakan preventif terhadap potensi ancaman siber.

Untuk itu, sangat penting bagi Kantor Camat Sendana Kota Palopo untuk mengembangkan sistem deteksi intrusi berbasis machine learning yang dapat meningkatkan keamanan jaringan komputer secara signifikan. Teknologi ini memiliki kemampuan untuk secara otomatis mendeteksi dan merespons ancaman dengan tingkat kecepatan dan akurasi yang lebih tinggi dibandingkan dengan metode konvensional. Dengan menggunakan algoritma machine learning, sistem ini mampu mempelajari pola aktivitas jaringan yang normal dan mendeteksi potensi ancaman yang tidak biasa, seperti serangan malware, DoS (Denial of Service), dan berbagai jenis eksploitasi lainnya. Hal ini memungkinkan kantor merespons ancaman dengan cepat sebelum menyebabkan kerusakan lebih besar.

Berdasarkan uraian tersebut penulis akan melakukan penelitian yang berjudul "Pengembangan Sistem Deteksi Intrusi untuk Jaringan Komputer Berbasis Machine learning di Kantor Camat Sendana Kota Palopo".

METODOLOGI

Penelitian ini termasuk dalam kategori penelitian pengembangan (*Research and Development*/R&D) yang bertujuan untuk menciptakan sebuah sistem berbasis teknologi yang inovatif. Dalam hal ini, penelitian berfokus pada pengembangan sistem deteksi *intrusi* (*Intrusion Detection System*/IDS) dengan memanfaatkan algoritma *machine learning*. Model penelitian yang digunakan adalah model ADDIE (*Analysis, Design, Development, Implementation, Evaluation*) yang sesuai dengan langkah-langkah sistematis dalam pengembangan teknologi.



Gambar 1. Konsep model ADDIE
Sumber: www.google.com (2025)

Tahapan penelitian ini dimulai dari pengumpulan data melalui observasi, wawancara, dan studi pustaka, lalu dilanjutkan dengan analisis data. Hasil analisis digunakan untuk merancang sistem, yang kemudian dikembangkan. Setelah itu, sistem dievaluasi dan menghasilkan hasil akhir penelitian. Selama pengembangan, berbagai metode pengujian diterapkan untuk memastikan keandalan dan akurasi sistem deteksi intrusi. Evaluasi dilakukan dengan membandingkan hasil deteksi sistem terhadap serangan yang disimulasikan dalam lingkungan pengujian. Hasil penelitian ini diharapkan menjadi referensi bagi pengelola jaringan dalam meningkatkan keamanan sistem mereka. Selain itu, penelitian ini mengidentifikasi tantangan yang muncul selama implementasi, seperti optimasi algoritma deteksi dan integrasi dengan infrastruktur jaringan yang ada.

Sistem IDS berbasis *machine learning* akan dirancang untuk mendeteksi anomali dalam lalu lintas jaringan secara otomatis. Sistem ini akan mengklasifikasikan data sebagai normal atau berbahaya menggunakan model *machine learning* (misalnya, *Random Forest* atau SVM).

HASIL DAN PEMBAHASAN

Penelitian ini bertujuan untuk mengembangkan sistem deteksi *intrusi* untuk jaringan komputer berbasis *machine learning* di Kantor Camat Sendana Kota Palopo. Metode yang digunakan dalam penelitian ini adalah *research and development* (R&D) dengan tujuan menghasilkan suatu sistem berbasis teknologi yang inovatif. Dalam hal ini, penelitian berfokus pada pengembangan sistem deteksi *intrusi* (*Intrusion Detection System*/IDS) dengan memanfaatkan algoritma *machine learning*. Sedangkan model pengembangan yang digunakan adalah model pengembangan *ADDIE (Analysis, Design, Development, Implementation, Evaluation)* yang merupakan suatu model yang di dalamnya merepresentasikan tahapan-tahapan secara sistematika (tertata) dan sistemis dalam penggunaan bertujuan untuk tercapainya hasil yang di inginkan.

Analysis

Di Kantor Camat Sendana Kota Palopo, masalah keamanan jaringan komputer masih menjadi perhatian utama. Meskipun jaringan komputer di kantor ini sudah terhubung dengan berbagai fasilitas pendukung administrasi dan pelayanan publik, banyak pegawai yang masih kurang memperhatikan pentingnya aspek keamanan jaringan. Hal ini menyebabkan kantor tersebut rentan terhadap berbagai jenis serangan yang dapat mengancam integritas data dan operasional sistem. Banyak pegawai yang belum sepenuhnya memahami risiko yang dapat timbul akibat kurangnya kesadaran dan tindakan preventif terhadap potensi ancaman siber. Kebijakan keamanan yang ada saat ini di Kantor Camat Sendana Kota Palopo masih belum optimal, dan hal ini menyebabkan deteksi serta mitigasi terhadap ancaman keamanan menjadi kurang efektif. Tanpa adanya pengawasan yang memadai terhadap aktivitas jaringan, potensi serangan seperti DoS (*Denial of Service*) atau penyebaran virus melalui jaringan seringkali terjadi tanpa terdeteksi. Akibatnya, serangan tersebut dapat merusak integritas data dan sistem, mengganggu kelancaran administrasi, serta merugikan layanan publik yang seharusnya berjalan dengan lancar.

Design

Tahap perancangan ini penulis akan membuat gambar *design topology* jaringan interkoneksi yang akan dibangun, *design* bisa berupa design struktur *topology*, design akses data, *design* tata layout perkabelan, dan sebagainya yang akan memberikan gambaran jelas tentang *network* yang akan dibangun serta hasil analisis kebutuhan perangkat, kebutuhan pengguna, dan kebutuhan layanan yang di perlukan.

Gambar 2. Topologi Jaringan

a. Analisis Kebutuhan Perangkat Keras (*Hardware*)

1) Laptop Intel® Celeron® N4020 (2 core / 2 thread, 1.1 GHz hingga 2.8 GHz, cache 4MB)
2) Perangkat *input* dan *output.*

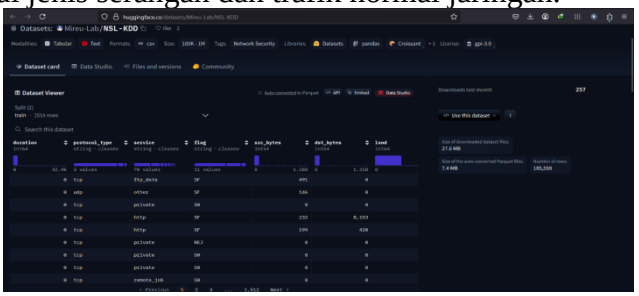
b. Analisis Kebutuhan Perangkat Lunak (*Software*)

1) Sistem Operasi *Windows* 10 64 bit.
2) *Power Shell (CMD)*
3) *Python 3*
4) *Pandas*
5) *Numpy*
6) *scikit-learn*
7) *datasets*
8) *matplotlib*
9) *seaborn*
10) *joblib*

3. Development

a. Dataset

Dataset yang digunakan adalah NSL-KDD, versi perbaikan dari dataset KDD Cup 1999. Dataset ini banyak digunakan untuk penelitian sistem deteksi intrusi karena mengandung berbagai jenis serangan dan trafik normal jaringan.



Gambar 3. *Dataset*

b. Pembuatan *Machine Learning*

Setelah dataset didapatkan maka proses selanjutnya adalah membuat *machine*

learning untuk *Intrusion Detection System* (IDS) menggunakan *power shell (CMD)* dengan bahasa pemongaman *python 3*.

```
D:
cd D:\
mkdir ids-nsl-kdd
cd ids-nsl-kdd
```

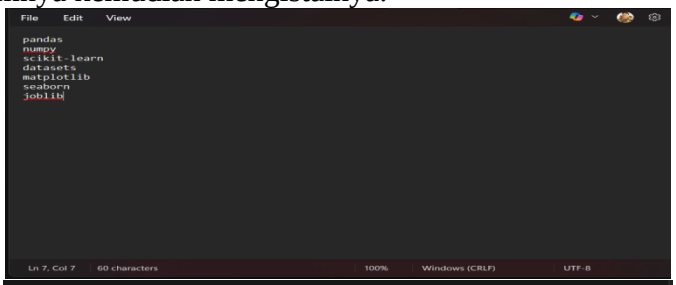
Gambar 4. Pembuatan Folder *Machine Learning*

```
python -m venv env
```

```
.\env\Scripts\Activate
```

Gambar 5. Pembuatan *Virual Environment* dan Mengaktifkan

Selanjutnya membuka notepad dan memasukkan libraly yang dibutuhkan untuk membuat *machine learning* kemudain save dengan nama "requirement.txt" pada folder yang telah dibuat sebelumnya kemudian mengistalnya.




```
pip install -r requirements.txt
```

```
(env) PS D:\ids-nsl-kdd> pip install -r requirements.txt
Collecting pandas
  Downloading pandas-2.2.3-cp311-cp311-win_amd64.whl (11.6 MB)
     ---------------------------------------- 11.6/11.6 MB 3.6 MB/s eta 0:00:00
Collecting numpy
  Using cached numpy-2.2.5-cp311-cp311-win_amd64.whl (12.9 MB)
Collecting scikit-learn
  Downloading scikit_learn-1.6.1-cp311-cp311-win_amd64.whl (11.1 MB)
     ---------------------------------------- 11.1/11.1 MB 3.7 MB/s eta 0:00:00
```

Gambar 6. Pembuatan dan Penginstalan *Libraly*

Langkah selanjutnya membuat skrip *main.py* untuk menjalankan *machine learning* yang telah dibuat menggunakan notepad kemudian save pada folder projek yang telah dibuat sebelumnya kemudian jalankan *machine learning* menggunakan perintah pada gambar di bawah ini.

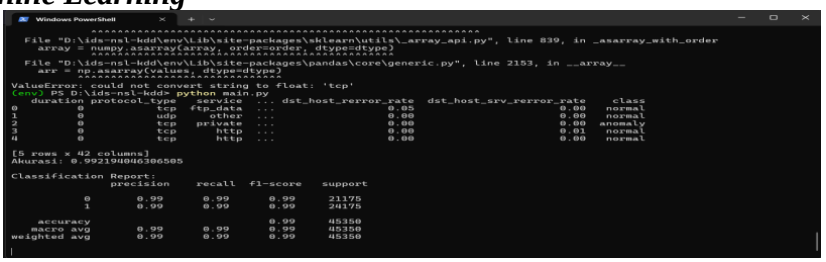
```
from datasets import load_dataset
import pandas as pd
from sklearn.preprocessing import LabelEncoder, StandardScaler
from sklearn.model_selection import train_test_split
from sklearn.svm import SVC
from sklearn.metrics import classification_report, accuracy_score
import matplotlib.pyplot as plt
import seaborn as sns
from sklearn.metrics import confusion_matrix
import joblib

# Muat dataset NSL-KDD dari Hugging Face
dataset = load_dataset("Mireu-Lab/NSL-KDD")

# Konversi dataset ke DataFrame
df = pd.DataFrame(dataset["train"])

# Pisahkan fitur dan label
X = df.drop(columns=["class"])
y = df["class"]

# Encode label (normal/anomaly)
label_encoder = LabelEncoder()
y_encoded = label_encoder.fit_transform(y)
```

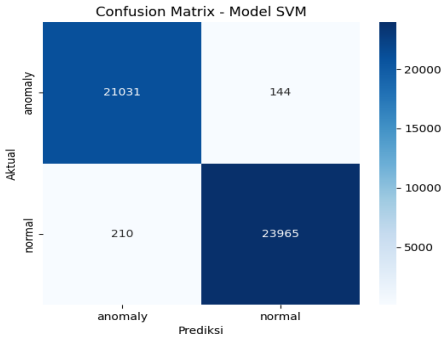
Ln 58, Col 1 1,729 characters 100% Windows (CRLF) UTF-8

```
python main.py
```

Gambar 7. Pembuatan dan Menjalankan *Main.py*

c. Hasil *Machine Learning*





Gambar 8. Hasil *Machine Learning*

Setelah dilakukan pelatihan dan pengujian terhadap model *Support Vector Machine* (SVM), hasil evaluasi kinerja model berdasarkan dataset pengujian ditunjukkan dalam di bawah ini.

Tabel 1 Hasil *Confusion Matrix*

Aktual \ Prediksi	*Anomaly*	Normal
Anomaly	21.031	144
Normal	210	23.965

Sumber: Hasil Olah Data (2025)

Tabel 2 Hasil Classification Report

Metric	*Anomaly (0)*	*Normal (1)*	*Macro Avg*	*Weighted Avg*
Precision	0.99	0.99	0.99	0.99
Recall	0.99	0.99	0.99	0.99
F1-Score	0.99	0.99	0.99	0.99
Support	21.175	24.175	45.350	45.350

Sumber: Hasil Olah Data (2025)

Sistem deteksi intrusi yang dikembangkan menggunakan algoritma SVM memberikan performa yang sangat baik dengan akurasi sebesar 99.21%. Dengan hasil *confusion matrix* dan *classification report*, dapat disimpulkan bahwa sistem ini sangat efektif dalam membedakan antara aktivitas jaringan normal dan serangan.

4. Implementasi

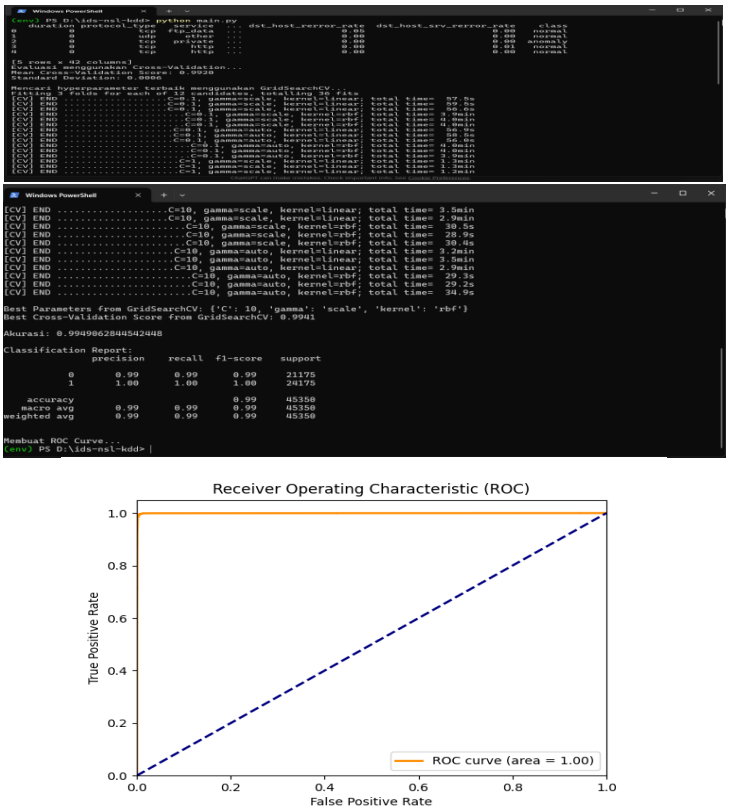
Pada tahap ini penulis akan melakukan penngembangan *machine learning* sistem deteksi *intrusi* menggunakan algoritma SVM agar dapat lebih akurat untuk mendeteksi aktifitas normal dan serangan. Pada pengembangan ini penulis menambahkan dua pengembangan utama yaitu *cross-validation* dan *hyperparameter tuning – gridsearchcv* pada sistem yang sebelumnya. Hasil dapat dilihat pada gambar di bawah ini.

```
from sklearn.model_selection import cross_val_score


# Cross-validation
cv_scores = cross_val_score(model, X_scaled, y_encoded, cv=5)
print(f"Mean Cross-Validation Score: {cv_scores.mean():.4f}")
```

Gambar 9. Skrip *Cross Validation*

```
from sklearn.model_selection import GridSearchCV

# Definisikan parameter yang akan diuji
param_grid = {
    'C': [0.1, 1, 10],
    'gamma': ['scale', 'auto'],
    'kernel': ['linear', 'rbf']
}

# Terapkan GridSearchCV
grid_search = GridSearchCV(SVC(), param_grid, refit=True, verbose=2, cv=3)
```

Gambar 10. Skrip *Hyperparameter Tuning Gridsearchcv*



Gambar 11. Hasil *Machine Learning* Setelah Pengembangan

Setelah dilakukan pelatihan dan pengujian terhadap model *Support Vector Machine* (SVM) yang telah dikembangkan, hasil evaluasi kinerja model berdasarkan dataset pengujian ditunjukkan dalam di bawah ini.

Tabel 3 Hasil *Cross Validation*

Aktual \ Prediksi	*Score*	Keterangan
Mean Cross Validation	0.9920	Melakukan *mean corss* validation pada model SVM
Standart Deviation	0.0006	Melakukan *standart deviation* pada model SVM

Sumber: Hasil Olah Data (2025)

Tabel 4. Hasil *Classification Report*

Metric	*Anomaly (0)*	*Normal (1)*	*Macro Avg*	*Weighted Avg*
Precision	0.99	1.00	0.99	0.99
Recall	0.99	1.00	0.99	0.99
F1-Score	0.99	1.00	0.99	0.99
Support	21.175	24.175	45.350	45.350

Sumber: Hasil Olah Data (2025)

Sistem deteksi intrusi yang dikembangkan menggunakan algoritma SVM memberikan performa yang sangat baik dengan akurasi sebesar 99.49%. Dengan hasil *cross validation* dan *hyperparameter tuning gridsearchcv*, dapat disimpulkan bahwa Model SVM yang dikembangkan mampu mendeteksi intrusi jaringan dengan sangat baik. Akurasi tinggi dan nilai AUC = 1.00 menandakan bahwa model sangat andal dalam klasifikasi trafik jaringan sebagai normal atau serangan (*anomaly*).

Setelah melakukan pengembangan *machine learning*, kemudian penulis melakukan penyerangan pada IDS menggunakan *hydra* untuk mengetahui apakah *machine learning* mampu medeteksi sebuah serangan sebagai anomali dan memberikan *alert*.

Tabel 5. Hasil Deteksi *IDS*

Timestamp	*Source IP*	*Source Port*	*Destination IP*	*Destination Port*	Hasil
2025-05-22 14:25:01	192.168.1.10	45678	192.168.1.5	80	Anomali
2025-05-22 14:26:10	192.168.1.11	50321	192.168.1.2	22	Normal
2025-05-22 14:27:30	192.168.1.13	60000	192.168.1.6	445	Anomali
2025-05-22 14:29:44	192.168.1.20	30000	192.168.1.1	80	Normal

Sumber: Hasil Olah Data (2025)

Berdasarkan tabel di atas, dari 4 *traffic* yang dianalisis, 2 insiden diklasifikasikan sebagai *serangan* oleh model SVM. Model berhasil menyaring lalu lintas yang dicurigai oleh *Snort* dan memberikan klasifikasi lebih lanjut. Dua dari empat *alert Snort* ternyata merupakan lalu lintas normal menurut SVM, menunjukkan bahwa model ini membantu mengurangi *false positive* dari *Snort*. *Port* 80 (HTTP) dan Port 445 (SMB) muncul sebagai protokol umum dalam lalu lintas yang diklasifikasikan sebagai serangan. Ini menunjukkan bahwa serangan kemungkinan berkaitan dengan eksploitasi layanan *web* dan *file sharing*.

5. Evaluasi

a. Pengembangan

Berdasarkan hasil pengembangan pada tahap sebelumnya dapat dilihat perbandingan antara *machine learning* menggunakan algoritma SVM sebelum dan sedudah dilakukan pengembangan pada tabel dibawah ini.

Tabel 6. Sebelum Pengembangan

Label	Precision	Recall	F1-Score	Support
Anomaly (0)	0.99	0.99	0.99	21175
Normal (1)	0.99	0.99	0.99	24175
Accuracy			0.99	45350
Macro Avg	0.99	0.99	0.99	45350
Weighted Avg	0.99	0.99	0.99	45350

Sumber: Hasil Olah Data (2025)

Tabel 7. Setelah Pengembangan

Label	Precision	Recall	F1-Score	Support
Anomaly (0)	0.99	0.99	0.99	21175
Normal (1)	1.00	1.00	1.00	24175
Accuracy			0.9949	45350
Macro Avg	0.99	0.99	0.99	45350
Weighted Avg	0.99	0.99	0.99	45350

Sumber: Hasil Olah Data (2025)

Tabel 8. Perbandingan

Tahap	Akurasi	Keterangan
Awal	~98.72%	Menggunakan model SVM default
Setelah *Cross-Validation*	99.20%	Stabilitas model diuji
Setelah *GridSearchCV*	99.49%	Performa tertinggi tercapai

Sumber: Hasil Olah Data (2025)

Berdasarkan tabel di atas Pengembangan sistem deteksi intrusi dilakukan dengan menggunakan teknik *GridSearchCV* untuk mengoptimalkan *hyperparameter* model SVM. Hasil menunjukkan peningkatan akurasi dari 0.9920 menjadi 0.9949 setelah tuning, dengan kombinasi parameter terbaik: {'C': 10, 'gamma': 'scale', 'kernel': 'rbf'}. Meskipun

peningkatan metrik terlihat kecil, hal ini penting dalam sistem keamanan karena berkaitan dengan kemampuan mendeteksi serangan (*anomaly*) secara akurat dan konsisten.

KESIMPULAN

Berdasarkan hasil dari penelitian ini dapat ditarik kesimpulan bahwa sistem deteksi intrusi untuk jaringan komputer berbasis machine learning di Kantor Camat Sendana Kota Palopo. Sistem deteksi intrusi yang dikembangkan menggunakan algoritma SVM memberikan performa yang sangat baik dengan akurasi sebesar 99.20%. Dengan hasil confusion matrix dan classification report, dapat disimpulkan bahwa sistem ini sangat efektif dalam membedakan antara aktivitas jaringan normal dan serangan. Kemudian setelah dilakukan pengembangan sistem deteksi intrusi dengan menambahkan teknik GridSearchCV untuk mengoptimalkan hyperparameter model SVM. Hasil menunjukkan peningkatan akurasi dari 99.20% menjadi 99.46% setelah tuning, dengan kombinasi parameter terbaik: {'C': 10, 'gamma': 'scale', 'kernel': 'rbf'}. Meskipun peningkatan metrik terlihat kecil, hal ini penting dalam sistem keamanan karena berkaitan dengan kemampuan mendeteksi serangan (anomaly) secara akurat dan konsisten.

DAFTAR PUSTAKA

Bustami, A. and Bahri, S. (2020) 'Tanpa perlindungan yang memadai berupa keamanan jaringan atau sistem informasi, organisasi berisiko kehilangan aset informasi mereka.', Unistek, 7(2), pp. 59–70.

Chazar, C. and Erawan, B. (2020) 'Machine Learning Diagnosis Kanker Payudara Menggunakan Algoritma Support Vector Machine', INFORMASI (Jurnal Informatika dan Sistem Informasi), 12(1), pp. 67–80. Available at: https://doi.org/10.37424/informasi.v12i1.48.

Cinderatama, T.A., Alhamri, R.Z. and Yunhasnawa, Y. (2022) 'Implementasi Metode K-Means, Dbscan, Dan Meanshift Untuk Analisis Jenis Ancaman Jaringan Pada Intrusion Detection System', INOVTEK Polbeng - Seri Informatika, 7(1), p. 169. Available at: https://doi.org/10.35314/isi.v7i1.2336.

Fauzi, R., Muhyidin, Y. and Singasatia, D. (2023) 'Sistem Keamanan Jaringan Komputer Berbasis Teknik Intrusion Detection System (IDS) Untuk Mendeteksi Serangan Distrubuted Denial Of Service (DDOS)', Jurnal Sains Komputer & Informatika (J-SAKTI, 7(1), pp. 72–86.

Indri Widya Wulandari and Hwihanus Hwihanus (2023) 'Peran Sistem Informasi Akuntansi Dalam Pengaplikasian Enkripsi Terhadap Peningkatan Keamanan Perusahaan', Jurnal Kajian dan Penalaran Ilmu Manajemen, 1(1), pp. 11–25. Available at: https://doi.org/10.59031/jkpim.v1i1.46.

Kurniawan, R. et al. (2023) 'Implementasi Arsitektur Xception Pada Model Machine Learning Klasifikasi Sampah Anorganik', Jurnal Informatika dan Teknik Elektro Terapan, 11(2), pp. 233–236. Available at: https://doi.org/10.23960/jitet.v11i2.3034.

Laksana, T.G. and Mulyani, S. (2024) 'Pengetahuan Dasar Identifikasi Dini Deteksi Serangan Kejahatan Siber Untuk Mencegah Pembobolan Data Perusahaan', Jurnal Ilmiah Multidisiplin, 3(01), pp. 109–122. Available at: https://doi.org/10.56127/jukim.v3i01.1143.

Mananggel, A.V., Mewengkang, A. and Djamen, A.C. (2021) 'Perancangan Jaringan Komputer Di Smk Menggunakan Cisco Packet Tracer', Edutik : Jurnal Pendidikan Teknologi Informasi dan Komunikasi, 1(2), pp. 119–131. Available at: https://doi.org/10.53682/edutik.v1i2.1124.

Maulana, Ilham, A. and Program (2022) 'Optimalisasi Deteksi Serangan DDoS Menggunakan Algoritma Random Forest, SVM, KNN dan MLP pada Jaringan Komputer', Indonesian Journal of Mathematics and Natural Sciences, 45(1), pp. 1–8.

Noor, E. and Chandra, J.C. (2020) 'Implementasi Firewall Pada Smp Yadika 5 Jakarta', IDEALIS : InDonEsiA journaL Information System, 3(1), pp. 449–456. Available at: https://doi.org/10.36080/idealis.v3i1.2088.

Papaceda, D.D., Mewengkang, A. and Pratasik, S. (2023) 'Analisis dan Pengembangan Jaringan Komputer di SMK Negeri 8 Weda Halmahera Tengah', Edutik : Jurnal Pendidikan Teknologi

Informasi dan Komunikasi, 3(1), pp. 1–13. Available at: https://doi.org/10.53682/edutik.v3i1.6465.
Pratomo, A.B. (2023) 'Pengembangan Sistem Firewall Pada Jaringan Komputer Berbasis Mikrotik Routeros', Bulletin of Network Engineer and Informatics, 1(2), p. 51. Available at: https://doi.org/10.59688/bufnets.v1i2.10.
Purba, W.W. and Efendi, R. (2021) 'Perancangan dan analisis sistem keamanan jaringan komputer menggunakan SNORT', Aiti, 17(2), pp. 143–158. Available at: https://doi.org/10.24246/aiti.v17i2.143-158.
Putra Rahmadi and Hilda Dwi Yunita (2020) 'Implementasi Pengamanan Basis Data Dengan Teknik Enkripsi', Jurnal Cendikia, 19(1), pp. 413–418.
Ritonga, A.P., Andini, N.P. and Iklmah, L. (2022) 'Pengembangan Bahan Ajaran Media', Jurnal Multidisiplin Dehasen (MUDE), 1(3), pp. 343–348. Available at: https://doi.org/10.37676/mude.v1i3.2612.
Rivaldi, O. and Marpaung, N.L. (2023) 'Penerapan Sistem Keamanan Jaringan Menggunakan Intrusion Prevention System Berbasis Suricata', INOVTEK Polbeng - Seri Informatika, 8(1), p. 141. Available at: https://doi.org/10.35314/isi.v8i1.3269.
Riza, F. (2022) 'Sistem Deteksi Intrusi pada Server secara Realtime Menggunakan Seleksi Fitur dan Firebase Cloud Messaging', Jurnal Sistim Informasi dan Teknologi, 5, pp. 7–9. Available at: https://doi.org/10.37034/jsisfotek.v5i1.161.
Saputri (2023) 'Penerapan AAA Security Dalam Aplikasi BNI Mobile Banking', Indonesian Journal of Innovation Multidisipliner Research, 63, pp. 63–73.
Sari (2024) 'Implementasi Machine Learning untuk Deteksi Intrusi pada Jaringan Komputer', 13(September), pp. 1389–1394.
Setyawan, O., Firizkiansah, A. and Nuryanto, A. (2021) 'Klasifikasi Tingkat Keparahan Serangan Jaringan Komputer Dengan Metode Machine Learning', Journal of Information System, Informatics and Computing, 5(1), p. 128. Available at: https://doi.org/10.52362/jisicom.v5i1.443.
Wardhani, N.F. (2024) 'Penggunaan Machine Learning Dalam Deteksi Intrusi Pada Jaringan Komputer', Duniadata.org, 1(4), pp. 1–16.