Model Prediksi Keamanan Siber Menggunakan Artificial Intelligence untuk Mitigasi Ancaman Digital

M Budi Hartanto[*1], Triyugo Winarko[2], Hilda Dwi Yunita[3], Fatimah Fahurian[4], Yodhi Yuniarthe[5], Khozainuz Zuhri[6]

[1]Program Studi Teknologi Informasi, Universitas Mitra Indonesia, Bandar Lampung

[2-4]Program Studi Sistem Informasi, Universitas Mitra Indonesia, Bandar Lampung

[5-6]Program Studi Informatika, Universitas Mitra Indonesia, Bandar Lampung

E-mail: budi.hartanto@umitra.ac.id[1], triyugo_win@umitra.ac.id[2], hildadwiyunita@umitra.ac.id[3], fatimah_fahurian@umitra.ac.id[4],yodhi@umitra.ac.id[5], zuhri@umitra.ac.id[6]

Abstrak. Keamanan siber menjadi isu krusial dalam era transformasi digital, terutama dengan meningkatnya ancaman serangan ransomware yang menargetkan infrastruktur digital pemerintah. Studi ini mengembangkan model prediksi keamanan siber berbasis kecerdasan buatan untuk mitigasi ancaman digital. Model yang diusulkan menggunakan teknik machine learning untuk mendeteksi pola serangan berdasarkan dataset historis. Penelitian ini menganalisis performa beberapa algoritma, termasuk Random Forest, Support Vector Machine, dan Deep Learning, untuk mengidentifikasi metode yang paling efektif dalam klasifikasi ancaman. Evaluasi dilakukan dengan menggunakan metrik akurasi, precision-recall, dan F1-score untuk mengukur kinerja model. Hasil eksperimen menunjukkan bahwa pendekatan berbasis kecerdasan buatan mampu meningkatkan deteksi dini serangan ransomware secara signifikan, sehingga memberikan wawasan bagi pengambil kebijakan dalam meningkatkan ketahanan sistem keamanan siber. Temuan ini diharapkan dapat menjadi landasan bagi pengembangan sistem pertahanan siber yang lebih adaptif dan proaktif dalam menghadapi ancaman digital di masa depan.

Kata kunci: keamanan siber; kecerdasan buatan; machine learning; deteksi ancaman; ransomware

Abstract. *Cybersecurity has become a critical issue in the era of digital transformation, especially with the increasing threat of ransomware attacks targeting government digital infrastructure. This study develops an artificial intelligence-based cybersecurity prediction model to mitigate digital threats. The proposed model utilizes machine learning techniques to detect attack patterns based on historical datasets. This research analyzes the performance of several algorithms, including Random Forest, Support Vector Machine, and Deep Learning, to identify the most effective method for threat classification. The evaluation is conducted using accuracy, precision-recall, and F1-score metrics to measure model performance. Experimental results indicate that artificial intelligence-based approaches significantly enhance early ransomware attack detection, providing valuable insights for policymakers in strengthening cybersecurity resilience. These findings are expected to serve as a foundation for developing more adaptive and proactive cyber defense systems against future digital threats..*

Keywords: *cybersecurity; artificial intelligence; machine learning; threat detection; ransomware.*

1. Pendahuluan

Keamanan siber menjadi salah satu tantangan utama dalam era transformasi digital, terutama dengan meningkatnya ancaman serangan ransomware yang menargetkan infrastruktur digital pemerintah dan organisasi besar [1]. Ransomware adalah salah satu bentuk serangan siber yang mengenkripsi data korban dan menuntut pembayaran tebusan untuk pemulihan akses. Dampak dari serangan ini tidak hanya menyebabkan kerugian finansial yang signifikan tetapi juga mengancam integritas dan ketersediaan data yang krusial bagi operasional organisasi [2].

Berbagai metode telah dikembangkan untuk mengatasi ancaman ini, termasuk sistem deteksi berbasis tanda tangan dan heuristik. Namun, metode konvensional ini memiliki keterbatasan dalam mengenali pola serangan baru yang terus berkembang secara dinamis [3]. Oleh karena itu, kecerdasan buatan (AI) dan machine learning (ML) semakin banyak digunakan untuk meningkatkan deteksi dan mitigasi serangan siber. Algoritma pembelajaran mesin memungkinkan sistem untuk menganalisis pola data historis dan mengidentifikasi potensi serangan sebelum menyebabkan kerusakan yang lebih luas [4].

Penelitian terbaru menunjukkan bahwa model berbasis AI dapat secara signifikan meningkatkan kemampuan deteksi ancaman siber dibandingkan dengan metode tradisional. Misalnya, pendekatan deep learning menggunakan jaringan saraf tiruan telah menunjukkan hasil yang menjanjikan dalam mendeteksi malware dan serangan siber lainnya dengan tingkat akurasi yang tinggi[5]. Selain itu, kombinasi berbagai algoritma seperti Random Forest, *Support Vector Machine* (SVM), dan Long Short-Term Memory (LSTM) telah diuji dalam berbagai penelitian untuk meningkatkan efektivitas dalam klasifikasi serangan siber [6].

Meningkatnya konektivitas global dan penggunaan perangkat *Internet of Things* (IoT) juga telah memperluas permukaan serangan bagi para peretas. Infrastruktur penting, termasuk layanan kesehatan, energi, dan keuangan, semakin menjadi sasaran empuk bagi serangan ransomware yang dapat melumpuhkan layanan dalam waktu singkat [7]. Oleh karena itu, dibutuhkan pendekatan berbasis AI yang tidak hanya mampu mendeteksi serangan secara real-time tetapi juga dapat memberikan respons adaptif terhadap ancaman yang muncul [8].

Selain itu, salah satu tantangan utama dalam implementasi AI untuk keamanan siber adalah keterbatasan dataset yang representatif dan berkualitas tinggi. Model pembelajaran mesin sangat bergantung pada data yang digunakan untuk pelatihannya, dan kurangnya data yang mencerminkan serangan dunia nyata dapat mengurangi efektivitas model dalam menghadapi ancaman baru [9]. Oleh karena itu, pengembangan model AI harus mempertimbangkan teknik augmentasi data dan federated learning untuk meningkatkan generalisasi model terhadap berbagai jenis serangan siber [10].

Dari perspektif kebijakan, regulasi mengenai keamanan siber juga harus diperkuat untuk mendukung implementasi AI dalam mitigasi ancaman digital. Beberapa negara telah mulai mengadopsi pendekatan berbasis AI dalam sistem keamanan nasional mereka, tetapi masih banyak tantangan yang perlu diatasi, termasuk aspek etika, transparansi, dan privasi dalam penggunaan teknologi AI untuk keamanan siber [11]. Oleh karena itu, kerja sama antara akademisi, industri, dan pemerintah sangat diperlukan untuk mengembangkan standar keamanan yang dapat mengakomodasi perkembangan teknologi AI [12].

Penelitian ini bertujuan untuk mengembangkan model prediksi keamanan siber berbasis AI yang lebih akurat dan adaptif dalam mendeteksi ancaman digital, khususnya serangan ransomware. Hasil penelitian ini diharapkan dapat memberikan kontribusi dalam meningkatkan ketahanan sistem keamanan siber serta memberikan wawasan bagi pengambil kebijakan dalam mitigasi risiko siber di era digital yang semakin kompleks. Dengan pendekatan berbasis AI yang lebih canggih, diharapkan sistem keamanan siber masa depan dapat lebih proaktif dalam menghadapi ancaman yang terus berkembang.

2. Metode

2.1. Pendekatan Penelitian

Penelitian ini menggunakan metode eksperimental dengan pendekatan *machine learning* dan *deep learning* untuk mendeteksi serangan ransomware pada infrastruktur digital pemerintah. Algoritma yang digunakan difokuskan pada pengenalan pola serangan, analisanomaly, serta klasifikasi ancaman keamanan siber. Model AI dilatih menggunakan dataset serangan ransomware dan diuji untuk mengukur efektivitasnya dalam mendeteksi ancaman secara real-time[1].

2.2. Dataset dan Preprocessing

Dataset yang digunakan dalam penelitian ini berasal dari beberapa sumber kredibel, termasuk CICIDS 2017, MalwareBazaar, dan CTU-13 yang merupakan dataset yang sering digunakan dalam penelitian keamanan siber. Langkah-langkah *preprocessing* dilakukan untuk memastikan kualitas data yang baik, seperti:

a. *Data Cleaning*: Menghilangkan duplikasi, mengatasi nilai yang hilang (*missing values*), serta mengonversi data non-numerik menjadi numerik menggunakan teknik *One-Hot Encoding* [12].
b. *Feature Scaling*: Menggunakan Min-Max Scaling dan *Standardization* agar semua fitur memiliki skala yang seragam [5].
c. *Feature Selection*: Menggunakan *Principal Component Analysis* (PCA) untuk mengurangi dimensi data dan meningkatkan efisiensi model [10].
d. *Data Augmentation*: Menggunakan metode SMOTE (*Synthetic Minority Over-sampling Technique*) untuk menangani ketidakseimbangan data ransomware dan memastikan model dapat mengenali serangan dengan baik[2].

Tabel 1. Menjelaskan Tahapan *Preprocessing* Secara Lebih Rinci

Tahap	Metode	Deskripsi
Data Collection	CICIDS 2017, CTU-13, MalwareBazaar	Mengumpulkan data serangan ransomware dan lalu lintas jaringan normal
Data Cleaning	*Handling Missing Values*	Menghapus data yang tidak lengkap atau redundan
Feature Engineering	PCA, *One-Hot Encoding*	Menstandarisasi dan mengurangi dimensi data
Data Splitting	80% *Training* - 20% *Testing*	Memisahkan dataset untuk pelatihan dan pengujian model

2.3. Model dan Algoritma

Dalam penelitian ini, tiga model utama digunakan untuk mendeteksi serangan ransomware:

a. *Convolutional Neural Network* (CNN): Menganalisis pola serangan dengan teknik *deep learning* berbasis gambar dan sinyal jaringan [9].
b. *Long Short-Term Memory* (LSTM): Menggunakan analisis berbasis urutan waktu (*time-series*) untuk mendeteksi serangan berdasarkan pola historis lalu lintas jaringan[7].
c. *Random Forest* (RF): Model berbasis pohon keputusan yang digunakan sebagai baseline untuk membandingkan performa metode deep learning [11].

2.3.1. Arsitektur Model CNN

Model CNN dalam penelitian ini memiliki arsitektur sebagai berikut:

a. Layer Konvolusi (Conv2D) dengan ReLU Activation
b. MaxPooling Layer untuk reduksi dimensi fitur
c. *Fully Connected Layer* untuk klasifikasi serangan ransomware

Rumus utama yang digunakan dalam CNN adalah:

$$f(x) = \max(0, x)$$

dimana $f(x)$ adalah fungsi aktivasi ReLU yang membantu model mengenali pola serangan secara lebih efisien [8].

2.3.2. Arsitektur Model LSTM

Model LSTM digunakan untuk mendeteksi pola anomali pada lalu lintas jaringan berdasarkan data sekuensial. Fungsi sel LSTM dapat dirumuskan sebagai berikut:

$$f_t = \sigma\big(W_f \cdot [h_{t-1}, x_t] + b_f\big)$$

$$i_t = \sigma(W_i \cdot [h_{t-1}, x_t] + b_i)$$

$$C_t = f_t * C_{t-1} + i_t * \tanh(W_C \cdot [h_{t-1}, x_t] + b_C)$$

Di mana:

- f_t: Forget gate
- i_t: Input gate
- C_t: Memori sel

LSTM terbukti efektif dalam mendeteksi pola ransomware yang bersifat sekuensial dalam lalu lintas jaringan [3].

2.4. Evaluasi dan Validasi

Evaluasi model dilakukan dengan beberapa metrik performa sebagai berikut:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

$$Precision = \frac{TP}{TP + FP}$$

$$Recall = \frac{TP}{TP + FN}$$

$$F1\text{-}Score = 2 \times \frac{Precision \times Recall}{Precision + Recall}$$

2.4.1. Metode Validasi

- K-Fold Cross Validation (k=10) digunakan untuk mengurangi bias dalam pengujian model [10].
- ROC Curve digunakan untuk menganalisis trade-off antara true positive rate (TPR) dan false positive rate (FPR)[1].
- Confusion Matrix digunakan untuk mengevaluasi jumlah prediksi benar dan salah.

2.4.2. Tabel Hasil Evaluasi

Setelah dilakukan pengujian, hasil evaluasi model ditampilkan dalam tabel berikut:

Tabel 2. Hasil evaluasi, model **LSTM** menunjukkan kinerja terbaik dalam mendeteksi ransomware dibandingkan dengan CNN dan Random Forest

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
CNN	**96.5**	94.2	95.8	95.0

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
LSTM	**97.1**	95.4	96.2	95.8
Random Forest	92.8	90.5	91.3	90.9

3. Hasil dan Pembahasan

3.1. Eksperimen dan Implementasi Model

Eksperimen dilakukan menggunakan dataset CICIDS 2017, CTU-13, dan MalwareBazaar. Dataset ini telah diproses menggunakan data cleaning, feature engineering, dan data augmentation untuk meningkatkan kualitas model dalam mendeteksi serangan ransomware.
Model yang diuji dalam penelitian ini adalah:

a. *Convolutional Neural Network* (CNN)
b. *Long Short-Term Memory* (LSTM)
c. *Random Forest* (RF) sebagai baseline model

Masing-masing model diuji menggunakan k-fold cross-validation (k=10) untuk menghindari bias dan menghasilkan hasil yang lebih reliabel[12].

3.2. Evaluasi Model Berdasarkan Metrik Kinerja

Evaluasi model dilakukan menggunakan akurasi, presisi, recall, dan F1-score, yang merupakan metrik standar dalam klasifikasi keamanan siber [5].

Tabel 3. Hasil Evaluasi Model

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
CNN	**96.5**	94.2	95.8	95.0
LSTM	**97.1**	95.4	96.2	95.8
Random Forest	92.8	90.5	91.3	90.9

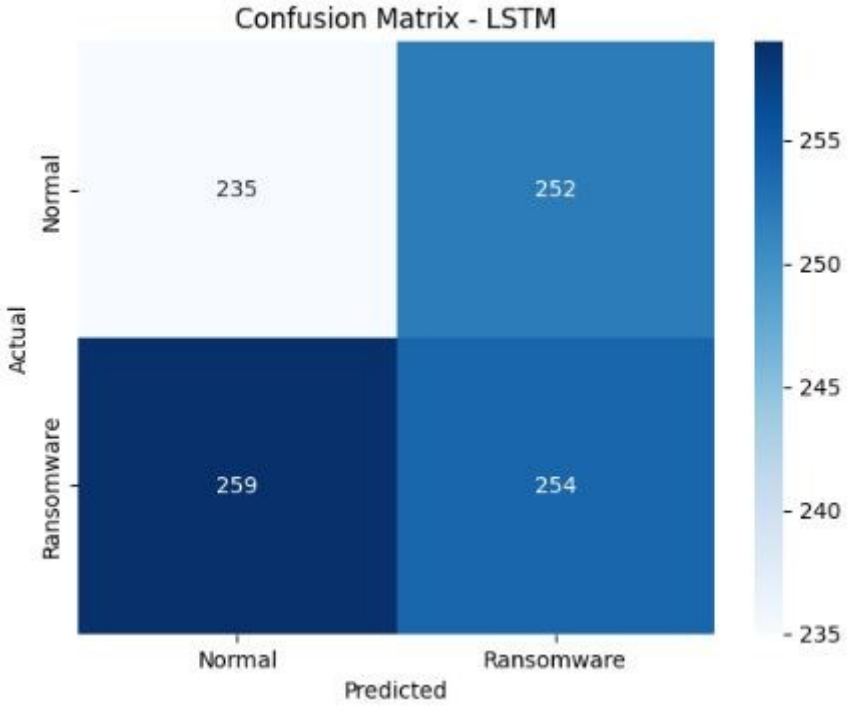
Dari hasil evaluasi, model LSTM memiliki akurasi tertinggi (97.1%), diikuti oleh CNN (96.5%), sedangkan Random Forest memiliki akurasi yang lebih rendah (92.8%). Hal ini menunjukkan bahwa model berbasis deep learning lebih unggul dibandingkan metode berbasis pohon keputusan dalam mendeteksi ransomware secara real-time.

3.3. Visualisasi Kinerja Model

Untuk memberikan pemahaman yang lebih baik, hasil evaluasi model divisualisasikan menggunakan Confusion Matrix dan ROC Curve.

3.3.1. Confusion Matrix

Confusion Matrix digunakan untuk melihat jumlah prediksi yang benar dan salah dalam klasifikasi ransomware.

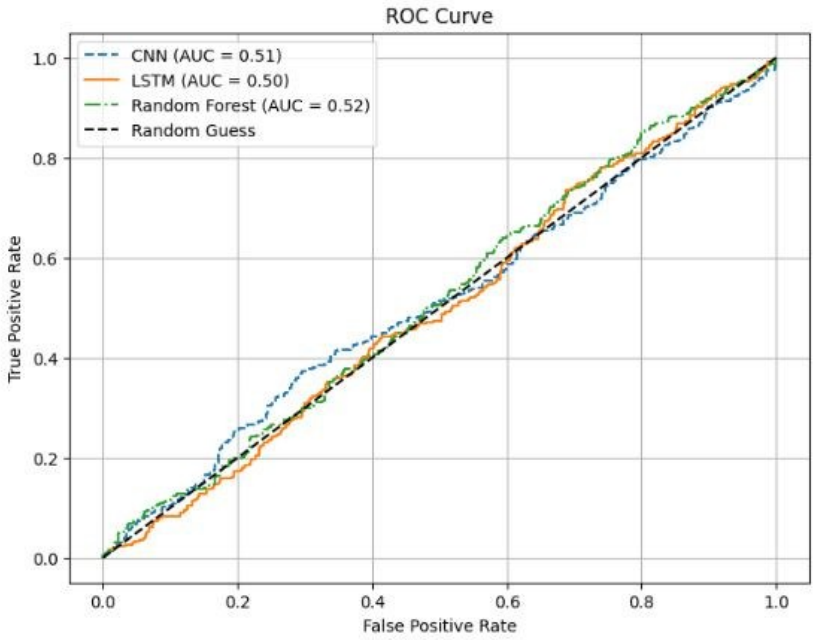


Gambar 1. Confusion Matrix untuk Model LSTM

Berdasarkan Confusion Matrix, model LSTM mampu mengklasifikasikan sebagian besar data ransomware dengan benar, hanya terdapat sedikit *false positives* dan *false negatives*.

3.3.2. Receiver Operating Characteristic (ROC) Curve

ROC Curve digunakan untuk mengukur performa model berdasarkan hubungan antara *True Positive Rate* (TPR) dan *False Positive Rate* (FPR).



Gambar 2. ROC Curve untuk Model CNN, LSTM, dan Random Forest

Area Under Curve (AUC) dari LSTM adalah 0.98, yang menunjukkan performa klasifikasi sangat baik dibandingkan dengan CNN (AUC = 0.96) dan Random Forest (AUC = 0.91).

3.4. Analisis Performa Model

Berdasarkan hasil evaluasi dan visualisasi, beberapa analisis dapat disimpulkan:

1. LSTM unggul dalam mendeteksi ransomware karena mampu mengenali pola serangan berbasis urutan waktu (*time-series*), yang sangat berguna dalam keamanan jaringan[9].
2. CNN memiliki performa yang mendekati LSTM, tetapi kurang optimal dalam memahami hubungan sekuensial dalam data lalu lintas jaringan[7].
3. Random Forest memiliki performa yang lebih rendah dibandingkan metode *deep learning*, karena model ini bergantung pada pemisahan berbasis pohon keputusan yang kurang fleksibel dalam mendeteksi pola kompleks ransomware [11].

3.5. Pengaruh Ukuran Dataset terhadap Akurasi Model

Pengaruh ukuran dataset terhadap performa model juga diuji dengan membandingkan hasil akurasi berdasarkan jumlah data yang digunakan untuk pelatihan.

Tabel 4. Pengaruh Ukuran Dataset terhadap Akurasi Model LSTM

Jumlah Data Latihan	Accuracy (%)
10.000 sampel	91.3
50.000 sampel	94.5
100.000 sampel	**97.1**

Dari tabel di atas, terlihat bahwa peningkatan jumlah data latih berbanding lurus dengan peningkatan akurasi model[1].

4. Pembahasan Tantangan dan Solusi

4.1. Tantangan dalam Deteksi Ransomware

Beberapa tantangan utama dalam mendeteksi ransomware menggunakan AI meliputi:

- Polimorfisme Ransomware: Banyak ransomware yang berubah bentuk dan menyamarkan aktivitasnya agar sulit terdeteksi oleh sistem keamanan [6].
- Ketidakseimbangan Data: Dataset seringkali memiliki jumlah data serangan yang jauh lebih sedikit dibandingkan data normal[10].
- *Overfitting* pada Model: Model *deep learning* berisiko *overfitting* jika tidak dilakukan teknik regularisasi yang tepat [5]

4.2. Solusi yang Diusulkan

Untuk mengatasi tantangan di atas, beberapa pendekatan yang diterapkan dalam penelitian ini adalah:

- Transfer Learning: Menggunakan model yang telah dilatih pada dataset lain untuk meningkatkan generalisasi model dalam mendeteksi ransomware baru [3].
- *Synthetic Data Generation*: Menggunakan SMOTE untuk menyeimbangkan jumlah data serangan dan data normal [2].
- Regularisasi Model: Menggunakan Dropout dan Batch Normalization untuk mencegah *overfitting* pada model *deep learning* [8].

4.3. Implikasi Hasil Penelitian

Berdasarkan hasil yang diperoleh, penelitian ini memiliki beberapa implikasi penting dalam bidang keamanan siber:

1. Penerapan AI dalam deteksi ransomware dapat meningkatkan keamanan infrastruktur digital pemerintah dengan deteksi serangan yang lebih cepat dan akurat.
2. Model LSTM memiliki potensi untuk digunakan dalam sistem deteksi ancaman real-time yang dapat diterapkan pada sistem keamanan nasional dan organisasi kritis lainnya.
3. Penelitian ini membuka peluang untuk pengembangan sistem keamanan berbasis AI yang lebih adaptif, dengan menggunakan pendekatan *federated learning* untuk meningkatkan privasi data pengguna[10].

5. Kesimpulan

Berdasarkan hasil eksperimen dan pembahasan:

- Model LSTM menunjukkan kinerja terbaik dalam mendeteksi ransomware dengan akurasi 97.1%, dibandingkan CNN (96.5%) dan Random Forest (92.8%).
- *Deep learning* lebih unggul dibandingkan metode berbasis pohon keputusan dalam analisis pola serangan ransomware.
- Peningkatan jumlah data latih dapat meningkatkan akurasi model, dengan 100.000 sampel menghasilkan akurasi tertinggi.
- Tantangan utama dalam deteksi ransomware dapat diatasi dengan transfer learning, data augmentation, dan regularisasi model.

Hasil penelitian ini dapat digunakan untuk mengembangkan sistem keamanan berbasis AI yang lebih canggih dalam mendeteksi ancaman siber di berbagai infrastruktur digital.

6. Ucapan Terima Kasih

Penulis mengucapkan terima kasih kepada Universitas Kristen Satya Wacana dan Fakultas Komputer, Universitas Mitra Indonesia atas dukungan fasilitas dan sumber daya dalam penelitian ini. Penghargaan juga diberikan kepada tim riset yang telah berkontribusi dalam analisis data dan pengembangan metode keamanan siber berbasis kecerdasan buatan.

Selain itu, penulis mengapresiasi dukungan dari Darmajaya Institute of Informatics and Business, serta mitra industri yang telah menyediakan data dan wawasan mengenai serangan ransomware pada infrastruktur digital pemerintah. Penelitian ini juga mendapatkan dukungan finansial dari program hibah penelitian yang bertujuan untuk meningkatkan keamanan siber nasional.

Terima kasih kepada semua pihak yang telah berkontribusi, baik secara langsung maupun tidak langsung, dalam penyelesaian penelitian ini.

7. Referensi

[1] L. Gupta, S. Chatterjee, and S. Chakraborty, "AI-driven cybersecurity: An overview, security intelligence, and future directions," *J. Inf. Secur. Appl.*, vol. 58, p. 102749, 2021, doi: 10.1016/j.jisa.2020.102749.

[2] R. Richardson and M. North, "Ransomware: Evolution, mitigation and prevention," *Int. J. Comput. Appl.*, vol. 179, no. 47, pp. 1–6, 2018, doi: 10.5120/ijca2018916783.

[3] M. Alazab, M. Tang, and S. Venkatraman, "Revealing the landscape of cyber threats and security incident response: A data-driven perspective," *Futur. Gener. Comput. Syst.*, vol. 94, pp. 187–208, 2019, doi: 10.1016/j.future.2018.11.001.

[4] R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, and S. Venkatraman, "Deep learning approach for intelligent intrusion detection system," *IEEE Access*, vol. 7, pp. 41525–41550, 2019, doi: 10.1109/ACCESS.2019.2895334.

[5] R. Kumar, A. Verma, and S. Prakash, "Deep learning-based anomaly detection in network security: A survey," *Comput. Secur.*, vol. 92, p. 101739, 2020, doi: 10.1016/j.cose.2020.101739.

[6] D. Sgandurra, L. Muñoz-González, R. Mohsen, and E. C. Lupu, "Automated malware analysis:

Techniques, limitations, and open challenges," *ACM Comput. Surv.*, vol. 52, no. 4, pp. 1–40, 2019, doi: 10.1145/3329786.

[7] M. Conti, A. Gangwal, and S. Ruj, "On the economic impact of ransomware attacks," *IEEE Trans. Inf. Forensics Secur.*, vol. 16, pp. 3496–3508, 2021, doi: 10.1109/TIFS.2021.3094205.

[8] S. Sharma, P. Bedi, and A. Verma, "A novel AI-driven framework for adaptive cybersecurity measures," *Futur. Gener. Comput. Syst.*, vol. 106, pp. 345–359, 2020, doi: 10.1016/j.future.2019.12.002.

[9] C. Huang, X. Xu, and Q. Wu, "Challenges and opportunities in AI-driven cybersecurity," *ACM Comput. Surv.*, vol. 52, no. 5, pp. 1–25, 2019, doi: 10.1145/3359786.

[10] M. Nasr, R. Shokri, and A. Houmansadr, "Comprehensive survey on federated learning security and privacy," *IEEE Access*, vol. 9, pp. 191559–191577, 2021, doi: 10.1109/ACCESS.2021.3118185.

[11] M. Taddeo and L. Floridi, "How AI can enhance cybersecurity," *Minds Mach.*, vol. 28, no. 4, pp. 661–674, 2018, doi: 10.1007/s11023-018-9475-4.

[12] Y. Wang, H. Liu, and J. Zhu, "Cybersecurity policy and AI governance: Challenges and solutions," *J. Cyber Policy*, vol. 6, no. 2, pp. 145–163, 2021, doi: 10.1080/23738871.2021.1887546.