OPTIMALISASI KEAMANAN DATA INFORMASI JARINGAN MELALUI ENKRIPSI DAN DETEKSI ANOMALI

Tubagus Toifur [1], Ibnu Mas'ud [2], Reynaldi Indrawijaya [3], Lulu Ilmahpudoh [4], Najwan Muhammad Farhat [5], Muhammad Afnan Feiza [6]
[1,2] Teknologi Informasi, Institut Teknologi Tangerang Selatan Komplek Komersial BSD, Jl.Raya Serpong NO. Kav.9, Lengkong Karya, Serpong Utara, South Tangerang City, Banten
[3,4,5,6] Informatika, Universitas Islam Negeri Sultan Maulana Hasanuddin Banten
Jl. Raya Syeikh Nawawi Bantani No . 30 Curug Kota Serang, Banten
tubagus@itts.ac.id

ABSTRAK

Keamanan data pada sistem informasi berbasis jaringan menjadi aspek yang sangat penting seiring meningkatnya pertukaran data secara digital di berbagai sektor. Ancaman seperti kebocoran data, akses tidak sah, dan serangan siber menuntut adanya mekanisme pengamanan yang efektif dan berkelanjutan. Permasalahan utama yang dihadapi adalah keterbatasan sistem keamanan konvensional dalam melindungi data sekaligus mendeteksi aktivitas mencurigakan, khususnya pada lalu lintas jaringan yang telah terenkripsi. Penelitian ini bertujuan untuk mengkaji penguatan keamanan data pada sistem informasi berbasis jaringan melalui penerapan enkripsi dan deteksi anomali. Metode penelitian yang digunakan adalah studi literatur dengan menganalisis jurnal ilmiah, buku referensi, dan publikasi terkait keamanan data, enkripsi, serta deteksi anomali jaringan. Hasil kajian menunjukkan bahwa enkripsi berperan penting dalam menjaga kerahasiaan dan integritas data, sedangkan deteksi anomali efektif dalam mengidentifikasi aktivitas yang menyimpang tanpa harus melakukan dekripsi data. Kombinasi kedua pendekatan tersebut dinilai mampu meningkatkan keamanan data secara signifikan dan relevan untuk diterapkan pada sistem informasi berbasis jaringan yang mengelola data sensitif.

Kata kunci : *keamanan data, sistem informasi, enkripsi, deteksi anomali, jaringan komputer*

1. PENDAHULUAN

Perkembangan sistem informasi berbasis jaringan telah mendorong peningkatan pertukaran data secara digital dalam berbagai sektor, seperti pemerintahan, pendidikan, bisnis, dan layanan publik. Kondisi ini memberikan manfaat signifikan dalam meningkatkan efisiensi dan kecepatan pengelolaan informasi, namun di sisi lain juga meningkatkan risiko terhadap keamanan data. Ancaman keamanan seperti kebocoran data, penyadapan lalu lintas jaringan, akses tidak sah, serta serangan siber semakin kompleks dan sulit diidentifikasi, terutama pada lingkungan jaringan yang bersifat terbuka dan terdistribusi [1], [14]. Keamanan data menjadi elemen penting dalam menjaga kerahasiaan, integritas, dan ketersediaan informasi, mengingat lemahnya mekanisme perlindungan data dapat berdampak pada kerugian finansial dan menurunnya kepercayaan pengguna terhadap sistem informasi [2], [9]. Selain itu, faktor manusia dan tingkat kesadaran keamanan pengguna turut memengaruhi kerentanan sistem terhadap serangan siber [4], [10], [16]. Salah satu pendekatan utama dalam pengamanan data adalah penerapan teknik enkripsi yang berfungsi melindungi data dari akses tidak sah, baik saat penyimpanan maupun transmisi melalui jaringan [6]. Meskipun enkripsi terbukti efektif dalam menjaga kerahasiaan data, penggunaan enkripsi secara luas menimbulkan tantangan baru dalam pemantauan keamanan jaringan karena lalu lintas data yang terenkripsi sulit dianalisis secara langsung [6], [14]. Kondisi ini berpotensi menyebabkan aktivitas berbahaya tersembunyi di dalam aliran data yang tampak normal. Oleh karena itu, diperlukan pendekatan tambahan yang mampu mendeteksi aktivitas mencurigakan tanpa harus mengorbankan aspek privasi dan keamanan data. Untuk mengatasi keterbatasan tersebut, pendekatan deteksi anomali menjadi solusi yang semakin banyak dikembangkan dalam bidang keamanan jaringan. Deteksi anomali bertujuan untuk mengidentifikasi pola aktivitas yang menyimpang dari perilaku normal sistem, yang berpotensi mengindikasikan adanya serangan atau aktivitas mencurigakan [11], [17]. Berbagai metode deteksi anomali telah diterapkan, mulai dari teknik statistik hingga pendekatan machine learning dan deep learning [7], [8], [10]. Penelitian terkini menunjukkan bahwa teknik pembelajaran mesin seperti Isolation Forest, Support Vector Machine, Convolutional Neural Network, autoencoder, serta model berbasis deep learning mampu meningkatkan akurasi deteksi anomali pada lalu lintas jaringan, termasuk pada data yang telah terenkripsi [3], [5], [13], [15]. Pendekatan ini memungkinkan sistem untuk mendeteksi ancaman tanpa harus melakukan dekripsi data secara langsung, sehingga tetap menjaga aspek privasi dan keamanan informasi [6], [8], [18]. Selain itu, kombinasi antara enkripsi dan deteksi anomali dinilai sebagai pendekatan yang saling melengkapi dalam memperkuat keamanan data. Enkripsi berperan dalam melindungi isi data, sementara deteksi anomali berfungsi sebagai mekanisme pengawasan terhadap aktivitas jaringan secara menyeluruh [1], [11], [19]. Integrasi kedua pendekatan ini menjadi semakin

relevan seiring dengan meningkatnya kompleksitas serangan siber dan penggunaan teknologi jaringan modern [12], [20]. Berdasarkan latar belakang tersebut, penelitian ini berfokus pada kajian penguatan keamanan data pada sistem informasi berbasis jaringan melalui pendekatan enkripsi dan deteksi anomali. Dengan menggunakan metode studi literatur terhadap berbagai jurnal ilmiah dan publikasi terkait, diharapkan penelitian ini dapat memberikan pemahaman komprehensif mengenai peran, manfaat, serta relevansi penerapan enkripsi dan deteksi anomali dalam meningkatkan keamanan data jaringan secara berkelanjutan.

2. TINJAUAN PUSTAKA

2.1. Keamanan Data pada Sistem Informasi Berbasis Jaringan

Keamanan data merupakan aspek fundamental dalam sistem informasi berbasis jaringan yang bertujuan untuk melindungi data dari ancaman kebocoran, penyalahgunaan, dan akses tidak sah. Keamanan data umumnya mencakup tiga prinsip utama, yaitu kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan (availability). Dalam lingkungan jaringan modern, meningkatnya volume dan kompleksitas lalu lintas data menjadikan sistem semakin rentan terhadap berbagai jenis serangan siber [11], [12]. Oleh karena itu, diperlukan mekanisme keamanan yang mampu melindungi data sekaligus memantau aktivitas jaringan secara berkelanjutan.

2.2. Enkripsi sebagai Mekanisme Keamanan Data

Enkripsi merupakan teknik pengamanan data dengan cara mengubah informasi asli menjadi bentuk yang tidak dapat dipahami oleh pihak yang tidak berwenang. Enkripsi banyak diterapkan untuk melindungi data baik pada proses penyimpanan maupun saat transmisi melalui jaringan. Penerapan enkripsi yang kuat terbukti efektif dalam mencegah serangan seperti penyadapan dan man-in-the-middle [6], [9]. Namun, penggunaan enkripsi secara luas juga menimbulkan tantangan baru dalam pengawasan keamanan jaringan karena lalu lintas data yang terenkripsi sulit dianalisis secara langsung oleh sistem keamanan konvensional [1], [18]. Kondisi ini mendorong perlunya pendekatan keamanan tambahan yang tidak bergantung pada isi data.

2.3. Deteksi Anomali pada Keamanan Jaringan

Deteksi anomali merupakan pendekatan yang digunakan untuk mengidentifikasi aktivitas yang menyimpang dari pola normal dalam sistem jaringan. Aktivitas serangan siber umumnya menghasilkan pola lalu lintas yang berbeda dibandingkan dengan aktivitas normal, sehingga dapat dikenali melalui analisis perilaku jaringan [3], [11]. Berbagai metode deteksi anomali telah dikembangkan, mulai dari pendekatan statistik hingga metode berbasis machine learning dan deep learning. Algoritma seperti Isolation Forest, Support Vector Machine, dan Random Forest banyak digunakan karena mampu mendeteksi anomali secara efektif pada data berskala besar [3], [15]. Selain itu, pendekatan deep learning seperti Convolutional Neural Network dan autoencoder dinilai lebih adaptif dalam mempelajari pola kompleks pada lalu lintas jaringan [5], [10], [17].

2.4. Deteksi Anomali pada Lalu Lintas Jaringan Terenkripsi

Seiring meningkatnya penggunaan enkripsi, penelitian terkait deteksi anomali pada lalu lintas jaringan terenkripsi semakin berkembang. Beberapa studi menunjukkan bahwa meskipun data terenkripsi, aktivitas mencurigakan tetap dapat dideteksi dengan memanfaatkan fitur statistik dan metadata jaringan, seperti ukuran paket, waktu transmisi, dan pola aliran data [1], [7], [8]. Pendekatan ini memungkinkan sistem keamanan untuk mendeteksi ancaman tanpa harus melakukan dekripsi data, sehingga privasi dan kerahasiaan informasi tetap terjaga [16], [18].

2.5. Integrasi Enkripsi dan Deteksi Anomali

Integrasi antara enkripsi dan deteksi anomali dinilai sebagai pendekatan yang saling melengkapi dalam meningkatkan keamanan data jaringan. Enkripsi berfungsi melindungi isi data, sedangkan deteksi anomali berperan sebagai mekanisme pemantauan aktif terhadap aktivitas jaringan [11], [19]. Beberapa penelitian menunjukkan bahwa kombinasi kedua pendekatan ini mampu meningkatkan efektivitas sistem keamanan dalam menghadapi serangan siber yang semakin kompleks [2], [12], [20]. Dengan demikian, integrasi enkripsi dan deteksi anomali menjadi dasar penting dalam pengembangan sistem keamanan data pada sistem informasi berbasis jaringan.

3. METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan metode studi literatur (literature review) untuk mengkaji penguatan keamanan data pada sistem informasi berbasis jaringan melalui pendekatan enkripsi dan deteksi anomali. Metode ini dipilih karena mampu memberikan pemahaman komprehensif mengenai konsep, teknik, serta perkembangan terkini yang berkaitan dengan keamanan data jaringan berdasarkan hasil penelitian terdahulu yang relevan.

3.1. Sumber Data Penelitian

Sumber data dalam penelitian ini berasal dari data sekunder yang diperoleh melalui jurnal ilmiah nasional dan internasional, prosiding, buku referensi, serta publikasi akademik yang relevan dengan topik keamanan data, enkripsi, dan deteksi anomali. Literatur yang digunakan dipilih berdasarkan kriteria kesesuaian topik, reputasi penerbit, serta keterkinian publikasi, dengan rentang tahun terbit yang disesuaikan untuk mencerminkan perkembangan terbaru di bidang keamanan jaringan.

3.2. Teknik Pengumpulan Data

Teknik pengumpulan data dilakukan melalui penelusuran literatur pada basis data jurnal ilmiah dan repositori publikasi akademik. Proses ini meliputi pencarian, pengumpulan, dan seleksi dokumen berdasarkan kata kunci yang relevan seperti keamanan data, enkripsi, deteksi anomali, dan sistem informasi berbasis jaringan. Setiap literatur yang terpilih kemudian dikaji secara mendalam untuk mengidentifikasi konsep, metode, serta hasil penelitian yang berkaitan dengan topik penelitian.

3.3. Teknik Analisis Data

Analisis data dilakukan dengan cara mengelompokkan literatur berdasarkan fokus pembahasan, yaitu konsep enkripsi, teknik deteksi anomali, serta integrasi kedua pendekatan dalam sistem keamanan jaringan. Selanjutnya, dilakukan analisis komparatif untuk membandingkan kelebihan, keterbatasan, dan relevansi masing-masing pendekatan berdasarkan temuan penelitian terdahulu. Hasil analisis kemudian disintesis untuk memperoleh gambaran menyeluruh mengenai efektivitas penerapan enkripsi dan deteksi anomali dalam meningkatkan keamanan data.

3.4. Tahapan Penelitian

Tahapan penelitian dimulai dengan identifikasi permasalahan dan perumusan tujuan penelitian berdasarkan fenomena meningkatnya ancaman keamanan data pada sistem informasi berbasis jaringan. Tahap selanjutnya adalah pengumpulan literatur yang relevan, diikuti dengan proses seleksi dan evaluasi kualitas sumber pustaka. Setelah itu, dilakukan analisis dan sintesis informasi dari literatur terpilih untuk menarik kesimpulan yang sesuai dengan tujuan penelitian.

4. HASIL DAN PEMBAHASAN

Berdasarkan hasil kajian literatur terhadap berbagai sumber ilmiah yang relevan, diperoleh gambaran bahwa penguatan keamanan data pada sistem informasi berbasis jaringan memerlukan pendekatan yang komprehensif dan berlapis. Ancaman keamanan yang semakin kompleks, terutama pada lalu lintas jaringan modern yang sebagian besar telah menggunakan enkripsi, menuntut adanya mekanisme perlindungan yang tidak hanya berfokus pada kerahasiaan data, tetapi juga pada kemampuan sistem dalam mendeteksi aktivitas yang tidak normal secara dini [1], [14].

Hasil kajian menunjukkan bahwa enkripsi masih menjadi fondasi utama dalam menjaga keamanan data jaringan. Penerapan algoritma enkripsi yang kuat mampu melindungi data dari penyadapan dan akses tidak sah, baik pada fase penyimpanan maupun transmisi data [6].

Beberapa penelitian menegaskan bahwa tanpa enkripsi yang memadai, data sangat rentan terhadap serangan seperti man-in-the-middle dan packet sniffing, yang dapat menyebabkan kebocoran informasi sensitif [2], [9]. Dengan demikian, enkripsi berperan penting dalam menjamin aspek kerahasiaan dan integritas data dalam sistem informasi berbasis jaringan.

Namun, hasil kajian juga mengungkapkan bahwa penggunaan enkripsi secara luas menghadirkan tantangan baru dalam pengawasan keamanan jaringan. Lalu lintas jaringan yang terenkripsi menyulitkan sistem keamanan konvensional dalam melakukan inspeksi konten secara langsung, sehingga berpotensi menyembunyikan aktivitas berbahaya di dalam aliran data yang tampak normal [1], [6]. Kondisi ini mendorong berkembangnya pendekatan deteksi anomali yang tidak bergantung pada isi data, melainkan pada pola dan karakteristik lalu lintas jaringan.

Deteksi anomali terbukti efektif dalam mengidentifikasi perilaku menyimpang pada sistem informasi berbasis jaringan. Berbagai penelitian menunjukkan bahwa aktivitas serangan siber cenderung menghasilkan pola lalu lintas yang berbeda dari aktivitas normal, baik dari sisi frekuensi, durasi, maupun karakteristik aliran data [11], [17]. Dengan memanfaatkan pendekatan deteksi anomali, sistem keamanan dapat mengenali indikasi awal serangan tanpa harus melakukan dekripsi data, sehingga tetap menjaga privasi dan keamanan informasi.

Perkembangan metode machine learning dan deep learning memberikan kontribusi signifikan terhadap peningkatan akurasi deteksi anomali. Beberapa studi menunjukkan bahwa algoritma seperti Isolation Forest, Support Vector Machine, dan Random Forest mampu mendeteksi anomali jaringan dengan tingkat akurasi yang tinggi, terutama pada data berskala besar [3], [15]. Selain itu, pendekatan berbasis deep learning seperti Convolutional Neural Network dan autoencoder dinilai lebih adaptif dalam mempelajari pola kompleks pada lalu lintas jaringan yang dinamis [5], [10], [18].

Hasil kajian terhadap penelitian yang berfokus pada lalu lintas jaringan terenkripsi menunjukkan bahwa deteksi anomali tetap dapat dilakukan secara efektif dengan memanfaatkan fitur statistik dan metadata jaringan. Penelitian oleh Rahman et al. dan beberapa studi lain menegaskan bahwa analisis karakteristik aliran data, seperti ukuran paket, waktu transmisi, dan arah komunikasi, dapat digunakan untuk membedakan aktivitas normal dan aktivitas mencurigakan meskipun data berada dalam kondisi terenkripsi [1], [7], [8]. Hal ini menunjukkan bahwa enkripsi tidak menjadi penghalang mutlak dalam upaya deteksi ancaman keamanan jaringan.

Selain aspek teknis, hasil kajian juga menyoroti pentingnya faktor kontekstual dalam penerapan keamanan data. Lingkungan sistem, jenis data yang dikelola, serta tingkat sensitivitas informasi memengaruhi efektivitas penerapan enkripsi dan deteksi anomali [4], [10]. Sistem yang mengelola data sensitif, seperti data pribadi dan data transaksi,

membutuhkan tingkat perlindungan yang lebih ketat dibandingkan sistem dengan risiko lebih rendah [9], [13]. Oleh karena itu, pendekatan keamanan data perlu disesuaikan dengan kebutuhan dan karakteristik masing-masing sistem.

Integrasi antara enkripsi dan deteksi anomali dinilai sebagai pendekatan yang saling melengkapi dalam memperkuat keamanan data jaringan. Enkripsi berfungsi sebagai mekanisme perlindungan pasif yang menjaga kerahasiaan data, sedangkan deteksi anomali berperan sebagai mekanisme aktif yang memantau dan mengidentifikasi potensi ancaman secara berkelanjutan [11], [19]. Kombinasi kedua pendekatan ini memungkinkan sistem keamanan untuk tidak hanya mencegah akses tidak sah, tetapi juga merespons secara cepat terhadap aktivitas mencurigakan yang muncul dalam jaringan.

Beberapa penelitian juga menekankan bahwa penerapan deteksi anomali berbasis pembelajaran mesin harus memperhatikan keseimbangan antara tingkat akurasi dan kompleksitas sistem. Model yang terlalu kompleks berpotensi meningkatkan beban komputasi, sedangkan model yang terlalu sederhana dapat menghasilkan tingkat kesalahan deteksi yang tinggi [7], [12]. Oleh karena itu, pemilihan metode deteksi anomali perlu mempertimbangkan efisiensi, skalabilitas, dan kemudahan integrasi dengan sistem keamanan yang sudah ada.

Hasil kajian literatur juga menunjukkan bahwa penerapan keamanan data tidak dapat dilepaskan dari kebijakan dan kesadaran keamanan organisasi. Tanpa dukungan kebijakan keamanan yang jelas dan pemahaman pengguna terhadap risiko keamanan, efektivitas penerapan enkripsi dan deteksi anomali dapat menurun [4], [10], [16]. Dengan demikian, penguatan keamanan data perlu dilakukan secara holistik, mencakup aspek teknis, organisatoris, dan manusia.

Secara keseluruhan, hasil dan pembahasan ini menunjukkan bahwa penguatan keamanan data pada sistem informasi berbasis jaringan melalui pendekatan enkripsi dan deteksi anomali merupakan strategi yang relevan dan efektif dalam menghadapi ancaman siber modern. Kajian terhadap berbagai penelitian terdahulu memperlihatkan bahwa kombinasi kedua pendekatan tersebut mampu meningkatkan perlindungan data secara signifikan, khususnya pada lingkungan jaringan yang kompleks dan mengelola data bersifat sensitif [1], [6], [18], [20]. Dengan demikian, pendekatan ini layak dijadikan dasar dalam pengembangan dan evaluasi sistem keamanan data jaringan yang berkelanjutan.

5. KESIMPULAN

Secara keseluruhan, dapat disimpulkan bahwa penguatan keamanan data pada sistem informasi berbasis jaringan melalui pendekatan enkripsi dan deteksi anomali merupakan strategi yang relevan, efektif, dan adaptif dalam menghadapi tantangan keamanan siber modern. Melalui metode studi literatur, penelitian ini memberikan gambaran komprehensif mengenai peran dan manfaat kedua pendekatan tersebut sebagai dasar dalam pengembangan sistem keamanan data yang lebih andal dan berkelanjutan. Hasil kajian ini diharapkan dapat menjadi referensi bagi peneliti, praktisi, maupun pengelola sistem informasi dalam merancang dan menerapkan mekanisme keamanan data yang sesuai dengan kebutuhan dan karakteristik lingkungan jaringan.

DAFTAR PUSTAKA

[1] Md M. Rahman, M. S. Soumik, M. S. Farids, C. A. Abdullah, B. Sutrudhar, M. Ali, & M. Hossain, “Explainable Anomaly Detection in Encrypted Network Traffic Using Data Analytics,” Journal of Computer Science and Technology Studies, vol. 6, no. 1, pp. 272–281, 2024.

[2] Niwat Angkawisittpan, et al., “Network Encryption Traffic Anomaly Detection Based on Integrated Machine Learning,” Hrcak, pp. 713–722, 2025.

[3] I. Tammamah Lubis, R. Roslina & L. Tanti, “Anomaly Detection in Computer Networks Using Isolation Forest in Data Mining,” Jurnal Teknik Informatika, 18(1), 2025. DOI: https://doi.org/10.15408/jti.v18i1.44285.

[4] M. F. Azmi, H. Abdul Karim & N. AlDahoul, “Anomaly Detection for Network Security,” International Journal of Membrane Science and Technology, 10(1), 2025. DOI: https://doi.org/10.15379/ijmst.v10i1.1808.

[5] Arief L. Hadiyani & Bana Handaga, “Implementasi Sistem Deteksi Anomali Berbasis Jaringan Menggunakan CNN dan SVM,” Jurnal Informatika Universitas Pamulang, vol. 10, no. 2, 75–85, 2025.

[6] G. Long & Z. Zhang, “Deep Encrypted Traffic Anomaly Detection Based on Parallel Automatic Feature Extraction,” Comput. Intell. Neurosci., 2023.

[7] Kalindi Singh, Aayush Kashyap, A. K. Cherukuri, “Interpretable Anomaly Detection in Encrypted Traffic Using SHAP with Machine Learning Models,” arXiv preprint, 2025.

[8] Anca Hangan, Dragos Lazea & Tudor Cioara, “Privacy Preserving Anomaly Detection on Homomorphic Encrypted Data from IoT Sensors,” arXiv preprint, 2024.

[9] Omer Sen, Mehdi A. Gurabi, Milan Deruelle, A. Ulbig & S. Decker, “Encryption-Aware Anomaly Detection in Power Grid Communication Networks,” arXiv preprint, 2024.

[10] Willian T. Lunardi, M. A. Lopez & J.-P. Giacalone, “ARCADE: Adversarially Regularized Convolutional Autoencoder for Network Anomaly Detection,” arXiv preprint, 2022.

[11] Rustamov R. B., J. Guliyev & K. Hasanova, "Network Anomaly Detection and Intrusion Detection Systems: Introduction, Review and Analyses," Aeron Aero Open Access J., vol. 9, no. 2, pp. 118–121, 2025.
[12] Weibao Zhang & J. P. Lazaro, "A Survey on Network Security Traffic Analysis and Anomaly Detection Techniques," Int. J. Emerging Tech. Adv. Appl., 2025. DOI: https://doi.org/10.62677/IJETAA.2404117.
[13] Rafly Yusuf & Sumarlin, "Penerapan Deep Learning untuk Deteksi Anomali dalam Jaringan Keamanan Siber," Blend Sains J. Teknik, vol. 3, no. 4, 2025.
[14] Delvita A. Artika, D. Rumahorbo, M. H. Al-Majid & D. Kiswanto, "Implementasi Sistem Keamanan Website dengan Analisis Log dan Deteksi Anomali menggunakan Isolation Forest," Jurnal Informatika dan Teknik Elektro, 13(3S1), 2025.
[15] Mujiono, A. L. Devita, M. Hermansyah & F. Fatimatuzzahra, "Deteksi Anomali dalam Sistem Keamanan Jaringan dengan Supervised ML," Jurnal Esensi Infokom, vol. 9, no. 1, 2025.
[16] I. S. Sattar, S. Khan, M. Ismail Khan, A. Akhmediyarova, O. Mamyrbayev, D. Kassymova, & D. Oralbekova, "Anomaly Detection in Encrypted Network Traffic Using Self-Supervised Learning," Scientific Reports, vol. 15, 26585, 2025.
[17] MI Kim, "Anomaly Detection in Imbalanced Encrypted Traffic with Autoencoder and Flow-based Features," CMES, 2024.
[18] M. B. Farbman, "Encrypted AI Techniques for Anomaly Detection," International Journal of Research and Review Techniques, vol. 3, no. 1, pp. 76–81, 2024.
[19] Sileshi N. Zeleke, Amsalu F. Jember & Mario Bochicchio, "Integrating Explainable AI for Effective Malware Detection in Encrypted Network Traffic," arXiv preprint, 2025.
[20] Chuanpu Fu, Qi Li & Ke Xu, "Detecting Unknown Encrypted Malicious Traffic in Real Time via Flow Interaction Graph Analysis," arXiv preprint, 2023