IMPLEMENTASI *INTRUSION DETECTION SYSTEM* (*IDS*) UNTUK *MONITORING* KEAMANAN WEB SERVER

PROJEK

Sebagai Salah Satu Syarat untuk Menyelesaikan Studi di

Program Studi Teknik Komputer DIII

Oleh :

RINDA AMBARWATI PUTRI

09030582226015

PROGRAM STUDI TEKNIK KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

AGUSTUS 2025

HALAMAN PENGESAHAN

PROJEK

IMPLEMENTASI *INTRUSION DETECTION SYSTEM (IDS)* UNTUK *MONITORING* KEAMANAN WEB SERVER

Sebagai salah satu syarat untuk penyelesaian studi di

Program Studi D3 Teknik Komputer

Oleh:

RINDA AMBARWATI PUTRI
09030582226015

Pembimbing 1	**:**	**Huda Ubaya, M.T.**
		NIP. 198106162012121003
Pembimbing 2	**:**	**Adi Hermansyah, M.T.**
		NIP. 198904302024211001

Mengetahui
Koordinator Program Studi Teknik Komputer

Dr. Ir. Ahmad Heryanto, M.T.
198701222015041002

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Senin

Tanggal : 28 Juli 2025

Tim Penguji :

1. **Ketua Sidang** : **Dr. Ir. Ahmad Heryanto, M.T.**
2. **Pembimbing I** : **Huda Ubaya, M.T**
3. **Pembimbing II** : **Adi Hermansyah, M.T.**
4. **Penguji** : **Muhammad Ali Buchari, M.T.**

Mengetahui

Koordinator Program Studi Teknik Komputer

Dr. Ir. Ahmad Heryanto, M.T.

NIP 198701222015041002

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini :

Nama	: Rinda Ambarwati Putri
NIM	: 09030582226015
Program Studi	: Teknik Komputer
Jenjang	: DIII
Judul Projek	: Implementasi *Intrusion Detection System (IDS)* untuk *Monitoring* Keamanan Web Server

Hasil Pengecekan Software iThenticate/Turnitin : 15%

Menyatakan bahwa Laporan Projek saya merupakan hasil karya sendiri dan bukan hasil penjiplakan/plagiat. Apabila ditemukan unsur penjiplakan/plagiat dalam laporan projek ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya sesuai dengan ketentuan yang berlaku.

Dengan pernyataan ini saya buat dengan sebenarnya dan tidak ada paksaan oleh siapapun.

Palembang, 04 Agustus 2025

Rinda Ambarwati Putri
NIM 09030582226015

MOTTO

MOTTO:

"Jatuh bukan masalah, gagal bukan aib. yang jadi masalahnya adalah saat aku berhenti berjuang untuk melangkah, dan itu tidak akan pernah kulakukan."

Kupersembahkan kepada:

- *Allah SWT*
- *Kedua Orang Tuaku Tersayang*
- *Dosen dan Pembimbing*
- *Teman-teman*
- *Almamaterku*

KATA PENGANTAR

Puji Syukur kehadirat Allah Subhanahu wa ta'ala, atas berkat dan Rahmat serta karunia-Nya, sehingga Laporan Proyek ini dapat terselesaikan dengan baik yang berjudul **"Implementasi *Intrusion Detection System* (*IDS*) untuk *Monitoring* Keamanan Web Server"**. Laporan ini disusun sebagai salah satu syarat untuk memenuhi mata kuliah pada Program Studi Teknik Komputer Universitas Sriwijaya.

Penyusunan laporan ini tidak terlepas dari dukungan dan bantuan yang diberikan oleh berbagai pihak. Adapun pihak yang mendukung keberhasilan dalam penyusunan laporan. Dalam hal ini, dengan penuh rasa hormat saya mengucapkan banyak terima kasih ter-khususnya kepada:

1. Saya mengucapkan terima kasih kepada Allah SWT atas berkat dan karunia-Nya, yang memungkinkan laporan proyek ini dapat diselesaikan.
2. Kepada kedua orang tua saya, untuk papa tercinta Turianto Wage dan mama tersayang Dwi Mikuwati yang selalu memberikan dukungan, doa, serta memberikan dan memenuhi kebutuhan apapun dalam pelaksanaan projek ini. Terima kasih atas semua doa untuk Rinda dalam menuntun setiap perjalanan yang akan ditempuh.
3. Kepada kakak pertamaku Masklara Belo Putro, dan kakak keduaku Mas Bayu Setio Putra yang memberikan doa, bantuan, dan dukungan untuk saya dalam melakukan penyelesaian laporan ini.
4. Bapak Dr. Ir. Ahmad Heryanto., M.T. Selaku Koordinator Program Studi Teknik Komputer Universitas Sriwijaya.
5. Bapak Huda Ubaya, M.T. selaku Dosen Pembimbing 1, atas kesediaan memberikan masukan dan arahan serta bimbingan yang sangat berguna bagi saya dalam penyelesaian laporan projek ini.
6. Bapak Adi Hermansyah, M.T. selaku Dosen Pembimbing 2, atas kesediaan memberikan masukan dan arahan yang berguna dalam penyempurnaan projek

dan bimbingan dalam penyelesaian laporan ini.

7. Bapak Dr. Ahmad Zarkasi, M.T. sebagai Dosen Pembimbing Akademik yang memberikan arahan pada selama masa studi.
8. Seluruh Dosen Program Studi Teknik Komputer Universitas Sriwijaya.
9. Seseorang yang senantiasa mendampingi saya pada masa pengerjaan proyek sampai selesainya laporan projek ini dengan selalu memberikan support dan selalu ada di saat suka dan duka. Beliau seseorang terpenting setelah keluarga saya yang sudah banyak sekali membantu dan memberikan dukungan serta doa dalam penyelesaian proyek ini yaitu M Saddam Hamidin.
10. Kakak-kakak yang telah banyak memberikan bantuan dalam proses pengerjaan proyek ini yaitu kakak Andrian, Arman, Bagas dan Dhani.
11. Teman-teman seperjuangan, atas dukungan yang diberikan.

Saya berharap Allah SWT selalu memberikan semua kemudahan serta kelancaran dalam penyelesaian proyek ini. Laporan Tugas Akhir ini saya tulis dengan sebaik mungkin. saya menyadari bahwa masih banyak terdapat kekurangan dan laporan ini masih jauh dari kesempurnaan. Oleh karena itu, saya sangat menghargai kritik dan saran yang konstruktif dalam penyempurnaan proyek ini. Penulis berharap agar Laporan Tugas Akhir ini dapat bermanfaat untuk semua pihak-pihak yang membutuhkan serta bagi penulis sendiri.

Palembang, 04 Agustus 2025

Penulis

Rinda Ambarwati Putri

NIM. 09030582226015

IMPLEMENTASI *INTRUSION DETECTION SYSTEM* (IDS) UNTUK *MONITORING* KEAMANAN WEB SERVER KOMPUTER

Oleh :

Rinda Ambarwati Putri (09030582226015)

Program Studi Teknik Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya

Email: rindaambarwati@gmail.com

Abstrak

Perkembangan teknologi, membawa dampak yang signifikan terhadap keamanan jaringan komputer, terutama pada *web server* yang rentan sekali terhadap berbagai ancaman *cyber*. Adapun serangan yang sering terjadi adalah serangan *Brute Force*, dan serangan *Denial of Service (DoS)* maka dari itu diperlukan sistem pengaman jaringan yang mampu untuk mendeteksi ancaman tersebut. Projek ini bertujuan untuk mengimplementasikan *Intrusion Detection System (IDS)* dengan menggunakan Snort pada web server berbasis Apache yang berjalan di atas perangkat Raspberry Pi 5 dengan sistem operasi Ubuntu. IDS berfungsi menjadi alat pemantauan keamanan yang dapat mengidentifikasi aktivitas yang mencurigakan serta memberikan peringatan awal terhadap kemungkinan serangan *Brute Force* dan serangan *Denial of Service (DoS*). Hasil pengujian menunjukkan bahwa IDS yang diimplementasikan untuk *monitoring* web server mampu mendeteksi serangan *Brute Force* dan *Denial of Service (DoS)* dengan tingkat akurasi yang tinggi. Dengan demikian, implementasi *Intrusion Detection System* (IDS) menjadi solusi yang efisien untuk meningkatkan keamanan web server dalam jaringan komputer.

Kata kunci: Keamanan Jaringan, *Intrusion Detection System*, Snort, Web Server, *Brute Force*, *Denial of Service*, Raspberry Pi 5

IMPLEMENTATION INTRUSION DETECTION SYSTEM (IDS) FOR MONITORING WEB SERVER SECURITY

By:

Rinda Ambarwati Putri (09030582226015)

Diploma Program in Computer Engineering, Faculty of Computer Science

Email: rindaambarwati@gmail.com

Abstract

The advancement of technology has a significant impact on computer network security, particularly on web servers that are highly vulnerable to various cyber threats. Common attacks Brute Force attacks and Denial of Service (DoS) attacks, therefore a network security system capable of detecting these threats is essential. This project aims to implement an Intrusion Detection System (IDS) using Snort on Apache based web server running on a Raspberry Pi 5 with the Ubuntu operating system. The IDS serves as a security monitoring tool that can identify suspicious activities and provide early warnings of potential Brute Force and Denial of Service attacks. Testing results indicate that the implemented IDS for monitoring the web server can detect Brute Force and Denial of Service attacks with a high level of accuracy. Thus, the implementation of the Intrusion Detection System (IDS) proves to be an efficient solution to enchancing the security of web servers within computer networks.

Keywords: Network Security, Intrusion Detection System, Snort, Web Server, Brute Force, Denial of Service, Raspberry Pi 5

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi yang pesat telah membawa dampak besar terhadap berbagai sektor, khususnya dalam pengelolaan data dan layanan digital melalui jaringan komputer. Seiring meningkatnya ketergantungan pada jaringan internet, muncul pula tantangan serius dalam menjaga keamanan sistem dari berbagai ancaman siber. Web server yang menjadi pusat layanan aplikasi dan informasi sangat rentan terhadap serangan. Pendekatan seperti penggunaan sistem autentikasi berbasis peran belum mampu memberikan perlindungan yang optimal terhadap berbagai jenis serangan tersebut[1].

Namun, dengan semakin kompleksnya arsitektur sistem dan meningkatnya jumlah titik serangan potensial, ancaman terhadap infrastruktur teknologi semakin sulit dideteksi secara konvensional. Sebagai respons terhadap tantangan terhadap serangan seperti *Brute Force,* dan *Denial of Service (DoS), Intrusion Detection System (IDS)* hadir sebagai solusi yang mampu memberikan deteksi dini terhadap aktivitas mencurigakan di dalam jaringan atau sistem. IDS dapat dimanfaatkan untuk memantau aliran data secara r*eal-time* dan mengidentifikasi anomali yang mengindikasikan adanya upaya intrusi atau serangan. Penggunaan IDS berbasis *machine learning* juga terbukti efektif dalam mendeteksi pola serangan yang tidak terdefinisi sebelumnya, dengan mempelajari perilaku normal sistem dan membandingkannya dengan data aktual. Dalam konteks keamanan web server, IDS menjadi elemen penting untuk mendeteksi atau perintah yang mengarah pada pengambilan alih kendali sistem, pencurian informasi, atau bahkan penghentian layanan. Dengan menanamkan IDS pada level yang strategis seperti server, jalur komunikasi, dan aplikasi web, maka proses identifikasi ancaman dapat dilakukan secara menyeluruh dan responsif. Oleh karena itu, implementasi IDS yang handal sangat dibutuhkan untuk meningkatkan ketahanan web server terhadap berbagai bentuk serangan siber yang semakin canggih dan terorganisir[2].

Menjawab kebutuhan tersebut, salah satu solusi IDS yang efektif dan efisien secara biaya adalah dengan menggunakan perangkat Raspberry Pi yang dikombinasikan dengan perangkat lunak Snort, sebuah IDS berbasis open-source. Sistem ini dirancang untuk mampu melakukan deteksi dengan pencegahan intrusi secara otomatis tanpa memerlukan investasi besar. Perangkat Raspberry Pi dan Snort dikonfigurasi untuk menjalankan sistem IDS/IPS dalam jaringan kecil menengah, terbukti mampu mendeteksi aktivitas berbahaya seperti pemindaian port dan penggunaan proxy VPN secara akurat dengan konsumsi daya rendah dan biaya implementasi yang minim. Selain itu, sistem ini dapat dimonitor secara jarah jauh oleh administrator, sehinga mendukung skenario seperti pengawasan keamanan web server pada pda lingkungan pendidikan dengan anggaran terbatas. Dengan fleksibilitas pemasangan dan kemudahan konfifurasi, solusi ini menjadi alternatif yang tepat dalam membangun sistem pemantaua keamanan jaringan yang andal, terjangkau dan mudah dikembangkan[3].

Dengan kemampuan mendeteksi lalu lintas mencurigakan dan konfigurasi fleksibel, Melalui penerapan pada teknologi keamanan jaringan pada sistem seperti *Intrusion Detection System* (*IDS)* dengan berbasis Raspberry Pi 5 dan Snort memiliki kemampuan memberikan suatu peringatan dalam aktivitas yang mencurigakan. Agar terciptanya suatu sistem keamanan jaringan yang mudah diterapkan untuk mendeteksi ancaman serangan *Brute Force dan DoS* pada web server. pendekatan ini memberikan alternatif solusi yang praktis, ringan, dan ekonomis, sekaligus meningkatkan kewaspadaan serta ketahanan sistem terhadap ancaman siber yang semakin kompleks. Berdasarkan latar belakang tersebut, penulis mengangkat topik ini sebagai fokus penelitian dalam proyek Tugas Akhir dengan judul **"Implementasi *Intrusion Detection System (IDS)* untuk *Monitoring* Keamanan Web Server".**

1.2 Rumusan Masalah

Berdasarkan penjelasan pada latar belakang, adapun Rumusan masalah dalam penyusunan proyek ini sebagai berikut:

1. Bagaimana cara pengimplementasian sistem *Intrusion Detection System (IDS)* berbasis Snort dengan menggunakan Raspberry Pi?

2. Seberapa efektif IDS dalam mendeteksi dan memberi peringatan dini terhadap serangan *brute force* dan serangan *Denial of Service (DoS)* pada *web server*?
3. Bagaimana tingkat akurasi dan kinerja IDS dalam memantau serta mengidentifikasi aktivitas mencurigakan yang mengancam keamanan web server?

1.3 Tujuan

Berdasarkan penjelasan yang terdapat dalam latar belakang dan rumusan masalah, tujuan dari penelitian dalam penyusunan laporan proyek akhir ini meliputi tiga tujuan yaitu:

1. Mengimplementasikan sistem *Intrusion Detection System (IDS)* pada *web server*.
2. Menguji efektivitas IDS dalam mendeteksi dan memberi peringatan dini terhadap serangan brute force dan *Denial of Service (DoS)* pada *web server.*
3. Menganalisis tingkat akurasi dan kinerja IDS dalam memantau keamanan pada *web server.*

1.4 Manfaat

Berdasarkan tujuan yang telah ditetapkan dalam penyusunan proyek ini, manfaat dari penelitian ini meliputi tiga manfaat sebagai berikut:

1. Mampu untuk mendeteksi dan memberikan peringatan dini terhadap aktivitas yang mencurigakan, yaitu seperti serangan *brute force* dan serangan *Denial of Service (DoS),* sehingga risiko pelanggaran keamanan dapat diminimalkan.
2. Melakukan *monitoring* aktivitas jaringan secara langsung, sehingga setiap percobaan akses ilegal dapat terdeteksi dengan cepat agar mencegah kerusakan lebih lanjut.
3. Memudahkan administrator dalam menganalisis pola serangan, serta merancang strategi pencegahan yang lebih efektif untuk menjaga keamanan sistem, melalui adanya *alert* dan hasil deteksi dari sistem IDS.

1.5 Batasan Masalah

Dalam penyusunan proyek ini, terdapat beberapa ruang lingkup atau batasan masalah yang ditetapkan, yaitu sebagai berikut:

1. Sistem *Intrusion Detection System (IDS)* yang diterapkan dalam penelitian ini dengan menggunakan Snort.
2. Fokus penelitian terbatas pada pendeteksian dua jenis serangan, yaitu serangan *brute force* yang dilakukan dengan menguji berbagai kombinasi *username* dan *password* untuk masuk ke sistem, serta serangan *Denial of Service (DoS)* bertujuan untuk membanjiri server meliputi lalu lintas berlebih hingga mengganggu layanan.
3. Web server yang digunakan dalam pengujian adalah Apache, yang dijalankan pada perangkat Raspberry Pi 5 dengan sistem operasi Ubuntu.
4. Evaluasi kinerja *monitoring* IDS dilakukan berdasarkan dua parameter, yaitu tingkat akurasi dalam membedakan aktivitas normal dan serangan, serta respons kecepatan IDS dalam memberikan peringatan dini terhadap serangan brute force dan serangan *Denial of Service (DoS)* yang terdeteksi.

1.6 Metode Penelitian

Dalam perancangan proyek ini, digunakan beberapa metode penelitian, diantaranya:

1. Metode Studi Literatur

   Metode ini dilakukan dengan mengumpulkan dan mencari berbagai informasi dari beragam referensi, seperti buku, artikel, jurnal, dan dokumen yang berkaitan dengan topik penelitian yaitu "Implementasi *Intrusion Detection System* (IDS) untuk *Monitoring* Keamanan Web Server". Tujuannya adalah untuk memperdalam terhadap konsep-konsep yang mendasari proyek ini.
2. Metode Observasi

   Dalam proyek ini, pada metode ini digunakan untuk pengamatan secara langsung dalam memahami penggunaan pada Raspberry Pi sebagai perangkat keras dalam menjalankan *Intrusion Detection System* (IDS) sebagai *monitoring* keamanan pada web server.
3. Metode Konsultasi

   Dalam proyek ini, pada bagian metode ini melakukan diskusi bersama dosen pembimbing melakukan tanya jawab untuk mendapatkan masukan, dan arahan selama proses penelitian dilakukan.

4. Metode Implementasi dan Pengujian Sistem

   a. Metode Implementasi

      Setelah perancangan sistem IDS dalam *monitoring* web server, diimplementasikan meliputi pada pemasangan, konfigurasi, dan integrasi Snort pada Raspberry Pi. IDS akan dihubungkan dengan web server untuk mendeteksi aktivitas yang mencurigakan dan untuk *monitoring* keamanan pada jaringan.

   b. Metode Pengujian

      Pengujian akan dilakukan sebagai evaluasi kemampuan pada sistem IDS untuk mendeteksi ancaman serangan. dalam pengujian ini bertujuan untuk menilai efektivitas pada sistem secara menyeluruh berdasarkan rancangan yang telah disusun.

1.7 Sistematika Penulisan

Struktur penulisan laporan ini terdiri dari lima bab utama, yang masing-masing berisi pembahasan sebagai berikut:

BAB I PENDAHULUAN

Bab ini menguraikan latar belakang penelitian, perumusan judul, tujuan dan manfaat proyek, batasan masalah, metode yang digunakan dalam penelitian, serta sistematika penulisan laporan secara keseluruhan.

BAB II TINJAUAN PUSTAKA

Pada bab ini dibahas teori-teori dasar dan referensi yang relevam dengan topik penelitian, mencangkup berbagai konsep yang mendukung serta keterkaitannya dengan implementasi proyek ini.

BAB III PERANCANGAN SISTEM

Pada bab ini dijelaskan langkah-langkah dalam merancang sistem proyek, yang mencakup spesifikasi perangkat keras dan perangkat lunak, proses konfigurasi Snort, serta penyusunan skenario Pengujian.

BAB IV HASIL DAN PEMBAHASAN

Bab ini menyajikan hasil implementasi dan pengujian sistem IDS, termasuk analisis parameter akurasi, kecepatan deteksi, dan efektivitas. Selain itu, dijelaskan pula kendala yang ditemui serta evaluasi performa sistem.

BAB V KESIMPULAN DAN SARAN

Bab terakhir ini berisi kesimpulan dari hasil seluruh hasil proyek yang telah dilaksanakan, serta memberikan rekomendasi untuk pengembangan sistem keamanan jaringan berbasis IDS di masa yang akan datang.

DAFTAR PUSTAKA

[1] Qaiwmchi, N. H. A., Amintoosi, H., and Mohajer, A., 2020. Intrusion Detection System Based on Gradient Corrected Online Sequential Extreme Learning Machine. *IEEE Access*, 6:1757-1769

[2] Rahman, M. A., Rahman, M. T., Kisacikoglu, M., and Akkaya, K., 2020. Intrusion Detection Systems-Enabled Power Electronics for Unmanned Aerial Vehicles. *Proc. IEEE*, 1–8

[3] Cruz, J. E. C., Goyzueta, C. A. R., and Cahuana, C. D., 2020. Intrusion Detection and Prevention System for Production Supervision in Small Businesses Based on Raspberry Pi and Snort. in Proc. IEEE.

[4] Saputra, M. I. and Yani, J. A., 2023. Literature Review Network Security. Journal of Computer Networks and Security, 4(3): 30-34

[5] Liu, J., Xiao, K., Luo, L., Li, Y., and Chen, L., 2020. An Intrusion Detection System Integrating Network-Level Intrusion Detection and Host-Level Intrusion Detection. IEEE 20th International Conference on Software Quality, Reliability, and Security (QRS), 51102: 122–129

[6] Aeraj, O. E. and Leghris, C., 2024. Analysis of the SNORT intrusion detection system using machine learning. International Journal of Information Science & Technology, 8(1): 1-8

[7] Prabhakaran, A., Chaurasiya, V. K., Singh, S., and Yadav, S., 2020. An Optimized Deep Learning Framework for Network Intrusion Detection System (NIDS). International Conference Engineering and Telecommunication, 2020: 1-6

[8] Liu, M., Xue, Z., and He, X., 2020. A Unified Host-Based Intrusion Detection Framework using Spark in Cloud. in Proceedings 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications, 97–103.

[9] Erlacher, F. and Dressler, F., 2022. On High-Speed Flow-Based Intrusion Detection Using Snort-Compatible Signatures, IEEE Trans Dependable Secure Comput, 19(1): 495–506

[10] Fadhilah, D. and Marzuki, M. I., 2020. Performance Analysis of IDS Snort and IDS Suricata with Many-Core Processor in Virtual Machines against Dos/DDoS Attacks. in 2020 2nd International Conference on Broadband Communications, Wireless Sensors and Powering (BCWSP), 157–162

[11] Made, I., Sulistya, A., Made, G., and Sasmita, A., 2020. Network Security Monitoring System on Snort with Bot Telegram as a Notification. International Journal of Computer Applications Technology and Research (IJCATR), 9(2): 59-64

[12] Zhang, G. and Li, E., 2020. Research on IDS Snort Based on Classic Clustering Algorithm. in Proceedings 2020 International Conference on Urban Engineering and Management Science (ICUEMS), 673–676

[13] Erlacher, F. and Dressler, F., 2022. On High-Speed Flow-Based Intrusion Detection Using Snort-Compatible Signatures. Journal of IEEE Trans Dependable Secure Comput, 19(1): 495–506

[14] Luxemburk, J., Hynek, K., and Cejka, T., 2021. Detection of HTTPS Brute-Force Attacks with Packet-Level Feature Set. in 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC), 114–122

[15] Hossain, M. D., Ochiai, H., Doudou, F., & Kadobayashi, Y. (2020). SSH and FTP brute-force Attacks Detection in Computer Networks: L STMand Machine Learning Approaches. International Conference on Computer and Communication Systems, 15-18

[16] Fadhilah, D. and Marzuki, M. I., 2020. Performance Analysis of IDS Snort and IDS Suricata with Many-Core Processor in Virtual Machines against Dos/DDoS Attacks. in 2020 2nd International Conference on Broadband Communications, Wireless Sensors and Powering (BCWSP), 157–162

[17] Anium, S., 2020. DoS Attacks, Triad and Privacy: Software Exposures in Microsoft, Apple and Google. in Proceedings 2020 1st International Conference of Smart Systems and Emerging Technologies, 53–58

[18] Rios, A. L. G., Li, Z., Bekshentayeva, K., and Trajkovi'c, L., 2020. Detection of Denial of Service Attacks in Communication Networks. IEEE International Symposium on Circuits and Systems, 10-21

[19] Sumanth, R. and Bhanu, K. N., 2020. Raspberry Pi Based Intrusion Detection System Using K-Means Clustering Algorithm. International Conference on Inventive Research in Computing Applications, 15-17

[20] Penyala, H., Ibrahim, S., and Mesalami, A. E., 2020. The Raspberry Pi Education Mine: For Teaching Engineering and Computer Science Students Concepts Like, Computer Clusters, Parallel Computing, and Distributed Computing. in IEEE International Conference on Electro Information Technology, 624–628

[21] Fezari, M., Dahoud, A. A., Fezari, M., and Dahoud, A. A., 2023. Raspberry Pi 5 : The new Raspberry Pi family with more computation power and AI integration. doi: 10.13140/RG.2.2.13547.52009.

[22] Liu, M. and Xue, Z., 2021. Two-Tier Intrusion Detection Framework for Embedded Systems. Journal of IEEE Consumer Electronics Magazine, 10(5): 102-108

[23] Williams, B., Dong, X., and Qian, L., 2020. Data Driven Network Monitoring and Intrusion Detection using Machine Learning. in 2020 7th International Conference on Social Network Analysis, Management and Security (SNAMS), 114-122

[24] Rezaeighaleh, H. and Zou, C. C., 2020. Multilayered Defense-in-Depth Architecture for Cryptocurrency Wallet. IEEE 6th International Conference on Computer and Communications, 2212-2217

[25] Yendamury, G. and Mohankumar, N., 2021. Defense in Depth Approach on AES Cryptographic Decryption Core to Enhance Reliability. IEEE International IOT, Electronics and Mechatronics Conference Proceedings, 2122-2127

[26] Lingkang, Z., Yuwei, L., and Xue, J., 2020. Detection of Abnormal Data Flow at Network Boundary of Renewable Energy Power System. IEEE 3rd International Conference on Automation, Electronics and Electrical Engineering, 309–312

[27] Zhou, Y., Luo, A., Kang, X., and Lyu, S., 2021. Face Forgery Detection Based on Segmentation Network. Proceedings - International Conference on Image Processing ICIP, 3597-3601

[28] Alsaqour, R., Majrashi, A., Alreedi, M., Alomar, K., Abdelhaq, M., 2021. Defense in Depth: Multilayer of Security. International Journal of Communication Networks and Information Security (IJCNIS), 13(2): 242-248

[29] Wai, E. and Lee, C. K. M., 2024. Depth in Defense: A Multi-layered Approach to Cybersecurity for SCADA Systems in Industry 4.0, 124-144