PERANCANGAN *INTRUSION PREVENTION SYSTEM* MENGGUNAKAN *SIGNATURE BASED* DAN IP *FILTERING* TERHADAP SERANGAN *BRUTEFORCE*

Tugas Akhir

Diajukan untuk melengkapi salah satu syarat
memperoleh gelar sarjana komputer

Oleh:

Paradika Dwi Oktaviansyah

09011181924015

PROGRAM STUDI ILMU KOMPUTER

JURUSAN SISTEM KOMPUTER

UNIVERSITAS SRIWIJAYA

2025

HALAMAN PENGESAHAN

SKRIPSI

PERANCANGAN *INTRUSION PREVENTION SYSTEM* MENGGUNAKAN *SIGNATURE BASED* DAN IP *FILTERING* TERHADAP SERANGAN *BRUTEFORCE*

Sebagai salah satu syarat untuk penyelesaian studi di
Program Studi S1 Sisitem Komputer

Oleh:

PARADIKA DWI OKTAVIANSYAH

09011181924015

Pembimbing 1 **: Dr. Ir. Ahmad Heryanto, M. T.**
NIP. 198701222015041002

Mengetahui

Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, M.T
196612032006041001

AUTHENTICATION PAGE

FINAL TASK

DESIGN OF AN INTRUSION PREVENTION SYSTEM USING SIGNATURE-BASED DETECTION AND IP FILTERING AGAINST BRUTEFORCE ATTACKS

As one of the requirements for the completion of studies in the Bachelor's Degree Program in Computer Systems

By:

PARADIKA DWI OKTAVIANSYAH

09011181924015

Supervisor 1 **: Dr. Ir. Ahmad Heryanto, M. T.**
NIP. 198701222015041002

Acknowledge
Head of Computer System Department

Dr. Ir. Sukemi, M.T
196612032006041001

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada

Hari : Senin

Tanggal : 14 April 2025

Tim Penguji :

1. **Ketua Sidang : Yoppy Sazaki, M.T.**
2. **Penguji Sidang : Dr. Ir. Sukemi, M.T.**
3. **Pembimbing : Dr. Ir. Ahmad Heryanto, M.T.**

Mengetahui, 14/5/25

Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, M.T.

NIP. 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini :

Nama : Paradika Dwi Oktaviansyah

NIM : 09011181924015

Judul : PERANCANGAN *INTRUSION PREVENTION SYSTEM* MENGGUNAKAN *SIGNATURE BASED* DAN *IP FILTERING* TERHADAP SERANGAN *BRUTEFORCE*

Hasil pengecekan *Software Turnitin* : 3%

Menyatakan bahwa laporan tugas akhir saya merupakan hasil karya sendiri dan bukan hasil penjiplakan atau plagiat. Apabila ditemukan unsur penjiplakan atau plagiat dalam laporan tugas akhir ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya. Demikian, pernyataan ini saya buat dalam keadaan sadar dan tidak dipaksakan.

Indralaya, 20 April 2025

Paradika Dwi Oktaviansyah
NIM. 09011181924015

KATA PENGANTAR

Assalamualaikum Warahmatullahi Wabarakatuh.

Puji syukur atas kehadirat Allah SWT yang telah memberikan segala rahmat dan hidayah-Nya, sehingga penulis dapat menyelesaikan penyusunan Proposal Tugas Akhir dengan judul **"Perancangan *Instrusion Prevention System* Menggunakan *Signature Based* dan IP *Filtering* Terhadap Serangan *Bruteforce*"**.

Penulis berharap proposal yang telah disusun ini dapat membantu dan bermanfaat bagi pihak yang membutuhkan, serta menjadi salah satu sumber bacaan atau referensi bagi peneliti yang lain juga.

Pada kesempatan ini penulis ingin mengucapkan terima kasih kepada beberapa pihak yang telah memberi masukan seperti ide dan saran, serta bantuan dalam menyelesaikan penulisan Proposal Tugas Akhir ini. Oleh karena itu, penulis ingin mengucapkan rasa syukur dan terima kasih kepada yang terhormat:

1. Allah SWT, yang telah memberikan rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan penulisan Tugas Akhir ini dengan baik.
2. Orang tua saya tercinta yang telah membesarkan saya dengan penuh kasih sayang serta memberikan do'a, motivasi dan dukungannya selama ini baik dari segi materil maupun spritual.
3. Bapak Prof. Dr. Erwin, S.Si., M.Si. selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Dr. Ir. H. Sukemi, M.T. selaku Ketua Jurusan Sistem Komputer Universitas Sriwijaya.
5. Bapak Dr. Ir. Ahmad Heryanto, M.T. selaku Dosen Pembimbing Tugas Akhir yang berkenan meluangkan banyak waktu untuk membimbing, memberikan saran dalam setiap pertemuan bimbingan kepada penulis dalam menyelesaikan Tugas Akhir ini.
6. Bapak Prof. Dr. Ir. Bambang Tutuko, M.T. selaku Dosen Pembimbing Akademik saya di Jurusan Sistem Komputer.

7. Kak Angga selaku admin Jurusan Sistem Komputer yang telah membantu mengurus seluruh keperluan berkas.
8. Serta semua pihak yang telah membantu.

Penulis menyadari sepenuhnya bahwa laporan ini masih memliki banyak kekurangan dan jauh dari kata sempurna. Untuk itu kritik dan saran dari semua pihak yang membangun sangat diharapkan penulis untuk evaluasi agar lebih baik lagi. Akhir kata penulis berharap, semoga proposal tugas akhir ini dapat bermanfaat bagi orang lain.

Wassalamualaikum Warahmatullahi Wabarakatuh.

Indralaya, 20 April 2025

Penulis,

Paradika Dwi Oktaviansyah

NIM. 09011181924015

PERANCANGAN *INTRUSION PREVENTION SYSTEM* MENGGUNAKAN *SIGNATURE BASED* DAN IP *FILTERING* TERHADAP SERANGAN *BRUTEFORCE*

PARADIKA DWI OKTAVIANSYAH (09011181924015)

Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya

Email : paradikadwio@gmail.com

ABSTRAK

Keamanan jaringan sangat penting untuk melindungi sistem dari berbagai ancaman siber, salah satunya adalah serangan *bruteforce*. Serangan ini dilakukan dengan mencoba berbagai kombinasi kata sandi secara berulang hingga menemukan yang benar. Jika tidak dicegah, serangan ini bisa menyebabkan akses ilegal ke sistem dan berpotensi menimbulkan kerugian yang besar. Oleh karena itu, diperlukan sistem perlindungan yang bisa mendeteksi dan menghentikan serangan ini sebelum terjadi kerusakan lebih lanjut. Penelitian ini bertujuan untuk merancang *Intrusion Prevention System* (IPS) yang menggunakan metode *Signature-Based Detection* dan IP *Filtering. Signature-Based Detection* bekerja dengan mengenali pola serangan yang sudah diketahui sebelumnya, sedangkan *IP Filtering* akan memblokir alamat IP yang terdeteksi melakukan aktivitas mencurigakan. Sistem ini kemudian diuji dalam lingkungan jaringan untuk melihat seberapa efektif kemampuannya dalam mendeteksi dan mencegah serangan brute force. Penelitian dilakukan dengan lima kali percobaan dengan parameter yang berbeda di tiap percobaannya. Berdasarkan pengujian yang telah dilakukan, didapatkan hasil terbaik dari *Detection Mode:* Langsung, *Whitelist/Blacklist*, dan *Rate Limiting:* 150 req/s, dengan nilai deteksi mencapai 93.8% dan nilai pencegahan mencapai 91.2%.

Kata Kunci: *Intrusion Prevention System*, Serangan *Brute Force*, *Signature-Based Detection*, *IP Filtering*, Keamanan Jaringan

Mengetahui

Ketua Jurusan Sistem Komputer	**Pembimbing Tugas Akhir**
Dr. Ir. Sukemi, M.T.	**Dr. Ir. Ahmad Heryanto, M.T.**
NIP. 196612032006041001	**NIP. 198701222015041002**

DESIGN OF AN INTRUSION PREVENTION SYSTEM USING SIGNATURE-BASED DETECTION AND IP FILTERING AGAINST BRUTEFORCE ATTACKS

PARADIKA DWI OKTAVIANSYAH (09011181924015)

Department of Computer Systems, Faculty of Computer Science, Sriwijaya University

Email : paradikadwio@gmail.com

ABSTRACT

Network security is crucial for protecting systems from various cyber threats, one of which is a brute force attack. This type of attack involves repeatedly trying different password combinations until the correct one is found. If left unchecked, brute force attacks can lead to unauthorized system access and potentially cause significant damage. Therefore, a security system is needed to detect and stop such attacks before they cause further harm. This study aims to design an Intrusion Prevention System (IPS) using Signature-Based Detection and IP Filtering. Signature-Based Detection works by recognizing attack patterns that have been previously identified, while IP Filtering blocks IP addresses that exhibit suspicious activity. The system is then tested in a network environment to evaluate its effectiveness in detecting and preventing brute force attacks. The research was conducted through five trial experiments, each with different parameters. Based on the testing results, the best performance was achieved using Detection Mode: Direct, Whitelist/Blacklist, and Rate Limiting: 150 req/s, with a detection rate of 93.8% and a prevention rate of 91.2%.

Keywords: Intrusion Prevention System, Brute Force Attack, Signature-Based Detection, IP Filtering, Network Security

Approved by

Head of the Computer Systems Department	**Supervisor**
Dr. Ir. Sukemi, M.T.	**Dr. Ir. Ahmad Heryanto, M.T.**
NIP. 196612032006041001	**NIP. 19870122201504100**

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB I

PENDAHULUAN

1.1 Pendahuluan

Bab pendahuluan akan membahas tentang latar belakang masalah, rumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah penelitian, dan sistematika penulisan. Bab ini akan memberikan penjelasan umum mengenai pokok pikiran dari keseluruhan penelitian.

1.2 Latar Belakang

Keamanan sistem informasi menjadi sangat penting seiring dengan perkembangan teknologi dan peningkatan ketergantungan organisasi dan individu terhadap infrastruktur digital. Salah satu tantangan utama dalam menjaga keamanan sistem adalah serangan cyber, di antaranya adalah serangan brute force. Serangan brute force adalah upaya untuk masuk ke dalam sistem dengan mencoba berbagai kombinasi kata sandi secara berulang hingga berhasil mendapatkan akses yang tidak sah. Serangan semacam ini dapat menimbulkan kerugian besar bagi korban, baik berupa pencurian data sensitif, kerusakan sistem, maupun gangguan operasional.

Meskipun sudah ada banyak teknik dan alat yang dikembangkan untuk mengatasi serangan brute force, namun masih terdapat beberapa permasalahan yang perlu dipecahkan. Beberapa metode yang ada mungkin kurang efektif dalam mendeteksi serangan secara tepat waktu, sehingga memungkinkan penyerang untuk berhasil masuk ke dalam sistem sebelum serangan terdeteksi. Selain itu, false positive juga merupakan masalah umum yang mengganggu operasional sistem, dimana sistem keamanan mengidentifikasi aktivitas normal sebagai serangan, sehingga memicu tindaakn yang tidak perlu.

Dalam konteks ini, diperlukan solusi yang lebih efektif dan efisien untuk melindungi sistem dari serangan brute force. Salah satu pendekatan yang diusulkan adalah pengembangan *Intrusion Prevention System* (IPS) yang

menggabungkan metode signature-based dan IP filtering. Metode *signature-based* memungkinkan deteksi pola serangan yang sudah diketahui secara efisien, sedangkan IP filtering dapat digunakan untuk memblokir alamat IP yang mencurigakan atau yang telah terdeteksi melakukan serangan brute force. Dengan demikian, diharapkan IPS yang dirancang dapat memberikan perlindungan yang lebih baik terhadap serangan brute force, mengurangi risiko kerusakan sistem, pencurian data, dan gangguan operasional yang dapat timbul akibat serangan tersebut.

Pada penelitian yang dilakukan oleh Thomas dan Huang [1], meskipun model pembelajaran mesin yang mereka gunakan mampu mendeteksi pola serangan baru, model ini membutuhkan waktu pelatihan yang cukup lama serta sumber daya komputasi yang besar. Hal ini dapat menjadi kendala ketika sistem harus mendeteksi dan merespon serangan secara *real-time*, terutama pada jaringan dengan keterbatasan kapasitas. Selain itu, model berbasis aturan yang digunakan masih rentan terhadap perubahan pola serangan yang tidak tercakup dalam aturan yang ada, sehingga tingkat akurasi deteksi menurun ketika pola serangan baru muncul.

Penelitian Singh dan Sahu [2] juga memiliki keterbatasan, terutama dalam hal ketergantungan pada algoritma hash. Meskipun hash efektif untuk mengamankan data sensitif, metode ini tidak dapat sepenuhnya menghentikan serangan brute force karena hanya mempersulit upaya penyerang, bukan mencegahnya. Selain itu, algoritma *hash* yang kompleks cenderung memperlambat proses autentikasi, sehingga dapat mengganggu pengalaman pengguna dan kinerja sistem secara keseluruhan, terutama pada sistem dengan jumlah pengguna yang tinggi.

Adapun metode IP filtering adaptif yang dikembangkan oleh Luo dan Zhu [3], walaupun mampu meningkatkan efisiensi dengan memblokir IP yang mencurigakan, metode ini masih rentan terhadap serangan distributed brute force, di mana penyerang menggunakan berbagai IP untuk mencoba mengakses sistem. Metode ini juga berpotensi menimbulkan *false positive*, terutama pada

pengguna yang memiliki koneksi dinamis atau berada di jaringan publik, sehingga IP mereka dapat terblokir secara tidak sengaja.

Oleh karena itu, metode yang digunakan dalam penelitian ini, yaitu pengembangan *Intrusion Prevention System* (IPS) yang menggabungkan metode signature-based dan IP filtering, diharapkan dapat mengatasi kelemahan dari metode terdahulu. Pendekatan signature-based memungkinkan deteksi pola serangan yang lebih cepat dan tepat waktu tanpa membutuhkan banyak sumber daya, sedangkan IP *filtering* yang diterapkan secara selektif dapat mengurangi risiko false positive dan serangan distributed brute force, sehingga memberikan perlindungan yang lebih optimal bagi sistem.

1.3 Rumusan Masalah

Berdasarkan penjelasan dari latar belakang, maka rumusan masalah dari penelitian ini sebagai berikut:

1. Bagaimana merancang sebuah *Intrusion Prevention System* (IPS) yang efektif dalam melindungi sistem dari serangan brute force, dengan mengintegrasikan metode *signature-based* dan IP *filtering* sehingga dapat mendeteksi dan mencegah serangan secara tepat waktu, mengurangi risiko *false positive*, serta memberikan perlindungan yang optimal terhadap kerugian yang dapat ditimbulkan oleh serangan brute force?

1.4 Tujuan Penelitian

Tujuan penelitian ini adalah sebagai berikut:

1. Merancang sebuah IPS yang dapat secara efektif mengatasi serangan brute force dengan menggabungkan metode *signature-based* dan IP *filtering*. IPS yang dirancang diharapkan mampu mendeteksi serangan secara real-time, mengurangi *false positive*, serta memberikan perlindungan yang optimal terhadap kerugian yang mungkin ditimbulkan oleh serangan brute force.

1.5 Manfaat Penilitian

Manfaat penelitian ini adalah sebagai berikut:

1. Memberikan kontribusi dalam pengembangan teknologi keamanan informasi dengan menyediakan solusi yang lebih efektif dan efisien dalam melindungi sistem dari serangan brute force. Implementasi IPS yang dirancang dapat membantu organisasi dan individu untuk meningkatkan keamanan sistem mereka, mengurangi risiko pencurian data, kerusakan sistem, dan gangguan operasional.

1.6 Batasan Masalah

Batasan masalah penelitian ini adalah sebagai berikut:

1. Data yang digunakan berupa IP *Address* yang dikategorikan sebagai IP *blocking* dan IP *attacking.*
2. Menggunakan wsl sistem pada os windows yang terintegrasi dengan ubuntu.

1.7 Sistematika Penulisan

Sistematika penulisan pada penelitian ini adalah sebagai berikut:

BAB I. PENDAHULUAN

Bab ini menguraikan mengenai latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah, dan sistematika penulisan pada penelitian ini.

BAB II. TINJAUAN PUSTAKA

Bab ini membahas mengenai landasan teori yang digunakan dalam penelitian ini, seperti rancangan sistem *Intrusion Prevention System* menggunakan *Signature-Based* dan IP *Filtering* terhadap serangan brute force, serta membahas beberapa penelitian yang relevan.

BAB III. METODOLOGI PENELITIAN

Bab ini berisi pembahasan mengenai metodologi dan tahapan perancangan penelitian seperti pengumpulan data, metode pengembangan perangkat lunak, dan manajemen proyek penelitian.

BAB IV. HASIL DAN ANALISIS PENELITIAN

Bab ini menguraikan hasil pengujian berdasarkan perancangan. Tabel hasil evaluasi pengujian dan analisis serta grafik menjadi patokan dari kesimpulan yang akan diambil dalam penelitian

BAB V. KESIMPULAN DAN SARAN

Bab ini membahas mengenai kesimpulan berdasarkan semua uraian pada bab sebelumnya dan juga saran yang diberikan dari hasil penelitian.

DAFTAR PUSTAKA

[1] M. Y. Huang, R. J. Jasper, and T. M. Wicks, “Large scale distributed intrusion detection framework based on attack strategy analysis,” *Comput. Networks*, vol. 31, no. 23, pp. 2465–2475, 1999, doi: 10.1016/S1389-1286(99)00114-0.

[2] S. K. Sahu, D. P. Mohapatra, J. K. Rout, K. S. Sahoo, and A. K. Luhach, “An Ensemble-Based Scalable Approach for Intrusion Detection Using Big Data Framework,” *Big Data*, vol. 9, no. 4, pp. 303–321, Jul. 2021, doi: 10.1089/big.2020.0201.

[3] J. Ling, Z. Zhu, Y. Luo, and H. Wang, “An intrusion detection method for industrial control systems based on bidirectional simple recurrent unit,” *Comput. Electr. Eng.*, vol. 91, no. February 2020, p. 107049, 2021, doi: 10.1016/j.compeleceng.2021.107049.

[4] A. Fadhlillah, N. Karna, and A. Irawan, “IDS Performance Analysis using Anomaly-based Detection Method for DOS Attack,” *IoTaIS 2020 - Proc. 2020 IEEE Int. Conf. Internet Things Intell. Syst.*, pp. 18–22, 2021, doi: 10.1109/IoTaIS50849.2021.9359719.

[5] W. Bul’ajoul, A. James, and S. Shaikh, “A New Architecture for Network Intrusion Detection and Prevention,” *IEEE Access*, vol. 7, pp. 18558–18573, 2019, doi: 10.1109/ACCESS.2019.2895898.

[6] P. Freitas De Araujo-Filho, A. J. Pinheiro, G. Kaddoum, D. R. Campelo, and F. L. Soares, “An Efficient Intrusion Prevention System for CAN: Hindering Cyber-Attacks with a Low-Cost Platform,” *IEEE Access*, vol. 9, pp. 166855–166869, 2021, doi: 10.1109/ACCESS.2021.3136147.

[7] W. Alhakami, A. Alharbi, S. Bourouis, R. Alroobaea, and N. Bouguila, “Network Anomaly Intrusion Detection Using a Nonparametric Bayesian Approach and Feature Selection,” *IEEE Access*, vol. 7, pp. 52181–52190, 2019, doi: 10.1109/ACCESS.2019.2912115.

[8] X. A. Larriva-Novo, M. Vega-Barbas, V. A. Villagra, and M. Sanz

Rodrigo, “Evaluation of Cybersecurity Data Set Characteristics for Their Applicability to Neural Networks Algorithms Detecting Cybersecurity Anomalies,” *IEEE Access*, vol. 8, pp. 9005–9014, 2020, doi: 10.1109/ACCESS.2019.2963407.

[9] P. L. S. Jayalaxmi, R. Saha, G. Kumar, M. Conti, and T. H. Kim, “Machine and Deep Learning Solutions for Intrusion Detection and Prevention in IoTs: A Survey,” *IEEE Access*, vol. 10, no. October, pp. 121173–121192, 2022, doi: 10.1109/ACCESS.2022.3220622.

[10] T. Girdler and V. G. Vassilakis, “Implementing an intrusion detection and prevention system using Software-Defined Networking: Defending against ARP spoofing attacks and Blacklisted MAC Addresses,” *Comput. Electr. Eng.*, vol. 90, no. January, p. 106990, 2021, doi: 10.1016/j.compeleceng.2021.106990.

[11] M. Poongodi, V. Vijayakumar, F. Al-Turjman, M. Hamdi, and M. Ma, “Intrusion Prevention System for DDoS Attack on VANET with reCAPTCHA Controller Using Information Based Metrics,” *IEEE Access*, vol. 7, pp. 158481–158491, 2019, doi: 10.1109/ACCESS.2019.2945682.

[12] M. H. Nasir, J. Arshad, and M. M. Khan, “Collaborative Device-level Botnet Detection for Internet of Things,” *Comput. Secur.*, vol. 129, p. 103172, 2023, doi: 10.1016/j.cose.2023.103172.

[13] M. Y. Aldarwbi, A. H. Lashkari, and A. A. Ghorbani, “The sound of intrusion: A novel network intrusion detection system,” *Comput. Electr. Eng.*, vol. 104, no. PA, p. 108455, 2022, doi: 10.1016/j.compeleceng.2022.108455.

[14] M. Lima, R. Lima, F. Lins, and M. Bonfim, “Beholder – A CEP-based intrusion detection and prevention systems for IoT environments,” *Comput. Secur.*, vol. 120, p. 102824, 2022, doi: 10.1016/j.cose.2022.102824.

[15] C. Birkinshaw, E. Rouka, and V. G. Vassilakis, “Implementing an intrusion detection and prevention system using software-defined networking: Defending against port-scanning and denial-of-service attacks,” *J. Netw. Comput. Appl.*, vol. 136, no. October 2018, pp. 71–85, 2019, doi:

10.1016/j.jnca.2019.03.005.

[16] L. Yu *et al.*, “PBCNN: Packet Bytes-based Convolutional Neural Network for Network Intrusion Detection,” *Comput. Networks*, vol. 194, no. January, p. 108117, 2021, doi: 10.1016/j.comnet.2021.108117.

[17] Z. Chiba, N. Abghour, K. Moussaid, O. Lifandali, and R. Kinta, “A Deep Study of Novel Intrusion Detection Systems and Intrusion Prevention Systems for Internet of Things Networks,” *Procedia Comput. Sci.*, vol. 210, no. C, pp. 94–103, 2022, doi: 10.1016/j.procs.2022.10.124.

[18] A. Kumar, K. Abhishek, M. R. Ghalib, A. Shankar, and X. Cheng, “Intrusion detection and prevention system for an IoT environment,” *Digit. Commun. Networks*, vol. 8, no. 4, pp. 540–551, 2022, doi: 10.1016/j.dcan.2022.05.027.

[19] P. Bountakas, C. Ntantogian, and C. Xenakis, “EKnad: Exploit Kits’ network activity detection,” *Futur. Gener. Comput. Syst.*, vol. 134, pp. 219–235, 2022, doi: 10.1016/j.future.2022.04.001.

[20] G. Xian, “Cyber Intrusion Prevention for Large-Scale Semi-Supervised Deep Learning Based on Local and Non-Local Regularization,” *IEEE Access*, vol. 8, pp. 55526–55539, 2020, doi: 10.1109/ACCESS.2020.2981162.

[21] J. Appiah-Kubi and C. C. Liu, “Decentralized Intrusion Prevention (DIP) against Co-Ordinated Cyberattacks on Distribution Automation Systems,” *IEEE Open Access J. Power Energy*, vol. 7, no. October, pp. 389–402, 2020, doi: 10.1109/OAJPE.2020.3029805.

[22] W. Seo and W. Pak, “Real-Time Network Intrusion Prevention System Based on Hybrid Machine Learning,” *IEEE Access*, vol. 9, pp. 46386–46397, 2021, doi: 10.1109/ACCESS.2021.3066620.

[23] A. Ali, A. Ali, and M. M. Yousaf, “Novel Three-Tier Intrusion Detection and Prevention System in Software Defined Network,” *IEEE Access*, vol. 8, pp. 109662–109676, 2020, doi: 10.1109/ACCESS.2020.3002333.