MENDESAIN SISTEM PENCEGAHAN INTRUSI YANG FLEKSIBEL DAN ADAPTIF UNTUK MENANGANI BERBAGAI JENIS ANCAMAN PADA SISTEM OPERASI WINDOWS

Rakhmadi Rahman[1], Risda[2], Muh Fauzan I Tisham[3]
rakhmadi.rahman@ith.ac.id[1], risrisda95@gmail.com[2], fauzanmuhammad8815@gmail.com[3]
Institut Teknologi Baharuddin Jusuf Habibie

ABSTRAK

Penelitian ini mengembangkan sistem pencegahan intrusi (IPS) yang fleksibel dan adaptif untuk menangani beragam ancaman keamanan pada sistem operasi Windows. Metodologi mencakup analisis ancaman, evaluasi kebutuhan sistem, dan perancangan arsitektur terintegrasi. IPS yang dihasilkan terdiri dari komponen deteksi menggunakan machine learning dan signature-based detection, komponen analisis memanfaatkan big data analytics dan analisis perilaku, serta komponen respons dengan sistem berbasis aturan dan respons otomatis. Sistem ini dilengkapi mekanisme pembelajaran dinamis, arsitektur modular, dan kustomisasi kebijakan. Integrasi dengan fitur keamanan Windows meningkatkan efektivitas perlindungan secara keseluruhan. Hasil penelitian menunjukkan potensi signifikan dalam memberikan perlindungan yang lebih komprehensif terhadap ancaman keamanan yang terus berkembang pada Windows.
Kata Kunci: Sistem Pencegahan Intrusi (IPS), Windows, Keamanan Siber, Kecerdasan Buatan, Pembelajaran Mesin, Malware, Ransomware, Phishing.

Abstract

This research develops a flexible and adaptive intrusion prevention system (IPS) to handle diverse security threats on Windows operating systems. The methodology includes threat analysis, system requirements evaluation, and integrated architecture design. The resulting IPS consists of a detection component using machine learning and signature-based detection, an analysis component utilizing big data analytics and behavioral analysis, and a response component with a rule-based system and automated response. The system features dynamic learning mechanisms, modular architecture, and policy customization. Integration with Windows security features increases the overall effectiveness of protection. The results show significant potential in providing more comprehensive protection against evolving security threats on Windows.
Keywords: *Intrusion Prevention System (IPS), Windows, Cyber Security, Artificial Intelligence, Machine Learning, Malware, Ransomware, Phishing.*

PENDAHULUAN

Sistem operasi Windows, dengan penggunaan globalnya yang luas, sering kali menjadi target utama ancaman keamanan siber yang terus berkembang. Meskipun ada fitur keamanan bawaan seperti Windows Defender dan Windows Firewall, evolusi pesat ancaman dunia maya terus menantang efektivitas pertahanan yang ada. Malware, ransomware, phishing, dan perangkat eksploitasi adalah contoh ancaman yang dapat merusak sistem dan mencuri data sensitif.

Sistem pencegahan intrusi (IPS) tradisional sering kali menghadapi keterbatasan dalam mendeteksi dan merespons ancaman baru atau serangan canggih. Tujuan dari penelitian ini adalah untuk mengembangkan IPS yang lebih fleksibel dan adaptif untuk Windows menggunakan teknologi seperti pembelajaran mesin dan analisis data besar.

Pentingnya penelitian ini adalah dapat meningkatkan keamanan siber pengguna Windows di seluruh dunia. Dengan mengintegrasikan kemampuan deteksi dan respons tingkat lanjut dengan fitur keamanan bawaan Windows, sistem ini bertujuan untuk

memberikan perlindungan yang lebih kuat dan komprehensif terhadap ancaman yang terus berkembang.

METODE PENELITIAN

Metodologi penelitian melibatkan beberapa tahapan penting, yang meliputi:

- Analisis Kebutuhan Sistem: Tahap ini melibatkan identifikasi kebutuhan fungsional dan non-fungsional, evaluasi sistem pencegahan intrusi tradisional, penilaian teknologi terkini, dan penyusunan spesifikasi sistem.
- Desain Arsitektur Sistem: Tahap ini mencakup pembuatan komponen utama, mekanisme adaptasi dan fleksibilitas, integrasi dengan fitur keamanan Windows, dan pembuatan diagram arsitektur sistem.
- Penggunaan Algoritma dan Teknik: Penelitian ini menggunakan berbagai algoritma dan teknik, termasuk algoritma pembelajaran mesin, teknik analisis data besar, algoritma pendeteksi anomali, algoritma berbasis aturan, teknik pemrosesan bahasa alami, algoritma pembelajaran reinforcement, dan teknik enkripsi dan otentikasi.
- Integrasi dengan Fitur Keamanan Windows: Sistem yang dirancang diintegrasikan dengan fitur keamanan Windows, termasuk Windows Defender, BitLocker, dan Windows Firewall. Integrasi ini memungkinkan sistem untuk bekerja sama dengan fitur-fitur ini untuk memberikan perlindungan yang lebih luas dan efektif.

A. Analisis Kebutuhan Sistem

Pada tahap ini, kebutuhan fungsional dan non-fungsional diidentifikasi dan teknologi yang tersedia dievaluasi. Langkah-langkah yang diambil meliputi:

- Identifikasi Ancaman: Malware, ransomware, spyware, phishing, rootkit, dan perangkat lunak eksploit.
- Evaluasi IPS Tradisional: Menilai kelebihan, kelemahan, teknik deteksi, dan efektivitas.
- Kebutuhan Fungsional: Deteksi real-time, respon cepat, adaptasi dinamis, dan integrasi dengan fitur keamanan Windows.
- Kebutuhan Non-Fungsional: Skalabilitas dan keandalan.
- Penilaian Teknologi: Evaluasi teknologi terbaru untuk memenuhi kebutuhan sistem.
- Spesifikasi Sistem: Menyusun spesifikasi berdasarkan analisis kebutuhan dan teknologi.

B. Desain Arsitektur Sistem

Untuk menangani berbagai jenis ancaman pada sistem operasi Windows, arsitektur sistem pencegahan intrusi mencakup beberapa komponen utama dan mekanisme yang memungkinkan deteksi, analisis, dan respons terhadap ancaman secara efektif dan efisien. Rincian desain arsitektur sistem yang diusulkan meliputi:

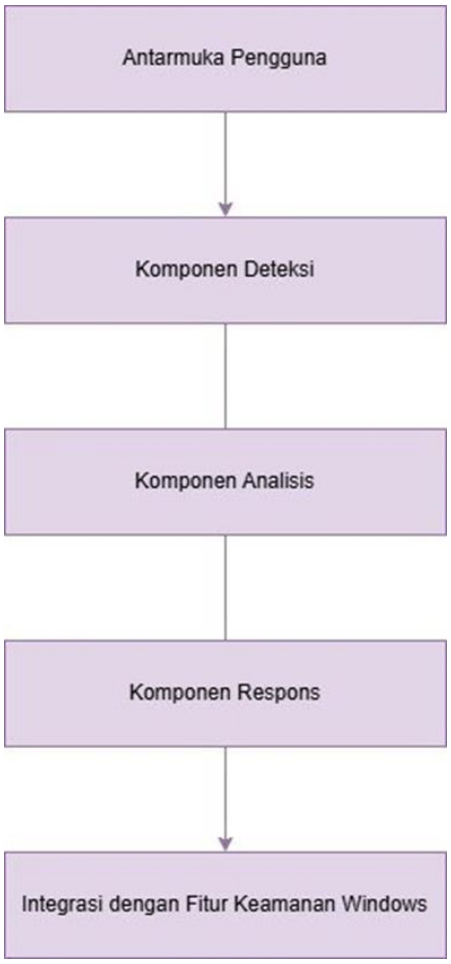
- Komponen Utama: Identifikasi komponen sistem pencegahan intrusi.
- Mekanisme Adaptasi: Desain mekanisme untuk adaptasi dan fleksibilitas terhadap ancaman baru.
- Integrasi dengan Keamanan Windows: Integrasi dengan Windows Defender, BitLocker, dan Windows
- Firewall.
- Diagram Arsitektur: Penyusunan diagram arsitektur sistem.

C. Algoritma dan Teknik yang Digunakan

Berbagai algoritma dan teknik digunakan dalam penelitian ini, termasuk algoritma pembelajaran mesin, teknik analisis data besar, algoritma pendeteksi anomali, algoritma berbasis aturan, teknik pemrosesan bahasa alami, algoritma pembelajaran reinforcement, dan teknik enkripsi dan otentikasi.

D. Integrasi dengan Windows Security Features

Sistem yang dirancang diintegrasikan dengan fitur keamanan Windows, termasuk Windows Defender, BitLocker, dan Windows Firewall. Integrasi ini memungkinkan sistem untuk bekerja sama dengan fitur-fitur ini untuk memberikan perlindungan yang lebih luas dan efektif.



Gambar 1.Diagram Arsitektur Sistem.

HASIL DAN PEMBAHASAN

Keamanan pada Windows

Penelitian mengidentifikasi ancaman utama pada Windows:

- Komponen Utama: Identifikasi komponen sistem pencegahan intrusi.
- Mekanisme Adaptasi: Desain mekanisme untuk adaptasi dan fleksibilitas terhadap ancaman baru.
- Integrasi dengan Keamanan Windows: Integrasi dengan Windows Defender, BitLocker, dan Windows
- Firewall.
- Diagram Arsitektur: Penyusunan diagram arsitektur sistem.

Kebutuhan Sistem Pencegahan Intrusi

Sistem harus memenuhi:

- **Fungsional:**
- Deteksi real-time
- Respon cepat
- **Non-Fungsional:**

- Ketersediaan tinggi
- Skalabilitas
- Kinerja optimal

Perancangan Sistem Pencegahan Intrusi Desain sistem mencakup:

- Komponen Utama:
- Sensor Deteksi: Memonitor aktivitas mencurigakan
- Modul Analisis: Mendeteksi pola ancaman
- Modul Respon: Tindakan terhadap ancaman
- Mekanisme Adaptasi:
- Pembelajaran Mesin: Algoritma untuk deteksi ancaman
- Pembaruan Dinamis: Pembaruan tanpa intervensi manual
- Integrasi API: Komunikasi dengan fitur keamanan Windows lainnya

Pendekatan ini memberikan perlindungan komprehensif terhadap berbagai ancaman di Windows, memastikan keamanan dan kinerja optimal sistem.

Gambar 1. 2 Visualisasi Diagram Arsitektur.

KESIMPULAN

Penelitian ini merancang sistem pencegahan intrusi (IPS) yang fleksibel dan adaptif untuk Windows dengan hasil:

- Komponen Utama: Identifikasi komponen sistem pencegahan intrusi. Deteksi Anomali dan Signature: Menggunakan machine learning dan deteksi berbasis signature untuk identifikasi ancaman.
- Analisis Data Besar: Mengidentifikasi pola kompleks ancaman.
- Respons Adaptif: Tindakan pencegahan yang menyesuaikan dengan jenis ancaman.
- Integrasi Keamanan Windows: Meningkatkan perlindungan dengan fitur keamanan bawaan seperti Windows Defender dan BitLocker.

SARAN

- Pengembangan Lebih Lanjut: Tingkatkan algoritma dan teknik analisis.
- Pengujian Lapangan: Uji sistem di lingkungan nyata.
- Integrasi Lanjutan: Tambah integrasi dengan solusi keamanan pihak ketiga.
- Pembaruan Berkelanjutan: Sediakan mekanisme pembaruan otomatis.
- Pelatihan Pengguna: Adakan pelatihan rutin bagi pengguna dan administrator.

DAFTAR PUSTAKA

[1] Bace, R. G., & Mell, P. (2001). Intrusion Detection Systems. National Institute of Standards and Technology. Retrieved from https://csrc.nist.gov/publications/detail/sp/800- 31/final

[2] Brown, C., & Gommers, J. (2014). Automated threat detection and prevention using machine learning. In Proceedings of the ACM Conference on Computer and Communications Security.Retrieved from https://doi.org/10.1145/2664243.2664250

[3] Chen, Z., & Xin, Y. (2020). Intrusion detection using deep learning and advanced preprocessing techniques. IEEE Access, 8, 59381-59399. Retrieved from https://doi.org/10.1109/ACCESS.2020.2983074

[4] Garuba, M., Liu, C., & Fraites, D. (2008). Intrusion techniques: Comparative study of network intrusion detection systems. Journal of Information Assurance and Security, 3(2), 79-87.

[5] Gates, C. S., & Taylor, C. N. (2007). Challenging the anomaly detection paradigm: A provocative discussion. In Proceedings of the 2007 Workshop on New Security Paradigms. Retrieved from https://doi.org/10.1145/1600176.1600183

[6] Liao, H. J., Lin, C. H. R., Lin, Y. C., & Tung, K. Y. (2013). Intrusion detection system: A comprehensive review. Journal of Network and Computer Applications, 36(1), 16-24. Retrieved from https://doi.org/10.1016/j.jnca.2012.09.004

[7] Scarfone, K., & Mell, P. (2007). Guide to Intrusion Detection and Prevention Systems (IDPS). NIST Special Publication 800-94. National Institute of Standards and Technology. Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf

[8] Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. In IEEE Symposium on Security and Privacy. Retrieved from https://doi.org/10.1109/SP.2010.25

[9] Stolfo, S. J., Fan, W., Lee, W., Prodromidis, A. L., & Chan, P. K. (2000). Cost-based modeling for fraud and intrusion detection: Results from the JAM project. In Proceedings DARPA Information Survivability Conference and Exposition. Retrieved from https://doi.org/10.1109/DISCEX.2000.821514

[10] Yao, Y., Hu, L., & Shen, C. (2021). Adaptive intrusion detection system using machine learning techniques. Computers & Security, 104, 102142. Retrieved from https://doi.org/10.1016/j.cose.2020.102142