# ABSTRACT

**Stefanus Pratama Adhi Prabowo (01679230004)**

**DEVELOPMENT OF AN ALPHA MINER-BASED ANOMALY DETECTION MODEL ON IOT SECURITY SYSTEM**
(xiii + 50 pages; 7 pictures; 4 tables; 2 attachments)

IoT devices are increasingly being integrated into modern security infrastructures, creating an urgent need for robust systems capable of identifying and preventing unauthorized access. However, the dynamic and complex nature of IoT ecosystems, with the continuous introduction of new devices and behaviors, presents significant challenges for traditional anomaly detection methods. This research aims to address these challenges by adapting the Alpha Miner algorithm, initially used in process mining, to identify suspicious behavioral patterns within IoT log data. By focusing on improving the detection of abnormal access patterns, this study seeks to strengthen IoT-based security systems and address critical vulnerabilities in current security protocols.

This study uses an experimental methodology that includes designing, implementing, and testing an anomaly detection model on log data from IoT system. The Alpha Miner algorithm is applied to extract process models from these logs and identify deviations that signal potential threats. Furthermore, the research explores the integration of the proposed model into existing security systems, ensuring smooth operation and adaptability to the dynamic IoT environment.

The research findings demonstrate that the anomaly detection model based on the Alpha Miner algorithm significantly enhances the accuracy of threat detection in IoT-based door security systems. By analyzing 141,616 log entries, the model successfully distinguishes between normal and anomalous patterns, including activities such as normal punch open (84.01%), access denied (1.56%), and person not registered (0.31%). The false positive rate was reduced to 0.77%, while anomalies such as unauthorized access were identified in 0.09% and blank logs in 0.094% of the total recorded activities.

Log data visualization generate a process model encompassing 10 main categories, facilitating the identification of risk patterns. Further analysis revealed that 56.03% of initiated activities were classified as access denied, highlighting the significant number of unauthorized access attempts successfully detected. Additionally, recurring patterns such as punch interval too short (0.77%) were identified. These contributions illustrate the model's significant advancements in detecting and preventing threats in IoT systems, while also providing a solid foundation for the development of more effective and adaptive security protocols in the future.

**Keywords** **:** Anomaly detection; Alpha Miner algorithm; Door security systems; IoT security; Log data analysis.
**References** : 41 (2003 - 2024)

# ABSTRAK

**Stefanus Pratama Adhi Prabowo (01679230004)**

**PENGEMBANGAN MODEL DETEKSI ANOMALI BERBASIS *ALPHA MINER* PADA *IOT* UNTUK SISTEM KEAMANAN PINTU**
(xiii + 50 halaman; 7 gambar; 4 tabel; 2 lampiran)

Perangkat *IoT* semakin banyak diintegrasikan ke dalam infrastruktur keamanan modern, menciptakan kebutuhan mendesak untuk sistem yang kuat dalam mengidentifikasi dan mencegah akses yang tidak sah. Namun, sifat ekosistem *IoT* yang dinamis dan kompleks, dengan diperkenalkannya perangkat dan perilaku baru secara terus-menerus, menghadirkan tantangan signifikan bagi metode deteksi anomali tradisional. Penelitian ini bertujuan untuk mengatasi tantangan tersebut dengan mengadaptasi algoritma *Alpha Miner*, yang awalnya digunakan dalam *process mining*, untuk mengidentifikasi pola perilaku mencurigakan dalam data log *IoT*. Dengan berfokus pada peningkatan deteksi pola akses abnormal, penelitian ini bertujuan untuk memperkuat sistem keamanan berbasis *IoT* dan mengatasi kerentanan kritis dalam protokol keamanan saat ini.

Penelitian ini menggunakan metodologi eksperimental yang mencakup desain, implementasi, dan pengujian model deteksi anomali pada data log dari sistem *IoT*. Algoritma *Alpha Miner* diterapkan untuk mengekstrak model proses dari log ini dan mengidentifikasi penyimpangan yang mengindikasikan potensi ancaman. Selain itu, penelitian ini mengeksplorasi integrasi model yang diusulkan ke dalam sistem keamanan yang sudah ada, memastikan operasi yang mulus dan adaptabilitas terhadap lingkungan *IoT* yang dinamis.

Hasil penelitian menunjukkan bahwa model deteksi anomali berbasis algoritma *Alpha Miner* secara signifikan meningkatkan akurasi deteksi ancaman pada sistem keamanan pintu berbasis IoT. Dengan menganalisis 141.616 entri log, model berhasil membedakan antara pola normal dan anomali, termasuk aktivitas seperti *normal punch open* (84,01%), *access denied* (1,56%), dan *person not registered* (0,31%). Tingkat *false positive* berkurang menjadi 0,77%, sementara anomali seperti *unauthorized access* teridentifikasi pada 0,09% dan log kosong sebanyak 0,094% dari total aktivitas yang tercatat.

Visualisasi data log menghasilkan model proses yang mencakup 10 kategori utama, yang memfasilitasi identifikasi pola risiko. Analisis lebih lanjut mengungkapkan bahwa 56,03% aktivitas yang dimulai diklasifikasikan sebagai *access denied*, menunjukkan jumlah upaya akses tidak sah yang signifikan yang berhasil terdeteksi. Selain itu, pola berulang seperti *punch interval too short* (0,77%) teridentifikasi. Kontribusi ini menggambarkan kemajuan signifikan dari model ini dalam mendeteksi dan mencegah ancaman pada sistem *IoT*, sekaligus memberikan dasar yang kuat untuk pengembangan protokol keamanan yang lebih efektif dan adaptif di masa depan.

**Kata Kunci** **:** Deteksi anomali; algoritma *Alpha Miner*; sistem keamanan pintu; keamanan *IoT*; analisis data log.
**Referensi** **:** 41 (2003 - 2024)