# BAB I
# PENDAHULUAN

## 1.1 Latar Belakang

Dalam era *Internet of Things (IoT)*, penggunaan perangkat pintar semakin meluas, termasuk dalam konteks sistem keamanan pintu. Implementasi *IoT* pada keamanan pintu memungkinkan integrasi perangkat keras pintu dengan jaringan internet, sehingga memungkinkan kontrol jarak jauh dan kemampuan pemantauan yang lebih baik. Namun, keamanan tetap menjadi perhatian utama dalam pengembangan sistem ini. Ancaman keamanan, seperti akses tidak sah, merupakan risiko yang harus diatasi. Oleh karena itu, pengembangan model deteksi anomali yang efektif untuk mengidentifikasi perilaku tidak biasa atau mencurigakan dalam sistem keamanan pintu berbasis IoT menjadi sangat penting [1].

Meskipun beberapa upaya telah dilakukan dalam mengembangkan model deteksi anomali untuk sistem IoT seperti yang dikatakan oleh Cook A, Misirli G, Fan Z dalam jurnal dalam jurnal Anomaly Detection for IoT Time-Series Data: A Survey *IEEE Internet of Things Journal (2020) "Bahwa keterbatasan metode deteksi anomali berbasis data log IoT, termasuk pemodelan yang tidak memadai untuk pola time series. Hal ini menyebabkan kelemahan dalam mendeteksi aktivitas abnormal yang kompleks" [2]*. Model yang saat ini digunakan cenderung mengabaikan struktur proses dasar dari data log yang dihasilkan oleh perangkat IoT, seperti pergerakan pengguna atau akses pintu yang tidak sah. Dikutip dari jurnal milik DeMedeiros K, Hendawi A, Alvarez M yang berjudul *A Survey of AI-Based Anomaly Detection in IoT and Sensor Networks, Sensors (2023) 23(3) 1352,* dikatakan bahwa "*tantangan dalam deteksi anomali IoT, termasuk kekurangan dalam pendekatan berbasis pembelajaran mesin terhadap representasi grafis dari data log. Masalah utama adalah ketidakmampuan model untuk menangkap pola kontekstual, yang dapat meningkatkan false positive"[3]*. Kurangnya pemodelan proses ini dapat mengurangi akurasi deteksi dan meningkatkan tingkat *false positive*. Selain itu, model-model ini mungkin belum sepenuhnya

memanfaatkan algoritma yang efisien dan terbukti untuk pengenalan pola dalam data *time series*, dimana data tersebut penting untuk mendeteksi anomali dalam data log dari sistem keamanan pintu berbasis *IoT* [4], [5].

Pendekatan yang diusulkan dalam studi ini menggunakan algoritma *Alpha Miner* seperti yang ditulis oleh Yapakçı B, Akdağcık Z, Ergenç A dalam jurnal *Application of Process Mining to Production Lines Using Industrial Internet of Things*, bahwa "*proses mining menggunakan data dari IoT untuk menganalisis proses industri, termasuk penerapan algoritma Alpha Miner sebagai salah satu metode untuk menghasilkan model proses dari log kejadian. Studi ini menunjukkan bagaimana pendekatan ini dapat meningkatkan pemahaman terhadap proses bisnis berbasis IoT"[6]*. Hal ini beguna untuk mengekstraksi model proses dari data log yang dihasilkan oleh perangkat *IoT*. Dengan memanfaatkan informasi struktur proses yang diidentifikasi oleh *Alpha Miner*, dapat dikembangkan model deteksi anomali yang lebih akurat dan efisien. Hal ini akan memungkinkan deteksi anomali berdasarkan pola pergerakan pengguna atau akses tidak sah dengan tingkat *false positive* yang lebih rendah [7].

Pengembangan model deteksi anomali berbasis *Alpha Miner* ini diharapkan dapat memberikan kontribusi dalam meningkatkan keamanan sistem pintu berbasis *IoT* yaitu dengan mendeteksi pola yang tidak biasa/anomali. Dengan kemampuan untuk mendeteksi anomali dengan akurasi lebih tinggi dan *false positive* yang lebih rendah, model ini akan membantu mengurangi risiko keamanan yang terkait dengan akses tidak sah pada sistem pintu berbasis *IoT* [8]. Selain itu, pendekatan yang diusulkan ini dapat memberikan wawasan baru seperti pemahaman tentang pola aktivitas IoT dan peningkatan deteksi anomali dengan model berbasis proses, sehingga menjadi dasar untuk penelitian lebih lanjut dalam pengembangan teknik deteksi anomali yang lebih maju [9].

Keamanan dalam sistem *IoT* rentan terhadap anomali karena beberapa alasan utama. Seperti yang ditulis oleh Sahu S, Mazumdar K dalam jurnal *Exploring security threats and solutions Techniques for Internet of Things (IoT): from vulnerabilities to vigilance* bahwa *"Serangan kontrol akses:*

*Kontrol akses adalah metode otentikasi penting bagi pengguna untuk mengakses informasi akun. Jika kontrol akses dikompromikan, penyerang dapat menguasai seluruh aplikasi IoT, menimbulkan ancaman signifikan terhadap keamanan" [10]*. Selain itu, seiring bertambahnya jumlah perangkat, kompleksitas jaringan juga meningkat, sehingga pemantauan dan deteksi anomali menjadi lebih sulit akibat keberagaman dan aliran data real-time yang terus-menerus dihasilkan. Banyak perangkat IoT juga dirancang tanpa fitur keamanan yang kuat, sering kali dibatasi oleh daya dan kapasitas komputasi, yang dapat membuat mekanisme enkripsi dan keamanan menjadi kurang efektif serta meningkatkan risiko akses tidak sah. Selain itu, data log yang dihasilkan oleh perangkat *IoT* sering kali tidak terstruktur dibandingkan dengan data sistem tradisional yang terstruktur homogen dan volume yang lebih kecil, yang membuat deteksi pola mencurigakan menjadi lebih rumit dan sistem menjadi rentan terhadap aktivitas abnormal [11].

Di sinilah process mining menjadi penting untuk menganalisis anomali tersebut, karena pendekatan ini memungkinkan pemodelan pola dari data log yang ada. Dengan menggunakan algoritma seperti *Alpha Miner*, *process mining* dapat meningkatkan akurasi deteksi anomali melalui pemodelan struktur proses dan memahami pola aktivitas normal dalam sistem, sehingga hanya aktivitas yang benar-benar menyimpang yang dianggap sebagai ancaman keamanan. Pemahaman tentang pola ini juga membantu mengurangi *false positive* atau deteksi anomali yang salah, karena process mining memeriksa konteks dan alur proses di balik data, bukan hanya informasi permukaan. Selain itu, process mining dapat disesuaikan dengan data real-time, memungkinkan deteksi anomali secara langsung saat terjadi—fitur yang sangat penting dalam sistem *IoT* dengan aktivitas tinggi. Dalam konteks keamanan *IoT, process mining* membantu mengidentifikasi dan memahami pola anomali yang terkait dengan aktivitas pengguna atau akses tidak sah, sehingga mendukung pengembangan sistem keamanan yang lebih kuat dan responsif [12].

Penelitian ini memberikan kontribusi dengan mengembangkan model deteksi anomali yang berbasis pada algoritma Alpha Miner untuk sistem

keamanan IoT. Model ini dirancang untuk mengekstraksi pola proses dari data log IoT, sehingga dapat mendeteksi perilaku anomali dengan lebih akurat, mengurangi tingkat *false positive*, dan menangani kompleksitas data log IoT yang terus meningkat. Adapun Manfaat dari kontribusi ini antara lain:

1. **Meningkatkan keamanan *IoT*:** Membantu dalam mengidentifikasi dan mencegah akses tidak sah atau aktivitas mencurigakan pada perangkat *IoT*.
2. **Meningkatkan efisiensi deteksi:** Dengan menggunakan model berbasis proses, sistem dapat mengenali anomali dalam konteks perilaku normal perangkat, sehingga mengurangi risiko serangan yang tidak terdeteksi.
3. **Memberikan dasar untuk penelitian lanjutan:** Menyediakan kerangka kerja bagi pengembangan algoritma deteksi yang lebih kompleks atau penggabungan teknologi keamanan lain seperti blockchain dan *machine learning*.
4. **Mendukung pengelolaan log yang efisien:** Mengurangi beban analisis log manual dalam lingkungan IoT dengan jumlah data yang besar.

Kami mengerjakan penelitian ini dengan menggunakan algoritma *Alpha Miner* untuk mengekstraksi model proses dari data log *IoT* yang dihasilkan oleh berbagai perangkat. Eksperimen dilakukan pada data log simulasi dan data log nyata untuk menguji kemampuan model dalam mendeteksi anomali.

## 1.2 Identifikasi Permasalahan

Identifikasi masalah pada penelitian ini adalah:

a. Struktur data log *IoT* yang terdiri dari beberapa atribut menjadi tantangan dalam mendeteksi anomali pada sistem keamanan pintu.
b. Integrasi *Alpha Miner* dengan konteks *IoT* dan keamanan pintu merupakan tantangan utama.
c. Terbatasnya analisis *IoT* menggunakan *Process Mining* menyulitkan pengembangan model deteksi anomali pada sistem keamanan *IoT*.

## 1.3 Batasan Masalah

Batasan pada penelitian ini:

a. Penelitian ini akan memusatkan perhatian pada pola aktivitas keamanan pintu yang terdapat dilokasi Universitas Pelita Harapan Lippo Village yang dihasilkan oleh perangkat IoT.
b. Penelitian ini akan membatasi penggunaan algoritma *Alpha Miner* sebagai basis untuk mengembangkan model pencarian anomali. Algoritma ini akan digunakan untuk mengekstraksi model proses dari data log yang dihasilkan oleh perangkat *IoT*. anomali dengan lebih baik dalam konteks keamanan pintu berbasis IoT.
c. Penelitian ini akan membatasi integrasi model pencarian anomali dengan infrastruktur keamanan *IoT* yang sudah ada. Model yang dikembangkan dapat diimplementasikan dalam lingkungan keamanan pintu berbasis *IoT* yang sudah ada tanpa memerlukan perubahan besar pada infrastruktur atau arsitektur yang ada.
d. Penelitian ini akan dilakukan menggunakan dataset yang representatif dan melalui eksperimen untuk memvalidasi kinerja model dalam mendeteksi anomali dengan efektif.

## 1.4 Rumusan Masalah

1. Apakah pendekatan process mining dapat dipergunakan untuk mencari anomali dalam sistem keamanan pintu berbasis *IoT*?
2. Apakah algoritma *Apha Miner* dapat digunakan dalam mencari anomali dalam sistem keamanan pintu berbasis *IoT*?
3. Fitur dari log data apa saja yang mempengaruhi pada pencarian anomali dalam sistem keamanan pintu berbasis *IoT*?
4. Bagaimana mengintegrasikan data log dari perangkat *IoT* ke dalam algoritma *Alpha Miner* untuk mengekstraksi model proses yang mewakili perilaku pengguna dan operasional pintu secara efektif?
5. Apa jenis anomali yang dapat terjadi dalam sistem keamanan pintu *IoT* dan bagaimana cara mendeteksinya menggunakan informasi struktur proses yang ditemukan oleh *Alpha Miner*?

## 1.5 Tujuan Penelitian

Tujuan penelitian ini adalah untuk mengembangkan sebuah model pencarian anomali yang efektif dan adaptif berbasis *Alpha Miner* dalam konteks sistem keamanan pintu berbasis *IoT*. Penelitian ini bertujuan untuk menyelidiki bagaimana *Alpha Miner* dapat digunakan untuk mengekstraksi pola perilaku yang mencurigakan dari data log yang dihasilkan oleh perangkat *IoT*, serta bagaimana model tersebut dapat diintegrasikan ke dalam infrastruktur keamanan yang sudah ada. Tujuan utama adalah untuk meningkatkan deteksi ancaman dan respons terhadap akses yang tidak valid pada sistem keamanan pintu *IoT*. Dengan demikian, penelitian ini diharapkan dapat memberikan kontribusi dalam meningkatkan keamanan sistem pintu *IoT* dengan menghadirkan sebuah model deteksi anomali yang efektif.

## 1.6 Sistematika Penulisan

Penulisan dalam penelitian ini terbagi menjadi sedikitnya dalam lima bab, dimana setiap bab mempunyai bahasan mengenai tujuan dan isi yang berbeda-beda. Adapun sistematikanya sebagai berikut:

Bab I Pendahuluan. Bab ini membahas tentang gambaran secara singkat mengenai latar belakang masalah mengapa penelitian ini dilakukan sampai pada tujuan penelitian

Bab II Kajian Teori. Bab ini membahas tentang teori-teori yang akan digunakan atau penelitian yang sudah dilakukan terkait dengan rumusan permasalahan yang dibicarakan pada Bab 1. Bagian ini merupakan bagian kunci untuk menentukan metoda yang akan dipakai pada bagian selanjutnya.

Bab III Metodologi Penelitian. Bab ini berisi tentang rancangan penelitian dan atau rancangan pengujian

Bab IV Hasil dan Pembahasan. Menguraikan hasil dari penelitian yang telah dilakukan dan melakukan argumentasi atas apa yang dihasilkan dengan melampirkan *paper* atau karya ilmiah yang sudah atau akan dipublikasi.

Bab V Kesimpulan dan Saran. Pada bab ini menjelaskan tentang kesimpulan berdasarkan hasil dari penelitian yang diperoleh, serta saran-saran konstruktif yang perlu dikembangkan untuk penelitian berikutnya sehingga penelitian berikutnya menjadi lebih baik.

Di bagian akhir dari penulisan ini dilampirkan daftar Pustaka, lampiran-lampiran serta daftar riwayat hidup peneliti.