# BAB I

# PENDAHULUAN

## 1.1 Latar Belakang

Ruang server merupakan fasilitas penting sebagai pusat pengelolaan informasi, penyimpanan dan distribusi data dalam suatu organisasi. Ruang ini berfungsi sebagai penyimpanan perangkat keras seperti server, *router*, *switch* dan perangkat jaringan lainnya yang mendukung operasi teknologi informasi. Karena sifat yang sangat krusial, ruang server harus memiliki sistem yang ketat untuk melindungi data dari berbagai ancaman. Menurut (Junaid, 2023) ruang server harus memiliki pengamanan fisik dan non-fisik, di mana sistem keamanan yang ideal mencakup pengaturan akses keluar dan masuk pengguna ke ruang server serta manajemen keamanan pada sistem yang berjalan di server. Keamanan ruang server juga mempengaruhi berlangsungnya layanan yang diberikan oleh instansi kepada pengguna, termasuk layanan berbasis teknologi yang bergantung dengan data yang tersimpan. Dengan demikian, pengelolaan ruang server tidak hanya melibatkan aspek teknis, tetapi juga memerlukan strategi pengamanan fisik yang memadai.

Ancaman yang diartikan ini yaitu kondisi yang berpotensi menyebabkan kehilangan ataupun kerusakan pada aset (Sugianto et al., 2020). Hal ini timbul akibat adanya penyalahgunaan kredensial akses atau melalui tindak pembobolan yang dilakukan oleh pihak yang tidak berwenang untuk masuk ke area khusus. Kondisi ini menjadi celah keamanan yang berpotensi untuk melakukan perusakan atau pencurian perangkat, maupun akses ilegal terhadap sistem. Kehilangan perangkat tidak hanya menimbulkan kerugian material, tetapi juga dapat berpotensi

sebagai penyebab 25% *downtime* dalam pengolahan informasi global, yang berdampak ke citra instansi, ketidakpuasan pelanggan, dan mempengaruhi pendapatan (Bakri et al., 2022). Perangkat keras yang dicuri, seperti server, *router*, *switch* atau modul jaringan sering kali memiliki peran krusial dalam menjaga kelangsungan operasional sistem. Contoh nyata dari ancaman ini adalah kasus pencurian perangkat di *data center* PT XL Axiata di Makassar pada April 2024, di mana perangkat penting yaitu *Quad Small Formfactor Pluggable* (QSFP ) sebanyak 36 unit dicuri oleh oknum yang menyalahgunakan akses kerjanya (Novianty, 2024). Kasus ini menyebabkan terganggunya layanan *data center* perusahaan, termasuk layanan yang diberikan kepada pelanggan, dan menimbulkan kerugian finansial yang signifikan bagi perusahaan. Selain itu, kasus semacam ini juga berdampak pada hilangnya kepercayaan pelanggan terhadap keamanan dan keandalan layanan yang ditawarkan oleh perusahaan.

Sejalan dengan pentingnya perlindungan ruang server, Universitas Pendidikan Ganesha (Undiksha) melalui Unit Penunjang Akademik Teknologi Informasi dan Komunikasi (UPA TIK) yang bertanggung jawab atas pengembangan, pengelolaan, dan pelayanan teknologi informasi dan komunikasi serta pengelolaan sistem informasi dan jaringan. Sebagai unit yang mendukung aktivitas akademik dan operasional universitas, UPA TIK memiliki infrastruktur server yang berfungsi untuk menyimpan dan mengelola data penting Universitas (Mandiasa et al., 2026). Layanan ini mencakup sistem informasi akademik, layanan kepegawaian, akses internet, hingga platform berbasis teknologi lain yang digunakan oleh sivitas akademik Undiksha. Oleh karena itu, keamanan ruang server menjadi prioritas

utama untuk memastikan layanan tetap berjalan dengan optimal dan aman dari gangguan untuk keberlangsungan akademik di Undiksha.

Saat ini, ruang server di UPA TIK Undiksha telah dilengkapi dengan sistem pengamanan dasar berupa *smart lock system* dan kamera pengawas (CCTV) komersial yang siap pakai. Kedua perangkat ini berfungsi sebagai alat pengamanan dan pengawasan fisik awal terhadap akses. Meskipun demikian, sistem yang digunakan masih memiliki keterbatasan dalam hal fungsionalitas. Namun, sistem penguncian yang digunakan masih cenderung mengandalkan mekanisme autentikasi satu faktor, sehingga berisiko apabila kredensial atau perangkat akses tersebut disalahgunakan. Selain itu, sistem yang ada belum mendukung monitoring akses secara *real-time*, tidak menyediakan notifikasi otomatis kepada pengelola ketika melakukan akses ke ruangan, serta belum memiliki kemampuan mendeteksi upaya akses ilegal, misalnya kondisi pintu terbuka tanpa prosedur autentikasi. Kondisi ini menimbulkan celah keamanan yang bisa dimanfaatkan oleh pihak tidak bertanggung jawab. Oleh karena itu, diperlukan sistem pengamanan yang lebih adaptif dan terintegrasi dalam mendeteksi dan menangani risiko keamanan, terutama yang berkaitan dengan akses ilegal ke ruang server.

Fenomena tersebut menunjukkan bahwa sistem keamanan yang digunakan saat ini masih belum mampu menjawab kebutuhan perlindungan yang menyeluruh terhadap ruang server. Sistem penguncian yang sudah digunakan tidak lagi memadai untuk menghadapi ancaman tindak akses ilegal yang semakin kompleks. Oleh karena itu, instansi perlu mengadopsi sistem keamanan modern yang lebih canggih dan terintegrasi dengan teknologi untuk melindungi ruang server dari risiko serupa. Langkah-langkah inovatif berbasis teknologi menjadi kunci untuk menjaga

keamanan perangkat keras, data, dan keberlangsungan operasional organisasi. Dengan itu contoh teknologi yang mutakhir saat ini yaitu sistem IoT (Saraya et al., 2022).

Berkaitan dengan hal tersebut, penelitian ini bertujuan untuk merancang dan membangun sistem penguncian pintar berbasis IoT untuk meningkatkan keamanan akses ruang server UPA TIK Undiksha. Sistem ini mengintegrasikan teknologi RFID dan sensor sidik jari (*fingerprint*) serta kamera pengenalan wajah *(face recognition)* sebagai mekanisme autentikasi dua faktor, sehingga hanya pengguna yang terdaftar yang dapat membuka dan mengakses ruang server. Selain itu, sistem ini akan dilengkapi dengan fitur pemantauan dan notifikasi otomatis melalui platform Telegram, yang memungkinkan pengelola menerima peringatan saat terjadi akses tidak sah. Proses ini menghubungkan setiap objek melalui jaringan internet dengan menerapkan protokol komunikasi ringan, yaitu protokol MQTT (Aryanto et al., 2020). Sistem ini diharapkan dapat memberikan solusi yang lebih efektif dan efisien dalam menjaga keamanan ruang server, sekaligus mempermudah pengelolaan akses dan pemantauan secara *real-time*. Dengan adanya sistem ini, pengelola dapat mengurangi risiko pencurian perangkat keras dan penyalahgunaan akses, serta memberikan perlindungan yang lebih baik terhadap perangkat vital di ruang server. Keamanan yang terjaga dengan baik juga akan mendukung kelancaran operasional layanan teknologi informasi di Undiksha, sehingga dapat terus memberikan layanan yang andal dan aman kepada sivitas akademika. Diharapkan, penelitian ini menjadi langkah penting bagi Undiksha untuk mengadopsi teknologi terkini dalam mengoptimalkan keamanan ruangan khususnya pada layanan-layanan penting.

## 1.2 Identifikasi Masalah

Berdasarkan latar belakang yang telah dijelaskan, beberapa masalah muncul dalam mengoptimalkan keamanan akses pada ruang server. Oleh karena itu, diperlukan identifikasi terhadap berbagai masalah yang muncul, antara lain sebagai berikut:

1. Ancaman penyalahgunaan akses terhadap tindak pencurian atau perusakan perangkat keras yang dapat mengganggu operasional dan layanan yang disediakan.
2. Belum adanya sistem peringatan akses untuk mendeteksi adanya upaya tindak akses ilegal, seperti penyalahgunaan akses bahkan pembobolan.
3. Sistem penguncian saat ini belum mendukung pemantauan aktivitas akses secara rinci sebagai evaluasi keamanan serta mewaspadai potensi pelanggaran akses.

## 1.3 Batasan Masalah

Adapun batasan masalah dalam penelitian ini difokuskan pada aspek-aspek berikut untuk memperjelas ruang lingkup penelitian, antara lain:

1. Penelitian difokuskan pada pengembangan dan implementasi sistem keamanan akses ruang server yang ada di gedung UPA TIK Undiksha.
2. Sistem ini hanya dapat memantau akses masuk yang berhasil, akses yang ditolak, serta kondisi pintu terbuka tanpa autentikasi resmi sebagai indikator akses.
3. Respons sistem terhadap akses ilegal dibatasi pada alarm *buzzer*/indikator dan pengiriman notifikasi.

4. Fitur administrasi pengguna dan media monitoring serta pengiriman notifikasi dilakukan menggunakan Bot Telegram.
5. Sistem belum mampu mencegah penyalahgunaan akses menggunakan identitas autentikasi milik orang lain dengan foto wajah pengguna yang terdaftar.
6. Kegagalan sistem akibat gangguan internet dan pemadaman listrik dikategorikan sebagai faktor eksternal di luar ruang lingkup penelitian.

## 1.4 Rumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan, adapun beberapa rumusan masalah yang ditemukan dalam penelitian ini adalah sebagai berikut:

1. Bagaimana perancangan *smart lock security system* berbasis IoT dengan autentikasi dua faktor sebagai keamanan akses pada ruang server?
2. Bagaimana mengintegrasikan *smart lock security system* berbasis IoT untuk pemantauan dan kontrol akses ruang server secara *real-time* melalui platform Telegram?
3. Bagaimana performa *smart lock security system* berbasis IoT dalam mengamankan akses ruang server?

## 1.5 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah disusun, maka tujuan penelitian ini dilakukan untuk mencapai hasil yang sesuai dengan permasalahan yang diteliti. Adapun tujuan dari penelitian ini adalah:

1. Merancang dan membangun *smart lock security system* berbasis IoT dengan menggunakan mekanisme autentikasi dua faktor sebagai keamanan akses pada ruang server.

2. Mengintegrasikan sistem dengan broker MQTT, *Firebase*, dan Telegram untuk monitoring, notifikasi, serta pencatatan log akses secara *real-time*.
3. Mengevaluasi sistem dalam mengamankan akses ruang server berdasarkan *Black Box Testing*, *Performance Testing*, dan *Usability Testing*.

## 1.6 Manfaat Penelitian

Berikut merupakan manfaat yang diharapkan dari penelitian ini antara lain adalah:

1. Bagi UPA TIK Undiksha, sistem yang dikembangkan dapat meningkatkan keamanan akses ruang server melalui autentikasi dua faktor, serta sistem yang dapat dipantau secara *real-time*.
2. Bagi akademis, penelitian ini dapat memberikan kontribusi dalam implementasi sistem berbasis IoT sebagai kontrol akses fisik ruang server.
3. Bagi penulis, penelitian ini meningkatkan wawasan dan pengalaman dalam perancangan dan implementasi sistem berbasis IoT, integrasi komunikasi perangkat yang telah dipelajari selama perkuliahan.