

BAB I

PENDAHULUAN

1.1 Latar Belakang

Teknologi yang semakin canggih telah menjadi bagian tak terpisahkan dari kehidupan manusia, memberikan kemudahan dan solusi inovatif di berbagai aspek kehidupan. Dari kecerdasan buatan (AI) yang mampu memproses data dalam jumlah besar hingga *Internet of Things* (IoT) yang menghubungkan perangkat secara global, teknologi terus berkembang dengan pesat. Keberadaan teknologi ini tidak hanya meningkatkan efisiensi kerja, tetapi juga membuka peluang baru dalam bidang pendidikan, transportasi, dan keamanan. Contohnya, penggunaan sensor pintar dan aplikasi berbasis IoT dalam sistem keamanan telah memungkinkan pemantauan *real-time* dan pengelolaan risiko yang lebih baik. Kemajuan dalam bidang komunikasi digital memungkinkan akses informasi yang cepat dan penyebaran data secara global dalam hitungan detik. Namun, di balik kemudahan yang ditawarkan, perkembangan teknologi juga menghadirkan tantangan, seperti ancaman keamanan *cyber* dan kebutuhan akan infrastruktur yang memadai. Oleh karena itu, pemanfaatan teknologi canggih perlu diimbangi dengan kebijakan yang bijak dan pengelolaan yang berkelanjutan untuk memastikan manfaatnya dapat dirasakan oleh semua kalangan. (Sucipto et al. 2024)

Robotik adalah cabang ilmu dan teknologi yang berfokus pada perancangan, pembuatan, pengoperasian, dan penggunaan robot untuk menggantikan atau membantu tugas manusia. Dalam perkembangannya, robotik telah menjadi elemen penting dalam berbagai sektor, seperti industri manufaktur, kesehatan, militer, dan bahkan kehidupan sehari-hari. Robot yang dirancang dengan teknologi canggih

mampu melakukan pekerjaan yang membutuhkan presisi tinggi, seperti merakit komponen elektronik, melakukan operasi medis, atau menjelajahi lingkungan berbahaya yang sulit diakses oleh manusia. Selain itu, integrasi kecerdasan buatan (AI) dan *Internet of Things* (IoT) telah meningkatkan kemampuan robot untuk beradaptasi, belajar dari lingkungan, dan berkomunikasi dengan sistem lain. Dengan manfaat yang luas, robotik terus menjadi solusi inovatif yang mendukung efisiensi, produktivitas, dan keamanan dalam berbagai bidang. (Ipanhar, Wijaya, dan Gunoto 2022)

Sistem keamanan merupakan serangkaian teknologi, perangkat, dan prosedur yang dirancang untuk melindungi aset, data, serta individu dari berbagai ancaman, baik fisik maupun digital. Dalam era modern, sistem keamanan telah berkembang pesat dengan memanfaatkan teknologi canggih seperti kamera pengawas (CCTV), sensor gerak, alarm, hingga perangkat berbasis *Internet of Things* (IoT) yang memungkinkan pemantauan dan pengelolaan secara real-time. Selain itu, perangkat lunak keamanan seperti *firewall*, antivirus, dan sistem enkripsi juga memainkan peran penting dalam melindungi informasi digital dari ancaman *cyber*. Sistem keamanan tidak hanya diterapkan pada skala kecil seperti rumah atau kantor, tetapi juga pada infrastruktur besar seperti pusat data, bank, dan fasilitas publik lainnya. (Sopandi Bara dan Dewi Hendrawati 2023)

Penggunaan aplikasi mobile untuk notifikasi, integrasi dengan kecerdasan buatan (AI) untuk analisis ancaman, serta kemampuan otomatisasi semakin memperkuat efektivitas sistem keamanan modern. Namun, meski teknologi terus berkembang, penerapan sistem keamanan yang optimal tetap membutuhkan perencanaan yang matang, pemeliharaan berkala, serta kesadaran pengguna

terhadap potensi risiko dan ancaman yang terus berubah. Kombinasi antara teknologi mutakhir dan pendekatan strategis dalam sistem keamanan mampu menciptakan lingkungan yang lebih aman dan terlindungi dari berbagai ancaman yang ada.(Kurniawa 2023.)

Kantor yang tidak memiliki sistem keamanan cenderung rentan terhadap berbagai risiko, baik dari ancaman fisik seperti pencurian, vandalisme, dan akses tidak sah, maupun ancaman non-fisik seperti kebocoran informasi penting. Tanpa sistem keamanan yang memadai, pengawasan terhadap aset-aset perusahaan menjadi sulit, dan deteksi dini terhadap kejadian mencurigakan tidak dapat dilakukan . Kondisi ini tidak hanya membahayakan barang-barang berharga, tetapi juga dapat mengancam keselamatan karyawan yang bekerja di dalamnya. Selain itu, ketidakadaan sistem keamanan juga dapat menurunkan kepercayaan karyawan dan mitra bisnis terhadap kemampuan kantor dalam menjaga kenyamanan dan privasi. Oleh karena itu, kantor yang tidak memiliki sistem keamanan berisiko mengalami kerugian finansial maupun reputasi yang sulit untuk dipulihkan.(Nizam, Haris Yuana, dan Zunita Wulansari 2022)

Setiap kantor memerlukan sistem keamanan yang andal untuk melindungi aset, data, dan privasi perusahaan, terutama pada akses penting seperti pintu masuk utama. Dengan tingkat ancaman yang semakin kompleks, penerapan sistem keamanan berbasis teknologi menjadi langkah yang krusial untuk memastikan bahwa hanya individu yang berwenang yang dapat mengakses area tertentu . Sistem keamanan yang terintegrasi pada pintu kantor, seperti penggunaan kartu akses, fingerprint, atau kode PIN, dapat memberikan kontrol lebih ketat dan meminimalkan risiko akses tidak sah. Selain itu, teknologi modern seperti

pengenalan wajah dan pemantauan real-time melalui aplikasi berbasis *Internet of Things* (IoT) semakin meningkatkan efisiensi dalam mengawasi aktivitas di area tersebut. Penerapan sistem ini juga dapat memberikan rasa aman bagi karyawan, menciptakan lingkungan kerja yang lebih produktif, dan meningkatkan kepercayaan mitra bisnis terhadap integritas operasional kantor. Dengan adanya batasan akses yang jelas, kantor dapat menjaga kerahasiaan informasi penting sekaligus memitigasi potensi kerugian yang dapat terjadi akibat kelalaian atau ancaman eksternal. (Kurniawan 2023)

Penulis ingin melakukan sebuah penelitian tentang implementasi Internet of Things (IoT) untuk meningkatkan sistem keamanan kantor berbasis mikrokontroler ESP32 dan aplikasi Telegram. Penelitian ini merancang dan mengembangkan sebuah sistem keamanan yang lebih canggih dan efisien dalam memantau serta mengendalikan akses pada kantor, khususnya di area pintu utama. Dengan memanfaatkan kemampuan ESP32 yang memiliki fitur konektivitas Wi-Fi dan Bluetooth, sistem ini dirancang untuk terhubung dengan berbagai sensor keamanan seperti sensor gerak, sensor pintu, kamera, serta modul RFID untuk autentikasi akses. Notifikasi dan laporan keamanan akan dikirimkan secara real-time melalui aplikasi Telegram, memungkinkan pengelola kantor untuk segera mengetahui aktivitas mencurigakan atau potensi ancaman, kapan saja dan di mana saja. (Selokaton et al. 2025)

Keamanan sistem ini didukung mekanisme akses pintu berbasis PIN dan RFID, di mana hanya pengguna yang memiliki akses yang dapat membuka pintu kantor. Dengan sistem ini, potensi akses ilegal dapat diminimalkan karena setiap pengguna harus memasukkan PIN yang benar atau menggunakan kartu RFID yang

telah terdaftar sebelumnya. Selain itu, penelitian ini menggunakan metode *Research and Development (R&D)* dalam proses perancangannya, yang melibatkan tahap perancangan, pengujian, dan evaluasi untuk memastikan sistem berjalan dengan optimal. Implementasi ini juga bertujuan untuk mengatasi keterbatasan pada sistem keamanan tradisional yang sering kali kurang responsif dan sulit diintegrasikan dengan perangkat modern. Dengan pendekatan berbasis IoT dan teknologi autentikasi RFID, penelitian ini diharapkan mampu memberikan solusi yang inovatif dan praktis dalam meningkatkan keamanan kantor serta menawarkan fleksibilitas dan kemudahan dalam pengelolaannya. (Putra 2019)

1.2 Rumusan Masalah

Dari paparan penelitian diatas, terdapat beberapa rumusan masalah pada penelitian ini, yaitu sebagai berikut.

1. Bagaimana implementasi mikrokontroler ESP32 dapat diintegrasikan dengan sensor keamanan dan aplikasi Telegram untuk menciptakan sistem keamanan kantor berbasis IoT?
2. Bagaimana proses pengiriman notifikasi keamanan real-time melalui aplikasi Telegram dapat meningkatkan responsivitas dalam menangani potensi ancaman di kantor?
3. Bagaimana efektivitas sistem keamanan berbasis IoT ini dibandingkan dengan sistem keamanan tradisional dalam mencegah akses tidak sah di kantor?

1.3 Batasan Masalah

Batasan masalah dalam penelitian ini mencakup beberapa aspek yang akan difokuskan untuk memastikan keberhasilan implementasi sistem keamanan

berbasis IoT menggunakan mikrokontroler ESP32 dan aplikasi Telegram. Pertama, penelitian ini hanya akan membahas penggunaan mikrokontroler ESP32 sebagai pusat kendali utama sistem, yang akan terhubung dengan sensor-sensor keamanan melalui koneksi Wi-Fi atau Bluetooth untuk mendeteksi potensi ancaman di kantor. Kedua, penelitian ini akan terbatas pada pemanfaatan aplikasi Telegram sebagai platform komunikasi utama untuk menerima notifikasi dan laporan secara real-time, tanpa melibatkan aplikasi atau sistem komunikasi lainnya. Ketiga, ruang lingkup pengujian akan dilakukan pada kantor dengan skala kecil dan terbatas, sehingga sistem yang dikembangkan hanya akan diuji pada area pintu utama kantor yang memerlukan pengawasan ketat. Penelitian ini tidak akan mencakup pengujian sistem di lingkungan kantor besar atau kompleks yang mungkin memiliki tantangan tambahan dalam hal skalabilitas dan integrasi sistem.

1.4 Tujuan Penelitian

Manfaat Peneli Berdasarkan penelitian ini, terdapat beberapa tujuan yang ingin dicapai untuk meningkatkan sistem keamanan kantor berbasis IoT dengan mikrokontroler ESP32 dan aplikasi Telegram:

- 1 Untuk memahami bagaimana mikrokontroler ESP32 dapat diintegrasikan dengan berbagai sensor keamanan dan aplikasi Telegram, serta bagaimana sistem ini dapat mengoptimalkan pemantauan keamanan di kantor.
- 2 Untuk menganalisis bagaimana proses pengiriman notifikasi keamanan secara real-time melalui aplikasi Telegram dapat meningkatkan responsivitas pengelola kantor dalam menangani ancaman atau kejadian mencurigakan.
- 3 Untuk mengevaluasi efektivitas sistem keamanan berbasis IoT

dibandingkan dengan sistem keamanan tradisional dalam mencegah akses tidak sah dan meningkatkan pengawasan di kantor.

1.5 Manfaat Penelitian

Dengan tercapainya tujuan penelitian ini, beberapa manfaat yang diharapkan adalah:

1. Sistem keamanan yang dibangun dapat meningkatkan efisiensi dan keandalan dalam memantau akses dan kejadian di kantor, sehingga meningkatkan keselamatan dan keamanan aset.
2. Penggunaan aplikasi Telegram sebagai platform komunikasi untuk notifikasi memungkinkan pengelola untuk segera merespons ancaman dengan lebih cepat dan akurat, meskipun berada jauh dari lokasi kantor.
3. Implementasi teknologi IoT dalam sistem keamanan kantor akan memberikan solusi yang lebih fleksibel dan skalabel, yang dapat diadaptasi pada kantor dengan berbagai ukuran, serta mengurangi biaya dan kompleksitas sistem keamanan tradisional.

1.6 Sistematika Penulisan

Sistematika penulisan adalah urutan dan struktur yang digunakan dalam menyusun proposal artikel ini, yang mencakup bagian-bagian penting seperti berikut.

BAB I : PENDAHULUAN

Pada bab ini merupakan tahapan awal pengerjaan dalam penyusunan laporan proposal skripsi yang berisi tentang latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian dan sistematika penulisan.

BAB II : KAJIAN PUSTAKA

Pada bab ini berisi tentang teori ataupun kajian yang dibahas pada penelitian ini dan berhubungan dengan Penelitian ini. Seperti teori tentang Arduino uno, robotik, IoT dan komponen lain yang digunakan pada penelitian ini.

BAB III : METODOLOGI PENELITIAN

Pada bab ini berisi tentang Lokasi dan waktu penelitian, alat dan bahan penelitian, metode yang digunakan pada Penelitian ini, analisis sistem yang digunakan, kebutuhan sistem, desain flowchart, perancangan alat dan penerapan alat.

BAB IV : HASIL DAN PEMBAHASAN

Pada bab ini merupakan hasil dari penelitian yang sudah dilakukan, jadi pada bab ini berisi tentang alat yang sudah dibuat dan akan dijelaskan cara penerapan dan fungsi dari alat yang digunakan. Pada bab ini juga akan dipaparkan cara penggunaan dan sampai alat dapat bekerja dengan baik.

BAB V : KESIMPULAN DAN SARAN

Pada bab ini merupakan akhir dari penulisan skripsi, hal ini karena pada bab ini berisi kesimpulan yang merupakan inti dari penelitian yang sudah dilakukan dan berisi saran yang merupakan kritikan yang menjadi perbaikan pada penelitian ini.