"Jurnal TRANSFORMASI (Informasi & Pengembangan Iptek)" (STMIK BINA PATRIA)

E-ISSN : 2827-8550
P- ISSN : 1978-5569

SISTEM KEAMANAN BRANKAS DENGAN RFID DOOR LOCK BERBASIS INTERNET OF THINGS (IOT) MENGGUNAKAN CISCO PACKET TRACER

Amirah[1)], Prisilia Talakua[2)], Opitasari[3)], Fitria [4)]

[1)] *"Teknik Informatika" Universitas DIPA Makasar*
[2)] *" Sistem Informasi" Institut Agama Kristen Negeri Ambon*
[3)] *"Teknik Informatika" Universitas Indraprasta PGRI Jakarta*
[4)] *" Sistem dan Teknologi Informasi" Universitas Siber Indonesia*
Email : amirah01.am@gmail.com, hmlutfima@gmail.com, prisiliatalakua@gmail.com , opitasari@gmail.com , fitria@cyber-univ.ac.id

Abstract

The development of Internet of Things (IoT) technology has brought significant transformations in various fields, including security systems in securing valuable assets, such as safes, which require a high level of security. The purpose of this study is to design and implement a safe security system based on RFID and IoT, simulate the system using Cisco Packet Tracer to ensure its functionality and evaluate the effectiveness of the system in securing access to the safe. The system development model used is the ADDIE method which consists of five stages of development, namely; (1) Analysis, (2) Design, (3) Development, (4) Implementation and (5) Evaluation. Problem analysis uses analysis and Feasibility Analysis uses TELOS analysis. The results of the System reliability analysis on this system are Verification Accuracy is 100% accurate in distinguishing valid and invalid tags based on data, while Response Speed is the response time between RFID reading and the door opening an average of <1 second. The system continues to run well as long as the server is active and the device is connected to the network. This research is expected to provide an alternative solution for an affordable and virtually simulated safe security system, as a reference or initial prototype for the development of a larger scale IoT security system and to demonstrate the potential use of Cisco Packet Tracer in RFID and IoT-based security system simulations.

Keywords: *Safe, Internet of Things, Cisco Packet Tracer, SWOT, TELOS..*

Abstrak

Perkembangan teknologi Internet of Things (IoT) telah membawa transformasi signifikan dalam berbagai bidang, termasuk sistem keamanan dalam pengamanan aset berharga, seperti brankas, yang membutuhkan tingkat keamanan tinggi. Tujuan dari penelitian ini adalah merancang dan mengimplementasikan sistem keamanan brankas berbasis RFID dan IoT, mensimulasikan sistem menggunakan *Cisco Packet Tracer* untuk memastikan fungsionalitasnya dan mengevaluasi efektivitas sistem dalam mengamankan akses ke brankas. Model pengembangan sistem yang digunakan adalah metode ADDIE yang terdiri dari lima tahapan pengembangan yaitu; (1) Analisis, (2) Desain, (3) Pengembangan, (4) Implementasi dan (5) Evaluasi. Analisis masalah menggunakan analisis dan Analisis Kelayakan menggunakan analisis TELOS. Hasil analisis keandalan Sistem pada sistem ini adalah Ketepatan Verifikasi adalah 100% akurat dalam membedakan tag valid dan tidak valid berdasarkan data, sedangkan Kecepatan Respon yaitu waktu respon antara pembacaan RFID hingga pintu terbuka rata-rata <1 detik. Sistem tetap berjalan dengan baik selama server aktif dan perangkat terhubung dalam jaringan. Penelitian ini diharapkan dapat memberikan solusi alternatif sistem keamanan brankas yang terjangkau dan dapat disimulasikan secara virtual, menjadi acuan atau prototipe awal untuk pengembangan sistem keamanan IoT dalam skala yang lebih besar dan menunjukkan potensi penggunaan *Cisco Packet Tracer* dalam simulasi sistem keamanan berbasis RFID dan IoT.

Kata kunci : *Brankas, Internet of Things, Cisco Packet Tracer, SWOT, TELOS.*

E-ISSN : 2827-8550
P- ISSN : 1978-5569

1. Pendahuluan

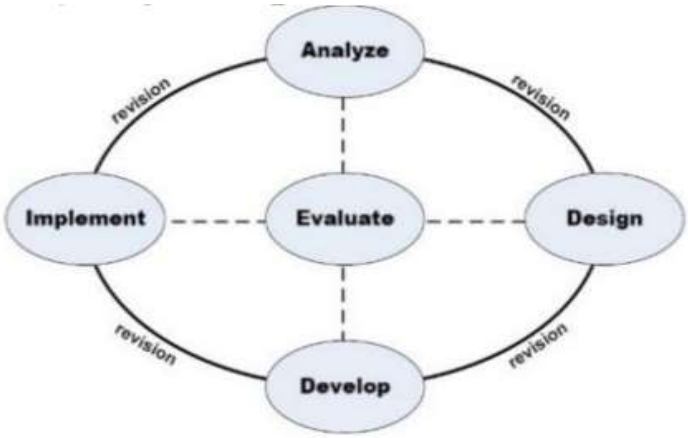
Perkembangan teknologi Internet of Things (IoT) telah membawa transformasi signifikan dalam berbagai bidang, termasuk sistem keamanan. Salah satu penerapan IoT yang semakin populer adalah dalam pengamanan aset berharga, seperti brankas, yang membutuhkan tingkat keamanan tinggi. Sistem keamanan tradisional yang mengandalkan kunci fisik atau kombinasi angka memiliki kelemahan, seperti risiko duplikasi kunci atau pembobolan kode. Oleh karena itu, diperlukan solusi yang lebih canggih, efisien, dan terintegrasi dengan teknologi modern.

Radio Frequency Identification (RFID) merupakan teknologi yang dapat digunakan untuk otentikasi akses dengan tingkat keamanan yang lebih baik karena memerlukan identifikasi unik melalui tag RFID. Integrasi antara RFID door lock dengan IoT memungkinkan pengawasan dan kontrol akses secara real-time melalui jaringan internet. *Cisco Packet Tracer* sebagai simulator jaringan dapat digunakan untuk memodelkan sistem ini sebelum diimplementasikan secara fisik, sehingga meminimalisir kesalahan dan biaya pengembangan.

Tujuan dari penelitian ini adalah merancang dan mengimplementasikan sistem keamanan brankas berbasis RFID dan IoT, mensimulasikan sistem menggunakan *Cisco Packet Tracer* untuk memastikan fungsionalitasnya dan mengevaluasi efektivitas sistem dalam mengamankan akses ke brankas. Penelitian ini diharapkan dapat memberikan solusi alternatif sistem keamanan brankas yang terjangkau dan dapat disimulasikan secara virtual, menjadi acuan atau prototipe awal untuk pengembangan sistem keamanan IoT dalam skala yang lebih besar dan menunjukkan potensi penggunaan Cisco Packet Tracer dalam simulasi sistem keamanan berbasis RFID dan IoT.

2. Metode Penelitian

Jenis Penelitian menggunakan *research and development* (Penelitian dan Pengembangan). Jenis Penelitian dan Pengembangan adalah jenis penelitian yang digunakan untuk menghasilkan produk tertentu dan menguji keefektifan produk. Sedangkan Model pengembangan sistem menggunakan metode ADDIE melalui lima tahapan pengembangan yaitu; (1) Analisis, (2) Desain, (3) Pengembangan, (4) Implementasi dan (5) Evaluasi. Model pengembangan ADDIE merupakan model yang efektif dalam pengembangan produk karena menggambarkan kerangka respon atau tanggapan dari berbagai situasi yang kompleks (M. Lutfi & Kristanto, n.d.)



Gambar 1. *Model Pengembangan ADDIE menurut Dick and Carry (1996) dalam (M. M. Lutfi et al., 2024)*

E-ISSN : 2827-8550
P- ISSN : 1978-5569

Berikut uraian pelaksanaan penelitian menggunakan Model Pengembangan ADDIE :

1. *Analyze* (Analisis)

Dalam model pengembangan ADDIE tahap pertama adalah menganalisis perlunya pengembangan produk baru dan menganalisis kelayakan serta syarat-syarat pengembangan produk. Pada tahapan analisis ini dilakukan analisis masalah menggunakan SWOT (Strenght, Weaknes, Opportunity dan Threat), Analisis Kebutuhan dan Analisis Kelayakan terhadap model, metode, dan media. Hasil evaluasi analisis digunakan sebagai pedoman untuk merancang sistem keamanan brankas yang sesuai dengan kebutuhan.

Tahapan selanjutnya adalah analisis kelayakan, Analisis kelayakan adalah analisis dari sistem yang akan di implementasikan mempunyai kelayakan dari segi teknis dan bisnis. Analisis yang digunakan adalah analisis TELOS.

2. *Design* (Perancangan)

Tahapan desain merupakan proses sistematik yang dimulai dari merancang konsep dan konten di dalam produk tersebut yang akan mendasari proses pengembangan di tahapan berikutnya. Pada penelitian ini tahapan desain dilakukan dengan merancang instrument yang terdiri atas instrumen software dan hardware. Software yang digunakan yaitu *Cisco Packet Tracer.* Tahapan pengembangan berisi kegiatan realisasi rancangan produk yang sebelumnya telah dibuat. Pada penelitian ini tahap pengembangan dilakukan dengan mengembangkan Desain produk Sistem Keamanan Brankas terdiri atas desain IOT dan desain Interface Aplikasi.

3. *Implement* (Implementasi)

Penerapan produk dalam model penelitian pengembangan ADDIE dimaksudkan untuk memperoleh umpan balik terhadap produk yang dibuat/dikembangkan. Umpan balik awal (awal evaluasi) dapat diperoleh dengan menanyakan hal-hal yang berkaitan dengan tujuan pengembangan produk. Penerapan dilakukan mengacu kepada rancangan produk yang telah dibuat.

4. *Evaluate* (Evaluasi)

Tahap evaluasi pada penelitian pengembangan model ADDIE dilakukan untuk memberi umpan balik kepada pengguna produk, sehingga revisi dibuat sesuai dengan hasil evaluasi atau kebutuhan yang belum dapat dipenuhi oleh produk tersebut. Tujuan akhir evaluasi yakni mengukur ketercapaian tujuan pengembangan. Pada tahapan evaluasi ini menggunakan *Black Box Testing*

3. Hasil dan Pembahasan

3.1. Hasil Penelitian

Penelitian dilakukan dengan menggunakan metode ADDIE dengan tahapan sebagai berikut :

a. Analyze (Analisis)

Dalam model pengembangan ADDIE tahap pertama adalah menganalisis perlunya pengembangan produk baru dan menganalisis kelayakan serta syarat-syarat pengembangan produk. Pada tahapan analisis ini dilakukan analisis masalah menggunakan *SWOT (Strenght, Weaknes, Opportunity dan Threat)*, Analisis Kebutuhan dan Analisis Kelayakan terhadap model, metode, dan media. Hasil evaluasi analisis digunakan sebagai pedoman untuk merancang sistem keamanan brankas yang sesuai dengan kebutuhan.

E-ISSN : 2827-8550
P- ISSN : 1978-5569

Tabel 1. *Analisis SWOT*

STRENGHT (Kekuatan)	Teknologi RFID dapat memberikan tingkat keamanan yang tinggi dalam mengontrol akses ke brankas. Integrasi dengan IoT memungkinkan pemantauan kondisi brankas secara realtime dari jarak jauh. Automatisasi dengan RFID mengurangi keterlibatan manual dalam manajemen keamanan brankas. Sistem dapat diperluas dengan mudah untuk memantau lebih banyak brankas atau area yang luas.
WEAKNESS (Kelemahan)	Kinerja sistem sangat tergantung pada koneksi internet yang stabil untuk operasi yang efektif. Implementasi teknologi RFID dan infrastruktur IoT awal memerlukan investasi yang signifikan. Tantangan dalam mengintegrasikan berbagai komponen teknologi (RFID, IoT, Cisco Packet Tracer) menjadi satu sistem yang berfungsi baik.
OPPORTUNITY (Peluang)	Menyediakan solusi inovatif untuk meningkatkan keamanan barang berharga dan melindungi dari ancaman pencurian. Permintaan akan solusi keamanan IoT terus meningkat, terutama dalam lingkungan bisnis dan perumahan. Peluang untuk mengembangkan fitur tambahan seperti analitik prediktif untuk deteksi dini potensi ancaman keamanan.
THREADS (Ancaman)	Risiko potensial terhadap kebocoran data atau serangan siber terhadap sistem IoT. Keharusan mematuhi peraturan privasi dan keamanan data yang berlaku dapat menjadi hambatan dalam implementasi. Cepatnya perkembangan teknologi dapat menghasilkan perubahan yang mempengaruhi keamanan dan interoperabilitas sistem.

Tahapan selanjutnya adalah analisis kelayakan, berikut tabel analisis kelayakan

Tabel 2. *Analisis Kelayakan TELOS*

Kelayakan Teknik ***(Technical feasibility)***	Teknologi Cisco Packet Tracer telah terbukti efektif dalam mensimulasikan jaringan IoT yang mencakup integrasi teknologi RFID. Dengan Packet Tracer, dapat dipelajari dan diuji kemampuan sistem dalam mengelola interaksi antara brankas yang dilengkapi RFID dengan infrastruktur jaringan yang relevan. Evaluasi ketersediaan komponen teknis seperti sensor RFID dan infrastruktur jaringan perlu dilakukan untuk memastikan kelancaran implementasi dan pemeliharaan sistem secara efektif.

E-ISSN : 2827-8550
P- ISSN : 1978-5569

Kelayakan Ekonomi ***(Economic feasibility)***	Dalam menghitung kelayakan ekonomi, perlu dipertimbangkan biaya total untuk pengembangan, implementasi, dan pemeliharaan sistem simulasi ini. Biaya yang perlu dievaluasi meliputi perangkat keras, perangkat lunak Packet Tracer, serta biaya tenaga kerja terkait. Penting juga untuk mengidentifikasi manfaat ekonomi yang dapat diperoleh dari penggunaan sistem ini, seperti potensi penghematan biaya keamanan atau peningkatan efisiensi operasional yang dapat mengimbangi biaya yang dikeluarkan.
Kelayakan Hukum ***(Law feasibility)***	Sebelum implementasi, perlu dipastikan bahwa sistem ini mematuhi semua regulasi hukum dan privasi yang berlaku terkait penggunaan teknologi RFID dalam konteks keamanan brankas. Izin dan persetujuan dari otoritas terkait mungkin diperlukan sebelum memulai proses implementasi. Memastikan kepatuhan terhadap regulasi lingkungan dan peraturan pemerintah juga menjadi bagian krusial dari kelayakan hukum.
Kelayakan Operasional ***(Operational feasibility)***	Evaluasi kelayakan operasional sistem ini meliputi kemampuan sistem untuk beroperasi secara efisien dalam berbagai kondisi lingkungan yang mungkin berubah, seperti fluktuasi cuaca atau perubahan kondisi brankas. Ketersediaan tenaga kerja yang terlatih untuk memelihara dan mengoperasikan sistem juga menjadi faktor penting yang perlu dievaluasi. Rencana darurat dan strategi pemulihan harus disusun untuk mengantisipasi dan mengatasi gangguan operasional yang mungkin terjadi selama implementasi dan penggunaan sistem ini.
Kelayakan Jadwal ***(Schedule feasibility)***	Menetapkan jadwal implementasi yang realistis merupakan langkah krusial untuk memastikan kesuksesan proyek. Perencanaan yang cermat termasuk pengujian sistem, integrasi dengan infrastruktur yang ada, serta pelatihan bagi pengguna harus dipertimbangkan dalam jadwal tersebut. Identifikasi risiko yang dapat mempengaruhi jadwal, seperti keterlambatan dalam pengadaan komponen atau kendala teknis, juga harus menjadi bagian dari strategi manajemen proyek untuk menjaga konsistensi dan kelancaran implementasi.

Analisis kebutuhan digunakan untuk merencanakan kebutuhan dalam penelitian ini, ada dua analisis kebutuhan yaitu analisis kebutuhan fungsional dan analisis kebutuhan non fungsional

Analisis Kebutuhan Fungsional

Kebutuhan fungsional menjelaskan fungsi utama yang harus dimiliki sistem agar berjalan sesuai tujuan. Berikut tabel analisis kebutuhan fungsional

E-ISSN : 2827-8550
P- ISSN : 1978-5569

Tabel 3. *Analisis Kebutuhan Fungsional Simulasi RFID door lock*

Kebutuhan	Fungsi
Autentikasi RFID	Sistem harus mampu membaca ID dari kartu RFID yang ditempelkan ke reader. Sistem harus mencocokkan ID RFID dengan database yang tersedia
Kontrol Akses Pintu Brankas	Jika ID RFID valid, pintu brankas terbuka secara otomatis (simulasi terbuka). Jika ID RFID tidak valid, akses ditolak dan alarm diaktifkan
Monitoring Jarak Jauh (IoT)	Sistem harus mengirim status buka/tutup pintu brankas secara real-time ke server/cloud (menggunakan protokol MQTT atau HTTP dalam simulasi). Pemilik dapat memonitor status brankas dari perangkat lain (simulasi dashboard di Cisco Packet Tracer).
Notifikasi Keamanan	Sistem harus memberikan notifikasi (simulasi LED, buzzer, atau pesan ke MQTT server) jika ada upaya akses tidak sah

Analisis Kebutuhan Non-Fungsional

Kebutuhan yang mendukung performa sistem, meskipun bukan fungsi utama. Berikut tabel analisis kebutuhan non fungsional

Tabel 4. *Analisis Kebutuhan Non Fungsional Simulasi RFID door lock*

Kebutuhan	Fungsi
Keamanan	Komunikasi data RFID dan IoT harus disimulasikan seaman mungkin (misalnya autentikasi ID hanya bisa diubah oleh admin).
Skalabilitas	Sistem dapat dikembangkan untuk mendukung beberapa brankas atau pintu akses lain di masa depan.
Keandalan	Sistem harus tetap berfungsi walaupun hanya secara virtual, dengan logika pengambilan keputusan berjalan benar
Kebutuhan Pengguna	**Admin / Pemilik Brankas** Mengelola ID RFID yang diizinkan Memantau status pintu Menerima notifikasi jika terjadi percobaan akses ilegal **Pengguna Umum** Hanya bisa membuka brankas jika memiliki RFID yang valid

b. Design (Perancangan)

Tahapan desain merupakan proses sistematik yang dimulai dari merancang konsep dan konten di dalam produk tersebut yang akan mendasari proses pengembangan di tahapan berikutnya. Pada penelitian ini tahapan desain dilakukan dengan merancang instrument yang terdiri atas instrumen software dan hardware. Software yang digunakan yaitu *Cisco Packet Tracer* dan *Figma*.

E-ISSN : 2827-8550
P- ISSN : 1978-5569

Perangkat yang digunakan adalah *Home gateway, Door, Sirene, RFID Sensor, Light, Smartphone, dan 2 RFID card* yang sudah diprogram dengan satu pin salah dan satu pin benar.

Tabel 5. *Perangkat internet of Things Simulasi RFID door lock*

Nama	Fungsi
Home gateway	Sebagai router, swicth, dan akses point untuk mengubungkan perangkan ke internet dan menyediakan connectivitas nirkabel.
Door	Sebagai penanda atau objek tujuan yang akan terbuka apabila pin benar.
Sirene	Sebagai penanda atau objek tujuan yang akan berbunyi apabila pin salah.
RFID Sensor	Untuk pelacakan objek dan otomatisasi identifikasi dari *RFID card*
Light	Sebagai penanda atau objek tujuan yang akan menyala apabila pin benar.
Smartphone	Sebagai perangkat yang dapat menghubungkan perangkat lain untuk mengakses internet melalui *Home Gateway.*
RFID card	Untuk akses contol dan masuk ke program yang dibuat.

c. Develope (Pengembangan)

Tahapan pengembangan berisi kegiatan realisasi rancangan produk yang sebelumnya telah dibuat. Pada penelitian ini tahap pengembangan dilakukan dengan mengembangkan Desain produk Sistem Keamanan Brankas terdiri atas desain IOT dan desain Interface Aplikasi.

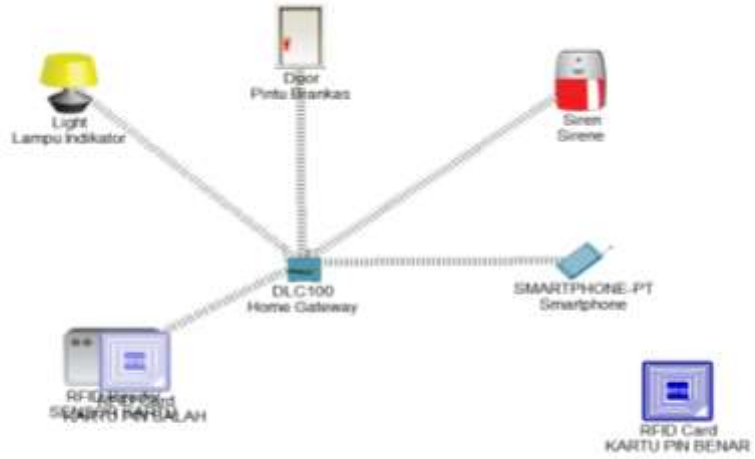
Tabel 6. *Rule dari Internet of Things Simulasi RFID Door Lock*

Rule	Kondisi
Sensor kartu benar	Set Pintu Brankas terbuka Set Lampu Indikator menyala Set Sirene mati
Sensor kartu salah	Set Pintu Brankas Terkunci Set Lampu Indikator mati Set Sirene menyala

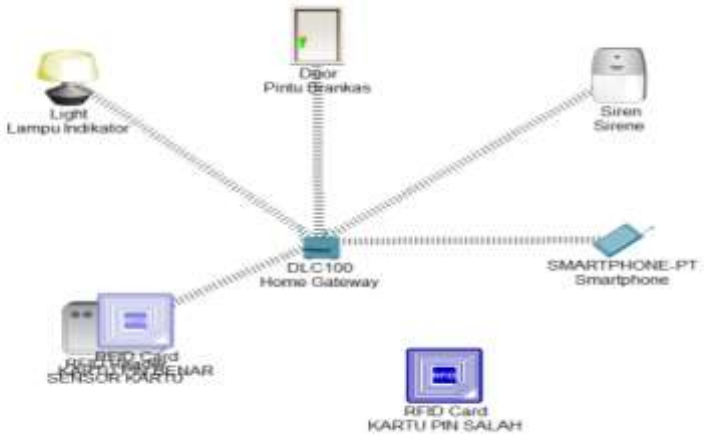
d. Implement (Implementasi)

Penerapan produk dalam model penelitian pengembangan ADDIE dimaksudkan untuk memperoleh umpan balik terhadap produk yang dibuat/dikembangkan. Umpan balik awal (awal evaluasi) dapat diperoleh dengan menanyakan hal-hal yang berkaitan dengan tujuan pengembangan produk. Penerapan dilakukan mengacu kepada rancangan produk yang telah dibuat.

E-ISSN : 2827-8550
P- ISSN : 1978-5569



Gambar 2. *Rancangan skema Internet of Things Simulasi RFID door Lock dengan PIN salah.*



Gambar 3. *Rancangan skema Internet of Things Simulasi RFID door Lock dengan PIN benar.*

Berikut adalah tampilan Dashboard Desain IoT dari sistem simulasi Simulasi RFID door Lock:

E-ISSN : 2827-8550
P- ISSN : 1978-5569

Gambar 4. *Desain Dashboard IoT Sistem Pemantauan RFID Lock Door*

e. Evaluate (Evaluasi)

Tahap evaluasi pada penelitian pengembangan model ADDIE dilakukan untuk memberi umpan balik kepada pengguna produk, sehingga revisi dibuat sesuai dengan hasil evaluasi atau kebutuhan yang belum dapat dipenuhi oleh produk tersebut. Tujuan akhir evaluasi yakni mengukur ketercapaian tujuan pengembangan. Pada tahapan evaluasi ini menggunakan *Black Box Testing.* Tujuan Analisis *Black Box* adalah Memastikan semua fitur bekerja sesuai spesifikasi sistem, mengetes semua kemungkinan skenario input (valid/invalid) dan Mengevaluasi reaksi sistem terhadap kesalahan/ancaman. Metode *Black Box Testing* digunakan untuk menguji fungsi sistem dari sisi luar (tanpa melihat kode program) berdasarkan *input* dan *output* yang diharapkan. Berikut tabel pengujian *black box*.

Tabel 7. *Analisis Black Box Perangkat internet of Things Simulasi RFID door lock*

Fitur Autentikasi RFID		
Input	Proses	Output yang Diharapkan
ID RFID valid	RFID Reader membaca dan kirim ke sistem	Pintu terbuka, status "Akses Diberikan"
ID RFID tidak valid	RFID Reader membaca dan kirim ke sistem	Alarm aktif, status "Akses Ditolak"
Tidak ada RFID ditempelkan	Tidak ada proses	Sistem tetap standby
ID RFID valid	RFID Reader membaca dan kirim ke sistem	Pintu terbuka, status "Akses Diberikan"
Fitur Penguncian dan Pembukaan Pintu Brankas		
Input	Proses	Output yang Diharapkan
Perintah tutup (otomatis/manual)	Kontrol menutup smart door	Pintu terkunci
Akses ilegal	Sistem menolak dan mengunci pintu	Pintu tetap terkunci, alarm menyala
Fitur Notifikasi Keamanan		

E-ISSN : 2827-8550
P- ISSN : 1978-5569

Input	Proses	Output yang Diharapkan
Deteksi akses tidak sah	Kirim data ke cloud/server	Notifikasi ditampilkan di dashboard
Akses berhasil	Kirim data ke cloud/server	Status update: "Brankas dibuka"
Status pintu berubah	Sensor mendeteksi perubahan	Update status real-time di dashboard pengguna
Fitur Monitoring IoT (Dashboard/Tablet)		
Input	Proses	Output yang Diharapkan
Permintaan status dari user	Ambil data dari cloud/server	Status pintu ditampilkan (terkunci/terbuka)
Permintaan log aktivitas	Ambil histori dari server (jika ada)	Riwayat akses RFID ditampilkan

1.2. Pembahasan

Cisco Packet Tracer merupakan program simulasi dari *Cisco Systems* sebagai sarana pembelajaran jaringan dan *internet of things* secara mudah. Hanya diperlukan laptop dengan spesifikasi yang mencukupi dan Anda sudah dapat untuk membuat simulasi jaringan dan *internet of things* secara mandiri yang akan mempermudah pemahaman penerapan di lapangan (Prayitno & Yakti, 2020)

Internet of Things saling berkomunikasi dalam melakukan pekerjaan berupa gambar, audio, video sehingga menghasilkan sebuah informasi dan saling berkoordinasi dalam membuat keputusan (Sandi & Fatma, 2023). IoT *(Internet of Things*) adalah sistem perangkat komputer yang saling berhubungan antara mesin digitalisasi, objek, hewan atau manusia yang saling melengkapi dengan cara mengidentifikasi kemampuan untuk mentransfer data melalui jaringan tanpa memerlukan interaksi manusia ke manusia maupun manusia kekomputer (M Lutfi MA, 2024)

Radio frequency identification (RFID) adalah proses identifikasi seseorang atau objek dengan menggunakan frekuensi transmisi radio. *Radio frequency identification (RFID)* menggunakan frekuensi radio untuk membaca informasi dari sebuah devais kecil yang disebut tag atau transponder (Transmitter + Responder). Tag RFID akan mengenali diri sendiri ketika mendeteksi sinyal dari devais yang kompatibel, yaitu pembaca RFID *(RFID Reader*) (Ramesh et al., 2021).

Setelah dilakukan perancangan sistem dan dilakukan pengujian *blackbox testing*, dapat diketahui bahwa teknologi RFID mampu di aplikasikan pada brankas sebagai sistem keamanan. Penggunaan *Radio Frequency Identification (RFID)* sebagai sistem keamanan brankas berjalan sesuai dengan perancangan dan program yang telah dibuat. Sistem dapat mendeteksi jika terjadi kesalahan nomor pin pada Tag RFID.

Hasil analisis Keandalan Sistem pada sistem ini adalah **Ketepatan Verifikasi** adalah 100% akurat dalam membedakan tag valid dan tidak valid berdasarkan database, sedangkan **Kecepatan Respon** yaitu waktu respon antara pembacaan RFID hingga pintu terbuka rata-rata <1 detik. Sistem tetap berjalan dengan baik selama server aktif dan perangkat terhubung dalam jaringan.

Adapun kelebihan Sistem adalah Simulasi Tanpa Biaya Perangkat Fisik karena Cisco Packet Tracer memungkinkan pengujian sistem secara lengkap sebelum implementasi nyata. Monitoring Real-Time yaitu setiap aktivitas akses langsung tercatat dan dapat dipantau melalui dashboard.

E-ISSN : 2827-8550
P- ISSN : 1978-5569

Sistem dapat diperluas untuk lebih banyak tag, pintu, atau area kontrol hanya dengan menambahkan perangkat dalam simulasi.

Sistem juga mempunyai Kekurangan dan Keterbatasan seperti Simulasi Bersifat Logis dimana Tidak semua aspek fisik (misalnya interferensi sinyal RFID, kegagalan perangkat keras) dapat diuji dalam simulasi. Sistem juga Tidak Mendukung Platform IoT Eksternal karena Cisco Packet Tracer belum mendukung integrasi langsung dengan platform cloud. Sistem juga belum Ada Enkripsi sehingga komunikasi data antarperangkat belum menggunakan protokol keamanan tingkat lanjut.

Kesimpulan

Berdasarkan hasil perancangan dan simulasi sistem keamanan brankas menggunakan RFID dan IoT pada Cisco Packet Tracer, dapat disimpulkan beberapa hal sebagai berikut:

1. **Sistem berhasil dirancang dan disimulasikan** secara fungsional dengan memanfaatkan RFID sebagai metode autentikasi akses dan IoT sebagai media pemantauan real-time.
2. **RFID Reader dapat membedakan antara tag yang valid dan tidak valid**, yang kemudian menentukan apakah akses ke brankas diberikan atau ditolak.
3. **Integrasi dengan IoT Server memungkinkan pencatatan log akses** serta pemantauan status pintu secara langsung melalui dashboard yang terhubung dalam jaringan lokal.
4. **Simulasi pada Cisco Packet Tracer berjalan stabil**, menunjukkan alur sistem yang responsif dan akurat, meskipun masih memiliki keterbatasan dalam hal konektivitas cloud dan keamanan komunikasi data.
5. **Sistem ini layak dijadikan prototipe awal** sebelum implementasi nyata dengan perangkat keras fisik.

Daftar Pustaka

Lutfi, M., & Kristanto, A. (n.d.). *"Jurnal TRANSFORMASI (Informasi & Pengembangan Iptek)" (STMIK BINA PATRIA) TRAINER FUZZY SEBAGAI SARANA PRAKTIKUM MAHASISWA*.

Lutfi, M. M., Andri Saputra, M., Indrawan Putranto, V., & Ridho, R. (2024). "Jurnal TRANSFORMASI (Informasi & Pengembangan Iptek)" (STMIK BINA PATRIA) SIMULASI SISTEM PENYIRAM TANAMAN HIAS MENGGUNAKAN KONTROL LOGIKA FUZZY BERBASIS INTERNET OF THINGS. *Jurnal TRANSFORMASI*, *20*(1), 1–19.

M Lutfi MA. (2024). *INTERNET OF THINGS* (M. K. Sepriano, Ed.; 1st ed., Vol. 1). Sonpedia. www.buku.sonpedia.com

Prayitno, R. H., & Yakti, B. K. (2020). SIMULASI SMART HOME MENGGUNAKAN CISCO PACKET TRACER. *Jurnal Ilmiah Informatika Komputer*, *25*(2), 115–126. https://doi.org/10.35760/ik.2020.v25i2.2577

Ramesh,] P, Sri,] M, Reddy, V. R., & Bhaskara Reddy, P. (2021). *Architecture, Protocols, Layers and Elements of IoT*. www.ijcrt.org

Sandi, G. H., & Fatma, Y. (2023). PEMANFAATAN TEKNOLOGI INTERNET OF THINGS (IOT) PADA BIDANG PERTANIAN. In *Jurnal Mahasiswa Teknik Informatika* (Vol. 7, Issue 1).