SISTEM KEAMANAN BERBASIS SIDIK JARI PADA PRODI TI UNIVERSITAS MUHAMMADIYAH KALIMANTAN TIMUR

Muhammad Khumaidi Nursyarif[1], Arbansyah[2*], Muhammad Taufiq Sumadi[3]

[1,2] Teknik Informatika, Sains dan Teknologi, Universitas Muhammadiyah Kalimantan Timur, Indonesia
[3] Teknik Informatika, Jurusan Teknologi Informasi, Politeknik Negeri Samarinda, Indonesia
[1]2011102441085@umkt.ac.id, [2] arb381@umkt.ac.id, [3] mts653@umkt.ac.id

Abstrak

Perkembangan teknologi yang pesat memberikan banyak manfaat dalam berbagai aspek kehidupan manusia, termasuk dalam bidang keamanan. Salah satu teknologi yang relevan ialah *Internet of Things*, yang memungkinkan berbagai perangkat terhubung dan dikendalikan melalui internet. Teknologi ini sangat cocok untuk sistem identifikasi dan keamanan, termasuk teknologi biometrik seperti sidik jari. Penelitian ini mengembangkan dan mengimplementasikan sistem keamanan pintar berbasis sidik jari menggunakan NodeMCU dan platform Thinger.io. Sistem ini dirancang untuk diterapkan pada pintu masuk ruangan Prodi Teknik Informatika Universitas Muhammadiyah Kalimantan Timur. Metode yang digunakan meliputi penggunaan sensor sidik jari untuk identifikasi pengguna, NodeMCU sebagai mikrokontroler, dan Thinger.io untuk pengelolaan data serta pengiriman notifikasi. Sistem bekerja dengan cara memindai sidik jari yang kemudian diverifikasi oleh NodeMCU. Jika sidik jari dikenali, pintu akan terbuka, dan jika tidak dikenali setelah tiga kali percobaan, sistem akan mengirim notifikasi peringatan akses tidak dikenal melalui email. Kelebihan dari penggunaan sidik jari ini mencakup tingkat keamanan yang tinggi karena sidik jari memiliki keunikan yang sulit diduplikasi. Selain itu, manfaat yang diperoleh meliputi peningkatan keamanan ruangan dan kemudahan akses tanpa kunci fisik. Hasil penelitian menunjukkan bahwa sistem keamanan berbasis sidik jari ini efektif dalam menjaga keamanan pintu, dengan mekanisme verifikasi yang andal dan deteksi percobaan akses yang tidak sah. Sistem ini juga memberikan notifikasi responsif secara *real-time* setelah upaya gagal dikenali sebanyak tiga kali. Sistem berfungsi dengan stabil dan dapat dikembangkan lebih lanjut untuk memenuhi kebutuhan spesifik pengguna serta diadaptasi dalam berbagai situasi yang berbeda.

Kata kunci : *Internet of Things*, Sidik Jari, NodeMCU, Thinger.io, Keamanan Pintar

1. Pendahuluan

Perkembangan teknologi saat ini menjadi sedemikian pesat sehingga kehadiran sebuah teknologi baru menjadi sangat membantu bagi manusia dalam melakukan aktifitas (Rahayu & Nurdin, 2019). Globalisasi terus mendorong dunia untuk bergerak menuju modernisasi, mendorong lahirnya berbagai inovasi dalam bidang teknologi dan informasi (Nugroho et al., 2021). Salah satu dampak yang dirasakan di dunia dan masyarakat modern adalah *Internet of Things* yang dapat menghubungkan beberapa perangkat jaringan melalui internet yang digunakan untuk memantau atau mengontrol suatu sistem tertentu, sehingga memungkinkan perangkat saling berkomunikasi, bertukar data, dan bertindak sesuai instruksi pengguna (Lagan & Ary, 2021; Prasetyo Eka Putra et al., 2023). Pemanfaatan teknologi ini sangat cocok untuk diterapkan pada sistem identifikasi yang membutuhkan sistem keamanan tinggi, beberapa diantaranya menggunakan sistem keamanan dalam teknologi biometrik seperti pengenalan retina mata, sidik jari, dan lain-lain (Bachtiar, 2022).

Teknologi sidik jari sendiri adalah pendekatan biometrik yang paling umum dikenal dan stabil karena memberikan tingkat perlindungan yang lebih baik serta ramah bagi pengguna (Wee, 2021). Hanya ada 1 dalam 1 miliar kemungkinan teknologi sidik jari dapat diduplikasi, sehingga identifikasi pengguna yang terbaca tidak dapat digantikan, disalin, atau dicuri (Nagarkar & Kadam, 2023). Oleh karena itu, akses yang tidak disetujui dapat dibatasi dan menjadi salah satu sistem yang paling solid karena sidik jari unik seseorang tidak pernah terkoordinasi dengan orang lain (Gupta et al., 2022).

Di era kemajuan teknologi saat ini, beberapa kantor masih menggunakan kunci konvensional sebagai pengamanan utama pada ruangan, sehingga untuk membuka dan menutup pintu kantor diserahkan kepada salah satu pegawai atau petugas keamanan (Ningrum & Basyir, 2022). Meskipun demikian, kerangka keamanan tradisional masih cukup lemah, khususnya kunci sering hilang atau tercecer dan ada berbagai cara pencuri merakit alat pembobol rumah sehingga perampokan sering terjadi dan menyebabkan kerugian. (Jodi et al., 2022). Oleh karena itu perlu untuk dapat meningkatkan sistem keamanan pada ruangan serta mencegah tingkat pencurian dan mengetahui siapa yang sedang mencoba mengakses pintu tersebut.

Pada penelitian sebelumnya melakukan sebuah sistem pemantauan sistem keamanan palang pintu berbasis *Long Range RFID (Radio Frequency Identification)* yang diterapkan pada perumahan, dimana untuk cara kerjanya semua informasi pengunjung disimpan pada cloud, sehingga sistem ini dibuat dengan pendaftaran RFID yang dapat diawasi oleh satpam dan membantu masyarakat komplek dalam memastikan akses masuk dan keluar. (Sari et al., 2023). Beberapa penelitian lain juga menyoroti mengenai sistem keamanan kunci, salah satunya otomatisasi sistem keamanan kunci lemari menggunakan sensor sidik jari berbasis Arduino Uno dan proses kerja dari sistem ini dengan melakukan scanning jari tangan, kemudian dikirim ke mikrokontroler untuk ditangani yang kemudian memerintahkan kunci solenoid untuk membuka atau menutup kunci lemari (Khalid et al., 2020).

Pada penelitian ini, peneliti mengusulkan pengembangan sistem keamanan menggunakan sensor sidik jari yang terintegrasi dengan NodeMCU dan Thinger.io. Teknologi sidik jari menawarkan keunggulan signifikan dibandingkan metode lain. Sidik jari lebih aman daripada sistem kartu yang bisa hilang atau dicuri, dan lebih cepat serta mudah digunakan dibandingkan pengenalan retina yang dipengaruhi pencahayaan dan posisi. Selain itu, sidik jari menawarkan akurasi dan kecepatan verifikasi yang lebih tinggi dibandingkan pengenalan wajah.

Sistem ini juga menyediakan solusi keamanan efisien dengan monitoring dan kontrol akses *real-time* serta pengelolaan data terintegrasi. NodeMCU mengendalikan sensor sidik jari dan solenoid lock, sementara Thinger.io memantau akses dan mengelola data secara otomatis. Solenoid lock juga secara otomatis mengontrol mekanisme penguncian pintu sehingga setelah pintu dibuka, pintu akan terkunci kembali setelah beberapa detik, mengurangi risiko keamanan tanpa memerlukan intervensi manual.

Keunggulan sistem ini terletak pada fleksibilitas dan kemampuannya dalam mengirim notifikasi peringatan akses secara *real-time* melalui email jika ada akses tidak dikenal. Integrasi ini memungkinkan pengelolaan keamanan yang lebih mudah dan adaptif di berbagai lingkungan, dari institusi pendidikan hingga ruang kantor. Dengan demikian, solusi ini menawarkan pendekatan keamanan yang handal, efisien, dan nyaman bagi prodi TI Universitas Muhammadiyah Kalimantan Timur.

2. Metode Penelitian

Metode yang digunakan pada penelitian ini terdiri dari 4 tahapan penelitian. Dimulai dari persiapan, perancangan, pembuatan prototipe, dan pengujian.

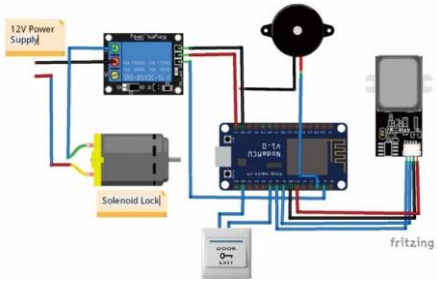
2.1 Persiapan

Pada tahap persiapan, peneliti mempelajari referensi terkait untuk memahami topik penelitian. Studi oleh (Handika et al., 2021) menunjukkan integrasi sensor sidik jari dengan Arduino Mega2560 dilakukan dengan baik sehingga memberikan pondasi teknis yang kuat untuk pengembangan sistem keamanan. Penelitian lain oleh (Dewi & Fikri, 2023) menunjukkan bahwa IoT dapat peningkatan signifikan dalam keamanan dan efisiensi sistem. Penelitian terakhir oleh (Anwar et al., 2021) memperlihatkan bahwa selain NodeMCU dapat terhubung ke Wi-Fi dengan baik, tetapi juga dapat diintegrasikan dengan Thinger.io untuk pengolahan data secara efektif. Dengan mempelajari penelitian ini, peneliti memiliki landasan yang kuat untuk mengembangkan sistem keamanan berbasis sidik jari yang handal dan efisien.

2.2 Perancangan Sistem

Dalam tahap ini, dilakukan penentuan konsep dan perancangan sistem keamanan berbasis sidik jari dengan NodeMCU dan Thinger.io. Rancangan ini mencakup desain alat dan *flowchart* sistem.

Berikut adalah skematik (*wiring diagram*) dari sistem yang direncanakan, menunjukkan hubungan dan koneksi antar perangkat pada NodeMCU.



Gambar 1. Diagram Sistem Keamanan Berbasis Sidik Jari

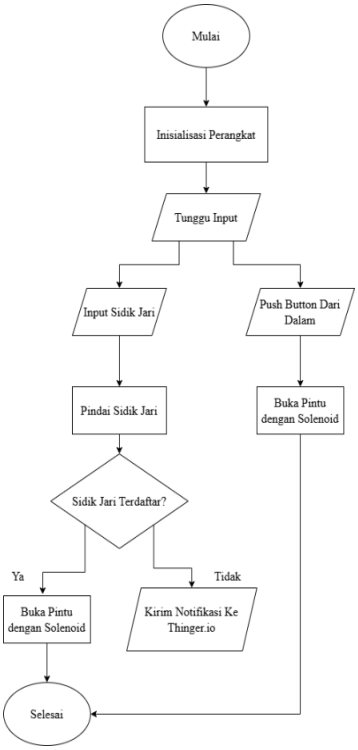
Pada Gambar 1, sistem keamanan ini menunjukkan bagaimana berbagai komponen terhubung melalui NodeMCU dengan konfigurasi yang detail. Sensor sidik jari terhubung ke pin D1 (RX) dan D2 (TX) untuk komunikasi serial yang memungkinkan proses pendaftaran dan verifikasi sidik jari. Relay yang mengendalikan solenoid lock terhubung ke pin D4, yang berfungsi membuka kunci pintu ketika sidik jari dikenali atau ketika push button pada pin D5 ditekan. Solenoid lock dan relay mendapatkan daya dari sumber 12V, yang memastikan kelancaran operasional sistem.

Selain komponen fisik, NodeMCU terhubung ke Thinger.io melalui koneksi Wi-Fi. Proses ini melibatkan konfigurasi di mana NodeMCU mengirimkan data log dan status sistem ke server Thinger.io setiap kali ada aktivitas seperti

pendaftaran sidik jari, verifikasi akses, atau upaya akses yang tidak sah. Thinger.io menyimpan data ini di dalam dashboard pengguna, yang dapat diakses melalui perangkat apa pun dengan koneksi internet.

Data yang disimpan di Thinger.io meliputi informasi tentang sidik jari yang terdaftar, status verifikasi, dan log waktu akses. Jika terjadi tiga kali percobaan akses dengan sidik jari yang tidak dikenali, NodeMCU akan memicu pengiriman notifikasi peringatan akses tidak dikenal melalui Thinger.io yang kemudian diteruskan ke email pengguna.

Dengan demikian, NodeMCU berperan sebagai pengelola utama yang menangani proses komunikasi dan kendali lokal, sementara Thinger.io berfungsi sebagai platform penyimpanan data dan notifikasi yang memastikan sistem dapat dipantau serta diakses dari jarak jauh dengan aman.

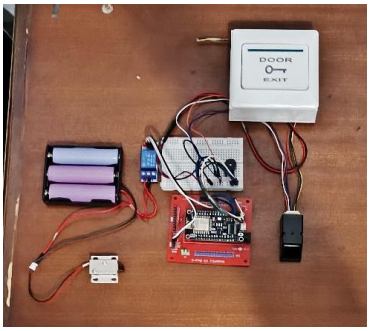


Gambar 2. Flowchart Sistem

Dari Gambar 2 menunjukkan cara kerja dari sistem yang dirancang. Proses dimulai dengan inisialisasi perangkat, kemudian sistem menunggu input dari pengguna. Input dapat berupa pemindaian sidik jari atau penekanan push button dari dalam ruangan. Jika sidik jari dipindai, sistem akan memeriksa apakah sidik jari tersebut terdaftar di database. Jika terdaftar, pintu akan dibuka dengan solenoid. Dan jika tidak terdaftar, sistem akan mengirim notifikasi ke Thinger.io dan mengaktifkan buzzer. Selanjutnya saat push button ditekan dari dalam, pintu langsung terbuka dengan solenoid. Dan proses diakhiri setelah pintu dibuka atau notifikasi dikirim dan buzzer diaktifkan.

2.3 Pembuatan Prototipe

Setelah perancangan sistem selesai, dilakukan pengembangan prototipe berdasarkan desain yang telah disusun sebelumnya. Prototipe ini mencakup perakitan perangkat keras (*hardware*) dan pengembangan perangkat lunak (*software*) untuk menjalankan sistem keamanan pintar.



Gambar 3. Prototipe Alat

Pada Gambar 3, menampilkan susunan komponen yang terintegrasi secara rapi. Gambar ini menunjukkan bagaimana sensor sidik jari, NodeMCU, relay, dan push button dipasang dalam satu unit, memberikan tampilan yang jelas tentang konfigurasi dan tata letak keseluruhan alat.

2.4 Pengujian

Tahap pengujian dilakukan untuk memastikan bahwa prototipe yang dikembangkan dapat berfungsi sesuai dengan yang diharapkan. Pengujian mencakup uji coba fungsionalitas, keamanan, dan koneksi internet untuk memastikan keandalan dan kinerja sistem secara keseluruhan.

3. Hasil Dan Pembahasan

Bagian ini membahas hasil pengujian dan analisis dari implementasi sistem pengenalan sidik jari menggunakan NodeMCU, modul fingerprint AS608, dan platform IoT Thinger.io. Proses persiapan mencakup pengadaan komponen seperti NodeMCU, modul fingerprint AS608, buzzer, relay, dan switch button, serta konfigurasi perangkat lunak melalui Arduino IDE. Implementasi meliputi inisialisasi perangkat keras, penulisan kode untuk sensor sidik jari, dan integrasi dengan Thinger.io untuk manajemen pendaftaran dan akses.

Modul fingerprint AS608 bekerja dengan menangkap citra sidik jari melalui sensor optik dan mengolah data untuk menghasilkan template yang disimpan dalam memori. Saat verifikasi dilakukan, template sidik jari baru dibandingkan dengan template yang telah tersimpan untuk memverifikasi atau mengidentifikasi sidik jari. Sensor ini mendukung penyimpanan hingga 162 template, memungkinkan pengelolaan data sidik jari yang efisien. Datasheet menunjukkan bahwa sensor ini

memiliki *false acceptance rate* kurang dari 0.001% dan *false reject rate* kurang dari 1.0% pada tingkat keamanan 3, dengan waktu imaging kurang dari 1 detik dan ukuran template 512 bytes.

Pengujian sistem dilakukan untuk memverifikasi fungsi pendaftaran dan verifikasi sidik jari, serta pengendalian akses ke ruangan. Hasil pengujian menunjukkan integrasi yang berhasil dengan Thinger.io, memungkinkan pemantauan real-time dan pengiriman notifikasi. Sistem ini terbukti efisien dalam mengelola identifikasi sidik jari dan memberikan tingkat keamanan serta respon yang sesuai dengan kebutuhan dalam pengendalian akses ke ruangan di Prodi Teknik Informatika Universitas Muhammadiyah Kalimantan Timur.dalam pengendalian akses ke ruangan.

3.1 Hasil Pengujian Dan Pembahasan

Pengujian dilakukan untuk memastikan bahwa sistem pengenalan sidik jari yang dikembangkan berfungsi sesuai dengan spesifikasi yang diharapkan. Langkah-langkah pengujian melibatkan pengamatan langsung terhadap rangkaian dan komponennya, serta evaluasi kinerja keseluruhan sistem. Hasil pengujian ini diperlukan untuk menentukan apakah sistem berfungsi dengan baik atau jika terdapat kesalahan yang perlu diperbaiki.

3.2 Pengujian Fungsionalitas Sistem

Pada pengujian ini, pengujian difokuskan pada parameter fungsional seperti jari yang digunakan, status penerimaan atau penolakan akses, waktu yang dibutuhkan dalam proses pengenalan sidik jari, serta output yang dihasilkan. Dengan memberikan gambaran mengenai performa sistem dalam kondisi operasional nyata, termasuk kehandalan dalam proses identifikasi dan respons terhadap input yang diterima. Dan hasil pengujian sebagai berikut:

3.2.1 Pendaftaran Sidik Jari

Pada pengujian ini, pendaftaran dilakukan dengan dua sidik jari penulis yang berbeda dalam dua kali percobaan. Proses pendaftaran dapat dilakukan melalui dua opsi: mengetikkan "e" pada serial monitor melalui Arduino IDE atau menggunakan fitur switch pada dashboard Thinger.io. Kemudian meletakkan jari pada modul fingerprint AS608 untuk pemindaian pertama. Setelah sidik jari disimpan, pengguna meletakkan jari yang sama untuk pemindaian kedua guna memastikan akurasi data. Jika kedua pemindaian cocok, sidik jari berhasil didaftarkan ke basis data sistem. Setiap sidik jari yang didaftarkan menghasilkan template berukuran 512-byte, yang mencakup informasi unik hasil pemindaian.

Gambar 4. Pendaftaran Sidik Jari

Tabel 1. Data Hasil Pengujian Pendaftaran Sidik Jari

No	Jari yang digunakan	Status	Waktu yang dibutuhkan
1	Ibu Jari Kiri	Sidik Jari Tersimpan	7,80 Detik
2	Jari Telunjuk Kiri	Sidik Jari Tersimpan	8,95 Detik

Pada Tabel 1 di atas menunjukkan hasil pengujian waktu yang dibutuhkan untuk pendaftaran sidik jari, dari dua kali pengujian, waktu yang diperlukan untuk menyimpan data sidik jari berkisar selama 7 hingga 8 detik untuk satu kali pendaftaran hingga data sidik jari tersimpan.

3.2.2 Pengujian Sidik Jari yang Terdaftar

Pengujian sidik jari yang terdaftar untuk membuka pintu dilakukan untuk memastikan bahwa sistem ini dapat melihat dan memeriksa sidik jari yang telah disimpan dalam basis data, serta mengaktifkan mekanisme pembukaan pintu. Proses pengujian dimulai dengan meletakkan sidik jari yang telah terdaftar pada fingerprint untuk proses pemindaian dan pencocokan sidik jari dengan data yang ada. Jika sidik jari dikenali, maka sistem akan mengirim data yang menampilkan informasi “sidik jari ditemukan” pada serial monitor dan relay yang mengontrol solenoid door lock akan terbuka. Data hasil pengujian sidik jari ditampilkan pada Tabel 2.

Tabel 2. Data Hasil Pengujian Sidik Jari yang Terdaftar

No	Jari yang digunakan	Status	Waktu yang dibutuhkan
1	Ibu Jari Kanan	Terverifikasi	1,80 Detik
2	Jari Telunjuk Kanan	Terverifikasi	2,05 Detik
3	Jari Kelingking Kanan	Terverifikasi	1,95 Detik
4	Ibu Jari Kiri	Terverifikasi	2,10 Detik
5	Jari Telunjuk Kiri	Terverifikasi	1,85 Detik

Hasil pengujian pada Tabel 2 menjelaskan dari pengujian yang dilakukan pada lima sidik jari, waktu yang diperlukan untuk memverifikasi sidik jari berkisar antara 1,80 hingga 2,10 detik. Hasil ini menunjukkan bahwa proses verifikasi berjalan dengan cepat dan baik, sehingga dapat memastikan respon yang memadai untuk kebutuhan sistem pengendalian akses.

3.2.3 Pengujian Penghapusan Sidik Jari

Pengujian penghapusan sidik jari dilakukan untuk memastikan sistem dapat menghapus data sidik jari yang telah disimpan dalam basis data dengan baik dan cepat. Proses pengujian dimulai dengan memilih sidik jari yang akan dihapus melalui sistem. Setelah sidik jari dipilih, pengguna mengkonfirmasi penghapusan, dan sistem kemudian menjalankan perintah untuk menghapus data sidik jari tersebut. Jika penghapusan berhasil, sistem akan menampilkan informasi "sidik jari dihapus" pada serial monitor. Pengujian ini dilakukan untuk dua sidik jari yang berbeda. Data hasil pengujian penghapusan sidik jari ditampilkan pada Tabel 3.

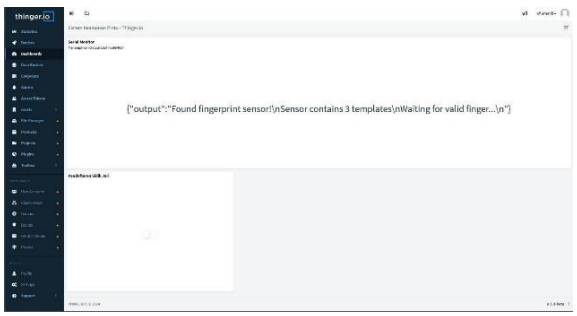
Tabel 3. Data Hasil Pengujian Penghapusan Sidik Jari

No	Jari yang digunakan	Status	Waktu yang dibutuhkan
1	Ibu Jari Kiri	Terverifikasi	1,70 Detik
2	Jari Telunjuk Kiri	Terverifikasi	1,65 Detik

Pada Tabel 3 ini dijelaskan hasil pengujian waktu yang dibutuhkan untuk penghapusan sidik jari yang telah terdaftar. Dari pengujian yang dilakukan pada dua sidik jari, waktu yang diperlukan untuk menghapus sidik jari berkisar antara 1,65 hingga 1,70 detik. Hasil ini menunjukkan bahwa proses penghapusan sidik jari berlangsung dengan cepat dan efisien, memastikan bahwa data sidik jari dapat dikelola dengan mudah dan responsif sesuai kebutuhan sistem.

3.3 Integrasi Thinger.io

Dari Gambar 5 dibawah, integrasi Thinger.io memberikan kemudahan dalam pengelolaan sidik jari, memungkinkan pengguna untuk menambahkan, dan mengatur akses pintu dengan cepat. Keamanan sistem juga ditingkatkan karena pengguna dapat melakukan manajemen akses secara terpusat dan terkontrol. Sehingga menjadi solusi efektif dalam meningkatkan pengelolaan akses pintu dengan teknologi yang terintegrasi secara baik.



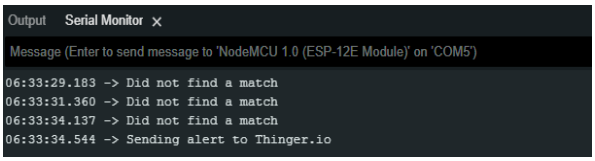
Gambar 5. Integrasi Thinger.io

3.4 Pengujian Sistem Keamanan

Pengujian keamanan dilakukan dengan mencoba mengakses sistem menggunakan sidik jari yang tidak terdaftar. Selain itu, dilakukan simulasi upaya pembobolan dengan mencoba sidik jari yang tidak terdaftar sebanyak tiga kali berturut-turut untuk memicu pengiriman notifikasi ke Thinger.io. Berikut rincian dari metode pengujian yang dilakukan:

3.4.1 Evaluasi Keamanan

Pengujian keamanan dilakukan dengan mencoba mengakses sistem menggunakan sidik jari yang tidak terdaftar. Metode ini bertujuan untuk memastikan bahwa sistem hanya mengizinkan akses bagi sidik jari yang telah terdaftar dalam basis data.



Gambar 6. Deteksi Sidik Jari Tidak Dikenali dan Notifikasi Dikirim Ke Thinger.io

Gambar 7. Notifikasi Dari Sistem Ke Email

Hasil pengujian menunjukkan bahwa sistem berhasil menolak upaya akses menggunakan sidik jari yang tidak terdaftar. Pada upaya ketiga kali menggunakan sidik jari yang tidak terdaftar, sistem mengirimkan notifikasi melalui Thinger.io, yang menunjukkan bahwa mekanisme ini berfungsi dengan baik. Visualisasi dari proses pengujian keamanan ini ditampilkan pada Gambar 6 di atas, yang memperlihatkan pemindaian sidik jari yang tidak terdaftar hingga pengiriman notifikasi setelah upaya pembobolan ketiga. Dan pada Gambar 7 menunjukkan notifikasi email yang berisi peringatan serta lokasi upaya dan status sidik jari yang tidak terdaftar pada email pengguna.

3.5 Implementasi Alat

Pada tahap ini, implementasi alat dilakukan dengan memasang langsung pada pintu ruangan prodi Teknik Informatika. Pada Gambar 8 dan 9 akan ditampilkan kondisi pintu ruangan prodi Teknik Informatika sebelum dan sesudah pemasangan alat yang telah selesai dibuat. Perangkat keras seperti NodeMCU, modul fingerprint, buzzer, relay, dan tombol fisik akan terlihat terintegrasi dalam satu rangkaian. Proses ini menjamin bahwa sistem dapat berfungsi dengan baik dan sesuai dengan spesifikasi

yang dibutuhkan untuk meningkatkan keamanan akses pintu.

Gambar 8. Pintu Sebelum Dipasang Alat

Dari Gambar 8 diatas menunjukkan kondisi pintu ruangan Prodi Teknik Informatika sebelum alat pengendalian akses dipasang. Pintu ini belum dilengkapi dengan perangkat keras seperti NodeMCU, modul fingerprint, buzzer, relay, dan tombol fisik push button.

Gambar 9. Pintu Setelah Dipasang Alat

Pada Gambar 9, terlihat pintu ruangan Prodi Teknik Informatika setelah alat dipasang. Fingerprint yang telah terintegrasi terpasang dengan rapi dan berfungsi sesuai dengan spesifikasi yang ditetapkan.

Gambar 10. Tampilan Alat Dari Dalam Ruangan

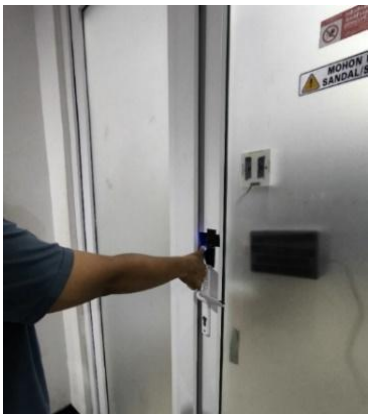
Gambar 10 menampilkan tampilan dari dalam ruangan, menunjukkan bagaimana perangkat keras seperti NodeMCU, dan tombol fisik terpasang di pintu. Tampilan ini memberikan gambaran mengenai bagaimana pengguna dapat berinteraksi dengan alat untuk membuka pintu secara manual.

3.6 Pengoperasian Alat Yang Telah Diimplementasikan

Pada bagian ini, ditampilkan beberapa pengujian yang menunjukkan cara pengoperasian alat pengendalian akses yang telah diimplementasikan di pintu ruangan Prodi Teknik Informatika.

3.6.1 Pengujian Sidik Jari Untuk Membuka Pintu

Pada Gambar 11 dibawah menampilkan proses autentikasi pengguna dengan sensor sidik jari. Sistem akan memverifikasi sidik jari yang ditempelkan pada sensor. Jika sidik jari tersebut terdaftar dalam sistem, pintu masuk akan terbuka. Gambar ini menunjukkan bagaimana pengguna dapat dengan mudah mengakses ruangan dengan hanya menggunakan sidik jari mereka untuk meningkatkan keamanan dan kemudahan akses.



Gambar 11. Pengujian Sidik Untuk Membuka Pintu

Tabel 4. Pengujian Keseluruhan Sistem Pada Fingerprint

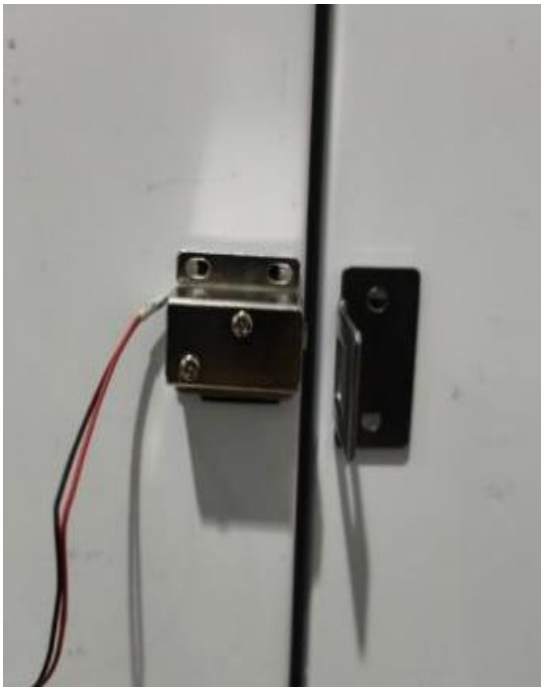
Jari Yang Digunakan	Input		Oouptput			
	Fingerprint	***Relay***	***Buzzer***	**Percobaan Gagal**	**Notifikasi Thinger.Io**	**Respon Solenoid**
Ibu Jari Kanan	Valid	On	Berbunyi Sekali	0	Off	On
Jari Telunjuk Kanan	Valid	On	Berbunyi Sekali	0	Off	On
Jari Kelingking Kanan	Valid	On	Berbunyi Sekali	0	Off	On
Ibu Jari Kiri	Invalid	Off	Berbunyi Dua Kali	1	Off	Off
Jari Telunjuk Kiri	Invalid	Off	Berbunyi Dua Kali	1	Off	Off
Jari Kelingking Kiri	Invalid	Off	Berbunyi Dua Kali	3	On	Off

Pada Tabel pengujian 4 diatas, secara rinci menjelaskan respon sistem terhadap berbagai sidik jari yang diuji. Tabel ini mencatat penggunaan sidik jari yang valid dan invalid dari berbagai jari pada kedua tangan, dengan mencatat input (validitas sidik jari), serta output berupa aktivasi relay (untuk membuka pintu), respon bunyi buzzer (sebagai indikasi akses yang berhasil atau tidak), notifikasi ke platform Thinger.io setelah 3 percobaan akses yang tidak berhasil, dan respon solenoid yang mengontrol penguncian pintu. Data ini memberikan gambaran tentang kemampuan sistem dalam mengelola akses pengguna berdasarkan verifikasi sidik jari, dan menguji validitas hipotesis keamanan serta kemudahan akses dalam sistem yang dikembangkan.

3.6.2 Pengujian Push Button Untuk Membuka Pintu Dari Dalam

Tombol push button dipasang di dekat pintu dan berfungsi sebagai alternatif dalam mengendalikan akses pintu secara manual. Sinyal dari tombol push diteruskan ke solenoid lock, yang mengendalikan mekanisme penguncian pintu. Integrasi antara tombol push dan solenoid lock dirancang untuk memberikan respon yang cepat dan handal dalam membuka pintu.

Gambar 12. Pengguna Menekan Push Button



Gambar 13. Respon Solenoid Door Lock

Saat push button ditekan, solenoid lock secara otomatis merespon dengan membuka pengunci pintu. Proses ini memastikan bahwa pengguna dapat dengan cepat memperoleh akses ke dalam ruangan tanpa memerlukan autentikasi sidik jari. Pengujian yang dilakukan menunjukkan bahwa tombol push dan solenoid lock beroperasi secara konsisten dan dapat diandalkan dalam situasi darurat maupun kondisi normal penggunaan sehari-hari. Integrasi antara tombol push dan solenoid lock juga memperkuat keamanan dan efisiensi dalam pengelolaan akses ke ruangan.

Tabel 5 menunjukkan bahwa sistem push button bekerja dengan cepat dan handal. Saat tombol ditekan, solenoid lock segera membuka pintu dalam waktu kurang dari 1 detik. Sistem ini juga didukung oleh powerbank yang berfungsi normal, memastikan kinerja tetap stabil meskipun terjadi kegagalan daya utama.

Tabel 5. Pengujian Keseluruhan Sistem Pada Push Button

Pengujian	Input		Output		
	Push Button	**Relay**	**Waktu Respon**	**Respon Solenoid**	**Sumber Daya Cadangan**
Tombol Ditekan	Ditekan	On	Kurang Dari 1 Detik	On	Powerbank Normal
Tombol Tidak Ditekan	Tidak Ditekan	Off	-	Off	Powerbank Normal

4. Kesimpulan

Penelitian ini berhasil menerapkan sistem keamanan berbasis sidik jari menggunakan NodeMCU dan Thinger.io pada ruangan Prodi Teknik Informatika Universitas Muhammadiyah Kalimantan Timur. Sistem ini efektif dalam mengidentifikasi dan mengautentikasi pengguna dengan tingkat kesalahan yang rendah, serta mampu memberikan respon cepat dalam membuka atau mengunci pintu. Manfaat utama dari sistem ini adalah peningkatan keamanan ruangan dan pencegahan akses tidak sah, serta kemampuan pemantauan secara real-time melalui Thinger.io.

Namun, penelitian ini memiliki beberapa keterbatasan, seperti ketergantungan pada koneksi internet untuk pemantauan jarak jauh dan performa sensor sidik jari dalam kondisi tertentu. Penelitian lanjutan disarankan untuk mengembangkan sistem yang lebih tahan terhadap gangguan koneksi internet. Implikasi penelitian ini menunjukkan potensi besar dalam penerapan sistem keamanan berbasis teknologi sidik jari di berbagai lingkungan, memberikan kontribusi nyata dalam peningkatan keamanan berbasis teknologi.

Daftar Pustaka:

Anwar, N., Widodo, A. M., Tundjungsari, V., Ichwani, A., Muiz, K. H., & Yulhendri, Y. (2021). Sistem Pemantauan Level Keasaman dan Total Dissolved Solids Limbah Cair Berbasis Internet of Things (IoT). *Prosiding SISFOTEK*, *5*(1), 21–26. https://scholar.google.com/citations?view_op=view_citation&hl=en&user=FOwZ8hUAAAAJ&pagesize=100&citation_for_view=FOwZ8hUAAAAJ:OP4eGU-M3BUC

Bachtiar, A. H. (2022). Rancang Bangun Dual Keamanan Sistem Pintu Rumah Menggunakan Pengenalan Wajah Dan Sidik Jari Berbasis Iot (Internet of Things). *Power Elektronik: Jurnal Orang Elektro*, *11*(1), 102. https://doi.org/10.30591/polektro.v11i1.3137

Dewi, I. P., & Fikri, R. (2023). Optimalisasi Keamanan Rumah dengan Implementasi Sistem Notifikasi Gerbang Cerdas Berbasis Internet of Things (IoT). *Journal of Computer System and Informatics (JoSYC)*, *4*(4), 816–829. https://doi.org/10.47065/josyc.v4i4.4004

Gupta, K., Jiwani, N., Sharif, M. H. U., Mohammed, M. A., & Afreen, N. (2022). Smart Door Locking System Using IoT. *2022 International Conference on Advances in Computing, Communication and Materials, ICACCM 2022*, *May*, 3090–3094. https://doi.org/10.1109/ICACCM56405.2022.10009534

Handika, R., Hartama, D., Kirana, I. O., Safii, M., & Parlina, I. (2021). Prototype Alat Pengamanan Pintu dengan Menggunakan Sensor Sidik Jari Berbasis Arduino Mega2560. *Kajian Ilmiah Informatika Dan Komputer*, *1*(6), 240–247.

Jodi, S., Siregar, M., Asmira, A., & Kusumawati, N. (2022). Prototype Sistem Keamanan Pintu Rumah Menggunakan Tag Card dan PIN Berbasis Arduino Uno. *Simkom*, *7*(2), 82–91. https://doi.org/10.51717/simkom.v7i2.83

Khalid, Z., Achmady, S., & Agustini, P. (2020). Otomatisasi Sistem Keamanan Kunci Lemari Menggunakan Sensor Sidik Jari Berbasis Arduino Uno. *Jurnal TEKSAGRO*, *1*(1), 1–11. https://journal.lp2stm.or.id/index.php/TEKSAGRO/article/view/1

Lagan, M. D., & Ary, M. (2021). Sistem Kendali Kunci Pintu Menggunakan Voice Command Berbasis Internet of Things (Iot). *EProsiding Teknik Informatika (PROTEKTIF)*, *2*(1), 1–12. http://eprosiding.ars.ac.id/index.php/pti/article/view/219

Nagarkar, D., & Kadam, A. (2023). *FINGERPRINT SECURITY SYSTEM USING ARDUINO*. *05*, 7665–7675.

Ningrum, N. K., & Basyir, A. (2022). PERANCANGAN SISTEM KEAMANAN PINTU RUANGAN OTOMATIS MENGGUNAKAN RFID BERBASIS INTERNET OF THINGS (IoT). *Jurnal Ilmiah Matrik*, *24*(1), 21–27. https://doi.org/10.33557/jurnalmatrik.v24i1.1651

Nugroho, I. I., Pratiwi, R., & Az Zahro, S. R. (2021). Optimalisasi Penanggulangan Kebocoran Data Melalui Regulatory Blockchain Guna Mewujudkan Keamanan Siber di Indonesia. *Ikatan Penulis Mahasiswa Hukum Indonesia Law Journal*, *1*(2), 115–129. https://doi.org/10.15294/ipmhi.v1i2.53698

Prasetyo Eka Putra, F., Mellyana Dewi, S., & Hamzah, A. (2023). Privasi dan Keamanan Penerapan IoT Dalam Kehidupan Sehari-Hari :

Tantangan dan Implikasi. *Jurnal Sistim Informasi Dan Teknologi*, *5*(2), 26–32. https://doi.org/10.37034/jsisfotek.v5i1.232

Rahayu, E. S., & Nurdin, R. A. M. (2019). Perancangan Smart Home Untuk Pengendalian Peralatan Elektronik Dan Pemantauan Keamanan Rumah Berbasis Internet of Things. *Jurnal Teknologi*, *6*(2), 136–148. https://doi.org/10.31479/jtek.v6i2.23

Sari, I. P., Hazidar, A. H., Basri, M., Ramadhani, F., & Manurung, A. A. (2023). Penerapan Palang Pintu Otomatis Jarak Jauh Berbasis RFID di Perumahan. *Blend Sains Jurnal Teknik*, *2*(1), 16–25. https://doi.org/10.56211/blendsains.v2i1.246

Wee, B. S. (2021). Design and Implementation of an Arduino Based Smart Fingerprint Authentication System for Key Security Locker. *International Applied Business and Engineering Conference*, 155–160.

Halaman ini sengaja dikosongkan