

Pengembangan Sistem Keamanan Pintu Menggunakan Fingerprint dengan Sistem Notifikasi Berbasis IoT (*Internet Of Things*)

Yusuf Mapeasse¹, Hilda Ashari², Hasrul Bakri³

Universitas Negeri Makassar

Email: hildaashari@unm.ac.id

Abstrak. Penelitian ini merupakan penelitian dan pengembangan atau *research and development* (R&D). Penelitian bertujuan untuk menghasilkan sistem keamanan pengunci pintu menggunakan *fingerprint & smartphone* berbasis *Internet of Things* (IoT) dan mengetahui hasil pengujian sistem tersebut menggunakan standar ISO/IEC 25010. Model penelitian yang digunakan yaitu model pengembangan *prototype*. Tahapan dalam pengembangan model *prototype* adalah 1) Analisis kebutuhan; 2) Membangun *prototyping*; 3) Evaluasi *prototyping*; 4) Pengkodean sistem (*coding*); 5) Menguji sistem; 6) Evaluasi sistem; dan 7) Implementasi sistem. Teknik pengumpulan data yang digunakan dalam penelitian ini adalah kuesioner (angket) untuk pengujian *black box testing* dan wawancara. Teknik analisis data menggunakan teknik analisis deskriptif untuk menjelaskan suatu data dengan mendeskripsikannya sehingga didapatkan kesimpulan dari data tersebut. Hasil penelitian diperoleh dengan melakukan uji coba sistem di berbagai tempat antara perangkat dan sistem yaitu aplikasi *smart doorlock* dapat mengakses sistem kontrol pintu ditempat yang berbeda apabila *smartphone* terhubung dengan internet dan sistem kontrol pintu tetap terhubung dengan koneksi wifi, dan perangkat solenoid membutuhkan waktu 3 detik untuk membuka pintu secara otomatis.

Kata Kunci: Research and Development (R&D), Fingerprint, Internet of Things (IoT), ISO/IEC 25010

PENDAHULUAN

Sistem keamanan pada umumnya diperlukan untuk mengamankan suatu objek yang berisi hal-hal penting untuk diamankan seperti rumah, sekolah, kantor, rumah sakit, dan industri (Widya Dharma et al., 2018). Sistem keamanan sangat diperlukan untuk mencegah peningkatan jumlah tindak kejahatan pencurian atau tindak kejahatan kriminal lainnya, seperti seringkali terjadi kejadian pencurian melalui pintu. Sistem keamanan pintu dengan menggunakan kunci konvensional yang banyak digunakan oleh masyarakat mudah sekali dilumpuhkan oleh pelaku tindak kejahatan (Dindha Amelia, 2020). Selain itu dengan menggunakan kunci konvensional dalam sistem pengamanan juga kurang terpercaya karena kunci konvensional mudah hilang dalam penggunaannya dan mudah diduplikat, sehingga sistem ini dirasa kurang praktis dan rentan terhadap tindakan pencurian (Andi, 2015).

Berdasarkan studi pendahuluan yang dilakukan di ruang dosen, admin, dan pimpinan Jurusan Pendidikan Teknik Elektro Fakultas Teknik Universitas Negeri Makassar pada tanggal 20 Maret 2023, peneliti melakukan wawancara dengan beberapa dosen, ditemukan fakta bahwa di ruang dosen telah terjadi beberapa kali terjadi pencurian barang pribadi dikarenakan sistem keamanan yang ada di ruangan tersebut masih rendah. Sistem keamanan pintu masih menggunakan kunci konvensional, dimana sering terjadi *human error* karena lupa mengunci pintu. Berdasarkan permasalahan tersebut, maka dibutuhkan suatu perangkat teknologi sebagai solusi untuk meningkatkan keamanan pintu ruang dosen, admin, dan pimpinan di JPTE.

Perangkat teknologi yang tercipta sederhana dan dikelola secara tepat akan sangat membantu aktivitas kehidupan manusia sehari-hari. Sejumlah sistem pengaman moderen telah diciptakan antara lain dengan menggunakan sistem suara, sistem pengenalan wajah, sistem penggunaan kartu dan sistem *fingerprnt* (H et al., 2019). Dari semua sistem pengaman ini memiliki tingkat kelemahan yang berbeda-beda. Sistem keamanan dengan suara seringkali dapat di sabotase karena banyak manusia yang dapat menirukan suara manusia lain, hal ini sering kali mudah diatasi oleh pencuri profesional. Sistem keamanan dengan pengenalan wajah memiliki masalah salah satunya yaitu sulit mendapatkan gambar wajah dengan beragam pose seseorang pada umur yang berbeda (Asad et al., 2015). Sistem keamanan kartu juga memiliki masalah yang sama ketika menggunakan kunci konvensional yaitu kartu harus dibawa terus-menerus yang bisa saja terjadi *human error* lupa membawa kartu tersebut. Dan selanjutnya Sistem keamanan *fingerprnt* yang dimana sistem ini sebagai sistem yang tingkat kelemahannya paling rendah dan memiliki tingkat keamanan serta kelebihan yang tinggi dari berbagai sistem yang telah dijelaskan sebelumnya. Kelebihan sistem *fingerprnt* salah satunya yaitu hanya dapat diakses oleh pemilik sidik jari (Imran & Rasul, 2020).

Penerapan teknologi *fingerprnt* yang dikombinasikan dengan *smartphone* berbasis *Internet of Things* (IoT) yang merupakan bagian dari teknologi informatika dan dapat diterapkan pada perangkat elektronika. Istilah *Internet of Things* (IoT) telah ramai dibicarakan orang tetapi masih banyak yang belum mengenalnya, IoT ini mengacu pada identifikasi suatu benda (objek) yang diinterpretasikan secara visual melalui jaringan kabel ataupun nirkabel ke dunia maya (internet) kemudian diolah menggunakan perangkat lunak aplikasi khusus untuk mendapatkan informasi (Nuraeni et al., 2021).

Perkembangan dari teknologi identifikasi *fingerprnt* yang dikombinasikan *smartphone* berbasis *Internet of Things* (IoT) sudah mulai berkembang dan dapat diimplementasikan pada kehidupan sehari-hari. Teknologi identifikasi *fingerprnt* dan *smartphone* adalah salah satu sistem keamanan yang tinggi karena menggunakan sidik jari dan aplikasi yang sudah diinstal pada *smartphone* sebagai sistem untuk membuka

pintu (M et al., 2023). Dengan sidik jari yang berbeda satu dengan yang lainnya maka orang yang tidak terdaftar didalam sistem tersebut tidak dapat megaksesnya. Begitu juga dengan menggunakan teknologi *smartphone* berbasis *Internet of Things* (IoT) dapat mengendalikan pengunci pintu ruangan dengan sistem yang dapat di buka dan dimonitoring dari mana saja menggunakan aplikasi yang sudah diinstal pada *smartphone* (Saputro & Wibawanto, 2016).

Dalam penggunaan sistem keamanan pintu menggunakan sensor *fingerprint* dan aplikasi *smartphone*. Semua *user* yang menggunakan sistem ini akan terdaftar pada database Sehingga segala aktivitas membuka pintu akan terekam dan dapat diakses secara langsung oleh pemilik ruangan. Berdasarkan latar belakang permasalahan diatas penulis akan melakukan penelitian di Jurusan Pendidikan Teknik Elektro Universitas Negeri Makassar. Dengan mengambil judul penelitian "Pengembangan Sistem Keamanan Pintu Menggunakan *Fingerprint* Dengan Sistem Notifikasi Berbasis lot (*Internet of Things*)".

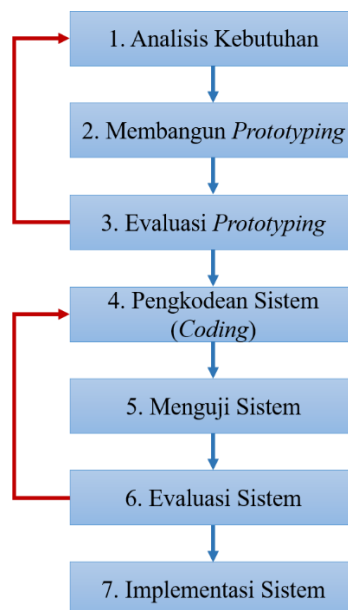
METODE PENELITIAN

A. Metode Penelitian

Pada penelitian ini model pengembangan yang digunakan yaitu model pengembangan *prototype* bertujuan untuk mengumpulkan informasi dari pelanggan sehingga pengguna dapat berinteraksi dengan model *prototype* yang dikembangkan (Sugiono, 2017).

B. Model Pengembangan

Tahapan pengembangan model *prototyping* adalah sebagai berikut:



Gambar 1. Tahapan Model Pengembangan *Prototyping*

1) Analisis Kebutuhan

Pengguna dan pengembang bersama-sama mendefinisikan format seluruh perangkat lunak, mengidentifikasi semua kebutuhan, dan garis besar sistem yang akan dibuat.

2) Membangun *Prototyping*

Membangun *prototype* dengan membuat perancangan sementara yang berfokus pada penyajian kepada pengguna (misalnya dengan membuat input dan format output).

3) Evaluasi *Prototype*

Evaluasi ini dilakukan oleh pengguna apakah *prototype* yang sudah dibangun sudah sesuai dengan keinginan pengguna. Jika sudah sesuai maka langkah 4 akan diambil. Jika tidak, *prototype* direvisi dengan mengulang langkah 1, 2, dan 3.

4) Mengkodekan Sistem (*Coding*)

Dalam tahap ini *prototyping* yang sudah disepakati diterjemahkan ke dalam bahasa pemrograman yang sesuai.

5) Menguji Sistem

Setelah sistem sudah menjadi suatu perangkat lunak yang siap pakai, harus dites dahulu sebelum digunakan. Pengujian ini dilakukan dengan ISO 25010 pada karakteristik *functionality* dan *usability*.

6) Evaluasi Sistem

Pengguna mengevaluasi apakah sistem yang sudah jadi sudah sesuai dengan yang diharapkan. Jika ya, langkah 7 dilakukan; jika tidak, ulangi langkah 4 dan 5.

7) Implementasi Sistem

Perangkat lunak yang telah diuji dan diterima pengguna siap untuk digunakan.

C. Teknik Pengumpulan Data

Teknik Pengumpulan data yang dilakukan dalam penelitian ini adalah:

1. Wawancara

Wawancara yaitu teknik pengumpulan data dengan cara mengadakan tanya jawab secara langsung dengan narasumber terkait dengan permasalahan yang diambil untuk memperoleh data dan informasi. Wawancara yang digunakan pada penelitian ini adalah wawancara tidak terstruktur.

2. Kuesioner (Angket)

Teknik kuesioner atau angket yang akan dilakukan peneliti digunakan untuk

mendapatkan data yang terkait dengan pengujian *Black Box testing* dan untuk memperoleh data kepuasan pengguna. Teknik kuesioner juga dilakukan untuk melakukan validasi instrumen. Pengujian dengan menggunakan metode kuesioner yaitu instrumen *test case*. *Test case* merupakan sekumpulan *input* yang akan diuji, kondisi yang harus dieksekusi dan hasil yang diharapkan (Santoso, 2015).

D. Teknik Analisis Data

Teknik analisis data pada penelitian ini menggunakan teknik analisis deskriptif. Teknik analisis deskriptif yaitu statistik yang digunakan untuk menjelaskan suatu data dengan mendeskripsikannya sehingga didapatlah kesimpulan dari sekelompok data tersebut. Analisis dilakukan berdasarkan aspek kualitas perangkat lunak ISO 25010. Teknik analisa data dalam penelitian ini adalah menggunakan analisis deskriptif dengan rumus perhitungan sebagai berikut (Sugiono, 2017).

$$PF = \frac{\text{skor yang diperoleh}}{\text{skor yang diharapkan}} \times 100\%$$

Setelah mendapatkan data skor dari hasil pengujian presentase *functionality*, kemudian dihitung persentasenya dengan menggunakan rumus tersebut. Setelah itu, presentase dikonversikan ke dalam pernyataan sesuai dengan Tabel 1.

Tabel 1. Interpretasi Persentase

No	Persentase <i>functionality</i> (%)	Interpretasi
1	> 80 – 100	Sangat Baik
2	> 60 - 80	Baik
3	> 40 - 60	Cukup Baik
4	> 20 - 40	Kurang Baik
5	≤ 20	Sangat Tidak Baik

HASIL DAN PEMBAHASAN

Hasil Penelitian

Penelitian ini menghasilkan *prototype* sistem keamanan pintu menggunakan *fingerprint* berbasis *Internet of Things* (IoT) yang dapat mengunci pintu secara otomatis dan membuka pintu menggunakan sidik jari dan atau menggunakan aplikasi pada *smartphone*. Sistem ini terdiri dari 2 perangkat, yaitu perangkat sensor dan perangkat solenoid. Perangkat sensor merupakan perangkat utama yang terdiri dari mikrokontroler ESP32, sensor *fingerprint*, dan LCD. Perangkat sensor ini dipasang pada luar pintu sebagai akses manual untuk membuka pintu. Kemudian perangkat yang kedua adalah perangkat modul solenoid. Perangkat solenoid ini di pasang dibagian dalam pintu sebagai alat pengunci pintu. Pada sistem ini pengguna dapat membuka pintu dengan menggunakan aplikasi *smart doorlock* di *smartphone* atau menggunakan sidik jari yang telah terdaftar pada perangkat sensor, kunci pintu akan otomatis terkunci 3 detik setelah terbuka.

1. Perancangan Sistem *Fingerprint Smart Doorlock*

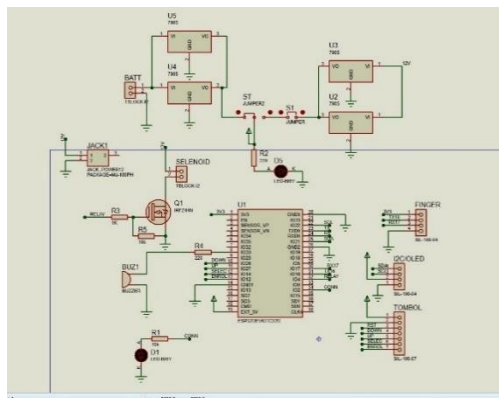
Perancangan sistem *smart doorlock* dibagi menjadi beberapa tahap yaitu:

a) Desain skematik dan PCB *Layout Fingerprint smart doorlock*

Tahap pertama pembuatan perangkat *fingerprint smart doorlock* dimulai dengan pembuatan skematik rangkaian. Pembuatan skematik menggunakan *software proteus 8 profesional*. Berikut adalah hasil desain skematik *finger print door lock*.

b) Skematik skematik perangkat kunci pintu

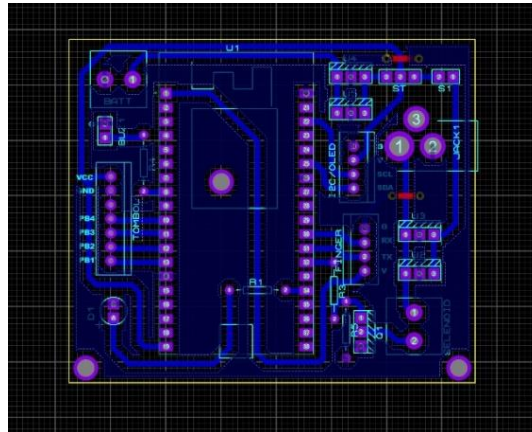
Perangkat sensor terdiri dari beberapa komponen yaitu *esp32*, sensor *fingerprint*, LCD, regulator terdangan, buzzer, dan 2 buah *push button*. Sensor *fingerprint* terhubung dengan Serial 2 pada *esp32* yaitu pin TX1 dan RX1 sebagai jalur komunikasi data. LCD terhubung pada pin SDA dan SCL *esp32* sebagai jalur pertukaran data untuk menampilkan karakter. Buzzer terhubung pada pi IO4 yang berfungsi sebagai indikator bunyi. *Push button* terhubung pada pin reset yang berfungsi untuk mereset perangkat jika terjadi *error*.



Gambar 2. Skematik Perangkat IoT *Smart doorlock*

c) *Printed Circuit Board (PCB) Layout Smart doorlock*

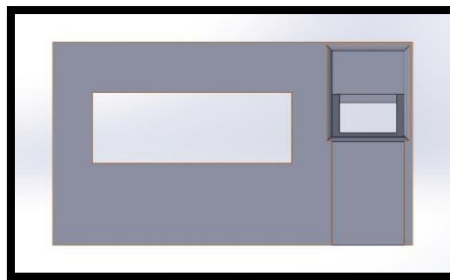
Printed Circuit Board (PCB) Layout merupakan gambar jalur rangkaian yang akan dicetak pada papan *Printed Circuit Board (PCB)*. Desain *PCB layout* ini dibuat menggunakan *software proteus 8 profesional*. Jalur yang sudah didesain dicetak menggunakan printer laser jet menggunakan kertas kinstruk. Kemudian disetrika pada papan PCB yang telah di bersikan. PCB berfungsi agar semua komponen dihubungkan menjadi satu tanpa harus menggunakan kabel. Hasil desain jalur *PCB layout* dapat dilihat pada Gambar 3.



Gambar 3. PCB Layout Perangkat IoT Smart doorlock

d) Desain Casing *Fingerprint smart doorlock*

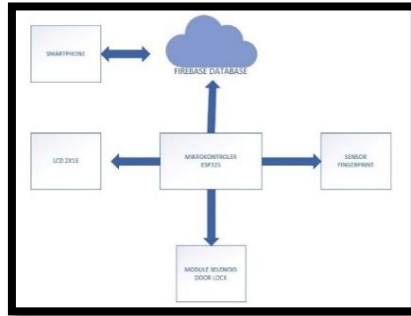
Desain casing *fingerprint smart doorlock* dibuat menggunakan *software* 3D Solidworks 2020. Model dan ukuran desain disesuaikan dengan kebutuhan komponen perangkat sensor *fingerprint smart doorlock*. Hasil desain selanjutnya akan dicetak menggunakan mesin 3D printer. Hasil desain casing dapat dilihat pada gambar 4.



Gambar 4. Tampilan Casing IoT Smart doorlock

2 Hasil Perancangan Sistem Keseluruhan

Sistem *fingerprint smart doorlock* memiliki 2 perangkat *Embended System* yang saling terhubung melalui protokol ESP32. Perangkat tersebut antara lain yaitu Perangkat Sensor dan Perangkat Selenoid. Perangkat sensor adalah perangkat utama atau master yang akan memberikan perintah. Hanya perangkat sensor yang terhubung langsung ke database melalui koneksi WiFi. Perangkat sensor terdiri dari beberapa komponen yaitu Esp32, LCD, dan Sensor *fingerprint*. Perangkat selenoid merupakan perangkat kunci pintu yang akan membuka atau menutup bila mendapat perintah dari perangkat sensor.



Gambar 5. Hasil Perancangan Sistem Keseluruhan

3. Hasil Perakitan dan Penkodean Perangkat

Setelah rancangan perangkat keras selesai, selanjutnya dilakukan proses perakitan komponen satu per-satu sesuai skema yang telah didesain sehingga menjadi perangkat *smart doorlock* yang siap diprogram secara keseluruhan.

a) Perakitan Perangkat Sensor

Perangkat sensor terdiri dari beberapa komponen yaitu ESP32, sensor *fingerprint*, LCD, dan 2 buah push button. ESP32 merupakan mikrokontroler utama yang memproses semua data pada perangkat sensor. Sensor *fingerprint* memiliki 4 pin yang terhubung dengan ESP32 dari 6 total pin pada sensor *fingerprint*. Pin tx dan rx sensor *fingerprint* terhubung dengan serial 2 ESP32 yaitu pin TX1 dan RX1 sebagai jalur komunikasi serial. Kemudian pin 3v3 pada sensor *fingerprint* terhubung ke pin 3v3 ESP32 dan pin GND pada sensor terhubung ke pin GND pada ESP32. LCD memiliki 4 pin yaitu VCC, GND, SCL, dan SDA. Pin VCC dan GND LCD terhubung dengan pin VCC dan GND ESP32. Pin SDA dan SCL LCD terhubung dengan pin SDA dan SCL ESP32. Kemudian 2 buah *push button* terhubung pada pin RESET dan GPIO 15 ESP32. Hasil perakitan perangkat sensor dapat dilihat pada Gambar 6.



Gambar 6. Perakitan Perangkat Sensor

b) Perakitan Perangkat Selenoid

Perangkat selenoid terdiri dari ESP32, Selenoid *smart doorlock*, transistor TIP31, regulator 7805, resistor 1 k ohm dan 2 buah kapasitor 100 uf. Selenoid di switch oleh TIP31 dengan resistor pada pin basis nya. Selenoid memiliki tegangan kerja 12 volt

sehingga memerlukan regulator 5v yaitu 7805 untuk *supply* tegangan ke mikrokontroler ESP32. Kapasitor dipasang pada pin input dan pin output 7805 untuk membuat tegangan menjadi stabil.

c) Pembuatan kode program

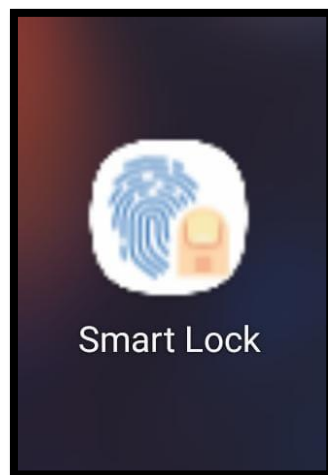
Pembuatan kode program perangkat menggunakan *software* Arduino IDE. Tiap perangkat pada *fingerprint smart doorlock* memiliki program yang berbeda. Setelah program selesai dibuat selanjutnya akan di upload ke perangkat *fingerprint smart doorlock*.

d) Hasil Pengkodean Aplikasi

Sistem *fingerprint smart doorlock* dapat di kontrol menggunakan aplikasi yang terhubung ke jaringan internet dan terkoneksi langsung dengan database firebase. *Software* yang digunakan dalam pembuatan aplikasi ini adalah android studio. Perangkat bahasa pemrograman yang digunakan adalah bahasa java. Berikut ini adalah bagian tampilan yang ada pada aplikasi.

e) Tampilan ikon aplikasi

Ikon Aplikasi adalah gambar yang digunakan untuk mewakili aplikasi yang telah di instal pada perangkat. Ikon ini akan ditampilkan pada bagian pengaturan dan pencarian.



Gambar 7. Tampilan Ikon Aplikasi

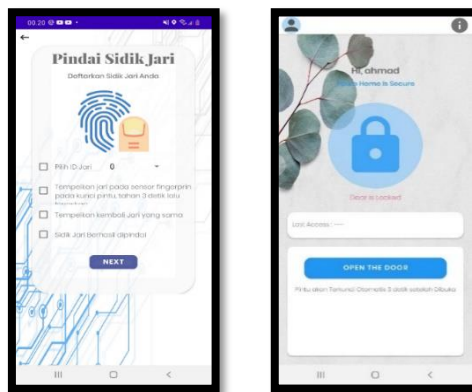
f) Halaman login dan register

Halaman Login adalah halaman proses untuk masuk ke beranda aplikasi. Pengguna dapat memasukkan Email dan *Password* yang sudah terdaftar pada halaman ini. Email yang sudah didaftarkan harus di verifikasi terlebih dahulu melalui email yang dikirimkan oleh firebase. Jika pengguna belum terdaftar maka akan di arahkan ke halaman registrasi. Halaman registrasi merupakan halaman untuk membuat akun bagi

pengguna baru. Pada halaman ini terdapat beberapa *form* yang harus diisi seperti nama, email, dan *password*. Informasi yang diisi pada halaman ini akan disimpan sebagai informasi *user* pada database firebase. Data ini lah kemudian yang akan digunakan oleh *user* untuk login pada aplikasi

g) Halaman Verifikasi sidik jari dan Beranda Halaman

Verifikasi sidik Jari merupakan halaman untuk menverifikasi sidik jari pengguna baru. Pengguna akan di minta untuk memilih id jari lalu mengikuti prosedur registrasi yang tertulis. Halaman Beranda merupakan halaman utama aplikasi. Halaman ini berisi beberapa tombol kontrol. Pengguna juga dapat melihat jaraknya dengan rumahnya pada aplikasi serta melihat riwayat akses pintu.



Gambar 8. Halaman Register *fingerprint* dan Beranda

4. Hasil Pengujian ISO 25010

a. Hasil Pengujian *functionality*

Pengujian faktor kualitas *functionality* dalam penelitian ini menggunakan metode *black box testing*. Dalam hal ini, penilaian dilakukan berdasarkan instrumen berupa *test case*. Instrumen pengujian fungsionalitas berisi 10 pertanyaan terkait fungsi-fungsi yang didesain dalam alat yang dikembangkan. Instrumen *functionality* divalidasi oleh dua dosen ahli alat. Setiap fungsi berjalan dengan baik maka ahli akan memberikan *checklist* pada kolom “Ya” sementara bila fungsi tidak berjalan dengan baik maka dosen ahli akan memberikan *checklist* pada kolom “Tidak”.

b. Hasil Pengujian *Usability*

Pengujian aspek *usability* dilakukan dengan metode instrument dengan skala Likert. Faktor kualitas *usability* yang digunakan dalam penelitian adalah hasil penelitian dari responden.

5. Pengujian Fungsional Aplikasi *Smart doorlock*

Pengujian fungsional aplikasi *smart doorlock* dilakukan untuk mengetahui seberapa jauh aplikasi *smart doorlock* dapat mengakses sistem. Pengujian ini dilakukan

dengan cara mengakses sistem dengan aplikasi *smart doorlock* dari beberapa jarak tempat yang berbeda dan melihat data yang dikirim pada database firebase. Pengujian dilakukan sebanyak 4 kali. Data hasil pengujian dapat dilihat pada Tabel 2.

Tabel 2. Tabel Pengujian Tombol Kunci Pintu Pada Aplikasi *Smart Doorlock*

Pengujian ke-n	Tempat (jarak)	Aspek Yang diuji	Lama Waktu Terbuka	Terkunci otomatis
1	(± 4 m)	Tombol Buka pintu	3 Detik	✓
2	(± 10m)	Tombol Buka pintu	3 Detik	✓
3	(± 50m)	Tombol Buka pintu	3 Detik	✓
4	(± 100m)	Tombol Buka pintu	3 Detik	✓

Berdasarkan tabel hasil pengujian, Aplikasi *smart doorlock* dapat mengakses sistem kontrol pintu ditempat yang berbeda apabila *smartphone* terhubung dengan internet dan sistem kontrol pintu tetap terhubung dengan koneksi wifi, pada pengujian tersebut menggunakan akses wifi “SSO_UNM_backup”. Ketika tombol kunci pintu ditekan maka akan mengirim data “1” ke *realtime database*. Kunci pintu akan terkunci otomatis setelah terbuka 3 detik. Selanjutnya data pengguna yang membuka kunci pintu akan masuk secara otomatis kedalam menu riwayat akses aplikasi *smart doorlock*. layak untuk digunakan.

6. Pengujian Fungsional *Fingerprint*

Pengujian fungsional *fingerprint* dilakukan untuk mengetahui respon sensor sidik jari terhadap selenoid dan. Pengujian ini dilakukan dengan cara mengakses sistem dengan *fingerprint* oleh beberapa pengguna (multi *user*) dan melihat data yang dikirim pada database firebase. Pengujian dilakukan dengan 2 *user*. Data hasil pengujian dapat dilihat pada Tabel 3.

Tabel 3. Pengujian Fungsional *Fingerprint*

User	Status <i>fingerprint</i>	Respon Selenoid
User 1	Terdaftar	Terbuka
User 2	Tidak Terdaftar	Terkunci

Berdasarkan tabel hasil pengujian, apabila sidik jari yang telah terdaftar pada sistem ditempelkan pada sensor *fingerprint* maka selenoid akan merespon untuk membuka pengunci pintu dan jika sidik jari yang belum terdaftar ditempelkan pada sensor *fingerprint* maka selenoid tidak akan merespon dan pintu akan tetap terkunci.

7. Pengujian Koneksi Wifi ke Sistem *Smart doorlock*

Pengujian koneksi wifi ke sistem *smart doorlock* dilakukan untuk mengetahui sejauh mana sistem *smart doorlock* menjangkau koneksi wifi internet. Data hasil pengujian dapat dilihat pada Tabel 4.

Tabel 5. Pengujian Koneksi Wifi

Pengujian ke-n	Wifi	Tempat	Data yang Diperoleh
1	SSO_UNM_backup	Gedung JPTE	85% (-60 dBm)
2	Wifi <i>Smartphone</i>	Lab JPTE	99% (-40 dBm)
3	Wifi <i>Smartphone</i>	Lantai 2 JPTE	36% (-76 dBm)
4	Wifi <i>Smartphone</i>	Parkiran JPTE	0%

Berdasarkan tabel hasil pengujian, akurasi wifi yang terdapat pada gedung JPTE menghasilkan data 85% (-60 dBm). Untuk wifi *smartphone* memperoleh data 99% (-40 dBm) ketika wifi *smartphone* berdekatan dengan sistem *smart doorlock* di lab JPTE dan data kedua diperoleh 36% (-76 dBm) ketika wifi *smartphone* diletakkan ditangga lantai 2 JPTE yang berjarak 8 meter dari sistem *smart doorlock*. Jika wifi *smartphone* diletakkan di parkiran JPTE sistem *smart doorlock* tidak dapat menjangkau koneksi wifi. Ketika sistem *smart doorlock* tidak mendapatkan koneksi wifi, sistem tidak bisa diakses menggunakan aplikasi dan hanya bisa diakses menggunakan sensor *fingerprint* dikarenakan sistem untuk aplikasi *smart doorlock* menggunakan data base firebase sedangkan untuk sensor *fingerprint* menggunakan database web server.

Pembahasan

Sistem keamanan pintu dengan *fingerprint* berbasis *Internet of Things* (IoT) ini mempunyai dua perangkat yaitu perangkat sensor *fingerprint* dan perangkat solenoid. Perangkat sensor *fingerprint* merupakan perangkat utama yang membuka pintu dengan menggunakan sidik jari. Selanjutnya perangkat solenoid sebagai perangkat pengunci yang dipasang pada pintu menggantikan kunci pintu mekanik. Sistem *smart doorlock* ini memiliki beberapa fitur diantaranya kunci pintu yang otomatis tertutup setelah solenoid membuka pintu selama 3 detik, sensor *fingerprint* sebagai akses membuka pintu menggunakan sidik jari, *smartphone* sebagai akses membuka pintu melalui aplikasi. Terdapat riwayat akses pintu, fitur notifikasi, sistem registrasi terintegrasi antara perangkat dan *smartphone*.

Aplikasi sistem *smart doorlock* hanya dapat digunakan melalui jaringan wifi internet karena menggunakan database firebase [9], jika tidak mendapatkan koneksi wifi internet, sensor *fingerprint* pintu dapat di akses menggunakan sensor sidik jari

pada perangkat. Setiap kali pengguna mengakses pintu maka data pengguna akan tercatat dimenu riwayat pada aplikasi. Riwayat mencakup nama pengguna, Id jari, dan jam masuk. Pada saat registrasi aplikasi dan perangkat sensor harus terhubung ke wifi. pengguna baru melakukan registasi melalui aplikasi pada *smartphone* dan mengisi data diri berupa nama, email dan password. Jika berhasil pengguna akan dialihkan kehalaman registasi sidik jari kemudian memilih id jari dan menempelkan jari 2 kali pada perangkat sensor untuk mendaftarkan jarinya. Selanjutnya pengguna akan diarahkan ke menu login dan melakukan verifikasi email. Jika berhasil pengguna akan masuk ke beranda aplikasi.

Smart doorlock ini juga dapat diberi sumber daya menggunakan baterai dengan tegangan 12 volt, baterai ini berfungsi sebagai penyuplai tenaga listrik ke sistem *smart doorlock*. Fungsi utama dari baterai ini adalah untuk mengubah arus listrik dari sumber menjadi tegangan, arus, dan frekuensi yang benar untuk memberi daya pada beban yang ada pada alat. Jadi ketika terjadi pemadaman listrik maka problem solvingnya sudah teratasi dengan adanya baterai pada *smart doorlock* ini. *Smart doorlock* ini dibangun dengan menggunakan metode pengembangan *prototype*. *Prototype* merupakan salah satu metode pengembangan yang banyak digunakan yang terdiri dari beberapa tahapan, yaitu pengumpulan kebutuhan sistem, merancang *prototype*, evaluasi *prototype*, pengkodean sistem, pengujian evaluasi sistem dan implementasi.

Pengujian sistem dilakukan sebagai acuan pengujian. Aspek pengujian yang di ujikan pada system ini yaitu aspek *functionality* dan aspek *usability*. Pengujian *functionality* dilakukan dengan menggunakan skala Guttman. Berdasarkan hasil pengujian oleh dua orang ahli konten maka nilai *funcnionality* sistem berada pada skala sangat baik dan telah memenuhi aspek *functionality*. Pengujian akurasi pengontrolan sistem aplikasi juga dilakukan untuk mengetahui apakah aplikasi dari sistem yang dibuat dapat diakses dimana saja. Pada pengujian pertama dilakukan dengan jarak ± 4 M, pengujian kedua dilakukan dengan jarak ± 10 M, pengujian ketiga berjarak ± 50 M, pengujian keempat dilakukan dengan jarak ± 100 dan pengujian dilakukan dengan jarak ± 1 KM. Dari pengujian tersebut diperoleh hasil bahwa sistem *smart doorlock* dapat berfungsi dan perangkat selenoid merespon ketika aplikasi digunakan.

KESIMPULAN

Pengembangan pengaman pintu otomatis dengan *fingerprint* dan *smartphone* berbasis

Internet of Things (IoT) ini menggunakan model pengembangan *prototype*. Pengembangan ini menghasilkan sebuah system pengaman pintu otomatis dengan *fingerprint* dan *smartphone* berbasis IoT sehingga dapat dikontrol dari jarak jauh dengan tetap terhubung ke dalam jaringan internet. Hasil pengujian pengembangan pengaman pintu otomatis dengan *fingerprint* dan *smartphone* berbasis *Internet of Things* berdasarkan standar ISO 25010 telah terpenuhi dengan hasil: a) pengujian aspek *functionality* yang telah memenuhi aspek dari 2 ahli konten dan pengujian aspek

usability berada pada kategori sangat baik.

Sistem keamanan pintu dengan menggunakan *fingerprint* berbasis *Internet of Things* yang di rancang telah menyelesaikan permasalahan yang terdapat pada latar belakang yang dimana sistem keamanan pintu (*smart doorlock*) telah memiliki keamanan tinggi yang hanya dapat diakses oleh otoritas laboratorium yang telah terdaftar pada sistem keamanan pintu (*smart doorlock*).

UCAPAN TERIMA KASIH

Ucapan terima kasih disampaikan kepada Rektor Universitas Negeri Makassar, Dekan Fakultas Teknik Universitas Negeri Makassar, Anggota Peneliti, Dosen Ahli, dan pihak-pihak terkait atas bantuan dan arahan dan pembinaannya selama proses kegiatan Penelitian berlangsung. Penelitian merupakan dana hibah dai PNPB Fakultas Teknik dengan Nomor: SP DIPA 023.17.2.677523/2023.

REFERENSI

- Andi, J. (2015). Pembangunan Aplikasi Child Tracker Berbasis Assisted – Global Positioning System (A-GPS) Dengan Platform Android. *Jurnal Ilmiah Komputer Dan Informatika (KOMPUTA)*, 1(1), 1–8.
- Asad, M. R., Nurhayati, O. D., & Widiyanto, E. D. (2015). Sistem Pengamanan Pintu Rumah Otomatis via SMS Berbasis Mikrokontroler ATmega328P. *Jurnal Teknologi Dan Sistem Komputer*, 3(1), 1–7. <https://doi.org/10.14710/jtsiskom.3.1.2015.1-7>
- Dindha Amelia. (2020). *Sistem Keamanan Pintu Ruang Server Menggunakan Fingerprint Berbasis Iot*. 21(1), 1–9. <http://mpoc.org.my/malaysian-palm-oil-industry/>
- H, K., Subrata, R. , H., & Gozali, F. (2019). Sistem Keamanan Ruang Berbasis Internet Of Things Dengan Menggunakan Aplikasi Android. *TESLA: Jurnal Teknik Elektro*, 20(2), 127. <https://doi.org/10.24912/tesla.v20i2.2989>
- Imran, A., & Rasul, M. (2020). Pengembangan Tempat Sampah Pintar Menggunakan Esp32. *Jurnal Media Elektrik*, 17(2), 2721–9100. <https://ojs.unm.ac.id/mediaelektrik/article/view/14193>
- M, A., Febryan, A., Andriani, & Rahmania. (2023). Rancang Bangun Sistem Keamanan Rumah Berbasis Telegram Menggunakan Esp 32 Cam. *VERTEX ELEKTRO-Jurnal Teknik Elektro UNIMUH*, 15(1), 64–71. <https://journal.unismuh.ac.id/index.php/vertex/article/view/10246/5624>
- Nuraeni, N., Anggraini, I., Humairah B, N. I., Ramadhani, I. P., Hadis, M. S., Muliadi, M., & Nurzaenab, N. (2021). Sistem Akses Pintu Berbasis Face Recognition Menggunakan ESP32 Module dan Aplikasi Telegram. *Jurnal MediaTIK*, 4(3), 115. <https://doi.org/10.26858/jmtik.v4i3.23700>
- Santoso. (2015). *Menguasai SPSS 22 From Basic to Expert Skills*. Jakarta. Elex Media Computindo.
- Saputro, E., & Wibawanto, D. H. (2016). Rancang Bangun Pengaman Pintu Otomatis



- Menggunakan E-KTP Berbasis Mikrokontroler Atmega328. *Jurnal Teknik Elektro*, 8(1), 1–4.
<https://journal.unnes.ac.id/nju/index.php/jte/article/view/8787>
- Sugiono. (2017). *Metode Penelitian Pendidikan, Pendekatan Kuantitatif, Kualitatif, Dan R&D*. Alfabeta.
- Widya Dharma, G., Piarsa, I. N., & Agus Dwi Suarjaya, I. M. (2018). Kontrol Kunci Pintu Rumah Menggunakan Raspberry Pi Berbasis Android. *Jurnal Ilmiah Merpati (Menara Penelitian Akademika Teknologi Informasi)*, 6(3), 159.
<https://doi.org/10.24843/jim.2018.v06.i03.p02>