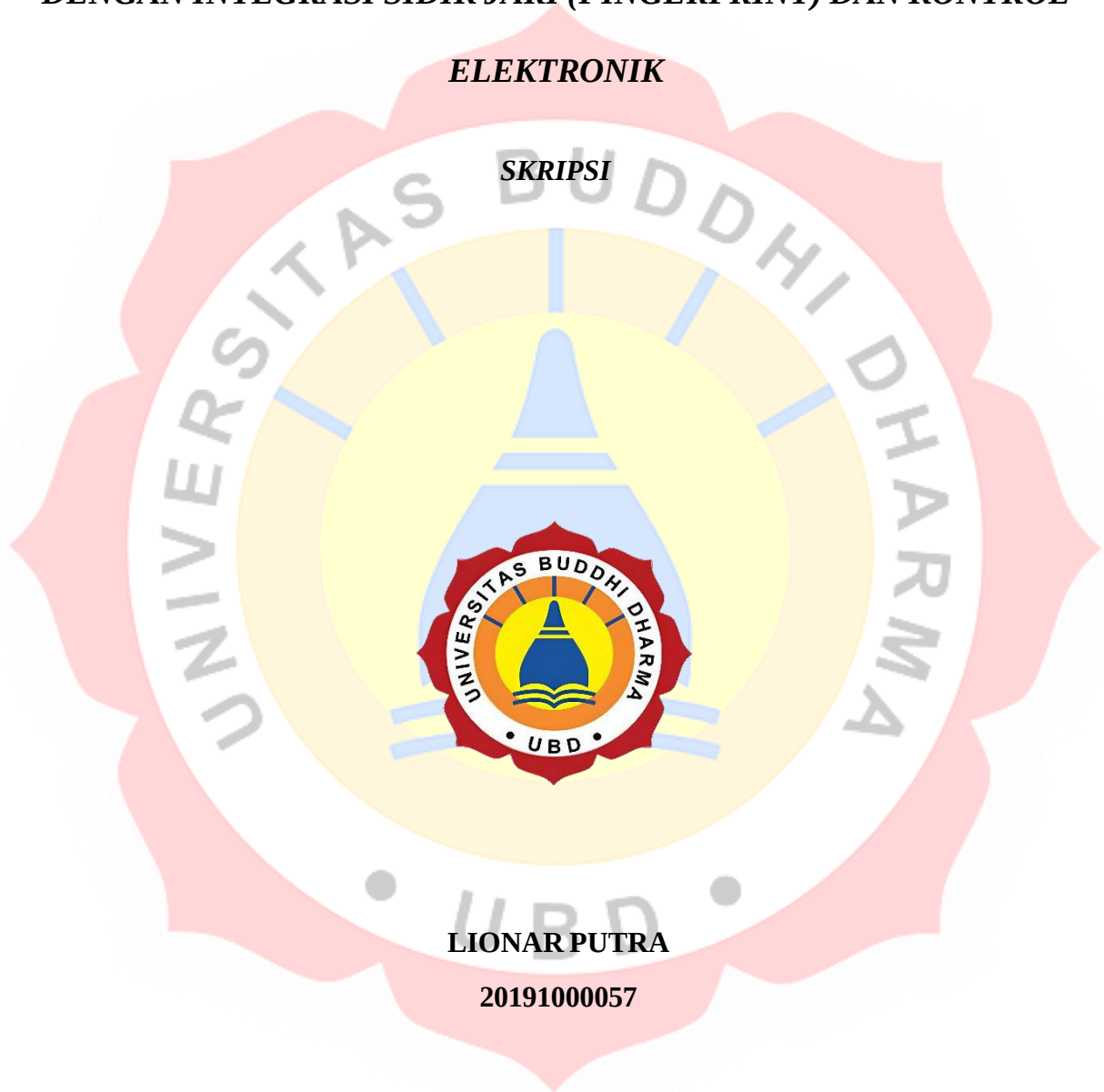


**RANCANG BANGUN SMART SYSTEM HOME BERBASIS IOT
DENGAN INTEGRASI SIDIK JARI (FINGERPRINT) DAN KONTROL**

ELEKTRONIK

SKRIPSI



LIONAR PUTRA

20191000057

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS BUDDHI DHARMA

TANGERANG

2025

**RANCANG BANGUN SMART SYSTEM HOME BERBASIS IOT
DENGAN INTEGRASI SIDIK JARI (FINGERPRINT) DAN KONTROL
ELEKTRONIK**

SKRIPSI

**Diajukan sebagai salah satu syarat untuk memperoleh Gelar Sarjana Komputer pada
Program Studi Teknik Informatika**

LIONAR PUTRA

20191000057

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS BUDDHI DHARMA

TANGERANG

2025

LEMBAR PERSEMBAHAN

“Pendidikan adalah paspor menuju masa depan, karena hari esok dimiliki oleh mereka yang mempersiapkan diri hari ini”

Dengan mengucapkan puji syukur kepada Tuhan Yang Maha Esa, Skripsi ini kupersembahkan untuk:

1. Bapak dan Ibu tercinta yang telah membesarkan aku dan selalu membimbing, mendukung, memotivasi, memberi apa yang terbaik bagiku serta selalu mendoakan aku untuk meraih kesuksesanku.
2. Kakak dan adik-adikku yang telah memberikan dukungan semangat serta dorongan yang senantiasa diberikan.
3. Teman-teman yang selalu berjuang bersama.
4. Rekan-rekan dari Universitas Buddhi Dharma yang selalu memberikan dukungan dan semangat.

UNIVERSITAS BUDDHI DHARMA
LEMBAR PERNYATAAN KEASLIAN SKRIPSI

Yang bertanda tangan di bawah ini,

NIM : 20191000057
Nama : Lionar Putra
Jenjang Studi : Strata 1
Program Studi : Teknik Informatika
Informatika Peminatan : Jaringan

Dengan ini saya menyatakan bahwa:

1. Skripsi ini adalah asli dan belum pernah diajukan untuk mendapatkan gelar akademik (Diploma/Sarjana) atau kelengkapan studi, baik di Universitas Buddhi Dharma maupun di Perguruan Tinggi lainnya.
2. Skripsi ini saya buat sendiri tanpa bantuan pihak lain, kecuali arahan dosen pembimbing.
3. Dalam Skripsi ini tidak terdapat karya atau pendapat yang telah ditulis atau dipublikasikan orang lain, kecuali secara tertulis dengan jelas dan dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan dicantumkan daftar pustaka.
4. Dalam Skripsi ini tidak terdapat pemalsuan (kebohongan), seperti buku, artikel, jurnal, data sekunder, pengolahan data, dan pemalsuan tanda tangan dosen atau Ketua Program Studi di Universitas Buddhi Dharma yang dibuktikan dengan keasliannya.
5. Lembar Pernyataan ini saya buat dengan sesungguhnya, tanpa paksaan dan apabila dikemudian hari atau pada waktu lainnya terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, saya bersedia menerima sanksi akademik berupa pencabutan gelar yang telah saya peroleh karena Skripsi ini, serta sanksi lainnya sesuai dengan peraturan dan norma yang berlaku.

Tangerang, 05 Febuari 2025



Lionar Putra
NIM. 20191000057

LEMBAR PERSETUJUAN PUBLIKASI KARYA ILMIAH

Yang bertanda tangan di bawah ini,

NIM : 20191000057
Nama : Lionar Putra
Jenjang Studi : Strata I
Program Studi : Teknik Informatika
Informatika Peminatan : Jaringan

Dengan ini menyetujui untuk memberikan ijin kepada pihak Universitas Buddhi Dharma, Hak Bebas Royalti Non- Eksklusif (*Non-exclusive Royalti-Free Right*) atas karya ilmiah kami yang berjudul: "*Rancang Bangun Smart Home System Berbasis Iot Dengan Integrasi Sidik Jari (Fingerprint) Dan Kontrol Elektronik*", beserta perangkat yang diperlukan.

Dengan Hak Bebas Royalti Non-Eksklusif ini pihak Universitas Buddhi Dharma berhak menyimpan, mengalih-media atau format-kan, mengelolanya dalam pangkalan data (*database*), mendistribusikannya, dan menampilkan atau mempublikasikannya di *internet* atau media lain untuk kepentingan akademis tanpa perlu meminta ijin dari saya selama tetap mencantumkan nama saya sebagai penulis atau pencipta karya ilmiah tersebut.

Saya bersedia untuk menanggung secara pribadi, tanpa melibatkan pihak Universitas Buddhi Dharma, segala bentuk tuntutan hukum yang timbul atas pelanggaran Hak Cipta dalam karya ilmiah saya ini.

Demikian pernyataan ini saya buat dengan sebenarnya.

Tangerang, 05 Febuari 2025


Lionar Putra 

NIM. 20191000057

UNIVERSITAS BUDDHI DHARMA
LEMBAR PENGESAHAN PEMBIMBING
RANCANG BANGUN SMART HOME SYSTEM BERBASIS IOT
DENGAN INTEGRASI SIDIK JARI (FINGERPRINT) DAN
KONTROL ELEKTRONIK

Dibuat Oleh:

NAMA : Lionar Putra

NIM : 20191000057

Telah disetujui untuk dipertahankan di hadapan Tim Penguji Ujian

Komprehensif

Program Studi Teknik Informatika
Peminatan Network Specialist

Tahun Akademik 2024/2025

Disahkan Oleh,

Tangerang, 05 Febuari 2025

Pembimbing,



Indah Fenriana, S.Kom., M.Kom

NIDN. 0406028801

UNIVERSITAS BUDDHI DHARMA
LEMBAR PENGESAHAN SKRIPSI
RANCANG BANGUN *SMART HOME SYSTEM* BERBASIS IOT
DENGAN INTEGRASI SIDIK JARI (*FINGERPRINT*) DAN
KONTROL ELEKTRONIK

Dibuat Oleh:

NAMA : Lionar Putra

NIM 20191000057

Telah disetujui untuk dipertahankan di hadapan Tim Penguji Ujian

Komprehensif

Program Studi Teknik Informatika

Peminatan *Network Specialist*

Tahun Akademik 2024/2025

Disahkan Oleh,

Tangerang, 05 Febuari 2025

Dekan,

Ketua Program Studi,



Dr. Yakub, S.Kom., M.Kom., M.M
NIDN : 0304056901



Hartana Wijaya, S.Kom., M.Kom
NIDN : 0412058102

UNIVERSITAS BUDDHI DHARMA
LEMBAR PENGESAHAN TIM PENGUJI

NAMA : Lionar Putra
NIM : 20191000057
Fakultas : Sains dan Teknologi

Judul Skripsi : RANCANG BANGUN SMART HOME SYSTEM BERBASIS IOT DENGAN INTEGRASI SIDIK JARI (FINGERPRINT) DAN KONTROL ELEKTRONIK

Dinyatakan LULUS setelah mempertahankan di depan Tim Penguji pada hari, Rabu 05 Febuari 2025.

Nama penguji :

Tanda Tangan :

Ketua Sidang : **Riki M.Kom**

NIDN : 0431128204

Penguji I : **Junaidi Akbar S.Pd., M.Pd.T.**

NIDN : 0431079403

Penguji II : **Indah Fenriana S.Kom., M.Kom**

NIDN : 0406028801

Mengetahui,

Dekan Fakultas Sains dan Teknologi

Dr. Yakub, S.Kom., M.Kom., M.M

NIDN : 0304056901

KATA PENGANTAR

Puji syukur penulis panjatkan kepada Tuhan yang Maha Esa, yang telah memberikan rahmat, kasih, serta karunia-Nya sehingga penulis dapat menyelesaikan skripsi ini dengan judul "RANCANG BANGUN SMART HOME SYSTEM BERBASIS IOT DENGAN INTEGRASI SIDIK JARI (FINGERPRINT) DAN KONTROL ELEKTRONIK."

Skripsi ini disusun sebagai salah satu syarat untuk memperoleh gelar Sarjana Teknik Informatika di Universitas Buddhi Dharma. Penulis ingin mengucapkan terima kasih kepada semua pihak yang telah memberikan dukungan, bimbingan, dan motivasi selama proses penulisan skripsi ini.

Dalam proses penyusunan karya ilmiah ini (Skripsi) saya banyak menerima masukan dan bantuan dari berbagai pihak, maka pada kesempatan kali ini saya akan menyampaikan banyak terimakasih yang sebesar-besarnya kepada: Universitas Buddhi Dharma.

1. Ibu. Dr. Limanjatini, SE., MM., BKP Selaku Rektor Universitas Buddhi Dharma.
2. Bapak. Dr. Yakub, S.Kom., M.Kom., Sebagai Dekan Fakultas Sains dan Teknologi Universitas Buddhi Dharma.
3. Bapak. Hartana Wijaya, S.Kom., M.Kom Selaku ketua program studi Teknik Informatika Universitas Buddhi Dharma.
4. Ibu. Indah Fenriana, S.Kom., M.Kom., Selaku Dosen Pembimbing saya yang telah membantu dan mendukung saya sehingga saya dapat menyelesaikan karya ilmiah ini.
5. Kedua orang tua saya serta keluarga yang telah memberi dukungan kepada saya
6. Serta teman-teman saya yang selalu membantu serta memberi semangat kepada saya, sehingga saya berhasil menyelesaikan karya ilmiah ini.

Akhir kata, peneliti berharap semoga penelitian ini dapat bermanfaat bagi para pembaca. Peneliti terbuka terhadap segala kritik dan saran yang positif dan dapat membangun. Peneliti juga memohon maaf apabila ada kekurangan di dalam penelitian ini, terima kasih.

Tangerang. 05 Febuari 2025

Penulis

Rancang Bangun *Smart System Home* Berbasis *Iot* Dengan Integrasi Sidik Jari (*Fingerprint*) Dan Kontrol Elektronik

Halaman 89 + XVII / 7 Tabel / 29 Gambar / 1 Lampiran

ABSTRAK

Keamanan rumah menjadi kebutuhan mendasar yang semakin krusial seiring meningkatnya angka kriminalitas. Sistem keamanan konvensional berbasis kunci manual memiliki keterbatasan dalam kepraktisan dan pemantauan akses secara *real-time*. Minimnya pemanfaatan teknologi *Internet of Things* (IoT) menyebabkan sistem masih bersifat statis dan kurang responsif terhadap ancaman. Penelitian ini bertujuan mengembangkan sistem *smart door lock* berbasis IoT dengan pemindai sidik jari menggunakan ESP8266 dan Blynk. Sistem ini memungkinkan pemilik rumah memantau akses secara jarak jauh serta menerima notifikasi *real-time* ketika terjadi akses tidak sah. Metode yang digunakan adalah metode *prototype* dengan ruang lingkup penelitian mencakup autentikasi biometrik, pencatatan aktivitas pengguna, serta pengujian keandalan sistem melalui *Black Box Testing*. Hasil penelitian menunjukkan bahwa integrasi sistem dengan Blynk meningkatkan keamanan dan efisiensi kontrol akses. Pengujian keandalan sidik jari memiliki waktu respons rata-rata 1,5 detik, lebih cepat dibandingkan pengendalian jarak (1,96 detik) dan metode PIN (17,75 detik). Uji t-test dan ANOVA menunjukkan perbedaan signifikan dalam kecepatan respons, mengindikasikan bahwa otentikasi sidik jari lebih unggul dalam eksekusi cepat, sementara pengendalian jarak lebih stabil dalam variasi waktunya. Implementasi sistem ini diharapkan dapat meningkatkan keamanan rumah secara efektif dan adaptif terhadap kebutuhan *modern*.

Kata Kunci: Keamanan rumah, autentikasi sidik jari, IoT, ESP8266, Blynk.

Design Smart Home System Based On Iot With Fingerprint Integration And Electronic Control

Page 89 + XVII / 7 Tables / 29 Images / 1 Attachment

ABSTRACT

Home security is becoming an increasingly crucial basic need as the number of crimes increases. Conventional security systems based on manual locks have limitations in practicality and real-time monitoring of access. The lack of utilization of Internet of Things (IoT) technology causes the system to be static and less responsive to threats. This research aims to develop IoT-based smart door lock system with fingerprint scanner using ESP8266 and Blynk. The system allows homeowners to remotely monitor access as well as receive real-time notifications when unauthorized access occurs. The method used is a prototype method with the scope of research includes biometric authentication, recording user activity, as well as testing the reliability of the system through Black Box Testing. The results showed that system integration with Blynk improved access control security and efficiency. Fingerprint reliability tests had an average response time of 1.5 seconds, faster than distance control (1.96 seconds) and PIN methods (17.75 seconds). The t-test and ANOVA showed significant differences in response speed, indicating that fingerprint authentication was superior in fast execution, while distance control was more stable in time variation. The implementation of this system is expected to improve home security effectively and adaptively to modern needs.

Keywords: Home security, fingerprint authentication, IoT, ESP8266, Blynk.

DAFTAR ISI

LEMBAR PERSEMBAHAN	iii
LEMBAR PERNYATAAN KEASLIAN SKRIPSI.....	iv
LEMBAR PERSETUJUAN PUBLIKASI KARYA ILMIAH	v
LEMBAR PENGESAHAN PEMBIMBING.....	vi
LEMBAR PENGESAHAN SKRIPSI.....	vii
LEMBAR PENGESAHAN TIM PENGUJI	viii
KATA PENGANTAR	ix
ABSTRAK.....	x
ABSTRACT.....	xi
DAFTAR ISI.....	xii
DAFTAR GAMBAR	xv
DAFTAR TABEL	xvi
DAFTAR LAMPIRAN	xvii
BAB I PENDAHULUAN	1
1.1 Latar Belakang Penelitian	1
1.2 Identifikasi Masalah.....	4
1.3 Ruang Lingkup Penelitian.....	5
1.4 Tujuan dan Manfaat Penelitian	6
1.4.1 Tujuan Penelitian.....	6
1.4.2 Manfaat Penelitian.....	6
1.5 Sistematika Penulisan	7
BAB II LANDASAN TEORI.....	9
Teori Umum	9

2.1.1	Pengertian Sistem	9
2.1.2	Pengertian Pengamanan.....	11
2.1.3	<i>Smart Door Lock</i>	13
2.1.4	Pengertian Sidik Jari.....	14
2.1.5	Pengertian <i>Internet Of Things</i>	16
2.1.6	Pengertian Otomasi	18
2.1.7	Pengertian <i>Internet</i>	22
2.1	Teori Khusus.....	24
2.2.1	Metode <i>Prototype</i>	24
2.2.2	Mikrokontroler ESP 8266.....	26
2.2.3	<i>Optical Fingerprint Sensor</i> AS608	29
2.2.4	LCD i2C	31
2.2.5	RFID RC522.....	33
2.2.6	<i>Solenoid Lock</i> 12V DC.....	35
2.2.7	Arduino IDE	37
2.2	Teori Analisa & Perancangan.....	39
2.3.1	<i>Block Diagram</i>	39
2.3.2	<i>Flowchart</i>	40
2.3	Teori Pengujian.....	42
2.4.1	Pengujian Black Box	42
2.4	Penelitian Yang Relevan.....	43
BAB III METODOLOGI PENELITIAN.....		58
3.1	Analisa Kebutuhan.....	58
3.2	Metode <i>Prototype</i>	60
3.3	Rencana Pengujian <i>Black Box Testing</i>	67

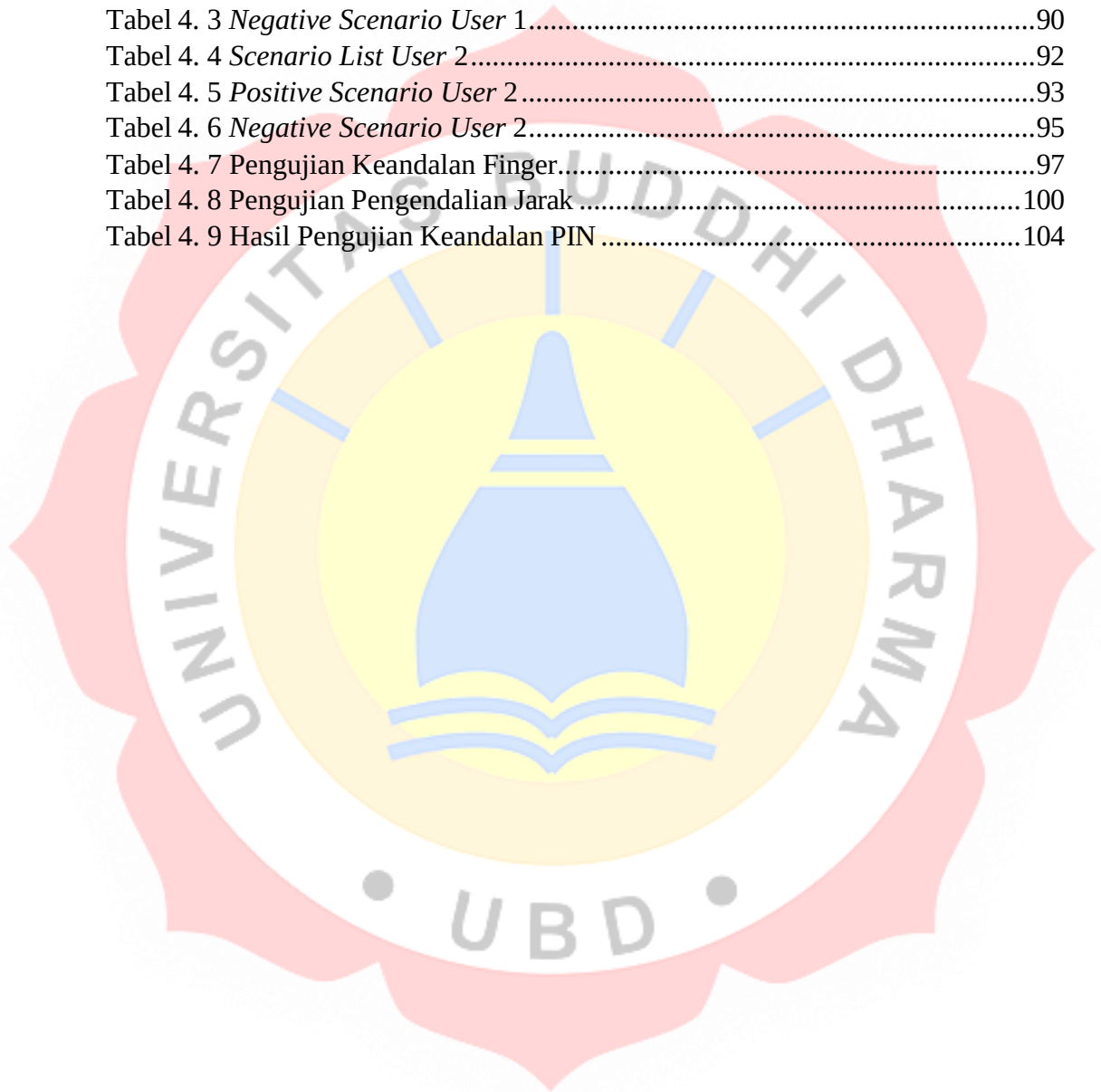
3.4	Spesifikasi Kebutuhan Sistem.....	68
3.2.1	<i>Hardware</i>	68
3.2.2	<i>Software</i>	69
3.5	<i>Flow Chart</i>	69
3.6	Jadwal Penelitian	71
3.7	Kerangka Pemikiran.....	72
BAB IV	HASIL DAN PEMBAHASAN.....	74
4.1	Blok Diagram.....	74
4.2	Proses Pembuatan Program dan <i>Prototype</i>	76
4.2.1	Install Package <i>Nodemcu ESP8266</i>	76
4.2.2	Tampilan <i>Prototype</i> Sistem	83
4.3	Spesifikasi <i>Software</i>	85
4.4	Spesifikasi <i>Hardware</i>	86
4.5	Pengujian Sistem.....	87
4.5.1	<i>Black Box Testing</i>	87
BAB V	SIMPULAN DAN SARAN	105
5.1	Simpulan	105
5.2	Saran	106
DAFTAR PUSTAKA		107
DAFTAR RIWAYAT HIDUP.....		115
DAFTAR LAMPIRAN		116

DAFTAR GAMBAR

Gambar 2. 1 Tahapan Metode Prototype.....	26
Gambar 2. 2 Mikrokontroler ESP8266.....	27
Gambar 2. 3 <i>Optical Fingerprint Sensor</i> AS608	30
Gambar 2. 4 LCD I2C	32
Gambar 2. 5 RFID RC522.....	34
Gambar 2. 6 <i>Solenoid Lock</i> 12V DC.....	35
Gambar 3. 1 Tahapan <i>Prototype</i>	60
Gambar 3. 2 Rancangan <i>Prototype</i>	61
Gambar 3. 3 <i>Source Code</i> Simpan Sidik Jari	63
Gambar 3. 4 <i>Source Code</i> Baca Sidik Jari.....	64
Gambar 3. 5 <i>Source Code</i> Koneksi <i>Server Cloud Bylink</i>	65
Gambar 3. 6 <i>Source Code</i> Koneksi Lampu	66
Gambar 3. 7 Prototype Awal	67
Gambar 3. 8 <i>Folw Chart</i> Alur Proses Sistem	70
Gambar 3. 9 Jadwal Penelitian	71
Gambar 3. 10 Kerangka Pemikiran	72
Gambar 4. 1 <i>Block Diagram Prototype</i>	74
Gambar 4. 2 Cara Kerja NodeMCU	76
Gambar 4. 3 Tampilan Menu Arduino IDE.....	77
Gambar 4. 4 Tampilan Menu Arduino IDE <i>Preference</i>	78
Gambar 4. 5 Tampilan Menu <i>Board Manager</i>	79
Gambar 4. 6 Tampilan Menu Board manager Proses Install	79
Gambar 4. 7 Tampilan Menu <i>Board Installed</i>	80
Gambar 4. 8 Tampilan <i>Coding led</i>	80
Gambar 4. 9 Tampilan Coding Simpan Sidik Jari	81
Gambar 4. 10 Tampilan Coding Baca Sidik Jari	82
Gambar 4. 11 Tampilan Coding Koneksi Bylnk	82
Gambar 4. 12 Tampilan Coding Lampu	83
Gambar 4. 13 Tampilan <i>Prototype</i>	83
Gambar 4. 14 Tampilan <i>Proses</i> Deteksi Sidik Jari	84
Gambar 4. 15 Tampilan Pintu Terbuka	84
Gambar 4. 16 Tampilan Finger Tidak Terdaftar	85
Gambar 4. 17 Tampilan Log Aktivitas	85
Gambar 4. 18 Grafik Pengujian Keandalan Finger	98
Gambar 4. 19 Grafik pengendalian Jarak	100
Gambar 4. 20 Perbandingan Pengujian	101

DAFTAR TABEL

Tabel 2. 1 Penelitian Relevan	54
Tabel 3. 1 Rencana Pengujian <i>Black Box</i>	67
Tabel 4. 1 <i>Scenario List User 1</i>	88
Tabel 4. 2 <i>Positive Scenario User 1</i>	89
Tabel 4. 3 <i>Negative Scenario User 1</i>	90
Tabel 4. 4 <i>Scenario List User 2</i>	92
Tabel 4. 5 <i>Positive Scenario User 2</i>	93
Tabel 4. 6 <i>Negative Scenario User 2</i>	95
Tabel 4. 7 Pengujian Keandalan Finger.....	97
Tabel 4. 8 Pengujian Pengendalian Jarak	100
Tabel 4. 9 Hasil Pengujian Keandalan PIN	104



DAFTAR LAMPIRAN

Lampiran 1 <i>Listing Program</i>	116
Lampiran 2 Kartu Bimbingan Skripsi.....	122
Lampiran 3 Form Pengujian <i>Black Box User 1</i>	123
Lampiran 4 Form Pengujian <i>Black Box User 2</i>	128



BAB I

PENDAHULUAN

1.1 Latar Belakang Penelitian

Keamanan merupakan kebutuhan mendasar yang harus dipenuhi untuk menciptakan lingkungan yang nyaman dan tenteram. Dalam kehidupan sehari-hari, rumah menjadi salah satu aset paling penting yang membutuhkan perlindungan ekstra. Kondisi keamanan rumah menjadi prioritas utama karena berkaitan dengan keselamatan penghuni dan perlindungan terhadap harta benda. Namun, sistem keamanan rumah konvensional yang umumnya masih menggunakan kunci manual sering kali dianggap tidak memadai. Hal ini memicu meningkatnya risiko tindak kriminalitas yang terjadi di lingkungan perumahan.

Berdasarkan data dari Badan Pusat Statistik, pada tahun 2013, Indonesia mencatat 10.683 kasus pencurian dengan kekerasan, 482 kasus pencurian dengan senjata api, dan 880 kasus pencurian dengan senjata tajam. Angka-angka tersebut menunjukkan bahwa masalah kriminalitas masih menjadi tantangan serius yang memerlukan perhatian khusus, terutama dalam menciptakan sistem keamanan yang lebih efektif untuk melindungi rumah dan isinya. Sistem keamanan pintu rumah yang masih mengandalkan kunci konvensional memiliki beberapa kelemahan yang signifikan.

Salah satu kelemahan utama adalah ketidakpraktisan dalam penggunaannya. Pemilik rumah harus membawa dan menyimpan kunci dengan baik agar tidak hilang atau dicuri. Kehilangan kunci dapat menyebabkan risiko keamanan yang besar karena orang yang tidak berwenang dapat mengakses rumah dengan mudah. Selain itu, kunci

konvensional juga tidak dapat mencatat atau memantau aktivitas yang terjadi secara real-time, sehingga tidak memungkinkan adanya respons cepat terhadap situasi darurat.

Keterbatasan dalam pemantauan akses jarak jauh dan notifikasi membuat sistem kurang responsif terhadap aktivitas mencurigakan. Minimnya pemanfaatan teknologi IoT dalam sistem kontrol akses menyebabkan sistem masih bersifat statis dan kurang adaptif terhadap kebutuhan modern. Selain itu, kurangnya integrasi dengan perangkat pintar, seperti aplikasi ponsel, menghambat optimalisasi efisiensi serta respons terhadap perubahan kondisi, sehingga sistem tidak dapat beroperasi secara maksimal dalam meningkatkan keamanan dan kenyamanan pengguna.

Dalam era modern yang ditandai dengan pesatnya perkembangan teknologi, diperlukan solusi inovatif untuk meningkatkan keamanan rumah secara signifikan. Salah satu solusi yang dapat diimplementasikan adalah sistem keamanan berbasis teknologi *Internet of Things* (IoT) yang menggunakan fingerprint scanner atau pemindai sidik jari. Teknologi ini menawarkan berbagai keunggulan dibandingkan sistem keamanan tradisional, seperti kepraktisan, akurasi tinggi, dan kemampuan untuk mencatat aktivitas pengguna secara *real-time*.

Sistem pengamanan pintu rumah berbasis sidik jari dan IoT memungkinkan pengguna untuk membuka pintu tanpa perlu membawa kunci fisik. Pengguna hanya perlu menempatkan sidik jarinya pada pemindai, dan sistem akan secara otomatis memverifikasi identitas mereka. Sidik jari memiliki keunikan yang tidak dapat dipalsukan, sehingga risiko akses tidak sah dapat diminimalisir. Selain itu, sistem ini dapat mencatat data pengguna yang masuk dan keluar rumah, serta menampilkan informasi tersebut pada perangkat seperti *smartphone*.

Dengan adanya fitur ini, pemilik rumah dapat dengan mudah memantau aktivitas di rumah mereka, bahkan jika mereka sedang berada di tempat yang jauh. Keunggulan lainnya dari teknologi IoT adalah kemampuannya untuk mengintegrasikan berbagai perangkat dalam satu jaringan. Sistem keamanan berbasis IoT dapat dihubungkan dengan perangkat lain, seperti kamera pengawas (CCTV) atau alarm keamanan, untuk menciptakan sistem yang lebih komprehensif.

Seperti kasus jika seseorang mencoba membuka pintu tanpa otorisasi, sistem dapat secara otomatis mengirimkan pemberitahuan ke ponsel pemilik rumah atau mengaktifkan alarm untuk memperingatkan lingkungan sekitar. Sistem keamanan pintu rumah berbasis IoT dengan sidik jari juga menawarkan solusi yang lebih ramah lingkungan dibandingkan dengan kunci konvensional. Karena tidak memerlukan penggunaan kunci fisik, sistem ini membantu mengurangi penggunaan logam yang sering digunakan untuk membuat kunci.

Sistem ini dirancang untuk tahan lama dan memerlukan sedikit perawatan, sehingga menjadi pilihan yang lebih ekonomis dalam jangka panjang. Meskipun menawarkan berbagai keunggulan, implementasi sistem pengaman pintu rumah berbasis sidik jari dan IoT juga menghadapi beberapa tantangan. Salah satu tantangan utama adalah kebutuhan akan koneksi internet yang stabil untuk mendukung pengoperasian sistem secara optimal. Selain itu, pengguna juga perlu memahami cara kerja sistem untuk menghindari kesalahan penggunaan yang dapat memengaruhi performa.

Maka dari itu edukasi dan pelatihan bagi pengguna menjadi bagian penting dalam penerapan teknologi ini. Penelitian ini bertujuan untuk mengembangkan sistem pengaman pintu rumah berbasis IoT dengan teknologi pemindai sidik jari yang dapat

memberikan keamanan yang lebih baik, kepraktisan, dan kemudahan bagi pengguna. Sistem ini dirancang untuk mengatasi kelemahan sistem keamanan tradisional, seperti ketidakpraktisan penggunaan kunci manual dan kurangnya kemampuan untuk memantau aktivitas secara *real-time*.

Penelitian ini juga berupaya untuk mengintegrasikan teknologi IoT guna menciptakan sistem keamanan rumah yang lebih cerdas dan responsif terhadap ancaman. Dengan mengadopsi teknologi ini, diharapkan masalah keamanan rumah dapat diminimalisir secara signifikan. Tidak hanya itu, sistem ini juga dapat membantu meningkatkan kesadaran masyarakat akan pentingnya memanfaatkan teknologi untuk menciptakan lingkungan yang lebih aman. Hasil penelitian ini diharapkan dapat menjadi dasar bagi pengembangan lebih lanjut dalam bidang sistem keamanan berbasis IoT, serta memberikan kontribusi positif bagi masyarakat luas.

1.2 Identifikasi Masalah

Dalam pengembangan sistem pengaman pintu rumah berbasis sidik jari dengan *Internet of Things* (IoT), terdapat beberapa masalah utama yang diidentifikasi:

1. Keamanan tradisional masih memiliki kelemahan penggunaan kunci fisik yang rentan terhadap duplikasi dan kehilangan.
2. Kontrol berbasis kunci konvensional tidak menyediakan kemampuan untuk memberikan peringatan atau respons otomatis terhadap ancaman keamanan yang muncul.
3. Perangkat rumah tangga seperti pintu otomatis dan lampu belum sepenuhnya terhubung dalam satu sistem yang terintegrasi, sehingga kurang efisien dalam memberikan perlindungan dan kenyamanan bagi pengguna.

1.3 Ruang Lingkup Penelitian

Penelitian ini berfokus pada pengembangan sistem pengaman pintu rumah berbasis sidik jari dengan integrasi teknologi *Internet of Things* (IoT). Ruang lingkup penelitian meliputi:

1. Sistem dirancang untuk menggunakan sensor sidik jari sebagai alat autentikasi utama dalam rumah pintar untuk membuka pintu. Data biometrik disimpan secara aman untuk memastikan hanya pengguna yang terdaftar yang dapat mengakses sistem menggunakan perangkat ESP8266.
2. Sistem mencatat setiap ada *fingger* yang tidak terdaftar. Data ini dapat diakses oleh pemilik rumah melalui aplikasi bylnk.
3. Sistem dirancang untuk meningkatkan tingkat keamanan yang lebih fleksibel dan terintegrasi. dan juga untuk memenuhi kebutuhan pengamanan rumah pribadi, dengan fokus pada pengamanan pintu utama yang lebih mudah dikendalikan secara jarak jauh, serta memungkinkan akses yang lebih aman dan praktis. Meskipun begitu, pengamanan ini tetap terbatas pada area tertentu dan belum mencakup seluruh bagian rumah secara menyeluruh.
4. Metode pengembangan sistem yang dalam penelitian ini adalah metode *prototype*.
5. Ruang lingkup juga mencakup pengujian sistem, seperti uji keandalan sensor sidik jari, kecepatan respons sistem, kestabilan koneksi IoT, dan uji kepuasan pengguna menggunakan pada *Black Box Testing* yang dilakukan dalam lingkungan dalam rumah atau *indoor*.

1.4 Tujuan dan Manfaat Penelitian

1.4.1 Tujuan Penelitian

Tujuan dari penelitian ini adalah untuk mengembangkan dan mengimplementasikan Sistem Pengaman Pintu Rumah Berbasis Sidik Jari dengan Teknologi *Internet of Things* (IoT). Secara spesifik, tujuan penelitian ini meliputi:

1. mengimplementasikan sistem keamanan berbasis sidik jari untuk mengatasi kelemahan sistem kunci fisik tradisional yang rentan terhadap duplikasi dan kehilangan.
2. Mengembangkan sistem notifikasi dan respons otomatis berbasis IoT yang dapat memberikan peringatan real-time kepada pemilik rumah saat terjadi upaya akses tidak sah.
3. Mengimplementasikan sistem smart home terintegrasi menggunakan ESP8266 dan Blynk untuk menghubungkan perangkat rumah tangga seperti pintu otomatis dan lampu dalam satu sistem kontrol terpadu, sehingga meningkatkan efisiensi perlindungan dan kenyamanan pengguna.

1.4.2 Manfaat Penelitian

Adapun manfaat terhadap perancangan pada sistem kontrol berbasis sidik jari dan otomasi elektronik di antara berikut:

1. Sistem kontrol berbasis otomatis ini dapat membantu mempermudah seseorang dalam hal menyalakan dan mematikan suatu alat elektronik secara otomatis serta dapat menciptakan efisiensi waktu dan menghemat energi
2. Dalam penggunaan sistem berbasis sidik jari (*Fingerprint*) dapat memproteksi lebih untuk keamanan rumah.

1.5 Sistematika Penulisan

Pembahasan tugas akhir ini akan di bagi menjadi lima bab dengan sistematika sebagai berikut:

BAB I PENDAHULUAN

Bab ini membahas tentang latar belakang, identifikasi masalah, rumusan masalah, tujuan dan manfaat, ruang lingkup, metode penelitian, Teknik pengumpulan data dan sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini memberikan penjelasan singkat tentang tinjauan pustaka, sistem keamanan rumah, sensor pemindayan sidik jari, arduinouno, arduino ethernet shield, solenoid dan software labView.

BAB III METODOLOGI PENELITIAN

Bab ini terdiri dari Analisa sistem bersama dengan metode yang digunakan lalu menjelaskan dan memberi gambaran ilustrasi objek apa saja yang digunakan.

BAB IV HASIL PEMBAHASAN

Bab ini membahas mengenai metode dan algoritma yang digunakan, spesifikasi dari perancangan sistem yang dibuat, tampilan program serta pengujian sistem.

BAB V KESIMPULAN DAN SARAN

Bab ini terdiri dari kesimpulan dari analisa dan rancangan serta saran yang berisi pandangan atau kritik yang dapat dilakukan pada era modern ini.



BAB II

LANDASAN TEORI

Teori Umum

2.1.1 Pengertian Sistem

Sistem adalah suatu kesatuan atau kumpulan elemen yang saling terhubung dan bekerja bersama untuk mencapai tujuan tertentu. Elemen-elemen dalam sistem dapat berupa komponen fisik, prosedur, manusia, atau teknologi yang dirancang untuk menjalankan fungsi tertentu. Dalam konteks yang lebih luas, sistem tidak hanya mencakup perangkat keras atau perangkat lunak, tetapi juga mencakup cara kerja, aturan, dan proses yang memungkinkan terciptanya hasil yang diinginkan. Pemahaman tentang sistem menjadi penting dalam berbagai bidang, seperti teknologi informasi, manajemen, biologi, dan bahkan kehidupan sehari-hari, karena sistem membantu kita memahami hubungan antara elemen yang berbeda dan bagaimana mereka berkontribusi untuk mencapai tujuan keseluruhan (Suminten & Sintawati, 2020).

Sebuah sistem memiliki karakteristik utama yang membedakannya dari kumpulan elemen biasa. Pertama, sistem memiliki tujuan yang jelas yang menjadi arah kerja dari semua elemen di dalamnya. Kedua, terdapat hubungan saling ketergantungan antara elemen-elemen yang ada, sehingga perubahan pada salah satu elemen dapat memengaruhi kinerja keseluruhan sistem. Ketiga, sistem memiliki batasan tertentu yang memisahkannya dari lingkungan eksternal. Batasan ini menentukan sejauh mana sistem dapat berinteraksi dengan elemen di luar dirinya. Selain itu, setiap sistem memiliki masukan (*input*), proses, dan keluaran (*output*),

yang merupakan komponen dasar untuk menjalankan fungsinya (Effendy et al., 2023).

Dalam bidang teknologi, sistem sering kali merujuk pada sistem informasi, yaitu sekumpulan komponen yang digunakan untuk mengumpulkan, memproses, menyimpan, dan mendistribusikan informasi (Purnama et al., 2024). Contoh sistem informasi meliputi perangkat lunak manajemen, aplikasi berbasis web, atau bahkan platform media sosial. Sementara itu, dalam manajemen, sistem dapat berupa kerangka kerja yang mengatur alur kerja, distribusi tugas, dan komunikasi antar individu dalam organisasi untuk mencapai efisiensi dan produktivitas.

Sistem juga bisa dikategorikan menjadi dua jenis utama, yaitu sistem terbuka dan sistem tertutup. Sistem terbuka adalah sistem yang berinteraksi dengan lingkungannya, menerima masukan, dan menyesuaikan diri terhadap perubahan eksternal (Baharuddin, 2015). Contohnya adalah organisasi yang terus menerus beradaptasi dengan kebutuhan pasar. Sebaliknya, sistem tertutup adalah sistem yang tidak berinteraksi dengan lingkungan eksternal dan cenderung mandiri dalam menjalankan fungsinya, seperti mekanisme pada jam analog.

Keberhasilan suatu sistem sangat bergantung pada desain dan implementasinya. Sebuah sistem yang baik harus mampu memenuhi kebutuhan penggunaanya dengan efisien dan efektif. Selain itu, sistem yang dirancang dengan baik juga harus mudah untuk dipelihara, diperbarui, dan diperluas sesuai kebutuhan. Untuk memastikan keberhasilan, sering kali dilakukan evaluasi terhadap kinerja sistem secara berkala, baik dari segi teknis maupun penggunaannya (Faridawati et al., 2024).

Dalam kehidupan sehari-hari, sistem digunakan hampir di semua aspek, seperti transportasi, komunikasi, pendidikan, hingga keamanan. Misalnya, sistem transportasi

mencakup jaringan jalan, kendaraan, dan aturan lalu lintas yang saling berhubungan untuk menciptakan mobilitas yang efisien. Pemahaman tentang sistem membantu individu maupun organisasi dalam mengelola sumber daya, menyelesaikan masalah, dan mencapai tujuan dengan cara yang terstruktur dan terorganisir. Dengan demikian, sistem bukan hanya sebuah konsep, tetapi juga alat yang esensial untuk keberlangsungan aktivitas manusia di berbagai bidang.

Dalam pengembangan *Smart System Home* atau *smart door lock* berbasis IoT dengan integrasi sidik jari (*fingerprint*) dan kontrol elektronik, pendekatan sistem digunakan untuk memastikan bahwa setiap komponen bekerja secara terstruktur dan efisien. Sistem keamanan rumah yang dirancang mencakup perangkat keras seperti sensor sidik jari dan modul ESP8266, perangkat lunak berbasis IoT untuk pemantauan *real-time*, serta prosedur autentikasi yang mengatur akses pengguna. Kombinasi elemen-elemen ini memungkinkan sistem untuk berfungsi secara otomatis dalam mendeteksi, mengontrol, dan memberikan notifikasi kepada pemilik rumah. Selain itu, integrasi teknologi IoT meningkatkan fleksibilitas dan adaptabilitas sistem dalam merespons ancaman keamanan serta mengoptimalkan kendali elektronik di dalam rumah. Dengan adanya hubungan antara komponen fisik dan digital, sistem ini mampu menciptakan lingkungan yang lebih aman dan efisien bagi penggunaanya.

2.1.2 Pengertian Pengamanan

Pengamanan adalah serangkaian upaya, tindakan, atau prosedur yang dilakukan untuk melindungi suatu objek, individu, sistem, atau informasi dari ancaman, bahaya, atau gangguan yang dapat merugikan. Tujuan utama pengamanan adalah menjaga integritas, keberlangsungan, dan keamanan dari berbagai aset, baik yang bersifat fisik

seperti properti maupun non-fisik seperti data dan informasi. Pengamanan dapat mencakup aspek fisik, teknologi, dan kebijakan yang saling mendukung untuk memastikan perlindungan yang optimal (Yulianto et al., 2022).

Dalam konteks fisik, pengamanan melibatkan langkah-langkah seperti pemasangan kunci, pengawasan melalui kamera pengintai (CCTV), atau penggunaan penjaga keamanan untuk melindungi bangunan atau fasilitas tertentu. Pada tingkat ini, pengamanan bertujuan untuk mencegah akses tidak sah, pencurian, atau kerusakan. Contoh lainnya adalah pengamanan rumah dengan pemasangan alarm atau kunci berbasis biometrik seperti sidik jari untuk meningkatkan perlindungan terhadap potensi ancaman (Kurnia, 2021).

Dalam dunia teknologi, pengamanan sering disebut sebagai keamanan siber atau keamanan informasi. Pengamanan dalam konteks ini melibatkan perlindungan terhadap data, sistem komputer, dan jaringan dari ancaman seperti peretasan, *malware*, atau pencurian data. Selain itu, pengamanan juga dapat mencakup langkah-langkah administratif dan kebijakan, seperti aturan dan regulasi yang mengatur akses, penggunaan, dan perlindungan aset tertentu. Misalnya, kebijakan perusahaan untuk membatasi akses hanya kepada individu yang memiliki otoritas tertentu adalah bentuk pengamanan administratif yang bertujuan untuk mengurangi risiko internal (Laksana & Mulyani, 2024).

Pengamanan yang efektif memerlukan kombinasi berbagai pendekatan, baik preventif maupun responsif. Pendekatan preventif bertujuan untuk mencegah terjadinya ancaman dengan meminimalkan kerentanan, sedangkan pendekatan responsif berfokus pada penanganan cepat dan pemulihan dari insiden yang terjadi. Misalnya, pemasangan

alarm adalah langkah preventif, sementara respons petugas keamanan setelah alarm berbunyi adalah tindakan *responsive* (Steven et al., 2023).

Dengan adanya pengamanan yang baik, potensi kerugian akibat ancaman seperti kerusakan fisik, kehilangan data, atau ancaman terhadap keselamatan manusia dapat diminimalkan. Oleh karena itu, pengamanan tidak hanya menjadi tanggung jawab individu atau organisasi tertentu, tetapi juga menjadi bagian penting dari keberlanjutan operasional dalam berbagai sektor, termasuk bisnis, pemerintahan, dan rumah tangga (Vimy et al., 2022).

Pengamanan yang efektif dalam sistem keamanan rumah berbasis IoT dengan sidik jari bertujuan untuk meningkatkan perlindungan terhadap akses yang tidak sah. Dengan memanfaatkan teknologi sidik jari dan kontrol elektronik, sistem ini memberikan keamanan yang lebih andal dibandingkan metode konvensional. Integrasi IoT memungkinkan pemilik rumah untuk memantau dan mengendalikan akses secara real-time, sehingga risiko ancaman dapat diminimalkan dan keamanan rumah menjadi lebih optimal.

2.1.3 Smart Door Lock

Smart door lock adalah sistem penguncian pintu yang menggunakan teknologi digital untuk meningkatkan keamanan dan kenyamanan pengguna. Berbeda dengan kunci konvensional yang mengandalkan mekanisme fisik seperti kunci dan gembok, *smart door lock* dapat dioperasikan menggunakan berbagai metode autentikasi, seperti sidik jari, kartu RFID, PIN, atau aplikasi berbasis *Internet of Things* (IoT). Sistem ini memungkinkan pengguna untuk membuka dan mengunci pintu tanpa

memerlukan kunci fisik, serta memberikan akses yang lebih aman dengan fitur pencatatan aktivitas pengguna secara *real-time* (Umam et al., 2023).

Smart door lock sering kali dilengkapi dengan koneksi *internet* atau *Bluetooth*, yang memungkinkan pemilik rumah untuk mengontrol akses pintu dari jarak jauh melalui *smartphone* atau perangkat lainnya. Dalam penelitian ini, pengembangan sistem pengaman pintu rumah berbasis IoT dengan teknologi pemindai sidik jari mengadopsi konsep *smart door lock* untuk meningkatkan efisiensi dan keamanan. Dengan memanfaatkan teknologi IoT, sistem ini tidak hanya memungkinkan autentikasi yang lebih akurat menggunakan sidik jari, tetapi juga mendukung fitur pemantauan akses secara *real-time*. Penggunaan pemindai sidik jari memastikan bahwa hanya individu yang telah terdaftar yang dapat membuka pintu, mengurangi risiko akses tidak sah yang sering terjadi pada sistem kunci konvensional. Integrasi dengan perangkat lain, seperti CCTV dan alarm, menjadikan *smart door lock* berbasis IoT sebagai solusi keamanan rumah yang lebih cerdas dan responsif terhadap ancaman potensial (Wahyudi et al., 2020).

2.1.4 Pengertian Sidik Jari

Sidik jari adalah pola unik yang terbentuk pada permukaan kulit ujung jari manusia, terdiri dari garis-garis lengkung, lingkaran, atau pola melingkar yang membentuk struktur kompleks. Pola ini bersifat individual dan tidak pernah sama antara satu individu dengan individu lainnya, bahkan pada orang yang memiliki hubungan biologis seperti kembar identik. Keunikan ini menjadikan sidik jari sebagai salah satu ciri biometrik yang paling sering digunakan untuk identifikasi dan verifikasi identitas seseorang (Yeni et al., 2023).

Sidik jari mulai terbentuk sejak manusia berada dalam kandungan, tepatnya pada usia kehamilan 10 hingga 16 minggu. Pola ini dipengaruhi oleh faktor genetik dan

lingkungan dalam rahim. Menariknya, pola sidik jari tidak berubah sepanjang hidup, meskipun ukuran jari dapat bertambah seiring pertumbuhan. Kerusakan pada kulit seperti luka ringan umumnya tidak memengaruhi pola dasar sidik jari, karena pola ini juga terdapat pada lapisan dermis kulit (Wati et al., 2020).

Dalam konteks ilmiah, sidik jari memiliki karakteristik utama yang digunakan untuk analisis, yaitu *minutiae points*. Karakteristik ini meliputi titik bercabang, titik akhir garis, dan pola-pola khusus lainnya yang membantu dalam proses identifikasi. Sidik jari sering dikelompokkan ke dalam beberapa kategori utama, seperti *loop* (lengkungan), *whorl* (pusaran), dan *arch* (busur). Variasi dari pola-pola ini memberikan informasi tambahan yang memperkuat keunikan sidik jari setiap individu (Hariyanto et al., 2020).

Sidik jari memiliki berbagai fungsi, baik secara biologis maupun praktis. Secara biologis, pola ini membantu manusia dalam meningkatkan daya cengkeram pada objek, terutama ketika permukaan tangan basah atau licin. Sementara itu, secara praktis, sidik jari banyak dimanfaatkan dalam berbagai bidang, seperti keamanan, forensik, dan teknologi modern. Dalam bidang forensik, sidik jari digunakan untuk mengidentifikasi pelaku kejahatan melalui jejak yang tertinggal di tempat kejadian perkara (Wati et al., 2020).

Di era digital dan teknologi informasi, sidik jari menjadi bagian penting dalam sistem keamanan biometrik. Teknologi pemindai sidik jari banyak diterapkan pada perangkat elektronik seperti ponsel, komputer, dan sistem keamanan rumah. Penggunaan sidik jari dalam teknologi ini didasarkan pada proses pengambilan pola sidik jari, mengonversinya menjadi data digital, dan mencocokkannya dengan data yang sudah tersimpan untuk verifikasi identitas (Nursyarif & Sumadi, 2022).

Penggunaan sidik jari dalam sistem keamanan modern memiliki keunggulan, seperti kepraktisan dan akurasi tinggi. Dengan hanya meletakkan jari pada pemindai, sistem dapat dengan cepat mengenali dan mengotorisasi pengguna. Teknologi ini juga sulit untuk dipalsukan, karena sidik jari seseorang tidak dapat dengan mudah direplikasi (Nursyarif & Sumadi, 2022).

Sidik jari merupakan identitas biologis yang unik, permanen, dan praktis. Hal ini menjadikannya salah satu metode identifikasi yang paling terpercaya dan sering digunakan dalam berbagai aplikasi keamanan dan teknologi.

2.1.5 Pengertian *Internet Of Things*

Internet of Things (IoT) adalah konsep teknologi yang menghubungkan berbagai perangkat fisik melalui internet untuk memungkinkan pengumpulan, pertukaran, dan analisis data secara *real-time*. IoT memungkinkan perangkat seperti sensor, perangkat rumah tangga, kendaraan, mesin industri, hingga perangkat medis untuk berkomunikasi satu sama lain tanpa interaksi manusia secara langsung. Tujuan utama dari IoT adalah menciptakan ekosistem yang cerdas, efisien, dan dapat memberikan wawasan yang berguna untuk pengambilan keputusan atau otomatisasi proses (Wilianto & Kurniawan, 2018).

Secara teknis, IoT terdiri dari tiga komponen utama: perangkat pintar (*smart devices*), jaringan komunikasi, dan platform analitik. Perangkat pintar mencakup sensor dan aktuator yang digunakan untuk menangkap data atau menjalankan tindakan tertentu. Jaringan komunikasi menghubungkan perangkat-perangkat ini ke internet, menggunakan protokol seperti *Wi-Fi*, *Bluetooth*, *Zigbee*, atau jaringan seluler. Sementara itu, platform analitik memproses dan menganalisis data yang dikumpulkan, menghasilkan wawasan yang relevan (Nahdi & Dhika, 2021).

Salah satu elemen penting dari IoT adalah sensor. Sensor digunakan untuk mengukur berbagai parameter, seperti suhu, kelembapan, tekanan, gerakan, atau posisi. Data yang dikumpulkan oleh sensor ini dikirimkan melalui jaringan ke *platform cloud* untuk disimpan dan dianalisis. Hasil analisis ini memungkinkan sistem IoT untuk mengambil keputusan atau mengontrol perangkat lain secara otomatis, seperti menyalakan lampu saat mendeteksi kehadiran seseorang atau mengatur suhu ruangan berdasarkan kondisi lingkungan. Penerapan IoT meluas di berbagai bidang, di antaranya (Malini, 2024):

1. *Smart Home*

IoT memungkinkan perangkat rumah tangga seperti termostat, lampu, kamera keamanan, dan alat rumah tangga lainnya untuk dikendalikan secara jarak jauh melalui smartphone atau perintah suara. Hal ini meningkatkan kenyamanan, keamanan, dan efisiensi energi.

2. *Healthcare*

Dalam bidang kesehatan, IoT digunakan untuk mengembangkan perangkat wearable seperti smartwatch yang dapat memantau tanda vital, memberikan peringatan dini tentang kondisi medis, atau membantu pasien dan dokter dalam pengelolaan kesehatan.

3. *Industrial IoT*

Dalam konteks ini, IoT digunakan untuk memonitor mesin, meningkatkan efisiensi produksi, dan memprediksi kerusakan mesin (predictive maintenance).

Teknologi ini sering disebut sebagai bagian dari revolusi industri 4.0.

4. *Transportasi dan Logistik*

IoT memungkinkan pelacakan barang secara real-time, optimalisasi rute kendaraan, hingga penerapan kendaraan otonom yang dapat bergerak tanpa pengemudi manusia.

5. *Smart Agriculture*

IoT membantu petani dalam mengelola lahan dengan lebih baik, seperti memantau kelembapan tanah, memprediksi cuaca, dan mengoptimalkan irigasi.

Meskipun IoT menawarkan berbagai manfaat, teknologi ini juga menghadapi tantangan, termasuk masalah keamanan data, privasi pengguna, dan integrasi antar perangkat dari berbagai vendor. Oleh karena itu, pengembangan IoT memerlukan pendekatan yang hati-hati untuk memastikan bahwa sistem yang dibangun aman, andal, dan berkelanjutan (Br. Sembiring, 2020).

Dengan kemajuan teknologi dan peningkatan konektivitas global, IoT diprediksi akan terus berkembang, menghadirkan peluang baru di berbagai sektor dan membentuk masa depan yang lebih cerdas serta terintegrasi.

2.1.6 Pengertian Otomasi

Otomasi, atau *automation*, adalah penerapan teknologi untuk menjalankan proses atau tugas tertentu secara otomatis, dengan sedikit atau tanpa campur tangan manusia. Otomasi bertujuan untuk meningkatkan efisiensi, produktivitas, dan akurasi dalam berbagai aktivitas, baik di bidang industri, bisnis, rumah tangga, maupun kehidupan sehari-hari. Dalam otomasi, teknologi seperti perangkat lunak, mesin, sensor, dan robot digunakan untuk menggantikan atau mendukung peran manusia dalam menyelesaikan pekerjaan. Konsep ini telah menjadi bagian penting dari perkembangan teknologi modern, memungkinkan pelaksanaan berbagai tugas yang sebelumnya membutuhkan waktu lama dan tenaga manusia yang signifikan (Rosidin et al., 2024).

Otomasi memiliki berbagai jenis aplikasi yang disesuaikan dengan kebutuhan spesifik di setiap sektor. Dalam industri manufaktur, misalnya, otomasi diterapkan melalui penggunaan robot untuk proses perakitan, pengemasan, atau pengujian produk. Teknologi seperti kontrol numerik komputer (CNC) digunakan untuk mengoperasikan mesin dengan presisi tinggi. Selain itu, otomasi rumah atau smart home automation memungkinkan perangkat rumah tangga seperti lampu, termostat, dan kamera keamanan dioperasikan secara otomatis atau dikendalikan dari jarak jauh melalui *smartphone*. Di sektor bisnis, otomasi diterapkan untuk mengelola proses administrasi, seperti pengiriman email massal, pemrosesan data pelanggan, atau pelaporan keuangan menggunakan perangkat lunak khusus (Rozy, 2023).

Salah satu aspek penting dari otomasi adalah penggunaan sensor dan aktuator. Sensor bertugas mengumpulkan data dari lingkungan, seperti suhu, tekanan, atau kelembapan, sementara aktuator digunakan untuk mengeksekusi tindakan tertentu, seperti membuka katup atau menggerakkan motor. Data yang dikumpulkan oleh sensor ini diproses oleh sistem kontroler, yang kemudian menentukan langkah selanjutnya berdasarkan algoritma yang telah diprogram sebelumnya. Dengan demikian, proses yang dilakukan menjadi lebih efisien dan terstruktur (Muzakki & Irianto, 2022).

Penerapan otomasi membawa banyak manfaat, di antaranya adalah efisiensi waktu, pengurangan biaya operasional, dan peningkatan konsistensi. Dengan otomasi, pekerjaan yang membutuhkan waktu lama dapat diselesaikan lebih cepat, dan hasilnya lebih konsisten karena minimnya faktor kesalahan manusia. Di sisi lain, otomasi juga memungkinkan peningkatan keselamatan kerja, terutama pada pekerjaan yang berisiko tinggi, seperti operasi di lingkungan berbahaya atau penanganan material beracun. Selain

itu, otomasi memungkinkan analisis data secara *real-time*, yang mendukung pengambilan keputusan yang lebih baik dan lebih cepat (Alayida et al., 2023).

Namun, otomasi tidak lepas dari tantangan. Salah satu tantangan utama adalah biaya investasi awal yang tinggi, terutama dalam pengadaan teknologi canggih seperti robot atau sistem IoT (*Internet of Things*). Selain itu, otomasi juga menimbulkan dampak sosial, seperti berkurangnya lapangan kerja manual, yang dapat memengaruhi tenaga kerja di sektor tertentu. Keamanan siber juga menjadi perhatian, karena banyak sistem otomatis yang terhubung ke internet rentan terhadap ancaman peretasan (Alayida et al., 2023).

Otomasi merupakan bagian integral dari transformasi teknologi yang terus berkembang. Dengan kemajuan di bidang kecerdasan buatan, pembelajaran mesin, dan IoT, otomasi semakin canggih dan berpotensi mengubah berbagai aspek kehidupan manusia. Meskipun memiliki tantangan, keunggulan yang ditawarkan oleh otomasi menjadikannya solusi penting dalam menciptakan sistem yang lebih efisien, aman, dan produktif (Nahuway, 2024).

1. Jenis-jenis Otomasi

- a. Otomasi ini digunakan di pabrik atau sektor manufaktur untuk mengendalikan proses produksi. Contohnya adalah penggunaan robot industri untuk merakit kendaraan, mesin CNC untuk pemotongan presisi, dan sistem *conveyor* otomatis untuk transportasi barang.
- b. Dalam kehidupan sehari-hari, otomasi diterapkan untuk meningkatkan kenyamanan dan keamanan rumah. Contohnya termasuk lampu otomatis yang menyala saat mendeteksi gerakan, pengaturan suhu ruangan

menggunakan termostat pintar, atau perangkat IoT yang terhubung untuk mengontrol peralatan rumah tangga dari jarak jauh.

- c. Dalam dunia bisnis, otomatisasi membantu menyelesaikan tugas-tugas administratif, seperti pengelolaan data, pengiriman email, atau pelaporan. Sistem manajemen pelanggan (CRM) dan perangkat lunak alur kerja adalah contoh alat yang digunakan untuk otomatisasi ini.
- d. Sistem transportasi *modern*, seperti kereta cepat atau kendaraan otonom, menggunakan otomasi untuk meningkatkan efisiensi, keselamatan, dan kecepatan layanan. Teknologi seperti autopilot pada pesawat terbang atau sistem navigasi cerdas pada kendaraan adalah bagian dari otomasi ini.
- e. Otomasi dalam pertanian melibatkan penggunaan teknologi seperti drone untuk pemantauan tanaman, sistem irigasi otomatis, atau traktor otonom untuk pengolahan tanah.
- f. Otomasi juga diterapkan pada pelayanan masyarakat, seperti penggunaan mesin tiket di stasiun, pembayaran tol otomatis, atau chatbot untuk layanan pelanggan.

2. Manfaat Otomasi

- a. Otomasi memungkinkan pekerjaan selesai lebih cepat dibandingkan dengan proses manual.
- b. Sistem otomatis cenderung lebih konsisten dan akurat dibandingkan pekerjaan yang dilakukan oleh manusia.
- c. Dalam jangka panjang, otomatisasi dapat mengurangi biaya operasional dengan mengurangi ketergantungan pada tenaga kerja manual.

- d. Dalam pekerjaan berisiko tinggi, otomasi melindungi manusia dari bahaya fisik.

3. Tantangan Otomasi

Namun, otomasi juga memiliki tantangan, seperti kebutuhan investasi awal yang tinggi, dampak sosial berupa berkurangnya lapangan kerja manual, serta risiko keamanan siber pada sistem otomatis yang terhubung dengan *internet*.

Dengan perkembangan teknologi, terutama kecerdasan buatan dan IoT, otomasi terus mengalami peningkatan yang signifikan, menciptakan peluang baru untuk berbagai sektor dan mendefinisikan ulang cara manusia bekerja dan hidup.

2.1.7 Pengertian *Internet*

Internet adalah jaringan global yang menghubungkan miliaran perangkat di seluruh dunia, memungkinkan pertukaran informasi secara cepat dan efisien. Sebagai sistem komunikasi terbesar yang pernah ada, internet menghubungkan komputer, *smartphone*, dan perangkat pintar lainnya melalui protokol standar yang dikenal sebagai TCP/IP (*Transmission Control Protocol/Internet Protocol*). Dengan internet, pengguna dapat mengakses berbagai layanan seperti email, media sosial, mesin pencari, dan aplikasi berbasis web, yang semuanya dirancang untuk memfasilitasi komunikasi, pertukaran data, dan akses informasi dalam hitungan detik (Peniarsih, 2020).

Internet berfungsi sebagai infrastruktur utama yang mendukung berbagai teknologi modern, termasuk *cloud computing*, *Internet of Things* (IoT), dan kecerdasan buatan (AI). Sejak awal perkembangannya pada akhir 1960-an sebagai proyek ARPANET yang dikelola oleh Departemen Pertahanan Amerika Serikat, internet telah berkembang pesat menjadi jaringan global yang digunakan oleh individu, organisasi, hingga pemerintahan di seluruh dunia. Pada intinya, internet bekerja dengan cara

mengirimkan data dalam bentuk paket-paket kecil melalui jaringan kabel, serat optik, atau gelombang radio, dari satu perangkat ke perangkat lainnya, menggunakan alamat IP sebagai identitas unik masing-masing perangkat (Barus et al., 2024).

Salah satu fitur utama internet adalah kemampuannya untuk menyediakan akses ke informasi dalam berbagai bentuk, seperti teks, gambar, *audio*, dan *video*. Melalui *World Wide Web* (WWW), pengguna dapat mengakses situs web yang menyediakan informasi, layanan, atau hiburan dengan menggunakan browser. Mesin pencari seperti *Google* memudahkan pengguna menemukan informasi yang mereka butuhkan di antara miliaran halaman web yang tersedia. Selain itu, internet juga memungkinkan komunikasi *real-time* melalui email, panggilan *video*, atau aplikasi pesan instan, sehingga dunia terasa lebih kecil dan lebih terhubung (Guk Guk et al., 2023).

Internet telah membawa banyak manfaat dalam berbagai aspek kehidupan. Dalam pendidikan, internet memberikan akses ke sumber belajar tanpa batas, mulai dari artikel, *e-book*, hingga kursus daring. Di bidang bisnis, internet memungkinkan transaksi *e-commerce*, pemasaran digital, dan komunikasi lintas negara secara mudah. Di sektor hiburan, internet menjadi *platform* untuk streaming *video*, musik, dan permainan daring. Selain itu, internet juga memainkan peran penting dalam inovasi teknologi, seperti otomatisasi industri, layanan berbasis cloud, dan pengembangan aplikasi berbasis data besar (*big data*) (Matiti et al., 2024).

Namun, di balik manfaatnya yang luar biasa, internet juga menghadirkan tantangan, seperti masalah keamanan dan privasi data. Dengan meningkatnya ketergantungan pada *internet*, risiko serangan siber, pencurian data, dan penyebaran informasi palsu juga meningkat. Selain itu, akses yang tidak merata ke internet di berbagai belahan dunia menciptakan kesenjangan digital, yang memengaruhi kemampuan individu

dan masyarakat untuk memanfaatkan peluang yang ditawarkan oleh internet secara maksimal (Br. Sembiring, 2020).

Dengan perkembangan teknologi yang terus berlangsung, internet akan semakin berkembang menjadi jaringan yang lebih cerdas dan lebih cepat, seperti yang terlihat pada implementasi jaringan 5G dan teknologi fiber optik. Sebagai bagian tak terpisahkan dari kehidupan modern, internet telah mengubah cara manusia berkomunikasi, bekerja, belajar, dan menikmati hiburan, menjadikannya salah satu inovasi paling revolusioner dalam sejarah manusia.

2.1 Teori Khusus

2.2.1 Metode *Prototype*

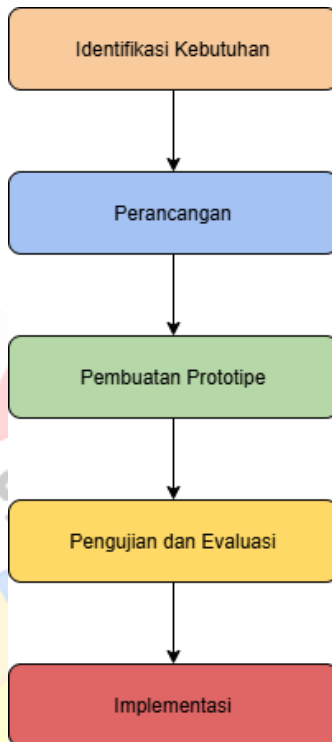
Metode *Prototype* adalah salah satu pendekatan dalam pengembangan perangkat lunak yang berfokus pada pembuatan model atau prototipe awal dari sistem yang akan dibangun. Prototipe ini berfungsi sebagai gambaran awal dari produk akhir dan dikembangkan untuk mendapatkan umpan balik langsung dari pengguna atau klien, yang kemudian digunakan untuk memperbaiki dan mengembangkan sistem lebih lanjut. Metode ini memungkinkan pengembang untuk mendemonstrasikan sebagian fungsi dari aplikasi kepada pengguna sejak tahap awal, sehingga mereka dapat memberikan masukan mengenai fungsionalitas, tampilan, dan kegunaan sistem (Fridayanthie et al., 2021).

Proses pembuatan *prototipe* dimulai dengan mengumpulkan persyaratan dasar dari pengguna tanpa terlalu mendalami rincian teknis pada awalnya. Selanjutnya, prototipe awal yang mencakup fitur-fitur utama sistem dikembangkan dengan cepat. Prototipe ini biasanya tidak lengkap dan mungkin hanya mencakup antarmuka pengguna dan beberapa fungsionalitas dasar. Setelah prototipe dikembangkan, pengguna dapat mencoba dan mengevaluasi sistem tersebut, memberikan umpan balik yang berharga

tentang kelebihan dan kekurangannya. Umpan balik ini kemudian digunakan untuk memperbaiki dan mengembangkan prototipe lebih lanjut, sehingga siklus pengembangan menjadi iterative (Kurniati, 2021).

Salah satu keunggulan utama metode *Prototype* adalah kemampuannya untuk mengurangi ketidakpastian dalam pengembangan perangkat lunak. Dengan adanya prototipe yang dapat dilihat dan diuji oleh pengguna, pengembang dapat lebih mudah memahami kebutuhan dan harapan pengguna. Selain itu, perubahan atau penyesuaian terhadap sistem dapat dilakukan dengan cepat karena pengembangan sistem dilakukan secara bertahap dan berkelanjutan berdasarkan umpan balik yang diterima. Pendekatan ini sangat efektif dalam proyek yang memiliki persyaratan yang tidak sepenuhnya jelas atau mudah diidentifikasi sejak awal (Wanas et al., 2015).

Metode *Prototype* juga membantu mengurangi risiko kesalahan pengembangan karena pengguna terlibat langsung dalam proses pembuatan sistem. Selain itu, prototipe yang diperbarui secara berkala memungkinkan pengembang untuk menyesuaikan fungsionalitas sesuai dengan kebutuhan yang terus berkembang. Namun, meskipun memiliki banyak keunggulan, metode ini juga memiliki beberapa kelemahan, seperti potensi biaya yang lebih tinggi akibat pengembangan ulang yang sering dilakukan, dan kemungkinan pengguna terlalu fokus pada antarmuka pengguna tanpa mempertimbangkan aspek teknis lainnya (Fridayanthie et al., 2021).



Gambar 2. 1 Tahapan Metode Prototype

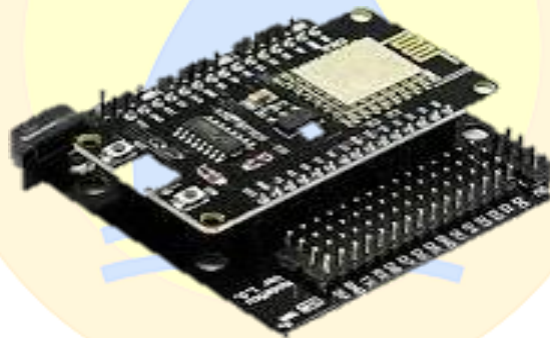
Metode *Prototype* sangat cocok diterapkan pada proyek perangkat lunak dengan ketidakpastian tinggi atau ketika klien sulit mendefinisikan secara rinci apa yang mereka inginkan. Dengan memberikan gambaran visual dan fungsional yang konkret, metode ini mempercepat komunikasi antara pengembang dan pengguna, sehingga produk akhir dapat lebih sesuai dengan harapan pengguna.

2.2.2 **Mikrokontroler ESP 8266**

ESP8266 adalah mikrokontroler yang dikembangkan oleh *Espressif Systems*, yang dikenal sebagai solusi serbaguna untuk berbagai aplikasi IoT (*Internet of Things*) dan perangkat elektronik pintar. Dilengkapi dengan fitur *dual-core* atau *single-core processor* Xtensa LX6, ESP8266 menawarkan kinerja tinggi yang dapat menangani tugas-tugas kompleks sekaligus efisien dalam konsumsi daya. *Mikrokontroler* ini

dirancang dengan konektivitas bawaan seperti *Wi-Fi* dan *Bluetooth*, menjadikannya pilihan ideal untuk aplikasi yang membutuhkan komunikasi nirkabel (Nizam et al., 2022).

Salah satu keunggulan utama ESP8266 adalah integrasi yang tinggi. Mikrokontroler ini dilengkapi dengan modul *Wi-Fi* 802.11 b/g/n dan *Bluetooth* 4.2, termasuk BLE (*Bluetooth Low Energy*), yang memungkinkan konektivitas yang cepat dan hemat daya. Fitur ini membuat ESP8266 sangat populer dalam pengembangan perangkat IoT seperti sensor lingkungan, kontrol rumah pintar, dan sistem automasi industri. Selain itu, ESP8266 memiliki fitur tambahan seperti ADC (*Analog to Digital Converter*), DAC (*Digital to Analog Converter*), I2C, SPI, UART, dan PWM, yang mendukung berbagai kebutuhan antarmuka perangkat keras (Nizam et al., 2022).



Gambar 2. 2 Mikrokontroler ESP8266

Dalam hal performa, ESP8266 mendukung kecepatan clock hingga 240 MHz dan memiliki RAM internal sebesar 520 KB, yang cukup untuk menjalankan aplikasi yang membutuhkan daya komputasi tinggi. Mikrokontroler ini juga dilengkapi dengan fitur keamanan canggih seperti enkripsi data, *secure boot*, dan *flash encryption*, yang sangat

penting untuk aplikasi yang membutuhkan perlindungan terhadap akses tidak sah (Widyatmika et al., 2021).

Keberadaan GPIO (*General Purpose Input Output*) yang banyak pada ESP8266 memungkinkan pengguna untuk menghubungkan berbagai perangkat eksternal, seperti *sensor*, *relay*, motor, dan modul lainnya. Selain itu, ESP8266 mendukung pemrograman melalui berbagai platform seperti *Arduino IDE*, dan *ESP-IDF (Espressif IoT Development Framework)*, sehingga memudahkan pengembang dengan tingkat keahlian berbeda untuk memanfaatkan fitur-fiturnya (Nizam et al., 2022).

Salah satu aspek yang membuat ESP8266 menonjol adalah konsumsi dayanya yang rendah. Dengan fitur seperti *mode deep-sleep*, ESP8266 dapat beroperasi dalam kondisi hemat daya, yang sangat berguna untuk aplikasi yang membutuhkan perangkat berjalan dalam waktu lama dengan baterai. Mode ini memungkinkan ESP8266 hanya mengonsumsi daya beberapa *mikroampere*, sehingga sangat efisien untuk aplikasi sensor jarak jauh atau perangkat *wearable* (Prabowo et al., 2022).

Dalam pengembangan perangkat IoT, ESP8266 sering digunakan untuk berbagai aplikasi seperti pengendali suhu, sistem keamanan rumah, pengelolaan energi, dan sistem pemantauan lingkungan. Fleksibilitas dan kemampuannya untuk menangani berbagai jenis antarmuka dan protokol komunikasi menjadikannya pilihan yang andal dalam berbagai scenario (Lasera & Wahyudi, 2020).

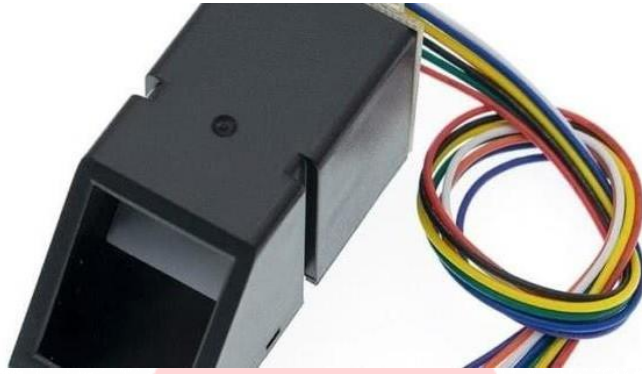
Dalam konteks *smart door lock*, ESP8266 berperan sebagai modul utama yang menghubungkan sistem kunci pintar dengan jaringan IoT, memungkinkan pengguna untuk mengontrol akses pintu dari jarak jauh melalui aplikasi atau platform berbasis web. Konsumsi daya yang rendah dari ESP8266, terutama dengan fitur *deep-sleep*, sangat menguntungkan untuk meningkatkan efisiensi energi perangkat, sehingga sistem dapat

beroperasi lebih lama dengan daya minimal. Selain itu, fleksibilitas *ESP8266* dalam menangani berbagai protokol komunikasi mendukung integrasi dengan sensor keamanan tambahan, seperti *fingerprint* atau *face recognition*, guna meningkatkan keamanan dan kenyamanan pengguna dalam sistem *smart door lock*.

2.2.3 Optical Fingerprint Sensor AS608

Optical Fingerprint Sensor AS608 adalah sensor biometrik yang dirancang untuk membaca, mengidentifikasi, dan memverifikasi sidik jari dengan akurasi tinggi menggunakan teknologi optik. Sensor ini bekerja dengan menangkap gambar sidik jari yang ditempatkan pada permukaan kaca optik, lalu memprosesnya menjadi data digital untuk analisis dan pencocokan. Dengan kemampuan untuk menyimpan hingga 128 template sidik jari di memori internalnya, AS608 memungkinkan proses identifikasi dan autentikasi dilakukan dengan cepat dan efisien. Sensor ini menggunakan modul optik canggih yang dapat menghasilkan gambar dengan resolusi tinggi, bahkan dalam kondisi lingkungan yang menantang, seperti pencahayaan rendah atau suhu ekstrem (Nasiroh, 2022).

AS608 memiliki prosesor internal untuk pengolahan data sidik jari, termasuk pembuatan template unik dan pencocokan data dengan informasi yang sudah tersimpan. Komunikasi antara sensor dan perangkat lain dilakukan melalui antarmuka serial TTL, yang sederhana dan kompatibel dengan berbagai mikrokontroler seperti *Arduino*, *Raspberry Pi*, dan *ESP8266*. Protokol komunikasi ini mendukung berbagai perintah, seperti pendaftaran sidik jari, penghapusan data, dan verifikasi, sehingga memudahkan integrasi dengan sistem lain (Jepri, Hendrayudi, 2022).



Gambar 2. 3 *Optical Fingerprint Sensor AS608*

Sensor ini dirancang dengan dimensi kompak dan permukaan kaca optik yang tahan lama, menjadikannya cocok untuk berbagai aplikasi, seperti sistem keamanan, kontrol akses, mesin absensi, hingga proyek IoT berbasis biometrik. Dengan tingkat akurasi dan kecepatan yang tinggi, AS608 mampu mengenali sidik jari dengan tingkat kesalahan rendah dalam hitungan milidetik, menjadikannya andal untuk keperluan personal maupun profesional (Akbar & Darmana, 2022).

Keunggulan utama AS608 terletak pada fleksibilitas penggunaannya dan kemudahan integrasi. Sensor ini sering digunakan dalam sistem keamanan rumah, perangkat pintar, dan proyek DIY, berkat dukungan dokumentasi yang luas dan komunitas pengembang yang aktif. Permukaan kaca optiknya dirancang tahan gores dan aus, sehingga dapat digunakan dalam jangka waktu lama tanpa penurunan kualitas. Dengan fitur hemat daya, AS608 juga cocok untuk aplikasi portabel yang membutuhkan efisiensi energi (Jepri, Hendrayudi, 2022).

Dalam sistem *smart door lock*, sensor AS608 berperan sebagai komponen utama dalam autentikasi berbasis sidik jari, menawarkan tingkat keamanan yang lebih tinggi dibandingkan metode PIN atau kartu akses. Dengan akurasi tinggi dan respon cepat, sensor ini memastikan akses yang efisien dan aman bagi pengguna. Permukaan kaca optiknya yang tahan lama membuatnya cocok untuk penggunaan jangka panjang tanpa

degradasi kualitas. Selain itu, kemudahan integrasi AS608 dengan mikrokontroler seperti ESP8266 memungkinkan pengembangan sistem keamanan rumah berbasis IoT yang lebih fleksibel dan hemat daya.

2.2.4 LCD i2C

LCD I2C adalah modul tampilan berbasis teknologi *Liquid Crystal Display* (LCD) yang dilengkapi dengan antarmuka komunikasi I2C (*Inter-Integrated Circuit*). Modul ini dirancang untuk mempermudah pengendalian LCD menggunakan koneksi yang lebih sederhana, mengurangi kebutuhan akan banyak pin pada mikrokontroler. Dalam modul LCD biasa, penggunaan hingga 16 pin untuk mengontrol layar dapat menjadi tantangan, terutama pada proyek dengan keterbatasan pin. Dengan antarmuka I2C, hanya dua pin, yaitu SDA (*Serial Data*) dan SCL (*Serial Clock*), diperlukan untuk menghubungkan LCD dengan mikrokontroler seperti *Arduino*, ESP8266, atau *Raspberry Pi* (Suryantoro, 2019).

LCD I2C biasanya menggunakan chip PCF8574 sebagai pengendali komunikasi. *Chip* ini bertindak sebagai konverter sinyal dari protokol I2C ke format paralel yang dibutuhkan oleh layar LCD. Modul ini mendukung tampilan teks pada layar dalam berbagai konfigurasi, seperti 16x2 (16 karakter per baris, dua baris) atau 20x4 (20 karakter per baris, empat baris). Fitur ini memungkinkan pengguna menampilkan informasi seperti status sensor, waktu, suhu, atau data lainnya dalam proyek elektronik (Suryantoro, 2019).

Keunggulan utama LCD I2C adalah kesederhanaan dalam pengkabelan dan efisiensi pemrograman. Dengan antarmuka I2C, pengembang dapat menghemat pin mikrokontroler untuk keperluan lain, sehingga modul ini sangat cocok untuk aplikasi dengan perangkat keras yang kompleks. Selain itu, banyak pustaka (*library*) yang tersedia untuk mendukung LCD I2C, seperti *LiquidCrystal_I2C* pada *Arduino*, yang mempermudah proses pengkodean. Pustaka ini menyediakan fungsi-fungsi bawaan untuk

menulis teks, mengatur posisi kursor, atau menghapus layar dengan mudah (Nugraha et al., 2023).



Gambar 2. 4 LCD I2C

Selain efisiensi, modul ini juga menawarkan fleksibilitas dengan kemampuan untuk mengatur alamat I2C-nya melalui jumper pada modul. Hal ini memungkinkan penggunaan beberapa LCD I2C secara bersamaan pada satu mikrokontroler, asalkan setiap modul memiliki alamat I2C yang berbeda (Nugraha et al., 2023). LCD I2C sering digunakan dalam berbagai aplikasi seperti sistem *monitoring*, antarmuka pengguna (HMI), atau proyek DIY yang memerlukan tampilan visual. Dengan konsumsi daya yang rendah dan kompatibilitas yang tinggi dengan berbagai *platform*, modul ini menjadi solusi yang ideal untuk proyek elektronik modern.

Dalam sistem *smart door lock*, LCD I2C berperan sebagai antarmuka visual yang menampilkan status kunci, notifikasi akses, atau pesan kesalahan kepada pengguna. Dengan konsumsi daya rendah dan kompatibilitas tinggi, modul ini dapat dengan mudah diintegrasikan dengan mikrokontroler seperti ESP8266 untuk menampilkan informasi autentikasi sidik jari atau instruksi operasional lainnya. Fleksibilitas dalam pengaturan alamat I2C juga memungkinkan penggunaan beberapa modul LCD dalam satu sistem, mendukung pengembangan *smart door lock* yang lebih interaktif dan informatif.

2.2.5 RFID RC522

RFID RC522 adalah modul pembaca RFID (*Radio Frequency Identification*) yang digunakan untuk mengidentifikasi dan membaca tag RFID menggunakan gelombang radio. Modul ini bekerja pada frekuensi 13,56 MHz dan sering digunakan dalam aplikasi seperti kontrol akses, sistem absensi, pembayaran tanpa kontak, serta berbagai proyek berbasis *Internet of Things* (IoT). RC522 adalah modul yang murah dan mudah diintegrasikan dengan berbagai mikrokontroler, seperti *Arduino*, *Raspberry Pi*, dan ESP8266, menjadikannya pilihan populer untuk berbagai aplikasi (Muzaki et al., 2024).

Modul RFID RC522 menggunakan teknologi MFRC522 sebagai *chip* pengendali, yang memungkinkan pembacaan tag RFID dalam jarak pendek, biasanya hingga beberapa sentimeter. Tag RFID yang digunakan bersama RC522 dapat berupa kartu, gantungan kunci, atau label RFID yang berisi informasi unik yang dapat dipindai oleh pembaca. Modul ini terhubung ke mikrokontroler melalui antarmuka SPI (*Serial Peripheral Interface*), yang memungkinkan komunikasi data yang cepat dan efisien antara pembaca dan mikrokontroler (Belada et al., 2019).

Salah satu keunggulan RC522 adalah kemampuannya untuk mendukung berbagai jenis tag RFID, seperti *MIFARE Classic* dan *MIFARE Ultralight*, yang memungkinkan fleksibilitas dalam pemilihan tag sesuai kebutuhan aplikasi. Modul ini juga dapat mengakses data yang disimpan dalam tag RFID dan mentransfer informasi tersebut ke sistem kontrol atau perangkat lain untuk diproses lebih lanjut. Misalnya, dalam sistem absensi, RC522 dapat membaca ID kartu RFID yang dibawa oleh pengguna dan menyimpannya untuk tujuan pengolahan data atau verifikasi (Zakaria & Prihantara, 2020).



Gambar 2. 5 RFID RC522

Selain itu, RC522 dilengkapi dengan berbagai fitur keamanan, seperti enkripsi untuk melindungi komunikasi antara pembaca dan tag *RFID*. Ini membuatnya lebih aman digunakan dalam aplikasi sensitif, seperti kontrol akses pintu dan sistem pembayaran. Kemudahan integrasi dan dokumentasi lengkap membuat modul ini sangat diminati oleh pengembang dan hobiis elektronik, yang sering menggunakannya dalam prototipe dan proyek berbasis mikrokontroler (Nataliana et al., 2019).

Modul *RFID* RC522 juga dikenal dengan kemudahan penggunaan dalam pemrograman. Berbagai pustaka (*library*) tersedia untuk platform seperti Arduino, yang memungkinkan pengembang untuk dengan cepat memulai penggunaan RC522 tanpa harus menulis kode yang kompleks. Fungsi-fungsi seperti membaca tag, menulis data ke tag, dan mengatur alamat tag dapat dilakukan dengan perintah yang sederhana, mempercepat proses pengembangan aplikasi (Arlina et al., 2023).

Dalam sistem *smart door lock*, modul *RFID* RC522 dapat digunakan sebagai alternatif atau pelengkap autentikasi sidik jari, memungkinkan akses menggunakan kartu

atau tag RFID. Dengan fitur enkripsi dan keamanan yang tinggi, modul ini memastikan bahwa komunikasi antara pembaca dan tag RFID terlindungi dari manipulasi. Kemudahan integrasi dengan *mikrokontroler* seperti ESP8266 atau Arduino membuatnya cocok untuk diterapkan dalam sistem kontrol akses rumah atau kantor, memberikan fleksibilitas tambahan dalam metode autentikasi pengguna.

2.2.6 ***Solenoid Lock 12V DC***

Solenoid Lock 12V DC adalah perangkat pengunci elektronik yang menggunakan prinsip elektromagnetik untuk mengunci dan membuka pintu atau objek lainnya. *Solenoid* ini bekerja dengan cara menggerakkan batang atau mekanisme pengunci menggunakan gaya magnet yang dihasilkan oleh kumparan solenoid saat diberi arus listrik 12V DC. Ketika listrik mengalir melalui kumparan solenoid, medan magnet terbentuk dan menarik atau mendorong batang logam yang terhubung dengan mekanisme pengunci. Proses ini mengunci atau membuka kunci perangkat, tergantung pada arah aliran arus dan desain solenoid tersebut (Ari Ramadhan et al., 2020).



Gambar 2. 6 *Solenoid Lock 12V DC*

Solenoid Lock 12V DC sering digunakan dalam aplikasi keamanan dan otomasi, seperti sistem kontrol akses pintu, kotak penyimpanan, dan perangkat lainnya yang

memerlukan penguncian elektronik. Kelebihannya adalah kemudahan dalam mengontrol kunci melalui sinyal listrik, yang dapat diaktifkan oleh berbagai perangkat seperti tombol, kartu *RFID*, atau sistem kendali jarak jauh. Modul pengunci ini juga dapat dipasangkan dengan mikrokontroler seperti *Arduino*, *Raspberry Pi*, atau ESP8266 untuk membuat sistem keamanan yang lebih kompleks dan terintegrasi (Asih & Hasibuan, 2023).

Salah satu keuntungan utama dari *Solenoid Lock* 12V DC adalah kemampuannya untuk bekerja dengan daya rendah dan relatif mudah dioperasikan. Biasanya, ketika aliran listrik dimatikan, *solenoid* akan mengembalikan posisinya ke keadaan terkunci, sedangkan saat aliran listrik menyala, *solenoid* membuka mekanisme pengunci dan memungkinkan akses. Desain yang sederhana ini memungkinkan penggunaan dalam berbagai jenis aplikasi dengan biaya rendah (Asih & Hasibuan, 2023).

Solenoid lock juga menawarkan tingkat keandalan yang tinggi dalam jangka panjang, asalkan perawatan dilakukan secara rutin dan tidak terjadi kerusakan pada komponen listriknya. Meskipun demikian, pengunci ini cenderung tidak dapat diandalkan untuk aplikasi dengan tingkat keamanan yang sangat tinggi karena tergantung sepenuhnya pada sumber daya listrik untuk berfungsi. Oleh karena itu, untuk aplikasi kritis, seringkali *solenoid lock* digunakan bersama dengan sistem pengamanan lainnya, seperti alarm atau pengunci fisik tambahan (Asih & Hasibuan, 2023).

Dalam sistem *smart door lock*, *Solenoid Lock* 12V DC berperan sebagai mekanisme utama dalam mengunci dan membuka pintu secara otomatis. Dengan kemampuannya untuk diintegrasikan dengan mikrokontroler seperti ESP8266, *solenoid lock* dapat dikendalikan melalui autentikasi *fingerprint*, *RFID*, atau PIN. Namun, karena ketergantungannya pada listrik, sistem ini sering dikombinasikan dengan sumber daya

cadangan atau mekanisme manual untuk memastikan tetap berfungsi dalam kondisi darurat.

2.2.7 *Arduino IDE*

Arduino IDE (Integrated Development Environment) adalah perangkat lunak yang digunakan untuk menulis, mengedit, dan mengunggah kode program ke papan mikrokontroler *Arduino*. IDE ini dirancang untuk mempermudah pengembangan perangkat keras dan perangkat lunak dalam ekosistem *Arduino*, sehingga memungkinkan para pengembang, hobiis, dan pembuat prototipe untuk dengan mudah membuat dan menguji proyek elektronik berbasis mikrokontroler. *Arduino IDE* mendukung berbagai jenis papan *Arduino* seperti *Arduino Uno*, *Mega*, *Nano*, dan lainnya, serta berbagai board berbasis mikroprosesor yang kompatibel dengan *Arduino* (Agustanti et al., 2022).

Salah satu fitur utama dari *Arduino IDE* adalah antarmuka pengguna yang sederhana dan mudah dipahami, meskipun sangat kuat dalam mendukung berbagai proyek elektronik. IDE ini menyediakan editor kode dengan sintaksis yang mudah dibaca, serta berbagai pustaka (*library*) dan contoh kode yang memungkinkan pengguna untuk memulai dengan cepat. *Arduino IDE* menggunakan bahasa pemrograman yang berbasis C/C++, namun dengan banyak fungsi dan abstraksi yang memudahkan pemrogram untuk menulis kode tanpa harus memahami semua detail teknis tentang mikrokontroler yang digunakan (Agustanti et al., 2022).

Setelah kode selesai ditulis dan diuji, pengguna dapat mengunggahnya ke papan *Arduino* melalui kabel USB. *Arduino IDE* secara otomatis mengonversi kode menjadi bahasa mesin yang dapat dipahami oleh mikrokontroler. Proses ini memudahkan pengguna untuk melihat hasil dari perubahan kode secara langsung, yang sangat

bermanfaat dalam eksperimen dan pengembangan perangkat keras berbasis mikrokontroler (Hermawanto & Herlambang, 2024).

Arduino IDE juga mendukung berbagai fitur debugging dan monitoring. Pengguna dapat memantau data dari *board* menggunakan *Serial Monitor* untuk memeriksa status sensor, melihat pesan kesalahan, atau melakukan *troubleshooting* pada program yang sedang berjalan. Selain itu, IDE ini mendukung pemrograman langsung melalui protokol serial, sehingga memungkinkan interaksi *real-time* antara perangkat keras dan perangkat lunak (Shiddiqi et al., 2021).

Kompatibilitas *Arduino* IDE dengan berbagai sistem operasi, seperti *Windows*, *macOS*, dan *Linux*, memungkinkan pengguna dari berbagai platform untuk mengakses dan mengembangkan proyek mereka tanpa hambatan. *Arduino* IDE juga memiliki ekosistem pustaka yang sangat besar, yang mencakup berbagai modul dan perangkat tambahan seperti sensor, motor, modul komunikasi, dan lain-lain, yang memudahkan integrasi dengan perangkat keras lain (Salwa, 2024).

Dalam sistem *smart door lock* berbasis IoT, *Arduino* IDE berperan penting sebagai platform utama untuk pemrograman dan *debugging mikrokontroler* seperti *ESP8266*. Dengan fitur *Serial Monitor*, pengembang dapat memantau komunikasi antara sensor sidik jari, modul RFID, atau *solenoid lock* secara *real-time*, memastikan sistem berfungsi dengan baik. Dukungan terhadap berbagai pustaka juga mempercepat pengembangan, memungkinkan integrasi yang lebih mudah dengan komponen tambahan untuk meningkatkan keamanan dan efisiensi sistem.

2.2 Teori Analisa & Perancangan

2.3.1 Block Diagram

Block diagram adalah representasi grafis dari suatu sistem, proses, atau perangkat yang digunakan untuk menggambarkan hubungan antar komponen atau sub-sistem secara sederhana dan jelas. Dalam *block diagram*, setiap komponen atau proses digambarkan dalam bentuk kotak (*block*), yang dihubungkan dengan garis atau panah untuk menunjukkan aliran informasi, energi, atau kontrol di dalam sistem. *Block diagram* sering digunakan dalam berbagai bidang, seperti rekayasa perangkat keras, pengembangan perangkat lunak, sistem kendali, dan desain sirkuit elektronik, untuk memberikan gambaran keseluruhan yang mudah dipahami tanpa harus masuk ke rincian teknis yang kompleks (Rosihan & Yuniarto, 2019).

Block diagram menyederhanakan representasi sistem yang rumit dengan menghilangkan detail operasional dan fokus pada hubungan antar bagian utama sistem. Setiap blok dalam diagram mewakili fungsi atau komponen tertentu, sedangkan garis atau panah menunjukkan aliran data atau sinyal antar blok tersebut. Dalam konteks sistem perangkat keras, misalnya, sebuah *block diagram* dapat menggambarkan hubungan antara mikrokontroler, sensor, aktuator, dan antarmuka pengguna. Untuk sistem perangkat lunak, diagram ini bisa menggambarkan alur data atau interaksi antara modul-modul perangkat lunak yang berbeda (Hartono, 2023)v.

Salah satu keunggulan *block diagram* adalah kemampuannya untuk memberikan gambaran sistem secara keseluruhan tanpa memerlukan pengetahuan teknis mendalam. Hal ini membuatnya sangat berguna dalam tahap perencanaan dan komunikasi antara tim pengembang, manajer proyek, atau pemangku kepentingan lainnya. *Block diagram* juga memudahkan identifikasi komponen-komponen penting dalam sistem serta hubungan

dan aliran data antar komponen tersebut. Dengan cara ini, diagram ini juga menjadi alat yang efektif dalam mengidentifikasi potensi masalah atau hambatan dalam desain sistem sebelum implementasi yang lebih rinci dilakukan (Wijoyo & Akbar, 2021).

Dalam desain perangkat keras, *block diagram* dapat digunakan untuk merencanakan dan memvisualisasikan koneksi antara berbagai elemen, seperti mikroprosesor, memori, antarmuka komunikasi, dan sensor. Dalam pengembangan perangkat lunak, *block diagram* sering digunakan untuk menggambarkan struktur modular dari aplikasi dan bagaimana data mengalir antara modul-modul tersebut. Dalam kedua kasus tersebut, *block diagram* memungkinkan pengembang untuk melihat dan memahami interaksi antar komponen dan mengidentifikasi potensi area untuk perbaikan (Mubarak et al., 2023)v.

Block diagram adalah alat yang sangat berguna dalam merancang, menganalisis, dan mengkomunikasikan sistem yang kompleks. Dengan kesederhanaannya, diagram ini memberikan pemahaman yang cepat tentang cara kerja sistem, membuatnya lebih mudah untuk melakukan evaluasi, perencanaan, dan pengembangan lebih lanjut.

2.3.2 Flowchart

Flowchart adalah representasi grafis dari langkah-langkah atau alur proses dalam sebuah sistem, prosedur, atau algoritma. *Flowchart* menggunakan simbol-simbol standar yang terhubung dengan garis untuk menunjukkan urutan dan hubungan antar langkah-langkah dalam suatu proses. Setiap simbol mewakili tindakan atau keputusan tertentu, dan garis yang menghubungkannya menggambarkan aliran data atau kontrol antara langkah-langkah tersebut. *Flowchart* sangat berguna dalam memvisualisasikan proses secara jelas dan terstruktur, yang membantu pengguna atau pengembang untuk

memahami, merencanakan, dan mengoptimalkan prosedur atau algoritma yang kompleks (Zalukhu et al., 2023).

Simbol-simbol yang umum digunakan dalam *flowchart* antara lain adalah oval untuk menunjukkan awal atau akhir suatu proses, persegi panjang untuk tindakan atau proses, belah ketupat untuk menunjukkan keputusan (ya/tidak), dan paralelogram untuk input atau *output* data. Setiap langkah dalam proses diwakili oleh simbol yang sesuai, dan garis yang menghubungkannya menunjukkan urutan eksekusi atau aliran data (Malabay, 2016).

Flowchart sering digunakan dalam berbagai bidang, terutama dalam pemrograman dan pengembangan perangkat lunak, untuk menggambarkan logika algoritma sebelum implementasi kode dilakukan. Ini membantu para pengembang untuk merancang dan menguji alur kerja sistem secara sistematis. Selain itu, *flowchart* juga digunakan dalam analisis proses bisnis, pembuatan manual prosedur, dan dokumentasi teknis untuk menggambarkan langkah-langkah yang harus diikuti dalam berbagai situasi (Zalukhu et al., 2023).

Salah satu keunggulan *flowchart* adalah kemampuannya untuk memecah proses yang kompleks menjadi langkah-langkah yang lebih sederhana dan mudah dipahami. Ini membuatnya menjadi alat komunikasi yang efektif antara pengembang dan pemangku kepentingan lainnya, yang mungkin tidak familiar dengan detail teknis suatu sistem. Dengan *flowchart*, ide atau konsep yang rumit dapat disajikan dengan cara yang mudah dimengerti, mengurangi potensi kesalahan dan meningkatkan efisiensi dalam perencanaan dan pengembangan (Listyoningrum et al., 2023).

Flowchart memungkinkan identifikasi masalah atau hambatan dalam suatu proses dengan lebih cepat, karena memungkinkan pengembang untuk melihat alur proses secara

keseluruhan. Ini juga memungkinkan perubahan atau perbaikan dilakukan dengan lebih mudah, karena setiap langkah dapat dianalisis secara terpisah dan dipahami secara menyeluruh (Listyoningrum et al., 2023).

Flowchart adalah alat yang sangat penting dalam perencanaan, pengembangan, dan dokumentasi sistem, baik dalam konteks pengembangan perangkat lunak, analisis proses bisnis, maupun dalam kegiatan lainnya yang membutuhkan pengorganisasian langkah-langkah atau keputusan dalam urutan tertentu. Dengan kemampuannya untuk memvisualisasikan alur proses secara jelas, *flowchart* membantu mempercepat pemahaman dan penyelesaian masalah dalam berbagai situasi.

2.3 Teori Pengujian

2.4.1 Pengujian Black Box

Black Box testing adalah metode pengujian perangkat lunak di mana penguji tidak memerlukan pengetahuan tentang struktur internal atau implementasi kode sumber aplikasi yang sedang diuji. Fokus utama dalam pengujian ini adalah pada input yang diberikan ke sistem dan *output* yang dihasilkan, untuk memastikan bahwa sistem bekerja sesuai dengan spesifikasi dan kebutuhan yang telah ditentukan. Dalam pendekatan ini, penguji hanya berinteraksi dengan aplikasi dari perspektif pengguna tanpa melihat bagaimana aplikasi memproses data atau bagaimana logika di balik layar bekerja (Kusuma, 2024).

Keuntungan utama dari *Black Box testing* adalah kemampuannya untuk menguji aplikasi dari sudut pandang pengguna akhir. Penguji dapat mengidentifikasi kesalahan atau kekurangan dalam fungsionalitas aplikasi yang mungkin tidak terlihat dalam pengujian yang lebih teknis. Metode ini juga memungkinkan pengujian untuk dilakukan

oleh orang yang tidak terlibat langsung dalam pengembangan aplikasi, sehingga memberikan perspektif yang objektif dan segar (Habibi & Aprilian, 2020).

2.4 Penelitian Yang Relevan

1. Rancangan *Radio Frequency Identification* (Rfid) *Smart Door Lock System* Berbasis *Internet Of Things* Untuk Manajemen Membership *Fitness Center*

Penelitian yang dilakukan (Umam et al., 2023) Hasil penelitian menunjukkan bahwa sistem *smart door lock berbasis Internet of Things* (IoT) telah berhasil dikembangkan untuk memverifikasi status keanggotaan pengunjung secara otomatis menggunakan teknologi *Radio Frequency Identification* (RFID) sebagai kontrol akses. Sistem ini mengadopsi konsep IoT, memungkinkan pengelolaan data anggota secara fleksibel melalui aplikasi yang dapat diakses dari berbagai lokasi, selama Raspberry Pi dan perangkat aplikasi tetap terhubung ke internet. Pengujian terhadap 60 kartu/tag RFID menunjukkan bahwa rata-rata waktu respons sistem dalam memproses data adalah 177,44 milidetik. Berdasarkan hasil tersebut, dapat disimpulkan bahwa sistem RFID *smart door lock* yang dikembangkan beroperasi dengan baik dan memiliki kinerja yang optimal dalam mendukung keamanan akses.

Penelitian (Umam et al., 2023) menggunakan sistem *smart door lock* berbasis IoT dengan RFID sebagai *access control*, yang memiliki risiko manipulasi karena kartu atau tag RFID dapat disalin atau dicuri. Sebaliknya, penelitian yang sedang dijalankan menggunakan *fingerprint sensor*, yang lebih aman karena autentikasi biometrik sulit untuk dimanipulasi. Selain itu, penelitian sebelumnya menggunakan *Raspberry Pi* sebagai pusat pemrosesan, sedangkan penelitian yang sedang dilakukan mengimplementasikan ESP8266, yang lebih ringan, hemat daya, dan tetap

mendukung konektivitas IoT. Dengan demikian, sistem yang dikembangkan dalam penelitian ini lebih unggul dalam keamanan autentikasi dan efisiensi perangkat keras dibandingkan dengan penelitian sebelumnya.

2. Pemanfaatan *Radio Frequency Identification* (RFID) Berbasis *Internet of Things* (IoT) untuk Perancangan Palang Pintu Otomatis di Universitas Nurul Jadid

Penelitian yang dilakukan (Wahyudi et al., 2020) Penelitian ini menghasilkan prototipe palang pintu otomatis berbasis *RFID*, dikendalikan oleh *NodeMCU* dan diprogram menggunakan *Arduino IDE*. Sistem ini beroperasi dengan baik, dengan kemampuan sensor *RFID* dalam membaca ID kartu dan menyimpannya dalam database. Pengujian menunjukkan bahwa *RFID* dapat mendeteksi kartu secara optimal dalam rentang jarak 2–3 cm.

Penelitian (Wahyudi et al., 2020) berbeda dengan sistem yang dikembangkan, di mana sistem yang digunakan dalam penelitian ini menerapkan *fingerprint* sebagai metode autentikasi utama, yang lebih aman dibandingkan *RFID* karena tidak dapat dimanipulasi atau disalin seperti kartu *RFID*. Dengan *fingerprint*, akses hanya diberikan kepada pengguna terdaftar berdasarkan data biometrik yang unik, sehingga meningkatkan keamanan sistem secara signifikan.

3. Prototipe *Smart Door Lock Berbasis Internet Of Things* (Studi Kasus Lab Komputer Politeknik Tedc Bandung)

Penelitian yang dilakukan (Juniawan & Rismayana, 2024) menggunakan metode *User Centered Design* (UCD) untuk mengembangkan sistem *smart door lock* berbasis IoT yang terintegrasi dengan jadwal akses pengguna laboratorium komputer. Sistem ini memungkinkan kontrol akses menggunakan *RFID* dan pengelolaan data melalui aplikasi, meningkatkan efisiensi dan keamanan. Namun, ketergantungan pada

koneksi *internet* yang stabil menjadi tantangan utama. Pengembangan lebih lanjut disarankan dengan integrasi CCTV dan peningkatan stabilitas serta keamanan data.

Penelitian (Juniawan & Rismayana, 2024) menggunakan *RFID* sebagai metode autentikasi, yang memiliki risiko manipulasi, sedangkan penelitian yang sedang dilakukan menerapkan *fingerprint*, yang lebih aman karena berbasis biometrik dan sulit dipalsukan. Selain itu, penelitian sebelumnya menggunakan metode *User Centered Design* (UCD) yang berfokus pada kebutuhan pengguna dalam pengembangan sistem, sedangkan penelitian saat ini menggunakan metode prototipe, yang lebih menekankan pada pengujian dan iterasi sistem sebelum implementasi akhir.

4. Perancangan Sistem Iot Pada *Smart Door Lock* Menggunakan Aplikasi Blynk

Penelitian (Sun et al., 2021) menghasilkan sistem *smart door lock* dalam bentuk miniatur dengan dua sisi, yakni depan dan belakang, masing-masing dengan fungsi spesifik. Sisi depan dilengkapi sensor *infrared* dan kamera ESP8266 untuk menangkap gambar pengunjung, sementara sisi belakang memiliki *push button* sebagai akses darurat. Sistem ini mempermudah pengguna dalam mengakses rumah dan dapat dikontrol melalui Blynk atau aplikasi *smartphone* menggunakan token untuk membuka *Solenoid Door Lock* secara otomatis.

Penelitian sebelumnya menggunakan ESP8266 dengan kamera dan sensor *infrared* untuk mengidentifikasi pengunjung, sementara penelitian yang sedang dilakukan menggunakan ESP8266 sebagai pusat kendali sistem. Selain itu, sistem sebelumnya mengandalkan kontrol akses melalui aplikasi *smartphone* menggunakan token *Blynk*, sedangkan penelitian ini menerapkan *fingerprint* sebagai metode

otentikasi utama, yang lebih aman dibandingkan RFID, karena tidak dapat dimanipulasi atau disalin dengan mudah.

5. Rancang Bangun Kotak Penyimpanan Dengan Akses Masuk Menggunakan Rfid Berbasis *Internet Of Things* (IOT)

Penelitian yang dilakukan (Farid et al., 2022) menghasilkan Sistem kotak penyimpanan berbasis IoT dengan akses *RFID* dirancang untuk meningkatkan keamanan dibandingkan kunci konvensional. Menggunakan *NodeMCU* ESP8266 sebagai pengendali dan modul *RFID* untuk otentikasi, sistem ini memungkinkan akses dengan kartu terdaftar dalam jarak maksimal 4 cm. Jika kartu dikenali, *relay* mengaktifkan *solenoid door lock* selama 3 detik, sementara LCD 16x2 menampilkan status kotak. Alternatifnya, kontrol dapat dilakukan melalui aplikasi *Blynk*, memungkinkan pembukaan dan penutupan kotak secara jarak jauh serta monitoring kondisi penyimpanan secara *real-time*.

Penelitian (Farid et al., 2022) menggunakan sistem akses berbasis *RFID*, yang rentan terhadap manipulasi kartu, sedangkan penelitian yang sedang dilakukan menerapkan *fingerprint* sebagai metode autentikasi, yang lebih aman karena setiap sidik jari bersifat unik dan sulit dipalsukan. Dengan penggunaan *fingerprint*, sistem tidak bergantung pada kartu fisik yang dapat hilang atau disalahgunakan, sehingga meningkatkan keamanan akses secara signifikan.

6. Sistem Keamanan pada Loker Berbasis *Internet of Things*

Penelitian yang dilakukan (Luthfi & Midyanti, 2022) menghasilkan Sistem keamanan loker berbasis IoT ini memungkinkan pembukaan dan penguncian pintu secara digital melalui aplikasi *Android* yang terhubung ke *NodeMCU* ESP8266 melalui *Firebase* dan jaringan *internet*. Pengujian menunjukkan bahwa sistem

berhasil mengontrol *solenoid door lock* menggunakan PIN 4 digit dalam jangkauan 15 meter, dengan rata-rata jeda waktu 23,52 detik untuk notifikasi dan 20,76 detik untuk aktivasi *buzzer*.

Perbedaan utama antara penelitian ini dengan penelitian yang sedang dilakukan terletak pada sistem keamanan yang digunakan. Penelitian ini menerapkan kendali akses berbasis PIN melalui aplikasi *Android* yang terhubung ke *NodeMCU ESP8266*, sementara penelitian yang sedang dijalankan menggunakan *fingerprint*, yang lebih aman karena tidak dapat dimanipulasi seperti *RFID* atau *PIN*. Selain itu, penelitian ini menggunakan *ESP8266*, sedangkan penelitian yang sedang dilakukan menerapkan *ESP8266* sebagai mikrokontroler, yang memiliki spesifikasi lebih ringan dibandingkan *ESP8266*.

7. Perancangan Sistem *Smart Door* Dengan Notifikasi Telegram

Penelitian yang dilakukan (Ma'muriyah et al., 2023) hasil penelitian yaitu Sistem *RFID* bekerja berdasarkan prinsip elektronika, menjadikannya lebih sulit dibuka dibandingkan sistem kunci konvensional yang bersifat universal. Untuk meningkatkan keamanan dan mencegah duplikasi kunci, diperlukan sistem yang lebih sulit diakses serta mampu mengirim notifikasi kepada pemilik saat terjadi upaya akses. Oleh karena itu, dirancang sistem keamanan berbasis *RFID* yang terintegrasi dengan Telegram sebagai notifikasi akses.

Penelitian (Ma'muriyah et al., 2023) mengembangkan sistem keamanan berbasis *RFID* yang terintegrasi dengan *Telegram* untuk notifikasi akses, sementara penelitian yang sedang dilakukan menggunakan sistem *fingerprint*, yang lebih aman karena tidak dapat dimanipulasi seperti *RFID*. *Fingerprint* memastikan identitas pengguna

secara unik tanpa risiko duplikasi atau penyalahgunaan kartu akses, sehingga meningkatkan keamanan sistem secara keseluruhan.

8. *Design and Build Automatic Home Door Security Using IoT-Based PIR and RFID Sensors*

Penelitian yang dilakukan (Maulana, 2024) hasil penelitian, telah berhasil dirancang sistem keamanan pintu rumah berbasis IoT menggunakan *RFID*, yang dikendalikan oleh *NodeMCU ESP8266* dengan sensor *PIR*, *RFID RC522*, *solenoid door lock*, *buzzer*, dan *relay*. Sistem ini dapat diakses melalui *Blynk Touch Sensor* untuk membuka atau menutup pintu dari jarak tertentu. Pengujian oleh tiga ahli media menunjukkan tingkat keberhasilan 96,9%, dengan kemampuan membaca kartu *RFID*, akses melalui aplikasi *Blynk*, serta pengiriman notifikasi ke *Email*. Sistem ini dirancang untuk memudahkan pemilik rumah dalam mengamankan hunian saat ditinggalkan, guna mencegah potensi pencurian.

Perbedaan utama antara penelitian (Maulana, 2024) dengan penelitian yang sedang dilakukan terletak pada sistem autentikasi yang digunakan. Penelitian (Maulana, 2024) mengimplementasikan *RFID* sebagai metode akses utama, yang masih memiliki potensi manipulasi, sedangkan penelitian yang sedang dilakukan menggunakan *fingerprint*, yang lebih aman karena hanya dapat diakses oleh individu terdaftar tanpa risiko duplikasi atau pemalsuan. Hal ini meningkatkan tingkat keamanan sistem dan mengurangi kemungkinan akses tidak sah.

9. *IoT-Based Smart Door Lock System with Fingerprint and Keypad Access*

Penelitian yang dilakukan (Ananta et al., 2024) sistem *Smart Door Lock* berhasil memenuhi ekspektasi akses kunci melalui aplikasi *Android*, *keypad*, sidik jari, dan tombol darurat. Integrasi perangkat keras dan lunak memastikan setiap fitur berfungsi

optimal dengan teknologi IoT, memungkinkan pemantauan dan kontrol jarak jauh melalui *Firebase RTDB*. Pengujian menunjukkan tingkat keberhasilan 100% dalam berbagai skenario, membuktikan keandalannya. Untuk pengembangan lebih lanjut, penelitian dapat difokuskan pada pengujian dalam berbagai kondisi lingkungan, integrasi fitur keamanan tambahan seperti RFID dan pengenalan wajah, serta optimalisasi sistem dalam ekosistem Smart Home dengan cadangan daya UPS untuk menjaga operabilitas saat listrik padam.

Perbedaan utama antara penelitian (Ananta et al., 2024) dan penelitian yang sedang dilakukan terletak pada metode pengembangan sistem dan perangkat keras yang digunakan. Penelitian sebelumnya menerapkan metode *Software Development Life Cycle* (SDLC), sedangkan penelitian yang sedang dilakukan menggunakan metode *prototype*, yang lebih iteratif dan fleksibel dalam menyesuaikan kebutuhan pengguna selama proses pengembangan. Selain itu, penelitian sebelumnya menggunakan ESP8266 sebagai mikrokontroler, sementara penelitian yang sedang dijalankan menggunakan ESP8266, yang memiliki spesifikasi lebih ringan namun tetap mendukung konektivitas IoT secara optimal.

10. *Smart Door Lock Using Face Recognition Access Based on Internet Of Things (IoT)*

Penelitian yang dilakukan (Murjitama et al., 2024) Sistem smart door lock ini menggunakan teknologi pengenalan wajah berbasis *Internet of Things* (IoT). Kunci dilengkapi dengan kamera *ESP8266-CAM* yang terintegrasi dalam modul *ESP8266MOD* untuk mengenali wajah yang telah terdaftar dalam database pada website. Selain itu, terdapat push button untuk membuka pintu dari dalam serta tombol cadangan jika fitur pengenalan wajah mengalami gangguan. Pengujian

perangkat menunjukkan sistem berfungsi dengan baik tanpa kendala signifikan. Uji akurasi kamera mencapai 100% dalam kondisi pencahayaan normal, menurun menjadi 60-80% pada kondisi buram, dan semakin berkurang pada pencahayaan redup, dengan akurasi 40-60% untuk gambar jelas serta 20% untuk gambar buram.

Penelitian (Murjitama et al., 2024) menggunakan sistem *face recognition* sebagai metode autentikasi, sedangkan penelitian yang sedang dilakukan menerapkan *fingerprint* yang dinilai lebih aman dan praktis dalam identifikasi pengguna. Selain itu, metode yang digunakan dalam penelitian sebelumnya adalah *Research & Development* (R&D) yang berfokus pada pengembangan dan evaluasi bertahap, sedangkan penelitian saat ini menggunakan *prototype*, yang memungkinkan pengembangan sistem secara cepat dan iteratif untuk menyesuaikan dengan kebutuhan pengguna.

11. *Design Smart Door Locks With Internet Of Things Based On Pin Security Features*

Penelitian (Wadly, 2023) berhasil merancang dan mengimplementasikan sistem kunci pintu cerdas berbasis IoT yang dikendalikan melalui *Telegram* dengan metode keamanan PIN. Sistem ini menawarkan solusi efisien, aman, dan praktis untuk mengelola akses pintu secara jarak jauh. Hasil penelitian diharapkan berkontribusi pada pengembangan teknologi keamanan pintu cerdas dan penerapan IoT secara lebih luas.

Penelitian (Wadly, 2023) mengembangkan sistem kunci pintu cerdas berbasis IoT yang dikendalikan melalui *Telegram* dengan metode keamanan PIN, namun sistem ini masih berpotensi mengalami manipulasi kode akses. Penelitian yang akan dilakukan mengadopsi teknologi *fingerprint* yang lebih aman untuk autentikasi

pengguna, menghilangkan risiko penyalahgunaan PIN. Selain itu, perangkat keras yang digunakan berbeda, di mana penelitian sebelumnya menggunakan *ESP8266*, sedangkan penelitian yang sedang dijalankan menggunakan *ESP8266* untuk mengoptimalkan efisiensi sistem.

12. *Smart Door Locks Based on Internet of Things Concept with mobile Backend as a Service*

Penelitian (Mahali, 2020) mengembangkan sistem *smart door lock* berbasis IoT dengan mengintegrasikan *ESP8266* sebagai pengendali dan *Firestore Realtime Database* sebagai *backend* untuk menyimpan serta mengelola data. *ESP8266* dapat membaca, mengeksekusi perintah, dan mengirim data ke *Firestore*, sementara aplikasi *Android* digunakan untuk membuka atau mengunci pintu melalui koneksi *internet*. Seluruh perangkat yang terhubung akan tersinkronisasi melalui *Firestore*, memastikan status pintu tetap konsisten, sehingga sistem ini dapat dikategorikan sebagai sistem berbasis *Internet of Things*.

Penelitian (Mahali, 2020) menggunakan sistem keamanan *smart door lock* berbasis IoT dengan autentikasi melalui PIN yang disimpan di *Firestore Realtime Database*. Namun, sistem ini berpotensi mengalami manipulasi atau peretasan terhadap PIN. Sebagai perbedaan, penelitian yang sedang dilakukan menggunakan autentikasi berbasis fingerprint, yang lebih aman karena setiap sidik jari bersifat unik dan sulit untuk dimanipulasi, sehingga meningkatkan tingkat keamanan akses dibandingkan dengan metode PIN.

13. *Smart Laboratory Using Radio Frequency Identification (RFID) Based on The Internet of Things*

Penelitian yang dilakukan (Nursuwars et al., 2022) Hasil penelitian menunjukkan bahwa pendaftaran kartu E-KTP hanya dapat diproses jika nomor loker dan meja masih tersedia. Akses ke loker dan meja hanya dapat dilakukan dengan kartu yang telah terdaftar sebelumnya, sementara kartu yang belum terdaftar tidak dapat digunakan. Pengguna baru tidak dapat mendaftarkan kartu E-KTP pada loker dan meja yang sudah terisi tanpa terlebih dahulu melakukan pembatalan pendaftaran. Untuk penyempurnaan sistem, diperlukan fitur tambahan seperti peminjaman, pemantauan suhu dan kelembaban ruangan, serta memori eksternal untuk penyimpanan data.

Penelitian (Nursuwars et al., 2022) menggunakan E-KTP sebagai kunci akses, yang berisiko hilang atau dicuri serta rentan terhadap kendala akses jika kartu tidak tersedia. Selain itu, penggunaan PIN juga memiliki potensi peretasan. Sebagai perbedaan, penelitian yang sedang dilakukan menerapkan sistem berbasis *fingerprint*, yang lebih aman karena hanya dapat diakses oleh individu yang terdaftar, menghilangkan risiko kehilangan kartu atau penyalahgunaan PIN.

14. *Design and Build a Safe Security System Using RFID With e-KTP as a Tag and Monitoring With IoT-Based Esp8266-Cam With Telegram Notifications*

Penelitian yang dilakukan (Ashar, 2021) menghasilkan brankas modern kini dilengkapi komponen elektronik tanpa kunci konvensional, menggunakan *RFID* dengan E-KTP dan *password* untuk akses. Sistem ini dilengkapi sensor *PIR* dan kamera *ESP8266* untuk memantau siapa yang mengakses brankas, serta dapat diawasi melalui *smartphone* dengan aplikasi *Telegram*, yang juga berfungsi mengendalikan alarm jika terdeteksi aktivitas mencurigakan.

Penelitian (Ashar, 2021) mengembangkan sistem keamanan brankas berbasis *RFID* yang terintegrasi dengan E-KTP dan *password*, menggunakan ESP8266 serta sensor PIR dan kamera untuk pemantauan melalui *Telegram*. Sementara itu, penelitian yang sedang dilakukan berfokus pada pengembangan *smart door lock* yang lebih aman dengan teknologi *fingerprint*, menghilangkan potensi manipulasi *RFID*. Selain itu, sistem yang dikembangkan menggunakan ESP8266 sebagai mikrokontroler utama, yang lebih sesuai dengan kebutuhan implementasi *smart door lock* berbasis IoT.

15. Rancang Bangun Sistem Keamanan Door Lock Menggunakan E-KTP Berbasis Arduino Wemos

Penelitian yang dilakukan (Azzizi, 2022) Hasil penelitian menunjukkan bahwa sistem kunci pintu berbasis E-KTP dapat dibangun dan dikendalikan menggunakan mikrokontroler Arduino Wemos ESP8266 sebagai pusat kontrol, dengan perangkat lunak Arduino IDE 1.8.20. Pembaca *RFID* 13,56MHz berfungsi optimal dalam membaca kartu ID elektronik pada jarak 3/4 inci, memungkinkan integrasi yang baik dengan relai sensor dan tombol kunci pintu.

Penelitian yang sedang dilakukan menggunakan sistem keamanan berbasis *fingerprint*, yang lebih aman dibandingkan dengan sistem berbasis *RFID* karena mengeliminasi risiko manipulasi atau penyalahgunaan kartu akses. Berbeda dengan penelitian (Azzizi, 2022) yang menggunakan *RFID* sebagai metode autentikasi, sistem *fingerprint* memastikan bahwa hanya individu yang terdaftar yang dapat mengakses, sehingga meningkatkan tingkat keamanan dan mengurangi potensi peretasan atau duplikasi akses.

Tabel 2. 1 Penelitian Relevan

Peneliti	Metode	Sistem	Kelebihan	Kekurangan
Umam et al. (2023)	RFID, IoT	<i>smart door lock</i>	Memungkinkan pengelolaan keanggotaan secara fleksibel, memiliki waktu respons cepat (177,44 ms)	Risiko manipulasi karena kartu/tag RFID dapat disalin atau dicuri
Wahyudi et al. (2020)	RFID, IoT	Palang pintu otomatis berbasis RFID	RFID dapat mendeteksi kartu secara optimal dalam jarak 2–3 cm, terhubung dengan <i>database</i>	Keamanan lebih rendah dibandingkan fingerprint karena kartu RFID bisa disalin
Juniawan & Rismayana (2024)	RFID, IoT, UCD	<i>Smart door lock</i>	Integrasi dengan jadwal akses pengguna laboratorium, meningkatkan efisiensi dan keamanan	Bergantung pada koneksi internet yang stabil
Sun et al. (2021)	Kamera ESP8266, Sensor Infrared, IoT	<i>Smart door lock</i>	Dapat dikontrol melalui aplikasi smartphone, memiliki akses darurat	Keamanan autentikasi lebih rendah dibandingkan fingerprint

Farid et al. (2022)	RFID, IoT	<i>Smart door lock</i>	Memungkinkan akses dengan kartu terdaftar dalam jarak 4 cm, kontrol melalui aplikasi Blynk	Rentan terhadap manipulasi kartu RFID yang dapat hilang atau dicuri
Luthfi & Midyanti (2022)	PIN, IoT	<i>Smart door lock</i>	Dapat dikontrol dari jarak jauh melalui Firebase, mendukung notifikasi dan <i>buzzer</i>	Keamanan berbasis PIN lebih rentan dibandingkan fingerprint karena dapat ditebak atau dibagikan
Ma'muriyah et al. (2023)	RFID, IoT, Telegram	<i>Smart door lock</i>	Mengirimkan notifikasi akses secara <i>real-time</i> , meningkatkan keamanan dibandingkan kunci konvensional	Rentan terhadap penyalahgunaan kartu RFID
Maulana (2024)	RFID, PIR Sensor, IoT	<i>Smart Home</i>	Tingkat keberhasilan 96,9%, mendukung akses melalui aplikasi <i>Blynk</i> dan notifikasi <i>email</i>	RFID masih memiliki potensi manipulasi dan duplikasi kartu

Ananta et al. (2024)	Keypad, IoT	<i>Smart door lock</i>	Tingkat keberhasilan 100% dalam pengujian, mendukung pemantauan dan kontrol jarak jauh	Rentan terhadap manipulasi kode akses (PIN).
(Murjitama et al., 2024)	Pengenalan wajah berbasis IoT, IoT	<i>Smart door lock</i>	Akurasi tinggi (100%) dalam kondisi pencahayaan normal.	Akurasi menurun signifikan pada pencahayaan redup.
Wadly, 2023)	Pin, IoT	<i>smart door lock</i>	Akses pintu dapat dikontrol jarak jauh dengan praktis.	Rentan terhadap manipulasi kode akses (PIN).
(Mahali, 2020)	PIN, IoT	<i>smart door lock</i>	berbasis IoT memungkinkan kontrol pintu jarak jauh melalui aplikasi Android dengan sinkronisasi data <i>real-time</i> di <i>Firebase</i> .	Autentikasi menggunakan PIN berisiko mengalami peretasan atau manipulasi data.
(Nursuwars et al., 2022)	RFID, E-KTP & PIN IoT	<i>Smart door lock</i>	Keunggulannya adalah sistem yang memastikan keamanan, validitas pendaftaran, dan	Kelemahannya adalah risiko kehilangan atau pencurian E-KTP, kendala akses jika kartu tidak

			kontrol akses kartu E-KTP.	tersedia, serta potensi peretasan PIN.
(Ashar, 2021)	RFID, E-KTP & PIN IoT	<i>Smart Door Lock</i>	dapat diawasi melalui <i>smartphone</i> dengan aplikasi <i>Telegram</i>	Rentan terhadap pencurian atau duplikasi kartu RFID, peretasan PIN
(Azzizi, 2022)	E-KTP, IoT	<i>Smart Door Lock</i>	memungkinkan integrasi yang baik dengan relai sensor dan tombol kunci pintu	Rentan terhadap pencurian atau duplikasi kartu RFID

BAB III

METODOLOGI PENELITIAN

3.1 Analisa Kebutuhan

Dalam proyek ini, peneliti mengidentifikasi beberapa kekurangan atau permasalahan pada sistem yang sedang berjalan. Berdasarkan berbagai pertimbangan, akan dirumuskan kebijakan sistem sebagai berikut:

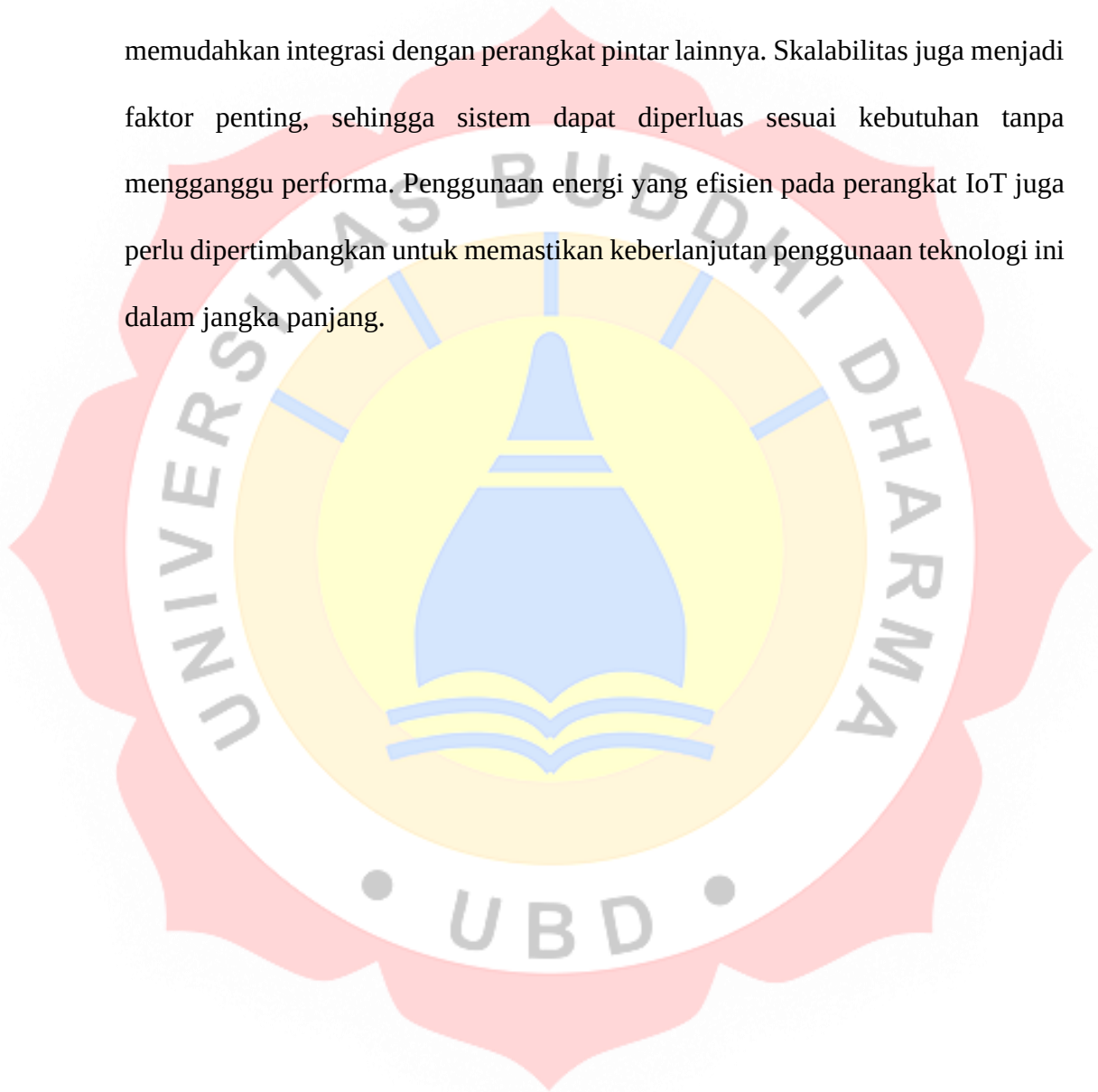
1. Kebutuhan Fungsional

Sistem keamanan smart home berbasis IoT dengan integrasi sidik jari dirancang untuk memenuhi berbagai kebutuhan pengguna. Sistem harus menyediakan akses masuk rumah menggunakan sidik jari dengan proses autentikasi yang cepat dan akurat. Selain itu, pencatatan aktivitas keluar-masuk penghuni, termasuk identitas pengguna dan waktu akses, menjadi fitur utama untuk memastikan pemantauan yang efektif. Sistem juga harus memiliki kemampuan mengirimkan notifikasi real-time ke perangkat *mobile* ketika terjadi aktivitas mencurigakan atau akses tidak sah. Fitur lain yang diperlukan adalah integrasi dengan otomasi elektronik lainnya, untuk menciptakan keamanan yang lebih komprehensif. Terakhir, sistem harus mampu mengontrol dan mengotomatisasi perangkat elektronik rumah, seperti lampu dan perangkat pendingin ruangan, untuk meningkatkan kenyamanan pengguna.

2. Kebutuhan Non-Fungsional

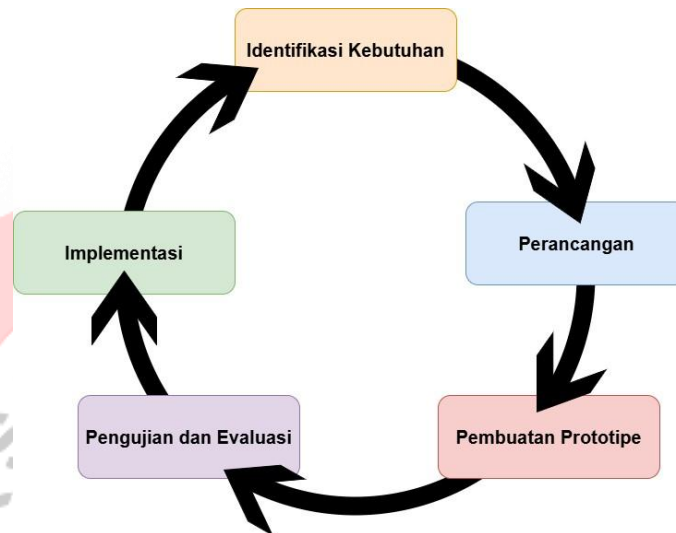
Untuk memastikan performa yang optimal, sistem harus memiliki tingkat keamanan tinggi dengan enkripsi data sidik jari dan aktivitas pengguna, sehingga mencegah potensi penyalahgunaan data. Sistem harus responsif, dengan waktu

autentikasi sidik jari tidak lebih dari 2 detik, serta dapat beroperasi dengan koneksi internet yang stabil. Aplikasi pendukung sistem harus memiliki antarmuka yang *user-friendly* agar mudah digunakan oleh pengguna dari berbagai latar belakang. Selain itu, sistem harus kompatibel dengan protokol IoT standar untuk memudahkan integrasi dengan perangkat pintar lainnya. Skalabilitas juga menjadi faktor penting, sehingga sistem dapat diperluas sesuai kebutuhan tanpa mengganggu performa. Penggunaan energi yang efisien pada perangkat IoT juga perlu dipertimbangkan untuk memastikan keberlanjutan penggunaan teknologi ini dalam jangka panjang.



3.2 Metode *Prototype*

Metode *Prototype* digunakan untuk mengembangkan sistem secara iteratif dan bertahap dengan melibatkan pengguna dalam proses perancangan.



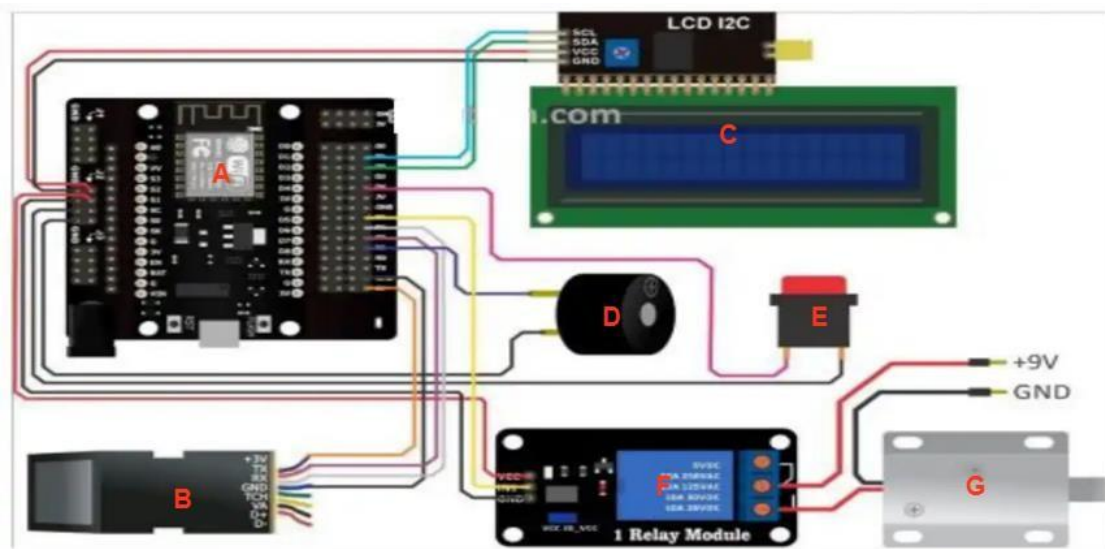
Gambar 3. 1 Tahapan *Prototype*

Berikut adalah tahapan yang diterapkan:

1. Pada tahap ini, dilakukan identifikasi kebutuhan sistem berdasarkan studi literatur, di mana beberapa kebutuhan yang dikumpulkan meliputi kemampuan sistem untuk mengenali sidik jari sebagai autentikasi pengguna serta mengontrol perangkat elektronik rumah tangga berbasis IoT.
2. Setelah kebutuhan dikumpulkan, dibuat rancangan awal sistem yang mencakup rancangan perangkat keras dengan pemilihan sensor sidik jari, mikrokontroler seperti ESP8266, serta aktuator untuk mengontrol perangkat elektronik, serta rancangan perangkat lunak yang meliputi desain tampilan antarmuka, alur sistem, dan integrasi *backend* dengan sistem IoT dan *database*, sementara diagram alir (*flowchart*) digunakan untuk membantu

memahami proses kerja sistem sebelum implementasi. (gambar dan penjelasan).

Berikut adalah rancangan *prototype* yang dibuat oleh peneliti untuk membuat sistem yang disusun.



Gambar 3. 2 Rancangan *Prototype*

Komponen yang Digunakan:

- a. ESP8266/ (Mikrokontroler IoT)

Berfungsi sebagai otak sistem untuk mengontrol semua perangkat dan menghubungkan ke jaringan *internet*. Bertanggung jawab dalam memproses data dari sensor sidik jari, menampilkan informasi ke LCD, dan mengaktifkan *relay*.

- b. Sensor Sidik Jari

Digunakan untuk mengenali dan memverifikasi sidik jari pengguna yang sudah terdaftar. Jika sidik jari cocok dengan *database* yang tersimpan, sistem akan membuka pintu melalui relay.

c. *LCD I2C (16x2 LCD dengan Modul I2C)*

Digunakan untuk menampilkan informasi status sistem, seperti "Akses Diterima" atau "Sidik Jari Tidak Dikenal". Modul I2C digunakan untuk mengurangi jumlah kabel yang diperlukan untuk komunikasi dengan mikrokontroler.

d. *Buzzerr*

Memberikan notifikasi suara ketika ada akses yang gagal atau terdeteksi percobaan masuk yang tidak sah.

e. *Push Button*

Berfungsi sebagai tombol manual untuk mengontrol sistem, misalnya untuk reset atau mode pendaftaran sidik jari.

f. *Relay Module (1-Channel Relay)*

Digunakan untuk mengontrol kunci elektronik atau *solenoid door lock*.

g. *Solenoid Door Lock*

Kunci elektronik yang dikendalikan oleh *relay* untuk membuka atau mengunci pintu.

3. Prototipe awal diuji untuk memastikan fungsionalitas dasar sudah sesuai, seperti kemampuan sensor sidik jari dalam mengenali pengguna yang terdaftar, pengendalian perangkat elektronik melalui antarmuka sistem, serta kelancaran komunikasi antara perangkat IoT.

4. Setelah evaluasi awal, sistem diperbaiki dengan mengoptimalkan sensor, memperbaiki algoritma pemrosesan sidik jari, dan meningkatkan responsivitas agar lebih cepat dan akurat. Komunikasi antara perangkat dan *server cloud* diperkuat untuk memastikan akses jarak jauh yang lebih stabil dan efisien. Untuk mengintegrasikan sistem dengan perangkat *mobile*, aplikasi dapat dikembangkan menggunakan C agar mendukung berbagai *platform*.

Berikut adalah *source code* yang dibuat oleh peneliti:

```
Serial.println("Remove finger");
delay(2000);
p = 0;
while (p != FINGERPRINT_NOFINGER) {
  p = finger.getImage();
}
Serial.print("ID "); Serial.println(id);
p = -1;
Serial.println("Place same finger again");
while (p != FINGERPRINT_OK) {
  p = finger.getImage();
  switch (p) {
    case FINGERPRINT_OK:
      Serial.println("Image taken");
      break;
    case FINGERPRINT_NOFINGER:
      Serial.print(".");
      break;
    case FINGERPRINT_PACKETRECEIVEERR:
      Serial.println("Communication error");
      break;
    case FINGERPRINT_IMAGEFAIL:
      Serial.println("Imaging error");
      break;
    default:
      Serial.println("Unknown error");
      break;
  }
}
```

Gambar 3. 3 Source Code Simpan Sidik Jari

Gambar 3.3 adalah *source code* untuk pengkodean penyimpanan sidik jari menggunakan modul sensor sidik jari.

```

SoftwareSerial mySerial(D6, D7);
Adafruit_Fingerprint finger = Adafruit_Fingerprint(&mySerial);
LiquidCrystal_I2C lcd(0x27, 16, 2);
//=====
void setup(){
  Serial.begin(115200);
  lcd.begin(16, 2);
  lcd.init();
  lcd.backlight();
  lcd.clear();
  lcd.print("    Baca ID    ");
  lcd.setCursor(0,1);
  lcd.print("    Sidik Jari  ");
  delay(2000);
  finger.begin(57600);
  lcd.clear();
  lcd.print("Test Koneksi");
  lcd.setCursor(0, 1);
  if (finger.verifyPassword()) {
    lcd.print("OK !");
  } else {
    lcd.print("ERROR !");
    while (1){ delay(1); }
  }
  finger.getTemplateCount();
  delay(2000);
}

```

Gambar 3. 4 Source Code Baca Sidik Jari

Gambar 3.4 adalah *source code* untuk pengkodean pembacaan sidik jari menggunakan sensor sidik jari.

```

#define BLYNK_TEMPLATE_ID "TMPL6AV7BddU4"
#define BLYNK_TEMPLATE_NAME "IoT Smart Doorlock"
#define BLYNK_AUTH_TOKEN "R20VmUir3hmygR4jDQlJKLwy5c5lQp6s"

#define BLYNK_PRINT Serial

#include <ESP8266WiFi.h>
#include <WiFiClient.h>
#include <BlynkSimpleEsp8266.h>
char auth[] = BLYNK_AUTH_TOKEN;;
//---GANTI SESUAI DENGAN JARINGAN WIFI
//---HOTSPOT ANDA
char ssid[] = "PUTRA19";
char pass[] = "123456789";

#include <Wire.h>
#include <LiquidCrystal_I2C.h>
#include <Adafruit_Fingerprint.h>

#define buzzer D8
#define SW D4
#define selenoid D5

SoftwareSerial mySerial(D6, D7);
Adafruit_Fingerprint finger = Adafruit_Fingerprint(&mySerial);
LiquidCrystal_I2C lcd(0x27, 16, 2);

byte ID1 = 1;
byte ID2 = 2;
byte ID3 = 3;
bool Switch = false;
int j;

```

Gambar 3. 5 Source Code Koneksi Server Cloud Bylnk

Gambar 3.5 adalah *source code* untuk pengkodean koneksi Server Cloud ByLnk. Kode ini dirancang untuk menghubungkan perangkat dengan platform ByLnk menggunakan API yang sesuai.


```

#define BLYNK_TEMPLATE_ID "TMPL6XXtCQCFZ"
#define BLYNK_TEMPLATE_NAME "Relay 8 Ch"
#define BLYNK_AUTH_TOKEN "WLibPjJCo7tn3NTbwI3dwKJXSUtbaPzA"
#define BLYNK_PRINT Serial
#include <ESP8266WiFi.h>
#include <WiFiClient.h>
#include <BlynkSimpleEsp8266.h>
char auth[] = BLYNK_AUTH_TOKEN;
// Sesuaikan dengan ssid dan password hotspot anda
char ssid[] = "PUTRA19";
char pass[] = "123456789";

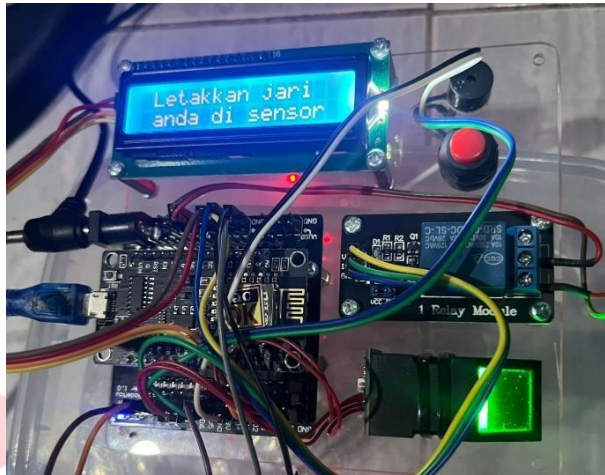
//=====
BLYNK_WRITE(V0)
{
  int value1 = param.asInt();
  digitalWrite(D1,value1);
}

```

Gambar 3. 6 *Source Code* Koneksi Lampu

Gambar 3.6 adalah *source code* untuk pengkodean pengendalian lampu. Kode ini dirancang untuk mengontrol lampu menggunakan mikrokontroler

5. Tahap akhir dilakukan pengujian sistem secara menyeluruh melalui metode *Black Box Testing* untuk memastikan kinerja dan keandalan sistem. Pengujian mencakup akurasi serta kecepatan sistem dalam mengenali sidik jari, keandalan akses menggunakan RFID dan PIN, serta respons sistem dalam mengontrol perangkat elektronik secara *real-time*. Selain itu, diuji kestabilan komunikasi IoT guna memastikan perangkat dapat berinteraksi dengan *server* tanpa gangguan, serta aspek keamanan sistem untuk mencegah akses tidak sah dan memastikan perlindungan data pengguna.



Gambar 3. 7 Prototype Awal

Pada gambar 3.6 terlihat prototipe awal sudah dapat diaktifkan maka tahapan selanjutnya adalah melakukan pengujian sistem dimana pengujian tersebut menggunakan *back box testing*.

3.3 Rencana Pengujian *Black Box Testing*

Metode *Black box Testing* digunakan dalam penelitian ini karena berfokus pada pengujian fungsionalitas sistem berdasarkan *input* dan *output* tanpa perlu memahami kode sumber, sehingga memastikan setiap fitur bekerja sesuai spesifikasi. Pendekatan ini efektif untuk menguji sistem berbasis pengguna, seperti autentikasi *fingerprinth* atau akses IoT, guna memastikan pengalaman pengguna yang optimal. Selain itu, metode ini memungkinkan identifikasi kesalahan dalam proses autentikasi atau komunikasi antar komponen tanpa mengganggu struktur kode. Dengan kemampuannya menguji integrasi perangkat keras dan perangkat lunak secara efisien, *Black box Testing* juga menghemat waktu serta sumber daya, sehingga menjadi pilihan yang tepat untuk memastikan sistem berjalan dengan baik sesuai kebutuhan pengguna.

Berikut adalah 3 rencana dalam pengujian *black box testing* yang akan diterapkan:

Tabel 3. 1 Rencana Pengujian *Black Box*

No	Pengujian	Tahapan
1	Pengujian Fitur sidik jari	Menguji apakah sistem dapat mengenali dan menyimpan sidik jari pengguna.
		Menguji apakah sistem dapat membuka pintu secara manual melalui tombol fisik.
2	Keandalan Autentikasi Finger	Menguji autentikasi dengan sidik jari terdaftar.
		Menguji autentikasi dengan sidik jari tidak terdaftar.
		Mengukur kecepatan autentikasi <i>fingerprint</i> .
3	Pengujian Pengendalian Jarak Jauh	Menguji apakah lampu bisa di nyalakan melalui aplikasi dari jarak jauh.
		Mengukur kecepatan pengendalian jarak jauh.

3.4 Spesifikasi Kebutuhan Sistem

3.2.1 Hardware

Pada pembuatan proyek tugas akhir ini, penyusun menggunakan beberapa *hardware* penunjang untuk mendukung proses pengembangan dan implementasi sistem. *Hardware* yang digunakan meliputi:

1. *Controller NodeMCU V3 / ESP8266*
2. *Board Controller NodeMCU Board*
3. *Sensor Fingerprint AS608*
4. *Display LCD 16x2*
5. *Sistem Door Lock Solenoid*
6. *Relat Module 1 Channel*
7. *Buzzer*
8. *Tombol Push-ON*

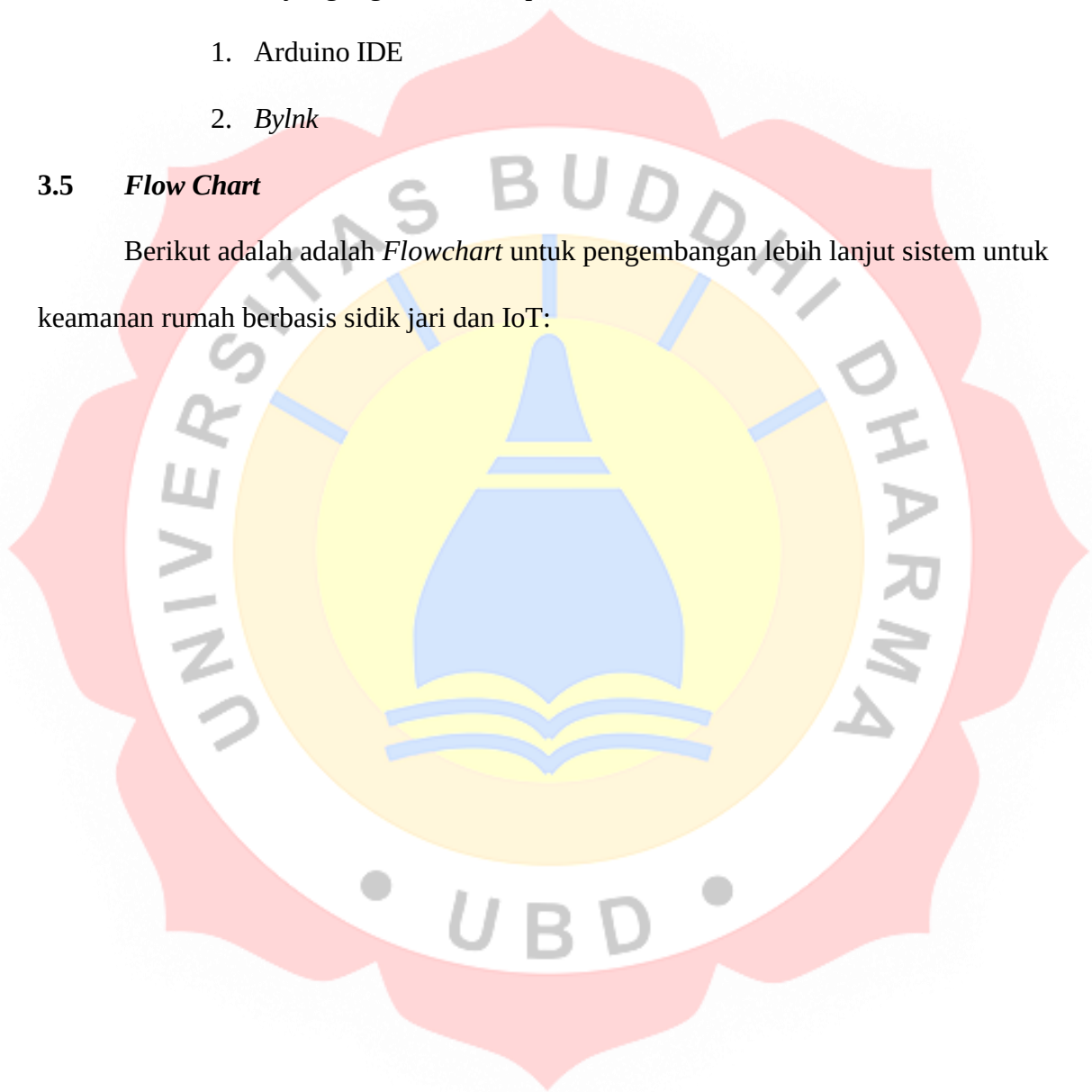
3.2.2 *Software*

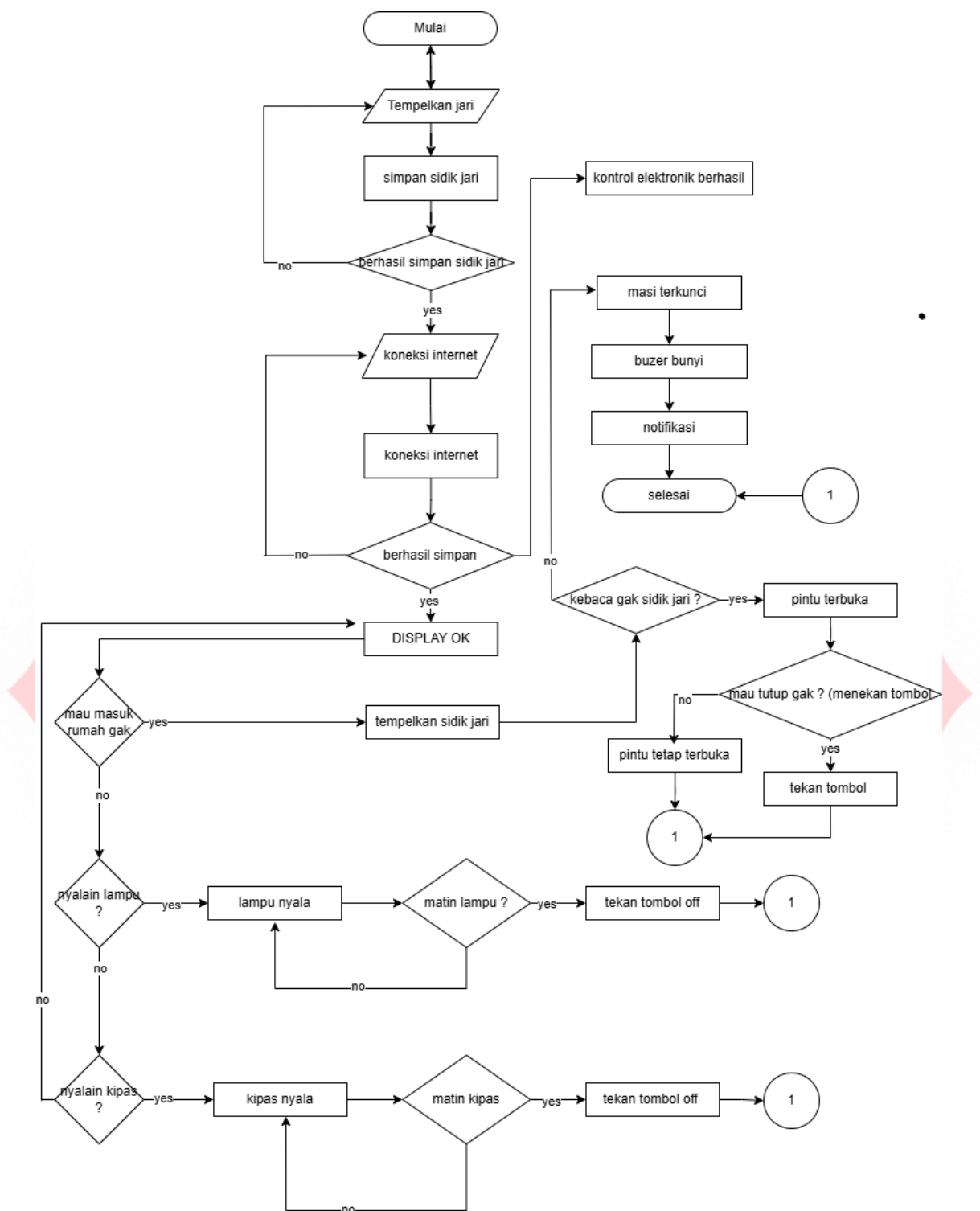
Pada pembuatan proyek tugas akhir ini, penyusun menggunakan beberapa software penunjang untuk mendukung proses pengembangan dan implementasi sistem. software yang digunakan meliputi:

1. Arduino IDE
2. *Bylnk*

3.5 *Flow Chart*

Berikut adalah *Flowchart* untuk pengembangan lebih lanjut sistem untuk keamanan rumah berbasis sidik jari dan IoT:





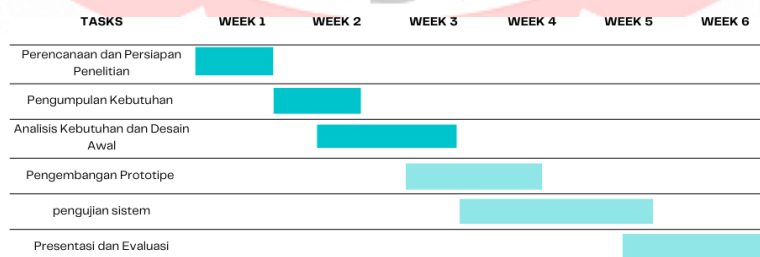
Gambar 3. 8 Folw Chart Alur Proses Sistem

Penjelasan:

1. Instalasi *hardware* dan instalasi *software* sampai ketahap siap digunakan atau diterapkan.
2. *Display* LCD Menampilkan “SMART Door Lock Fingerprint”.
3. Melakukan koneksi ke sensor, jika berhasil terhubung maka menampilkan *Display* “ok” jika tidak maka kembali ke koneksi.
4. Lanjutan dari *display* “ok” lalu melakukan set parameter sensor dan cek data sidik jari. selanjutnya otomatis mengkoneksikan koneksi dengan internet dan koneksi ke *bylnk console server*.
5. Memberikan secara otomatis ID sidik jari yang didaftarkan.
6. Pengujian dengan melakukan masuk dengan sidik jari yang sudah didaftarkan lalu *fingerprint* otomatis mengecek data ID sidik jari apakah terdaftar atau tidak.
7. Jika sidik jari terdaftar maka *solenoid door lock* akan terbuka dan elektronik akan menyala. Namun jika tidak terdaftar maka menampilkan warning user tidak terdaftar.

3.6 Jadwal Penelitian

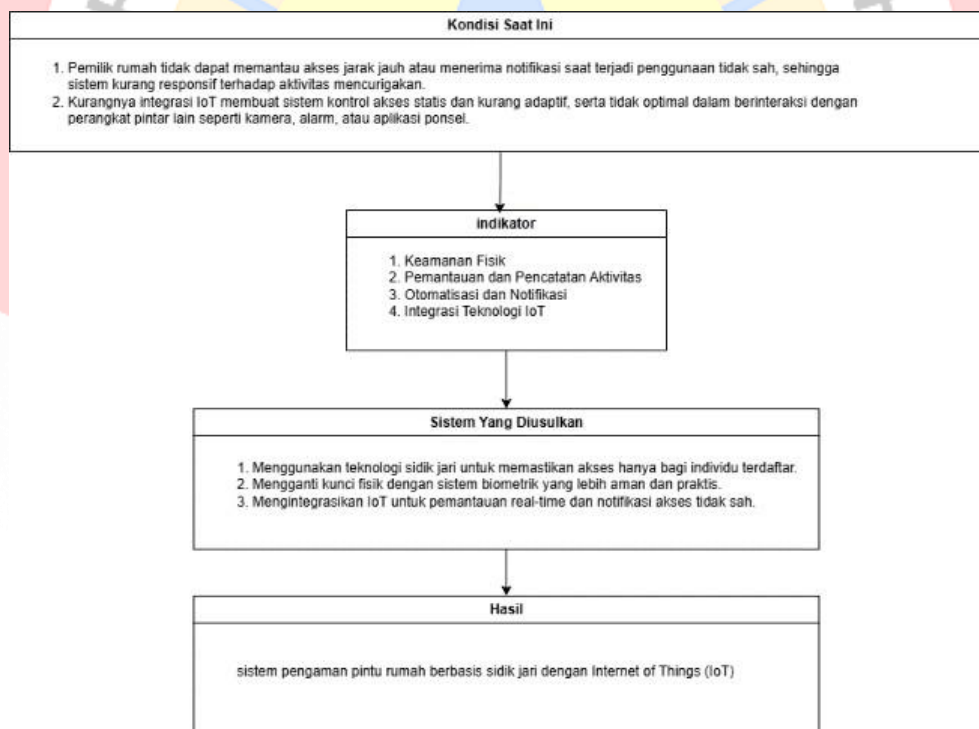
Berikut adalah pengembangan lebih lanjut dari jadwal penelitian untuk sistem keamanan rumah berbasis sidik jari dan IoT:



Gambar 3. 9 Jadwal Penelitian

Jadwal penelitian ini terdiri dari enam minggu dengan tahapan yang terstruktur untuk memastikan kelancaran proses penelitian. Minggu pertama difokuskan pada perencanaan dan persiapan penelitian, diikuti oleh pengumpulan kebutuhan pada minggu kedua. Selanjutnya, analisis kebutuhan dan desain awal dilakukan pada minggu ketiga. Pengembangan prototipe berlangsung dari minggu keempat hingga kelima, yang kemudian diikuti oleh tahap pengujian sistem yang dimulai pada minggu kelima dan berlanjut ke minggu keenam. Akhirnya, penelitian diakhiri dengan presentasi dan evaluasi yang dilakukan pada minggu keenam sebagai tahap final untuk menilai hasil yang telah dicapai.

3.7 Kerangka Pemikiran



Gambar 3. 10 Kerangka Pemikiran

Kerangka penelitian ini menggambarkan permasalahan pada sistem keamanan rumah konvensional yang masih bergantung pada kunci fisik, tidak memiliki pemantauan real-time, serta kurangnya integrasi teknologi IoT. Untuk mengatasi masalah tersebut, penelitian ini mengusulkan sistem keamanan berbasis sidik jari yang lebih aman dan praktis, serta mengintegrasikan IoT untuk pemantauan dan notifikasi *real-time*. Indikator yang digunakan meliputi keamanan fisik, pencatatan aktivitas, otomatisasi, serta integrasi teknologi IoT. Implementasi sistem ini diharapkan menghasilkan sistem pengamanan pintu rumah yang lebih modern dan efektif, dengan tingkat keamanan yang lebih tinggi serta kemampuan pemantauan jarak jauh.

