








UNIVERSITAS DIPONEGORO – FAKULTAS TEKNIK
DEPARTEMEN TEKNIK ELEKTRO

Jl. Prof. H. Soedarto, SH, Tembalang, Semarang 50275

Telp/Faks. (024)-7460057 e-mail: departemen@elektro.undip.ac.id

Dokumen Pengembangan Produk
Lembar Sampul Dokumen

Judul Dokumen	TUGAS AKHIR: Rancang Bangun Sistem Keamanan Kunci Pintu Gedung Berbasis <i>Internet of Things</i>
Jenis Dokumen	PROPOSAL Catatan: Dokumen ini dikendalikan penyebarannya oleh Dept. Teknik Elektro Undip
Nomor Dokumen	B100-03-TA2223.2.19012
Nomor Revisi	03
Nama File	B100-2-TA2223
Tanggal Penerbitan	30 Januari 2023
Unit Penerbit	Departemen Teknik Elektro Undip
Jumlah Halaman	77 (termasuk lembar sampul ini)

Data Pengusul				
Pengusul	Nama	Henric Dhiki Wicaksono	Jabatan	Anggota
	NIM	21060119120011	Tanda Tangan	
	Nama	Novi Dianasari	Jabatan	Anggota
	NIM	21060119120039	Tanda Tangan	
	Nama	Muhammad Khoiril Wafi	Jabatan	Anggota
	NIM	21060119140133	Tanda Tangan	
Pembimbing Utama	Nama NIP	M. Arfan, S.Kom., M.Eng. 198408172015041002	Tanda Tangan	
Pendamping	Nama NIP	Imam Santoso, S.T., M.T. 197012031997021001	Tanda Tangan	

DAFTAR ISI

1	PENDAHULUAN	4
1.1	RINGKASAN ISI DOKUMEN	4
1.2	APLIKASI DOKUMEN	5
1.3	REFERENSI.....	5
1.4	DAFTAR SINGKATAN	7
2	PROPOSAL PENGEMBANGAN PRODUK	9
2.1	PENDAHULUAN	9
2.1.1	Latar Belakang Masalah	9
2.1.2	Rumusan Masalah	10
2.1.3	Tujuan	11
2.1.4	Alternatif Desain.....	11
2.2	KONSEP DESAIN	27
2.2.1	Konfigurasi Umum	27
2.2.2	Kemampuan dan Kapasitas Produk	46
2.2.3	Dasar Teori yang Mendukung Proses Pengembangan	49
2.2.4	Teknologi yang Digunakan	60
2.2.5	Batasan – Batasan Sistem.....	61
2.2.6	Standarisasi Produk.....	62
2.2.7	Etika Profesi yang Dijunjung.....	63
2.3	SKENARIO PEMANFAATAN PRODUK	64
2.4	NILAI STRATEGIS	68
2.5	USAHA PENGEMBANGAN.....	69
2.5.1	<i>Man-Month</i>	69
2.5.2	<i>Machine-Month</i>	69
2.5.3	<i>Development Tools</i>	69
2.5.4	<i>Test Equipment</i>	70
2.5.5	Kebutuhan <i>Expert</i>	70
2.5.6	Perkiraan Biaya	71
2.5.7	Peluang Keberhasilan	71
2.5.8	Jadwal dan Waktu Pengembangan	72
3	KESIMPULAN.....	73
4	BIODATA TIM PENGUSUL	74

Catatan Sejarah Perbaikan Dokumen

VERSI, TGL, OLEH	PERBAIKAN
01, 21 November 2022, oleh Henric Dhiki Wicaksono, Novi Dianasari, dan Muhammad Khoiril Wafi.	<ul style="list-style-type: none"> • Penulisan • Perbandingan alternatif • <i>Constraint</i> kurang • Bisa dicarikan literatur dari Undip atau paper jurnal • Untuk referensi ditulis sesuai format IEEE • Apakah tidak menggunakan protokol yang khusus untuk IoT? • Apakah tidak dimungkinkan dengan 4G sebagai komplemen bila koneksi Wi-Fi sedang <i>off</i>? • Bagaimana <i>hosting server</i>-nya? Di-<i>cloud</i>? • Bagaimana pengenalan wajah oleh kamera di android? Adakah keamanan lainnya sebagai komplemen pengaman pendeteksi wajah? • Data apa saja yang disimpan dalam <i>database server</i>? • Mengapa pakai MySQL? • Mengapa pakai FCM?
02, 21 Desember 2022, oleh Henric Dhiki Wicaksono, Novi Dianasari, dan Muhammad Khoiril Wafi.	<ul style="list-style-type: none"> • Kompleksitas masalahnya kurang • Penulisan referensi tidak sesuai pedoman • Rujukan dalam tulisan malah tidak ada pada referensi • Tidak ada rumus matematika • 1. Sudah banyak TA di luar yang membahas ini dan semua memiliki kesamaan topik yaitu: menggunakan ESP8266, <i>firebase</i>, arduino, mysql, android. Rata-rata dikerjakan hanya satu orang saja cukup. • 2. Kenapa tidak pakai <i>micro</i> ESP32 yang sudah <i>all in one</i> atau <i>raspberry</i> yang lebih <i>advanced</i>? • 3. Tunjukkan kelebihan sistem anda dan kalau mungkin pakai alternatif lain selain ESP8266 (karena semua topik di no 1 selalu pakai arduino dan ESP8266) sebagai pembeda utama. Syukur kalau bisa <i>support</i> IOS.
03, 13 Januari 2023, oleh Henric Dhiki Wicaksono, Novi Dianasari, dan Muhammad Khoiril Wafi.	<ul style="list-style-type: none"> • Penulisan referensi tidak sesuai format. • 1. Pembahasan <i>Basic Science and math</i> minim. • 2. Belum terlihat <i>standard engineering</i> yang dirujuk. • 3. Kerja sama tim dan pembagian kerja tidak terlihat. Pada proposal pertama sudah ada diagram pembagian tugas (Gambar 2.1), yang sekarang malah tidak ada.

PROPOSAL

Rancang Bangun Sistem Keamanan Kunci Pintu Gedung Berbasis *Internet of Things*

1 PENDAHULUAN

1.1 RINGKASAN ISI DOKUMEN

Dokumen ini berisikan uraian proposal proyek pengembangan Rancang Bangun Sistem Keamanan Kunci Pintu Gedung Berbasis *Internet of Things*. Dokumen rancang bangun sistem keamanan kunci pintu gedung berbasis *Internet of Things* (IoT) adalah dokumen yang menjelaskan tentang cara membangun sistem keamanan kunci pintu gedung yang menggunakan teknologi IoT. Sistem ini akan menggunakan sensor kunci pintu yang terhubung dengan jaringan internet, sehingga dapat diakses dan dikontrol secara *remote* melalui perangkat yang terhubung dengan internet. Sistem ini akan memiliki beberapa fitur seperti kemampuan untuk membuka dan mengunci pintu secara *remote*, memantau aktivitas pintu secara *real-time*, dan memberikan notifikasi kepada pengguna jika terjadi aktivitas yang tidak diinginkan di pintu. Dokumen ini juga akan menjelaskan tentang komponen-komponen yang dibutuhkan untuk membangun dan konfigurasi sistem ini. Dokumen ini digunakan sebagai acuan dalam pelaksanaan proyek dan pengerjaan produk Rancang Bangun Sistem Keamanan Kunci Pintu Gedung Berbasis *Internet of Things* yang direncanakan.

Rancangan awal tugas akhir Rancang Bangun Sistem Keamanan Kunci Pintu Gedung Berbasis *Internet of Things* yang dimuat dalam dokumen B100 ini mencakup empat bagian, yaitu:

- Bagian satu meliputi ringkasan isi dokumen, aplikasi dokumen, referensi, serta daftar singkatan.
- Bagian dua berisi pendahuluan, konsep desain, skenario pemanfaatan produk, nilai strategis, serta usaha pengembangan produk.
- Bagian tiga berisi kesimpulan.
- Bagian empat berisi biodata tim pengusul.

1.2 APLIKASI DOKUMEN

Dokumen ini berlaku untuk pengembangan produk “Rancang Bangun Sistem Keamanan Kunci Pintu Gedung Berbasis *Internet of Things*” untuk:

- (1) Sebagai gambaran umum dari segi teknik maupun non-teknis tugas akhir Rancang Bangun Sistem Keamanan Kunci Pintu Gedung Berbasis *Internet of Things* yang akan dikerjakan.
- (2) Memastikan kelayakan tugas akhir Rancang Bangun Sistem Keamanan Kunci Pintu Gedung Berbasis *Internet of Things*, baik dari segi teknik, waktu, biaya/ekonomis, maupun strategis.
- (3) Pencatatan proses kerja dan revisi yang dilakukan.

Proposal ini diajukan kepada dosen pembimbing dan tim tugas akhir Program Studi Sarjana Teknik Elektro Undip sebagai bahan penilaian tugas akhir.

1.3 REFERENSI

- [1] G. R. G. Wisnu, “RANCANG BANGUN SISTEM KEAMANAN PADA SMART BUILDING DENGAN PENERAPAN IoT (INTERNET OF THINGS),” *JATI (Jurnal Mahasiswa Teknik Informatika)*, vol. 1, no. 1, hlm. 828–835, 2017, doi: <https://doi.org/10.36040/jati.v1i1.2074>.
- [2] A. T. Sianturi, “RANCANG BANGUN SISTEM KEAMANAN RUANGAN DENGAN SENSOR CAHAYA BERBASIS ARDUINO UNO MENGGUNAKAN SMS GATEWAY,” Universitas Sumatra Utara, Medan, 2019. Diakses: Jan 19, 2023. [Daring]. Available: <https://123dok.com/document/zpnl36v4-rancang-keamanan-ruangan-berbasis-arduino-menggunakan-gateway-laporan.html>
- [3] Y. Efendi, “Internet Of Things (Iot) Sistem Pengendalian Lampu Menggunakan Raspberry Pi Berbasis Mobile,” *JURNAL ILMIAH ILMU KOMPUTER*, vol. 4, no. 2, hlm. 21–27, Sep 2018, doi: 10.35329/jiik.v4i2.41.
- [4] M. K. Syabibi dan A. Subari, “RANCANG BANGUN SISTEM MONITORING KEAMANAN RUMAH BERBASIS WEB MENGGUNAKAN RASPBERRY PI B+ SEBAGAI SERVER DAN MEDIA KONTROL,” *GEMA TEKNOLOGI*, vol. 19, no. 1, hlm. 22–29, 2016.

- [5] O. R. Galaxy, B. W. Sanjaya, dan F. T. P. W, “RANCANG BANGUN SISTEM PENGAMAN RUMAH TINGGAL BERBASIS ARDUINO UNO MENGGUNAKAN TELEPON PINTAR / SMARTPHONE ANDROID,” *JURNAL TEKNIK ELEKTRO UNIVERSITAS TANJUNGPURA*, vol. 1, no. 1, 2020, Diakses: Jan 20, 2023. [Daring]. Available: <https://jurnal.untan.ac.id/index.php/jteuntan/article/view/39605>
- [6] D. Widcaksono dan Masyhad, “RANCANG BANGUN SECURED DOOR AUTOMATIC SYSTEM UNTUK KEAMANAN RUMAH MENGGUNAKAN SMS BERBASIS ARDUINO,” *Ejournal Kajian Teknik Elektro*, vol. 3, no. 1, hlm. 52–66, 2018.
- [7] I. P. A. W. Widyatmika, N. P. A. W. Indrawati, I. W. W. A. Prastya, I. K. Darminta, I. G. N. Sangka, dan A. A. N. G. Sapteka, “Perbandingan Kinerja Arduino Uno dan ESP32 Terhadap Pengukuran Arus dan Tegangan,” *Jurnal Otomasi, Kontrol & Instrumentasi*, vol. 13, no. 1, hlm. 37–45, 2021.
- [8] S. Tjandra dan G. S. Chandra, “Pemanfaatan Flutter dan Electron Framework pada Aplikasi Inventori dan Pengaturan Pengiriman Barang,” *Journal of Information System, Graphics, Hospitality and Technology*, vol. 2, no. 02, hlm. 76–81, Des 2020, doi: 10.37823/insight.v2i02.109.
- [9] P. F. Nahak, N. M. R. Mamulak, dan Y. C. H. Siki, “Sistem Informasi Geografis Untuk Pemetaan Wifi.id Corner Dan Wifi Gratis di Kota Kupang Berbasis Web,” *Jurnal Teknik Informatika UnikaSt. Thomas (JTIUST)*, vol. 5, no. 1, hlm. 71–79, Jun 2020.
- [10] F. Luthfi, “Penggunaan Framework Laravel dalam Rancang Bangun Modul Back-End Artikel Website Bisnisbisnis.ID,” *JISKA (Jurnal Informatika Sunan Kalijaga)*, vol. 2, no. 1, hlm. 34–41, Agu 2017, doi: 10.14421/jiska.2017.21-05.
- [11] N. S. Hapsari, Y. Fatman, dan Isbandi, “Implementasi Metode One Time Password pada Sistem Pemesanan Online,” *JURNAL MEDIA INFORMATIKA BUDIDARMA*, vol. 4, no. 4, hlm. 930–939, Okt 2020.
- [12] J. Dedy irawan dan E. Adriantantri, “PEMANFAATAN QR-CODE SEBAGAI MEDIA PROMOSI TOKO,” *Jurnal Mnemonic*, vol. 1, no. 2, hlm. 56–61, Des 2019, doi: 10.36040/mnemonic.v1i2.39.

1.4 DAFTAR SINGKATAN

Tabel 1.1 Daftar Singkatan

SINGKATAN	ARTI
IoT	<i>Internet of Things</i>
iOS	<i>iPhone Operating System</i>
CCTV	<i>Closed Circuit Television</i>
RFID	<i>Radio Frequency Identification</i>
QR Code	<i>Quick Response Code</i>
SSO	<i>Single Sign On</i>
ESP	<i>Espressif</i>
GPIO	<i>General Purpose Input/Output</i>
IDE	<i>Integrated Development Environment</i>
Wi-Fi	<i>Wireless Fidelity</i>
BLE	<i>Bluetooth Low Energy</i>
DBMS	<i>Database Management System</i>
Ms. Access	<i>Microsoft Office Access</i>
SQL	<i>Structured Query Language</i>
VBA	<i>Visual Basic for Applications</i>
MVCC	<i>Multi-Version Concurrency Control</i>
JS	<i>Java Script</i>
API	<i>Application Programming Interface</i>
JWT	<i>JSON Web Token</i>
JSON	<i>Java Script Object Notation</i>
URL	<i>Uniform Resource Locator</i>
PWA	<i>Progressive Web Apps</i>
GPS	<i>Global Positioning System</i>
MVC	<i>Model View Controller</i>
HTTPS	<i>Hypertext Transfer Protocol Secure</i>
MQTT	<i>Message Queuing Telemetry Transport</i>
SSL/TLS	<i>Secure Sockets Layer/Transport Layer Security</i>

SINGKATAN	ARTI
WPA	<i>Wi-Fi Protected Access</i>
AES	<i>Advanced Encryption Standard</i>
LED	<i>Light Emitting Diode</i>
PC817	<i>Photo Coupler 817</i>
FCM	<i>Firebase Cloud Messaging</i>
OTP	<i>One Time Password</i>
SMS	<i>Short Messaging Services</i>
CCTV	<i>Closed Circuit Television</i>
kB	<i>kilo Byte</i>
ROM	<i>Read Only Memory</i>
SRAM	<i>Static Random-Access Memory</i>
RTC	<i>Real-Time Clock</i>
MB	<i>Mega Byte</i>
ADC	<i>Analog to Digital Converter</i>
SPI	<i>Serial Peripheral Interface</i>
SDK	<i>Software Development Kit</i>
PAN	<i>Personal Area Networks</i>
GHz	<i>Giga Hertz</i>
PHP	<i>Hypertext Preprocessor</i>
OOP	<i>Object Oriented Programming</i>
HOTP	<i>HMAC-based OTP</i>
TOTP	<i>Time-based OTP</i>
IEEE	<i>Institute of Electrical and Electronics Engineers</i>
NSPE	<i>National Society of Professional Engineer</i>
PCB	<i>Printed Circuit Board</i>
FTP	<i>File Transfer Protocol</i>
SMTP	<i>Simple Mail Transfer Protocol</i>
IMAP	<i>Instant Messaging Protocol</i>
HP	<i>Handphone</i>

2 PROPOSAL PENGEMBANGAN PRODUK

2.1 PENDAHULUAN

2.1.1 Latar Belakang Masalah

Sistem keamanan menjadi suatu aspek penting untuk menunjang kinerja dari sebuah gedung[1]. Gedung itu memiliki beberapa ruangan dan beberapa pintu untuk masuk. Tidak banyak orang yang meninggalkan ruangan, namun tidak menutup pintu dengan sempurna. Hal ini mungkin terdengar sepele tetapi siapa tahu ruangan tersebut memiliki privasi atau hal-hal penting yang perlu dijaga. Gedung pasti memiliki cara tersendiri dalam menjaga privasi dan keamanan setiap ruangnya.

Salah satu masalah utama dalam sistem keamanan kunci pintu gedung adalah bagaimana cara mengelola akses masuk ke dalam gedung dengan cepat dan efisien. Biasanya, dibutuhkan seorang petugas untuk mengelola akses masuk ke dalam gedung, yang tentunya dapat menyebabkan kesalahan atau kelambatan dalam proses pengelolaan akses. Selain itu, sistem keamanan kunci pintu gedung yang biasa digunakan saat ini juga sering mengalami masalah seperti kunci hilang atau tidak dapat digunakan, yang dapat menyebabkan gangguan dalam aktivitas di dalam gedung. Dengan sistem keamanan yang terintegrasi akan sangat membantu meminimalisir sebuah masalah sistem keamanan dalam gedung/ruangan dari bahaya adanya orang lain yang masuk tanpa seizin pemilik[2].

Sebuah sistem keamanan *Access Control* memungkinkan pemilik bangunan dan properti untuk melakukan lebih dari sekedar mengontrol masuk ke daerah yang diproteksi[2]. Sistem ini juga dapat membuat catatan *history* atau informasi secara elektronik mengenai siapa saja yang masuk ke dalam ruangan yang sudah diproteksi[2]. Dengan adanya catatan informasi tersebut membantu pemilik usaha mengidentifikasi siapa saja yang masuk ke ruangan pada waktu-waktu tertentu[2].

Internet of Thing (IoT) merupakan suatu konsep yang bertujuan untuk memperluas manfaat dari konektivitas internet yang tersambung secara terus menerus[3]. *Internet of Things* (IoT) bisa dimanfaatkan pada gedung perkantoran maupun rumah sebagai alat untuk mengendalikan peralatan elektronik dan juga sebagai suatu sistem keamanan yang dapat dioperasikan dari jarak jauh melalui jaringan komputer. Sehingga tidak dapat dipungkiri bahwa teknologi ini harus bisa diterapkan dalam kehidupan sehari-hari.

Dengan menggunakan sistem keamanan kunci pintu gedung berbasis IoT, diharapkan dapat memudahkan pengelolaan akses masuk ke dalam gedung, serta meningkatkan keamanan dengan mengontrol akses masuk hanya kepada orang-orang yang memiliki izin saja. Sistem ini menggunakan teknologi IoT untuk mengontrol akses masuk ke dalam gedung dengan menggunakan perangkat seluler atau kartu akses yang terhubung ke internet. Misalnya, dengan menggunakan aplikasi atau *web interface* yang terhubung ke internet, admin dapat dengan mudah mengelola akses masuk ke gedung, menambah atau menghapus kunci elektronik, dan mengontrol pintu dari jarak jauh. Selain itu, sistem keamanan kunci pintu gedung berbasis IoT juga dapat dilengkapi dengan sensor dan memberikan notifikasi kepada admin jika terdeteksi aktivitas yang tidak diinginkan. Hal ini dapat membantu meningkatkan keamanan gedung dan mengurangi risiko kejahatan seperti pencurian.

Oleh karena itu, berdasarkan uraian latar belakang masalah di atas maka muncul sebuah gagasan yang berjudul “Rancang Bangun Sistem Keamanan Kunci Pintu Gedung Berbasis *Internet of Things*” yang diharapkan dapat meningkatkan efisiensi dan keamanan dalam pengelolaan akses masuk ke dalam gedung.

2.1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang telah dijelaskan di atas, maka permasalahan yang akan dibahas yaitu:

1. Bagaimana perancangan sistem keamanan kunci pintu gedung dengan *Access Control*?
2. Bagaimana perancangan perangkat penguncian yang mendukung sistem keamanan kunci pintu gedung berbasis IoT?
3. Bagaimana perancangan sistem *database* dan *server* untuk mendukung sistem keamanan *Access Control* dan pembuatan catatan *history* atau informasi?
4. Bagaimana perancangan aplikasi perangkat *mobile* yang dapat *support* android dan iOS sebagai piranti akses masuk pintu gedung?
5. Bagaimana perancangan *website* untuk mendukung sistem *monitoring* dan *controlling* jarak jauh?
6. Bagaimana perancangan sistem komunikasi data dua arah untuk mendukung sistem keamanan kunci pintu gedung berbasis IoT?

2.1.3 Tujuan

Produk yang dirancang pada proposal tugas akhir ini adalah sebuah sistem keamanan kunci pintu gedung berbasis *Internet of Things* dengan tujuan pengembangan sebagai berikut:

1. Merancang sistem keamanan kunci pintu gedung dengan *Access Control*.
2. Merancang perangkat penguncian yang mendukung sistem keamanan kunci pintu gedung berbasis IoT.
3. Merancang sistem *database* dan *server* untuk mendukung sistem keamanan *Access Control* dan pembuatan catatan *history* atau informasi.
4. Merancang aplikasi perangkat *mobile* yang dapat *support* android dan iOS sebagai piranti akses masuk pintu gedung.
5. Merancang *website* untuk mendukung sistem *monitoring* dan *controlling* jarak jauh.
6. Merancang sistem komunikasi data dua arah untuk mendukung sistem keamanan kunci pintu gedung berbasis IoT.

2.1.4 Alternatif Desain

a. Perancangan sistem keamanan kunci pintu gedung dengan *Access Control*

Membangun sistem keamanan berbasis teknologi memerlukan perhatian khusus baik dari instansi pemerintah maupun swasta. Bagian dari sistem keamanan adalah kontrol akses, yang tidak hanya menjaga keamanan gedung tetapi juga membatasi akses masuk. Sistem kontrol akses membatasi akses ke sumber daya baik secara fisik maupun virtual. Dengan demikian, hanya pengguna tertentu yang memiliki hak akses untuk menjaga keamanan gedung.

Orang yang menerima hak pakai harus memiliki informasi identifikasi dan dapat diverifikasi dengan identifikasi. Oleh karena itu, sistem keamanan gedung dapat diimplementasikan menggunakan kode atau nilai biometrik, sedangkan proses otentikasi dapat diimplementasikan menggunakan berbagai metode. Proses otentikasi dapat dilakukan melalui penggunaan kata sandi atau PIN, pengukuran biometrik seperti pemindaian retina, sidik jari, wajah, dan lainnya. Faktor lain dalam proses otentikasi dapat diimplementasikan oleh kartu atau kunci pengguna.

Selain menjadikan keamanan gedung lebih terjaga, akses kontrol membantu memantau riwayat akses secara rinci.

Biasanya hotel, perusahaan, rumah dan kantor menerapkan sistem akses kontrol, bahkan ada yang menggunakannya di rumah pribadi. Sistem ini tidak hanya penting dari segi keamanan, tetapi juga dapat membantu meningkatkan kinerja karyawan di perusahaan. Kontrol akses hanya memberikan hak akses terbatas kepada pihak yang memiliki informasi lisensi. Sistem akses ini juga memberikan kemudahan bagi petugas keamanan untuk memantau dengan fitur-fitur yang disediakan oleh sistem.

Setiap akses dapat dikelola dengan baik karena terdapat riwayat penggunaan yang detail. Bayangkan perusahaan tidak memiliki sistem keamanan, seperti kontrol akses yang tidak menyebabkan hak akses terbatas. Akibatnya, ada risiko bagi perusahaan bahwa penyusup dapat memasuki pintu masuk melalui kontrol akses seperti di hotel yaitu dengan kartu. Sistem keamanan juga dilengkapi dengan fasilitas CCTV untuk memantau dengan baik lingkungan hotel demi kenyamanan pelanggan.

Berdasarkan hasil analisis sistem *Access Control* untuk sistem keamanan kunci pintu gedung berbasis *Internet of Things*, maka terdapat beberapa alternatif desain yang dapat digunakan, yaitu:

1) Sistem *Access Control* berbasis kartu

Sistem ini menggunakan kartu yang diberikan kepada pengguna gedung untuk membuka pintu-pintu gedung. Kartu dapat berupa kartu RFID.

Sistem *Access Card* berbasis RFID sangat populer di kalangan perusahaan atau perkantoran. Dengan menggunakan kartu RFID setiap pengguna akan memiliki kunci atau *key* yang tersimpan di dalam kartu tersebut. Setiap kartu RFID mempunyai ruang penyimpanan cukup besar yaitu *2000byte* yang dapat digunakan untuk menyimpan data untuk keperluan tertentu.

Adapun kelemahan sistem akses *card* berbasis RFID adalah RFID memiliki tingkat keamanan yang rendah, setiap kartu RFID dapat dengan mudah disalin hanya dengan menggunakan *reader* yang beredar dipasaran, sehingga data di dalamnya dapat disalahgunakan oleh orang lain yang tidak berwenang. Selain

itu, karena berukuran kecil, sebuah kartu RFID juga sering hilang atau tertinggal, sehingga perlu mencetak kartu baru untuk mendapatkan akses lagi.

2) Sistem *Access Control* berbasis biometrik

Sistem ini menggunakan fitur-fitur biometrik seperti sidik jari, iris, atau wajah sebagai cara untuk memverifikasi identitas pengguna gedung.

Sistem biometrik sangat banyak digunakan sebagai metode untuk melakukan autentikasi pada keamanan *Access Control*. Sistem biometrik menggunakan fisik manusia sebagai suatu identitas yang unik sehingga sangat sulit untuk dipalsukan.

Adapun kelemahannya adalah mesin identifikasi biometrik lebih mahal untuk dibeli daripada yang tradisional. Selain itu, beberapa pengguna mungkin menentang biometrik sama sekali, menganggapnya sebagai pelanggaran privasi. Selain itu, perangkat pengenalan biometrik tidak selalu akurat. Misalnya, orang yang kedinginan tidak dapat mengidentifikasi dirinya dengan perangkat pengenalan suara, dan orang yang mengalami kenaikan atau penurunan berat badan tiba-tiba dapat kehilangan akses ke area yang dilindungi oleh sistem yang menganalisis fitur wajah.

3) Sistem *Access Control* berbasis *Single Sign On* (SSO)

Sistem *Access Control* berbasis *Single Sign On* (SSO) adalah salah satu jenis sistem keamanan kunci pintu gedung yang memungkinkan pengguna gedung untuk membuka pintu-pintu gedung dengan menggunakan satu akun yang sama yang digunakan untuk *login* ke sistem manajemen gedung atau aplikasi keamanan lainnya. Hal ini sangat memudahkan pengguna karena tidak perlu banyak akun untuk mengakses beberapa layanan yang ada. Dikarenakan hanya menggunakan satu akun maka *log* akses dapat mencatat semua riwayat tentang siapa saja yang telah mengakses sistem atau aplikasi, sehingga siapa saja yang telah menyalahgunakan akun bisa diketahui melalui *log* akses ini.

Namun, sistem *Access Control* berbasis SSO juga memiliki beberapa kekurangan. Salah satunya adalah bahwa perangkat yang digunakan untuk *login* ke sistem harus terhubung dengan *Internet of Things* agar dapat bekerja dengan baik. Selain itu, ada kemungkinan bahwa akun yang digunakan dapat

dicuri atau disalahgunakan oleh pihak yang tidak bertanggung jawab, sehingga mengurangi keamanan sistem.

4) Sistem *Access Control* berbasis QR Code

Sistem *Access Control* berbasis QR Code atau kode QR adalah salah satu jenis sistem keamanan kunci pintu gedung yang menggunakan kode QR sebagai cara untuk membuka pintu-pintu gedung. Pengguna gedung dapat memindai kode QR yang terpasang di dekat pintu dengan menggunakan *smartphone* atau perangkat lain yang terhubung dengan *Internet of Things*.

Kelebihan dari sistem *Access Control* berbasis kode QR adalah mudah digunakan dan tidak memerlukan perangkat tambahan seperti kartu atau *keypad*. Sistem ini juga dapat dengan mudah diintegrasikan dengan aplikasi manajemen gedung atau aplikasi keamanan lainnya. Selain itu, kode QR memiliki layar yang lebih kecil daripada *barcode*. Karena kode QR dapat menerima informasi secara horizontal dan vertikal, maka ukuran tampilan gambar kode QR otomatis hanya sepersepuluh dari ukuran *barcode*. Oleh karena itu, meskipun beberapa simbol kode QR kotor atau rusak, informasinya masih dapat disimpan dan dibaca. Kode QR juga dapat dengan mudah diakses dengan cepat sehingga cocok digunakan dengan *smartphone*.

Namun, sistem *Access Control* berbasis kode QR juga memiliki beberapa kekurangan. Sebuah kode QR memerlukan sebuah *scanner* untuk membaca data yang tersimpan di dalamnya dan juga memerlukan sebuah sistem yang dapat menerjemahkan data tersebut sehingga prosesnya cukup kompleks.

b. Perancangan perangkat penguncian yang mendukung sistem keamanan kunci pintu gedung berbasis IoT

Perangkat penguncian merupakan alat yang akan dipasang pada setiap pintu dan digunakan untuk melakukan proses penguncian. Pada perangkat penguncian terdapat 4 bagian yaitu sensor, mikrokontroler, aktuator, dan *power*.

1) Sensor

Pada perangkat penguncian, sensor digunakan untuk melakukan *monitoring* kondisi pintu, sensor yang digunakan harus dapat mengetahui kondisi pintu sedang terbuka atau tertutup.

Berdasarkan kedua kondisi pintu tersebut (terbuka dan tertutup), untuk sistem keamanan kunci pintu gedung berbasis *Internet of Things*, maka terdapat beberapa alternatif desain sensor yang dapat digunakan, yaitu:

- *Limit switch*

Kelebihan menggunakan *limit switch* untuk sistem keamanan kunci pintu gedung berbasis IoT adalah harganya relatif murah, sehingga dapat menjadi pilihan yang ekonomis untuk mengontrol akses ke pintu gedung. Tidak memerlukan banyak perawatan atau pemeliharaan, sehingga dapat mengurangi biaya pemeliharaan. Dapat bekerja dengan baik dalam kondisi yang keras, seperti suhu tinggi atau lingkungan yang berdebu.

Kelemahan menggunakan *limit switch* untuk sistem keamanan kunci pintu gedung berbasis IoT adalah pemasangan dan kalibrasi dapat menjadi rumit, terutama jika digunakan dalam aplikasi yang kompleks. Dapat menjadi tidak akurat jika terkena benturan atau terguncang. Dapat menjadi tidak responsif dalam situasi yang berubah cepat. Dapat terpengaruh oleh lingkungan yang berdebu atau kotor, yang dapat menyebabkan kontak terbuka atau tertutup secara tidak sengaja.

- Saklar magnetik

Saklar magnetik menggunakan magnet yang terpasang pada daun pintu untuk memicu saklar sehingga tidak ada kontak langsung dengan daun pintu.

Kelebihan menggunakan saklar magnetik untuk sistem keamanan kunci pintu gedung berbasis IoT adalah dapat mendeteksi objek dengan akurasi yang tinggi, sehingga dapat meningkatkan keamanan gedung dengan membatasi akses hanya untuk orang yang memiliki izin atau otorisasi yang sesuai. Dapat bekerja dengan baik dalam kondisi yang keras, seperti suhu tinggi atau lingkungan yang berdebu. Dapat bekerja dengan baik dalam kondisi yang terlalu cepat atau terlalu lambat.

Kelemahan menggunakan saklar magnetik untuk sistem keamanan kunci pintu gedung berbasis IoT adalah harganya relatif lebih mahal dibandingkan dengan sensor lain yang memiliki fungsi yang sama. Pemasangan dan kalibrasi dapat menjadi rumit, terutama jika digunakan dalam aplikasi yang kompleks. Dapat menjadi tidak responsif dalam situasi yang berubah cepat.

Dapat terpengaruh oleh lingkungan yang berdebu atau kotor, yang dapat menyebabkan kontak terbuka atau tertutup secara tidak sengaja.

2) Mikrokontroler

Untuk membaca sensor, kita memerlukan sebuah mikrokontroler. Dikarenakan sensor yang digunakan hanya memiliki dua kondisi maka kita cukup menggunakan *input* digital, yaitu pin *input* pada mikrokontroler yang digunakan untuk membaca nilai atau data digital (nilai benar atau salah).

Untuk sistem keamanan kunci pintu gedung berbasis *Internet of Things*, maka terdapat beberapa alternatif desain mikrokontroler yang dapat digunakan, yaitu:

- Arduino

Arduino memiliki 14 GPIO dan 6 *input* analog yang dapat kita gunakan dan juga lingkungan pengembangan yang mudah menggunakan ArduinoIDE.

Kelebihan Arduino untuk sistem keamanan kunci pintu gedung berbasis IoT adalah Arduino sangat mudah diprogram dan tidak memerlukan pemrograman yang rumit. Arduino memiliki banyak sensor yang tersedia yang dapat digunakan untuk mendeteksi gerakan, suhu, kelembaban, dan banyak lagi. Arduino sangat terjangkau dan mudah didapat dipasaran. Arduino memiliki banyak dokumentasi dan sumber daya *online* yang tersedia untuk membantu memulai proyek.

Kelemahan Arduino untuk sistem keamanan kunci pintu gedung berbasis IoT adalah Arduino tidak memiliki kemampuan pemrosesan yang kuat, sehingga mungkin tidak cocok untuk proyek yang membutuhkan pemrosesan data yang intensif. Arduino memiliki batasan dalam hal penyimpanan data, sehingga mungkin tidak cocok untuk proyek yang membutuhkan penyimpanan data yang besar. Arduino tidak memiliki kemampuan konektivitas yang kuat, sehingga mungkin tidak cocok untuk proyek yang membutuhkan konektivitas yang kuat atau konektivitas ke internet. Arduino mungkin tidak cocok untuk proyek yang membutuhkan keamanan yang ketat, karena tidak memiliki fitur keamanan yang canggih.

- ESP8266

ESP8266 tidak memiliki banyak GPIO, akan tetapi ESP8266 memiliki modul WiFi yang dapat kita gunakan untuk berkomunikasi dengan pengguna.

Kelebihan ESP8266 untuk sistem keamanan kunci pintu gedung berbasis IoT adalah ESP8266 memiliki kemampuan konektivitas yang kuat, sehingga mudah terhubung ke internet melalui WiFi. ESP8266 memiliki kemampuan pemrosesan yang lebih baik dibandingkan Arduino, sehingga lebih cocok untuk proyek yang membutuhkan pemrosesan data yang intensif. ESP8266 memiliki penyimpanan data yang lebih besar dibandingkan Arduino, sehingga lebih cocok untuk proyek yang membutuhkan penyimpanan data yang besar. ESP8266 memiliki fitur keamanan yang lebih canggih dibandingkan Arduino, sehingga lebih cocok untuk proyek yang membutuhkan keamanan yang ketat.

Kelemahan ESP8266 untuk sistem keamanan kunci pintu gedung berbasis IoT adalah ESP8266 mungkin lebih sulit diprogram dibandingkan Arduino, karena memerlukan pemrograman yang lebih rumit. ESP8266 mungkin lebih mahal dibandingkan Arduino, karena memiliki kemampuan yang lebih baik. ESP8266 mungkin kurang tersedia dipasaran dibandingkan Arduino, sehingga mungkin lebih sulit didapat. Dokumentasi dan sumber daya *online* untuk ESP8266 mungkin lebih terbatas dibandingkan Arduino, sehingga mungkin lebih sulit untuk memulai proyek dengan ESP8266.

- ESP32

ESP32 merupakan pengembangan dari ESP8266, ESP32 mempunyai banyak GPIO (seperti Arduino), memiliki modul WiFi dan ditambah dengan modul BLE (*Bluetooth Low Energy*) yang dapat digunakan secara bersamaan.

Kelebihan ESP32 untuk sistem keamanan kunci pintu gedung berbasis IoT adalah ESP32 memiliki kemampuan pemrosesan yang lebih baik dibandingkan ESP8266, sehingga lebih cocok untuk proyek yang membutuhkan pemrosesan data yang intensif. ESP32 memiliki penyimpanan data yang lebih besar dibandingkan ESP8266, sehingga lebih cocok untuk proyek yang membutuhkan penyimpanan data yang besar. ESP32 memiliki fitur keamanan yang lebih canggih dibandingkan ESP8266, sehingga lebih

cocok untuk proyek yang membutuhkan keamanan yang ketat. ESP32 memiliki kemampuan konektivitas yang kuat, sehingga mudah terhubung ke internet melalui WiFi atau *Bluetooth*.

Kelemahan ESP32 untuk sistem keamanan kunci pintu gedung berbasis IoT adalah ESP32 mungkin lebih sulit diprogram dibandingkan ESP8266, karena memerlukan pemrograman yang lebih rumit. ESP32 mungkin lebih mahal dibandingkan ESP8266, karena memiliki kemampuan yang lebih baik. ESP32 mungkin kurang tersedia dipasaran dibandingkan ESP8266, sehingga mungkin lebih sulit didapat. Dokumentasi dan sumber daya *online* untuk ESP32 mungkin lebih terbatas dibandingkan ESP8266, sehingga mungkin lebih sulit untuk memulai proyek dengan ESP32.

3) Aktuator

Aktuator adalah perangkat yang digunakan untuk mengeluarkan sinyal atau tindakan sesuai dengan perintah yang diterima dari sistem keamanan kunci pintu gedung berbasis *Internet of Things*. Berikut adalah beberapa alternatif desain aktuator yang dapat digunakan dalam sistem keamanan kunci pintu gedung berbasis *Internet of Things*:

- Motor elektronik

Motor elektronik dapat digunakan sebagai aktuator untuk membuka dan menutup pintu-pintu gedung.

Kelebihan motor elektronik untuk sistem keamanan kunci pintu gedung berbasis IoT adalah motor elektronik memiliki torsi yang lebih tinggi dibandingkan motor mekanik, sehingga lebih cocok untuk menggerakkan beban yang berat. Motor elektronik lebih efisien dibandingkan motor mekanik, karena memiliki rendahnya kehilangan daya. Motor elektronik memiliki umur pakai yang lebih panjang dibandingkan motor mekanik, karena tidak memiliki bagian-bagian mekanik yang harus diganti. Motor elektronik memiliki kecepatan yang mudah diatur, sehingga lebih mudah untuk mengontrol kecepatan gerakan sistem keamanan kunci pintu.

Kelemahan motor elektronik untuk sistem keamanan kunci pintu gedung berbasis IoT adalah motor elektronik mungkin lebih mahal dibandingkan motor mekanik, karena memiliki kemampuan yang lebih baik. Motor elektronik mungkin membutuhkan lebih banyak peralatan elektronik untuk

mengontrolnya, sehingga mungkin lebih sulit untuk dipasang dan diatur. Motor elektronik mungkin lebih rentan terhadap kerusakan akibat kelebihan arus atau tegangan, sehingga membutuhkan proteksi yang lebih baik. Motor elektronik mungkin tidak cocok untuk aplikasi yang membutuhkan kekuatan yang tinggi, karena tidak dapat menghasilkan torsi yang sama dengan motor mekanik.

- Solenoid

Solenoid adalah perangkat yang mengeluarkan medan magnet yang bisa digunakan untuk membuka atau mengunci pintu-pintu gedung.

Kelebihan solenoid untuk sistem keamanan kunci pintu gedung berbasis IoT adalah solenoid mudah diatur dan dioperasikan, karena hanya memerlukan arus listrik untuk bekerja. Solenoid memiliki ukuran yang kecil dan ringan, sehingga mudah dipasang dan dipindahkan. Solenoid memiliki kecepatan yang tinggi, sehingga dapat dengan cepat mengunci atau membuka kunci pintu. Solenoid memiliki umur pakai yang panjang, karena tidak memiliki bagian-bagian mekanik yang harus diganti.

Kelemahan solenoid untuk sistem keamanan kunci pintu gedung berbasis IoT adalah solenoid tidak dapat menghasilkan torsi yang tinggi, sehingga tidak cocok untuk aplikasi yang membutuhkan kekuatan yang tinggi. Solenoid mungkin tidak cocok untuk aplikasi yang membutuhkan gerakan yang lincah atau akurasi yang tinggi, karena tidak dapat menghasilkan gerakan yang halus. Solenoid mungkin tidak cocok untuk aplikasi yang membutuhkan kecepatan yang tinggi, karena tidak dapat bekerja dengan cepat dalam jangka waktu yang lama. Solenoid mungkin tidak cocok untuk aplikasi yang membutuhkan keandalan yang tinggi, karena mungkin rentan terhadap kerusakan akibat kelebihan arus atau tegangan.

- Relay

Relay adalah perangkat yang bisa mengeluarkan sinyal atau tindakan sesuai dengan perintah yang diterima dari sistem.

Kelebihan *relay* untuk sistem keamanan kunci pintu gedung berbasis IoT adalah *relay* dapat mengontrol arus yang lebih besar dibandingkan solenoid, sehingga lebih cocok untuk aplikasi yang membutuhkan kekuatan yang

tinggi. *Relay* memiliki umur pakai yang panjang, karena tidak memiliki bagian-bagian mekanik yang harus diganti. *Relay* dapat diatur dan dioperasikan dengan mudah, karena hanya memerlukan arus listrik untuk bekerja. *Relay* memiliki keandalan yang tinggi, karena tidak rentan terhadap kerusakan akibat kelebihan arus atau tegangan.

Kelemahan *relay* untuk sistem keamanan kunci pintu gedung berbasis IoT adalah *relay* mungkin tidak cocok untuk aplikasi yang membutuhkan gerakan yang lincah atau akurasi yang tinggi, karena tidak dapat menghasilkan gerakan yang halus. *Relay* mungkin tidak cocok untuk aplikasi yang membutuhkan kecepatan yang tinggi, karena tidak dapat bekerja dengan cepat dalam jangka waktu yang lama. *Relay* mungkin memiliki ukuran yang lebih besar dan berat dibandingkan solenoid, sehingga mungkin lebih sulit dipasang dan dipindahkan. *Relay* mungkin membutuhkan lebih banyak peralatan elektronik untuk mengontrolnya, sehingga mungkin lebih sulit untuk dipasang dan diatur.

4) *Power*

Berikut adalah beberapa alternatif desain *power* yang dapat digunakan untuk sistem keamanan kunci pintu gedung berbasis *Internet of Things*:

- Baterai

Baterai dapat digunakan sebagai *power* untuk sistem keamanan kunci pintu gedung berbasis *Internet of Things*. Baterai memiliki kelebihan dalam hal portabilitas dan tidak tergantung pada sumber listrik, namun memiliki masa pakai yang terbatas dan harus diganti secara teratur.

- Adaptor listrik

Adaptor listrik dapat digunakan sebagai *power* untuk sistem keamanan kunci pintu gedung berbasis *Internet of Things*. Adaptor listrik tergantung pada sumber listrik yang tersedia, namun memiliki masa pakai yang lebih panjang dibandingkan baterai.

c. Perancangan sistem *database* dan *server* untuk mendukung sistem keamanan *Access Control* dan pembuatan catatan *history* atau informasi

Database merupakan salah satu komponen teknologi informasi yang mutlak diperlukan bagi setiap organisasi yang ingin memiliki sistem informasi yang

terintegrasi untuk mendukung operasional organisasi dalam mencapai tujuannya. Pada sistem kunci pintu gedung berbasis IoT ini, *database* digunakan untuk menyimpan data-data yang diperlukan untuk menjalankan sistem kunci pintu gedung. Data yang akan disimpan terdiri dari beberapa tabel data seperti data pengguna, data perangkat yang terpasang, data jadwal perangkat, data riwayat akses, dan lain sebagainya. Sebuah *database* membutuhkan sebuah DBMS atau *Database Management System* yang digunakan untuk mengatur kinerja dan pengolahan data di dalam *database*. Pada pengembangan sistem kunci pintu gedung berbasis IoT, terdapat beberapa DBMS yang dapat digunakan, yaitu:

1) Ms. Access

Salah satu keunggulan *Microsoft Access* yaitu kompatibilitasnya dengan bahasa pemrograman *Structured Query Language* (SQL). Pengguna dapat mencampur dan mencocokkan kedua bahasa (VBA dan makro) untuk memprogram bentuk dan logika serta menerapkan konsep berorientasi objek. Namun, *Microsoft Access* kurang baik jika digunakan melalui *web*, sehingga aplikasi yang digunakan banyak pengguna biasanya menggunakan solusi sistem manajemen basis data yang bersifat *client-server*.

2) MySQL

MySQL merupakan salah satu sistem *database* yang banyak digunakan untuk mendukung kinerja dari berbagai aplikasi. MySQL dapat mendukung berbagai macam bahasa pemrograman sehingga dapat digunakan untuk berbagai *platform*. MySQL memberikan kemudahan pengelolaan *database* dengan dukungan dari komunitas yang banyak serta keamanan dan perkembangan *software*-nya yang cepat.

MySQL sangat cocok digunakan untuk mengelola data yang terstruktur akan tetapi untuk data yang berukuran besar MySQL akan mengalami penurunan performa. MySQL juga memiliki keterbatasan kinerja pada *server* ketika data yang disimpan melebihi kapasitas maksimal *server* karena tidak menggunakan konsep teknologi *server cluster*.

3) PostgreSQL

Dengan *PostgreSQL*, tidak ada yang dapat menuntut pelanggaran perjanjian lisensi karena tidak ada (paket) biaya lisensi yang terkait dengan perangkat

lunak. Akibatnya, *PostgreSQL* menawarkan keuntungan tambahan, termasuk bisnis yang lebih menguntungkan dengan penerapan skala besar. Tidak ada cara untuk memeriksa kepatuhan lisensi, fleksibilitas untuk mengimplementasikan konsep penelitian dan penggunaan eksperimental tanpa biaya lisensi tambahan. *Postgre* juga dapat menyimpan data dengan banyak baris (*multiple rows*) yang dinamakan MVCC sehingga *PostgreSQL* sangat responsif pada *high volume environments*.

Dilihat dari layanan yang diberikan, *PostgreSQL* kurang unggul dalam hal ketersediaan fungsi *built-in* dan replikasi di *PostgreSQL* belum disertakan dalam distribusi standarnya yang terbatas hanya bisa melakukan penambahan kolom, penggantian nama kolom, dan penggantian nama tabel.

4) *Firebase*

Firebase menawarkan fitur pengelolaan data yang cepat dan gratis, *Firebase* juga dapat digunakan pada berbagai *platform* IoT. Akan tetapi, *Firebase* memiliki penyimpanan data tidak terstruktur sehingga sangat sulit untuk mengelola data yang terstruktur.

Selain membutuhkan *database*, sistem kunci pintu gedung berbasis IoT juga membutuhkan sebuah *server*. *Server* digunakan untuk melakukan operasi dan pengolahan data, melakukan autentikasi, serta mencatat riwayat pengguna. Beberapa *server* yang dapat digunakan untuk mendukung kinerja dari sistem kunci pintu berbasis IoT yaitu:

1) *NodeJS*

Node.js merupakan sebuah *environment* lintas *platform* yang dibangun berdasarkan *engine JavaScript V8 Chrome*. Pembuatan aplikasi dengan *NodeJS* dilakukan melalui *virtual private server*. *NodeJS* menawarkan operasi *input/output non-blocking*, serta dibangun dengan arsitektur asinkron dan *event-driven* untuk membantu *developer* membuat berbagai *project* dengan mudah dan efisien. *NodeJS* cocok digunakan untuk aplikasi *realtime* yang membutuhkan waktu respon cepat.

2) *Laravel*

Laravel menyediakan cara mudah untuk membangun *Restful API* yang aman dengan sebuah sistem autentikasi dengan menerapkan sistem autentikasi

dengan JWT. *Restful* API digunakan untuk bertukar sumber daya *web* seperti data dalam *database*, gambar, dan file. Independen dari format sumber daya ini mengirimkannya ke klien dalam format JSON oleh URL. Klien meminta sumber daya melalui metode yang sesuai seperti (GET) permintaan jika klien ingin mendapatkan sumber daya, dan POST permintaan untuk mengirim sumber daya ke sisi *server*, atau permintaan (DELETE) untuk menghapus sumber daya tertentu.

d. Perancangan aplikasi perangkat *mobile* yang dapat *support* android dan iOS sebagai piranti akses masuk pintu gedung

Perancangan aplikasi *mobile* penguncian pintu dapat digunakan untuk mengontrol sistem penguncian pintu melalui perangkat *mobile*. Aplikasi *mobile* dapat membantu meningkatkan keamanan dan kenyamanan dengan memungkinkan pengguna untuk membuka atau mengunci pintu dengan mudah dan cepat. Aplikasi *mobile* penguncian pintu dapat membantu meningkatkan keamanan dan kenyamanan dengan memungkinkan pengguna untuk memantau dan mengontrol akses kepada pintu. Beberapa alternatif desain yang dapat digunakan untuk membuat aplikasi *mobile* yang dapat *support* android dan iOS pada pengembangan sistem keamanan kunci pintu gedung yaitu:

1) *Flutter*

Flutter adalah *framework open source* yang dikembangkan oleh *Google* untuk membuat aplikasi *mobile* yang dapat dijalankan di sistem operasi Android dan iOS. *Flutter* menyediakan fitur *Hot Reload* yang memungkinkan *developer* untuk mengedit, menambahkan, atau menghapus kode tanpa harus memulai ulang aplikasi. Ini mempercepat proses pengembangan dan memudahkan *developer* untuk mencoba ide-ide baru. *Flutter* juga menyediakan *widget* yang responsif sehingga aplikasi yang dibuat akan terlihat baik di berbagai ukuran layar.

Flutter memiliki kekurangan yaitu hanya dapat digunakan dengan bahasa pemrograman Dart, yang mungkin tidak *familiar* bagi sebagian *developer*. Meskipun *Flutter* dapat digunakan untuk membuat aplikasi yang dapat dijalankan di Android dan iOS, terkadang ada keterbatasan dalam integrasi

dengan fitur-fitur *native* pada sistem operasi tersebut. Aplikasi yang dibuat dengan *Flutter* cenderung lebih besar dibandingkan dengan aplikasi yang dibuat dengan *framework* lain karena *Flutter* membawa *library* dan komponen-komponen yang dibutuhkan untuk menjalankannya.

2) *Progressive Web Apps* (PWA)

Progressive Web Apps (PWA) adalah aplikasi *web* yang dapat di-*install* di perangkat seperti aplikasi *native*, tetapi masih dibuka dan dijalankan melalui *browser*. PWA dapat di-*install* di perangkat dengan mudah melalui *browser*, tanpa perlu mengunduh dari toko aplikasi seperti *Google Play* atau *App Store*. PWA cenderung memiliki performa yang lebih baik dibandingkan dengan aplikasi *native* karena tidak membutuhkan waktu untuk di-*download* dan di-*install*. PWA dapat dijalankan di berbagai perangkat yang mendukung *browser*, seperti *smartphone*, tablet, maupun desktop.

Dibalik dari kelebihanannya, PWA terkadang memiliki keterbatasan dalam mengakses fitur-fitur perangkat seperti kamera atau GPS, tergantung pada *browser* yang digunakan. PWA terkadang memiliki keterbatasan dalam mengirim notifikasi *push* ke perangkat, tergantung pada *browser* yang digunakan.

e. Perancangan *website* untuk mendukung sistem *monitoring* dan *controlling* jarak jauh

Perancangan aplikasi berbasis *website* dimaksudkan untuk lebih memudahkan admin untuk mengendalikan atau mengatur sistem kunci pintu gedung berbasis IoT seperti mengatur penjadwalan, menambahkan pengguna baru, membuat undangan, dan lain sebagainya. Beberapa pilihan *framework* yang dapat digunakan untuk membuat *website* pada pengembangan sistem keamanan kunci pintu gedung yaitu:

1) *ReactJS*

ReactJS merupakan sebuah *library javascript* yang digunakan untuk membangun tampilan pada sebuah aplikasi berbasis *website*. Keunggulan dari *ReactJS* yaitu setiap tampilan yang dibuat menggunakan basis komponen sehingga setiap komponen dapat digunakan secara berulang pada tampilan yang

berbeda. Keunggulan lainnya yaitu *ReactJS* bersifat *Single Page Application* sehingga aplikasi yang dibuat tidak perlu melakukan *reload* halaman secara utuh setiap ada perubahan data.

2) Laravel

Laravel mengikuti pola arsitektur *Model View Controller* (MVC). MVC memisahkan aplikasi berdasarkan komponen aplikasi seperti komputasi, pengontrol, dan antarmuka pengguna. Keuntungan pengembangan aplikasi *web* menggunakan metode ini adalah dalam proses *maintenance* dan *scalability* yang lebih mudah. Dengan menggunakan *laravel*, sebuah *website* juga dapat bekerja dengan *web API* secara simultan dalam satu *server*.

f. Perancangan sistem komunikasi data dua arah untuk mendukung sistem keamanan kunci pintu gedung berbasis IoT

Untuk mendukung sistem keamanan kunci pintu gedung berbasis IoT, perlu membuat sistem komunikasi data yang dapat mengirim dan menerima data dari perangkat IoT yang terhubung ke sistem. Ada beberapa hal yang perlu dipertimbangkan dalam perancangan sistem komunikasi ini:

1) Protokol Komunikasi

Protokol komunikasi perlu disesuaikan dengan kemampuan dan operasi yang akan dijalankan dalam sistem tersebut. Beberapa protokol komunikasi standar dapat digunakan dalam pengembangan sistem keamanan kunci pintu gedung berbasis IoT seperti HTTPS dan MQTT.

- HTTPS

Hypertext Transfer Protocol Secure (HTTPS) adalah versi aman dari protokol jaringan internet yang paling umum, yaitu *Hypertext Transfer Protocol* (HTTP). HTTPS menggunakan enkripsi untuk mengamankan koneksi jaringan antara klien (seperti peramban *web*) dan *server*. Ini membuat komunikasi antara klien dan server tidak dapat diintip atau dimodifikasi oleh pihak ketiga yang tidak berwenang.

HTTPS biasanya digunakan untuk melakukan komunikasi jaringan yang membutuhkan keamanan tinggi, seperti transaksi finansial atau pertukaran informasi pribadi. HTTPS dapat digunakan pada berbagai jenis protokol

jaringan, termasuk *File Transfer Protocol* (FTP), *Simple Mail Transfer Protocol* (SMTP), dan *Instant Messaging Protocol* (IMAP).

Untuk menggunakan HTTPS, server harus memiliki sertifikat SSL (*Secure Sockets Layer*) atau TLS (*Transport Layer Security*). Sertifikat ini digunakan untuk memverifikasi identitas *server* dan mengamankan koneksi jaringan dengan enkripsi. Klien (seperti peramban *web*) kemudian dapat memverifikasi sertifikat tersebut untuk memastikan bahwa koneksi jaringan dengan *server* aman.

- MQTT

MQTT (*Message Queuing Telemetry Transport*) adalah protokol komunikasi yang digunakan untuk mentransfer data di internet terutama untuk sistem IoT. MQTT merupakan protokol yang sangat cepat dan efisien, karena tidak memerlukan banyak data *overhead*. Ini sangat penting untuk sistem keamanan kunci pintu gedung, karena harus responsif dan dapat membuka pintu secara cepat. MQTT memerlukan jumlah data yang sangat kecil untuk mentransfer pesan, sehingga sangat efisien dari segi penggunaan *bandwidth*. Akan tetapi, MQTT tidak menyediakan enkripsi secara *default*, sehingga harus menambahkan enkripsi tambahan untuk menjamin keamanan komunikasi data. Beberapa pilihan yang umum digunakan adalah enkripsi SSL/TLS (*Secure Sockets Layer/Transport Layer Security*) atau penggunaan MQTT-TLS (MQTT *over* TLS).

2) Modul Komunikasi

Sebuah modul komunikasi digunakan untuk menghubungkan sistem kunci pintu dengan jaringan komunikasi di luar. Penggunaan modul komunikasi disesuaikan dengan kemampuan perangkat serta metode penggunaan yang akan dipakai contohnya seperti WiFi dan *Bluetooth*.

- Wi-Fi

Wi-Fi adalah salah satu pilihan komunikasi yang umum digunakan untuk sistem berbasis IoT. Wi-Fi dapat menyediakan kecepatan yang cukup tinggi untuk mentransfer data, tergantung pada jenis dan kekuatan jaringan yang digunakan. Wi-Fi menyediakan enkripsi secara *default* dengan menggunakan WPA2 dan WPA3. Penggunaan jaringan Wi-Fi tidak

memerlukan biaya tambahan, kecuali jika menggunakan jaringan publik yang memerlukan pembayaran. Namun, perlu mempertimbangkan biaya perangkat yang diperlukan untuk terhubung ke jaringan Wi-Fi, seperti *router* atau *access point*.

- *Bluetooth*

Bluetooth merupakan modul komunikasi yang dapat digunakan dalam sistem IoT. Dalam sistem kunci pintu gedung berbasis IoT, diperlukan sebuah koneksi *peer-to-peer* antara perangkat kunci pintu dengan aplikasi pengguna sehingga penggunaan *bluetooth* sangat dimungkinkan dalam sistem kunci pintu ini. *Bluetooth* hanya dapat digunakan untuk mentransfer data dalam jarak yang terbatas. Ini cocok dengan kebutuhan dari sistem keamanan kunci pintu gedung untuk mendukung kinerjanya. *Bluetooth* juga menyediakan enkripsi secara *default* dengan menggunakan AES. Sehingga proses transmisi data dapat dilakukan dengan aman melalui proses enkripsi.

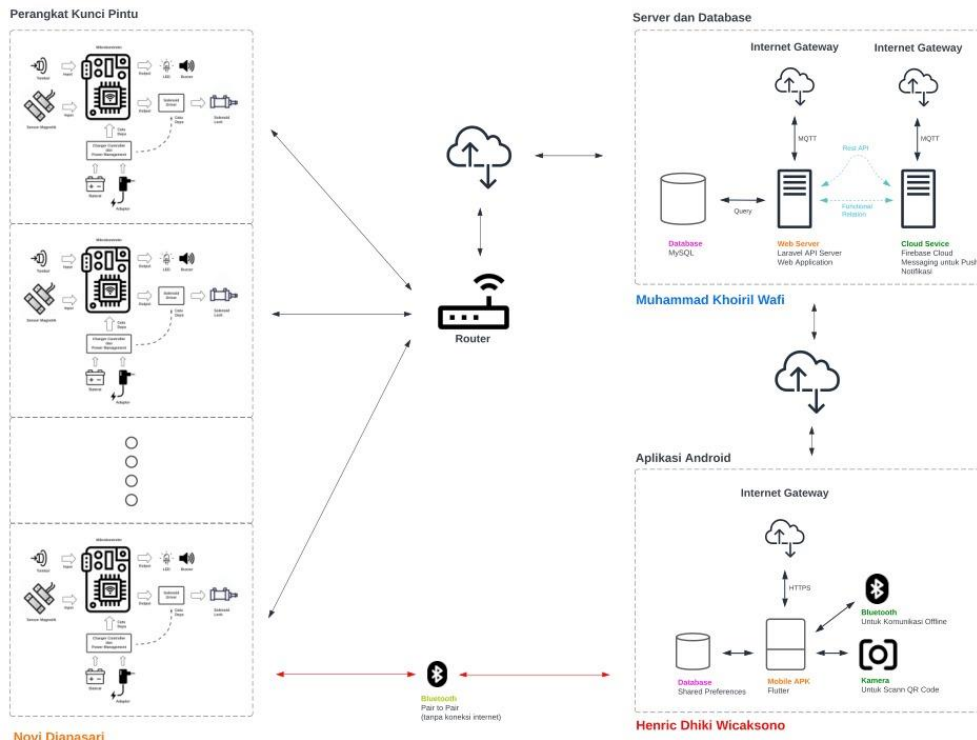
2.2 KONSEP DESAIN

2.2.1 Konfigurasi Umum

a. Bagian-Bagian Sistem Keamanan Kunci Pintu Gedung Berbasis IoT

Konfigurasi umum sistem keamanan kunci pintu gedung berbasis *Internet of Things* (IoT) terdiri dari beberapa komponen utama, yaitu perangkat kunci pintu, *internet gateway*, *server*, aplikasi *mobile* atau *web apps*.

Konfigurasi ini memungkinkan pihak yang berwenang (admin) untuk mengontrol dan mengakses kunci pintu gedung secara *remote* melalui perangkat yang terhubung ke internet. Selain itu, sistem ini juga memungkinkan pihak yang berwenang untuk mencatat dan mengelola data akses ke gedung secara elektronik. Adapun diagram bagian-bagian sistem keamanan kunci pintu gedung berbasis IoT dan pembagian tugas dapat dilihat pada Gambar 2.1.



Gambar 2.1 Diagram Bagian-Bagian Sistem Keamanan Kunci Pintu Gedung Berbasis IoT dan Pembagian Tugas

Berdasarkan Gambar 2.1 di atas, sistem keamanan kunci pintu gedung berbasis IoT mempunyai 4 bagian utama yaitu:

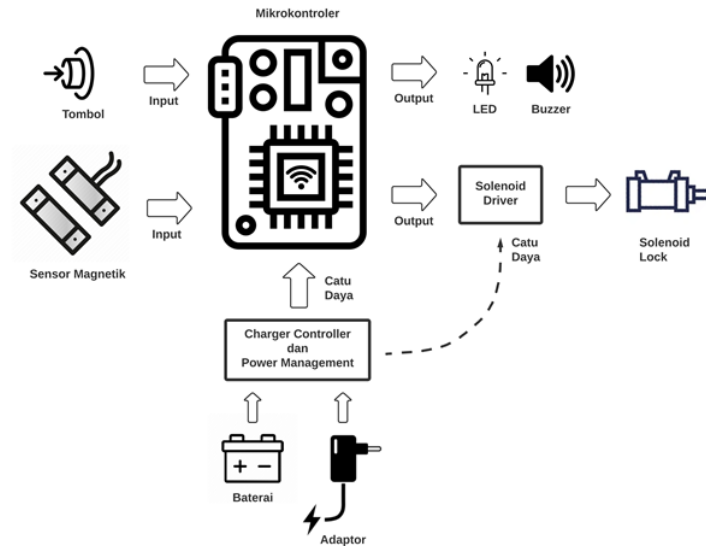
1) Perangkat Kunci Pintu

Kunci pintu yang dilengkapi dengan sensor saklar magnetik dan QR *code* yang dapat diakses melalui *smartphone* atau perangkat lain yang terhubung ke internet untuk *monitoring* dan *controlling* jarak jauh.

Perangkat kunci pintu akan terpasang pada setiap pintu dalam gedung dan akan terhubung ke *server* untuk membangun sebuah konektivitas IoT. Setiap perangkat kunci pintu dilengkapi dengan 2 modul komunikasi yaitu modul WiFi dan *Bluetooth* dengan menggunakan mikrokontroler ESP32.

Modul WiFi digunakan untuk menghubungkan perangkat kunci pintu dengan *server* utama, *server* utama akan mengirimkan perintah dan data ke perangkat kunci pintu seperti data pengguna yang diizinkan untuk membuka akses pintu tersebut, perintah penjadwalan serta perintah kontrol jarak jauh dari admin. Modul WiFi juga digunakan oleh perangkat kunci pintu untuk mengirimkan data riwayat pengguna yang mengakses pintu dan juga mengirimkan peringatan jika pintu terbuka secara tidak normal.

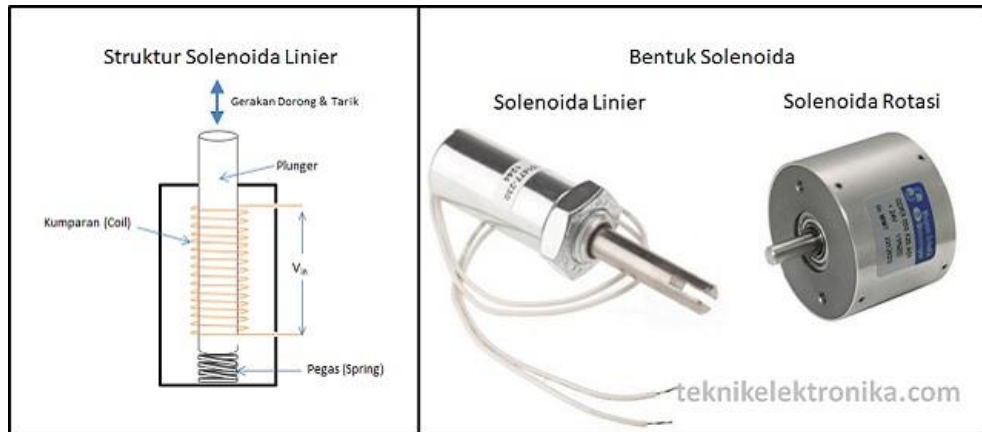
Modul *Bluetooth* digunakan untuk menghubungkan perangkat kunci pintu dengan aplikasi *mobile* pengguna secara *peer-to-peer*. Hal tersebut dimaksudkan untuk memastikan bahwa pengguna terhubung secara langsung dengan perangkat kunci pintu saat melakukan *scanning QR-Code* untuk membuka kunci pintu.



Gambar 2.2 Diagram Perangkat Kunci Pintu

Dapat dilihat pada Gambar 2.2 perangkat kunci pintu menggunakan solenoid. Solenoid adalah salah satu jenis komponen mekanik yang digunakan dalam sistem keamanan kunci pintu gedung berbasis IoT. Solenoid merupakan sebuah alat yang mengubah energi listrik menjadi energi mekanik.

Pada sistem keamanan kunci pintu gedung berbasis IoT, solenoid digunakan untuk mengontrol akses masuk ke dalam gedung dengan cara menarik atau menolak komponen mekanik yang digunakan untuk membuka atau menutup pintu. Solenoid terhubung dengan sensor magnetik yang digunakan untuk mengidentifikasi dan mengautentikasi pengguna. Untuk gambar struktur solenoida linier dapat dilihat pada Gambar 2.3.



Gambar 2.3 Struktur Solenoida Linier

Secara sains, solenoid seperti yang terlihat pada Gambar 2.3 menggunakan prinsip kerja magnet yaitu ketika arus listrik diberikan ke kumparan, kumparan tersebut akan menghasilkan medan magnet, medan magnet tersebut akan menarik *plunger* yang berada di dalam kumparan masuk ke pusat kumparan dan merapatkan atau mengompreskan pegas yang terdapat di satu ujung *plunger* tersebut. Gaya dan kecepatan *plunger* tergantung pada kekuatan fluks magnetik yang dihasilkan oleh kumparan. Saat arus listrik dimatikan, medan elektromagnetik yang terbentuk sebelumnya menghilang, sehingga energi yang tersimpan di pegas terkompresi mendorong piston kembali ke posisi semula. Secara matematis, solenoid dapat dihitung dengan menggunakan hukum *Faraday* yaitu:

$$\Phi = B \cdot A \cdot L = N \cdot I \cdot dt \quad (2.1)$$

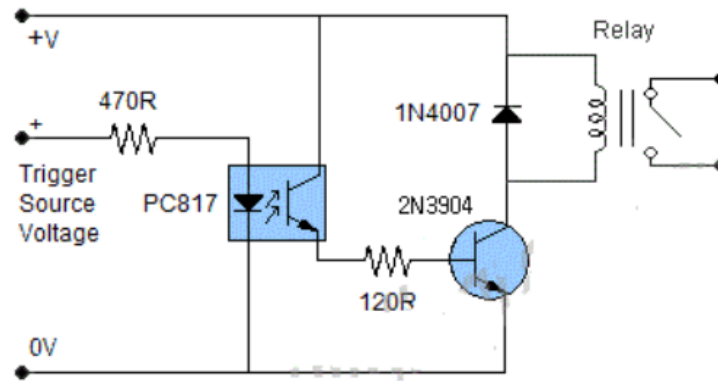
dimana Φ adalah fluks magnet, B adalah kuat medan magnet, A adalah luas penampang solenoid, L adalah panjang solenoid, N adalah jumlah lilitan, I adalah arus listrik, dan dt adalah waktu.

Pada *datasheet* solenoid bekerja pada tegangan 12volt dan mempunyai nilai resistansi 16 ohm, sehingga untuk dapat bekerja solenoid tersebut membutuhkan arus dari mikrokontroler sebesar:

$$I = \frac{V}{R} = \frac{12}{16} = 0.75 \text{ A atau } 750 \text{ mA} \quad (2.2)$$

Sedangkan mikrokontroler hanya dapat memberikan arus sebesar 250 mA, tentunya sangat kurang untuk menggerakkan solenoid. Oleh karena itu, perlu sebuah *driver* untuk menggerakkan solenoid tersebut.

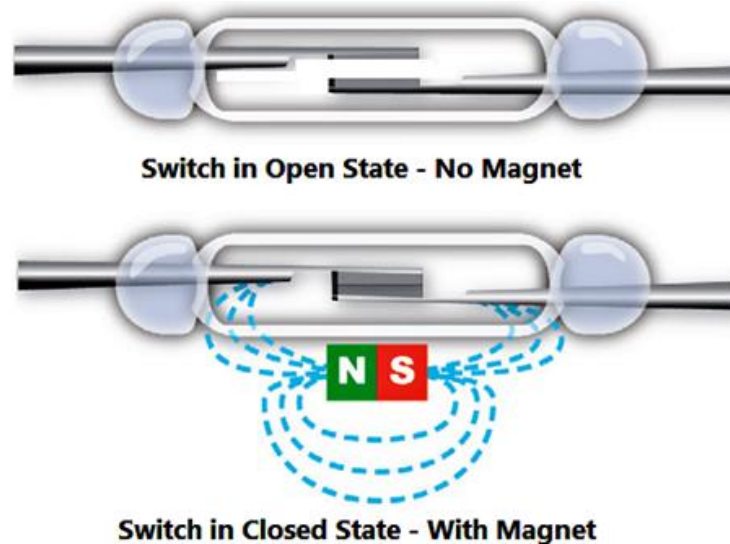
Pada Gambar 2.2 mikrokontroler yang digunakan adalah ESP32 untuk mengontrol sistem keamanan kunci pintu gedung berbasis IoT. Dalam sistem ini, ESP32 akan digunakan untuk mengontrol akses ke pintu dengan mengirimkan perintah ke sistem kunci pintu melalui koneksi internet.



Gambar 2.4 Rangkaian *Driver Solenoid*

Dengan menggunakan *driver solenoid* seperti yang terlihat pada Gambar 2.4 maka mikrokontroler hanya perlu menyalakan LED pada *optocoupler* PC817 dengan karakteristik $V_f = 1.2\text{volt}$ dan $I_f = 50\text{ mA}$. Sehingga arus yang dikeluarkan oleh mikrokontroler senilai 3.3volt 250mA sudah lebih dari cukup untuk menyalakan *optocoupler* tersebut.

Pada Gambar 2.2 juga terlihat bahwa perangkat kunci pintu menggunakan sebuah sensor magnetik. Sensor magnetik tersebut digunakan untuk mengetahui kondisi pintu sedang terbuka atau tertutup, sehingga selain untuk keperluan autentikasi juga dapat memberikan informasi kepada admin tentang kondisi pintu secara *realtime*. Untuk gambar prinsip kerja sensor *magnetic* dapat dilihat pada Gambar 2.5.



Gambar 2.5 Prinsip Kerja Sensor *Magnetic*

Secara sains, sensor *magnetic* ini pada dasarnya cara kerjanya sama dengan *reed switch* menggunakan prinsip kerja magnet. Saat satu bagian sensor *magnetic* terpasang pada pintu dan satu bagian lain pada bingkai pintu. Salah satu dari dua bagian tersebut memiliki magnet sementara yang lainnya memiliki *reed switch* yang menutup saat berada di dekat magnet. Ketika kedua bagian tersebut terpisah, maka medan magnet akan kehilangan kekuatannya, dan rangkaian akan terputus[4]. Sensor *magnetic* ini bersifat *normally open*. Jadi, ketika pintu tertutup, maka arus mengalir melalui *switch*, ketika pintu terbuka, maka arus akan terputus[4].

Secara matematis, sensor magnetik menggunakan hukum gaya magnet yang dijelaskan oleh hukum *Coulomb* yaitu:

$$F = k(Q_1Q_2)/r^2 \quad (2.3)$$

dimana F adalah gaya magnet, k adalah konstanta gaya magnet, Q_1 dan Q_2 adalah muatan listrik, dan r adalah jarak antara kedua muatan listrik.

2) *Internet Gateway*

Internet gateway atau perangkat yang terhubung ke jaringan internet dan ke kunci pintu gedung. *Internet gateway* ini berfungsi sebagai perantara antara kunci pintu gedung dengan jaringan internet. Dalam sistem ini, *internet gateway* digunakan untuk mengirimkan dan menerima perintah dari ESP32 ke sistem kunci pintu melalui koneksi internet.

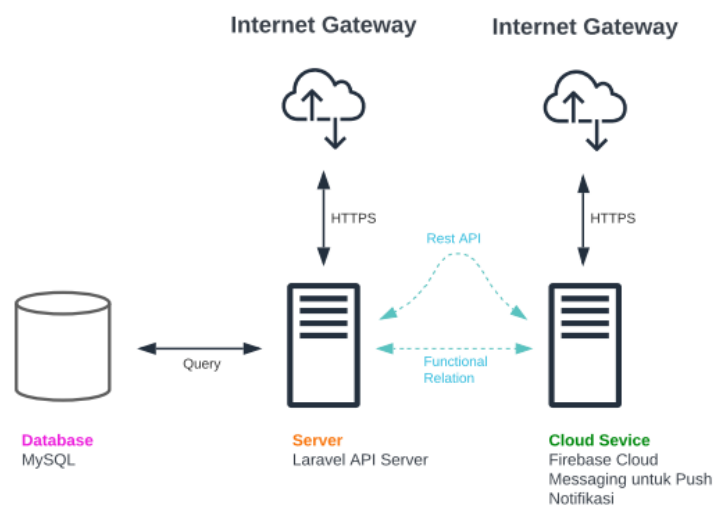
Sains dasar yang digunakan dalam *internet gateway* meliputi komunikasi dan jaringan komputer, yang digunakan untuk mengirimkan dan menerima data

melalui koneksi internet. Matematika dasar yang digunakan meliputi algoritma jaringan, yang digunakan untuk mengatur aliran data dan menjamin kualitas koneksi.

Internet gateway harus dapat menangani trafik data yang tinggi dan memiliki kemampuan enkripsi data yang kuat, untuk menjamin keamanan data yang dikirimkan dan diterima. Selain itu, *internet gateway* harus kompatibel dengan perangkat keras yang digunakan dalam sistem dan dapat diintegrasikan dengan sistem keamanan kunci pintu gedung yang ada.

3) *Server dan Database*

Server atau perangkat yang digunakan untuk menyimpan dan mengelola data akses ke gedung. *Server* ini terhubung ke jaringan internet dan dapat diakses oleh pihak yang berwenang melalui aplikasi *smartphone* atau perangkat lain yang terhubung ke internet. Setiap perangkat kunci pintu akan terhubung ke sebuah *server*. *Server* akan mengatur kinerja dari perangkat kunci pintu dan mencatat setiap aktivitas pengguna di dalam sebuah *database*. Diagram dari *server* dan *database* yang digunakan pada sistem kunci pintu dapat dilihat pada Gambar 2.6.



Gambar 2.6 Diagram *Server* dan *Database*

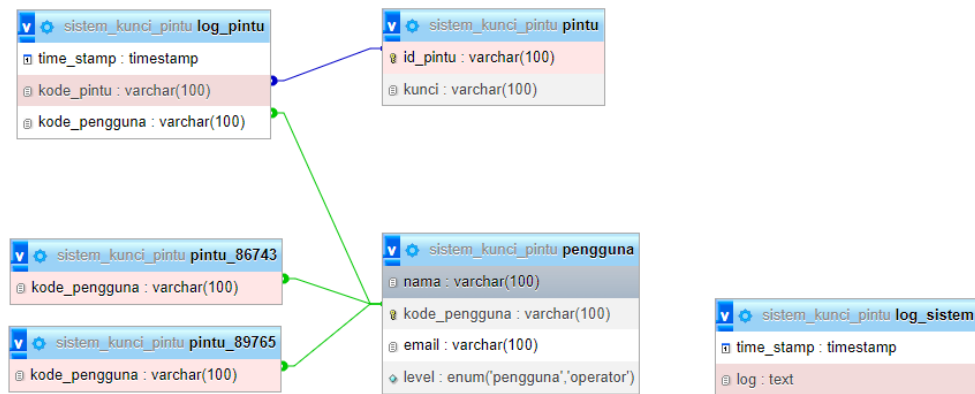
Dengan berbagai macam operasi yang dilakukan pengguna maupun admin seperti *login*, *management* pengguna, *management* perangkat kunci pintu, pencatatan riwayat atau *log*, *monitoring* dan lain sebagainya maka diperlukan sebuah *server* yang mendukung operasi tersebut.

Jika menggunakan protokol standar IoT saja yaitu dengan menggunakan metode *publish* dan *subscribe* maka tidak akan mengakomodasi semua operasi tersebut. Oleh karena itu, pada pengembangan sistem keamanan kunci pintu gedung berbasis IoT ini menggunakan sebuah *server* API yang berjalan pada sebuah *cloud hosting*.

Dengan adanya kebutuhan penyimpanan data yang terstruktur baik itu berupa akun pengguna, daftar perangkat kunci pintu dalam satu sistem, daftar pengguna yang memiliki akses pada kunci pintu tertentu, dan lain sebagainya maka diperlukan sebuah sistem *database* yang dapat memudahkan pengolahan data tersebut. Sistem *database* yang paling sesuai yaitu dengan menggunakan MySQL yang dikombinasikan menggunakan Laravel API *server* dengan kelebihan masing-masing sudah dijelaskan pada bagian alternatif desain.

Pada Gambar 2.6 juga terlihat bahwa *server* terhubung dengan *cloud service* yaitu *Firebase Cloud Messaging* atau FCM. FCM digunakan untuk melakukan *push notification* baik ke admin jika terjadi penerobosan di pintu gedung maupun ke pengguna jika ada informasi yang harus dikirimkan oleh *server* ke *client*. Penggunaan FCM memudahkan dan meringankan beban kinerja dari aplikasi dan *server* karena *server* dan *client* tidak harus terhubung secara terus-menerus.

Sebuah *database* digunakan untuk menyimpan data yang diperlukan untuk keseluruhan sistem keamanan kunci pintu gedung berbasis IoT. Skema *database* yang digunakan pada sistem ini dapat dilihat pada Gambar 2.7.



Gambar 2.7 Skema Database Sistem Keamanan Kunci Pintu Gedung Berbasis IoT

Dapat dilihat pada Gambar 2.7, terdapat tabel pengguna yang digunakan untuk menyimpan data *user* baik itu untuk pengguna maupun admin yang berwenang seperti nama, kode_pengguna, email, dan level dengan penjelasan seperti pada tabel 2.1.

Tabel 2.1 Tabel Pengguna

No	Nama	Tipe	Keterangan
1	Nama	varchar(100)	Menyimpan nama pengguna
2	Kode_pengguna	varchar(100)	Menyimpan kode atau ID pengguna
3	Email	varchar(100)	Menyimpan email pengguna untuk verifikasi 2 langkah
4	Level	enum(pengguna,operator)	Menyimpan level pengguna

Pada Gambar 2.7 juga terdapat tabel pintu, tabel pintu digunakan untuk menyimpan daftar pintu yang terdapat dalam satu sistem dengan isi yaitu id_pintu dan kunci dengan penjelasan seperti pada Tabel 2.2.

Tabel 2.2 Tabel Pintu

No	Nama	Tipe	Keterangan
1	Id_pintu	varchar(100)	Menyimpan ID dari

			pintu
			Untuk menyimpan
2	Kunci	varchar(100)	kunci yang valid
			untuk membuka kunci
			pintu

Pada Gambar 2.7 juga terdapat tabel pintu_xxxxx, tabel ini merupakan tabel yang dibuat oleh *server* secara otomatis sesuai dengan pintu yang ada. Tabel ini akan menyimpan daftar pengguna yang memiliki akses terhadap pintu tersebut dengan penjelasan seperti pada Tabel 2.3.

Tabel 2.3 Tabel Pintu_xxxx

No	Nama	Tipe	Keterangan
1	Kode_pengguna	varchar(100)	Kode pengguna yang mempunyai akses ke pintu

Pada Gambar 2.7 juga terdapat tabel log_pintu, tabel ini digunakan untuk menyimpan data riwayat akses pengguna pada setiap pintu dengan penjelasan seperti pada Tabel 2.4.

Tabel 2.4 Tabel Log_pintu

No	Nama	Tipe	Keterangan
1	Time_stamp	Timestamp	Menyimpan waktu akses sistem
2	Kode_pintu	varchar(100)	Menyimpan kode pintu yang diakses
3	Kode_pengguna	varchar(100)	Menyimpan kode pengguna yang mengakses pintu tersebut

Pada Gambar 2.7 juga terdapat tabel *log_sistem*, tabel *log_sistem* digunakan untuk menyimpan riwayat aktivitas dari sistem dengan penjelasan seperti pada Tabel 2.5.

Tabel 2.5 Tabel Pintu

No	Nama	Tipe	Keterangan
1	Time_stamp	Timestamp	Menyimpan waktu akses sistem
2	Log	Text	Menyimpan teks riwayat aktivitas sistem

Sains dasar yang digunakan dalam *server* dan *database* meliputi jaringan komputer dan basis data, yang digunakan untuk menyimpan dan mengelola data. Matematika dasar yang digunakan meliputi algoritma pengelolaan data, yang digunakan untuk mengelola dan mengambil keputusan dari data yang tersimpan.

Server dan *database* harus dapat menangani jumlah data yang besar dan memiliki kemampuan enkripsi data yang kuat, untuk menjamin keamanan data yang disimpan. Selain itu, *server* dan *database* harus dapat diakses secara *remote* oleh ESP32 dan *internet gateway* untuk memungkinkan akses ke data dari mana saja. *Server* dan *database* juga harus dapat diintegrasikan dengan sistem keamanan kunci pintu gedung yang ada dan diuji secara berkala untuk memastikan bahwa sistem kerja dengan baik dan stabil.

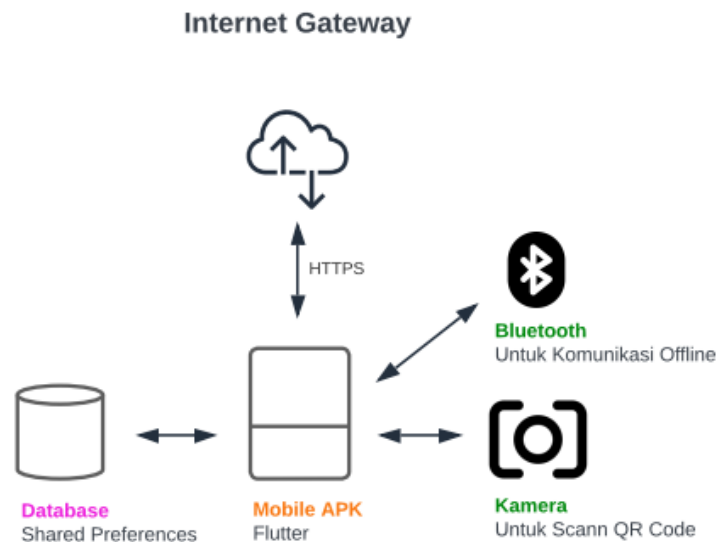
4) Aplikasi *Mobile* atau *Web Apps*

Sebuah aplikasi *mobile* dan aplikasi *web* diperlukan untuk mendukung kinerja dari sistem keamanan kunci pintu gedung yaitu digunakan untuk mengontrol dan mengakses kunci pintu gedung.

Aplikasi *mobile* ini digunakan oleh pengguna untuk membuka kunci pintu dengan cara memindai QR-Code yang ada pada pintu. Di mana aplikasi *mobile* ini dapat digunakan pada *smartphone* Android dan iOS.

Aplikasi *web* digunakan oleh admin untuk mengatur kinerja dari sistem keamanan kunci pintu gedung, seperti menambahkan pengguna baru, membuat undangan pengguna sementara, membuka kunci dari jarak jauh, mengatur

jadwal penguncian, dan lain sebagainya. Diagram dari aplikasi *mobile* dapat dilihat pada Gambar 2.8.

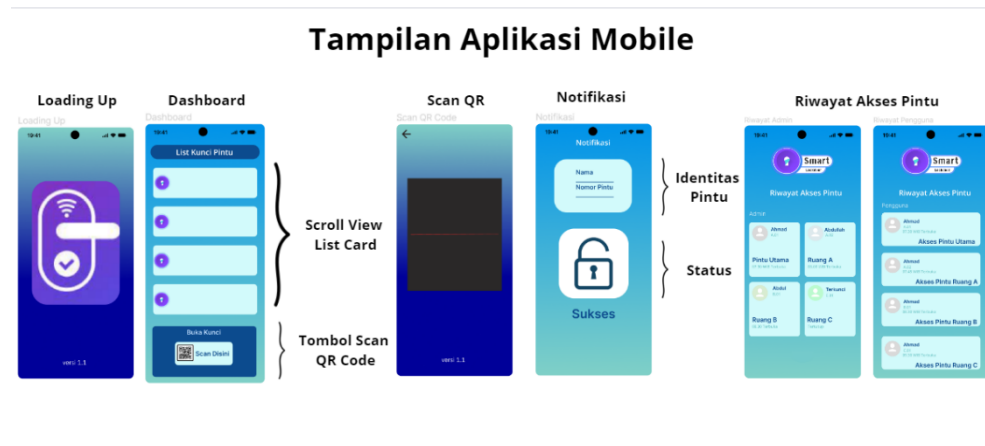


Gambar 2.8 Diagram Aplikasi *Mobile*

Terlihat pada Gambar 2.8 pada aplikasi *mobile* menggunakan kamera untuk memindai QR-Code pada pintu dan mengirimkan kode autentikasi melalui *bluetooth* untuk komunikasi *peer-to-peer* dalam membuka pintu. Alasan penggunaan *bluetooth* supaya lebih cepat atau tidak terkendala dengan kondisi WiFi, serta hanya untuk memastikan antara *device* yang digunakan dengan perangkat kunci pintu dalam kondisi baik. Jadi, *bluetooth* digunakan oleh pengguna untuk komunikasi *peer-to-peer* dengan menggunakan aplikasi *mobile* (Android atau iOS) dalam membuka pintu.

Selain itu, pada sistem ini internet (WiFi) tetap dibutuhkan untuk kebutuhan kontrol jarak jauh, pencatatan *log* aksesnya, juga untuk berkomunikasi secara *real-time* dengan *server* sebagai *command center*. Jadi, WiFi digunakan oleh admin untuk *monitoring* dan *controlling* (pengelolaan akses gedung secara penuh) dengan menggunakan *website* karena tampilannya lebih lengkap.

Adapun tampilan aplikasi *mobile* (Android dan iOS) pengguna dapat dilihat pada Gambar 2.9 berikut.

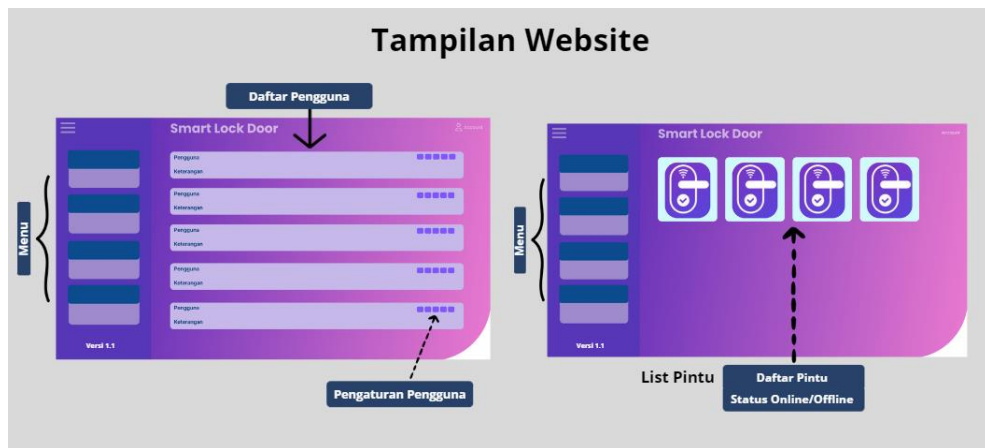


Gambar 2.9 Tampilan Aplikasi *Mobile*

Berdasarkan pada Gambar 2.9 di atas, fitur-fitur yang terdapat pada aplikasi *mobile* sistem keamanan kunci pintu gedung berbasis IoT (*Internet of Things*) ini adalah sebagai berikut:

- Autentikasi pengguna: Fitur ini memungkinkan pengguna untuk masuk ke aplikasi dengan menggunakan kredensial seperti nama pengguna dan kata sandi.
- Tampilan daftar pintu: Fitur ini menampilkan daftar pintu yang terhubung ke sistem keamanan kunci pintu gedung yang dapat diakses oleh pengguna.
- Tombol scan QR code: Setiap pintu dalam daftar harus memiliki tombol *scan QR code* yang dapat digunakan oleh pengguna untuk membuka pintu tersebut.
- Riwayat akses: Fitur ini mencatat riwayat akses pintu oleh pengguna dan waktu di mana pintu dibuka atau ditutup.
- Notifikasi: Fitur ini memberi notifikasi kepada pengguna ketika ada aktivitas yang terdeteksi di pintu yang terhubung ke sistem.

Adapun tampilan untuk *website* admin dapat dilihat pada Gambar 2.10 berikut.



Gambar 2.10 Tampilan *Website*

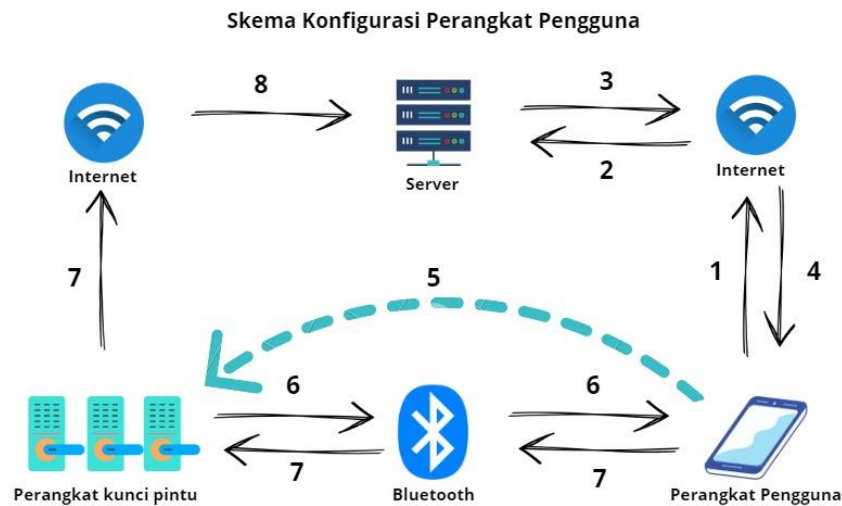
Berdasarkan pada Gambar 2.10 di atas, tampilan *website* admin pada sistem keamanan kunci pintu gedung berbasis IoT (*Internet of Things*) terdiri dari beberapa fitur utama, seperti:

- **Dashboard:** Halaman utama yang menampilkan statistik penting seperti jumlah kunci yang terhubung, jumlah akses masuk/keluar yang tercatat, dan sebagainya.
- **Manajemen Kunci:** Fitur yang memungkinkan admin menambah, mengedit, atau menghapus kunci yang terhubung ke sistem.
- **Manajemen Pengguna:** Fitur yang memungkinkan admin menambah, mengedit, atau menghapus pengguna yang terdaftar dalam sistem, serta memberikan akses kepada pengguna terhadap kunci yang terhubung.
- **Laporan Akses:** Fitur yang menampilkan riwayat akses masuk/keluar untuk setiap kunci yang terhubung, termasuk informasi tanggal, waktu, dan pengguna yang terlibat.
- **Pengaturan Sistem:** Fitur yang memungkinkan admin mengatur pengaturan sistem seperti koneksi jaringan, notifikasi email, dan sebagainya.

Secara umum, tampilan *website* admin pada sistem keamanan kunci pintu gedung berbasis IoT harus mudah digunakan dan memungkinkan admin untuk mengelola sistem dengan efisien.

b. Skema Konfigurasi Perangkat Pengguna

Adapun skema konfigurasi perangkat pengguna dapat dilihat pada Gambar 2.11.



Gambar 2.11 Skema Konfigurasi Perangkat Pengguna

Berdasarkan pada Gambar 2.11 di atas, skema konfigurasi perangkat pengguna sebagai berikut ini.

- 1) Pengguna membuka aplikasi dan aplikasi melakukan *request* kunci pintu ke *server* melalui internet.
- 2) *Server* menerima *request*.
- 3) *Server* mengirim *list* kunci pintu yang dapat diakses oleh pengguna.
- 4) Aplikasi pengguna menerima *list* kunci pintu.
- 5) Aplikasi memindai QR Code.
- 6) Aplikasi membuat koneksi ke perangkat kunci pintu dan mengirimkan kunci pintu ke *Bluetooth* (Data dari *list* kunci pintu yang diambil dari *server*).
- 7) Perangkat kunci pintu memberikan respon autentikasi berhasil/gagal.

c. Penggunaan QR-Code untuk membuka kunci pintu

QR code (*Quick Response code*) adalah jenis kode matriks yang digunakan untuk menyimpan dan memindai informasi secara cepat. Penggunaan QR code untuk membuka kunci pintu diperlukan sistem yang telah terintegrasi dengan pemindai QR code dan dapat mengontrol kunci pintu secara otomatis. Sistem ini dapat dibuat dengan menggunakan perangkat keras dan perangkat lunak yang tersedia

secara komersial atau dibuat sendiri dengan menggunakan perangkat keras dan perangkat lunak yang tersedia secara bebas.

Untuk penggunaannya nantinya pada setiap pintu akan terpasang sebuah QR-Code yang menjadi identitas dari pintu. QR-Code pada pintu bersifat statis dan hanya menyimpan ID dari pintu. QR-Code dibuat oleh *server* secara acak dan unik pada saat perangkat kunci pintu pertama kali didaftarkan ke dalam sistem. Untuk bisa membuka kunci pintu maka pengguna memerlukan kunci (*key*) dan kredensial *bluetooth*. Dengan cara setiap pengguna memindai QR-Code menggunakan aplikasi kunci pintu, maka aplikasi akan mengecek data pada penyimpanan lokal aplikasi untuk mendapatkan kunci (*key*) dari pintu beserta kredensial *bluetooth* yang akan menghubungkan aplikasi pengguna dengan perangkat kunci pintu. Data tersebut disimpan di *server* dan akan dikirimkan ke aplikasi pengguna pada saat pengguna melakukan *login* ke aplikasi. Jika informasi yang tersimpan dalam QR code cocok dengan yang terdaftar di sistem, maka kunci pintu akan terbuka. Jika informasi yang tersimpan dalam QR code tidak cocok dengan yang terdaftar di sistem, maka kunci pintu tidak akan terbuka. Sehingga dari sistem yang sudah dijelaskan, meskipun orang mempunyai QR-Code atau memindai QR-Code menggunakan aplikasi lain, maka orang tersebut tidak akan bisa membuka kunci pintu dan hanya mendapatkan data acak.

QR code dapat digunakan untuk membuka kunci pintu dengan mengikuti beberapa langkah-langkah pada Gambar 2.12 berikut:



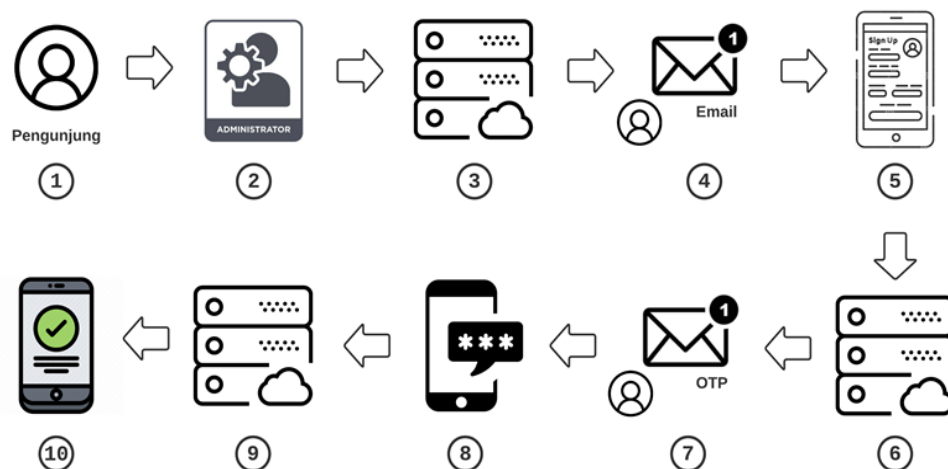
Gambar 2.12 Membuka Kunci Menggunakan QR-Code

- 1) Pengguna memindai QR-Code pada pintu menggunakan aplikasi *mobile* sehingga mendapatkan ID dari pintu.
- 2) Selanjutnya, aplikasi akan mengecek data pada penyimpanan lokal aplikasi.

- 3) Jika data ditemukan, maka aplikasi akan menghubungkan *smartphone* pengguna ke *bluetooth* sesuai dengan data yang ditemukan.
- 4) Kemudian, melalui *bluetooth* aplikasi mengirimkan *username* dan *password* pengguna yang tersimpan di aplikasi untuk membuka kunci pintu.
- 5) Jika berhasil, maka pada aplikasi akan tampil notifikasi berhasil.

d. Pendaftaran pengguna baru

Untuk pengguna yang belum mempunyai akun untuk mengakses kunci pintu, pengguna dapat mengajukan pembuatan akun ke admin dengan mengikuti langkah-langkah sesuai dengan Gambar 2.13 berikut ini.



Gambar 2.13 Pendaftaran Pengguna Baru

- 1) Pengguna baru atau pengunjung menghubungi admin dengan keperluan untuk membuat akun baru dengan mengirimkan identitas yang valid.
- 2) Admin akan memasukkan identitas pengguna ke *server*.
- 3) *Server* akan mengolah data tersebut serta menyesuaikan pengaturan level akses ke perangkat kunci pintu.
- 4) Kemudian, *server* akan menerbitkan undangan yang dikirimkan ke email pengguna.
- 5) Selanjutnya, pengguna melakukan pendaftaran melalui aplikasi yang telah disediakan.

- 6) Kemudian, *server* akan mengecek pendaftaran dan mengirimkan kode OTP untuk autentikasi 2 langkah.
- 7) Pengguna menerima kode OTP melalui email yang sudah terdaftar di *server*.
- 8) Pengguna memasukkan kode OTP ke aplikasi dan mengirimkannya ke *server*.
- 9) *Server* akan mengecek kode OTP.
- 10) Jika berhasil, maka di aplikasi akan tampil notifikasi berhasil.

Langkah-langkah tersebut juga berlaku untuk proses *login* pegawai, tetapi untuk langkah-langkah nomor 1 sampai 4 dilewati dan pada langkah ke 5 pegawai memasukkan *username* dan *password* masing-masing. Pada langkah ke 7, *server* akan membuat sebuah kode OTP yang digunakan untuk verifikasi 2 langkah. Kode OTP sendiri dibuat dengan menggunakan *timestamp* dan kunci rahasia di dalam *server* dengan langkah-langkah sebagai berikut:

- 1) *Server* membuat kunci rahasia, misalnya “ADMIN”.
- 2) Kemudian, *server* mengambil *timestamp*, misalnya “89764765547753”.
- 3) Data tersebut kemudian digabungkan menjadi “ADMIN89764765547753”.
- 4) Dari data di atas, maka dilakukan proses *hashing* menggunakan SHA-256 sehingga menghasilkan kode berikut:
“7b84e61e82892f34c0587d87afb3c9b3f1dbd55e50a30a64b6c64a70a0f44a87”
- 5) Dari *hash* tersebut diambil 5byte pertama sehingga menghasilkan kode berikut:
“7b84e61e82”
- 6) Selanjutnya, *hash* tersebut diubah ke dalam nilai desimal untuk setiap *byte*-nya menggunakan rumus:

$$desimal = (d_1 \times 16^1) + (d_0 \times 16^0) \quad (2.4)$$

Dimana:

d: digit

n: jumlah digit

r: posisi digit

sehingga menghasilkan nilai 711481461482

- 7) Selanjutnya, nilai desimal tersebut dipotong sesuai dengan kebutuhan kode OTP dengan menggunakan rumus berikut:

$$kode_{otp} = D \% (10^n) \quad (2.5)$$

Dimana:

d: nilai desimal

n: jumlah digit yang diperlukan

8) Misalkan kita menginginkan 6digit kode OTP maka:

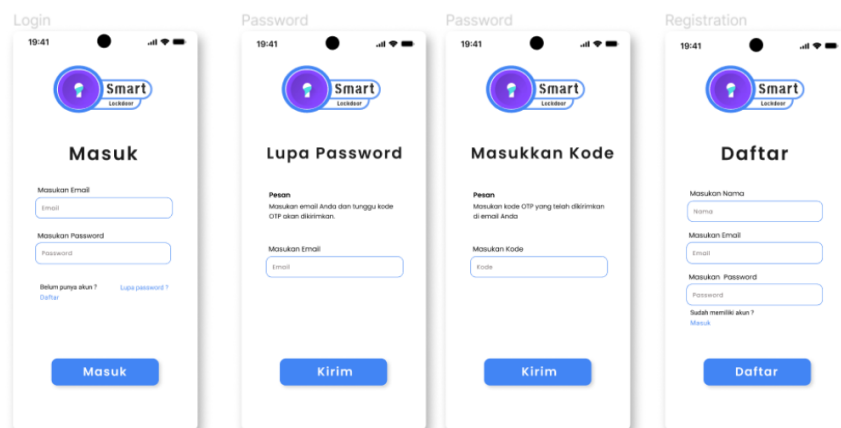
$$kode_{otp} = 711481461482 \% (10^6)$$

$$kode_{otp} = 711481461482 \% 1000000$$

$$kode_{otp} = 461482$$

Adapun untuk tampilan halaman *login* pengguna di aplikasi *mobile* ketika pertama kali *login* dapat dilihat pada Gambar 2.14 di bawah ini.

Halaman Login Pengguna



Gambar 2.14 Halaman *login* pengguna

Berdasarkan pada Gambar 2.14 pada tampilan halaman *login* pengguna pertama kali di aplikasi *mobile* sistem keamanan kunci pintu gedung berbasis IoT, terdapat beberapa elemen yang biasa terdapat pada halaman *login*. Elemen-elemen tersebut diantaranya:

- *Form login/masuk*: merupakan bagian yang digunakan untuk memasukkan informasi *login* seperti *username* dan *password*.
- Tombol *login/masuk*: merupakan tombol yang digunakan untuk memproses *login* dengan mengirimkan informasi *login* yang telah dimasukkan ke *server*.

- *Link lupa password*: merupakan *link* yang mengarah ke halaman untuk mengatur ulang *password* jika pengguna lupa *password*-nya.
- *Link daftar*: merupakan *link* yang mengarah ke halaman daftar jika pengguna belum memiliki akun.
- Tampilan logo aplikasi: merupakan tampilan logo aplikasi yang menunjukkan bahwa ini adalah halaman *login* aplikasi sistem keamanan kunci pintu gedung berbasis IoT.

2.2.2 Kemampuan dan Kapasitas Produk

Sistem keamanan kunci pintu gedung berbasis *Internet of Things* (IoT) memiliki beberapa kemampuan dan kapasitas yang dapat memberikan keamanan tambahan bagi gedung. Berikut ini beberapa kemampuan dan kapasitas sistem keamanan kunci pintu gedung berbasis IoT:

1) Kendali Jarak Jauh

Proses pengaturan kunci pintu (*lock* dan *unlock*) dapat dilakukan dari jarak jauh. Pengendalian dilakukan dengan menggunakan *website*. Kendali jarak jauh hanya bisa dilakukan oleh admin yang memiliki akses penuh atas sistem kunci pintu IoT. Jadi, salah satu keuntungan utama dari desain sistem keamanan kunci pintu gedung berbasis IoT adalah kemampuan untuk mengontrol akses ke gedung secara *remote*. Dengan sistem ini, pihak yang berwenang (admin) dapat mengakses kunci pintu gedung melalui perangkat yang terhubung ke internet, seperti *smartphone* atau komputer, dan mengontrol akses ke gedung dari jarak jauh.

Ini memungkinkan pihak yang berwenang untuk memberikan atau mencabut akses ke gedung tanpa harus berada di lokasi gedung secara fisik. Ini bisa sangat bermanfaat dalam situasi di mana pihak yang berwenang tidak bisa datang ke gedung secara fisik, misalnya karena sedang berada di luar kota atau di luar negeri.

Selain itu, dengan mengontrol akses ke gedung secara *remote*, pihak yang berwenang juga dapat memantau aktivitas akses ke gedung secara *real-time* dan membuat laporan atas aktivitas tersebut. Ini memudahkan pengelolaan akses ke gedung dan membantu menjamin keamanan gedung.

2) *History* akses

Salah satu keuntungan menggunakan desain sistem keamanan kunci pintu gedung berbasis IoT adalah kemampuan untuk mencatat aktivitas akses ke gedung. Dengan sistem ini, setiap kali seseorang masuk atau keluar dari gedung, aktivitas tersebut akan tercatat dalam sistem dan dapat diakses oleh pihak yang berwenang. Ini memungkinkan pihak yang berwenang untuk memantau aktivitas akses ke gedung dan membuat laporan atas aktivitas tersebut.

Informasi yang biasanya dicatat dalam sistem keamanan kunci pintu gedung berbasis IoT termasuk tanggal dan waktu akses, informasi tentang orang yang melakukan akses (seperti nama atau nomor identitas), dan informasi tentang pintu yang diakses. Informasi ini dapat bermanfaat untuk menganalisis pola akses ke gedung atau untuk membantu menyelidiki kejadian yang mungkin terjadi di gedung.

3) Kemudahan pengelolaan akses ke gedung

Desain sistem keamanan kunci pintu gedung berbasis IoT juga dapat memudahkan pengelolaan akses ke gedung. Dengan sistem ini, pihak yang berwenang dapat dengan mudah menambah atau menghapus akses ke gedung untuk individu tertentu. Misalnya, jika seseorang hendak memasuki gedung untuk pertama kalinya, pihak yang berwenang dapat dengan mudah menambahkan akses untuk orang tersebut ke dalam sistem. Begitu juga, jika seseorang tidak lagi memerlukan akses ke gedung, pihak yang berwenang dapat dengan mudah menghapus akses untuk orang tersebut dari sistem. Ini memudahkan pengelolaan akses ke gedung karena pihak yang berwenang tidak perlu mengeluarkan atau mengganti kunci fisik setiap kali ada perubahan dalam akses ke gedung.

4) Pengawasan

Setiap perangkat penguncian pintu akan mengawasi kondisi pintu setiap saat. Jika pintu terbuka secara tidak normal, maka sistem akan memberikan notifikasi peringatan bahwa ada pintu yang terbuka dan dimungkinkan adanya indikasi penerobosan. Jadi, sistem ini dapat memantau aktivitas pintu secara *real-time* serta memberikan notifikasi kepada pengguna jika terjadi aktivitas yang tidak diinginkan di pintu.

5) Penjadwalan

Sistem yang dibuat memungkinkan admin mengatur dan menetapkan jadwal *lock* dan *unlock* pada setiap pintu. Hal tersebut akan memudahkan jika sistem penguncian ini dipasang pada ruangan umum seperti ruang kelas atau gedung perkuliahan yang mempunyai pintu yang harus dibuka dan ditutup secara periodik.

6) Undangan

Admin dapat membuat undangan untuk memberikan akses ke pengguna. Setiap pengguna akan mendaftar pada sistem dengan menggunakan *link* yang sudah dibagikan.

7) Pengaturan Hak Akses

Admin juga dapat mengatur level akses dari setiap pengguna yang terdaftar sehingga hak akses dari setiap pengguna dapat disesuaikan dengan kondisi dan kebutuhan yang ada.

8) Kartu Pengunjung

Selain dapat mengendalikan pintu dari jarak jauh, admin juga dapat memberikan kartu pengunjung (berupa URL dan kode akses) yang dapat digunakan oleh pengunjung untuk mendapatkan akses pada pintu tertentu. Akses ini bersifat sementara dan hanya valid pada periode waktu tertentu.

9) *Unlock* Cepat

Di setiap pintu yang telah terpasang perangkat penguncian akan ditandai dengan *QR-code*. Setiap pengguna (admin, pengguna, dan pengunjung) dapat memindai *QR-code* tersebut untuk membuka pintu secara cepat dan aman.

10) Keamanan

Keamanan menjadi fokus utama dalam mengerjakan proyek ini, setiap pengguna memiliki *username* dan *password* serta *email* sebagai identitas pengguna. Pengguna akan diminta melakukan *login* pada saat pertama kali meng-*install* aplikasi serta memasukkan kode autentikasi yang dikirim melalui *email* (autentikasi 2 arah). Setiap aktivitas yang dilakukan oleh pengguna akan tercatat di *database* sebagai *log* aktivitas.

2.2.3 Dasar Teori yang Mendukung Proses Pengembangan

a. Saklar Magnetik/ *Magnetic Switch*

Magnetic Switch/ Door Sensor merupakan saklar yang dapat merespon medan magnet yang berada di sekitarnya. *Magnetic switch* ini seperti sensor *limit switch* dengan tambahan pelat logam yang dapat bereaksi dengan adanya magnet. *Magnetic Switch* biasa digunakan untuk pengamanan pada pintu dan jendela[5]. *Switch* ini di dalamnya terdapat dua buah lempengan logam yang terbuat dari nikel dan besi, dimana secara keadaan elektromagnetik *door sensor* ini adalah *normally open*. Ketika magnet diletakkan di dekat *Electromagnetic door sensor* maka dua lempengan logam akan menempel dan *switch* ini akan tersambung sehingga keadaannya adalah *normally closed*. Ketika magnet dijatuhkan dari *switch* ini, maka *reed switch* akan kembali ke posisi semula yaitu *normally open*. Adapun gambar dari *Magnetic Switch* dapat dilihat pada gambar 2.15 di bawah ini.



Gambar 2.15 *Magnetic Switch/ Door Sensor*

Saklar magnetik dapat digunakan dalam sistem keamanan kunci pintu gedung berbasis *internet of things* (IoT) dengan cara memasang saklar magnetik pada pintu gedung dan menghubungkannya ke sistem keamanan yang terhubung ke internet. Saat pintu dibuka, medan magnet akan terputus dan sistem keamanan akan memberikan notifikasi kepada pemilik gedung atau petugas keamanan

melalui aplikasi. Dengan demikian, saklar magnetik dapat digunakan sebagai tambahan keamanan untuk mencegah akses pintu gedung yang tidak sah.

Selain itu, saklar magnetik juga dapat digunakan untuk memantau keadaan pintu gedung secara *real-time*. Saat pintu terbuka, sistem keamanan dapat memberikan notifikasi kepada pemilik gedung atau petugas keamanan, sehingga dapat segera diambil tindakan jika terjadi keadaan yang tidak diinginkan. Dengan demikian, saklar magnetik dapat meningkatkan tingkat keamanan gedung dan memberikan kemudahan bagi pemilik gedung untuk memantau keadaan gedung secara *real-time*.

b. Solenoid Door Lock

Solenoid door lock merupakan alat elektromekanik yang berfungsi sebagai pengunci pintu otomatis[6]. Dalam kondisi normal *solenoid door lock* dalam posisi terkunci jika diberi tegangan maka *solenoid door lock* akan terbuka[6]. Tegangan yang dibutuhkan untuk menjalankan perangkat ini sebesar 12vdc, di dalamnya terdapat *coil* kawat tembaga[6]. Jika kawat tembaga dialiri arus listrik maka akan terjadi medan magnet untuk menghasilkan gaya magnet yang akan menarik inti besi kedalam[6]. *Solenoid door lock* ini dapat dihubungkan ke arduino untuk kunci pintu otomatis[6].

Tampilan *Solenoid door lock* dapat dilihat pada gambar 2.16 di bawah ini.



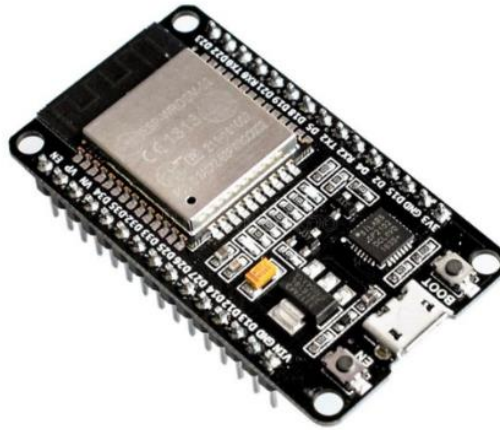
Gambar 2.16 *Solenoid Door Lock*

Pada sistem keamanan kunci pintu gedung berbasis *internet of things*, solenoid dapat digunakan untuk mengontrol akses masuk ke dalam gedung. Misalnya, saat seseorang ingin masuk ke dalam gedung, mereka harus memasukkan kode akses. Jika kode akses yang dimasukkan cocok dengan *database* yang tersimpan, maka solenoid akan diaktifkan dan menggerakkan inti ke arah yang tepat untuk membuka kunci pintu.

Selain itu, solenoid juga dapat digunakan untuk mengontrol akses ke ruangan-ruangan tertentu di dalam gedung. Misalnya, solenoid dapat digunakan untuk mengontrol akses masuk ke ruangan *server* atau ruangan penting lainnya dengan cara yang sama seperti yang telah dijelaskan di atas. Dengan menggunakan solenoid, sistem keamanan kunci pintu gedung berbasis *internet of things* dapat lebih efektif dan mudah diintegrasikan dengan sistem keamanan lainnya, seperti sistem pengawasan CCTV atau sistem pemantauan akses.

c. ESP32

ESP32 adalah mikrokontroler yang diperkenalkan oleh *Espressif System* merupakan penerus dari ESP8266[7]. Selain itu, ESP32 juga memiliki keunggulan dibandingkan mikrokontroler lainnya, mulai dari *output* pin yang lebih banyak, pin analog yang lebih banyak, memori yang lebih besar, dan *Bluetooth* 4.0 yang hemat energi. Mikrokontroler ini sudah menyertakan modul WiFi dalam *chip* prosesor *dual-core* yang berjalan pada instruksi Xtensa LX16, sehingga mendukung pembuatan sistem aplikasi IoT dengan sangat baik. Memori ESP32 terdiri atas 448 kB ROM, 520 kB SRAM, dua 8 kB RTC *memory*, dan *flash memory* 4MB[7]. *Chip* ini mempunyai 18 pin ADC (12-bit), empat unit SPI, dan dua unit I2C[7]. Kelebihan utama dari mikrokontroler ini adalah harganya relatif murah, mudah diprogram, dan memiliki jumlah pin I/O yang cukup. Tampilan ESP32 dapat dilihat pada gambar 2.17 di bawah ini.



Gambar 2.17 ESP32

Dalam pengembangan sistem keamanan kunci pintu gedung berbasis *internet of things*, ESP32 dapat digunakan sebagai kontroler utama yang bertugas untuk mengontrol seluruh sistem keamanan. Modul ini dapat terhubung ke jaringan internet melalui WiFi atau *Bluetooth*, sehingga dapat terkoneksi dengan perangkat lain yang terhubung ke internet, seperti *smartphone* atau komputer.

Dengan menggunakan ESP32, sistem keamanan kunci pintu gedung dapat diakses dan dikontrol secara *remote* melalui internet. Misalnya, pengguna dapat membuka atau mengunci pintu gedung dengan menggunakan aplikasi *smartphone* yang terhubung ke internet. Selain itu, ESP32 juga dapat digunakan untuk mengirim notifikasi ke pengguna saat ada aktivitas yang tidak diinginkan di area gedung, seperti masuknya orang yang tidak memiliki izin.

Di samping itu, ESP32 juga dapat digunakan untuk mengumpulkan data dari sensor-sensor yang terpasang di gedung. Data tersebut dapat diolah dan dianalisis oleh ESP32 untuk mengambil keputusan yang sesuai, seperti membuka atau mengunci pintu gedung. Dengan demikian, ESP32 merupakan komponen penting yang mendukung proses pengembangan sistem keamanan kunci pintu gedung berbasis *internet of things*.

d. *Flutter* SDK

Flutter adalah SDK untuk pengembangan aplikasi *mobile* dengan kinerja tinggi, aplikasi untuk iOS dan Android, dari satu *codebase* (basis kode) yang dibuat oleh *Google* dengan lisensi *open source*. Tujuannya adalah memungkinkan pengembang untuk menghadirkan aplikasi berkinerja tinggi[8].

Dalam pengembangan sistem keamanan kunci pintu gedung berbasis *internet of things*, *Flutter* SDK dapat digunakan untuk membuat aplikasi yang akan di-*install* pada *smartphone* pengguna. Aplikasi tersebut dapat digunakan oleh pengguna untuk mengakses dan mengontrol sistem keamanan kunci pintu gedung secara *remote* melalui internet.

Flutter memiliki banyak fitur yang memudahkan pengembangan aplikasi *mobile*, seperti *hot reload*, yang memungkinkan *developer* untuk memperbarui kode aplikasi tanpa harus mengompilasi ulang. Selain itu, *Flutter* juga memiliki seperangkat *widget* yang dapat digunakan untuk membangun *interface* aplikasi dengan cepat dan mudah. Dengan demikian, *Flutter* SDK merupakan pilihan yang tepat untuk membangun aplikasi *mobile* yang akan digunakan dalam sistem keamanan kunci pintu gedung berbasis *internet of things*.

e. *MySQL*

MySQL adalah sistem manajemen basis data sumber terbuka. *MySQL* adalah sistem manajemen basis data relasional. Dengan kata lain, data yang dikelola dalam *database* ditempatkan dalam tabel terpisah, yang secara signifikan mempercepat pemrosesan data. *Database* dari kecil hingga sangat besar dapat dikelola dengan *MySQL*. Dalam pengembangan sistem keamanan kunci pintu gedung berbasis *internet of things*, *MySQL* dapat digunakan untuk menyimpan data yang dibutuhkan oleh sistem, seperti data akses pengguna, data kunci pintu, dan data lainnya yang berkaitan dengan sistem keamanan. Dengan menggunakan *MySQL*, data tersebut dapat dengan mudah diakses dan dimanipulasi oleh sistem keamanan kunci pintu gedung untuk mengambil keputusan yang sesuai.

Dengan demikian, *MySQL* merupakan komponen penting yang mendukung proses pengembangan sistem keamanan kunci pintu gedung berbasis *internet of things*. *MySQL* memungkinkan sistem untuk menyimpan dan mengolah data dengan cepat dan efisien, sehingga sistem dapat beroperasi dengan baik dan menjamin keamanan yang optimal bagi gedung yang diproteksi.

f. *Cloud Hosting*

Cloud hosting adalah jenis *hosting web* yang menggunakan banyak *server* untuk menyeimbangkan beban dan memaksimalkan kinerja. Contohnya, *cloud* sebagai *web* dari beberapa komputer berbeda dan semuanya akan saling terhubung.

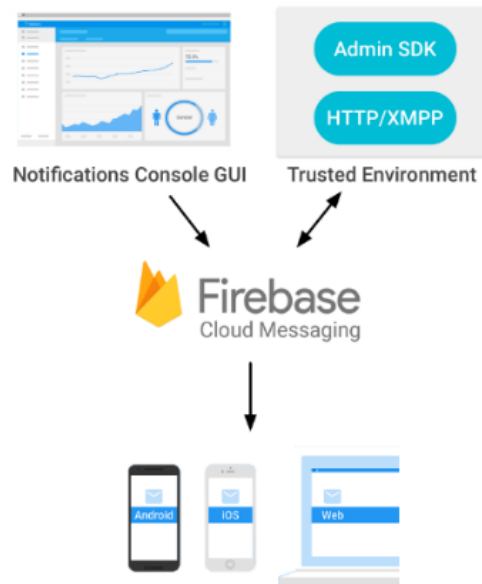
Dalam pengembangan sistem keamanan kunci pintu gedung berbasis *internet of things*, *cloud hosting* dapat digunakan untuk menyimpan dan menjalankan aplikasi yang digunakan untuk mengontrol sistem keamanan. Dengan menggunakan *cloud hosting*, aplikasi tersebut dapat diakses secara *remote* melalui internet, sehingga pengguna dapat mengakses sistem keamanan dari mana saja dengan koneksi internet.

Cloud hosting juga memiliki keuntungan lain seperti skalabilitas yang tinggi, yang memungkinkan sistem keamanan kunci pintu gedung untuk menangani jumlah akses yang tinggi tanpa terganggu. Selain itu, *cloud hosting* juga menyediakan keamanan yang tinggi, sehingga data yang disimpan aman dari serangan *cyber* atau kebocoran data. Dengan demikian, *cloud hosting* merupakan pilihan yang tepat untuk mendukung proses pengembangan sistem keamanan kunci pintu gedung berbasis *internet of things*.

g. *Firebase Cloud Messaging (FCM)*

Firebase Cloud Messaging (FCM) adalah layanan perpesanan lintas *platform* gratis dari *Google*. FCM juga menawarkan fungsi untuk membuat *push notification*, yaitu notifikasi yang muncul di bagian atas layar *smartphone* dan dapat ditarik ke bawah. Untuk mengakses seluruh pesan, pengguna cukup menekan pesan yang ditampilkan di notifikasi. Menggunakan fitur *push notification* dengan FCM sangat berguna karena FCM mengirimkan notifikasi secara *real time*.

(Proses pengiriman pesan notifikasi dari aplikasi melalui FCM ke perangkat klien dapat dilihat pada Gambar 2.18.



Gambar 2.18 Proses Pengiriman Notifikasi FCM

Dalam pengembangan sistem keamanan kunci pintu gedung berbasis *internet of things*, FCM dapat digunakan untuk mengirim notifikasi ke pengguna saat terjadi aktivitas yang tidak diinginkan di gedung, seperti masuknya orang yang tidak memiliki izin. Dengan menggunakan FCM, pengguna dapat dengan cepat menerima notifikasi dan mengambil tindakan yang diperlukan, seperti memanggil polisi atau mengunci pintu gedung.

Selain itu, FCM juga dapat digunakan untuk mengirim notifikasi ke pengguna saat ada perubahan pada sistem keamanan kunci pintu gedung, seperti perubahan kode akses atau perubahan izin akses pengguna. Dengan demikian, FCM merupakan komponen penting yang mendukung proses pengembangan sistem keamanan kunci pintu gedung berbasis *internet of things*, karena memungkinkan sistem untuk memberikan informasi ke pengguna secara cepat dan efisien.

h. JSON

JSON (*JavaScript Object Notation*) adalah format sederhana untuk memasukkan data ke dalam variabel. Mudah bagi manusia untuk memahami dan menerapkan dan mudah bagi komputer untuk menganalisis. JSON adalah bagian dari bahasa pemrograman JavaScript (standar ECMA-262, edisi ke-3 - Desember 1999). JSON merupakan format teks yang sepenuhnya *independent*, tetapi menggunakan konvensi yang *familiar* dengan bahasa pemrograman dari keluarga-C, termasuk C,

C++, C#, Java, JavaScript, Perl, Python, dan sebagainya. Keunggulan ini menjadikan JSON sebagai bahasa komunikasi yang ideal.

Dalam pengembangan sistem keamanan kunci pintu gedung berbasis *internet of things*, JSON dapat digunakan untuk menyimpan dan mengirimkan data yang dibutuhkan oleh sistem, seperti data akses pengguna, data kunci pintu, dan data lainnya yang berkaitan dengan sistem keamanan. Dengan menggunakan JSON, data-data tersebut dapat dengan mudah diakses dan dimanipulasi oleh sistem keamanan kunci pintu gedung untuk mengambil keputusan yang sesuai.

Dengan demikian, JSON merupakan komponen penting yang mendukung proses pengembangan sistem keamanan kunci pintu gedung berbasis *internet of things*. JSON memungkinkan sistem untuk menyimpan dan mengirimkan data dengan cepat dan mudah, sehingga sistem dapat beroperasi dengan baik dan menjamin keamanan yang optimal bagi gedung yang diproteksi.

i. WiFi

WiFi adalah teknologi terkenal yang memanfaatkan peralatan elektronik untuk bertukar data secara nirkabel (menggunakan gelombang radio) melalui jaringan komputer, termasuk koneksi internet berkecepatan tinggi[9]. Dalam pengembangan sistem keamanan kunci pintu gedung berbasis *internet of things*, WiFi dapat digunakan sebagai salah satu cara untuk terhubung ke internet. Dengan menggunakan WiFi, sistem keamanan kunci pintu gedung dapat terkoneksi ke internet dan berkomunikasi dengan perangkat lain yang terhubung ke internet, seperti *smartphone* atau komputer.

Dengan menggunakan WiFi, sistem keamanan kunci pintu gedung dapat diakses dan dikontrol secara *remote* melalui internet. Misalnya, pengguna dapat membuka atau mengunci pintu gedung dengan menggunakan aplikasi *smartphone* yang terhubung ke internet. Selain itu, WiFi juga dapat digunakan untuk mengumpulkan data dari sensor-sensor yang terpasang di gedung.

Di samping itu, WiFi juga memiliki keuntungan lain seperti kecepatan yang tinggi dan biaya yang relatif rendah, sehingga menjadi pilihan yang tepat untuk digunakan dalam sistem keamanan kunci pintu gedung berbasis *internet of things*. Dengan demikian, WiFi merupakan komponen penting yang mendukung proses pengembangan sistem keamanan kunci pintu gedung berbasis *internet of things*.

j. Bluetooth

Bluetooth adalah spesifikasi industri untuk *Personal Area Network (PAN)* nirkabel. *Bluetooth* membuat koneksi dan dapat digunakan untuk bertukar data antar perangkat. Spesifikasi perangkat *Bluetooth* ini dikembangkan dan didistribusikan oleh *Bluetooth Special Interest Group*. *Bluetooth* beroperasi di pita frekuensi 2,4 GHz menggunakan frekuensi melompat, mampu menyediakan layanan komunikasi data dan suara *real-time* antara *host Bluetooth* dalam jangkauan terbatas.

Dalam pengembangan sistem keamanan kunci pintu gedung berbasis *internet of things*, *Bluetooth* dapat digunakan untuk terhubung dengan perangkat-perangkat lain yang terpasang di gedung, seperti sensor-sensor atau kunci pintu. Dengan menggunakan *Bluetooth*, sistem keamanan kunci pintu gedung dapat menerima *input* dari perangkat-perangkat tersebut dan mengambil tindakan yang diperlukan. Selain itu, *Bluetooth* juga dapat digunakan untuk mengirimkan notifikasi ke pengguna saat terjadi aktivitas yang tidak diinginkan di gedung, seperti masuknya orang yang tidak memiliki izin. Dengan menggunakan *Bluetooth*, pengguna dapat menerima notifikasi secara *real-time* dan mengambil tindakan yang diperlukan, seperti memanggil polisi atau mengunci pintu gedung.

Bluetooth memiliki keuntungan lain seperti biaya yang relatif rendah dan mudah digunakan, sehingga menjadi pilihan yang tepat untuk digunakan dalam sistem keamanan kunci pintu gedung berbasis *internet of things*. Dengan demikian, *Bluetooth* merupakan komponen penting yang mendukung proses pengembangan sistem keamanan kunci pintu gedung berbasis *internet of things*.

k. *Laravel Web Apps*

Laravel adalah kerangka kerja pengembangan *web MVC* yang dirancang untuk meningkatkan kualitas perangkat lunak dengan mengurangi biaya pengembangan dan pemeliharaan serta meningkatkan produktivitas kerja dengan sintaks yang bersih dan fungsional yang dapat mengurangi waktu penerapan. Laravel merupakan *framework* dengan versi PHP yang *up-to-date*, karena Laravel mensyaratkan PHP versi 5.3 ke atas. Laravel adalah *framework* PHP yang menekankan kesederhanaan dan fleksibilitas dalam desainnya. Laravel menyediakan alat yang diperbarui untuk berinteraksi dengan *database* yang disebut Migrasi. Dengan Migrasi, pengembang dapat dengan mudah untuk melakukan modifikasi secara *independent* karena implementasi skema *database*

direpresentasikan dalam sebuah *class*. Migrasi dapat dilakukan dengan beberapa *database* yang didukung oleh Laravel (MySQL, PostgreSQL, MSSQL dan SQLITE) dan implementasi *Active Record* di Laravel disebut *Eloquent*, yang menggunakan standar OOP *modern*. Laravel juga memberikan sebuah *Command Line Interface* disebut dengan *artisan* dengan *artisan*, pengembang dapat berinteraksi dengan aplikasi untuk sebuah aksi seperti *migrations*, *testing*, atau membuat *controller* dan model[10]. Selain itu, laravel juga memiliki *Blade template engine* yang memberikan estetika dan kebersihan kode pada *view* secara parsial[10].

Dalam pengembangan sistem keamanan kunci pintu gedung berbasis *internet of things*, Laravel dapat digunakan untuk membangun aplikasi *web* yang digunakan untuk mengontrol sistem keamanan. Dengan menggunakan Laravel, aplikasi tersebut dapat dikembangkan dengan cepat dan mudah, sehingga pengguna dapat dengan mudah mengakses sistem keamanan dari mana saja dengan koneksi internet.

Selain itu, Laravel juga dapat digunakan untuk mengembangkan aplikasi *web* yang digunakan untuk menyimpan dan mengolah data yang diperoleh dari sensor-sensor yang terpasang di gedung. Data tersebut dapat diolah dan dianalisis oleh sistem keamanan kunci pintu gedung untuk mengambil tindakan yang sesuai, seperti membuka atau mengunci pintu gedung.

Dengan demikian, Laravel merupakan komponen penting yang mendukung proses pengembangan sistem keamanan kunci pintu gedung berbasis *internet of things*.

1. Laravel API Server

Laravel API server adalah sebuah aplikasi yang dikembangkan menggunakan *framework* Laravel yang digunakan untuk membuat API (*Application Programming Interface*). API merupakan sekumpulan fungsi yang tersedia untuk digunakan oleh aplikasi, yang memungkinkan aplikasi tersebut untuk berkomunikasi dengan sistem lain atau mengakses data yang tersimpan di sistem tersebut.

Dalam pengembangan sistem keamanan kunci pintu gedung berbasis *internet of things*, Laravel API server dapat digunakan untuk membuat API yang digunakan oleh aplikasi yang terhubung dengan sistem keamanan kunci pintu gedung.

Dengan menggunakan Laravel API server, aplikasi tersebut dapat dengan mudah

mengakses data yang diperlukan dari sistem keamanan kunci pintu gedung, seperti data akses pengguna atau data kunci pintu.

Selain itu, Laravel API *server* juga dapat digunakan untuk mengirimkan data yang diperoleh dari sensor-sensor yang terpasang di gedung ke aplikasi yang terhubung dengan sistem keamanan kunci pintu gedung. Data tersebut dapat diolah dan dianalisis oleh sistem keamanan kunci pintu gedung untuk mengambil tindakan yang sesuai, seperti membuka atau mengunci pintu gedung.

Dengan demikian, Laravel API *server* merupakan komponen penting yang mendukung proses pengembangan sistem keamanan kunci pintu gedung berbasis *internet of things*.

m. *One Time Password*

One Time Password terdiri dari 2 kategori besar, yaitu HOTP (HMAC-based OTP) dan TOTP (Time-based OTP)[11]. *One Time Password* (OTP) yang disebut dengan istilah sandi sekali pakai, biasanya digunakan untuk transaksi *online* atau pendaftaran sebuah akun[11]. Kode OTP terdiri dari kombinasi nomor unik dan rahasia yang diperoleh secara acak, di mana kode OTP dimaksudkan untuk keamanan dan OTP dianggap lebih aman karena perubahan *password* secara terus-menerus[11].

Dalam pengembangan sistem keamanan kunci pintu gedung berbasis *internet of things*, OTP dapat digunakan untuk meningkatkan keamanan akses pengguna ke sistem. Misalnya, saat pengguna ingin mengakses sistem keamanan kunci pintu gedung, sistem akan mengirimkan OTP ke perangkat *mobile* pengguna. Pengguna harus memasukkan OTP tersebut ke sistem untuk dapat masuk dan mengakses sistem keamanan kunci pintu gedung.

Dengan menggunakan OTP, sistem keamanan kunci pintu gedung dapat menjadi lebih aman karena hanya pengguna yang memiliki OTP yang dapat mengakses sistem. Selain itu, OTP juga dapat digunakan untuk menghindari akses yang tidak sah ke sistem keamanan kunci pintu gedung, seperti masuknya orang yang tidak memiliki izin.

Dengan demikian, OTP merupakan komponen penting yang mendukung proses pengembangan sistem keamanan kunci pintu gedung berbasis *internet of things*. OTP memungkinkan sistem untuk menjadi lebih aman dan menghindari akses yang tidak sah ke sistem keamanan kunci pintu gedung.

n. *QR-Code*

Qr code merupakan teknik yang mengubah data tertulis menjadi kode-kode 2 dimensi yang tercetak ke dalam suatu media yang lebih ringkas. QR code adalah *barcode* 2 dimensi yang diperkenalkan pertama kali oleh perusahaan Jepang Denso Wave pada tahun 1994[12]. *Barcode* ini pertama kali digunakan untuk pendataan inventaris produksi suku cadang kendaraan dan sekarang sudah digunakan dalam berbagai bidang[12]. QR adalah singkatan dari *Quick Response* karena bertujuan untuk menerjemahkan kontennya dengan cepat. QR-Code salah satu tipe dari *barcode* yang dapat dibaca dengan kamera *handphone*[12].

Dalam pengembangan sistem keamanan kunci pintu gedung berbasis *internet of things*, QR code dapat digunakan untuk mempermudah akses pengguna ke sistem keamanan kunci pintu gedung. Misalnya, saat pengguna ingin masuk ke gedung, pengguna hanya perlu meng-scann QR code yang terpasang di pintu gedung menggunakan aplikasi QR code reader. Sistem keamanan kunci pintu gedung akan mengenali QR code tersebut dan membuka pintu gedung untuk pengguna.

Selain itu, QR code juga dapat digunakan untuk mengirimkan informasi yang diperlukan oleh sistem keamanan kunci pintu gedung, seperti data akses pengguna atau data kunci pintu. Dengan menggunakan QR code, data tersebut dapat dengan mudah diakses oleh sistem keamanan kunci pintu gedung untuk mengambil tindakan yang sesuai.

Dengan demikian, QR code merupakan komponen penting yang mendukung proses pengembangan sistem keamanan kunci pintu gedung berbasis *internet of things*.

2.2.4 Teknologi yang Digunakan

Teknologi yang digunakan pada sistem keamanan kunci pintu gedung berbasis *Internet of Things* (IoT) tergantung pada jenis sistem yang digunakan. Berikut ini beberapa teknologi yang digunakan pada sistem keamanan kunci pintu gedung berbasis IoT:

- a. Pemindai QR code
- b. Kontroler akses
- c. Perangkat kontrol kunci pintu
- d. Sistem operasi

- e. Sensor
- f. Aktuator
- g. Mikrokontroler
- h. Aplikasi *Mobile* pemindai QR-Code
- i. *Database*
- j. *Server*
- k. *Cloud Hosting*
- l. *Firebase Cloud Messaging*
- m. JSON
- n. WiFi
- o. *Bluetooth*
- p. *Website*
- q. Laravel API *Server*
- r. *One Time Password*
- s. *QR-Code*

2.2.5 Batasan – Batasan Sistem

Berikut ini merupakan batasan – batasan dalam perancangan sistem keamanan kunci pintu gedung berbasis *Internet of Things*:

- a. Komunikasi antara perangkat kunci pintu dengan aplikasi *mobile* dilakukan secara *realtime*. Setiap terjadi perubahan kondisi pada pintu, maka perangkat akan langsung mengirimkan notifikasi ke aplikasi pengguna melalui *server* yang tersedia serta mencatat *log* perubahan dan disimpan di dalam *database*.
- b. Untuk proses membuka pintu, perangkat akan membuat sebuah kunci yang disimpan di dalam perangkat dan akan dibagikan oleh *server*. Pada saat pengguna masuk ke aplikasi, *server* akan mengirimkan kunci pintu sesuai dengan level aksesnya. Kunci tersebut digunakan untuk melakukan autentikasi ditambah dengan *username* dan *password* untuk menambah tingkat keamanan penguncian.
- c. Aplikasi pengguna akan menyimpan kunci yang digunakan untuk autentikasi sehingga hanya pengguna tertentu saja yang dapat membuka.
- d. *Web apps* memiliki akses untuk mengatur semua pengguna yang dapat membuka pintu dan dapat membuka pintu dari jarak jauh menggunakan koneksi internet.

- e. Pada aplikasi pengguna terdapat fitur *scann*-QR yang digunakan untuk membuka pintu hanya dengan memindai *QR-Code* pada pintu.
- f. Keamanan: Sistem ini harus memastikan bahwa tidak ada yang dapat mengakses sistem tanpa izin dan tidak ada yang dapat memanipulasi atau membajak sistem.
- g. Integritas data: Sistem keamanan kunci pintu gedung berbasis IoT harus memastikan integritas data yang disimpan dan ditransmisikan, agar tidak ada yang dapat mengubah atau memalsukan data tersebut.
- h. Ketersediaan: Sistem keamanan kunci pintu gedung berbasis IoT harus selalu tersedia dan dapat diakses oleh pengguna yang memiliki izin, karena ini merupakan bagian penting dari keamanan gedung.
- i. Skalabilitas: Sistem keamanan kunci pintu gedung berbasis IoT harus mampu menangani jumlah pengguna yang beragam dan meningkat dengan mudah.
- j. Biaya: Sistem keamanan kunci pintu gedung berbasis IoT mungkin membutuhkan biaya yang lebih tinggi daripada sistem keamanan tradisional, terutama jika harus diimplementasikan di banyak lokasi atau gedung.
- k. Kompatibilitas: Sistem keamanan kunci pintu gedung berbasis IoT harus kompatibel dengan perangkat yang digunakan oleh pengguna, seperti ponsel pintar atau *smartphone*.
- l. Performa: Sistem keamanan kunci pintu gedung berbasis IoT harus mampu memberikan performa yang tinggi dan respons yang cepat terhadap permintaan akses dari pengguna.

2.2.6 Standarisasi Produk

Ada beberapa standar *engineering* yang dapat dirujuk dalam rancang bangun sistem keamanan kunci pintu gedung berbasis *Internet of Things* (IoT). Beberapa standar yang paling penting adalah:

- 1) ISO/IEC 27001:2013: Standar ini mengatur tentang manajemen keamanan informasi, yang membantu dalam menentukan kontrol keamanan yang harus diterapkan dalam sistem IoT.
- 2) ISO/IEC 27002:2013: Standar ini menyediakan panduan untuk implementasi kontrol keamanan yang ditentukan dalam ISO/IEC 27001.

- 3) ISO/IEC 15408 (*Common Criteria*): Standar ini mengatur tentang evaluasi keamanan produk, yang dapat digunakan untuk mengevaluasi produk IoT dari segi keamanan.
- 4) IEEE 802.15.4: Standar ini mengatur tentang komunikasi *wireless* yang digunakan dalam sistem IoT yang digunakan dalam sistem kontrol akses pintu.
- 5) IEEE P2413: Standar ini menyediakan panduan untuk arsitektur IoT, yang dapat digunakan dalam mendesain sistem keamanan kunci pintu gedung berbasis IoT.
- 6) NIST SP 800-160: Standar ini menyediakan panduan untuk desain keamanan sistem IoT, yang dapat digunakan dalam menentukan kontrol keamanan yang harus diterapkan dalam sistem keamanan kunci pintu gedung berbasis IoT.
- 7) UL 294: Standar ini mengatur tentang keamanan sistem akses kontrol, yang dapat digunakan dalam menentukan kontrol keamanan yang harus diterapkan dalam sistem keamanan kunci pintu gedung berbasis IoT.
- 8) UL 681: Standar ini mengatur tentang keamanan sistem akses kontrol yang digunakan dalam lingkungan komersial, yang dapat digunakan dalam menentukan kontrol keamanan yang harus diterapkan dalam sistem keamanan kunci pintu gedung berbasis IoT.

Ketentuan-ketentuan dari standar-standar tersebut harus diperhatikan dalam proses pembuatan sistem keamanan kunci pintu gedung berbasis IoT, untuk memastikan sistem tersebut aman dan sesuai dengan standar industri yang ditentukan.

2.2.7 Etika Profesi yang Dijunjung

Dalam melakukan perancangan dan pengerjaan tugas akhir, prinsip – prinsip kode etik insinyur yang diterapkan tercantum dalam *fundamental canons National Society of Professional Engineer (NSPE)*, meliputi:

- 1) Mengutamakan keselamatan, kesehatan, dan kesejahteraan publik.
Penerapan etika profesi tersebut dalam pembuatan proyek tugas akhir ini yaitu dalam pengerjaan proyek ini jam kerjanya disesuaikan berdasarkan kemampuan dan kapasitas masing-masing anggota tim tugas akhir sesuai yang ada di bagian *man-month*. Hal tersebut dilakukan demi mengutamakan keselamatan, kesehatan, dan kesejahteraan masing-masing anggota tim tugas akhir.
- 2) Melakukan pelayanan hanya dalam bidang kompetensi masing-masing.

Penerapan etika profesi tersebut dalam pembuatan proyek tugas akhir ini yaitu dalam pembagian tugas (*partitioning*) pengerjaan proyek ini disesuaikan dengan bidang kompetensi masing-masing atau konsentrasi yang diambil oleh anggota tim tugas akhir. Untuk pembagian tugasnya dapat dilihat pada Gambar 2.1 dan Tabel 4.1. Hal tersebut dilakukan demi menjunjung etika profesi melakukan pelayanan hanya dalam bidang kompetensi masing-masing.

- 3) Mengeluarkan pernyataan secara objektif dan jujur.

Penerapan etika profesi tersebut dalam pembuatan proyek tugas akhir ini yaitu dalam penulisan laporan tugas akhir salah satunya dokumen B-100 ini dilakukan secara objektif dan jujur dengan didukung adanya referensi dari berbagai sumber, seperti paper jurnal baik itu dari Undip atau tidak, internet, dan sumber lainnya. Hal tersebut dilakukan demi menjunjung etika profesi mengeluarkan pernyataan secara objektif dan jujur.

- 4) Bertindak untuk setiap *employer* atau klien sebagai orang kepercayaan.

Penerapan etika profesi tersebut dalam pembuatan proyek tugas akhir ini yaitu mengerjakan tugas akhir sesuai dengan pedoman tugas akhir.

- 5) Menghindari perbuatan menipu/berbohong.

Penerapan etika profesi tersebut dalam pembuatan proyek tugas akhir ini yaitu tidak melebih-lebihkan tanggung jawab dalam atau untuk masalah pokok penugasan sebelumnya.

- 6) Berperilaku terhormat, bertanggung jawab, etis, dan sah untuk meningkatkan kehormatan, nama baik, dan kegunaan profesi.

Penerapan etika profesi tersebut dalam pembuatan proyek tugas akhir ini yaitu antara anggota tim yang satu dengan lainnya selalu mengingatkan untuk meningkatkan kehormatan, nama baik, dan kegunaan profesi tim dengan menjalankan atau mengerjakan tugas akhir sesuai dengan jadwal dan waktu pengembangan yang tertera pada Tabel 2.7 disertai etika yang ada.

2.3 Skenario Pemanfaatan Produk

Desain rekayasa perancangan sistem keamanan kunci pintu gedung berbasis *Internet of Things* ini secara umum ditujukan untuk membangun sistem keamanan pada sebuah gedung, seperti hotel, perusahaan, apartemen, maupun instansi untuk meningkatkan keamanan dalam ruangan.

Adapun pihak yang menjadi pengguna sistem keamanan kunci pintu gedung berbasis *Internet of Things* (IoT) adalah:

- 1) Pemilik gedung: Pemilik gedung merupakan pengguna utama sistem keamanan ini, karena ia bertanggung jawab atas keamanan gedung yang dimilikinya.
- 2) *Tenant*/penyewa: *Tenant* atau penyewa gedung juga merupakan pengguna sistem keamanan, karena mereka membutuhkan akses masuk dan keluar dari gedung yang aman.
- 3) Karyawan: Karyawan yang bekerja di gedung tersebut juga merupakan pengguna sistem keamanan, karena mereka membutuhkan akses masuk dan keluar dari gedung yang aman.
- 4) Tamu: Tamu atau pengunjung yang datang ke gedung tersebut juga merupakan pengguna sistem keamanan, karena mereka membutuhkan akses masuk ke gedung yang aman.

Oleh karena itu, sistem keamanan kunci pintu gedung berbasis IoT akan berguna bagi berbagai pihak yang membutuhkan akses masuk dan keluar dari gedung yang aman.

Berikut adalah beberapa karakteristik (para) pengguna sistem keamanan kunci pintu gedung berbasis *Internet of Things*:

- 1) Menggunakan *smartphone*: Pengguna sistem keamanan kunci pintu gedung berbasis IoT biasanya memiliki *smartphone* yang dapat terhubung ke internet, karena aplikasi atau *platform* yang digunakan untuk mengontrol akses masuk dan keluar dari gedung tersebut biasanya tersedia dalam bentuk aplikasi *mobile*.
- 2) Menggunakan jaringan nirkabel: Pengguna sistem keamanan kunci pintu gedung berbasis IoT biasanya terhubung ke jaringan nirkabel, seperti WiFi, karena setiap kunci pintu yang terhubung ke jaringan tersebut harus terkoneksi ke internet.
- 3) Memiliki akses ke aplikasi atau *platform*: Pengguna sistem keamanan kunci pintu gedung berbasis IoT harus memiliki akses ke aplikasi atau *platform* yang digunakan untuk mengontrol akses masuk dan keluar dari gedung, serta melihat riwayat akses dan melakukan pemantauan keamanan.
- 4) Memiliki mekanisme autentikasi: Pengguna sistem keamanan kunci pintu gedung berbasis IoT harus memiliki mekanisme autentikasi yang aman, seperti *password* untuk memastikan hanya pengguna yang sah yang dapat mengakses sistem keamanan.

- 5) Memiliki kebutuhan akses masuk dan keluar yang aman: Pengguna sistem keamanan kunci pintu gedung berbasis IoT memiliki kebutuhan akses masuk dan keluar yang aman, karena sistem ini bertujuan untuk meningkatkan keamanan gedung.

Berikut adalah beberapa informasi mengenai waktu, tempat, dan cara penggunaan produk sistem keamanan kunci pintu gedung berbasis *Internet of Things* (IoT) oleh pihak-pihak:

- 1) Waktu penggunaan: Penggunaan produk sistem keamanan kunci pintu gedung berbasis IoT dapat dilakukan kapan saja, tergantung pada kebutuhan pengguna. Misalnya, pemilik gedung dapat mengontrol akses masuk dan keluar dari gedung pada jam kerja saja, atau *tenant* dapat mengakses gedung hanya pada waktu-waktu tertentu saja.
- 2) Tempat penggunaan: Produk sistem keamanan kunci pintu gedung berbasis IoT dapat digunakan di gedung yang telah dipasang kunci pintu yang terhubung ke jaringan.
- 3) Cara penggunaan: Penggunaan produk sistem keamanan kunci pintu gedung berbasis IoT dilakukan melalui aplikasi atau *platform* yang disediakan. Pengguna dapat mengontrol akses masuk dan keluar dari gedung, melihat riwayat akses, dan melakukan pemantauan keamanan melalui aplikasi atau *platform* tersebut.

Oleh karena itu, produk sistem keamanan kunci pintu gedung berbasis IoT dapat digunakan oleh berbagai pihak sesuai dengan kebutuhan dan di tempat yang telah dipasang kunci pintu yang terhubung ke jaringan.

Jika memungkinkan diproduksi massal, berikut adalah beberapa skenario pemasaran produk sistem keamanan kunci pintu gedung berbasis *Internet of Things* (IoT):

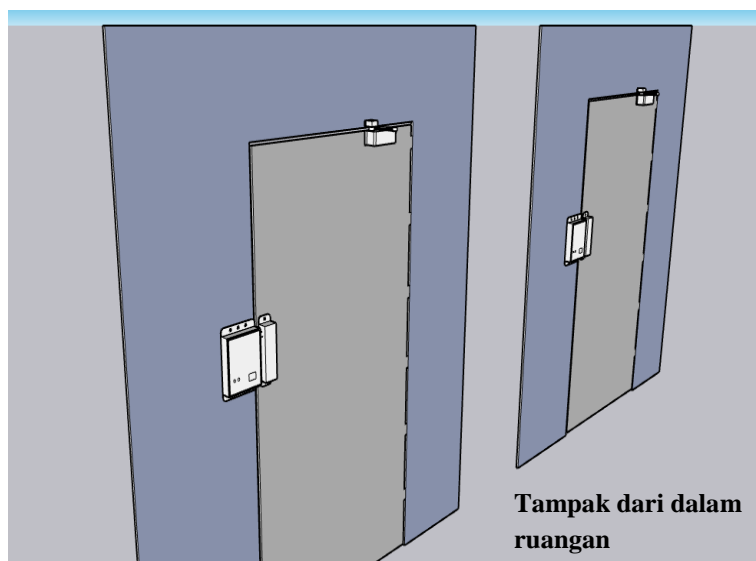
- 1) Menggunakan media *online*: Caranya dengan mempromosikan produk sistem keamanan kunci pintu gedung berbasis IoT melalui media *online*, seperti situs *web*, media sosial, dan forum *online*. Selain itu, juga dapat dipromosikan dengan menggunakan iklan *banner* atau postingan di media sosial yang menjelaskan fitur-fitur dan keunggulan produk yang dipasarkan.
- 2) Menghadiri pameran atau seminar: Pemasaran produk dapat dilakukan dengan menghadiri pameran atau seminar yang terkait dengan teknologi IoT atau keamanan gedung, dan menyajikan produk kepada para pengunjung. Selain itu,

juga dapat dengan cara membagikan brosur atau katalog produk kepada para pengunjung.

- 3) Menggunakan media cetak: Pemasaran produk dapat dilakukan dengan mempromosikan produk sistem keamanan kunci pintu gedung berbasis IoT melalui media cetak, seperti surat kabar, majalah, atau brosur. Selain itu, dapat juga dengan membuat iklan atau artikel yang menjelaskan fitur-fitur dan keunggulan produk.
- 4) Mengadakan demo produk: Pemasaran produk dapat dilakukan dengan mengadakan demo produk sistem keamanan kunci pintu gedung berbasis IoT kepada para calon pembeli atau *investor*. Demo ini dapat dilakukan di gedung yang telah dipasang produk, atau di tempat lain yang sesuai.
- 5) Menggunakan jaringan koneksi: Pemasaran produk dapat dilakukan dengan memanfaatkan jaringan koneksi yang dimiliki untuk mempromosikan produk sistem keamanan kunci pintu gedung berbasis IoT kepada teman, kolega, atau rekan bisnis yang mungkin berminat.

Dengan demikian, ada beberapa cara yang dapat dilakukan untuk memasarkan produk sistem keamanan kunci pintu gedung berbasis IoT kepada para calon pembeli atau investor.

Gambar 2.19 dan 2.20 diperlihatkan pemanfaatan produk sistem keamanan kunci pintu gedung berbasis IoT.



Gambar 2.19 Pemanfaatan Produk Sistem Keamanan Kunci Pintu Gedung Berbasis IoT Tampak dari Dalam Ruangan



Gambar 2.20 Pemanfaatan Produk Sistem Keamanan Kunci Pintu Gedung Berbasis IoT Tampak dari Luar Ruangan

2.4 Nilai Strategis

Berikut adalah beberapa dampak yang diharapkan dari pengembangan produk sistem keamanan kunci pintu gedung berbasis *Internet of Things* (IoT) terhadap masyarakat secara umum:

- 1) Peningkatan keamanan: Produk sistem keamanan kunci pintu gedung berbasis IoT diharapkan dapat meningkatkan keamanan gedung, sehingga masyarakat yang tinggal atau bekerja di gedung tersebut merasa lebih aman.
- 2) Peningkatan efisiensi: Produk ini diharapkan dapat meningkatkan efisiensi, karena pengguna dapat mengontrol akses masuk dan keluar dari gedung secara mudah melalui aplikasi atau *platform* yang disediakan.
- 3) Peningkatan kenyamanan: Produk ini diharapkan dapat meningkatkan kenyamanan pengguna, karena mereka dapat mengakses gedung dengan lebih mudah dan cepat, serta tidak perlu repot-repot membawa kunci atau kartu akses.
- 4) Peningkatan kinerja: Produk ini diharapkan dapat meningkatkan kinerja pengguna, karena mereka dapat mengontrol akses masuk dan keluar dari gedung secara cepat dan tepat waktu.
- 5) Peningkatan inovasi: Pengembangan produk sistem keamanan kunci pintu gedung berbasis IoT diharapkan dapat mendorong inovasi di bidang keamanan gedung dan teknologi IoT.

Dengan demikian, pengembangan produk sistem keamanan kunci pintu gedung berbasis IoT diharapkan dapat memberikan dampak positif bagi masyarakat secara umum.

2.5 Usaha Pengembangan

Produk akhir yang hendak dikembangkan adalah perangkat *monitoring* dan *controlling* pintu gedung sebagai suatu sistem yang utuh, dengan subsistem berupa modul sensor dan perangkat aktuator yang terpisah. Subsistem tersebut diarahkan untuk menjadi produk-produk tunggal yang mandiri, memiliki kompatibilitas untuk dirakit menjadi sistem terpadu dan dapat dipasarkan secara terpisah sesuai kebutuhan pasarnya masing-masing.

Usaha dalam proses pengembangan didefinisikan sebagai berikut:

2.5.1 *Man-Month*

Proyek tugas akhir ini dikerjakan oleh satu tim tugas akhir Teknik Elektro Universitas Diponegoro yang terdiri dari 3 orang mahasiswa S1 yaitu 2 orang mahasiswa konsentrasi Teknologi Informasi dan 1 orang mahasiswa konsentrasi Telekomunikasi. Selain itu, proyek ini dibimbing oleh 2 orang dosen. Pengerjaan proyek ini berlangsung selama 5 bulan dengan jam kerja masing – masing mahasiswa adalah 20 jam per minggu.

2.5.2 *Machine-Month*

Dalam perancangan sistem ini, memerlukan *software* ataupun *hardware* sebagai berikut:

- a. Komputer/laptop sebanyak 3 buah untuk melakukan berbagai aktivitas, seperti pembuatan prototipe, *programming*, simulasi, administrasi, dan pengujian sistem. Komputer/laptop diperkirakan digunakan selama 300 jam.
- b. Perlengkapan pengembang.

2.5.3 *Development Tools*

Proses pengembangan produk ini menggunakan beberapa perangkat lunak sebagai berikut:

- *Android Studio* untuk pengembangan aplikasi *mobile*.
- *Arduino IDE* merupakan *software* untuk melakukan penulisan program, *compile* serta *upload* program ke ESP32.

- *Visual Code Studio* digunakan sebagai *software code editor*.
- *Firebase Console* digunakan untuk mempermudah dalam pengaturan FCM.

Selain itu, ada beberapa perangkat keras yang diperlukan dalam pengembangan produk ini, diantaranya:

- Laptop
- Perlengkapan pengembang (*toolkit* perangkat keras)

2.5.4 *Test Equipment*

Untuk keseluruhan proses pengembangan, diperlukan peralatan-peralatan pengujian sebagai berikut:

- Perangkat Android dengan minimal Android 5.0 APIs digunakan sebagai piranti untuk melakukan *monitoring* dan *controlling* keamanan kunci pintu gedung.
- Multimeter digital
- *Postman* digunakan untuk pengujian API.
- *Wireshark*
- *QR-Code reader*
- *Stopwatch*

2.5.5 *Kebutuhan Expert*

Tim pengembang perancangan sistem ini terdiri dari Dosen, 2 Mahasiswa Konsentrasi Teknologi Informasi, dan 1 Mahasiswa Konsentrasi Telekomunikasi.

Untuk mengembangkan dan mengoperasikan sistem keamanan kunci pintu gedung berbasis *Internet of Things* (IoT), mungkin diperlukan *expert* dengan keahlian dalam beberapa bidang, di antaranya:

- Keamanan *cyber*: *Expert* ini bertanggung jawab untuk mengelola kerentanan sistem terhadap serangan *cyber* dan memastikan bahwa sistem tidak mudah disusupi oleh pihak yang tidak berwenang.
- Jaringan: *Expert* ini bertanggung jawab untuk mengelola jaringan yang terhubung dengan sistem keamanan dan memastikan bahwa sistem dapat beroperasi dengan baik.
- Pemrograman: *Expert* ini bertanggung jawab untuk menulis kode yang mengendalikan perangkat keras dan mengakses data dari sensor.

- *Hardware: Expert* ini bertanggung jawab untuk mengelola perangkat keras yang terhubung dengan sistem keamanan, seperti sensor dan kontroler IoT.
- *Cloud: Expert* ini bertanggung jawab untuk mengelola *platform cloud* yang digunakan untuk menyimpan dan mengelola data dari sistem keamanan.

2.5.6 Perkiraan Biaya

Tim proyek tugas akhir menghitung perkiraan biaya yang diperlukan untuk mengembangkan produk ini berdasarkan konsep produk yang diusulkan dan bahan serta peralatan yang akan dibeli atau disewa, serta biaya tenaga kerja eksternal. Tim juga memastikan biaya tersebut terpenuhi, baik dari tim sendiri atau pihak luar. Perkiraan biaya yang dibutuhkan dalam rancang bangun sistem ini dapat dilihat pada Tabel 2.6 di bawah.

Tabel 2.6 Perkiraan Biaya

No.	Pengeluaran	Jumlah	Harga Satuan (Rp)	Estimasi Harga (Rp)
1	Mikrokontroler ESP32	2 buah	70.000	140.000
2	Sensor magnetic	2 buah	10.000	20.000
3	Kabel	5 meter	2.500	12.500
4	Cetak PCB	4 buah	25.000	100.000
5	Baut, mur, <i>spacer</i>	2 buah	15.000	30.000
6	Adaptor 12 Volt	2 buah	20.000	40.000
7	Tombol	2 buah	3000	6.000
8	<i>Hosting</i>	5 buah	50.000	250.000
9	Solenoida	2 buah	40.000	80.000
Jumlah Total				678.500

2.5.7 Peluang Keberhasilan

Dengan mempertimbangkan semua aspek teknik dan non-teknis, termasuk misalnya kerumitan integrasi antar perangkat dan kerumitan dalam *programming*, serta tersedianya referensi dari berbagai sumber yang sesuai dengan sistem terkait, maka dapat diperkirakan proyek tugas akhir ini dapat selesai selama 5 bulan sesuai yang telah direncanakan. Oleh karena itu, tim membuat estimasi peluang keberhasilan menyelesaikan proyek pengembangan ini.

2.5.8 Jadwal dan Waktu Pengembangan

Proyek perancangan sistem keamanan kunci pintu gedung berbasis IoT dirancang untuk rentang 5 bulan, dimulai pada Januari 2023 – Mei 2023. *Time table* proyek ini dapat dilihat pada Tabel 2.7.

Tabel 2.7 Jadwal dan Waktu Pengembangan

Fase	<i>Deliverables</i>	Jadwal	Kebutuhan Sumber Daya
Konsep Produk	Dokumen B100 Proposal	Januari 2023	Literatur
Analisis	Dokumen B200 Spesifikasi Fungsional	Februari 2023	1. Spek standar 2. <i>Engineer</i>
Desain	Dokumen B300 Skematik Rangkaian Rancangan	Maret 2023	1. <i>Dvlp. Tools</i> 2. Penguasaan teknologi pendukung 3. Literatur 4. <i>Engineer</i>
Implementasi (Pedoman standar perencanaan instalasi)	Dokumen B400 Lab Redesain	April 2023	1. <i>Dvlp. Tools</i> 2. <i>Software Cadsoft Eagle</i> 3. <i>Software</i> Arduino IDE 4. <i>Software</i> Android Studio 5. <i>Engineer</i> 6. Komponen-komponen <i>hardware</i>
Uji subsistem (Berdasarkan standar instalasi)	Dokumen B-500 <i>Error Report</i> , redesain skematik, ralat kode program	Mei 2023	1. <i>Dvlp. Tools</i> 2. <i>Software Cadsoft Eagle</i> 3. <i>Software</i> Arduino IDE 4. <i>Engineer</i>

3 KESIMPULAN

Kesimpulan yang dapat diambil dari dokumen ini sebagai berikut:

1. Sistem keamanan kunci pintu gedung berbasis *Internet of Things* (IoT) adalah sistem yang menggunakan teknologi IoT untuk mengelola dan mengontrol akses ke pintu gedung. Sistem ini terdiri dari perangkat keras seperti sensor, kontroler IoT, dan modul komunikasi seluler yang terhubung dengan jaringan internet. Sistem ini juga terdiri dari perangkat lunak yang mengendalikan perangkat keras dan mengakses data dari sensor. Data yang dihasilkan oleh sistem keamanan ini kemudian disimpan dan dikelola menggunakan *platform cloud*. Sistem keamanan ini dapat membantu meningkatkan keamanan gedung dengan cara mengontrol akses ke pintu hanya untuk orang yang berwenang saja.
2. Proyek Rancang Bangun Sistem Keamanan Kunci Pintu Gedung Berbasis *Internet of Things* yang hendak dibuat dan dikembangkan memiliki kelayakan untuk dijalankan, dari sisi kajian ekonomis, strategis, penguasaan teknologi, maupun kemampuan fabrikasi yang ada. Hal tersebut dikarenakan sistem ini sesuai dengan kebutuhan keamanan gedung. Biaya yang dibutuhkan untuk mengembangkan dan mengoperasikan sistem ini relatif murah. Pendapatan yang akan dihasilkan dari pemasaran sistem ini cukup untuk menutup biaya yang dikeluarkan. Dari sisi ekonomi sistem ini akan memberikan nilai tambah bagi pemilik gedung. Dari sisi strategis sistem ini akan memberikan keuntungan bagi pemilik gedung, seperti meningkatkan reputasi gedung atau meningkatkan loyalitas pelanggan. Pengelolaan dan pengoperasian sistem ini mudah dilakukan. Serta dari segi kemampuan fabrikasi, pemilik gedung memiliki kemampuan untuk memproduksi atau memperoleh perangkat keras yang dibutuhkan untuk pengoperasian sistem ini dengan baik.
3. Beberapa keunggulan sistem keamanan kunci pintu gedung berbasis *Internet of Things* (IoT) adalah keamanan yang tinggi, mudah dioperasikan, dapat terintegrasi dengan sistem keamanan yang ada, tingkat keandalan yang tinggi, dan dapat menghemat biaya.
4. Tujuan dari rancang bangun sistem keamanan kunci pintu gedung berbasis *Internet of Things* ini adalah untuk meningkatkan efisiensi dan keamanan dalam pengelolaan akses masuk ke gedung dengan menggunakan teknologi internet dan sensor.

4 BIODATA TIM PENGUSUL

Tim akan melampirkan biodata yang mencakup informasi demografis dan keahlian/kualifikasi. Kualifikasi meliputi mata kuliah paket yang diselesaikan, pelatihan terkait yang diikuti, kompetisi terkait yang dimenangkan, dan portofolio terkait lainnya (kemampuan menggunakan perangkat lunak/perangkat keras).

4.1 Daftar Nama dan Spesifikasi Pekerjaan

Tabel 4.1 Daftar Nama dan Spesifikasi Pekerjaan

No.	Nama	Keahlian	Pembagian Tugas
1.	Henric Dhiki Wicaksono 21060119120011 Teknologi Informasi	Pemrograman arduino, <i>database</i> , aplikasi android.	Perancangan perangkat <i>mobile</i> sebagai piranti akses masuk pintu gedung dan <i>website</i> untuk mendukung sistem <i>monitoring</i> dan <i>controlling</i> jarak jauh.
2.	Novi Dianasari 21060119120039 Telekomunikasi	Pemrograman mikrokontroler, <i>matlab</i> , <i>software</i> proteus.	Perancangan sistem komunikasi data dua arah dan perangkat penguncian yang mendukung sistem keamanan kunci pintu gedung berbasis IoT.
3.	Muhammad Khoiril Wafi 21060119140133 Teknologi Informasi	Pemrograman arduino, <i>database</i> , aplikasi android.	Perancangan sistem <i>database & server</i> serta sistem keamanan kunci pintu gedung dengan <i>Access Control</i> .

4.2 Biodata Tim Tugas Akhir

A. Biodata Pengusul 1

Nama Lengkap : Henric Dhiki Wicaksono
Jenis Kelamin : Laki - laki
NIM : 21060119120011
Tempat, Tanggal Lahir : Boyolali, 12 Desember 2000
Alamat : Jl. Baskoro Raya No. 61
Tembalang Semarang
Email : henricwicaksono@gmail.com
Nomor Telepon / HP : 085866844261
Peminatan Konsentrasi : Teknologi Informasi



Kompetensi / Keahlian yang Dimiliki

No	Mata Kuliah Pilihan yang Diambil	SKS
1	Sistem Operasi	2
2	Pengembangan Aplikasi Perangkat Bergerak	3
3	Interaksi Manusia dan Komputer	2
4	<i>Interface dan Peripheral</i>	2
5	Kriptografi	3
6	Struktur Data	3

Pelatihan yang Pernah Diikuti

No	Jenis Pelatihan	Lembaga	SKS
1	HCIA Datacom	Huawei Indonesia	2022
2	HCIA AI	Huawei Indonesia	2022

B. Biodata Pengusul 2

Nama Lengkap : Novi Dianasari
Jenis Kelamin : Perempuan
NIM : 21060119120039
Tempat, Tanggal Lahir : Kab. Semarang, 7 Februari 2002
Alamat : Jl. Baskoro Raya No. 61
Tembalang Semarang
Email : novidianasari722@gmail.com
Nomor Telepon / HP : 085290662689
Peminatan Konsentrasi : Telekomunikasi

**Kompetensi / Keahlian yang Dimiliki**

No	Mata Kuliah Pilihan yang Diambil	SKS
1	Kecerdasan Buatan	3
2	Pengolahan dan Analisis Sinyal	3
3	Perencanaan Jaringan Telekomunikasi	3
4	Manajemen Jaringan Telekomunikasi	3
5	Perbaikan Kinerja Jaringan	3

Pelatihan yang Pernah Diikuti

No	Jenis Pelatihan	Lembaga	SKS
1	<i>Internet of Things</i>	IoT Telkom	2022

C. Biodata Pengusul 3

Nama Lengkap : Muhammad Khoiril Wafi
Jenis Kelamin : Laki - laki
NIM : 21060119140133
Tempat, Tanggal Lahir : Demak, 4 Maret 2001
Alamat : Jl. Baskoro Raya No.61
Tembalang Semarang
Email : khoirilwafi123@gmail.com
Nomor Telepon / HP : 083116291606
Peminatan Konsentrasi : Teknologi Informasi



Kompetensi / Keahlian yang Dimiliki

No	Mata Kuliah Pilihan yang Diambil	SKS
1	Sistem Operasi	2
2	Pengembangan Aplikasi Perangkat Bergerak	3
3	Interaksi Manusia dan Komputer	2
4	<i>Interface dan Peripheral</i>	2
5	Kriptografi	3
6	Pemrograman Berorientasi Objek	3

Pelatihan yang Pernah Diikuti

No	Jenis Pelatihan	Lembaga	SKS
1	HCIA Datacom	Huawei Indonesia	2022
2	HCIA AI	Huawei Indonesia	2022