|  |  |
| --- | --- |
|  | 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 GedungBerbasis *Internet of Things* | |
|  |  | |
| Jenis Dokumen | DESAIN | |
|  | Catatan: Dokumen ini dikendalikan penyebarannya oleh Dept. Teknik Elektro Undip | |
| Nomor Dokumen | B300-01-TA2223.2.19012 | |
|  |  | |
| Nomor Revisi | 01 | |
|  |  | |
| Nama File | B300-2-TA2223 | |
|  |  | |
| Tanggal Penerbitan | 9 Maret 2023 | |
|  |  | |
| Unit Penerbit | Departemen Teknik Elektro Undip | |
|  |  | |
| Jumlah Halaman | 39 | (termasuk lembar sampul ini) |

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

**DAFTAR ISI**

[1 PENDAHULUAN 4](#_Toc129728206)

[1.1 Ringkasan Isi Dokumen 4](#_Toc129728207)

[1.2 Aplikasi Dokumen 4](#_Toc129728208)

[1.3 Referensi 5](#_Toc129728209)

[1.4 Daftar Singkatan 5](#_Toc129728210)

[2 DESKRIPSI UMUM 6](#_Toc129728211)

[2.1 Definisi, Fungsi, dan Desain Sistem 6](#_Toc129728212)

[2.2 Spesifikasi dan Performa Fungsi 10](#_Toc129728213)

[2.2.1 Diagram Blok *Level* 0 10](#_Toc129728214)

[2.2.2 Diagram Blok *Level* 1 12](#_Toc129728215)

[3 PERANCANGAN SISTEM 15](#_Toc129728216)

[3.1 Desain Subsistem Komunikasi Data Dua Arah dan Perangkat Penguncian yang Mendukung Sistem Keamanan Kunci Pintu Gedung Berbasis IoT 15](#_Toc129728217)

[3.1.1 Modul Mikrokontroler ESP32 15](#_Toc129728218)

[3.2 Desain Subsistem *Internet of Things* dan Sistem Antarmuka *Website* 20](#_Toc129728219)

[3.3 Desain Subsistem Antarmuka Perangkat Bergerak Berbasis Android dengan *Database Firebase* 25](#_Toc129728220)

[4 PENUTUP 35](#_Toc129728221)

**Catatan Sejarah Perbaikan Dokumen**

|  |  |
| --- | --- |
| **Versi, Tgl, Oleh** | **Perbaikan** |
| 01,  9 Maret 2023,  oleh Henric Dhiki Wicaksono, Novi Dianasari, dan Muhammad Khoiril Wafi. | *Draft* dokumen B300 |

**DESAIN**

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

# PENDAHULUAN

## **Ringkasan Isi Dokumen**

Dokumen B300 ini terdiri dari empat bagian utama yaitu deskripsi umum, perancangan alat, perancangan algoritma program, dan perancangan metode analisis. Pada bagian deskripsi umum dijelaskan skenario penggunaan sistem serta spesifikasi dan performa fungsi dari sistem. Pada dokumen ini digambarkan diagram blok dari sistem secara umum sampai dengan diagram blok dari setiap subsistem yang ada.

Pada bagian perancangan alat akan dijelaskan desain dari produk Rancang Bangun Sistem Keamanan Kunci Pintu Gedung Berbasis *Internet of Things* yang terdiri dari desain subsistem komunikasi data dua arah dan perangkat penguncian yang mendukung sistem keamanan kunci pintu gedung berbasis IoT, subsistem *database* dan *serve*r serta keamanan kunci pintu gedung dengan *Access Control,* dan subsistem aplikasi *mobile* sebagai pirantiakses masuk pintu gedung serta *website* untuk mendukung sistem *monitoring* dan *controlling* jarak jauh.

Pada perancangan algoritma program akan membahas penerapan *library* yang digunakan pada sistem. Pada perancangan metode analisis akan membahas analisis terhadap spesifikasi yang direncanakan terhadap produk. Dokumen B300 ini selanjutnya digunakan sebagai acuan dalam pelaksanaan proyek dan pengerjaan produk Rancang Bangun Sistem Keamanan Kunci Pintu Gedung Berbasis *Internet of Things* yang direncanakan.

## **Aplikasi Dokumen**

Dokumen ini digunakan dalam tahapan pengembangan produk Rancang Bangun Sistem Keamanan Kunci Pintu Gedung Berbasis *Internet of Things* untuk:

1. Sebagai tahap desain sistem dalam memenuhi spesifikasi produk yang direncanakan, baik perancangan perangkat keras maupun perangkat lunak.
2. Sebagai acuan dalam proses implementasi dan pengujian proyek pada tahap selanjutnya.
3. Menjadi catatan proses pengerjaan dan revisi yang dilakukan.

Dokumen B300 ini juga diajukan kepada dosen pembimbing tugas akhir dan tim tugas akhir Program Studi Sarjana Teknik Elektro Undip sebagai bahan penilaian tugas akhir.

## **Referensi**

## **Daftar Singkatan**

Tabel 1.1 Daftar Singkatan

|  |  |
| --- | --- |
| **SINGKATAN** | **ARTI** |
| IoT | *Internet of Things* |
| Wi-Fi | *Wireless Fidelity* |
| BLE | *Bluetooth Low Energy* |
| HTTPS | *Hypertext Transfer Protocol Secure* |
| SSL/TLS | *Secure Sockets Layer/Transport Layer Security* |
| QR *Code* | *Quick Response Code* |
| iOS | *iPhone Operating System* |
| ESP | *Espressif* |
| LED | *Light Emitting Diode* |
| SDA | *Serial Data* |
| SCL | *Serial Clock* |
| GPIO | *General Purpose Input Output Pins* |
| DC | *Direct Current* |
| SPI | *Serial Peripheral Interface* |
| UART | *Universal Asynchronous Receiver-Transmitter* |

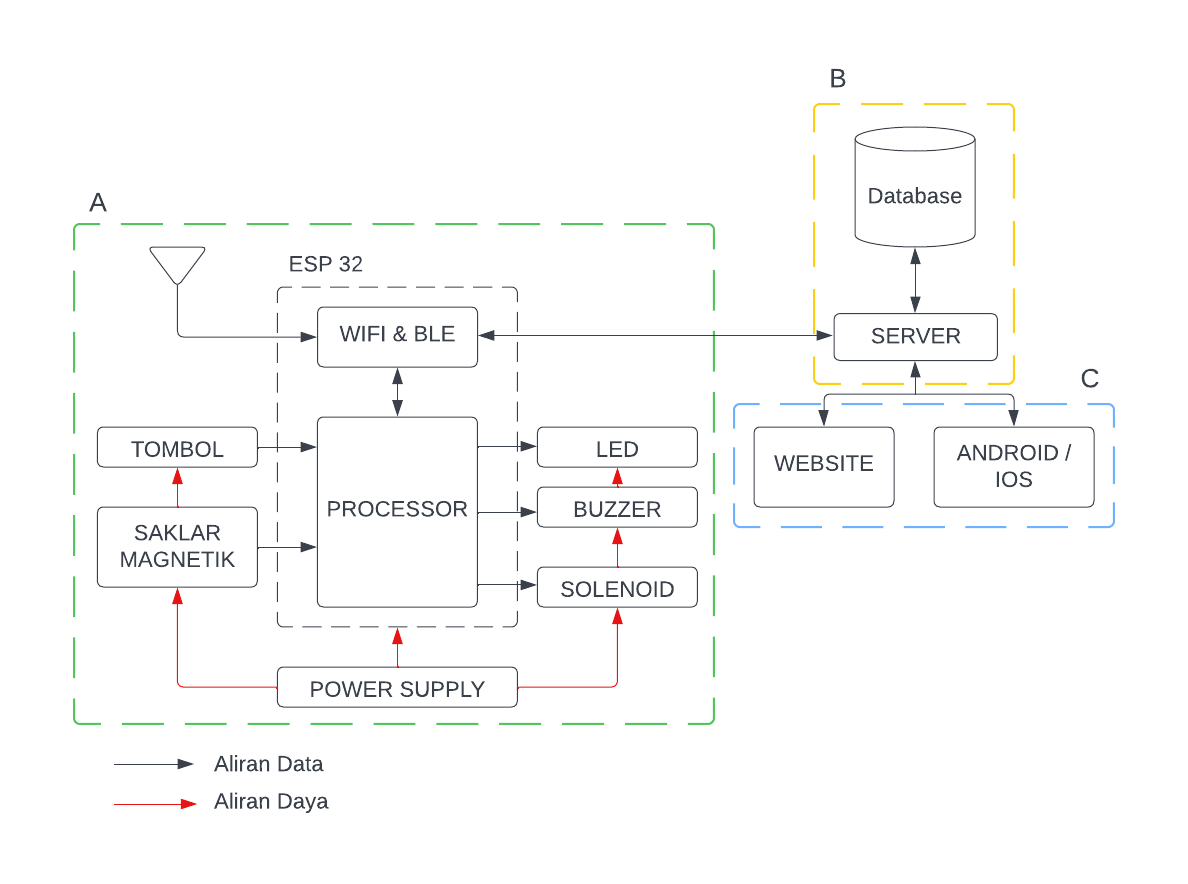
# DESKRIPSI UMUM

## **Definisi, Fungsi, dan Desain Sistem**

Definisi sistem keamanan kunci pintu gedung berbasis *Internet of Things* (IoT) adalah sistem keamanan yang menggunakan teknologi IoT untuk mengontrol akses ke gedung. Sistem ini menghubungkan kunci pintu dan perangkat pintu lainnya ke internet untuk memberikan penggunaan yang lebih aman dan mudah. Fungsi utama sistem keamanan kunci pintu gedung berbasis IoT adalah untuk memberikan akses yang aman dan terkontrol ke gedung atau ruangan tertentu.

Pengguna dapat memanfaatkan teknologi ini untuk mengunci dan membuka kunci pintu menggunakan *smartphone* atau perangkat lainnya yang terhubung ke internet. Sistem ini juga dapat memberikan notifikasi dan laporan aktivitas yang mencurigakan atau tidak terotorisasi, sehingga memperkuat keamanan dan memberikan kontrol yang lebih besar atas akses ke gedung atau ruangan tersebut. Desain sistem keamanan kunci pintu gedung berbasis IoT harus mempertimbangkan beberapa faktor, seperti jenis kunci pintu dan akses ke internet yang tersedia. Sistem ini biasanya terdiri dari perangkat pintu yang terhubung ke internet dan perangkat lunak yang memungkinkan pengguna untuk mengontrol akses. Keamanan sistem ini harus dirancang dengan baik untuk menghindari serangan siber atau pelanggaran keamanan lainnya. Selain itu, sistem ini harus mudah digunakan dan dikelola oleh pengguna agar dapat mengoptimalkan keamanan dan kenyamanan.

Dalam mendukung fungsi utama sistem keamanan kunci pintu gedung berbasis IoT, sistem memiliki beberapa subsistem yang saling mendukung. Diagram blok dari sistem secara umum ditunjukkan pada Gambar 2.1.



**Gambar 2.1** Diagram Blok Sistem Keamanan Kunci Pintu Gedung Berbasis *Internet of Things*

Produk “Rancang BangunSistem Keamanan Kunci Pintu Gedung Berbasis *Internet of Things*” mempunyai 3 subsistem antara lain subsistem komunikasi data dua arah dan perangkat penguncian pintu gedung berbasis IoT yang ditunjukkan pada Gambar 2.1 bagian A, subsistem *server* dan *database* yaitu blok aliran data pada *server* yang ditunjukkan pada Gambar 2.1 bagian B, sertasubsistem *user interface* yaitu blok antarmuka perangkat *mobile* berbasis android dan iOS serta *website* yang ditunjukkan pada Gambar 2.1 bagian C.

Subsistem komunikasi data dua arah dan perangkat penguncian yang mendukung sistem keamanan kunci pintu gedung berbasis IoT ditunjukkan pada Gambar 2.1 bagian A. Untuk mendukung sistem keamanan kunci pintu gedung berbasis IoT, dibutuhkan subsistem komunikasi data dua arah yang dapat mengirim dan menerima informasi antara kunci pintu dan *server* pusat. Berikut ini adalah beberapa bagian dari desain subsistem komunikasi data dua arah.

1. Modul komunikasi: Komponen ini berfungsi sebagai jembatan komunikasi antara kunci pintu dan *server* pusat. Modul komunikasi dapat menggunakan teknologi nirkabel seperti Wi-Fi dan Bluetooth.
2. Protokol komunikasi: Protokol komunikasi HTTPS dapat digunakan untuk mengirimkan dan menerima data antara kunci pintu dan *server* pusat.
3. Keamanan: Untuk menjaga keamanan data, dapat digunakan protokol keamanan seperti SSL/TLS untuk melindungi data yang dikirimkan dari pengintai yang tidak sah.

Dengan subsistem komunikasi data dua arah ini, kunci pintu dapat terhubung ke *server* pusat dan dapat diatur dari jarak jauh. Pengelola juga dapat memantau status kunci pintu dan memberikan akses ke orang lain. Untuk menjalankan mekanisme penguncian yang dilakukan secara elektronik tentunya diperlukan metode penguncian yang didesain sedemikian rupa. Berikut ini merupakan beberapa komponen yang digunakan dalam sistem penguncian.

1. Solenoid: Komponen ini digunakan sebagai pengganti kunci pintu manual dimana solenoid mampu melakukan mekanisme penguncian dengan perintah secara digital.
2. Saklar Magnetik: Komponen ini digunakan untuk mengenali perubahan kondisi pintu apakah sedang terbuka atau tertutup, sehingga sistem mampu membaca perubahan kondisi dari pintu.
3. Mikrokontroler: Komponen ini berfungsi sebagai otak dari sistem. Mikrokontroler akan membaca dan mengirimkan data dari sensor keamanan, motor atau solenoid, antarmuka pengguna, dan modul komunikasi.
4. Modul Komunikasi: perangkat komunikasi seperti WiFi dan Bluetooth digunakan untuk membentuk suatu sistem komunikasi sebagai jalur pertukaran data.

Dengan subsistem perangkat penguncian ini, kunci pintu dapat terhubung ke *server* pusat dan dapat diatur dari jarak jauh. Pengelola juga dapat memantau status kunci pintu dan memberikan akses ke orang lain. Selain itu, dengan sistem keamanan yang kuat, pintu akan lebih aman dari tindakan yang tidak diinginkan.

Subsistem *database* dan *server* serta sistem keamanan kunci pintu gedung dengan *Access Control* ditunjukkan pada Gambar 2.1 bagian B terdiri dari beberapa bagian seperti berikut:

1. *Database*: Sebuah *database* digunakan untuk menyimpan data pengguna, data akses, data kunci pintu dan lain sebagainya. *Database* ini harus diatur dengan baik untuk memastikan keamanan dan keakuratan data.
2. *Server*: Sebuah *server* digunakan untuk mengelola data dan mengontrol akses ke kunci pintu gedung. Semua perangkat penguncian akan terhubung ke *server* pusat untuk melaporkan kondisi pintu atau menerima perintah membuka atau mengunci pintu.
3. *Access Control: Access Control* adalah sebuah mekanisme pengelolaan akses pengguna terhadap beberapa sumber daya seperti ruangan atau lainnya. Dengan menerapkan *access* *control* maka setiap pintu akan mempunyai data siapa saja yang diijinkan untuk mengakses pintu tersebut sehingga pengelolaan akses dapat dilakukan secara aman dan efisien.

Dengan subsistem ini, maka akan membentuk sebuah lingkungan sistem penguncian dengan menggunakan konsep IoT dimana setiap perangkat penguncian akan terhubung ke sebuah server untuk melakukan mekanisme penguncian yang telah disediakan. Subsistem *database* dan *server* juga menjadikan pengelolaan kunci pintu menjadi lebih optimal dengan menggunakan penyimpanan akses secara digital dan terstruktur ditambah dengan adanya metode penjadwalan yang memungkinkan adanya jadwal untuk membuka atau mengunci pintu secara otomatis akan menambah kemudahan dalam pengelolaan kunci pintu. Subsistem ini juga memastikan bahwa data pengguna, data akses, data kunci pintu, dan *log* akses dapat disimpan dan diakses dengan aman dan akurat. Dengan demikian, sistem ini dapat membantu memperkuat keamanan gedung dan memudahkan pengelolaan akses kunci pintu dengan mudah dan efektif.

Subsistem aplikasi *mobile* sebagai piranti akses masuk pintu gedung dan *website* untuk mendukung sistem *monitoring* dan *controlling* jarak jauh ditunjukkan pada Gambar 2.1 bagian C digunakan sebagai antarmuka pengguna dan pengelola untuk menggunakan dan pengelola sistem penguncian secara penuh. Subsistem ini dapat mencakup beberapa komponen seperti berikut:

1. Aplikasi *mobile*: Sebuah aplikasi *mobile* yang dapat diunduh dan diinstal pada perangkat *mobile* seperti *smartphone* atau tablet. Aplikasi ini dapat digunakan untuk melakukan otentikasi pengguna dan membuka pintu gedung.
2. *Website*: Sebuah layanan yang disediakan oleh sistem kunci pintu gedung untuk melakukan pengelolaan sistem penguncian secara menyeluruh seperti menambahkan pintu baru, pengguna baru dan lain sebagainya.
3. Mekanisme Autentikasi: metode yang digunakan untuk memeriksa akses setiap pengguna, metode autentikasi memegang peranan penting untuk memastikan sistem dapat berjalan dengan aman.

Dengan subsistem ini, pengguna dapat menggunakan perangkat *mobile* untuk membuka pintu gedung secara digital dengan menggunakan fitur yang telah disediakan seperti pindai kode QR, pengguna juga dapat melihat riwayat aktifitas yang telah tersimpan. Disamping aplikasi *mobile* yang dapat digunakan oleh pengguna, disediakan pula tampilan *website* yang dapat diguankan pengelolan untuk mengatur sistem penguncian secara menyeluruh serta memantau kondisi pintu secara jarak jauh.

## **Spesifikasi dan Performa Fungsi**

Spesifikasi dari desain produk “Rancang BangunSistem Keamanan Kunci Pintu Gedung Berbasis *Internet of Things*” memiliki fungsi untuk tiap bagian subsistem dari produk. Fungsi tersebut dapat menjelaskan diagram kerja dari diagram blok yang telah dituliskan. Berikut ini akan dijelaskan spesifikasi dari sistem melalui diagram blok di bawah ini.

### **Diagram Blok *Level* 0**

Perangkat Kunci Pintu Gedung

Komunikasi Data Berbasis IoT

Antarmuka *Website* dan Perangkat Bergerak

Gambar 2.2 Diagram Blok *Level* 0 Sistem

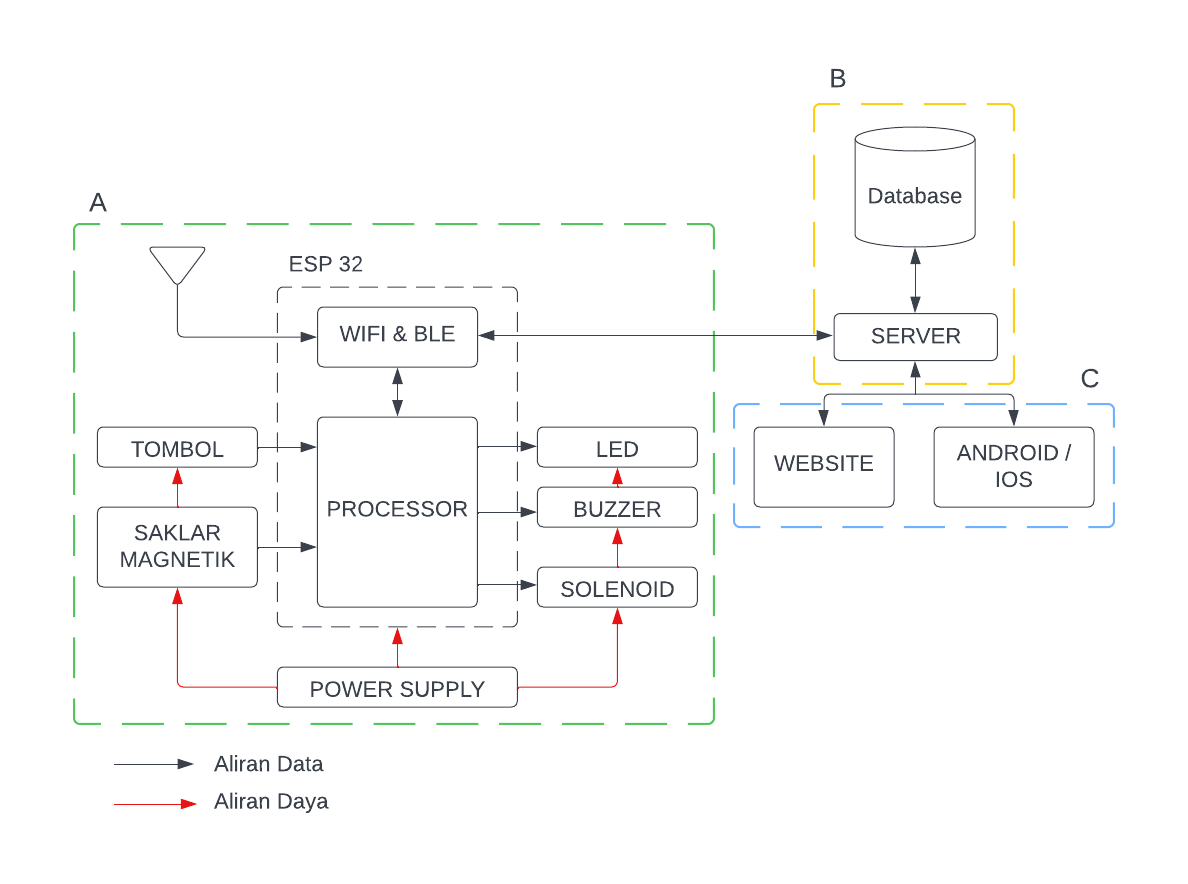
Gambar 2.2 menunjukkan diagram kerja dari produk Tugas Akhir yaitu pada diagram blok *level* 0. Diagram blok *level* 0 memperlihatkan gambaran umum sistemkeamanan kunci pintu gedung berbasis *Internet of Things*. Berdasarkan pada Gambar 2.2 terdapat 3 bagian utama dalam sistem yaitu perangkat kunci pintu gedung, komunikasi data berbasis IoT, serta antarmuka *website* dan perangkat bergerak. Diagram kerja ini dapat dijelaskan dengan rinci sebagai berikut.

Tabel 2.1 Penjelasan Diagram Blok *Level* 0 Sistem

|  |  |
| --- | --- |
| **Blok** | **Penjelasan** |
| Perangkat Kunci Pintu Gedung Berbasis IoT | Perangkat kunci pintu gedung berbasis IoT adalah sebuah solusi otomatisasi pengamanan pintu yang terkoneksi ke jaringan internet dan dapat dikontrol melalui aplikasi *smartphone* atau sistem kontrol akses lainnya. Komponen *input* untuk subsistem perangkat kunci pintu gedung adalah sensor saklar magnetik yang digunakan untuk mendeteksi kondisi pintu. |
| Komunikasi data berbasis IoT | Komunikasi data berbasis IoT pada sistem keamanan kunci pintu gedung berbasis IoT melibatkan pengiriman dan penerimaan data antara berbagai komponen sistem yang terkoneksi ke jaringan internet. Berikut adalah beberapa komponen sistem dan cara komunikasi data antara mereka pada sistem keamanan kunci pintu gedung berbasis IoT:   1. Perangkat Kunci Pintu: Perangkat kunci pintu berkomunikasi dengan *server* melalui jaringan internet. Ketika seseorang telah men-scann QR-*code*, sensor pendeteksi kunci akan mengirimkan sinyal ke perangkat pengendali kunci pintu. Perangkat pengendali kunci pintu akan mengecek apakah kunci tersebut terdaftar di sistem dan apakah pengguna memiliki akses yang sesuai. Jika iya, maka perangkat pengendali kunci pintu akan membuka pintu dan mengirimkan notifikasi ke *server* tentang akses yang berhasil dilakukan. 2. Aplikasi *Smartphone*: Pengguna dapat membuka kunci pintu melalui aplikasi *smartphone* yang terhubung dengan perangkat kunci pintu dan *server*. Dalam aplikasi ini, pengguna dapat melihat riwayat akses yang telah dilakukan. 3. *Website*: Pengguna dapat mengontrol penguncian melalui *website* yang terhubung dengan perangkat kunci pintu dan *server*. Dalam *website* ini, pengguna dapat memberikan akses ke orang lain, mengatur waktu akses, serta melihat riwayat akses yang telah dilakukan. 4. Sistem *Server*: Sistem *server* berfungsi sebagai pusat pengolahan data dan menghubungkan semua komponen sistem. Sistem *server* menerima data dari perangkat kunci pintu dan aplikasi *smartphone* melalui jaringan internet dan menyimpan data tersebut di *database*. Sistem *server* juga memproses permintaan dari pengguna untuk memberikan akses ke orang lain dan mengatur waktu akses. 5. Jaringan Internet: Jaringan internet merupakan infrastruktur yang menghubungkan semua komponen sistem. Jaringan internet memungkinkan komunikasi data antara perangkat kunci pintu, aplikasi *smartphone*, dan sistem *server*. Selain itu, jaringan internet juga memungkinkan sistem keamanan kunci pintu gedung berbasis IoT untuk diakses dan dikontrol dari jarak jauh.   Dalam sistem keamanan kunci pintu gedung berbasis IoT, komunikasi data yang aman dan terenkripsi sangat penting untuk mencegah akses yang tidak sah dan kerentanan sistem terhadap serangan siber. Oleh karena itu, sistem keamanan kunci pintu gedung berbasis IoT harus dirancang dengan baik dan memperhatikan keamanan data dan privasi pengguna. |
| Antarmuka *website* dan perangkat bergerak | Antarmuka pengamatan dan pengendalian dijalankan dalam 3 *platform* yaitu platform Android, iOS, dan *website*. |

### **2.2.2 Diagram Blok *Level* 1**

Diagram blok *level* 1 memperlihatkan penggunaan komponen di dalam blok sistemkeamanan kunci pintu gedung berbasis *Internet of Things*. Diagram blok *level* 1 sistem ditunjukkan pada Gambar 2.3.



Gambar 2.3 Diagram Blok *Level* 1 Sistem

Sistem keamanan kunci pintu gedung berbasis *Internet of Things* terbagi menjadi 3 subsistem seperti yang ditunjukkan pada Gambar 2.3. Subsistem komunikasi data dua arah dan perangkat penguncian yang mendukung sistem keamanan kunci pintu gedung berbasis IoT ditunjukkan pada bagian A. Subsistem *database & serve*r serta sistem keamanan kunci pintu gedung dengan *Access Control* ditunjukkan pada bagian B. Subsistem perangkat *mobile* sebagai pirantiakses masuk pintu gedung dan *website* untuk mendukung sistem *monitoring* dan *controlling* jarak jauh ditunjukkan pada bagian C. Penjelasan diagram blok *level* 1 sistem dijabarkan pada Tabel 2.2.

Tabel 2.2 Penjelasan Diagram Blok *Level* 1 Sistem

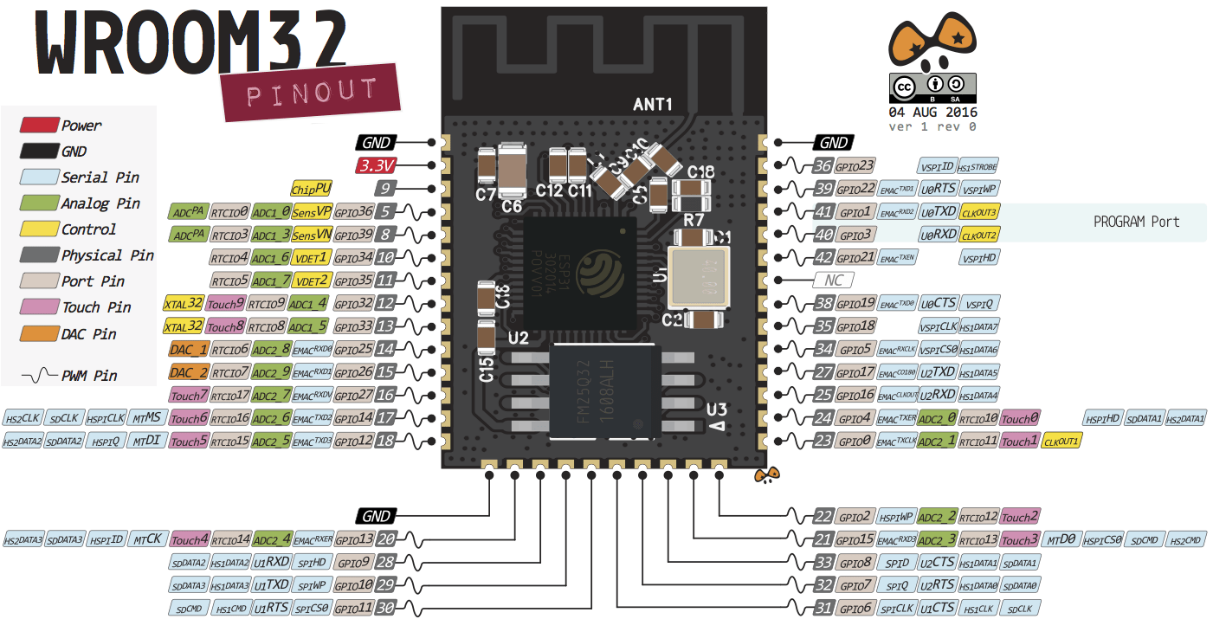
|  |  |
| --- | --- |
| Modul | * Mikrokontroler ESP32: sebagai otak dari sistem yang mengendalikan akses pintu dengan memproses data yang diterima dari sensor dan perangkat lainnya yang terhubung ke jaringan Internet. * Sensor saklar magnetik: untuk mendeteksi status terbuka atau tertutupnya pintu. * Solenoid: untuk mengontrol kunci pintu secara mekanis dan otomatis. * Tombol: sebagai tombol akses. * LED: sebagai indikator status. * *Buzzer*: sebagai peringatan suara. * *Power supply*: untuk menyediakan daya listrik yang diperlukan untuk semua komponen sistem. * *Server*: sebagai pusat kendali yang mengelola dan memonitor semua informasi yang terkait dengan sistem keamanan pintu gedung tersebut. * *Database* : untuk menyimpan dan mengelola data pengguna, informasi akses, dan *log* aktivitas yang terkait dengan penggunaan pintu gedung. * Antarmuka *website* dan Android/IOS : berfungsi sebagai antarmuka pengguna ke sistem keamanan kunci pintu gedung berbasis IoT. |
| Masukan | * Sensor saklar magnetik: Sensor ini terpasang pada pintu dan memberikan informasi tentang apakah pintu terbuka atau tertutup. * Tombol: Pengguna dapat menekan tombol untuk membuka kunci pintu yang berada di dalam ruangan. * Antarmuka *website* dan aplikasi *mobile*: Pengguna dapat menggunakan *website* dan aplikasi *mobile* untuk *monitoring* dan *controlling* sistem keamanan kunci pintu gedung. Antarmuka ini dapat menghubungkan pengguna dengan sistem keamanan gedung dan memberikan akses yang aman dan mudah. |
| Keluaran | * Kunci pintu: Komponen *output* yang paling utama adalah kunci pintu yang membuka atau menutup pintu. Kunci pintu dapat diaktifkan oleh pengguna melalui berbagai cara, seperti sensor saklar magnetik, aplikasi *mobile*. * Layar atau tampilan: Layar atau tampilan dapat digunakan untuk menampilkan informasi terkait dengan sistem keamanan, seperti status pintu (terbuka atau tertutup), nama pengguna yang berhasil masuk, atau peringatan keamanan jika ada upaya masuk yang mencurigakan. * *Buzzer*: *Buzzer* dapat diaktifkan ketika ada upaya masuk yang tidak sah atau ketika pintu terbuka terlalu lama. *Buzzer* ini dapat memberikan peringatan suara atau visual untuk memberitahu pengguna atau pengawas keamanan tentang situasi yang mencurigakan. * Lampu indicator (LED): Lampu indikator dapat digunakan untuk menunjukkan apakah pintu terbuka atau tertutup. Lampu indikator ini dapat membantu pengguna untuk memastikan bahwa pintu telah dikunci dengan benar dan memberikan peringatan jika ada situasi yang mencurigakan. |
| Fungsionalitas | Melakukan pengontrolan kunci pintu di dalam gedung. |

# PERANCANGAN SISTEM

## **Desain Subsistem Komunikasi Data Dua Arah dan Perangkat Penguncian yang Mendukung Sistem Keamanan Kunci Pintu Gedung Berbasis IoT**

### **3.1.1 Modul Mikrokontroler ESP32**

Modul mikrokontroler ESP32 akan menjadi otak dari sistem keamanan kunci pintu gedung. Mikrokontroler ESP32 akan mengontrol operasi sistem secara keseluruhan, termasuk pengolahan data, kontrol akses, dan komunikasi dengan perangkat lain melalui WiFi atau *Bluetooth*. Alokasi penggunaan pin pada mikrokontroler ESP32 terlihat pada Gambar 3.1.



**Gambar 3.1** Gambar Alokasi Penggunaan *Pin* pada Mikrokontroler

Berikut ini adalah alokasi penggunaan pin ESP32 untuk sistem keamanan kunci pintu gedung berbasis IoT:

1. Sensor Saklar Magnetik
   * SDA: GPIO21
   * SCL: GPIO22
2. Solenoid *Lock*
   * PIN: GPIO4
3. *Buzzer*
   * PIN: GPIO5
4. LED Indikator
   * PIN: GPIO2
5. Tombol
   * PIN: GPIO27

Perangkat yang terhubung pada *interface pin* ESP32 dijabarkan sebagai berikut:

1. Sensor saklar magnetik

Sensor saklar magnetik akan dipasang di dekat pintu untuk mendeteksi status terbuka atau tertutupnya pintu, kemudian mikrokontroler ESP32 akan memberikan sinyal ke sistem keamanan.



**Gambar 3.2** Gambar Sensor Saklar Magnetik

Spesifikasi sensor saklar magnetik yang digunakan pada sistem keamanan kunci pintu gedung berbasis IoT dapat bervariasi tergantung pada kebutuhan dan preferensi pengguna. Berikut adalah beberapa spesifikasi umum dari sensor saklar magnetik yang digunakan pada sistem keamanan kunci pintu gedung berbasis IoT:

* Tipe sensor: *Reed switch*
* Tegangan kerja: 5V DC
* Arus kerja: 0,5 A
* Jarak deteksi: 10-15 mm
* Kecepatan respons: kurang dari 0,5 ms
* Tegangan isolasi: 100V DC
* Tahan suhu: -40 hingga 85 derajat Celsius
* Dimensi: sekitar 14 mm x 2 mm x 2 mm

Sensor saklar magnetik juga dapat dilengkapi dengan pelindung logam atau plastik untuk melindungi kontak saklar dari kerusakan atau keausan. Selain itu, beberapa sensor saklar magnetik dapat memiliki opsi untuk mengatur sensitivitas atau kekuatan tarikan yang diperlukan untuk mengaktifkan kontak saklar.

Penting untuk memilih sensor saklar magnetik yang tepat untuk kebutuhan sistem keamanan kunci pintu gedung berbasis IoT. Hal ini dapat meliputi mempertimbangkan jarak deteksi yang diperlukan, kecepatan respons yang diinginkan, dan lingkungan operasi di mana sensor saklar magnetik akan digunakan.

1. Solenoid *Lock*

Solenoid *lock* adalah jenis kunci elektronik yang dapat dibuka dan dikunci dengan menggunakan sinyal listrik. Komponen ini terdiri dari solenoid, motor yang dapat menghasilkan medan magnet, dan mekanisme penguncian.



**Gambar 3.3** Gambar Solenoid *Lock*

Spesifikasi solenoid *lock* dapat bervariasi tergantung pada kebutuhan dan preferensi pengguna. Berikut adalah beberapa spesifikasi umum dari solenoid *lock* yang digunakan pada sistem keamanan kunci pintu gedung berbasis IoT:

* Tegangan kerja: 12V DC
* Arus kerja: 1A
* Waktu respon: kurang dari 1 detik
* Tekanan pengunci: 800-1200 kg
* Tahan suhu: -10 hingga 55 derajat Celsius
* Dimensi: sekitar 70 mm x 30 mm x 20 mm

Solenoid *lock* juga dapat dilengkapi dengan fitur keamanan tambahan seperti alarm yang aktif saat pintu terbuka secara paksa atau perangkat sensor untuk mendeteksi gerakan atau kehadiran orang. Hal ini dapat meningkatkan keamanan dan keandalan sistem kunci pintu gedung berbasis IoT.

1. *Buzzer*

*Buzzer* adalah jenis komponen elektronik yang digunakan untuk menghasilkan suara. Pada sistem keamanan kunci pintu gedung berbasis IoT, *buzzer* digunakan sebagai indikator suara untuk memberikan informasi tentang status pintu, seperti ketika pintu terbuka atau tertutup, atau ketika terjadi masalah pada sistem.



**Gambar 3.4** Gambar *Buzzer*

Spesifikasi *buzzer* dapat bervariasi tergantung pada jenis dan model *buzzer* yang digunakan. Berikut adalah beberapa spesifikasi umum dari *buzzer* yang digunakan pada sistem keamanan kunci pintu gedung berbasis IoT:

* Tegangan kerja: 3-5V DC
* Frekuensi suara: 2-4 kHz
* Kebisingan: 80-90 dB
* Dimensi: sekitar 12 mm x 9 mm x 5 mm
* Jenis: *active buzzer* atau *passive buzzer*

*Buzzer* juga dapat dilengkapi dengan fitur tambahan seperti lampu LED yang dapat menunjukkan status pintu atau sistem dengan warna yang berbeda-beda. Hal ini dapat meningkatkan kegunaan dan kemudahan penggunaan *buzzer* pada sistem keamanan kunci pintu gedung berbasis IoT.

1. LED Indikator

LED Indikator adalah jenis lampu LED yang digunakan sebagai indikator visual pada sistem keamanan kunci pintu gedung berbasis IoT. LED indikator dapat digunakan untuk memberikan informasi tentang status pintu, seperti ketika pintu terbuka atau tertutup, atau ketika terjadi masalah pada sistem.



**Gambar 3.4** Gambar LED indikator

Spesifikasi LED indikator dapat bervariasi tergantung pada jenis dan model LED indikator yang digunakan. Berikut adalah beberapa spesifikasi umum dari LED indikator yang digunakan pada sistem keamanan kunci pintu gedung berbasis IoT:

* Tegangan kerja: 3-5V DC
* Kecerahan cahaya: 50-100 lumen
* Konsumsi daya: 0.1-0.5 watt
* Dimensi: sekitar 5 mm - 10 mm
* Jenis: LED monokromatik atau LED RGB

LED Indikator juga dapat dilengkapi dengan fitur tambahan seperti difuser atau lensa yang dapat menyebar cahaya LED secara merata, sehingga dapat meningkatkan kualitas tampilan visual pada sistem keamanan kunci pintu gedung berbasis IoT.

1. Tombol Buka Pintu

Tombol buka pintu adalah komponen yang digunakan untuk membuka kunci pintu secara manual dan berada di dalam ruangan pada sistem keamanan kunci pintu gedung berbasis IoT. Tombol ini dapat terdiri dari beberapa jenis, seperti tombol tekan, tombol geser, atau tombol magnetik.



**Gambar 3.4** Gambar Tombol Buka Pintu

Spesifikasi tombol buka pintu dapat bervariasi tergantung pada jenis dan model tombol buka pintu yang digunakan. Berikut adalah beberapa spesifikasi umum dari tombol buka pintu yang digunakan pada sistem keamanan kunci pintu gedung berbasis IoT:

* Tegangan kerja: 12-24V DC
* Arus kerja: 0.1-0.5 A
* Dimensi: sekitar 30 mm - 50 mm
* Jenis: tombol tekan, tombol geser, atau tombol magnetik

Tombol buka pintu juga dapat dilengkapi dengan fitur tambahan seperti pelindung air atau pelindung debu, yang dapat meningkatkan daya tahan dan keandalan tombol buka pintu pada sistem keamanan kunci pintu gedung berbasis IoT.

### **3.1.2 Desain Skema Koneksi**

Desain skema koneksi pada sistem keamanan kunci pintu gedung berbasis IoT melibatkan beberapa komponen yang harus dihubungkan satu sama lain untuk memastikan sistem dapat berfungsi dengan baik. Berikut adalah beberapa komponen yang perlu dihubungkan dan skema koneksi yang dapat digunakan:

1. Sensor pintu

Sensor pintu digunakan untuk mendeteksi apakah pintu sudah terkunci atau belum. Sensor ini dapat dihubungkan dengan mikrokontroler menggunakan kabel *jumper* atau komunikasi nirkabel seperti Bluetooth atau Wi-Fi.

1. Mikrokontroler

Mikrokontroler adalah komponen yang bertanggung jawab untuk mengendalikan sistem keamanan kunci pintu gedung. Mikrokontroler dapat menggunakan protokol komunikasi seperti Wi-Fi, *Bluetooth*, atau ZigBee untuk berkomunikasi dengan *server* atau aplikasi *mobile*.

1. Modul Wi-Fi

Modul Wi-Fi digunakan untuk menghubungkan sistem keamanan kunci pintu gedung dengan jaringan internet. Modul ini dapat dihubungkan dengan mikrokontroler menggunakan SPI atau UART *interface*.

1. *Server*

*Server* digunakan untuk mengelola data dari sistem keamanan kunci pintu gedung dan dapat berfungsi sebagai perantara antara aplikasi *mobile* dan sistem. *Server* dapat menggunakan protokol komunikasi seperti HTTP atau MQTT.

1. Aplikasi *mobile*/*Website*

Aplikasi *mobile/Website* digunakan untuk mengontrol sistem keamanan kunci pintu gedung dari jarak jauh. Aplikasi ini dapat terhubung ke *server* menggunakan protokol komunikasi seperti HTTP atau MQTT.

Berikut adalah skema koneksi pada sistem keamanan kunci pintu gedung berbasis IoT:

Sensor pintu --> Mikrokontroler --> Modul Wi-Fi --> *Server* --> Aplikasi *mobile*/*Website*

Dalam skema koneksi ini, sensor pintu terhubung ke mikrokontroler melalui kabel *jumper* atau komunikasi nirkabel. Mikrokontroler terhubung ke modul Wi-Fi menggunakan SPI atau UART *interface*, dan modul Wi-Fi terhubung ke *server* melalui jaringan internet. Aplikasi *mobile*/*Website* terhubung ke *server* melalui jaringan internet dan dapat mengontrol sistem keamanan kunci pintu gedung dari jarak jauh.

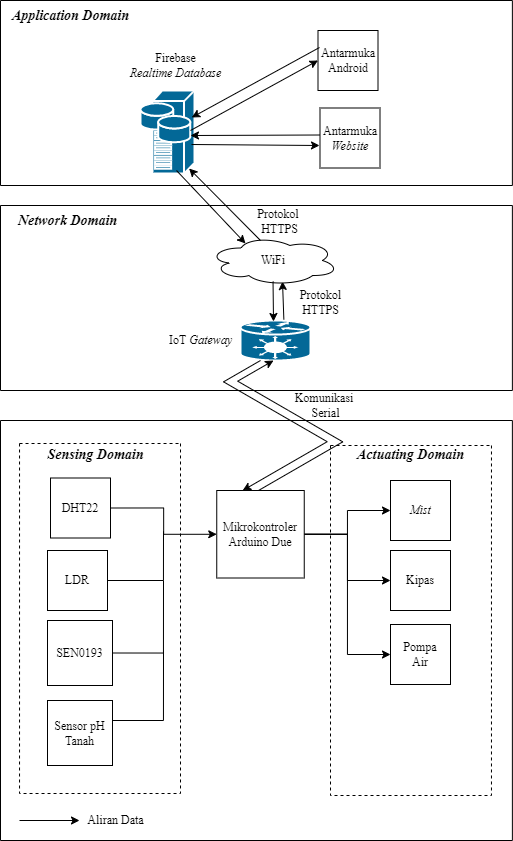
Demikianlah desain skema koneksi pada sistem keamanan kunci pintu gedung berbasis IoT. Dengan menggunakan skema koneksi ini, sistem keamanan kunci pintu gedung dapat berfungsi dengan baik dan memenuhi kebutuhan pengguna.

## **Desain Subsistem Internet *of Things* dan Sistem Antarmuka *Website***

Perancangan komunikasi data berbasis IoT terfokus pada 1 *node* saja. Untuk pengembangan berikutnya, telah dirancang *node* 2 di dalam *database* dan perancangan antarmuka *website* dengan menggunakan sampel data.Perancangan komunikasi data berbasis IoT bertujuan untuk membangun arsitektur komunikasi data agar dapat berjalan 2 arah antara komunikasi *serial* Arduino Due dan IoT *gateway*. *Gateway* tersebut bertindak sebagai perangkat perantara yang menjembatani antara jaringan perangkat M2M dan *remote peer* melalui konektivitas internet[10]. IoT *gateway* tersebutberfungsi untuk menghubungkan sensor – sensor dengan jaringan *cloud* pada internet.

* + 1. **Desain Arsitektur Domain IoT**

Perancangan arsitektur IoT mengadopsi dari perancangan IoT pada penelitian dengan judul *An* IoT *Gateway Centric Architecture to Provide Novel M2M Service* oleh S.K. Datta[10], *A Brief Introduction to* IoT *Gateway* oleh Hao Chen[11] ,dan Standar IEEE *Standard for an Architectural Framework for The* Internet *of Things* (IEEE std 2413TM – 2019)[12]. Pada standar IEEE std 2413TM – 2019 membagi sebuah arsitektur umum IoT menjadi beberapa domain, yaitu domain *application*, domain data, domain *network*, dan domain *device*. Domain *application* menyediakan antarmuka untuk dapat melakukan manajemen *edge* *device*. Domain data menyediakan layanan optimalisasi dan manajemen data. Domain *network* atau jaringan memberikan layanan interkoneksi sistem, pengumpulan data, dan transmisi data. Domain *device* terdiri atas sistem tertanam, seperti robot, aktuator, ataupun *device* lainnya yang berfungsi melakukan operasi.



Gambar 3.9 Arsitektur IoT pada Smart Greenhouse

Pada perancangan arsitektur *domain* IoT pada tugas akhir ini, terabstraksi menjadi 4 domain, yaitu domain *sensing,* domain *actauting*, domain *network*, dan domain *application*. Masing – masing domain memiliki fungsi yang spesifik, seperti yang terlihat pada Gambar 3.9.

Domain *sensing* terdiri dari perangkat pengindera atau sensor yang digunakan untuk mendapatkan data nilai *input* dari sistem jaringan berbasis IoT. Domain *actuating* terdiri dari perangkat yang bertindak sebagai aktuator, meliputi *mist,* pompa air, dan kipas.Sensor yang digunakan meliputi sensor DHT22, LDR, sensor kelembapan tanah SEN0193, dan sensor pH. Sensor DHT22 membaca nilai data suhu dan kelembapan udara di *greenhouse*. Sensor LDR membaca nilai intensitas cahaya di *greenhouse* Perangkat sensor tersebut mengubah nilai yang semulanya dapat berupa besaran fisika menjadi besaran arus atau tegangan yang kemudian diterjemahkan menjadi sebuah data riil yang dapat dibaca oleh manusia. Data yang dikolektifkan oleh domain *sensing* kemudian dikirim ke domain *network*/jaringan melalui komunikasi *serial*.

Domain *network* atau jaringan tersusun dari *network gateway* dan infrastruktur komunikasi, seperti GPRS/EDGE, PSTN, WiFi, 2G/3G, satelit, ataupun yang lain[11]. Adapun koneksi yang digunakan adalah jaringan WiFi 2,4 GHz IEEE 802.11n. Pada perancangan, digunakan mikrokontroler ESP8266 NodeMCU sebagai IoT *gateway*. ESP8266 memperoleh data dari domain *sensing* melalui komunikasi *serial* dengan mikrokontroler Arduino Due. Kemudian ESP8266 mengirimkan data ke internet melalui jaringan WiFi. Proses pengiriman data menggunakan protokol HTTPS. Protokol HTTPS merupakan protokol komunikasi data yang disediakan oleh Firebase untuk dapat berkomunikasi dengan *server realtime database.* Data yang dikirimkan oleh ESP8266 akan disimpan di dalam Firebase *realtime database.* Tujuan utama dari domain jaringan adalah untuk mentransmisikan data yang dikolektif oleh domain *sensing* ke perangkat *remote*, seperti *server database*[11].

Domain aplikasi merupakan domain yang memiliki responsibilitas untuk melakukan pemrosesan data dan penyedia layanan[11]. Data yang ditransmisikan oleh domain jaringan tersebut akan disimpan di dalam *server database* sebagai manajemen data. *Server database* yang digunakan adalah Firebase *realtime database*. Penggunaan Firebase *realtime database* dimaksudkan agar data dapat tersinkronisasi secara otomatis pada setiap *client*, sehingga data yang diperoleh perangkat Android dan *website* dapat sama. Jika terdapat perubahan data pada *database*, maka aplikasi *client* yang terhubung dapat memperoleh perubahan pada saat yang sama (*realtime*).Data di dalam *database* kemudian ditampilkan pada antarmuka aplikasi berbasis *website* dan Android.

* + 1. **Desain Antarmuka *Website***

Perangkat lunak *website* diperlukan untuk mengawasi dan mengendalikan variabel – variabel yang mempengaruhi metabolisme tanaman kangkung agar pertumbuhan dapat optimal. Secara umum, perangkat lunak *website* untuk sistem pemantauan dan pengendalian memiliki fungsi – fungsi sebagai berikut :

1. Autentikasi dan Otorisasi

Autentikasi berfungsi untuk melakukan proses verifikasi identitas pengguna yang mencoba memasuki sistem. Fungsi otorisasi berperan dalam melakukan pengecekan hak akses seorang pengguna dalam mengakses beberapa fitur di dalam sistem.

1. Komunikasi

Antarmuka *website* sistem pemantauan dan pengendalian melakukan komunikasi dengan *sensing domain* melalui jaringan internet dengan menggunakan beberapa metode standar HTTPuntuk melakukan :

1. Pengirimandata *flag* aktuator ke *database* untuk mengontrol *mode* dan aktuator.
2. Pengunduhandata pembacaan sensor dari *database*.
3. Pengelolaan data pengukuran sensor

Antarmuka *website* memproses dan menampilkan data pembacaan sensor dari masing – masing *node* yang disimpan di dalam *database* dalam bentuk tabel, numeris, maupun grafik. Dalam perancangan IoT, hanya digunakan satu *node* saja, namun dalam antarmuka *website*, akan berinteraksi dengan 2 *node*, *node* 1 merupakan *node* pada perancangan IoT, sedangkan *node* 2 merupakan *node* yang berisi sampel data yang digunakan sebagai referensi pengembangan berikutnya.

Antarmuka sistem pengamatan dan pengendalian *smart greenhouse* berbasis *website* memiliki beberapa aktor yang berkontribusi pada sistem. Setiap aktor tersebut memiliki hak akses masing – masing.

1. Administrator (Admin)

Admin memiliki hak akses yang mencakup keseluruhan hak akses yang ada pada sistem. Admin memiliki hak untuk melakukan pengamatan dan pengendalian *smart greenhouse*, serta mengelola *user* yang terdaftar di dalam sistem.

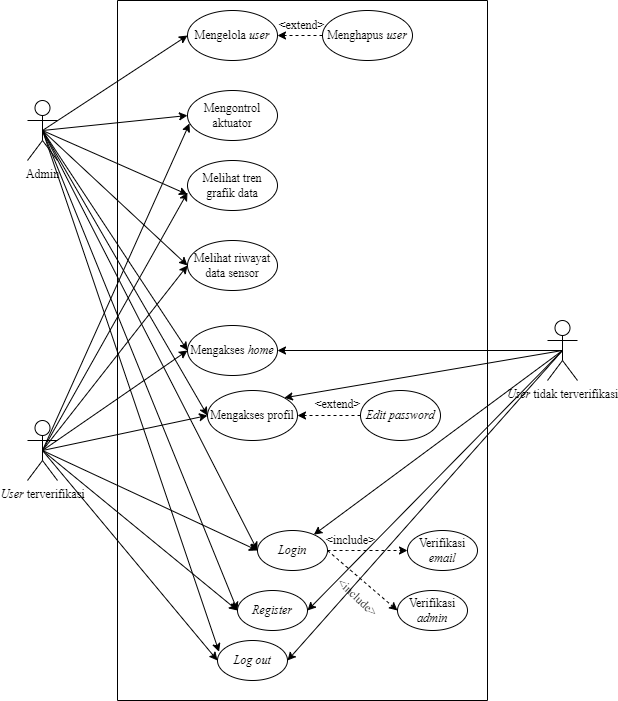
1. *User* Terverifikasi

*User* terverifikasi merupakan *user* yang telah melakukan verifikasi alamat *email* saat melakukan *login* untuk pertama kali setelah registrasi. *User* terverifikasi dapat melakukan seluruh fungsi pengamatan dan pengendalian pada sistem.

1. *User* Tidak Terverifikasi

*User* tidak terverifikasi merupakan *user* yang belum melakukan verifikasi alamat *email* saat melakukan *login* untuk pertama kali setelah registrasi. Proses verifikasi *email* bertujuan untuk melakukan validasi bahwa alamat *email* yang digunakan adalah asli. Untuk mencegah tindakan yang berpotensi merusak sistem, maupun serangan dari *bot*, maka u*ser* yangtidak terverifikasi hanya dapat mengakses halaman awal (*home*) pada sistem.

Diagram *use case website* sistem pengamatan dan pengendalian *smart greenhouse* ditunjukkan oleh Gambar 3.10.

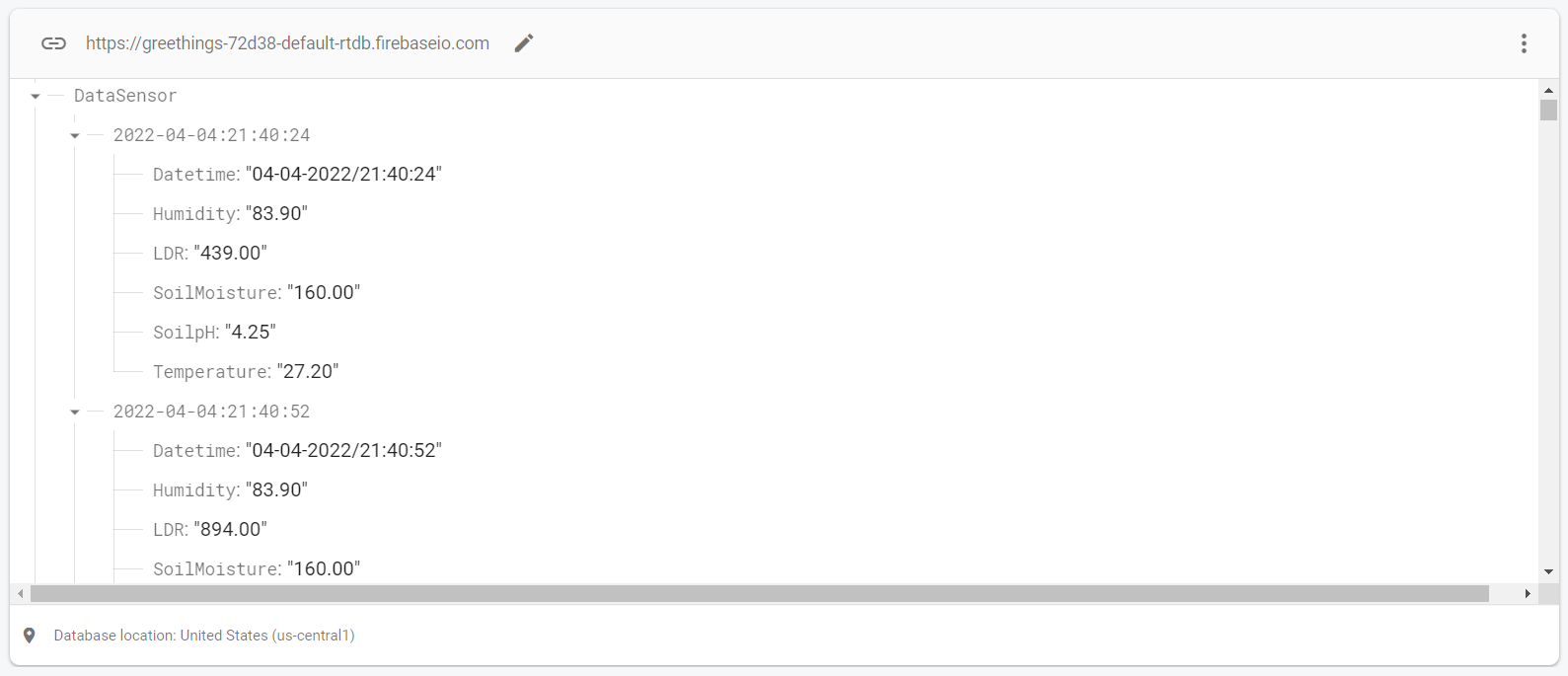


Gambar 3.10 Diagram *Use* *Case* *Website* Sistem Pengamatan dan Pengendalian *Smart* *Greenhouse*

## **Desain Subsistem Antarmuka Perangkat Bergerak Berbasis Android dengan Database Firebase**

* + 1. **Perancangan Basis Data**

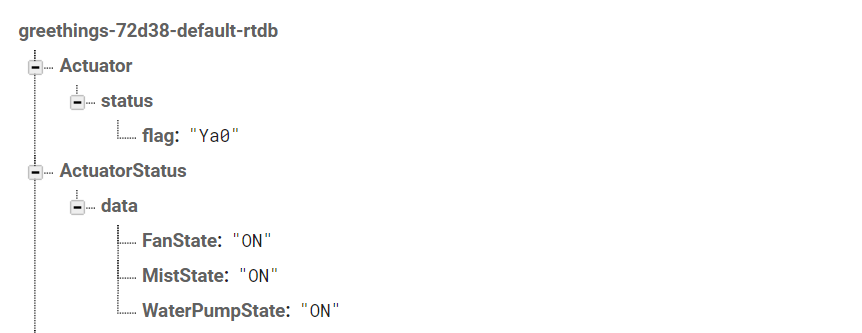
Pada sistem *smart greenhouse* ini menggunakan basis data NoSQL Firebase sebagai penyimpanan data dan bersifat *real time*. Berikut ini struktur data untuk penyimpanan tangkapan data kondisi *greenhouse* yang dikirimkan dari *microcontroller*.



Gambar 3.11 Struktur Basis Data

Pada Gambar 3.11 menunjukkan bahwa terdapat beberapa data yang dikirimkan dari *microcontroller*, yaitu *Datetime, Humidity, SoilMoisture, SoilpH,* dan *Temperature.* *Key Datetime* digunakan untuk waktu dan penanggalan, *Humidity* untuk menyimpan data kelembaban, *SoilMoisture* digunakan untuk menyimpan kelembapan tanah, *SoilpH* untuk menyimpan pH tanah, dan *Temperature* untuk menyimpan data suhu udara di dalam *greenhouse*.

*Real* *time* *database* ini selain digunakan untuk menyimpan tangkapan data kondisi *greenhouse*, juga digunakan untuk menyimpan status dari *actuator*. Berikut struktur *real* *time* *database* untuk menyimpan status *actuator*.



Gambar 3.12 Struktur Penyimpanan *Flag* Aktuator

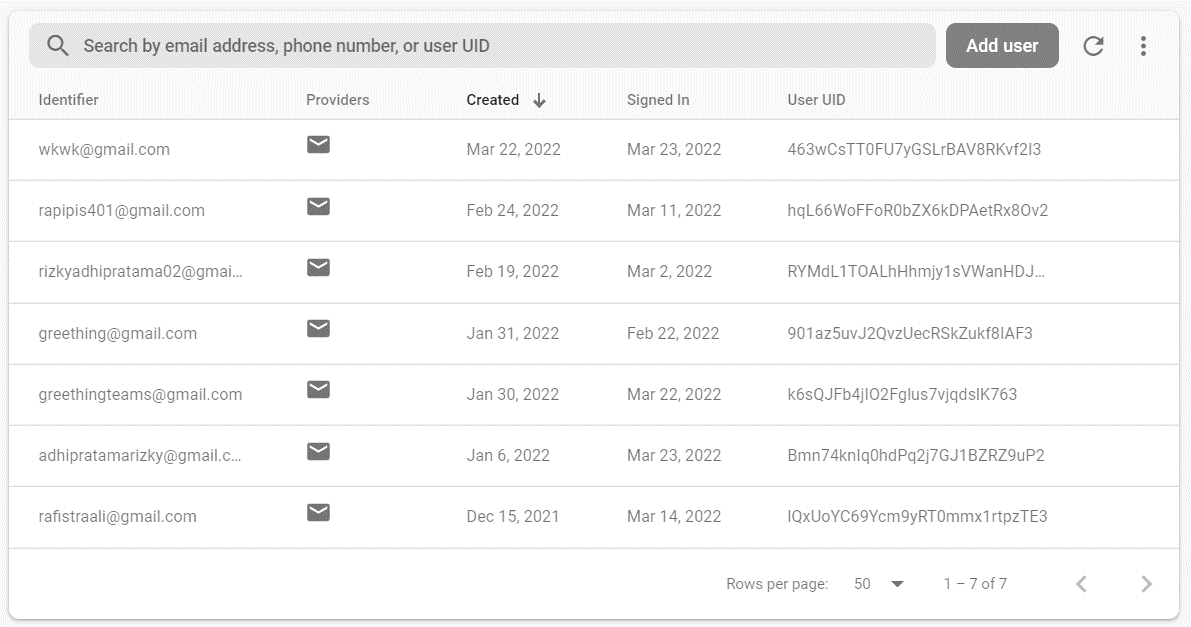
Pada Gambar 3.12, terdapat dua *child* untuk penyimpanan status *actuator*. *Child Actuator* digunakan untuk menyimpan perintah dari aplikasi Android dan web. Tabel 3.2 merupakan perintah-perintah yang digunakan dalam mengendalikan *actuator*.

Tabel 3.2 Perintah dalam Mengendalikan Actuator

|  |  |
| --- | --- |
| Kode Perintah | Perintah |
| Ya0 | Mode Otomatis |
| Ya110 | Mode manual *water* *pump* *state* ON |
| Ya111 | Mode manual *water pump state* OFf |
| Ya120 | Mode manual *mist maker state* ON |
| Ya121 | Mode manual *mist maker state* OFF |
| Ya130 | Mode manual kipas *state* ON |
| Ya131 | Mode manual kipas *state* OFF |

Pada Tabel 3.2, terdapat juga *child ActuatorStatus* yang digunakan untuk mengetahui kondisi *Actuator* saat ini, yang mana nanti akan ditampilkan di dalam aplikasi Android dan web.

Pada sistem aplikasi *smart greenhouse* dilengkapi dengan fitur autentikasi dengan memanfaatkan fitur *Firebase Authentication*. Fitur ini digunakan sebagai keamanan dalam penggunaan aplikasi dimana pengguna diwajibkan *login* terlebih dahulu ketika menggunakan aplikasi. Pada Firebase Authentication ini terdapat table *users* di mana isinya adalah daftar akun pengguna yang nantinya digunakan untuk melakukan *login* pada aplikasi. Berikut ini merupakan tampilan dari tabel *users* di Firebase *Authentication*.

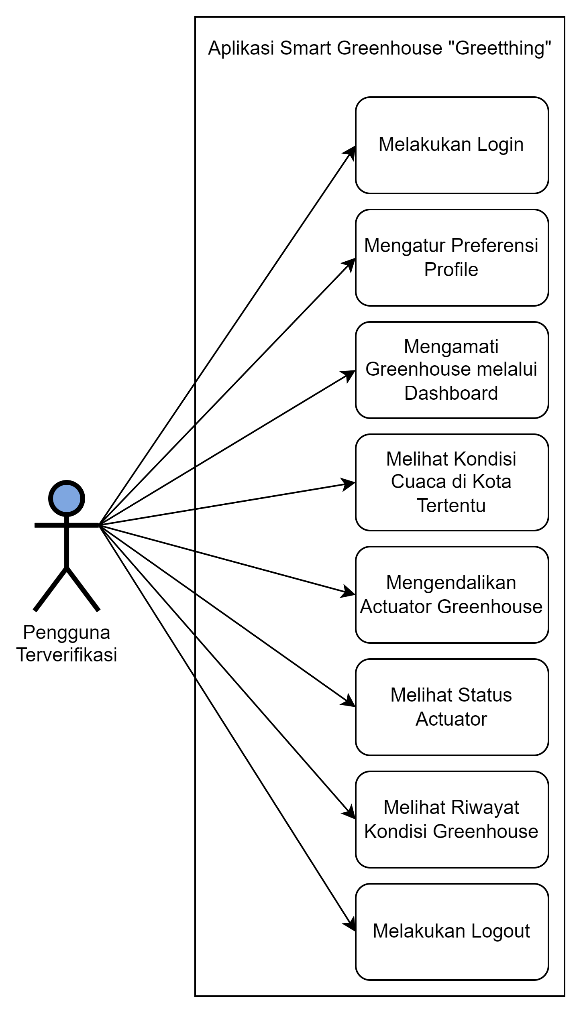


Gambar 3.13 Daftar *User* dalam Firebase *Authentication*

Dari Gambar 3.13 dapat dilihat bahwa tabel users terdiri dari *Identifier*, *providers*, C*reated*, *Signed* *In*, dan *User* UID. *Identifier* merupakan e-mail dari pengguna, *provider* merupakan metode *login* yang digunakan, *Created* menjelaskan kapan *user* dibuat, *Sign* *In* menjelaskan kapan terakhir kali *users* melakukan *login*, dan *User* UID merupakan ID dari tiap *users*. Tabel ini nantinya digunakan oleh sistem untuk memverifikasi alamat email dan *password* pengguna saat melakukan *login*.

* + 1. **Perancangan Aplikasi Sistem Keamanan Kunci Pintu Gedung Berbasis *Internet of Things***
       1. **Diagram *Use Case***

Diagram *use case* menggambarkan tindakan yang dapat dilakukan pengguna dengan sistem. Diagram ini lebih memfokuskan pada fungsi-fungsi sistem dari sudut pandang orang luar, yang dalam hal ini adalah pengguna aplikasi.



Gambar 3.14 *Activity* Diagram Aplikasi *Smart* *Greenhouse*

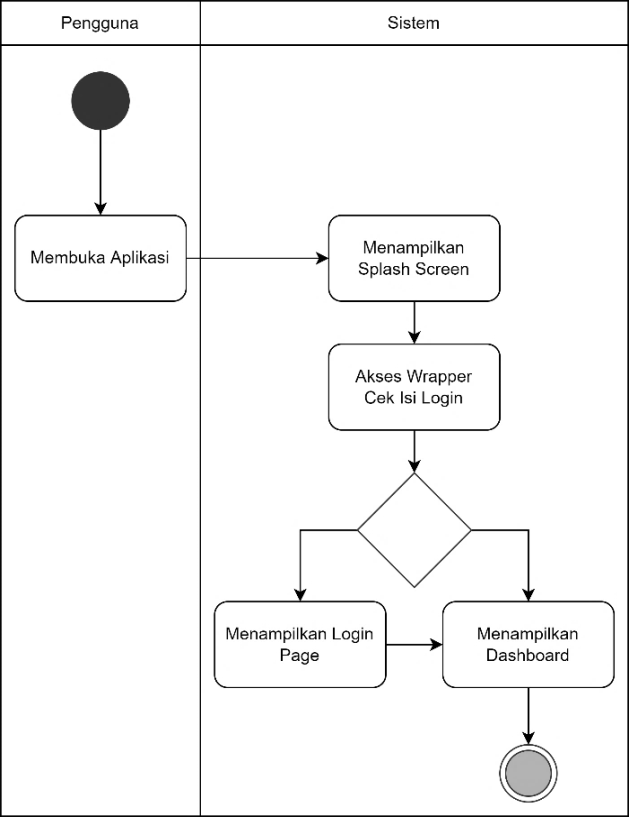
Gambar 3.14 menunjukkan fitur-fitur yang dapat diakses oleh pengguna yang telah terverifikasi. Pengguna dapat menggunakan fitur melakukan *login* akun, mengatur preferensi *profile*, mengamati kondisi *greenhouse* melalui *dashboard*, melihat kondisi cuaca di kota tertentu, mengendalikan *actuator* *greenhouse*, melihat riwayat kondisi *greenhouse*, dan melakukan *logout*.

* + - 1. **Diagram Aktivitas**

Diagram aktivitas digunakan untuk menunjukkan bagaimana aplikasi mengalir dari satu aktivitas ke aktivitas berikutnya. Logika prosedural dan alur kerja dari sistem yang dibuat digambarkan dalam diagram aktivitas. Selanjutnya, diagram aktivitas dapat digunakan untuk menggambarkan operasi paralel yang terjadi dalam beberapa eksekusi. Untuk memisahkan tanggung jawab aktivitas setiap item, diagram aktivitas dapat dibagi menjadi objek *swimlane*.

1. Diagram Aktivitas Menu Utama

Saat pengguna pertama kali menggunakan aplikasi ditunjukkan pada diagram aktivitas ini. *Splash screen* dan menu utama akan terlihat oleh pengguna. Gambar 3.15 menunjukkan diagram aktivitas menu utama.

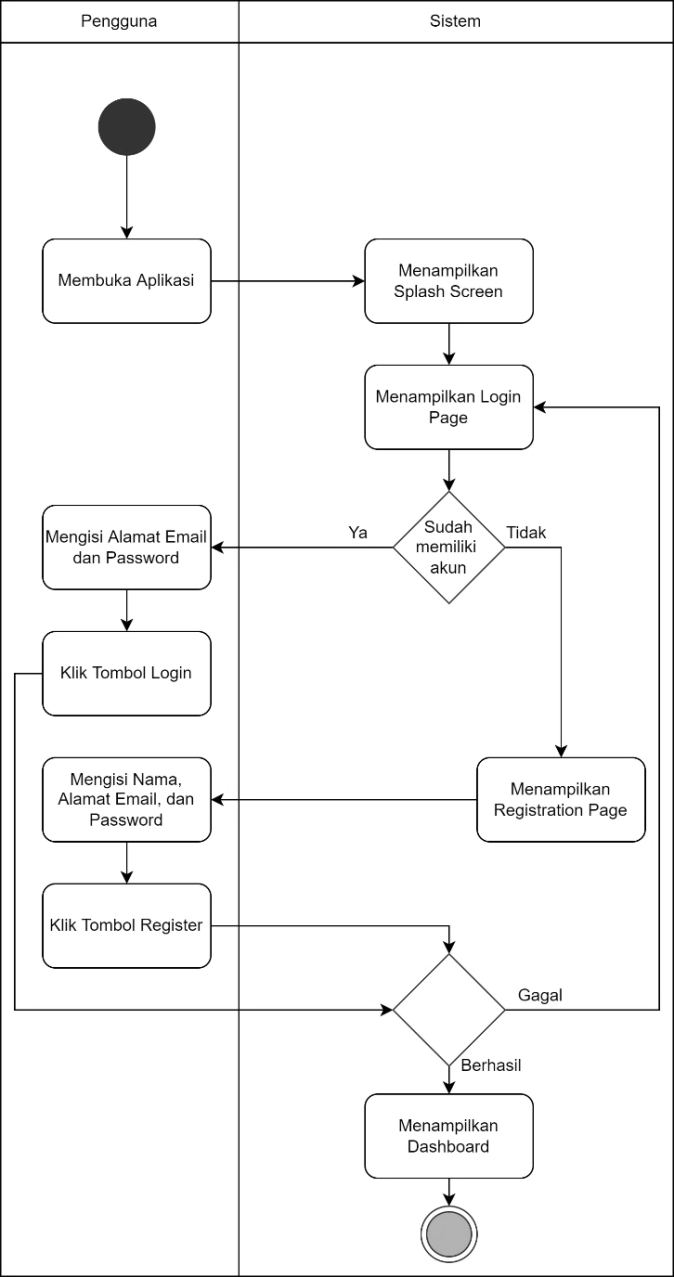


Gambar 3.15 Diagram Aktivitas Menu Utama

Gambar 3.15 memperlihatkan diagram aktivitasmenu utama ketika pengguna memulai menggunakan aplikasi. Setelah aplikasi terbuka, sistem akan menampilkan *activity splash screen*. Setelah itu sistem akan mengecek apakah pengguna sudah pernah login di perangkat yang sama apa belum. Jika pengguna belum melakukan *login*, sistem akan mengarahkan ke *activity* *login*, sebaliknya jika pengguna sebelumnya sudah *login*, sistem akan langsung mengarahkan pengguna pada *main activity* lebih tepatnya *fragment dashboard*.

1. Diagram Aktivitas Menu *Login*

Diagram aktivitas ini menunjukkan aktivitas pengguna saat pertama kali memulai aplikasi dan melakukan *login*. Pengguna akan melihat tampilan *splash* *screen* dan menu *login*. Diagram aktivitas menu *login* ditunjukkan pada Gambar 3.16.

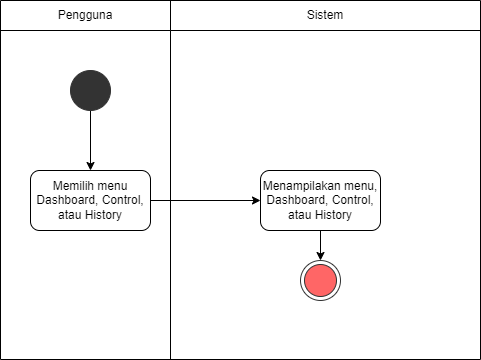


Gambar 3.16 *Activity* Diagram Menu *Login*

Gambar 3.16 memperlihatkan diagram aktivitasuntuk *login* dan *registration*. Setelah *splash screen* maka akan tampil *activity login*. Jika pengguna sudah memiliki akun maka pengguna bisa langsung mengisi alamat *email* dan *password*, setelah sistem mengautentikasi, jika salah akan tetap di *activity* *login* jika benar sistem akan mengarahkan ke *fragment* *dashboard* pada main *activity*. Jika pengguna belum memiliki akun, maka pengguna harus membuat akun terlebih dahulu, dengan menekan tombol registrasi. Pada *activity* *registration* pengguna harus memasukkan nama lengkap, email, dan *password*. Setelah berhasil registrasi maka pengguna akan diarahkan ke *fragment* *dashboard* pada main *activity*.

1. Diagram Aktivitas *Main Activity*

Diagram aktivitas ini menggambarkan aktivitas pengguna saat berada di *Main Activity*. Pengguna akan dihadapkan pada *fragment* *dashboard* pertama kalinya, kemudian dapat berpindah ke *fragment* lainnya, yaitu *fragment* *control* atau *fragment* *history*. Diagram aktivitas pada main activity terdapat pada Gambar 3.17.

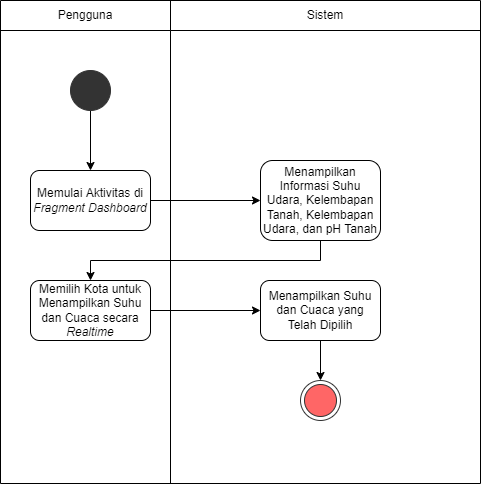


Gambar 3.17 Diagram Aktivitas *Main* *Activity*

Gambar 3.17 memperlihattkan gambar diagram aktivitas *main activity* untuk mengguna yang sedang melakukan pengamatan dan pengendalian. Pada *activity* ini pengguna dapat menuju ke tiga *fragment* yaitu *dashboard*, *control*, dan *history* yang masing-masing akan dijelaskan pada poin berikutnya.

1. Diagram Activitas *Main Activity* *Dashboard Fragment*

Diagram aktivitas ini menggambarkan aktivitas pengguna saat berada di *fragment* *dashboard*. Diagram aktivitas pada *fragment dashboard* dapat dilihat pada Gambar 3.18.

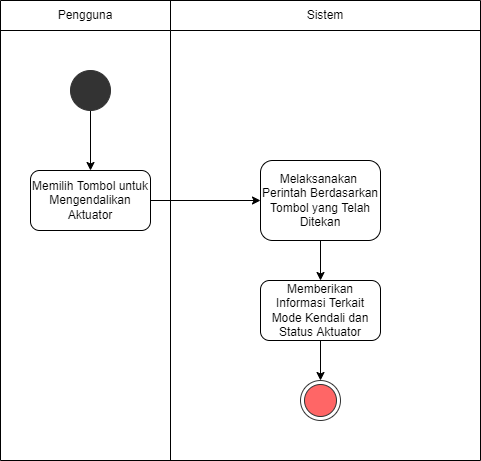


Gambar 3.18 Diagram Aktivitas pada *Fragment* *Dashboard*

Gambar 3.18 memperlihatkan diagram aktivitaspada *fragment* *dashboard*. Pada *fragment* ini pengguna akan ditampilkan informasi berupa suhu udara, kelembapan tanah, kelembapan udara, dan pH tanah di *greenhouse*. Pengguna dapat memilih kota tertentu untuk pembanding suhu dan cuaca pada *greenhouse*.

1. Diagram Aktivitas *Main Activity Control Fragment*

Diagram aktivitas ini menggambarkan aktivitas pengguna saat berada di *fragment* *control* untuk melakukan pengendalian *actuator*. Pengguna akan melihat tampilan beberapa tombol yang digunakan untuk mengendalikan *actuator*. Diagram aktivitas *fragment* *control* ditunjukkan pada Gambar 3.19.

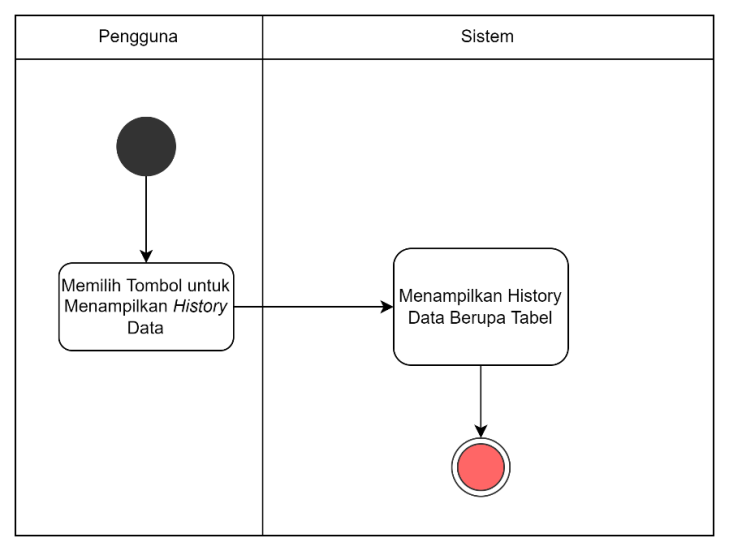


Gambar 3.19 Diagram Aktivitas pada *Fragment* *Control*

Pada *Fragment* *Control* terdapat beberapa tombol untuk mengendalikan aktuator di *greenhouse*. Yang pertama terdapat tombol mode kendali untuk memilih kendali secara otomatis atau secara manual, kemudian ada tombol-tombol ON/OFF dari tiap *actuator* ketika mode kendali dipilih mode manual.

1. Diagram Aktivitas *Main Activity History Fragment*

Diagram aktivitas ini menggambarkan aktivitas pengguna saat berada di *fragment* *history*. Diagram aktivitas *fragment* *history* ditunjukkan pada Gambar 3.20.



Gambar 3.20 Diagram Aktivitas pada *Fragment* *History*

Gambar 3.20 memperlihatkan diagram aktivitas pada *fragment* *history*. Pengguna dapat memilih tombol untuk menampilkan riwayat data berupa tabel.

1. **PENUTUP**

Dokumen B300 menjelaskan desain perancangan sistem keamanan kunci pintu gedung berbasis *internet of things* yang meliputi perancangan subsistem komunikasi data dua arah dan perangkat penguncian yang mendukung sistem keamanan kunci pintu gedung berbasis IoT, perancangan subsistem *database & serve*r serta keamanan kunci pintu gedung dengan *Access Control,* dan perancangan subsistem perangkat *mobile* sebagai pirantiakses masuk pintu gedung serta *website* untuk mendukung sistem *monitoring* dan *controlling* jarak jauh. Hasil perancangan desain sistem keamanan kunci pintu gedung berbasis *internet of things* akan menjadi acuan dalam pengimplementasiannya.