

Implementasi Keamanan Rumah Cerdas Menggunakan *Internet of Things* dan *Biometric Sistem*

Implementation of Smart Home Security Using Internet of Things and Biometric Systems

Anastasia Mude¹, Leonardus Benediktus Finansius Mando²
Universitas Flores, Indonesia

Informasi Artikel

Genesis Artikel:

Diterima, 4 September 2021
Direvisi, 16 September 2021
Disetujui, 18 Oktober 2021

Kata Kunci:

Internet of Things
Sistem Keamanan Pintu
Biometric Sistem
Mikrokontroler

Keywords:

Internet of Things
Door lock security system
Biometric system
Microcontroller

ABSTRAK

Pintu adalah salah satu fitur pertahanan pertama untuk menjaga keamanan fisik rumah. Dalam sebuah rumah, pintu memiliki peranan penting dalam masalah keamanan. Terkadang kelalaian penghuni rumah dalam menjaga keamanan rumah membuat keamanan pintu rumah menjadi tidak terkontrol seperti, lupa mengunci pintu saat keluar rumah, kehilangan kunci rumah, dan mungkin lupa apakah sudah mengunci pintu atau belum. Kelemahan keamanan lainnya adalah mudahnya pencuri membobol pintu rumah yang masih menggunakan kunci manual. Dari masalah-masalah tersebut dalam penelitian ini mengusulkan sebuah sistem keamanan pintu rumah menggunakan sistem kontrol *biometric* dan sistem kontrol manual berbasis *Internet of Things* untuk mengendalikan pintu dan meningkatkan keamanan rumah. Dalam penelitian ini menerapkan dua mekanisme pengontrolan pintu rumah yaitu dengan memanfaatkan sensor sidik jari sebagai sistem kontrol *biometric*, dan sistem kontrol manual berbasis *Internet of Things* untuk langkah alternatif, apabila terdapat masalah dengan kondisi fisik jari penghuni rumah. Metode implementasi perancangan sistem menggunakan mikrokontroler NodeMCU ESP8266 dengan bahasa pemrograman Arduino dan aplikasi mobile blynk berbasis android. Hasil evaluasi menunjukkan bahwa adanya integrasi yang baik antara kontrol menggunakan sensor sidik jari dan kontrol manual berbasis *Internet of Things* dimana kedua kontrol melakukan respon membuka dan mengunci pintu rumah selama 5 detik sehingga tidak ada celah kelalaian yang dapat berdampak buruk bagi keamanan rumah.

ABSTRACT

Doors are one of the first defensive features to keep a home physically safe. In a house, the door has an important role in security issues. Sometimes the negligence of the occupants of the house in maintaining the security of the house makes the security of the door of the house uncontrollable, such as forgetting to lock the door when leaving the house, losing the house key, and perhaps forgetting whether or not to lock the door. Another security weakness is that it is easy for thieves to break into house doors that still use manual keys. From these problems, this study proposes a home door security system using a biometric control system and an Internet of Things-based manual control system to control doors and improve home security. In this study, two mechanisms are applied to control the door of the house by utilizing a fingerprint sensor as a biometric control system, and an Internet of Things-based manual control system for alternative steps, if there are problems with the physical condition of the residents' fingers. System design implementation method using the NodeMCU ESP8266 microcontroller with the Arduino programming language and the android-based blynk mobile application. The evaluation results show that there is good integration between controls using fingerprint sensors and Internet of Things-based manual controls where both controls respond to open and lock the door of the house for 5 seconds so that there is no loophole of negligence that can have a bad impact on home security.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Penulis Korespondensi:

Anastasia Mude,
Program Studi Sistem Informasi,
Universitas Flores,
Email: annmude87@gmail.com

1. PENDAHULUAN

Pintu adalah salah satu fitur pertahanan pertama untuk menjaga keamanan fisik rumah. Jika pintu rumah dapat dibuka dengan mudah, pencuri dapat dengan mudah masuk dan mencuri isi rumah. Pada awalnya, pintu hanya mencakup kunci fisik untuk mengunci atau membuka pintu namun kemudian dengan kemajuan teknologi telah dibuat inovasi pintu yang lebih modern yaitu pintu digital yang dapat mengunci atau membuka kunci pintu tanpa memerlukan kunci fisik. Untuk selalu menjaga keamanan rumah, penghuni rumah akan selalu mengunci pintu baik saat keluar rumah, maupun saat beristirahat di dalam rumah, namun terkadang penghuni rumah lupa mengunci pintu karena terburu-buru saat keluar rumah, atau mereka mungkin ragu apakah mereka telah mengunci pintu atau tidak. Ini adalah salah satu faktor yang dapat menjadi ancaman bagi keamanan rumah, untuk meningkatkan sistem keamanan sebuah rumah, salah satunya adalah dengan menerapkan sistem keamanan rumah berbasis *Internet of Things* (IoT).

Internet of Things (IoT) terus berkembang pada konsep lingkungan cerdas dan membuka jalan bagi penerapan berbagai aplikasi dengan dampak signifikan pada banyak bidang kehidupan sehari-hari di masa depan [1]. Beberapa pemanfaatan IoT dalam mendukung kemajuan industri 4.0 [2] diantaranya dalam bidang logistik [3], sistem transportasi cerdas [4], efisiensi energi rumah pintar [5], sistem keamanan rumah pintar [6], sistem pembersihan cerdas [7] dan *e-health* [8]. Dari beberapa contoh pengaplikasian IoT tersebut memungkinkan di mana paradigma baru ini akan memainkan peran utama di masa depan. Untuk itu penelitian ini memungkinkan IoT dapat diterapkan dalam menjaga keamanan rumah lewat sistem penguncian rumah menggunakan sidik jari dan kontrol jarak jauh. IoT memanfaatkan kemampuan sensor seperti sidik jari sebagai input untuk mendeteksi sidik jari pemilik rumah. IoT juga memanfaatkan kemampuan alat seperti mikrokontroler yang dapat mengontrol perangkat lain seperti saklar otomatis ataupun kunci pintu digital yang dapat mengunci atau membuka kunci tanpa memerlukan perangkat fisik. Sistem komunikasi IoT dalam penelitian ini juga menggunakan sistem komunikasi cloud, dimana penghuni dapat membuka dan mengunci pintu rumah dari jarak jauh menggunakan *smartphone*.

Beberapa penelitian telah dilakukan tentang pemanfaatan IoT dalam peningkatan keamanan rumah. Penelitian yang dilakukan Surantha menggunakan IoT dengan memanfaatkan beberapa sensor untuk mengantisipasi celah keamanan dalam rumah. Penerapan sensor gerak digunakan untuk mengantisipasi gerakan dalam rumah menggunakan Raspberry Pi 3 dan Arduino [9]. Tujuan penerapan sensor gerak ini adalah untuk mengantisipasi apabila rumah akan ditinggalkan atau rumah dalam keadaan kosong sensor gerak akan diaktifkan. Apabila terdapat gerakan dalam rumah, penghuni rumah akan mendapatkan signal peringatan secara *realtime* melalui *smartphone*. Penelitian yang dilakukan oleh Orji terkait sistem keamanan pintu adalah penggunaan mikrokontroler, *keypad*, dan motor servo yang berfungsi sebagai sakelar untuk mengunci dan membuka pintu. Sistem penguncian pintu menggunakan metode penginputan *password*. Apabila *password* yang dimasukan benar maka motor servo akan terbuka [10]. Penelitian lain terkait sistem keamanan pintu adalah menggunakan BLEDoorGuard yaitu sistem akses pintu nirkabel yang memanfaatkan indikator kekuatan sinyal yang diterima dari bluetooth untuk mengekstrak fitur untuk pengenalan tindakan. Penelitian tersebut mengidentifikasi pola dan durasi waktu manusia dalam kecepatan yang konstan [11].

Berdasarkan pada perbandingan dengan setiap penelitian-penelitian sebelumnya, dalam penelitian ini peneliti akan mengembangkan sistem keamanan rumah dengan mengkombinasikan satu *door lock* dengan dua mekanisme pembuka kunci lewat penggunaan sistem *biometric* scan dan sistem IoT atau kontrol jarak jauh. Selain itu percobaan yang dilakukan dalam penelitian ini yaitu dengan menggunakan mikrokontroler NodeMCU dengan modul ESP8266 yang sudah terintegrasi langsung didalam satu papan mikrokontroler untuk melihat efektifitas dan efisiensi waktu pengerjaan sistem. Sistem penguncian pintu yang dibangun mampu menerima inputan dari dua sumber, dengan kata lain dapat dikontrol menggunakan *smartphone* dari jarak jauh dan juga dapat dikontrol menggunakan sidik jari. Penggunaan dua mekanisme kontroling ini diharapkan mampu mengatasi kelalaian dari penghuni rumah dalam menjaga keamanan rumah. penulisan dari makalah ini selanjutnya adalah sebagai berikut: pembahasan sub ke 2 tentang metodologi penelitian. Sub ke 3 membahas tentang Hasil dan analisis dan sub bagian ke 4 membahas Kesimpulan dari studi yang dilakukan yaitu tentang temuan dari penelitian ini, kebaharuan yang diberikan dan saran untuk penelitian lanjut.

2. METODE PENELITIAN

Dalam penelitian ini Implementasi perancangan sistem menggunakan mikrokontroler NodeMCU ESP8266, Bahasa program yang digunakan adalah Bahasa pemrograman Arduino serta aplikasi mobile *Blynk* berbasis android. Penggunaan mikrokontroler NodeMCU ESP8266 bertujuan untuk mengintegrasikan semua perangkat elektronik dalam satu kesatuan. NodeMCU ESP8266 memiliki modul *Wi-Fi* dan memiliki memori yang cukup besar. Modul *Wi-Fi* ESP8266 digunakan untuk menerima signal *Wi-Fi* dari *router* agar mikrokontroler dapat terhubung dengan internet. Selain itu untuk mekanisme sistem penguncian pintu lainnya menggunakan sensor *fingerprint* yang terintegrasi dengan mikrokontroler ESP8266.

2.1. *Internet of Things* dan Perangkat Pendukung

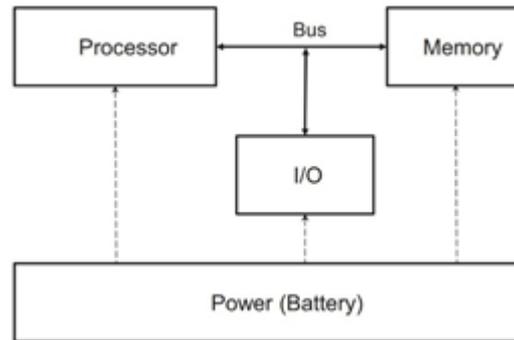
1. *Internet of Things*

IoT atau *Internet of Things* secara garis besar didefinisikan dengan suatu objek atau alat yang mampu mentransmisikan data ke internet tanpa memerlukan interaksi dari manusia. IoT itu sendiri terdiri dari beberapa layer atau lapisan diantaranya, *Perception Layer*, *Network Layer*, *Middleware Layer*, *Application Layer*, dan *Business Layer* [12]. Agar dapat mengirimkan data melalui *cloud/internet* IoT setidaknya memiliki, *Wireless Sensor Network* (WSN), *Radio Frequency Identification* (RFID) dan *Cloud computing* [12].

Sistem IoT berkomunikasi ujung-ke-ujung / multi-hop. Sistem IoT dapat menunjukkan hubungan yang kompleks antara sumber data dan penerima data. IoT secara umum, mengumpulkan data melalui *sensing device*, memproses data, dan mengambil tindakan

mulai dari mengirim pemberitahuan dan meningkatkan alarm, hingga mengambil tindakan melalui aktuator pada sistem fisik. Sistem IoT juga merupakan sistem komputasi tertanam yang menggunakan arsitektur polisilikon untuk tujuan umum.

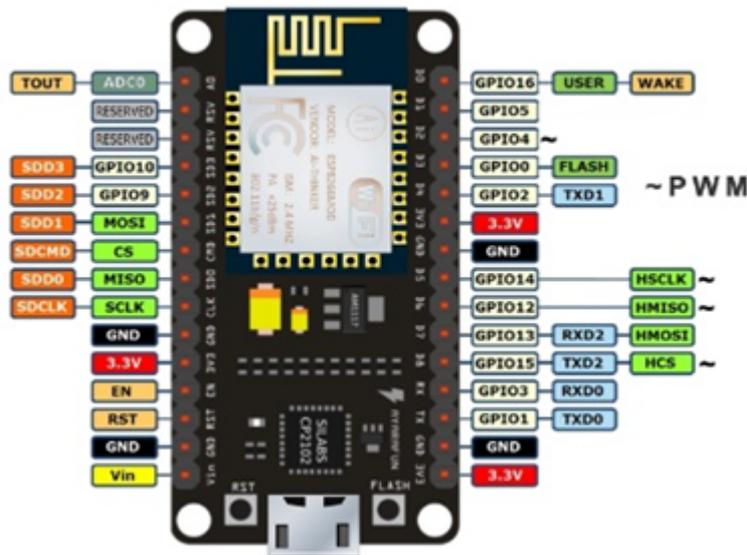
Struktur khas sistem IoT ditunjukkan pada Gambar 1, di mana sistem tersebut berisi empat subsistem utama: (i) pemrosesan, (ii) memori, (iii) input / output, dan (iv) daya.



Gambar 1. Struktur khas sistem IoT

2. Microcontroller

Dalam proses pembangunan sistem penghematan energi akan digunakan Arduino Mikrokontroler. Fungsi dari arduino mikrokontroler itu sendiri adalah sebagai pusat kontrol dan pengolahan data analog dari hasil tangkapan sensor [13].



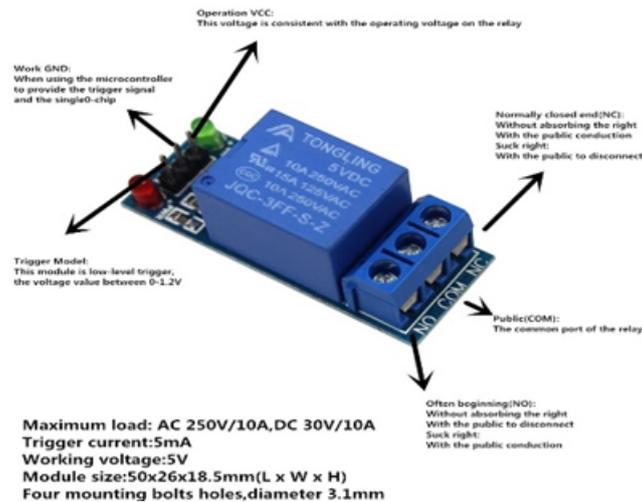
Gambar 2. NodeMCU ESP8266

3. Blynk

Blynk merupakan sebuah platform yang memungkinkan setiap orang dapat membangun sebuah *interface* untuk dapat mengontrol dan memantau *project* perangkat keras dari perangkat *mobile* [14]. *Blynk* dapat diunduh dari *smatphone* dan langsung dapat digunakan dalam proyek yang sedang dikembangkan. Dalam membangun sebuah *project*, aplikasi *Blynk* mampu membuat sebuah antarmuka sebagai fungsi kontrol diantaranya tombol saklar/*button switch*, menampilkan grafik bacaan sensor, dan berbagai fitur kontrol lainnya. Melalui *Blynk* tersebut anda dapat mengontrol dari jauh semua pin dalam mikrokontroler yang sudah terhubung ke internet. Setiap *project* yang dibangun dalam *blynk* masing-masing memiliki id token yang berbeda untuk memastikan keamanan akses perangkat keras. Disini kita dapat membuat beberapa *project* sekaligus dalam *blynk*. Dapat dikatakan bahwa *Blynk* merupakan IoT itu sendiri yang didesain sebagai remot kontrol data dari perangkat mikrokontroler secara *realtime*.

4. Relay

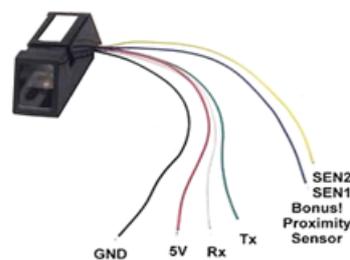
Relay merupakan saklar atau *switch* listrik. *Relay* dapat mengganti arus hingga 10 Ampere pada tegangan 30 V DC atau 220 V AC [15]. Dalam paper ini *relay* berperan penting sebagai saklar listrik yang dapat dijalankan dengan fungsi kontrol *blynk* dan sensor sidik jari untuk menyambungkan dan memutuskan tegangan 12V yang terhubung ke *solenoid door lock*.



Gambar 3. Relay

5. Fingerprint sensor

Sensor sidik jari merupakan perangkat keras yang berfungsi sebagai penerima inputan sidik jari yang nantinya akan diteruskan dan diproses oleh mikrokontroler [16]. Sensor sidik jari hanya dapat mengenali inputan sidik jari yang telah tersimpan dalam *memory*. Semua data sidik jari yang terbaca di *scanner* akan dicocokkan dengan data dalam *memory*. Apabila ada kecocokan data sidik jari maka sensor sidik jari akan mengirimkan *signal HIGH* ke mikrokontroler dan sebaliknya.



Gambar 4. Sensor Sidik Jari

6. Door lock solenoid

Door lock solenoid merupakan sebuah perangkat kunci pintu yang menggunakan tegangan listrik 12V untuk dapat berfungsi. *Door lock solenoid* akan terbuka apabila menerima tegangan sebesar 12V dan sebaliknya, akan menutup apabila tidak menerima tegangan.



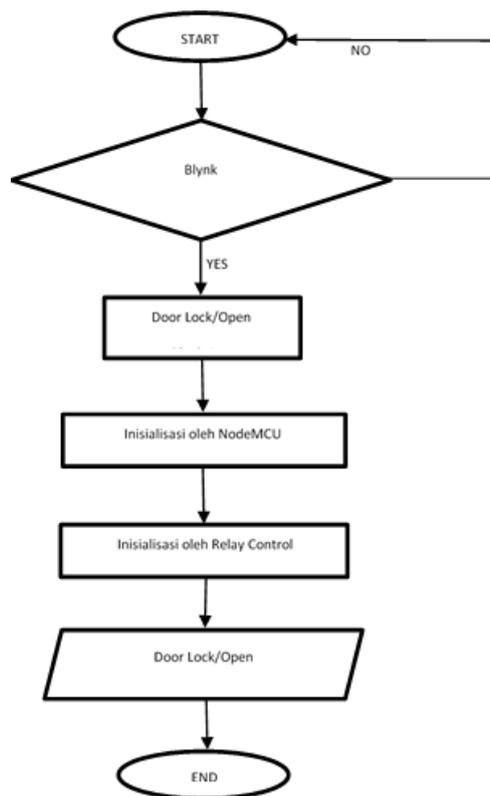
Gambar 5. Door lock solenoid

2.2. Alur kerja sistem

Sistem dibangun berdasarkan pada penggunaan mikrokontroler NodeMCU ESP8266 [17] sebagai IoT dan sensor *fingerprint* sebagai penerima inputan *biometric scanning*. Secara keseluruhan sistem penguncian pintu rumah berbasis IoT akan terhubung ke internet dari koneksi *Wi-Fi* rumah ke sirkuit ESP8266 dan *smartphone*. Dalam menghubungkan Mikrokontroler NodeMCU dengan *smartphone* penghuni rumah secara *online*, dibutuhkan identifikasi SSID *Wi-Fi*, *password*, dan kode token, agar *cloud server blynk* dapat menghubungkan mikrokontroler dan *smartphone* penghuni rumah. Pada Gambar 6 dapat dilihat Prinsip koneksi *blynk*.

Gambar 6. Prinsip Kerja *Blynk*

Gambar 7 menjelaskan alur kerja sistem kontrol *blynk*, dimana server *blynk* akan memeriksa koneksi internet antara *smartphone* dan NodeMCU. NodeMCU harus menyertakan kode token, nama SSID Wi-Fi dan kata sandinya. Informasi yang disertakan dalam kode harus sesuai dengan informasi *Wi-Fi* agar ESP8266 terhubung dengan *Wi-Fi* sebagai saluran untuk bertukar perintah antara ponsel pintar dan NodeMCU. Proses yang tersisa hanyalah perintah yang dikirim dari aplikasi *Blynk* ke NodeMCU untuk mengontrol beban yang terhubung ke kit *relay*.

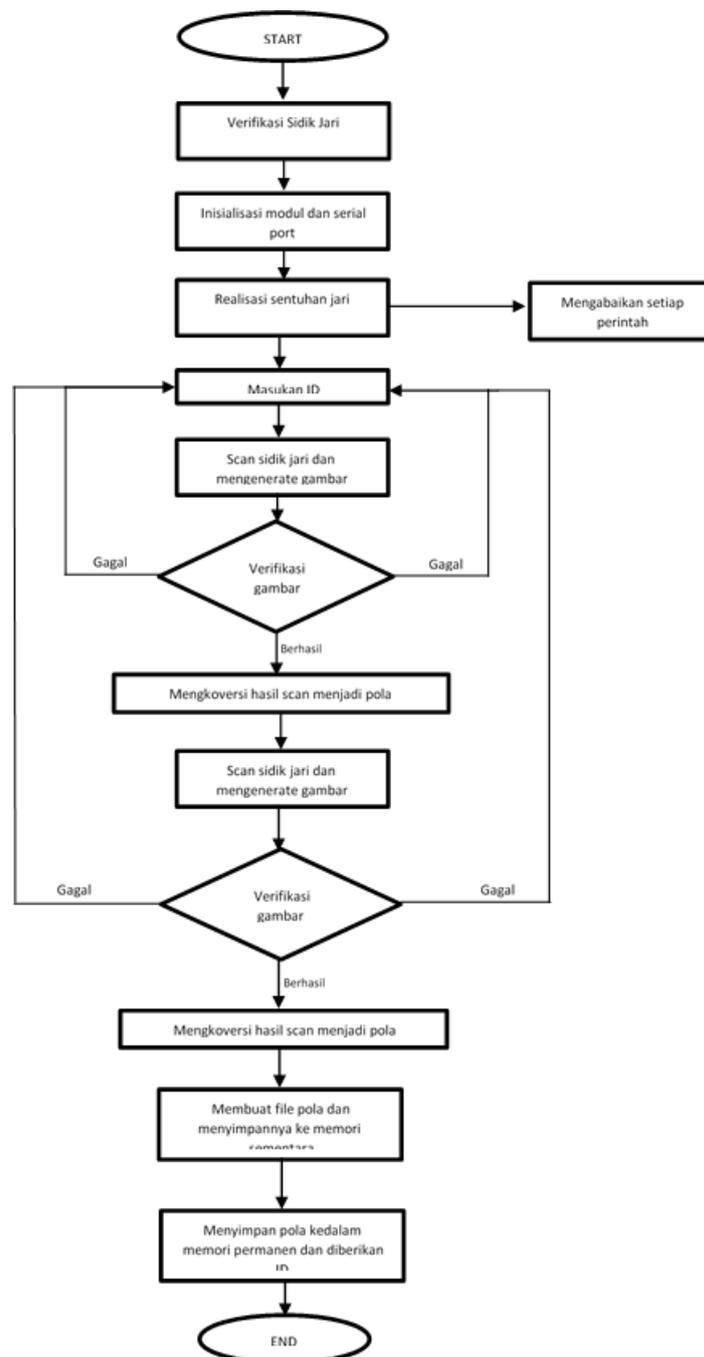
Gambar 7. Alur kerja Sistem Kontrol *Blynk*

Selain penggunaan *Blynk APP* sebagai media kontrol pintu dari jarak jauh menggunakan internet, dalam desain sistem juga menerapkan sensor sidik jari sebagai salah satu cara akses untuk membuka pintu rumah. Hal pertama dalam penggunaan sensor sidik jari adalah menghubungkan sensor sidik jari dengan mikrokontroler dan mengambil gambar sidik jari untuk disimpan dalam *database*. Sidik jari yang disimpan akan menjadi kunci akses pintu saat akan membuka pintu.

Ada berbagai macam metode untuk mengambil sampel sidik jari, salah satu metode yang digunakan dalam penelitian ini adalah penggunaan *optical scanning*. Inti utama dari *optical scanner* adalah CCD atau *charge couple Device* [18]. Proses pertama dalam metode CCD dimulai saat jari diletakkan pada lempengan kaca dan kamera CCD menangkap gambar sidik jari tersebut. Sumber cahaya CCD biasanya berupa *Light Emitting Diodes* (LED) untuk penerangan alur sidik jari saat melakukan *scanning*. Gambar sidik

jari yang dihasilkan sistem CCD biasanya berupa gambar sidik jari yang terbalik, area gelap merepresentasikan banyaknya cahaya yang dipantulkan menggambarkan punggung dari alur sidik jari, sebaliknya area terang merepresentasikan sedikitnya cahaya yang dipantulkan menggambarkan lembah sidik jari. Saat sebelum melakukan perbandingan gambar sidik jari yang baru saja diambil dengan data gambar sidik jari yang disimpan, prosesor *Scanner* melakukan verifikasi gambar yang diambil oleh CCD berdasarkan pada rata-rata kegelapan *pixel*, dan akan menolak akses apabila gambar yang diambil terlalu terang atau terlalu gelap. Apabila pengambilan gambar yang dilakukan CCD ditolak maka *scanner* akan melakukan pengaturan waktu pencahayaan dan mengulangi pengambilan gambar.

Gambar 8 menunjukkan diagram alur aktivasi sensor sidik jari. Proses aktivasi perangkat sidik jari dilakukan dengan beberapa tahapan. Sebelum melakukan tahapan aktivasi, perangkat mikrokontroler yang terhubung ke sensor sidik jari akan di masukan *source code* aktivasi. Setelah proses *upload source code* berhasil langkah awal pada tahapan aktivasi adalah dengan melakukan inisialisasi serial *port* yang sesuai. Apabila sensor sidik jari telah terhubung pada *port*, langkah selanjutnya adalah memasukan Id sidik jari. Ketika sensor membaca sidik jari yang tertempel pada kaca *scanner*, sensor secara otomatis akan *generate* gambar sidik jari yang tertangkap, dan mengkonversinya kedalam pola. Jika terdapat kegagalan atau kesalahan penangkapan gambar sidik jari maka proses akan diulang kembali. Sistem akan memastikan validasi untuk satu identitas melalui dua kali penginputan sidik jari yang sama. Setelah proses konfersi sidik jari kedalam pola berhasil, akan dibuat sebuah *template file* dan dimasukkan kedalam memori sementara. Langkah terakhir adalah menyimpan *template file* kedalam memori permanen dan memberikan ID.



Gambar 8. Diagram alur aktivasi sensor sidik jari

Dalam sistem penguncian pintu rumah sensor sidik jari akan menerima setiap inputan sidik jari yang menempel pada kaca *scanner* dan melakukan verifikasi kecocokan dengan gambar sidik jari sampel yang ada dalam *database*. Apabila hasil verifikasi kecocokan sama, maka mikrokontroler Node MCU akan mengirimkan *signal HIGH* ke *pin output digital* yang terhubung dengan *solenoid door lock* dan pintu akan terbuka. Apabila hasil verifikasi kecocokan sidik jari berbeda dengan sampel dalam *database* maka sensor akan mengulangi pengambilan gambar sidik jari.

3. HASIL DAN ANALISIS

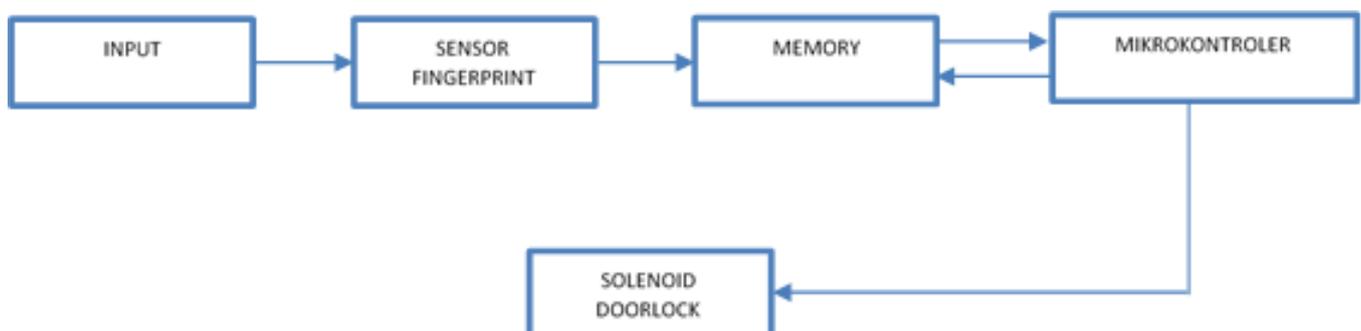
3.1. Blynk Testing

Hasil pengujian koneksi menggunakan aplikasi *Blynk* dengan menggunakan android *smartphone* berhasil berkomunikasi secara baik saat *smartphone* menggunakan tombol kontrol untuk membuka/mengunci *solenoid door lock*. Langkah pengujian awal adalah melakukan registrasi ke dalam *cloud* sistem *blynk* lewat Android *smartphone*. Aplikasi *blynk* yang sudah diinstal di android *smartphone* dijalankan dan dibuat sebuah project baru. Secara otomatis *blynk* akan mengirimkan kode token *project* yang dibuat ke alamat *email*. Autentikasi token yang diterima dimasukkan kedalam kode program beserta SSID Wi-Fi, dan *password Wi-Fi* kemudian di upload kedalam mikrokontroler. Hasil *uploading* kode program dicek menggunakan serial monitor untuk memastikan mikrokontroler sudah terhubung ke *cloud blynk* atau tidak. Sebelum pengecekan di serial monitor dipastikan *smartphone* sudah terhubung dengan internet. Apabila status dalam serial monitor terkoneksi dengan *blynk cloud* pastikan status koneksi *project* di *smartphone* juga telah terhubung.

Blynk menggunakan sistem *virtual* pin untuk melakukan komunikasi dengan papan mikrokontroler NodeMCU. *Virtual* pin berbeda dengan analog/digital pin. Analog/digital pin merupakan pin dalam perangkat keras papan mikrokontroler yang mampu menghubungkan sensor maupun *actuator*. Aplikasi *blynk* dapat mengontrol pin digital/analog perangkat keras yang terhubung tanpa harus memasukan koding kedalam papan mikrokontroler terlebih dahulu. Dalam penelitian ini, antarmuka aplikasi *blynk* dimasukan satu fungsi tombol kontrol dengan *port virtual output* digital sesuai pin output yang digunakan dalam papan mikrokontroler yang terhubung dengan *relay*. Setelah fungsi kontrol telah ditambahkan pada aplikasi *blynk* selanjutnya dilakukan percobaan membuka *solenoid door lock*. Ketika tombol kontrol pada aplikasi *blynk* di *smartphone* di tekan maka secara otomatis *relay* akan menerima *signal* digital *HIGH* untuk menyambungkan arus 12V dari *power supply* ke *solenoid door lock* selama 5 detik dan kemudian diputuskan.

3.2. Fingerprint Testing

Gambar 9 menunjukkan diagram rangkaian Kunci Pintu menggunakan Teknologi Sidik Jari *Biometric*. Diagram skematik dibagi menjadi tiga unit yaitu *Door Lock*, *Relay*, dan *Fingerprint sensor*. Sistem *Door Lock* adalah sistem utama yang ditempatkan di pintu dan membutuhkan Perangkat Pembaca Sidik Jari untuk diaktifkan. Sistem akan diatur dari 220V AC ke 12V untuk dapat bekerja secara efektif dengan keadaan operasi unit mikrokontroler NodeMCU ESP8233. Status operasi mikrokontroler direferensikan dari rangkaian datanya. Dimana kapasitor terhubung ke tegangan output regulator dan *ground* untuk menyaring kebisingan yang datang dari regulator. Rangkaian *driver relay* mengontrol daya AC yang digunakan oleh sistem *Door Lock* yang terdiri dari transistor PNP, resistor, *relay* 12V dan dioda. Resistor memungkinkan arus kecil melewati persimpangan basis-emitor. Jalur keluaran rangkaian relay kemudian dihubungkan ke port keluaran RC5 dari PIC168F77A, dan ke dioda 1N4006 dan dihubungkan ke keluaran 12V dari pengatur sistem kunci pintu dan terakhir dihubungkan ke *ground*. Transistor berfungsi sebagai rangkaian yang mengontrol keadaan *relay*. Ketika volt positif (3,3V) diterapkan di dasar transistor, persimpangan kolektor-emitor akan terhubung. Dengan demikian, daya 12V mengalir melalui bagian induktor relay yang kemudian memberi energi pada saklar di dalam relay. Status saklar menentukan apakah daya AC mengalir ke soket AC. Dioda *reverse-bias* berfungsi sebagai pelindung tegangan pada bagian induktor dari *relay* sedemikian rupa sehingga tidak ada arus yang mengalir ketika transistor tidak aktif. Jika tidak ada tegangan positif yang diterapkan ke basis transistor, transistor tidak akan dalam keadaan aktif dan daya AC terputus ke soket AC. Sensor sidik jari mengumpulkan sidik jari pengguna dan diatur oleh tegangan keluaran 5V. Sebuah osilator 20 MHz terhubung ke salah satu pin mikrokontroler untuk tujuan frekuensi waktu.



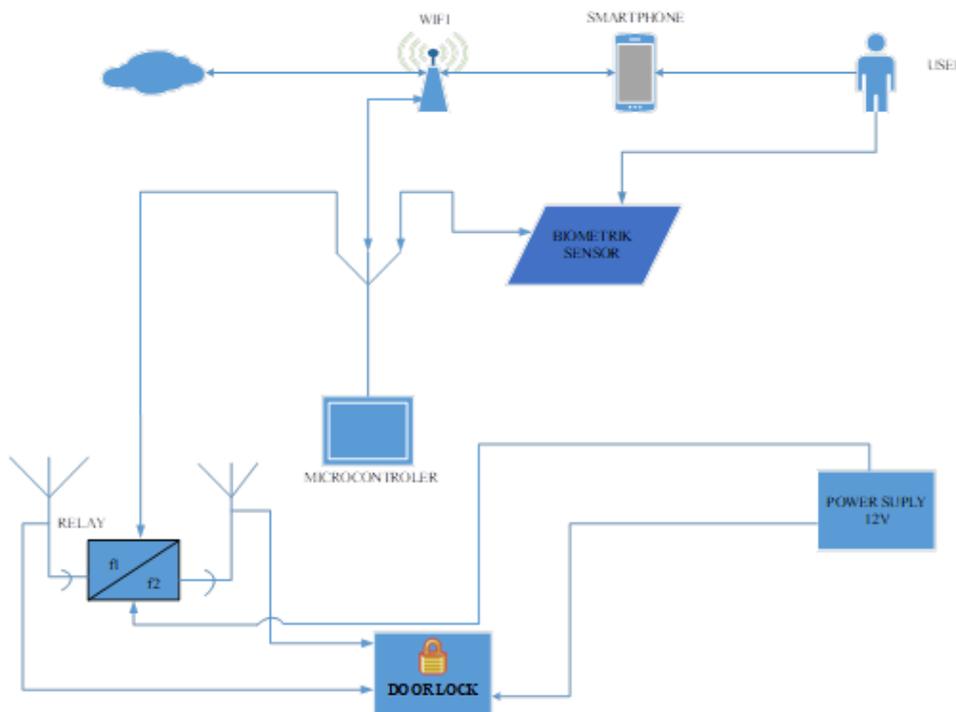
Gambar 9. Sistem kerja sensor sidik jari pada pintu rumah

3.3. Analisis Sistem

Dalam penelitian ini, mengkombinasikan satu *door lock* dengan dua mekanisme pembuka kunci lewat penggunaan sensor sidik jari dan sistem kontrol jarak jauh. Penggunaan sensor mengacu pada hasil penelitian yang dilakukan Surantha untuk mengantisipasi gerakan dalam rumah menggunakan Raspberry Pi 3 dan Arduino [9]. Tujuannya adalah untuk mengantisipasi apabila rumah akan ditinggalkan atau rumah dalam keadaan kosong sensor gerak akan diaktifkan secara *realtime* melalui *smartphone*. Berdasarkan *flowchart* pada gambar 10, yang terdiri dari sensor dan aplikasi *blynk* sebagai input, dan *relay* sebagai output yang dipakai sebagai saklar untuk menghubungkan atau memutuskan tegangan 12V dari *power supply* ke perangkat solenoid. Langkah pertama adalah mendefinisikan pin sebagai input atau output. Ketika pin sudah ditentukan, program akan memanggil beberapa *file* berupa *library*, kemudian menghubungkan board mikrokontroler NodeMCU ESP8266 di pin digital dengan aplikasi *blynk*. Dalam Penelitian ini menggunakan 2 pin digital untuk rangkaian input dan output. 1 pin digital untuk input dan 1 pin digital untuk output. Selain menggunakan input/output *hardware*, *Smartphone* android juga digunakan sebagai media kontrol melalui aplikasi *blynk*. Dalam antarmuka *project* pada aplikasi *blynk* diberi satu tombol saklar untuk memberikan perintah pada pin *digital* output atau *relay* yang terhubung dengan *solenoid door lock*. Salah satu pin digital dihubungkan dengan sensor sidik jari untuk menerima inputan data sidik jari. Jika ada kecocokan sidik jari dalam *database*, sensor akan mengirimkan signal perintah pada pin *digital* output atau *relay* yang terhubung dengan *solenoid door lock*.

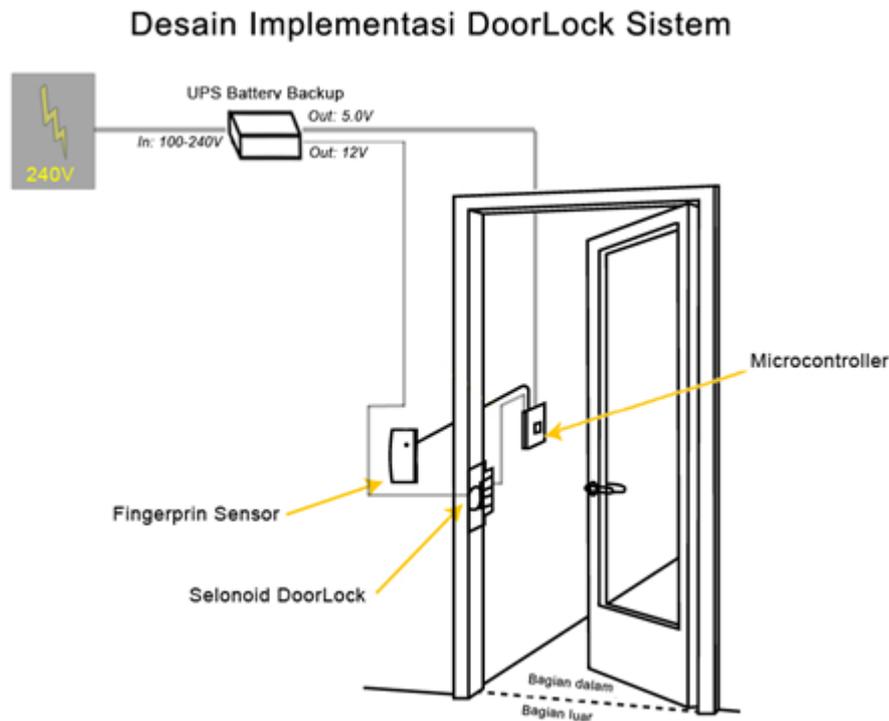
Output yang digunakan peneliti hanya 1, dimana satu pin output dapat menerima *signal* dari dua inputan. Inputan pertama merupakan inputan yang diterima oleh pin digital berasal dari sensor sidik jari dan inputan kedua berasal dari inputan yang diterima berupa *signal virtual* dari aplikasi *blynk*. Setiap komponen terhubung dengan pin yang dipasang pada papan mikrokontroler NodeMCU. Penentuan Pin set ini dilakukan pada software Arduino IDE dimana bahasa yang digunakan adalah bahasa C yang diupload ke kepapan mikrokontroler menggunakan kabel USB. Dalam IDE Arduino ini, program yang diunggah terdiri dari head program, bagian inisiasi atau pengaturan variabel, dan bagian utama program atau loop. Variabel-variabel dalam head program digunakan untuk menambahkan program *file* yang diperlukan atau disebut juga dengan *library*.

Selain *library*, peneliti juga memasukkan beberapa komponen yang digunakan dalam program ini. Salah satunya adalah informasi tentang token, SSID *Wi-Fi* dan Sandi *Wi-Fi*. Token ini adalah alamat yang digunakan untuk menghubungkan perangkat keras dengan aplikasi *Blynk*. Token ini didapat dari aplikasi *Blynk* dengan mengirimkannya ke email pengguna. Sedangkan SSID dan *Password Wi-Fi* digunakan untuk menghubungkan perangkat keras dengan *Wi-Fi* yang digunakan. Karena perangkat yang akan dikembangkan akan dioperasikan dengan koneksi internet sehingga membutuhkan alamat *Wi-Fi* yang digunakan. Juga, kepala program berisi informasi tentang pin yang digunakan dan namanya. Karena dalam penelitian ini menggunakan sensor sidik jari maka ketika objek/sidik jari tidak mengenai sensor lagi maka output akan mati secara otomatis. Pada bagian kedua terdapat *setup* yang digunakan untuk menginisiasi atau menamai variabel yang digunakan dalam penelitian ini. Inisiasi yang dimaksud adalah memberi nama dan membuat pin apa saja yang ada pada pin yang digunakan dalam program. Sebagai contoh *relay* yang pada bagian program adalah pin D5 sebagai output. Setelah bagian *setup*, ada bagian *loop* dimana bagian ini merupakan bagian terpenting dari program. Pada bagian *loop* ini digunakan mengirim data secara *realtime* dan berulang. Data yang dikirimkan adalah data koneksi antara ESP8266 dengan *blynk* dan data dari sensor sidik jari. Sistem *loop* akan menerima salah satu inputan dengan jeda selama 5 detik. Hal ini dilakukan adalah untuk menahan *solenoid door lock* tetap menerima arus/terbuka.



Gambar 10. Flowchart Design Sistem

Gambar 11 menunjukkan desain implementasi tata letak lokasi penempatan *hardware* beserta jalur sumber energi listrik. Desain tersebut dibangun untuk mencapai target efisiensi biaya pengaplikasian sistem pada setiap titik pintu rumah. Hal lain yang ditemukan dalam penelitian ini yaitu pada saat pengaplikasian sistem, sistem penguncian pintu tidak akan berfungsi apabila sumber listrik utama rumah putus. Untuk menghindari hal tersebut dilakukan penempatan sumber arus cadangan (*UPS Battery Backup*) [19] dengan dua output *chanell* 12V dan 5V, yang dihubungkan langsung pada *solenoid door lock* dan mikrokontroler. Hal ini sangat membantu dalam menghindari kegagalan sistem penguncian pintu rumah.



Gambar 11. Desain Implementasi *Door Lock* Sistem

4. KESIMPULAN

Berdasarkan pada keseluruhan pengujian sistem, *smart door lock* berfungsi sesuai dengan tujuan dilakukannya penelitian ini. Perbandingan dengan setiap penelitian sebelumnya adalah dalam penelitian ini mampu mengkombinasikan satu *door lock* dengan dua mekanisme pembuka kunci lewat penggunaan sensor sidik jari dan sistem kontrol jarak jauh. Kedua mekanisme yang digunakan tersebut mampu berjalan secara bergantian dalam selang waktu 5 detik tanpa ada kendala tabrakan pemrosesan dua inputan sekaligus. Selain itu percobaan yang dilakukan dalam penelitian ini dengan menggunakan mikrokontroler NodeMCU dengan modul ESP8266 yang sudah terintegrasi langsung didalam satu papan mikrokontroler menunjukkan efektifitas dan efisiensi waktu pengerjaan sistem, dikarenakan untuk dapat menghubungkan mikrokontroler ke internet tidak lagi diperlukan perangkat/modul *Wi-Fi* tambahan dan merakitnya kembali. Hal lainnya yang ditemui dalam penelitian ini adalah tidak ada lagi kehilangan kunci rumah ataupun kelalaian penghuni rumah dalam menjaga keamanan pintu rumah. Pemilik rumah akan dapat mendaftarkan sidik jari setiap orang yang dipercaya sebagai kunci untuk membuka pintu rumah.

Saran untuk peneliti selanjutnya dalam pengembangan sistem adalah untuk dapat lebih memperhatikan celah keamanan lainnya untuk menyempurnakan sistem keamanan rumah yang lebih efektif dan efisien. Pemanfaatan teknologi IoT yang mungkin dapat dikembangkan lebih lanjut adalah mengkombinasikan penguncian pintu rumah dengan teknologi *facial recognition system* untuk kemudahan akses serta konfirmasi identitas penghuni rumah atau juga sebagai *alert* bagi keamanan saat rumah ditinggalkan.

REFERENSI

- [1] C. Yukonhiatou, T. Yoshihisa, T. Kawakami, Y. Teranishi, and S. Shimojo, "A Fast Stream Transaction System for Real-Time IoT Applications," *Internet of Things*, vol. 11, p. 100182, 2020.
- [2] V. D. Corte, K. Umachandran, I. Jurcic, and D. S. F. James, "Industry 4.0: The New Industrial Revolution," in *Big Data Analytics for Smart and Connected Cities*. IGI Global, 2019, ch. 6, pp. 138–156.
- [3] A. Rejeb, S. Simske, K. Rejeb, H. Treiblmaier, and S. Zailani, "Internet of Things Research in Supply Chain Management and Logistics: A Bibliometric Analysis," *Internet of Things*, vol. 12, p. 100318, 2020.

- [4] N. Suthanthira Vanitha, J. Karthikeyan, G. Kavitha, and K. Radhika, "Modelling of Intelligent Transportation System for Human Safety Using IoT," *Materials Today: Proceedings*, vol. 33, no. xxxx, pp. 4026–4029, 2020.
- [5] M. Radja and A. W. Emanuel, "A review: Design of Smart Home Electrical Management System Based on IoT," in *2019 International Conference on Information and Communications Technology, ICOIACT 2019*, no. 2. Yogyakarta: IEEE, 2019, pp. 910–915.
- [6] C. Sisavath and L. Yu, "Design and Implementation of Security System for Smart Home Based on IOT Technology," *Procedia Computer Science*, vol. 183, pp. 4–13, 2021.
- [7] S. Sauda and E. P. Agustini, "Implementasi Prototype Model dalam Pengembangan Aplikasi Smart Cleaning sebagai Pendukung Aplikasi Smart City," *MATRIK : Jurnal Manajemen, Teknik Informatika dan Rekayasa Komputer*, vol. 20, no. 1, pp. 73–84, 2020.
- [8] L. Bai, D. Yang, X. Wang, L. Tong, X. Zhu, N. Zhong, C. Bai, C. A. Powell, R. Chen, J. Zhou, Y. Song, X. Zhou, H. Zhu, B. Han, Q. Li, G. Shi, S. Li, C. Wang, Z. Qiu, Y. Zhang, Y. Xu, J. Liu, D. Zhang, C. Wu, J. Li, J. Yu, J. Wang, C. Dong, Y. Wang, Q. Wang, L. Zhang, M. Zhang, X. Ma, L. Zhao, W. Yu, T. Xu, Y. Jin, X. Wang, Y. Wang, Y. Jiang, H. Chen, K. Xiao, X. Zhang, Z. Song, Z. Zhang, X. Wu, J. Sun, Y. Shen, M. Ye, C. Tu, J. Jiang, H. Yu, and F. Tan, "Chinese Experts' Consensus on The Internet of Things-Aided Diagnosis and Treatment of Coronavirus Disease 2019 (COVID-19)," *Clinical eHealth*, vol. 3, pp. 7–15, 2020.
- [9] N. Surantha and W. R. Wicaksono, "Design of Smart Home Security System Using Object Recognition and PIR Sensor," *Procedia Computer Science*, vol. 135, pp. 465–472, 2018.
- [10] E. Z. Orji, U. I. Nduanya, and C. V. Oleka, "Microcontroller Based Digital Door Lock Security System Using Keypad," *International Journal of Latest Technology in Engineering, Management & Applied Science*, vol. 8, no. 1, pp. 92–97, 2019.
- [11] W. Shao, T. Nguyen, K. Qin, M. Youssef, and F. D. Salim, "BLEDoorGuard: A Device-Free Person Identification Framework Using Bluetooth Signals for Door Access," *IEEE Internet of Things Journal*, vol. 5, no. 6, pp. 5227–5239, 2018.
- [12] M. Mahbub, "A Smart Farming Concept Based on Smart Embedded Electronics, Internet of Things and Wireless Sensor Network," *Internet of Things*, vol. 9, p. 100161, 2020.
- [13] O. J. Oyejide, M. O. Okwu, L. K. Tartibu, and O. I. Olayode, "Development of Sensor Controlled Convertible Cart-Trolley," *Procedia CIRP*, vol. 91, pp. 71–79, 2020.
- [14] E. Media's, S. ., and M. Rif'an, "Internet of Things (IoT): BLYNK Framework for Smart Home," *KnE Social Sciences*, vol. 3, no. 12, pp. 579–586, 2019.
- [15] M. Radja, G. G. Hungilo, G. Emmanuel, and S. Suyoto, "IoT: Improved Home Energy Control System Based on Consumer," *IOP Conference Series: Materials Science and Engineering*, vol. 1098, no. 4, p. 042028, 2021.
- [16] M. Magdin, Š. Koprda, and L. Ferenczy, "Biometrics Authentication of Fingerprint with Using Fingerprint Reader and Microcontroller Arduino," *Telkomnika (Telecommunication Computing Electronics and Control)*, vol. 16, no. 2, pp. 755–765, 2018.
- [17] M. Kashyap, V. Sharma, and N. Gupta, "Taking MQTT and NodeMcu to IOT: Communication in Internet of Things," *Procedia Computer Science*, vol. 132, no. Iccids, pp. 1611–1618, 2018.
- [18] J. Xiong, Z. Liu, R. Lin, R. Bu, Z. He, Z. Yang, and C. Liang, "Green Grape Detection and Picking-Point Calculation in A Night-Time Natural Environment Using a Charge-Coupled Device (CCD) Vision Sensor with Artificial Illumination," *Sensors*, vol. 18, no. 4, p. 969, 2018.
- [19] A. H. Sabry, Y. Hasan, W. Z. W., Alkubaisi, and M. Z. A. Ab-Kadir, "Battery Backup Power System for Electrical Appliances with Two Options of Primary Power Sources," in *IEEE International Conference on Smart Instrumentation, Measurement and Applications (ICSIMA)*. IEEE, 2018, pp. 1–5.