# BAB 2
# DASAR TEORI

## 2.1 KAJIAN PUSTAKA

Penelitian sistem keamanan Brankas saat ini telah banyak dikembangkan salah satunya adalah penelitian dengan judul "Rancang Bangun Alat Pengaman Brankas Menggunakan Sensor Sidik Jari Berbasis Arduino" oleh Okta Rea Arsyad, Kurnia dan P. Kartika yang merancang sistem keamanan brankas. Hasil dari penelitian ini adalah *Prototype* Brankas yang dapat diakses dengan menggunakan sensor sidik jari, dimana sidik jari yang telah ditetapkan pada sistem keamanan tersebut akan digunakan untuk autentikasi pemilik [4]. Metode autentikasi biometrik dengan melakukan pengujian terhadap akurasi sensor *fingerprint*. Setelah melakukan pengujian terhadap status akurasi dengan melakukan 5 kali pengujian maka didapatkan bahwa dengan menggunakan jari yang sama sebanyak 4 kali, 2 kali percobaan autentikasi dengan menggunakan jari yang sama berhasil dan akurat dan dua percobaan dengan hasil sidik jari tidak terdeteksi dan status akurasi tidak akurat.

Penelitian berjudul "Sistem Keamanan Pintu Rumah Berbasis *Internet of Things* via Pesan Telegram" oleh Jery Frenando, Jaenal Arifin S.T., M.Eng. dan Herryawan Pujiharsono, S.T., M.Eng. yang merancang sistem keamanan pintu rumah yang berbasis *Internet of Things*. hasil dari penelitian ini adalah *Prototype* pintu rumah yang berguna untuk memberikan keamanan yang lebih baik dengan memanfaatkan konsep *Internet of Things* melalui telegram untuk mengirim notifikasi ketika mendeteksi orang yang tidak dikenali dan memanfaatkan kamera untuk menangkap gambar dari orang tersebut untuk selanjutnya dikirimkan melalui telegram kepada penggunanya yang kemudian dapat mengirimkan perintah untuk membuka kunci pintu melalui *chat* di telegram [8]. Sistem keamanan kunci pintu rumah pada penelitian ini memberikan notifikasi kepada pemilik brankas bahwa telah terdeteksi objek di depan pintu yang selanjutnya akan mengambil gambar dan mengirimkan gambar tersebut pada *bot* telegram yang nantinya akan melakukan konfirmasi kepada pemilik brankas tersebut. Pengujian pada penelitian ini dilakukan dengan menguji kinerja sistem dengan hasil performa menunjukkan

bahwa setelah melakukan percobaan sebanyak 30 kali dengan rata-rata waktu yang didapatkan saat sistem bekerja secara otomatis adalah 16754ms sedangkan waktu rata-rata untuk sistem bekerja secara manual adalah 9751ms dengan jumlah pengujian yang sama sebanyak 30 kali.

Penelitian berjudul "Sistem Kendali Kunci Pintu Menggunakan *Voice Command* Berbasis *Internet of Things* (IOT)" oleh Maria Danu Lagan yang merancang sistem keamanan pintu rumah dengan menggunakan perintah suara yang berbasis *Internet of Things* sebagai kendali pintu. Hasil penelitian ini berupa *Prototype* sistem kunci pintu yang terintegrasi dengan aplikasi yang dibuat melalui *platform* antares yang dapat melakukan proses penguncian pintu melalui perintah suara dan juga dapat dikontrol melalui aplikasi [9]. Pada penelitian ini *Platform* Antares IoT digunakan sebagai tempat pengiriman data perintah dan pengambilan data yang akan diguanakan untuk ditampilkan pada aplikasi android. Data pergerakan dan data saat pintu rumah didobrak atau saat terkunci. Dengan menggunakan basic4android dalam pembuatan aplikasi android. Aplikasi ini dapat terhubung dengan *platform* IoT Antares dengan memanfaatkan protokol MQTT. Data komunikasi yang ada pada aplikasi ini akan ditampilkan dan tersimpan pada dashboard antares.

Penelitian yang dilakukan oleh Nasha Dewandra Putra dengan judul "*Wireless Smart Tag Device* Sebagai Sistem Keamanan Rumah Berbasis IoT" mengembangkan sistem keamanan rumah berbasis IoT dengan memanfaatkan sensor *accelerometer* serta mikrokontroler yang saling terhubung melalui jaringan *wireless tag* yang dapat memberikan peringatan kepada pemilik rumah melalui *buzzer* dan email. selain itu penelitian ini juga memanfaatkan IFTTT sebagai penghubung adafruit dengan email untuk mengirimkan email kepada pemilik rumah berdasarkan parameter sensor yang terbaca dengan memanfaatkan MQTT *server* yang terhubung dengan mikrokontroler [10]. IFTTT digunakan sebagai penghubung untuk mengirimkan email apabila suatu kondisi tercapai. Kondisi sensor ditentukan sebagai parameter penentu untuk IFTTT mengirimkan email yang dimana apabila parameter tersebut terpenuhi maka IFTTT akan mengirimkan pesan notifikasi melalui email yang telah ditentukan sehingga pemilik rumah dapat mengetahui keadaan pintu dan jendela melalui notifikasi email.

Penelitian yang dilakukan oleh Padeli, Erick Febriyanto dam Danang Suprayogi dengan judul "*Prototype* Sistem *Smart Lock Door* Dengan *Timer* Dan Fingerprint Sebagai Alat Autentikasi Berbasis Arduino Uno Pada Ruangan" merancang sebuah sistem keamanan pintu dengan memanfaatkan *Real Time Clock* (RTC) dan juga sensor *Fingerprint* sebagai sistem kendali dari pintu tersebut [11]. Sistem keamanan pintu dengan memanfaatkan *Real Time Clock* (RTC) memiliki kelebihan karena dengan menggunakan waktu sebagai *input* dari pintu tersebut maka pemilik dapat menetapkan interval untuk membuka dan menutup pintu tersebut secara otomatis.

Penelitian dengan judul "*Prototype* Sistem Keamanan Menggunakan RFID Dan Keypad Pada Ruang Penyimpanan Di Bank Berbasis Arduino Uno" oleh Amelia Maryam Nurul Syams, Suhartini yang merancang tentang sistem keamanan pintu yang memanfaatkan keypad dan RFID [12]. Penelitian ini memiliki sistem keamanan yang berlapis dengan lapisan pertama memanfaatkan RFID apabila autentikasi menggunakan RFID telah berhasil maka selanjutnya pada lapisan kedua akan dilakukan autentikasi menggunakan *Keypad*, apabila kedua autentikasi tersebut berhasil maka pemilik dapat masuk ke ruang penyimpanan tersebut. Sistem keamanan ini memiliki sistem keamanan yang cukup baik dengan menggunakan dua faktor sebagai parameter keamanan yang mana dapat meminimalisir kemungkinan akses oleh pihak lain namun sistem keamanan ini tidak memiliki konfirmasi akses kepada pemilik ketika terjadi percobaan akses yang mana pada sistem ini masih memiliki peluang untuk pihak lain mencoba mengakses perangkat tersebut ketika memiliki RFID dan mengetahui *password* dari ruangan tersebut. Sedangkan penelitian serupa juga telah dilakukan degan judul "Rancang Bangun Sistem Keamanan Pada Brankas Menggunakan Kode Sistem Otp Dan E-Ktp Berbasis Mikrokontroller Atmega 328" oleh Muhammad Fauzi merancang metode yang lebih kompleks pada metode autentikasinya dengan tetap menggunakan RFID dan juga keypad, namun telah diperbaiki dengan menambahkan sistem *One Time Password* dan memanfaatkan modul GSM pada brankas sehingga pemilik dari brankas tersebut dapat melakukan konfirmasi jarak jauh sehingga pemilik brankas dapat mengetahui apabila terjadi percobaan akses terhadap brankas tersebut dengan *input password* yang diberikan kepada *Keypad* harus dilihat via sms yang ditujukan

sebagai bentuk konfirmasi secara langsung kepada pemilik untuk dapat membuka brankas[3]. Metode keamanan brankas dengan memanfaatkan modul GSM sebagai metode autentikasi dengan jarak jauh untuk mengirimkan *One Time Password* sangat bermanfaat untuk memberikan notifikasi dan lapisan keamanan yang lebih aman karena *password* yang diberikan akan selalu berbeda-beda untuk dijadikan *password* autentikasi dari keamanan brankas yang hanya menggunakan sistem *rf* statis yang hanya menggunakan 1 *password* yang sama di setiap kali percobaan akses dilakukan.

Sistem autentikasi keamanan brankas telah banyak dikembangkan seperti yang digunakan pada penelitian[4] dan [11] sistem keamanan yang digunakan pada penelitian ini memanfaatkan sensor sidik jari sedangkan pada penelitian [12] dan [3] menggunakan RFID dan *Keypad*. Pada penelitian [4] setelah dilakukan pengujian terhadap percobaan autentikasi dengan menggunakan objek jari yang sama sebanyak 4 kali, 2 diantaranya gagal mendeteksi sidik jari dan 2 diantaranya berhasil, dari dua keadaan sidik jari terlihat bahwa 2 kegagalan deteksi sidik jari dengan objek jari yang sama yang membuktikan sistem deteksi sidik jari masih memiliki peluang untuk tidak terbaca sedangkan penggunaan keypad pada [12] digunakan untuk autentikasi berdasarkan kata sandi yang telah ditetapkan, sedangkan pada penelitian [3] sistem keamanan brankas menggunakan keypad untuk dijadikan sistem keamanan brankas dengan mengintegrasikan modul GSM untuk memberikan *One Time Password* yang berbeda-beda sebagai bentuk verifikasi kepada pemilik untuk *input* autentikasi keamanan brankas, dari segi perancangan penggunaan *Keypad* pada penelitian ini mengharuskan peng*input*an langsung, penggunaan *Keypad* pada penelitian [3] memiliki waktu dalam pengiriman sms yaitu sebanyak 60 detik dan setiap percobaan memasukkan One time *Password* gagal maka akan melakukan proses pengiriman sms baru sistem ini memiliki kelebihan karena dapat menghindari percobaan peng*input*an *password* karena telah diberikan waktu dan batas untuk peng*input*an, namun di sisi lain juga dapat menambah waktu dari percobaan akses setiap kali salah melakukan peng*input*an *Keypad*. Selain dengan menggunakan *Keypad*, penelitian [12] dan[3] juga menggunakan sistem RFID, dimana pembacaan dari RFID dilakukan dengan pengujian jarak, RFID pada penelitian[3] dapat dideteksi hingga jarak 3,5cm

sedangkan RFID pada [12] dilakukan pengujian pembacaan RFID dengan jarak maksimal yang dapat dibaca RFID maksimal 2,5 cm pembacaan RFID yang dilakukan dipengaruhi oleh gerak rambat gelombang radio, penggunaan RFID lebih aman dikarenakan peng*input*an sudah memanfaatkan gelombang radio yang dimiliki pada *tag* pasif maupun kartu RFID sebagai parameter pembacaan dengan memperhatikan jarak antara pembaca RFID dan Kartu RFID, dan untuk waktu pengunaan RFID sebagai metode autentikasi dapat memberikan waktu akses yang lebih cepat jika dibandingkan dengan penggunaan *Keypad* karena sistem autentikasi dilakukan dengan memanfaatkan gelombang radio yang di*input* melalui pembacaan RFID, yang mana pada pengunaan *Keypad* masih harus meng*input*kan katasandi berupa angka dengan proses *input* yang bergantung kepada sms untuk mengirimkan *One Time Password* sehingga membutuhkan beberapa Perangkat.

## 2.2 DASAR TEORI

### 2.2.1 AUTENTIKASI

Autentikasi adalah suatu proses untuk melakukan identifikasi antara pengguna dan informasi yang telah tersimpan pada suatu sistem. Autentikasi dilakukan dengan memastikan kerahasiaan data setiap pengguna dan dilakukan dengan tujuan untuk memastikan bahwa pengguna yang mengakses suatu data atau objek merupakan pengguna yang otentik dengan memanfaatkan informasi yang hanya dimiliki oleh pengguna saja untuk dijadikan parameter yang disimpan sebagai informasi rahasia yang hanya dimiliki oleh pengguna dan pihak yang bertanggung jawab untuk melakukan autentikasi. Proses autentikasi yang umum digunakan adalah dengan menggunakan dua faktor *input* yaitu *username* dan *Password* sebagai dua faktor *input*, semakin banyak faktor *input* dan semakin kompleks suatu metode autentikasi maka akan mempengaruhi kekuatan keamanan terhadap serangan [13]. Autentikasi sangat penting dalam suatu sistem keamanan, autentikasi dapat dijadikan sebagai parameter untuk melakukan akses pada suatu objek ataupun informasi dan melalui autentikasi, pengguna dapat membatasi akses terhadap suatu objek maupun informasi sehingga dapat menjamin keamanan informasi maupun objek yang dilindungi.

Autentikasi merupakan salah satu bentuk pengaplikasian dari sistem keamanan. Sistem keamanan dapat diaplikasikan kedalam berbagai aspek, yaitu kerahasiaan, integritas, otentik, dan tanpa penolakan. Keempat aspek tersebut dapat dijadikan sebagai parameter yang harus dicapai dalam merancang sebuah Sistem keamanan [14]. berdasarkan keempat aspek tersebut, parameter sistem keamanan autentikasi dapat diuraikan kedalam beberapa hal diantaranya:

1. Informasi yang digunakan pada saat melakukan autentikasi bersifat rahasia dan tidak boleh diketahui oleh pihak lain
2. Dalam proses autentikasi, pengiriman informasi harus memiliki integritas untuk mencegah pengubahan informasi.
3. Pengguna harus memiliki informasi otentik dan berupa informasi asli yang digunakan untuk mengakses data atau objek, informasi tersebut dapat berupa *password*, kartu RFID, biometrik dan lain – lain.
4. Informasi yang dimiliki oleh pengguna harus sama dengan informasi yang telah tersimpan pada perangkat atau pusat informasi untuk dapat melakukan autentikasi sehingga tidak akan terjadi penolakan atau penyangkalan atas akses yang telah dilakukan selama proses autentikasi

### 2.2.2 MIKROKONTROLER

Mikrokontroler merupakan serangkaian sistem yang terdiri dari mikroprosesor dan antarmuka I/O yang mana dapat digunakan untuk melakukan pemrosesan *input* dan *output*. Mikroprosesor dari mikrokontroler berbeda dengan mikrokontroler yang dimiliki pada komputer, mikroprosesor yang dimiliki oleh mikrokontroler terdiri dari memori, cpu, eeprom dan adc [15]. ESP8266 merupakan salah satu sistem chip yang berfungsi sebagai perangkat tambahan mikrokontroler yang digunakan agar mikrokontroler dapat terhubung langsung dengan wifi, ESP8266 memiliki komponen yang terdiri dari prosesor, memori dan juga akses ke antarmuka I/O[10].

Dalam melakukan proses komunikasi pengiriman data, ESP8266 menggunakan komunikasi serial. Komunikasi serial digunakan untuk dapat memungkinkan komunikasi antara komputer dengan ESP8266 dan perangkat komunikasi lainnya [16]. Dalam komunikasi serial, data dikirimkan dalam bentuk bit dan hanya 1 bit yang dapat dikirimkan dalam satu waktu seacara sekuensial.

Berikut ini merupakan beberapa standar komunikasi yang digunakan untuk komunikasi dalam mikrokontroler:

1. *Wired* dan *Microwire*

   *Wired* dan *Microwire* merupakan salah satu standar komunikasi yang banyak digunakan untuk komunikasi mikrokontroler dengan menggunakan kabel serial. jenis komunikasi ini sering diaplikasikan untuk melakukan sistem kendali sederhana dan untuk melakukan identifikasi perangkat.

2. *Inter-Integrated Circuit (*I2C)

   *Inter-Integrated Circuit* merupakan salah satu jenis standar komunikasi yang menghubungkan antara satu IC dengan IC lainnya. I2C digunakan untuk melakukan komunikasi antara IC komputer dengan perangkat tambahan seperti mikrokontroler.

3. RS-232

   RS-232 merupakan standar komunikasi yang digunakan untuk melakukan komunikasi serial dan berfungsi sebagai standarisasi untuk antarmuka serial yang dikenal sebagai "*Serial Port*" dan "*Serial Communication Interface* (SCI)". RS232 banyak digunakan dalam pembuatan mesin otomatisasi dan *programmable Logic Controller* .

4. Wifi

   Wifi merupakan salah satu antarmuka nirkabel yang digunakan untuk menghubungkan suatu perangkat dengan Internet. Dalam komunikasinya,Wifi menggunakan standarisasi *Institute of Electrical* and *Electronic Engineering* (IEEE) dengan protokol IEEE 802.11[17].

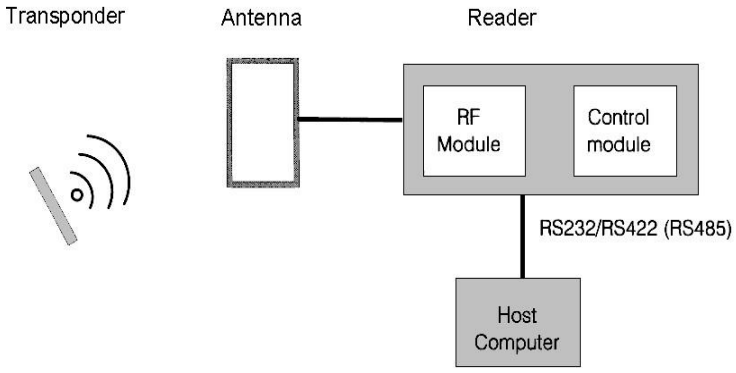
NodeMCU merupakan mikrokontroler yang didalam mikrokontroler tersebut sudah dilengkapi dengan modul ESP8266. Seperti mikrokontroler pada umumnya namun mikrokontroler NodeMCU memiliki kelebihan karena sudah termasuk dengan modul ESP8266 untuk melakukan akses terhadap jaringan wifi, selain itu

mikrokontroler ini juga memiliki chip komunikasi USB ke Serial sehingga dapat diprogram melalui komputer dengan menggunakan kabel USB [10]. Mikrokontroler NodeMCU dapat digunakan dalam membuat perangkat berbasis *Internet of Things* dikarenakan dapat melakukan interaksi dengan perangkat jaringan dengan memanfaatkan modul ESP8266 dan juga dapat diprogram dengan menggunakan komunikasi serial dengan memanfaatkan chip *USB to Serial*.

### 2.2.3 *RADIO FREQUENCY IDENTIFICATION* (RFID)

*Radio Frequency Identification* (RFID) merupakan suatu metode identifikasi yang digunakan untuk mendeskripsikan identitas dalam bentuk nomor serial unik dari sebuah objek atau manusia dengan memanfaatkan gelombang radio. Secara umum sistem RFID terdiri dari tiga komponen diantaranya:

1. Antena
2. *Transceiver (decoder)*
3. *Transponder (Radio Frequency tag)* yang telah diprogram secara elektronik dengan informasi unik.




**Gambar 2. 1 Sistem RFID[18]**

Pada Gambar 2.1 terdapat gambar Sistem RFID. Sistem RFID dapat dibagi kedalam dua bagian yaitu *transponder* (RFID *tag*) dan RFID *Reader*. Tujuan dari sistem RFID adalah untuk memungkinkan data dikirimkan melalui perangkat RFID *tag* yang nantinya akan dibaca oleh RFID *Reader* untuk selanjutnya diproses berdasarkan kebutuhan. Data yang ditransmisikan oleh RFID *tag* dapat memberikan identifikasi maupun informasi dari suatu objek. Antena digunakan

dalam sistem RFID untuk mengirimkan gelombang radio dan mengirimkan sinyal dari tag sehingga RFID *reader* dapat meneruskan informasi dalam bentuk digital kedalam sistem komputer. RFID *tag* dapat diklasifikasikan kedalam dua jenis yaitu:

1. *Tag* aktif

   *Tag* aktif merupakan jenis RFID tag yang membutuhkan sumber daya. *tag* dengan jenis ini biasanya terhubung dengan infrastruktur daya atau dengan menggunakan energi batre. RFID *tag* dengan jenis ini hanya dapat digunakan selama perangkat ini masih memiliki energi.

2. *Tag* pasif

   *Tag* pasif merupakan jenis RFID yang tidak membutuhkan sumber daya. RFID *reader* pada *tag* pasif bertanggung jawab dalam memberikan energi kepada *tag* pasif sehingga dapat berkomunikasi dengan *tag* pasif[18].

### 2.2.4 *INTERNET OF THINGS* (IOT)

*Internet of Things* (IoT) merupakan suatu konsep sistem otomatisasi dimana alat dapat terhubung melalui internet dengan memanfaatkan kemampuan transfer data melalui jaringan tanpa memerlukan manusia untuk mengendalikan proses secara manual. Teknologi micro-electromechanical systems semakin berkembang dengan memanfaatkan *Internet of Things* [6]. Penggunaan dari konsep *Internet of Things* memungkinkan komunikasi antar mesin karena komunikasi dapat dilakukan melalui internet, selain itu pemanfaatan *Internet of Things* dalam micro-electromechanical dapat membuat proses monitoring menjadi sangat berkembang karena data yang dimiliki oleh sensor seperti RFID, *Accelerometer, fingerprint* dan lain-lain dapat dikirimkan melalui internet untuk selanjutnya dijadikan parameter untuk membuat sistem kendali jarak jauh ataupun hanya sekedar menjalankan proses *monitoring*.

Dalam menjalankan sistemnya perangkat berbasis Internet of Things menggunakan beberapa protokol komunikasi. Dalam konsep Internet of Things terdapat sistem client dan server yang dimana server merupakan penyedia layanan dan client merupakan pengguna layanan, sistem *client* dan *server* ini banyak dipakai dalam protokol komunikasi. Protokol komunikasi dalam sistem *Internet of Things* dapat memberikan layanan yang dibutuhkan dalam sistem IoT itu sendiri.

berikut ini merupakan beberapa protokol yang digunakan dalam komunikasi perangkat berbasis *Internet of Things* :

1. HTTP

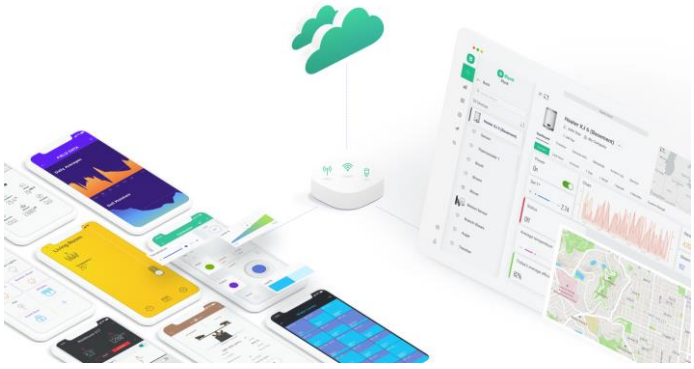
   Pada perangkat IoT, protokol ini digunakan untuk meminta objek dalam bentuk *hypertext* dan kemudian akan direspon dengan pengiriman objek oleh *server* atau penyedia layanan IoT.

2. *Publish/Subscribe*

   *Publish/Subscribe* digunakan dalam perangkat IoT untuk mengirim dan menerima pesan yang diantarai oleh broker untuk mengirim dan menerima pesan.

3. REST

   Protokol REST digunakan dalam Komunikasi perangkat IoT untuk mengakses layanan berbasis web. REST dapat digunakan untuk mentransfer data dimana client dapat mengakses sumber daya dengan menggunakan perintah *GET,PUT,POST*, dan *DELETE* [19].



**Gambar 2. 2 *Platform* IoT [20]**

*Platform Internet of Things* digunakan untuk membuat project berbasis *Internet of Things* dimana pengguna dapat menghubungkan mikrokontroler ke jaringan internet sehingga dapat melakukan akses dan interaksi secara bebas secara online. Salah satu *platform* yang saat ini banyak digunakan dalam membuat project otomatisasi menggunakan mikrokontroler adalah Antares, Firebase, IFTTT dan Blynk [21]. Penggunaan *platform* IoT ini memungkinkan mikrokontroler melakukan interaksi-interaksi tambahan karena dengan terhubung melalui *platform*

tersebut seperti pada gambar 2.2 dimana pengguna dapat melakukan interaksi antara *smartphone* dan aplikasi dengan perantara *Platform Internet Of Things*. Pengguna dapat membuat sistem monitoring yang dapat diakses melalui perangkat apa saja selama perangkat tersebut terhubung dengan internet karena data yang dimiliki oleh mikroprosesor dapat dikirimkan dan diterima melalui *platform* tersebut disaat yang bersamaan dapat dijadikan sebagai media untuk membuat aplikasi untuk sistem kendali mikroprosesor berbasis *Internet of Things*.

**Gambar 2. 3 *Platform* Blynk[20]**

Blynk merupakan salah satu *platform* IoT berbasis mobile yang dapat diakses melalui aplikasi pada *smartphone* android dan IOS. Aplikasi ini mengizinkan penggunaan kendali jarak jauh dengan perangkat yang terhubung dengan aplikasi ini dan mengambil data untuk dilakukan visualisasi. Dalam aplikasi ini pengguna dapat membuat *widget* sederhana hingga *widget* kompleks yang dapat dijadikan sebagai sistem kendali dengan mengirimkan data dari kepada *hardware* untuk dieksekusi sebagai perintah kendali [20]. Aplikasi blynk dengan ikon seperti pada gambar 2.3, dapat digunakan sebagai *platform* IoT untuk desain perangkat elektronika sederhana. Aplikasi ini dapat menjalankan sistem kendali jarak jauh ketika perangkat terhubung dengan sehingga memungkinkan untuk membuat project mikrokontroler sederhana berbasis IoT.

**Gambar 2. 4 *Platform* IFTTT[22]**

Pada Gambar 2.4 terdapat aplikasi *IF This Then That* (IFTTT). Aplikasi IFTTT merupakan *platform* yang berfungsi untuk menghubungkan dua atau lebih layanan menjadi *Applets*. Aplikasi ini dapat menghubungkan lebih dari 700 aplikasi dan layanan berbeda termasuk Twitter, Dropbox, Evernote, Fitbit, Amazon Alexa

and Google Assistant. *Applets* dapat mengeksekusi lebih dari satu perintah dan juga dapat menggunakan filter untuk mengeksekusi perintah apabila kondisi yang diberikan terpenuhi [22]. Layanan Google Assistant dihubungkan dengan layanan Blynk melalui IFTTT dan disatukan menjadi *Applet* yang menjadi satu fungsi dimana perintah suara yang dimasukkan akan dijadikan kondisi untuk selanjutnya dikirimkan ke *platform* Blynk yang nantinya akan mengirimkan perintah kepada NodeMCU untuk dijalankan.

### 2.2.5 *VOICE COMMAND*

*Speech Recognition* atau pengenalan suara adalah teknik yang digunakan untuk memahami dan mengenali suara manusia. Dengan menggunakan speech recognition, mesin dapat memiliki kemampuan linguistik untuk memahami makna atau arti dari suatu kata. Salah satu pemanfaatan pengenalan suara adalah dengan kecerdasan pengendalian suara atau *Intelligent voice control* (IVC) telah banyak digunakan untuk interaksi antar mesin dan manusia. Sistem kendali dengan menggunakan pengenalan suara dapat digunakan untuk melakukan penafsiran untuk mengetahui perintah suara alami dan melakukan eksekusi terhadap operasi yang sesuai dengan yang dikirimkan. Salah satu implementasi *intelligent voice control* dengan menggunakan Google Assistant untuk melakukan eksekusi perintah dengan menggunakan perintah suara (*Voice Command*) [23].


**Gambar 2. 5 Google Assistant[24]**

Pada gambar 2.5, terdapat aplikasi Google Assistant yang merupakan suatu *Software* yang berfungsi untuk membantu pengguna dalam mengerjakan pekerjaan sehari-hari. Google Assistant dapat berinteraksi dengan aplikasi berbasis android dan mampu meningkatkan kinerja aplikasi dengan memberikan akses perintah suara. Google Assistant dapat dijadikan sebagai perancangan aplikasi berbasis perintah suara, dapat menjalankan pencarian konten dengan mengakses google search dan juga dapat dihubungkan dengan perangkat rumah pintar untuk

mengendalikan kunci, lampu, dan mesin sederhana [24]. Pemanfaatan *voice command* saat ini telah banyak digunakan sebagai alat otomatisasi seperti asisten virtual dan pengendalian perangkat elektronika. Google Assistant dapat dimanfaatkan sebagai alat otomatisasi karena memiliki kemampuan untuk mengubah *input* suara menjadi perintah yang diintegrasikan kedalam perangkat berbasis *Internet of Things* sehingga memungkinkan pengendalian dan otomatisasi dengan menggunakan komunikasi yang dilakukan melalui jaringan internet.