



## **PROPOSAL SKRIPSI**

**Rancang Bangun *Smart Lock System* menggunakan *QR-Code* pada  
Loker Perpustakaan Fakultas Teknik Universitas Riau**

**Oleh:**

**Luthfi Afif**

**NIM : 1507116911**

**PROGRAM STUDI TEKNIK ELEKTRO S1**

**FAKULTAS TEKNIK**

**UNIVERSITAS RIAU**

**2020**

## **HALAMAN PENGESAHAN**

Proposal skripsi dengan judul “Rancang Bangun *Smart Lock System* menggunakan *QR-Code* pada Loker Perpustakaan Fakultas Teknik Universitas Riau”

Yang dipersiapkan dan disusun oleh

**Luthfi Afif**

**NIM. 1507116911**

Program Studi Teknik Elektro S1, Fakultas Teknik Universitas Riau

**Menyetujui,**

**Dosen Pembimbing I**

**Dr. Yusnita Rahayu, ST., M.Eng**

**NIP. 19751104 200501 2 001**

Mengetahui,

Koordinator Program Studi Teknik Elektro S1

Fakultas Teknik Universitas Riau

**Feranita, ST., MT**

**NIP. 19730201 200501 2 002**

## DAFTAR ISI

<b>DAFTAR ISI.....</b>	<b>iii</b>
<b>DAFTAR GAMBAR.....</b>	<b>iv</b>
<b>DAFTAR TABEL .....</b>	<b>v</b>
A. Judul Penelitian .....	1
B. Bidang Ilmu .....	1
C. Latar Belakang .....	1
D. Rumusan Masalah .....	4
E. Batasan Masalah .....	4
F. Tujuan Penelitian .....	5
G. Manfaat Penelitian .....	5
H. Tinjauan Pustaka .....	5
H.1. Penelitian Terkait .....	5
H.2. Teori Dasar.....	7
I. Metodologi Penelitian .....	21
J. Hasil Sementara .....	26
J.1 Pemograman Alat .....	26
J.2 Implementasi dan Pengukuran Alat .....	28
K. Kesimpulan .....	31
L. Jadwal Kegiatan .....	32
M. Rancangan Biaya .....	33
DAFTAR PUSTAKA .....	34

## DAFTAR GAMBAR

Gambar 1. Kode QR.....	8
Gambar 2. Struktur Kode QR .....	9
Gambar 3. Sistem Komunikasi Wi-Fi.....	10
Gambar 4. Solenoid.....	13
Gambar 5.Prinsip Kerja Solenoid .....	13
Gambar 6. Bentuk komponen Relay .....	14
Gambar 7. Simbol Relay NO dan NC .....	15
Gambar 8. NodeMCU8266 .....	15
Gambar 9.GPIO NodeMCU ESP8266.....	16
Gambar 10. Software ARDUINO IDE .....	18
Gambar 11. Diagram alir metodologi penelitian.....	22
Gambar 12.Perancangan Aplikasi.....	23
Gambar 13. Perancangan Sistem.....	24
Gambar 14.Rangkaian alat pengontrolan Smart Lock System .....	25
Gambar 15.Proses pemograman menggunakan Arduino IDE .....	27
Gambar 16. Komponen Alat Hasil Sementara .....	28
Gambar 17. Tampilan ketika Solenoid bernilai 0 .....	29
Gambar 18. Tampilan Ketika Solenoid bernilai 1 .....	30
Gambar 19. Hasil Pengukuran Alat (a) Tanpa beban (b) Nyala/diberi beban .....	30

## DAFTAR TABEL

Tabel 1. Kategori <i>Throughput</i> .....	20
Tabel 2. Kategori Standar <i>Packet Loss</i> .....	21
Tabel 3. Perkiraan Jadwal Pelaksanaan Penelitian .....	32
Tabel 4. Pengeluaran lain-lain ( administrasi, publikasi dan operasional) .....	33

## OUTLINE PROPOSAL

### A. Judul Penelitian

Rancang Bangun *Smart Lock System* menggunakan *QR-Code* pada Loker Perpustakaan Fakultas Teknik Universitas Riau

### B. Bidang Ilmu

Teknik Elektro – Telekomunikasi

### C. Latar Belakang

Sistem keamanan sangat diperlukan untuk mencegah tindak kejahatan pencurian atau tindak kejahatan kriminal lainnya, hal ini dibuat untuk mencegah tingkat kejahatan pencurian yang meningkat dari tahun ke tahun (Subrata & Gozali, 2018). Biasanya orang-orang menggunakan sistem keamanan dengan kunci konvensional dan kunci berupa pin code. Namun, kunci ini memiliki beberapa kekurangan seperti salah tempat menyimpan kunci atau lupa kata sandi. (Kassem et al., 2016)

Sistem keamanan yang tengah populer digunakan pada saat ini adalah dengan menggunakan bantuan teknologi IoT (*Internet of Things*). IoT adalah sebuah konsep yang membahas seputar jaringan informasi global yang terdiri dari hal-hal seperti perangkat pintar, sensor, aktuator serta protokol jaringan yang digunakan untuk berkomunikasi dengan server cloud atau database yang memproses dan mengolah data besar yang datang dari berbagai perangkat, lalu dianalisis dan membantu dalam pengambilan keputusan. (Cynthia et al., 2019). Salah satu aplikasi sistem keamanan pada IoT dapat diterapkan pada *Smart Lock System*.

Smart Lock System biasanya terdiri dari tiga bagian. Pertama adalah Kontroller pengunci (*Door Lock Controller*) sebagai pengunci, Kontrol pusat (*Central Controller*) sebagai pusat pengendalian kunci untuk membuka dan menutup atau mengeksekusi perintah yang krusial dalam sistem tersebut dan Aplikasi Seluler (*Mobile Application*) berfungsi sebagai tempat perintah dimana kunci untuk membuka perangkat digunakan dan

juga dapat berfungsi untuk mendaftarkan anggota keluarga atau mendaftarkan tamu. (Kassem et al., 2016).

Beberapa penelitian mengenai *Smart Lock System* telah dilakukan. Contohnya penelitian yang dilakukan oleh Ilkyu ha (2015) yang membahas tentang kunci pintu digital dengan fungsi keamanan yang ditingkatkan dirancang untuk bekerja dengan Internet of Things. Penelitian ini menggunakan sensor kamera, *keypad*, sensor *ultrasonic* dan sensor pendeteksi gerakan. Setiap sensor yang dipasang berfungsi untuk memvalidasi pengguna dalam 2 detik. Contohnya, pada sensor *ultrasonic* mampu membaca dan memvalidasi pengguna dalam waktu 1.6 detik sampai 1.8 detik. Alat ini memiliki rata-rata 1.4 detik dalam memvalidasi pengguna, mengambil gambar dan mengirimkannya ke perangkat seluler. Namun alat ini memiliki kelemahan yaitu ketika pengguna yang tidak tervalidasi memasukkan kata sandi yang salah, maka dia dapat menutup kamera dengan tangan atau menggerakkan wajah sehingga hasil pengambilan gambar pada kamera tersebut menjadi tidak akurat. (Ha, 2015).

Sedangkan pada penelitian yang dilakukan oleh Rasid (2018) yang membahas tentang desain dan konstruksi sistem keamanan pintu otomatis dengan menggunakan teknologi RFID (*Radio Frequency Identification*). Penelitian ini menggunakan dua *tag* RFID untuk membedakan masing-masing pengguna yang mana kedua *tag* ini sudah diprogram terlebih dahulu. Kedua *tag* ini dapat bekerja dan dikenali oleh sistem sehingga pintu dapat terbuka otomatis hanya dalam waktu kurang dari 4 detik saja, sedangkan untuk proses *scanning* hanya dapat dilakukan dalam jarak 5 cm. (Rasid et al., 2018)

Kedua metode diatas memang sudah cukup bagus dari segi keamanan. Namun, tidak efektif jika digunakan di ruang publik dimana akses pintu akan digunakan oleh banyak pengguna. Metode keamanan dengan menggunakan sensor *biometric* berupa sidik jari, mata, suara serta pengenalan wajah memiliki kelemahan diantaranya membutuhkan biaya yang mahal untuk memiliki alat pemindai dengan sensitivitas yang tinggi serta akurat. Sedangkan Metode pengamanan dengan RFID, pin digital ataupun

dengan *physical key* (kunci fisik konvensional) memiliki kekurangan karena terdapat resiko kehilangan kunci dan kata sandi yang terlupakan. Sehingga selain biaya perawatan juga terdapat resiko tambahan biaya untuk fabrikasi, duplikasi dan distribusi kunci yang hilang.

Sehingga pada penelitian ini akan digunakan kode QR sebagai kunci untuk mengakses pintu yang akan digunakan. Penggunaan kode QR dapat mewakili teks yang kemudian digunakan oleh perangkat seluler untuk melakukan suatu tindakan. Kode bisa dibuat untuk menautkan langsung ke URL (*Uniform Resource Locator*), membuat vCard (Kartu virtual yang dapat disimpan ke perangkat seluler) atau memulai panggilan telepon, teks atau e-mail dan fungsi-fungsi lainnya (Parabhoi et al., 2017). Struktur kode QR terlalu rumit untuk manusia, tetapi mesin dapat membaca dan mendekode kode QR dengan mudah. Ini membuat kode QR sangat cocok untuk perangkat yang sering digunakan dalam IoT karena banyak smartphone modern dilengkapi dengan kamera dan perangkat lunak pemindaian (Marktscheffel et al., 2016). Lalu untuk pengamanan tambahan agar akses pintu tidak digunakan oleh pihak yang tidak bertanggung jawab pengguna diharuskan mendaftar dan membuat akun pada *central controller* yang berupa *data base*. Proses pendaftaran ini juga diakses pada perangkat seluler pengguna.

Dalam penelitian ini akan dilakukan perancangan dan pengujian terhadap sistem dan alat yang akan diterapkan pada loker di perpustakaan Fakultas Teknik Universitas Riau (FT-UR). Metode observasi telah dilakukan dengan menggunakan wawancara dengan pihak perpustakaan FT-UR serta kuesioner online untuk mengetahui permasalahan umum yang terjadi di perpustakaan FT-UR. Data yang didapatkan dari hasil wawancara adalah kondisi loker yang hanya memiliki penghalang kecil sebagai penutup loker membuat loker menjadi rawan kasus pencurian ataupun barang yang tertukar pada saat perpustakaan ramai pengunjung dan penggunaan kunci konvensional terkadang memiliki berbagai permasalahan seperti hilangnya anak kunci ataupun terbawa pulang oleh Mahasiswa.



Sedangkan dari hasil kuesioner online didapatkan data sebanyak 4.2% responden pernah mengalami kehilangan barang, sebanyak 18% merasa tidak aman, 66% merasa kurang aman dan 10% merasa aman. Sebanyak 96.2% responden setuju agar keamanan loker perpustakaan FT-UR ditingkatkan lagi. Oleh karena itu penelitian ini dibuat dan ditujukan untuk meningkatkan keamanan sebagai salah satu tindakan pencegahan pencurian ataupun untuk menghindari resiko terjadinya barang yang tertukar sehingga mahasiswa dapat berkunjung ke perpustakaan dengan nyaman tanpa harus khawatir kehilangan barang ataupun tertukar.

#### **D. Rumusan Masalah**

Dari latar belakang tersebut, rumusan masalah yang akan dibahas pada penelitian ini adalah:

1. Bagaimana perancangan alat yang dilakukan dengan NodeMCU ESP8266 sebagai mikrokontroler dan aplikasi android sebagai perangkat untuk antarmuka dan pembacaan *QR-code*.
2. Bagaimana menganalisa efektifitas dan perbandingan antara *Smart Lock System*, Kunci fisik konvensional dan *Digital Door Lock System*
3. Bagaimana pengaruh kualitas kecepatan Internet dan pengaruh kualitas sistem yang digunakan terhadap *delay* yang akan ditimbulkan.

#### **E. Batasan Masalah**

Batasan masalah dari penelitian ini antara lain:

1. Penelitian ini menghasilkan Satu alat dan sistem aplikasi yang mana ini adalah prototipe yang nantinya diimplementasikan pada loker yang ada di perpustakaan Fakultas Teknik Universitas Riau.
2. Lokasi penelitian ini dilakukan pada loker Perpustakaan Fakultas Teknik Universitas Riau.

## **F. Tujuan Penelitian**

Adapun tujuan dari pembuatan tugas akhir ini adalah sebagai berikut:

1. Merancang sebuah alat dan aplikasi *Smart Lock System* yang dapat membuka kunci loker dengan menggunakan proses *scan QR code*
2. Menghasilkan sebuah alat atau sistem yang lebih aman dan efektif dibandingkan dengan alat yang sudah terpasang sebelumnya pada loker FT-UR.

## **G. Manfaat Penelitian**

Menghasilkan sebuah alat dan sistem aplikasi android yang mampu memindai QR-Code untuk mengakses loker yang ada pada perpustakaan Fakultas Teknik Universitas Riau dan dengan adanya sistem aplikasi ini sistem keamanan pada loker dapat ditingkatkan sehingga mahasiswa diharapkan dapat berkunjung dengan nyaman tanpa khawatir dengan masalah keamanan loker serta pegawai perpustakaan tidak perlu khawatir mengenai kehilangan kunci pada loker tersebut.

## **H. Tinjauan Pustaka**

### **H.1. Penelitian Terkait**

Pada penelitian yang dilakukan oleh Hazarah dkk,2019 yang membahas tentang Rancang Bangun Smart Door Lock menggunakan *QR Code* dan Solenoid, penelitian ini menjelaskan bagaimana proses pembuatan dan perancangan alat keamanan rumah secara otomatis dengan menggunakan arduino uno sebagai mikrokontroller dari solenoid dan android sebagai pembaca QR-code dengan menggunakan Bluetooth HC05 untuk koneksi dari arduino ke aplikasi android. Untuk menjalankan alat ini diperlukan *power supply* sebagai sumber daya untuk alat tersebut. Setelah itu, nyalakan Bluetooth pada smartphone dan hubungkan ke Bluetooth HC-05 yang terhubung dengan Arduino. Setelah terkoneksi satu dengan yang lain, kemudian buka aplikasi Barcode Scanner di android pada smartphone.

Setelah itu lakukan *scanning QR Code* menggunakan *smartphone*. Kemudian secara otomatis *relay* akan mengontrol dan membuka pintu tersebut. Alat ini dapat bekerja dan membaca QR code dalam jarak 10 meter (Hazarah,2019).

Penelitian serupa juga dilakukan oleh Rao dkk ,2017 yang berjudul tentang QR Code for Safety and Security Applications menjelaskan tentang penggunaan QR code sebagai pengaman pada pintu mobil. Penelitian ini dilakukan dengan Atmega328P pada Arduino uno sebagai mikrokontroller dan module HC-05 Bluetooth sebagai komunikasi *wireless* sehingga dapat memutar motor servo (Micro Servo DXW90) sekitar 180 derajat (90 derajat setiap putaran) digunakan untuk mebuca dan mengunci pintu mobil. Pengunci pintu sebelumnya sudah diprogram dengan data yang sudah terenkripsi dan nantinya akan dicocokkan dengan aplikasi pengunci sehingga sulit untuk diretas sedangkan perancangan aplikasi dilakukan menggunakan MIT App inventor.

Al-Ghaili dkk,2019 juga melakukan penelitian menggunakan kode QR, penelitian tersebut berjudul “*Smart Verification Algorithm for IoT Applications using QR Tag*”. Dalam penelitian ini dijelaskan *Smart Verification Algorithm* (SVA) digunakan dengan Internet of Things (IOT) sebagai aplikasi yang diusulkan dalam melakukan prosedur verifikasi untuk mengaktifkan fitur otorisasi permintaan pengguna agar dapat mengakses sistem pintar dengan bantuan *Tag QR* yang terenkripsi. Untuk tujuan keamanan penelitian ini menggunakan tiga lapis tahap verifikasi. Lapisan pertama mengimplementasikan perbandingan untuk menjaga sistem terintegrasi. Di lapisan kedua, nilai-nilai asli disimpan dalam penyimpanan database offline untuk menonaktifkan akses yang disebabkan oleh ancaman. ketiga menggunakan tag QR yang telah diautentikasi menggunakan *1-session private key* untuk mencegah kebocoran informasi dan akses yang tidak sah. SVA bertujuan untuk meningkatkan keamanan dan privasi sistem. Hasil penelitian ini mengkonfirmasi bahwa teknik ini lebih cepat daripada teknik kompetitif lainnya (Al-Ghaili et al., 2019).

Kanumuru dkk (2018) juga membahas tentang penggunaan QR code untuk mengetahui ketersediaan tempat parkir dalam ruangan seperti basement. Setiap tempat parkir diberi kode QR. Ketika kendaraan akan memasuki tempat parkir, sensor akan mendeteksi kendaraan tersebut lalu kode QR akan otomatis dibuat dan diberikan kepada pengemudi untuk parkir ke tempat yang sudah diberikan. Nomor kendaraan dan jumlah slot parkir kemudian akan di update pada database. Jika pengemudi lupa dimana memarkir kendaraan mereka ,maka dengan melakukan scanning pada kode QR sehingga lokasi kendaraan nantinya akan diketahui. Sebelum pengemudi meninggalkan tempat parkir, kode QR akan di scan kembali pada pintu keluar dan setelah mobil keluar meninggalkan tempat parkir maka database akan di update kembali. (Kanumuru, 2018)

Penelitian yang lain dilakukan juga oleh Aathira yang berjudul E Toll System Using IoT ini membahas cara kerja *tag* QR code dan RFID ( *Radio Frequency Identification* ) yang nantinya akan digunakan pada proses pembayaran toll. penelitian ini dilakukan untuk mengurangi kemacetan di pintu toll yang disebabkan oleh antrian pembayaran. Sistem ini bekerja dengan cara setiap kendaraan harus memiliki RFID transmitter yang bertujuan untuk mentrasfer informassi kendaraan tersebut. Informasi setiap kendaraan yang melewati pintu toll akan dibedakan dengan tag RFID, tag RFID ini mengandung antenna dan chip yang berisi tentang informasi pengguna dan jenis kendaraan yang dimilikinya. Ketika tag RFID mendekati RFID reciever yang sudah dipasang dan terintegrasi pada komputer di pintu toll maka data kendaraan dan pengguna akan didapatkan. Selanjutnya pembayaran otomatis akan dilakukan bersamaan dengan foto kendaraan ketika akan melewati pintu gerbang toll lalu kemudian akan tersimpan di *database*. (Aathira et al., 2018)

## **H.2. Teori Dasar**

### **1. Kode QR ( *QR code* )**

*QR code* adalah singkatan dari *Quick Response code*. Kode QR pertama kali dibuat pada tahun 1994 oleh Denso Wave Incorporated, di

Jepang. Denso Wave adalah perusahaan induk Toyota. Kode QR dirancang untuk pengelolaan pabrik pembuat mobil dan persediaan suku cadang mobil. (Chang, 2014) Adapun contoh gambar kode QR ditunjukkan pada gambar 1.



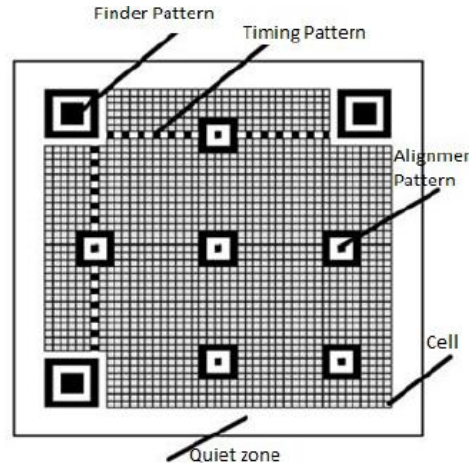
Gambar 1. Kode QR

Sistem ini pada dasarnya adalah kode batang matriks yang dibuat untuk mengautentikasi pengguna atau perangkat. Kode QR dapat menyimpan data dalam dua dimensi, baik horizontal maupun vertikal sehingga memungkinkan untuk menampung data yang lebih besar jika dibandingkan dengan kode batang tradisional karena secara statistik kode QR dapat menyimpan 4296 karakter alfanumerik didalamnya dimana 20 kali karakter lebih banyak jika dibandingkan dengan barcode tradisional. (Vaidhyesh et al., 2018)

Jumlah data yang dapat disimpan dalam simbol QR Code tergantung pada tipe data, versinya dan tingkat koreksi kesalahan. Kapasitas penyimpanan maksimum ditandai dengan simbol 40-L (versi 40, koreksi kesalahan level L). Berikut ini adalah banyak kapasitas penyimpanan yang dapat dipakai berdasarkan jenis data yang digunakan (Várallyai, 2013) :

- 1) numerik maksimal sebanyak 7089 karakter (0-9)
- 2) Alphanumerik maksimal sebanyak 4296 karakter (0-9, A – Z, [hanya huruf besar], spasi, \$, %, \*, +, -, ., /, :)
- 3) Biner/Byte maksimal sebanyak 2953 karakter (8-bit byte, 23624 bit)
- 4) Kanji/Kana maksimal sebanyak 1817 karakter.

Untuk membaca dan menyimpan data atau informasi rahasia kode QR memiliki beberapa struktur dalam melindungi data tersebut. Adapun struktur kode QR adalah sebagai berikut (V. Ramya, 2014):



Gambar 2. Struktur Kode QR

a) *Finder Pattern*

Posisi pola kode QR sudah terdeteksi, pola ini digunakan untuk mengidentifikasi dengan benar tentang sudut dan dimensi dari kode QR.

b) *Alignment Pattern*

Untuk memperbaiki segala jenis distorsi setelah kode QR dipindai, pola ini sangat tinggi bermanfaat. Modul hitam di tengah pola membuat identifikasi distorsi ini sangat sederhana dan efisien.

c) *Timing Pattern*

Pola ini adalah pola pendukung yang membantu untuk mengidentifikasi pusat koordinat, jika terdapat kesalahan maka akan terlihat pada kedua arah baik horizontal maupun vertikal.

d) *Quiet Zone*

ini merupakan identifikasi kode QR dari latar belakang dan disederhanakan untuk teknik penyimpanan data.

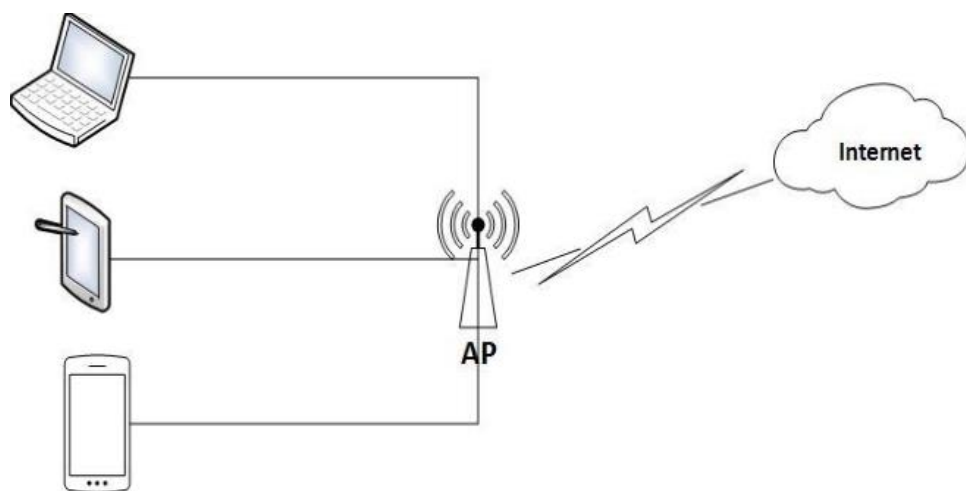
e) *Data Area*

Pada area ini data informasi secara rahasia disematkan. jika kode QR dalam format biner maka dapat disematkan dengan mudah, angka nol di hitam dan satu di putih. metode ini sangat mudah untuk

menyembunyikan informasi dan koreksi kesalahan juga ditambahkan dengan metode *Reed-Solomon*

## 2. WLAN

Wireless LAN (WLAN) atau disebut juga *Wireless Fidelity* (Wi-Fi) merupakan teknologi yang digunakan untuk melakukan perpindahan data dari satu perangkat ke perangkat lainnya tanpa menggunakan kabel sebagai media transmisinya dengan memanfaatkan radiasi elektromagnetik atau disebut juga gelombang radio. Meskipun kehadiran teknologi ini tidak menggantikan peran jaringan kabel secara keseluruhan, namun sejak kehadirannya teknologi ini telah memudahkan penggunaannya untuk terkoneksi ke jaringan global (Afdhal, 2014). Dengan adanya teknologi WiFi ini perangkat seperti komputer pribadi, Telepon pintar, *Personal Digital Assitant* ataupun terminal lainnya dapat saling terhubung. Umumnya untuk mempersiapkan jaringan nirkabel ini biasanya membutuhkan titik akses (Access Point) dan adaptor jaringan nirkabel tersebut sebagai kebutuhan dasar. Adapun alat yang digunakan untuk mengakses Wi-Fi dapat dilihat pada gambar 3.



Gambar 3. Sistem Komunikasi Wi-Fi

Wi-Fi sendiri awalnya adalah sebuah merek teknologi komunikasi jaringan nirkabel yang dipegang oleh WiFi Alliance. Wi-Fi pertama kali

diluncurkan pada tahun 1997 dengan menggunakan standar yang sudah ditetapkan oleh organisasi IEEE (*Institute of Electrical and Electronics Engineers*) yaitu 802.11. Hingga saat ini, Wi-Fi sudah memiliki banyak perkembangan sehingga terdapat beberapa standarisasi yang umum digunakan yaitu (Arief, 2013):

a) Standar 802.11a

Digunakan untuk mendefinisikan jaringan wireless yang menggunakan frekuensi 5 GHz Unlicensed National Information Infrastructure (UNII). Kecepatan jaringan ini lebih cepat dari standar 802.11. Walaupun standar 802.11a memiliki kesamaan dengan standar 802.11b pada lapisan Media Access Control (MAC), ternyata tetap tidak kompatibel dengan standar 802.11 atau 802.11b karena pada standar 802.11a menggunakan frekuensi radio 5 GHz sementara pada standar 802.11b menggunakan frekuensi 2,4 GHz.

b) Standar 802.11b

Standar 802.11b merupakan standar yang paling banyak digunakan di kelas standar 802.11. Standar ini merupakan pengembangan dari standar 802.11 untuk lapisan fisik dengan kecepatan tinggi. 802.11b digunakan untuk mendefinisikan jaringan wireless direct-sequence spread spectrum (DSSS) yang menggunakan gelombang frekuensi industrial, scientific, medicine (ISM) 2,4 GHz dan berkomunikasi pada kecepatan hingga 11 Mbps. Standar 802.11b juga kompatibel dengan semua perangkat DSSS yang beroperasi pada standar 802.11.

c) Standar 802.11g

Standar 802.11g pada dasarnya mirip dengan standar 802.11a yaitu menyediakan jalur komunikasi kecepatan tinggi hingga 54 Mbps. Namun, frekuensi yang digunakan pada standar ini sama dengan frekuensi yang digunakan standar 802.11b yaitu frekuensi gelombang 2,4 GHz dan juga dapat kompatibel dengan standar 802.11b. Hal ini tidak dimiliki oleh standar 802.11a. Perangkat-perangkat pada standar 802.11g menggunakan modulasi OFDM untuk memperoleh kecepatan transfer data berkecepatan tinggi.



Tidak seperti perangkatperangkat pada standar 802.11a, perangkatperangkat pada standar 802.11g dapat secara otomatis berganti ke quadrature phase shift keying (QPSK) untuk berkomunikasi dengan perangkatperangkat pada jaringan wireless yang menggunakan standar 802.11b.

d) Standar 802.11n

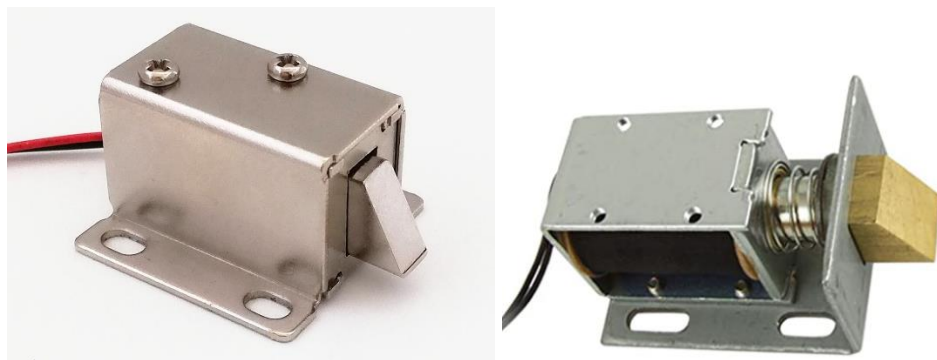
802.11n merupakan standar yang memprioritaskan *High Throughput* (HT) sehingga sebuah *datastream* dapat didistribusikan dengan cara membagi menjadi beberapa bagian yang disebut dengan *spatial stream* dan mengirimkannya masing-masing *spatial stream* melalui antena yang berbeda-beda. Standar 802.11n mampu mentransmisikan data dengan kecepatan sampai dengan 600 Mbps dan menggunakan HT-OFDM yang dapat beroperasi pada pita frekuensi 2.4 GHz dan 5GHz. Fitur utama dari standar IEEE 802.11n adalah kapabilitas dari Multiple Input Multiple Output (MIMO) untuk meningkatkan datarate sehingga mencapai jumlah ratusan mega bit per detik. Teknik MIMO memanfaatkan penggunaan beberapa antena untuk meningkatkan jarak, kehandalan dan kecepatan pen-transmisian data (Afdhal, 2014).

e) Standar 802.11ac

Pada rancangan Standar 802.11ac, sejumlah peningkatan dilakukan meliputi: pelebaran pita kanal (80 dan 160 MHz), peningkatan aliran data (*spatial data streams*) sampai dengan delapan streams, dan menambahkan metode 256 Quadrature Amplitude Modulation (256-QAM) untuk mengefisienkan teknik modulasi pada lapisan PHY. Untuk mendukung hal tersebut IEEE menetapkan bahwa 802.11ac beroperasi pada pita frekuensi dibawah 6 GHz dan teknik antena yang digunakan adalah Multiple-User MIMO (MU-MIMO). Standar ini juga menyederhanakan transmisi beamforming dan memperbesar agregasi frame-frame data pada lapisan MAC (Afdhal, 2014).

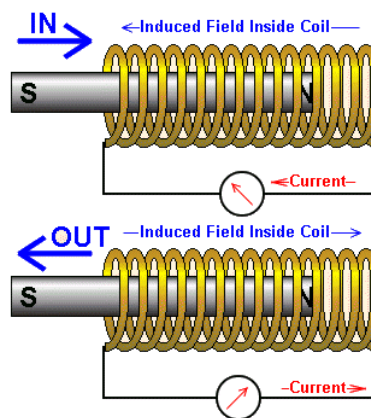
### 3. Solenoid

Prinsip solenoid pada dasarnya adalah menggunakan elektromagnet. Prinsip solenoid ini ditemukan oleh fisikawan perancis yang bernama Andre Marie Ampere. Pada bidang rekayasa istilah ini menunjukkan pada perangkat transduser yang mengkonversi energi ke gerakan linear (Arafat, 2016). Solenoid terbuat dari kumparan kawat tembaga dan sebuah armature (batang logam) di bagian tengah. Adapun gambar solenoid dapat dilihat pada gambar 4.



Gambar 4. Solenoid

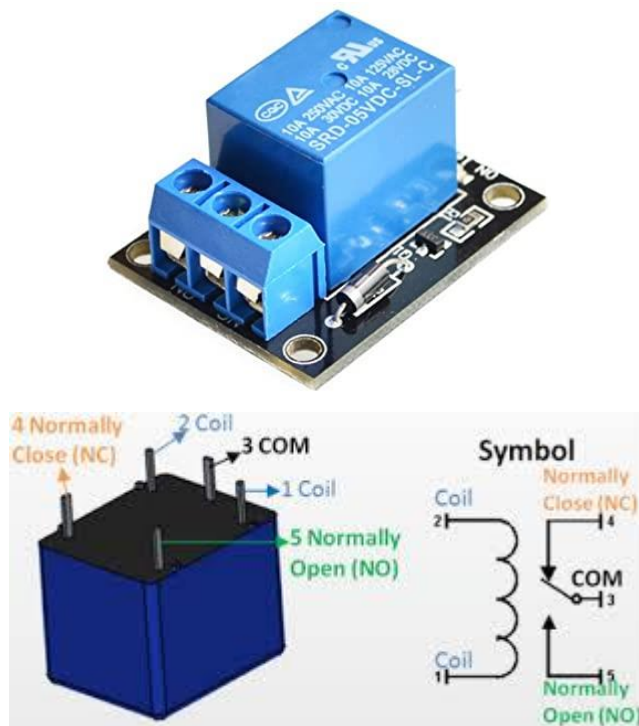
Solenoid bekerja ketika kumparan diberi energi listrik, maka gaya elektromagnet akan menarik batang logam ke dalam pusat kumparan secara linear begitu juga dengan sebaliknya. Prinsip kerja solenoid dapat dilihat pada gambar 5.



Gambar 5. Prinsip Kerja Solenoid

#### 4. Relay

Relay adalah Saklar (Switch) yang dioperasikan secara listrik dan merupakan komponen Electromechanical (Elektromekanikal) yang terdiri dari 2 bagian utama yakni Elektromagnet (Coil) dan Mekanikal (seperangkat Kontak Saklar/Switch). Relay menggunakan Prinsip Elektromagnetik untuk menggerakkan Kontak Saklar sehingga dengan arus listrik yang kecil (low power) dapat menghantarkan listrik yang bertegangan lebih tinggi (Saleh & Haryanti, 2017). Relay tersusun dari empat komponen yaitu elektromagnet (*coil*), *armature*, saklar dan *spring*. Adapun gambar bentuk dan komponen relay ditunjukkan pada gambar 6.



Gambar 6. Bentuk komponen Relay

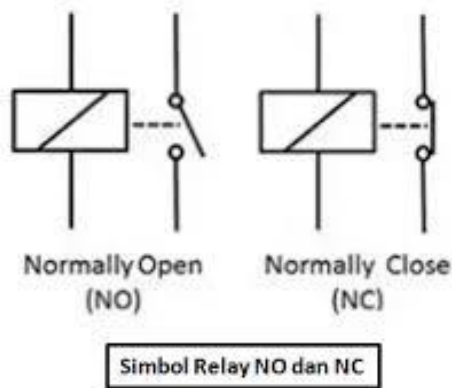
Sedangkan dari segi jenis terdapat dua macam jenis relay yaitu:

- a) Normally Open (NO)

Pada saat keadaan NO kondisi awal saklar relay akan selalu terbuka (open) atau terputus.

- b) Normally Closed (NC)

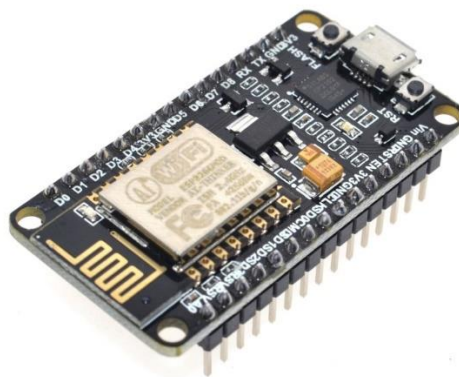
Kondisi awal saklar akan selalu tertutup (close) atau terhubung



Gambar 7. Simbol Relay NO dan NC

## 5. NodeMCU ESP8266

NodeMCU ESP8266 merupakan modul turunan pengembangan dari modul platform IoT (Internet of Things) keluarga ESP8266 tipe ESP-12. NodeMCU adalah sebuah board elektronik yang berbasis chip ESP8266 dengan kemampuan menjalankan fungsi mikrokontroler dan juga koneksi internet (WiFi). Terdapat beberapa pin I/O sehingga dapat dikembangkan menjadi sebuah aplikasi monitoring maupun controlling pada proyek IOT. NodeMCU ESP8266 dapat diprogram dengan compiler-nya Arduino, menggunakan Arduino IDE (Hidayati et al., 2018). Gambar 8 adalah bentuk komponen dari NodeMCU ESP8266

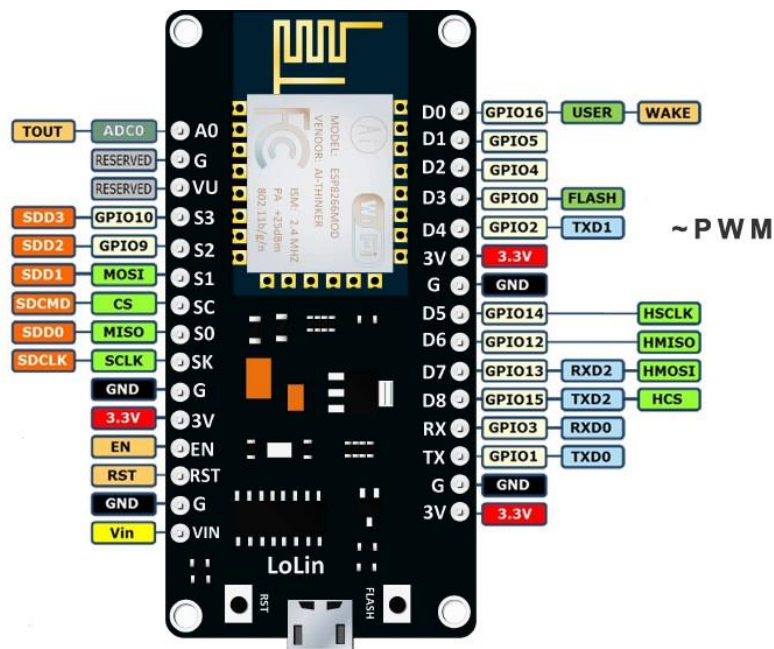


Gambar 8. NodeMCU8266

NodeMCU ESP8266 memiliki spesifikasi sebagai berikut:

- a) Tegangan Input : 3.3 ~ 5V
- b) Wi-Fi Direct (*peer-to-peer*), Soft-AP(*software access point*).
- c) WiFi : IEEE 802.11 b/g/n
- d) Frekuensi : 2.4 GHz – 2.5 Ghz
- e) Flash Memory : 4 MB
- f) Analog to Digital : 1 pin 10 bit ADC
- g) GPIO(*General-purpose input/output*) : 13 Pin
- h) USB Port : Micro USB
- i) USB Chip : CH340G

Alasan pemilihan NodeMCU ESP8266 karena mudah diprogram dan memiliki pin I/O yang memadai dan dapat mengakses jaringan internet untuk mengirim atau mengambil data melalui koneksi WiFi (Pangestu et al., 2019). Adapun GPIO NodeMCU ESP8266 dapat dilihat pada gambar 9.



Gambar 9.GPIO NodeMCU ESP8266

Adapun susunan kaki-kaki dai GPIO dapat dijelaskan sebagai berikut:

1. RST : Berfungsi mereset modul
2. ADC : *Analog Digital Converter*. Rentang tegangan masukani0-1v, dengan skup nilai digital 0-1024
3. EN : *Chip Enable, Active High*
4. IO16 : GPIO16, dapat digunakan untuk membangunkan *chipset* dari mode *deep sleep*
5. IO14 : GPIO14; HSPI\_CLK
6. IO12 : GPIO12: HSPI\_MISO
7. IO13 : GPIO13; HSPI\_MOSI; iiUART0\_CTS
8. VCC : Catu daya 3.3V (VDD)
9. CS0 : Chip selection
10. MISO : *Slave output, Main input*
11. IO9 : GPIO9
12. IO10 : GBIO10
13. MOSI : *Main output slave input*
14. SCLK : *Clock*
15. GND : *Ground*
16. IO15 : iGPIO15; MTDO; HSPICS; iiUART0\_RTS
17. IO2 ii : iGPIO2;UART1\_TXD
18. IO0 ii : iGPIO0
19. IO4 ii : iGPIO4
20. IO5 ii : iGPIO5
21. RXD ii : iUART0\_RXD; iiGPIO3
22. TXD ii : iUART0\_TXD; iiGPIO1

## 6. Arduino IDE

*Arduino Integrated Design Environment* (IDE) merupakan *software* yang dirancang untuk memudahkan menuliskan kode program ke dalam *arduino*, atau secara sederhana merupakan lingkungan terintegrasi yang digunakan untuk melakukan pengembangan. Disebut sebagai lingkungan

karena melalui *software* inilah *Arduino* dilakukan pemrograman untuk melakukan fungsi-fungsi yang dibenamkan melalui sintaks pemrograman. *Arduino* menggunakan bahasa pemrograman sendiri yang menyerupai bahasa C. Bahasa pemrograman *Arduino* (*Sketch*) sudah dilakukan perubahan untuk memudahkan pemula dalam melakukan pemrograman dari bahasa aslinya. Sebelum dijual ke pasaran, IC mikrokontroler *Arduino* telah ditanamkan suatu program bernama *Bootlader* yang berfungsi sebagai penengah antara *compiler Arduino* dengan mikrokontroler.

*Arduino* IDE dibuat dari bahasa pemrograman JAVA. *Arduino* IDE juga dilengkapi dengan librari C/C++ yang biasa disebut *Wiring* yang membuat operasi input dan output menjadi lebih mudah. *Arduino* IDE ini dikembangkan dari *software Processing* yang dirombak menjadi *Arduino* IDE khusus untuk pemrograman dengan *Arduino*, Bentuk dari software arduino IDE dapat dilihat pada gambar di bawah berikut.



Gambar 10. Software ARDUINO IDE

## 7. Android

Android adalah sistem operasi untuk telepon seluler yang berbasis Linux. Android menyediakan platform terbuka bagi para pengembang untuk

menciptakan aplikasi mereka sendiri untuk digunakan oleh bermacam piranti bergerak. Android begitu pesat perkembangannya di era saat ini karena Android menyediakan platform terbuka (open source) bagi para pengembang untuk menciptakan aplikasi mereka sendiri. Perkembangan yang pesat pada sistem Android karena juga didukung oleh hampir keseluruhan vendor smartphone. hal ini karena sifatnya yang open source sehingga siapa saja bisa mengembangkan OS tersebut untuk digunakan pada perangkat mereka dan disesuaikan dengan kebutuhan dan pasar (Claudia, 2017)

Arsitektur Android terdiri dari bagian-bagian seperti berikut (Heru, 2014) :

1. Applications dan Widgets: layer (lapisan) dimana pengguna hanya berhubungan dengan aplikasi saja.
2. Applications Framework: lapisan dimana para pengembang melakukan pembuatan aplikasi yang akan dijalankan di sistem operasi Android dengan komponen-komponennya meliputi views, contents provider, resource manager, notification manager, activity manager.
3. Libraries: lapisan dimana fitur-fitur android berada yang berada diatas kernel meliputi library C/C++ inti seperti Libc dan SSL.
4. Android Run Time: lapisan yang membuat aplikasi Android dapat dijalankan dimana dalam prosesnya menggunakan implementasi Linux yang terbagi menjadi dua bagian yaitu Core Libraries dan Dalvik virtual Machine.
5. Linux Kernel: Layer yang berisi file-file system untuk mengatur processing, memory, resource, driver, dan sistem operasi android lainnya



## 8. Delay

Delay adalah waktu tunda suatu paket yang diakibatkan oleh proses transmisi dari satu titik ke titik lain yang menjadi tujuannya. Oleh karenanya delay dalam suatu jaringan juga merupakan unjuk kerja yang dapat dijadikan acuan dalam menilai kemampuan dan kualitas pentransmisian data. Akibat dari delay, data yang diterima akan mengalami keterlambatan waktu datang sehingga hal ini menyebabkan menunggu sejenak data tersebut sampai pada tujuan. Delay akan sangat dirasakan ketika melakukan transmisi paket data yang bersifat UDP atau secara realtime (Subandi, 2018). Berikut ini cara menghitung delay:

$$\text{Delay rata - rata} = \frac{\text{Total Delay}}{\text{Total Paket yang Diterima}} \dots\dots\dots(1)$$

## 9. Throughput

Throughput yaitu kecepatan (rate) transfer data efektif, yang diukur dalam bps (bit per second). Throughput adalah jumlah total kedatangan paket yang sukses yang diamati pada tujuan selama interval waktu tertentu dibagi oleh durasi interval waktu tersebut. Kategori Throughput diperlihatkan di Tabel 1 (Wulandari, 2016).

Tabel 1. Kategori *Throughput*

Kategori Throughput	Throughput (bps)	Indeks
Sangat Bagus	100	4
Bagus	75	3
Sedang	50	2
Jelek	< 25	1

Sementara itu, untuk menghitung Throughput dapat menggunakan persamaan berikut:

$$\text{Throughput} = \frac{\text{Paket data yang Diterima}}{\text{Lama Pengamatan}} \dots\dots\dots(2)$$

## 10. Packet Loss

Packet loss didefinisikan sebagai kegagalan transmisi paket data mencapai tujuannya. Kegagalan paket tersebut mencapai tujuan, dapat disebabkan oleh beberapa kemungkinan, diantaranya yaitu:

1. Terjadinya overload traffic di dalam jaringan.
2. Tabrakan (congestion) dalam jaringan.
3. Error yang terjadi pada media fisik.
4. Kegagalan yang terjadi pada sisi penerima antara lain bisa disebabkan karena overflow yang terjadi pada buffer

Di dalam implementasi jaringan IP, nilai packet loss ini diharapkan mempunyai nilai yang minimum. Secara umum biasanya terdapat pengkategorian performansi jaringan berdasarkan nilai packet loss yaitu sangat bagus, bagus, jelek, dan sedang (Subandi, 2018). Berikut ini pada tabel 2 menunjukkan kategori standar packet loss.

Tabel 2. Kategori Standar *Packet Loss*

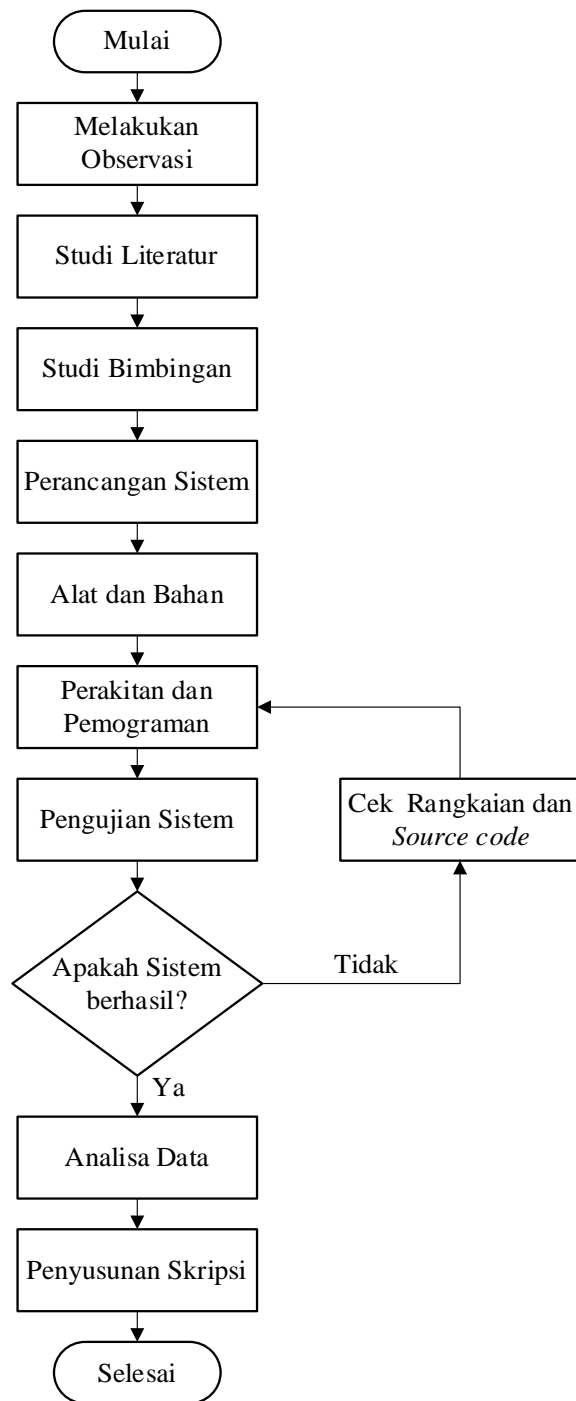
Kategori Peforma	Packet Loss (%)
Sangat Bagus	0
Bagus	3
Sedang	15
Jelek	25

Adapun persamaan untuk menghitung packet loss adalah sebagai berikut:

$$Packet Loss = \left( \frac{Jumlah\ paket\ dikirim - jumlah\ paket\ hilang}{Jumlah\ paket\ dikirim} \right) \times 100\% \dots \dots (3)$$

### I. Metodologi Penelitian

Penelitian ini dilakukan dengan beberapa tahap dan metode. metode penelitian ini dilakukan dan digunakan oleh penulis sebagai pedoman dalam melakukan penelitian agar hasil yang diperoleh sesuai dengan tujuan sebelumnya. Adapun tahapan dan metedoe tersebut ditunjukkan pada gambar diagram alir berikut ini:



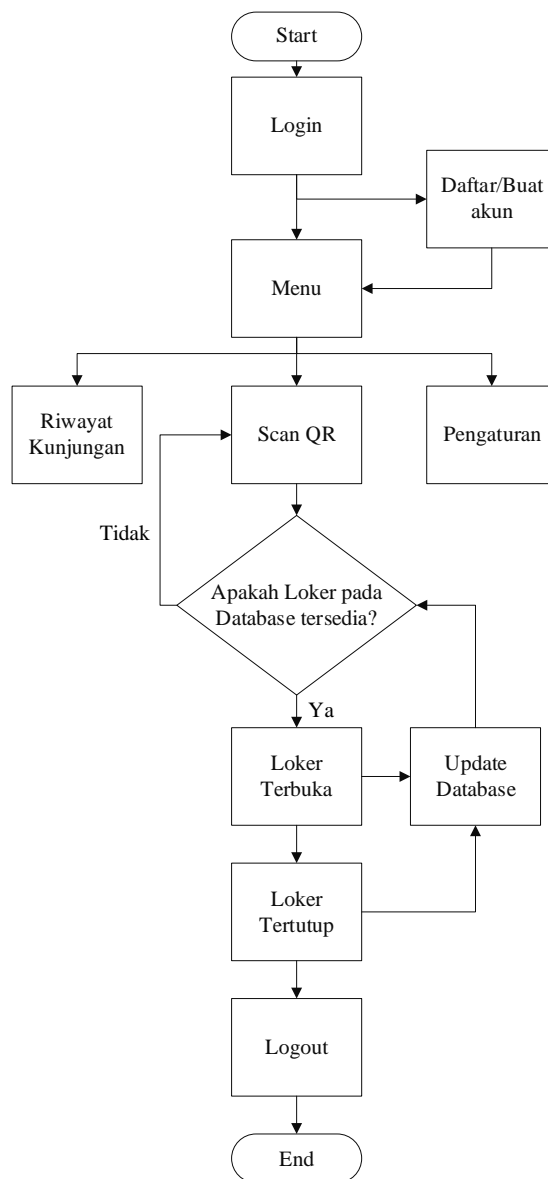
Gambar 11. Diagram alir metodologi penelitian

1. Studi literatur dan pengumpulan data  
Berupa studi kepustakaan dan kajian dari jurnal atau buku yang relevan.
2. Studi bimbingan

Metode dimana penulis melakukan diskusi dengan dosen pembimbing mengenai masalah-masalah yang timbul selama penelitian berlangsung sehingga penelitian berjalan lancar dan terarah.

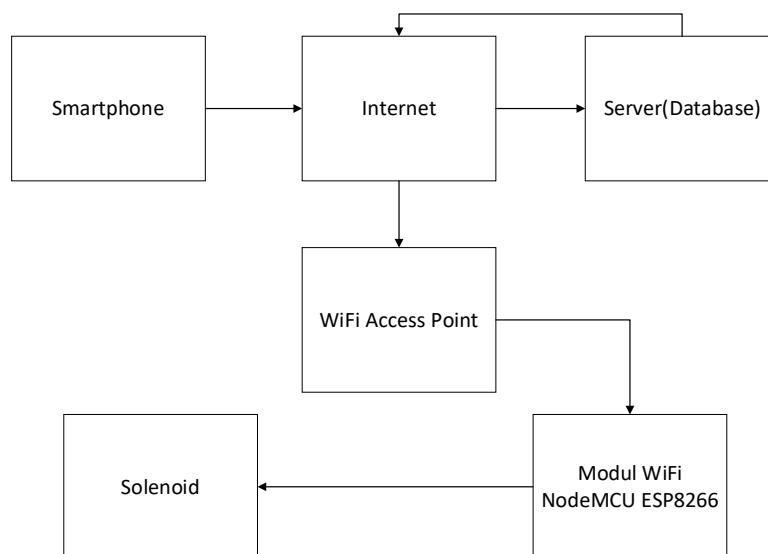
### 3. Perancangan Sistem

Tahap ini meliputi perancangan dari sistem dan pemodelan pengontrolan *Smart Lock* dengan menggunakan *QR-code*. Perancangan sistem pada penelitian ini dimulai dengan *smartphone* sebagai perangkat antar muka pengguna. Adapun rancangan aplikasi dapat dilihat pada gambar 12.



Gambar 12. Perancangan Aplikasi

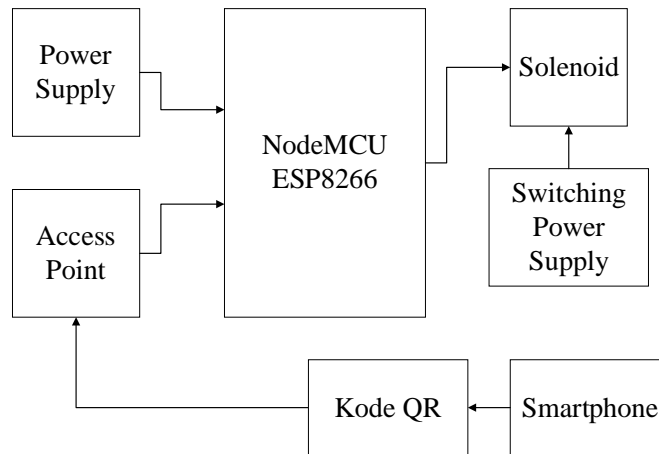
Pengguna harus terlebih dahulu mendaftarkan akunnya pada database melalui smartphone pribadi, hal ini bertujuan agar pengguna yang hendak menggunakan akses loker dapat dikenali oleh sistem dan juga sebagai salah satu bentuk pencegahan agar pihak yang tidak bertanggung jawab tidak dapat mengakses loker perpustakaan tersebut. Kemudian setelah mendaftarkan akun pengguna bisa melakukan proses scanning QR code yang sudah ditempelkan pada loker tersebut. Database bertugas untuk menyimpan data pengguna dan bertindak sebagai kontrol akses. Setelah permintaan akses dilakukan maka server akan mentransmisikan data kepada Arduino melalui modul wifi ESP8266 yang sudah terkoneksi pada *access point* yang sudah disediakan. Arduino disini berperan sebagai mikrokontroler yang mengontrol penguncian pintu loker. Berikut pada Gambar 13 adalah bentuk perancangan sistem *smart lock* berbasis IoT.



Gambar 13. Perancangan Sistem

Desain sistem pengontrolan dalam penelitian ini meliputi Modul NodeMCU ESP8266, Solenoid dan power supply. Alat ini digunakan untuk menerima data dari server database ke modul NodeMCU ESP8266 lalu kemudian solenoid sebagai pengunci loker itu sendiri dan untuk alasan keamanan solenoid akan melakukan penguncian otomatis

apabila terdapat pengguna yang lupa memberikan perintah untuk mengunci loker tersebut. Gambar 14 menunjukkan desain sistem pengontrolan dalam penelitian ini.



Gambar 14. Rangkaian alat pengontrolan Smart Lock System

#### 4. Alat dan Bahan

Setelah melakukan desain, maka dilakukan pemilihan alat dan bahan dilakukan sesuai dengan desain yang dilakukan dengan melihat data sheet pada komponen tersebut dan melihat beberapa hasil penelitian-penelitian sebelumnya. Adapun alat yang digunakan pada penelitian ini adalah sebagai berikut:

- a. Modul WiFi NodeMCU ESP8266
- b. *Solenoid Lock Door*
- c. DC to DC stepdown
- d. *Project Board* dan kabel
- e. PC
- f. *Smartphone*

#### 5. Perakitan dan Pemograman

Pada tahap ini akan dilakukan perakitan dan pemograman setelah dilakukannya perancangan pada desain, menggunakan modul NodeMCU ESP8266 sebagai mikrokontroler, sedangkan aplikasi android digunakan sebagai tampilan antarmuka pengguna untuk mengakses kunci loker tersebut.

#### 6. Pengujian Sitem

Pengujian sistem alat akan dilakukan dengan melihat hasil dari *prototype* menggunakan aplikasi android. Pengujian dilakukan untuk menguji keberhasilan dan nilai delay yang dihasilkan, untuk pengujian delay alat apabila alat yang digunakan diakses secara bersamaan akan digunakan 10 buah LED sebagai *prototype*. Apabila, terdapat hasil yang tidak sesuai maka akan dilakukan peninjauan kembali pada desain dan pemilihan komponen sehingga setelah dilakukan perbaikan akan menghasilkan sistem sesuai dengan yang diinginkan.

#### 7. Analisa data

Melakukan analisa pada alat *prototype* agar sesuai dengan perancangan yang telah dibuat sebelumnya sehingga nantinya dapat dihasilkan sebuah kesimpulan untuk hasil dari penelitian ini

#### 8. Penyusunan Skripsi

Tahapan ini dilakukan bersamaan dengan tahapan pengumpulan analisa data. Tahapan ini penulis menyusun skripsi dari Bab I – Bab V.

### J. Hasil Sementara

Penelitian sementara dilakukan dengan melakukan koneksi antara NodeMCU ESP8266 dengan firebase sebagai database. Hasil penelitian sementara ini dilakukan dengan beberapa tahapan yaitu:

#### J.1 Pemograman Alat

Agar alat dapat digunakan otomatis maka diperlukan pemograman pada NodeMCU ESP8266. Pada gambar 15 menunjukkan proses pemograman menggunakan software Arduino IDE.

```

#include <ESP8266WiFi.h>
#include <FirebaseArduino.h>

#define WIFI_SSID "luthfi"
#define WIFI_PASSWORD "luthfi90"

#define FIREBASE_HOST "bus-tracker-luthfi.firebaseio.com"
#define FIREBASE_AUTH "21Vp77Z9aS6Q4XpDxKhtUFOaSIXwVlbJZ0j2WYzG"

int SolenoidPower = D5;

void setup() {

  Serial.begin(9600);

  WiFi.begin(WIFI_SSID, WIFI_PASSWORD);
  Serial.print("connecting");
  while (WiFi.status() != WL_CONNECTED) {
    Serial.print(".");
    delay(500);
  }
  Serial.println();
  Serial.print("connected: ");
  Serial.println(WiFi.localIP());

  Firebase.begin(FIREBASE_HOST, FIREBASE_AUTH);
  pinMode(SolenoidPower, OUTPUT);
}

void loop() {

  int Solenoid = Firebase.getInt("Solenoid");
  if(Solenoid == 1){
    digitalWrite(SolenoidPower, HIGH);
    Serial.println ("Buka");
    delay(10000);
  } else {
    digitalWrite(Solenoid, LOW);
    Serial.println("Terkunci");
    delay(10000);
  }

  //set data:
  //Firebase.set(ledStatus, "1");
}

```

Gambar 15. Proses pemrograman menggunakan Arduino IDE

Langkah pertama agar alat dapat bekerja sebagaimana mestinya adalah melakukan penambahan library pada Arduino sesuai dengan alat yang digunakan yaitu ESP8266 dan Firebase. Proses pengkoneksian internet dengan modul ESP8266 dilakukan dengan mendeklarasikan SSID(*Service Set Identifier*) atau lebih dikenal dengan nama jaringan wifi

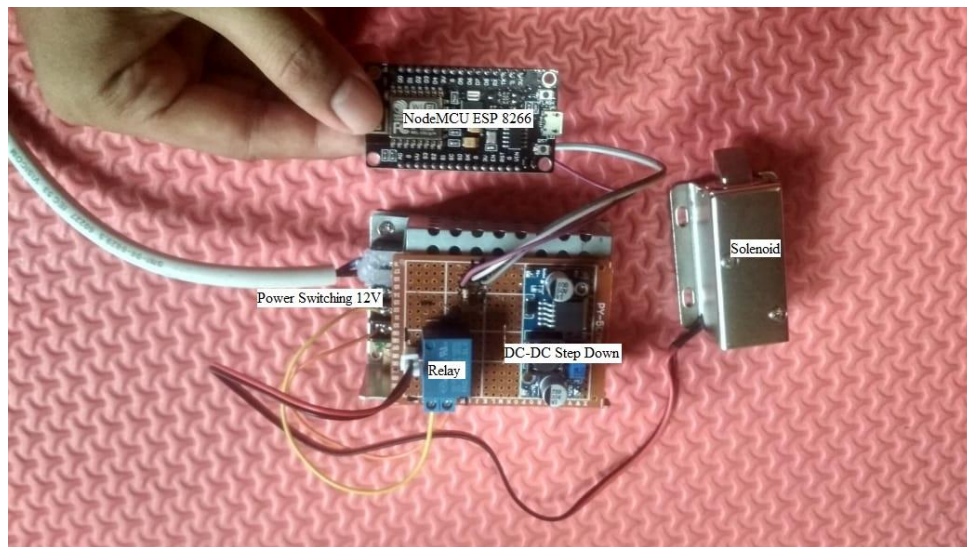


dan password wifi yang akan digunakan, lalu untuk sinkronisasi Arduino dengan firebase membutuhkan pendeklarasian berupa token pengguna firebase dan alamat project yang akan digunakan. Semua proses pendeklarasian ini kemudian akan dijalankan pada void setup().

Setelah void setup() dijalankan, void loop() akan melakukan eksekusi dan menjalankan program yang telah dibuat. Pada hasil sementara ini dilakukan pemograman untuk membuka Solenoid, apabila pada database firebase Solenoid bernilai 1 (satu) maka Solenoid akan terbuka dan apabila Solenoid bernilai selain dari satu maka akan tertutup.

## J.2 Implementasi dan Pengukuran Alat

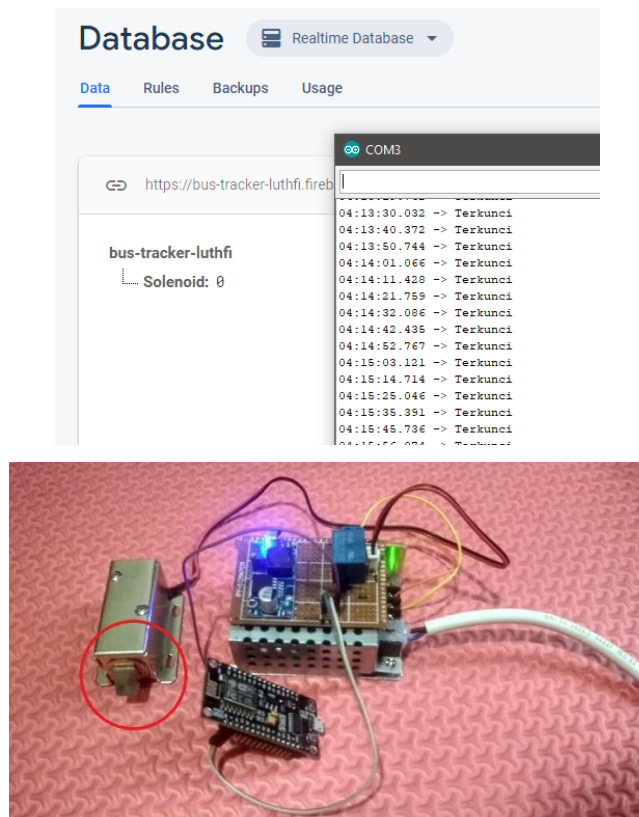
Pada hasil sementara ini telah dilakukan perakitan alat berdasarkan rancangan sistem alat yang telah ditentukan. Gambar 16 menunjukkan komponen-komponen yang digunakan pada hasil sementara ini.



Gambar 16. Komponen Alat Hasil Sementara

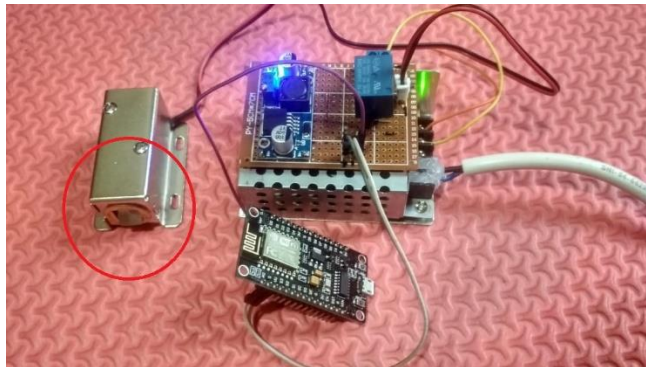
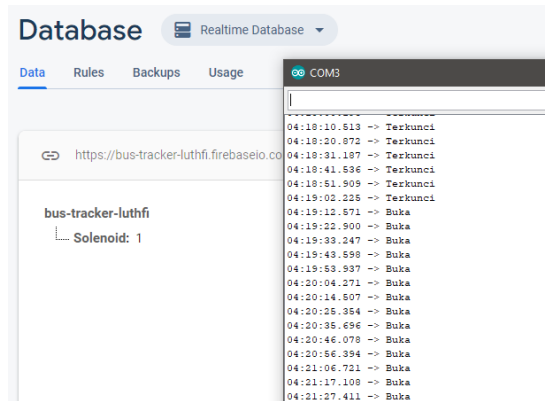
Sistem ini bekerja ketika alat dihubungkan ke power supply dari PLN, kemudian arus AC (*Altermatic Current*) ini diubah menjadi arus DC(*Direct Current*) menggunakan power switching regulator 12V. Pemilihan power switching 12V karena komponen solenoid akan bekerja jika diberi tegangan 12V sedangkan komponen DC-DC step down berfungsi untuk menurunkan tegangan 12V ke 5V sebagai sumber tegangan untuk

NodeMCU ESP 8266. Sedangkan untuk sistem koneksi alat ke firebase dapat dilihat pada gambar 17 dan 18



Gambar 17. Tampilan ketika Solenoid bernilai 0

Gambar 17 menunjukkan bahwa ketika solenoid bernilai 0 maka solenoid tidak akan terbuka karena relay bersifat normally open maka ketika relay belum diaktifkan, maka saklar pada relay akan selalu terbuka atau terputus sehingga arus tidak dapat mengalir ke solenoid.



Gambar 18. Tampilan Ketika Solenoid bernilai 1

Ketika nilai di firebase bernilai satu maka solenoid akan terbuka karena telah diaktifkan pada firebase sehingga arus dapat mengalir ke solenoid dan solenoid pun menjadi terbuka seperti yang ditunjukkan pada Gambar 18. Sedangkan dari pengukuran alat didapatkan tegangan sekitar 12V dengan arus sekitar 17.4 mA ketika tanpa beban dan 810 mA ketika diberi beban. Berikut ini gambar 19 menunjukkan hasil pengukuran alat.



Gambar 19. Hasil Pengukuran Alat (a) Tanpa beban (b) Nyala/diberi beban

## **K. Kesimpulan**

Berdasarkan hasil perancangan dan pengujian sementara diperoleh kesimpulan bahwa pengujian alat penelitian sementara telah berhasil dilakukan baik pada WiFi dan Firebase serta diperlukan penambahan aplikasi android agar alat dapat berjalan sebagaimana mestinya. Alat yang dibuat merupakan suatu sistem yang memiliki satu kesatuan, sehingga apabila salah satu sistem terputus maka komunikasi data baik ke internet maupun ke firebase tidak akan berhasil.

## L. Jadwal Kegiatan

Tabel 3. Perkiraan Jadwal Pelaksanaan Penelitian

No.	Kegiatan	Minggu ke-													
		1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	Studi Literatur														
2	Diskusi dengan Dosen Pembimbing mengenai topik penelitian														
3	Mempelajari Software dan melakukan simulasi sistem														
4	Merancang dan merangkai Alat														
5	Mencatat data dari aplikasi														
6	Analisa dan Evaluasi Data														
7	Pembuatan Laporan Akhir														

### **M. Rancangan Biaya**

Tabel 4. Pengeluaran lain-lain ( administrasi,publikasi dan operasional)

No	Uraian Kegiatan	Volume	Biaya Satuan	Jumlah
1	Perbanyak proposal	5 Rangkap	Rp 40.000	Rp 200.000
2	Seminar proposal	1 kali	Rp 400.000	Rp 400.000
3	Pengetikan dan perbanyak laporan hasil penelitian	6 Rangkap	Rp 50.000	Rp 300.000
4	Seminar hasil penelitian	1 kali	Rp 500.000	Rp 500.000
5	Dokumentasi hasil penelitian	5 kali	Rp 50.000	Rp 250.000
6	Pembuatan Alat	1 kali	Rp 500.000	Rp 500.000
Jumlah biaya				Rp 2.150.000

## DAFTAR PUSTAKA

- Aathira, R., Indhupriya, E., Bhadusha, I., & Onn, U. H. (2018). *E TOLL SYSTEM USING IOT*. 120(6), 11523–11534.
- Afdhal, E. (2014). IEEE 802.11ac sebagai Standar Pertama untuk Gigabit Wireless LAN. *Jurnal Rekayasa Elektrika*, 11(1), 36–44.  
<https://doi.org/10.17529/jre.v11i1.1994>
- Arafat. (2016). SISTEM PENGAMANAN PINTU RUMAH BERBASIS Internet Of Things (IoT) Dengan ESP8266. *Jurnal Ilmiah Fakultas Teknik "Technologia," Vol 7, No.4*. <https://doi.org/10.1126/science.195.4279.639>
- Arief, M. R. (2013). Teknologi Jaringan Tanpa Kabel ( Wireless ). *Seminar Nasional Teknologi 2007*, 2007(November), 1–8.
- Chang, J. H. (2014). An introduction to using QR codes in scholarly journals. *Science Editing*, 1(2), 113–117. <https://doi.org/10.6087/kcse.2014.1.113>
- Cynthia, J., Sultana, H. P., Saroja, M. N., & Senthil, J. (2019). *Ubiquitous Computing and Computing Security of IoT* (Vol. 47). Springer International Publishing. <https://doi.org/10.1007/978-3-030-01566-4>
- Ha, I. (2015). Security and usability improvement on a digital door lock system based on internet of things. *International Journal of Security and Its Applications*, 9(8), 45–54. <https://doi.org/10.14257/ijisia.2015.9.8.05>
- Hidayati, N., Dewi, L., Rohmah, M. F., & Zahara, S. (2018). Prototype Smart Home Dengan Modul NodeMCU ESP8266 Berbasis Internet of Things (IoT). *Teknik Informatika Universitas Islam Majapahit*, 1–9.
- Kanumuru Rajesh, K.V. Mounika Reddy, S.Swaranalatha, M. S. (2018). QR Code-based Real Time Vehicle Tracking in Indoor Parking Structures. *Proceedings of the Second International Conference on Intelligent Computing and Control Systems (ICICCS 2018)*, *Iciccs*, 11–16.
- Kassem, A., Murr, S. El, Jamous, G., Saad, E., & Geagea, M. (2016). A smart

- lock system using Wi-Fi security. *2016 3rd International Conference on Advances in Computational Tools for Engineering Applications, ACTEA 2016*, 222–225. <https://doi.org/10.1109/ACTEA.2016.7560143>
- Marktscheffel, T., Gottschlich, W., Popp, W., Werli, P., Fink, S. D., Bilzhause, A., & De Meer, H. (2016). QR code based mutual authentication protocol for Internet of Things. *WoWMoM 2016 - 17th International Symposium on a World of Wireless, Mobile and Multimedia Networks*. <https://doi.org/10.1109/WoWMoM.2016.7523562>
- Pangestu, A. D., Ardianto, F., & Alfaresi, B. (2019). Sistem Monitoring Beban Listrik Berbasis Arduino Nodemcu Esp8266. *Jurnal Ampere*, 4(1), 187. <https://doi.org/10.31851/ampere.v4i1.2745>
- Parabhoi, L., Bhattacharya, N., & Dhar, R. (2017). Use of QR Code in Library. *Application of Modern Tools & Technology in Library Services, January*, 237–243.
- Rasid, S. M. R., Rashid, F., Sabri, A. A., & Islam, R. (2018). *Design and Construction of an Automatic Security System of a Door Using RFID Technology*. 9(9), 1067–1073.
- Saleh, M., & Haryanti, M. (2017). Rancang Bangun Sistem Keamanan Rumah Menggunakan Relay. *Jurnal Teknologi Elektro*, Universitas Mercu Buana Muhamad Saleh Program Studi Teknik Elektro Universitas Suryadarma, Jakarta Program Studi Teknik Elektro ISSN : 2086 - 9479. *Jurnal Teknologi Elektro, Universitas Mercu Buana*, 8(3), 181–186. <http://publikasi.mercubuana.ac.id/index.php/jte/article/download/2182/1430>
- Subandi, A. (2018). *IMPLEMENTASI DAN ANALISIS QoS ( QUALITY OF SERVICE ) PADA VoIP ( VOICE OVER INTERNET PROTOCOL ) BERBASIS LINUX*. 5(2).
- Subrata, R. H., & Gozali, F. (2018). *Sistem Keamanan Ruang Berbasis Internet Of Things Dengan Menggunakan Aplikasi Android*.



- V. Ramya, G. G. (2014). Review On Quick Response Codes In The Field Of Information Security (Analysis Of Various Imperceptibility Characteristics On Grayscale And Binary QR code). *IEEE - International Conference on Advances in Engineering and Technology, Icaet*.
- Vaidhyesh, P. S., N, M. W., G, S. V., & Harini, D. N. (2018). SECURING IoT DEVICES BY GENERATING QR CODES. *International Journal of Pure and Applied Mathematics, 119*(12), 13743–13749. <http://www.ijpam.eu>
- Várallyai, L. (2013). From Barcode to QR Code Applications. *Journal of Agricultural Informatics, 3*(2), 9–17. <https://doi.org/10.17700/jai.2012.3.2.92>
- Wulandari, R. (2016). ANALISIS QoS ( QUALITY OF SERVICE ) PADA JARINGAN INTERNET ( STUDI KASUS : UPT LOKA UJI TEKNIK PENAMBANGAN JAMPANG KULON – LIPI ). 2, 162–172.