

SKRIPSI

**PENGEMBANGAN *SMART KEY READER* MENGGUNAKAN
*MULTI BIOMETRIC AUTHENTICATION***

Disusun dan diajukan oleh:

MUHAMMAD YUSUF

D041 19 1041



**PROGRAM STUDI SARJANA TEKNIK ELEKTRO
FAKULTAS TEKNIK
UNIVERSITAS HASANUDDIN
GOWA
2024**



LEMBAR PENGESAHAN SKRIPSI

**PENGEMBANGAN *SMART KEY READER* MENGGUNAKAN
*MULTI BIOMETRIC AUTHENTICATION***

Disusun dan diajukan oleh

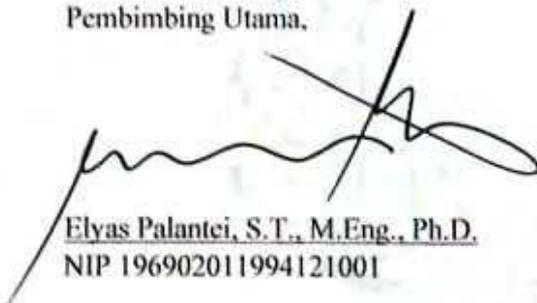
MUHAMMAD YUSUF

D041191041

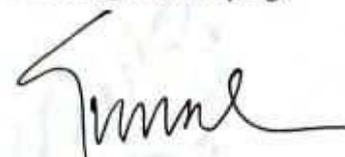
Telah dipertahankan di hadapan Panitia Ujian yang dibentuk dalam rangka
Penyelesaian Studi Program Sarjana Program Studi Teknik Elektro
Fakultas Teknik Universitas Hasanuddin
Pada Tanggal 19 Februari 2024
dan dinyatakan telah memenuhi syarat kelulusan

Menyetujui,

Pembimbing Utama,


Elyas Palantei, S.T., M.Eng., Ph.D.
NIP 196902011994121001

Pembimbing Pendamping,


Ir. Samuel Panggalo, M.T
NIP 196203041988111001

Ketua Program Studi,



Dr. Eng. Ir. Dewiani, M.T. IPM
NIP 19691026 199412 2 001



PERNYATAAN KEASLIAN

Yang bertanda tangan dibawah ini :

Nama : MUHAMMAD YUSUF

NIM : D041191041

Program Studi : Teknik Elektro

Jenjang : S1

Menyatakan dengan ini bahwa karya tulisan saya berjudul

PENGEMBANGAN SMART KEY READER MENGGUNAKAN MULTI BIOMETRIC AUTHENTICATION

Adalah karya tulisan saya sendiri dan bukan merupakan pengambilan alihan tulisan orang lain dan bahwa skripsi yang saya tulis ini benar-benar merupakan hasil karya saya sendiri.

Semua informasi yang ditulis dalam skripsi yang berasal dari penulis lain telah diberi penghargaan, yakni dengan mengutip sumber dan tahun penerbitannya. Oleh karena itu semua tulisan dalam skripsi ini sepenuhnya menjadi tanggung jawab penulis. Apabila ada pihak manapun yang merasa ada kesamaan judul dan atau hasil temuan dalam skripsi ini, maka penulis siap untuk diklarifikasi dan mempertanggungjawabkan segala resiko.

Segala data dan informasi yang diperoleh selama proses pembuatan skripsi, yang akan dipublikasi oleh Penulis di masa depan harus mendapat persetujuan dari Dosen Pembimbing.

Apabila dikemudian hari terbukti atau dapat dibuktikan bahwa sebagian atau keseluruhan isi skripsi ini hasil karya orang lain, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Gowa, 19 Februari 2024

Yang Menyatakan



Muhammad Yusuf



KATA PENGANTAR

Assalamu'alaikum Warohmatullahi Wabarokatuh

Puji syukur peneliti panjatkan kepala Allah Subhanahu Wata'ala yang telah memberikan rahmat-Nya, kesehatan, petunjuk, serta kesabaran sehingga peneliti dapat menyelesaikan skripsi yang berjudul “Pengembangan *Smart Key Reader* menggunakan *Multi Biometric Authentication*”. Peneliti menyadari bahwa masih terdapat banyak kekurangan dalam isi dari skripsi ini sehingga semua kritik dan saran akan sangat bermanfaat untuk penulis agar dapat lebih baik lagi dikemudian hari.

Pembuatan skripsi ini berdasarkan perkembangan dunia teknologi dan telekomunikasi yang semakin hari semakin pesat di dunia yang memanfaatkan IoT (Internet of Things). Tujuan skripsi ini adalah sebagai salah satu syarat kelulusan pada Pendidikan Strata Satu (S1) Departemen Teknik Elektro Fakultas Teknik Universitas Hasanuddin.

Dalam skripsi ini, peneliti banyak mendapatkan bantuan dari berbagai pihak, untuk itu peneliti mengucapkan terima kasih atas bantuan, dukungan, dan doanya. peneliti mengucapkan terima kasih antara lain kepada:

1. Kedua Orang tua, serta keluarga penulis yang tak pernah lelah memberikan dukungan, bantuan, dan doa.
2. Bapak Elyas Palantei, S.T., M.Eng., Ph.D. selaku pembimbing 1 dan bapak Ir. Samuel Panggalo, M.T. selaku pembimbing 2 yang telah memberikan bimbingan, saran, dukungan, dan motivasinya dalam penyusunan skripsi ini.
3. Ibu Dr.Eng.Ir. Dewiani, M.T selaku penguji 1 dan Ibu Merna Baharuddin, ST., M.Tel. Eng., Ph.D selaku penguji 2 yang telah memberikan kritik dan saran dalam penyusunan skripsi ini



4. Bapak/Ibu dosen Departemen Teknik Elektro Fakultas Teknik Universitas Hasanuddin yang telah banyak memberikan ilmu yang tidak terbatas selama kuliah dan membantu untuk kelancaran proses penyusunan skripsi ini.

5. Teman-teman riset Laboratorium Telekomunikasi, Radio dan Microwave yang telah menjadi rekan seperjuangan, memberikan banyak pengalaman bersama, selalu berbagi kebahagiaan, berbagi waktu, dan selalu memberikan dukungan.
6. Teman-teman TR19GER yang telah menjadi rekan seperjuangan, selalu berbagi kebahagiaan, waktu, dan kesedihan selama berproses menjadi mahasiswa.

Akhir kata peneliti mengucapkan terima kasih kepada semua pihak yang telah membantu peneliti, serta peneliti berharap semoga skripsi ini dapat bermanfaat bagi kita semua dan menjadi bahan masukan dalam dunia pendidikan.

Gowa, 6 Februari 2024

Muhammad Yusuf



ABSTRAK

Muhammad Yusuf. Pengembangan *Smart Key Reader* menggunakan *Multi Biometric Authentication* (Dibimbing oleh Elyas Palantei dan Samuel Panggalo)

Kejahatan yang semakin berkembang dengan beragam motif mendorong pengembangan metode untuk meningkatkan keamanan suatu tempat. Salah satu pendekatan yang mengandalkan teknologi komputer adalah teknologi *biometric*, yang mengimplementasikan sistem autentikasi menggunakan beberapa faktor untuk memberikan tingkat keamanan yang tinggi. Oleh karena itu, tujuan penelitian ini untuk mengembangkan sistem *Smart Key Reader* dengan *Multi Biometric Authentication* pada akses pintu ruangan yang menggabungkan teknologi *biometric*, smartcard, dan Web Browser. Sistem *Smart Key Reader* dapat beroperasi pada dua mode. Mode 1 menggunakan *smartcard*, *Fingerprint Sensor*, *Voice Recognition* dan *Face Recognition*. Lalu mode 2 Web Browser, *Fingerprint Sensor*, *Voice Recognition* dan *Face Recognition*. *Smartcard* dapat terbaca pada jarak maksimum 15mm baik menggunakan penghalang maupun tanpa penghalang. *Smartcard* dapat bekerja tanpa adanya delay. *Fingerprint sensor* dapat membaca semua sidik jari user yang terdaftar dengan baik dan tidak terjadi *error*. Data hasil pengukuran delay fingerprint sensor bervariasi mulai dari 125,7ms hingga 245,5ms. *Voice Recognition* mampu mengenali suara yang telah di daftarkan dengan baik. Hasil pengukuran *delay voice recognition* mulai 1,88s sampai 2,82s. *Face recognition* dapat mengidentifikasi wajah, baik itu dalam keadaan mata terbuka ataupun tertutup. *Delay* dari *face recognition* beragam mulai dari 1,76s sampai 3,1s. Nilai *delay biometric reader* saat menggunakan *web browser* bervariasi mulai dari 5,79s hingga 12,37s. Sedangkan nilai *delay biometric reader* saat menggunakan *smartcard* mulai dari 6,54s hingga 10,08s.

Kata kunci: *Smart key reader, multi biometric authentication, smartcard, fingerprint sensor, voice recognition, face recognition*



ABSTRACT

Muhammad Yusuf. *Development of Smart Key Reader using Multi Biometric Authentication*

(Supervised by Elyas Palantei and Samuel Panggalo).

Growing crime with various motives encourages the development of methods to improve the security of a place. One approach that relies on computer technology is biometric technology, which implements an authentication system using several factors to provide a high level of security. Therefore, the purpose of this research is to develop a Smart Key Reader system with Multi Biometric Authentication on room door access that combines biometric technology, smartcard, and Web Browser. The Smart Key Reader system can operate in two modes. First mode using a smartcard, Fingerprint Sensor, Voice Recognition and Face Recognition. And the second mode using Web Browser, Fingerprint Sensor, Voice Recognition and Face Recognition. The smartcard can be read at a maximum distance of 15mm both using a barrier and without a barrier. Smartcard can work without any delay. Fingerprint sensors can read all registered user fingerprints properly and no errors occur. Measurement data of fingerprint sensor delay varies from 125,7ms to 245,5ms. Voice Recognition is able to recognize the voice that has been registered properly. Voice recognition delay measurement results ranging from 1,88s to 2,82s. Face recognition can identify faces, whether it is in a state of open or closed eyes. Delay of face recognition varies from 1,76s seconds to 3,1s. The delay value of the biometric reader when using a web browser varies from 5,79s to 10,37s. Then the delay value of the biometric reader when using smartcard start from 6,54 to 10,08s.

Keywords: *Smart key reader, multi biometric authentication, smartcard, fingerprint sensor, voice recognition, face recognition*



DAFTAR ISI

HALAMAN PENGESAHAN SKRIPSI.....	i
PERNYATAAN KEASLIAN KARYA ILMIAH ... Error! Bookmark not defined.	
KATA PENGANTAR.....	iii
ABSTRAK.....	v
ABSTRACT.....	vi
DAFTAR ISI.....	vii
DAFTAR TABEL.....	ix
DAFTAR GAMBAR.....	x
DAFTAR LAMPIRAN.....	xi
DAFTAR SINGKATAN DAN ARTI SIMBOL.....	xii
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	4
1.3 Tujuan Penelitian.....	4
1.4 Manfaat Penelitian.....	5
1.5 Batasan Masalah.....	5
BAB II TINJAUAN PUSTAKA.....	6
2.1. Internet Of Things (IoT).....	6
2.2. Multi-Factor Authentication (MFA).....	7
2.3. <i>Smart Key Reader</i>	8
2.4. <i>Biometric Security</i>	8
2.5. Penguncian Cerdas.....	8
2.6. ESP32.....	9
2.7. ESP32-CAM.....	10
2.8. Software Arduino IDE (Integrated Development Environment).....	11
2.9. LCD.....	12
2.10. Smartcard.....	14
2.11. Radio Frequency Identification (RFID).....	16
Sensor <i>Fingerprint AS608</i>	17
<i>Face Recognition V3</i>	18
Teknologi Wi-Fi.....	18



2.15. Delay	19
BAB III METODE PENELITIAN.....	20
3.1. Rancangan Penelitian.....	20
3.2. Waktu dan Lokasi Penelitian	21
3.3. Bahan dan Alat.....	22
3.4. Blok Diagram Sistem Kerja <i>Reader</i>	23
3.5. Perancangan dan Pembuatan <i>Reader</i>	26
3.5.1. Perancangan <i>Hardware</i>	26
3.5.2. Perancangan <i>Software</i>	27
3.5.3. Perancangan <i>Web Server</i> dan <i>Website Login</i>	28
3.6. Pengujian Kinerja <i>Reader</i>	28
3.6.1. Pengujian Kinerja <i>Hardware</i>	28
3.6.2. Pengujian Kinerja <i>Software Website Login</i> melalui <i>Web Browser</i>	31
BAB IV HASIL DAN PEMBAHASAN.....	32
4.1. Hasil Pengujian <i>Hardware</i>	32
4.1.1. Pengujian Jarak Baca <i>Reader</i> dengan <i>Smartcard</i>	32
4.1.2. Pengujian <i>Delay Scan Smartcard</i> pada <i>Reader</i>	34
4.1.3. Pengujian <i>Biometric Reader</i>	35
4.1.4. Pengujian <i>user</i> yang tidak terdaftar dalam <i>database</i>	43
4.1.5. Pengujian Jangkauan Sinyal WiFi pada <i>Reader</i>	46
4.2. Hasil Pengujian <i>Software</i>	47
4.2.1. Pengujian <i>Interface Login</i>	47
4.2.2. Pengujian <i>User Interface</i>	48
BAB V KESIMPULAN DAN SARAN.....	51
5.1. Kesimpulan.....	51
5.2. Saran	52
DAFTAR PUSTAKA	53



DAFTAR TABEL

Tabel 1 Kategori delay versi THYPON	19
Tabel 2 Kategori delay versi ITU-T	19
Tabel 3 Alat dan bahan.....	22
Tabel 4 Pengujian jarak baca reader dengan smartcard	33
Tabel 5 Pengujian delay smartcard	35
Tabel 6 Pengujian delay sensor fingerprint.....	36
Tabel 7 Pengujian delay voice recognition	38
Tabel 8 Pengujian intensitas suara	39
Tabel 9 Pengujian delay face recognition	40
Tabel 10 Pengujian delay biometric reader.....	42
Tabel 11 Pengujian smarcard yang tidak terdapat dalam database	43
Tabel 12 Pengujian jari yang tidak terdapat dalam database	44
Tabel 13 Pengujian suara yang tidak terdaftar dalam database.....	45
Tabel 14 Pengujian wajah yang tidak terdaftar dalam database.....	46
Tabel 15 Pengujian jarak jangkauan sinyal.....	46
Tabel 16 Pengujian login interface.....	48
Tabel 17 Pengujian user interface	49
Tabel 18 History User Masuk	50



DAFTAR GAMBAR

Gambar 1 ESP32.....	9
Gambar 2 ESP32-CAM	10
Gambar 3 Software Arduino IDE (Integrated Development Environment)	11
Gambar 4 LCD (Liquid Crystal Display)	12
Gambar 5 Arsitektur Smartcard	14
Gambar 6 Tag Mifare Classic 1K.....	15
Gambar 7 Radio Frequency Identification (RFID)	16
Gambar 8 Diagram Alir Penelitian.....	20
Gambar 9 Blok Diagram Sistem Kerja Smart Key Reader.....	23
Gambar 10 Flowchart Proses Akses Reader Menggunakan Web Browser, Sidik Jari, Sensor Suara dan Face Recognition.....	24
Gambar 11 Flowchart Proses Akses Reader Menggunakan Smartcard, Sidik Jari, suara dan Face Recognition.....	25
Gambar 12 Skematik Hardware	26
Gambar 13 Hasil Perakitan Hardware (a) akses keluar, (b) akses masuk	32
Gambar 14 Pengujian Jarak Baca Reader dengan Smartcard (a) Tapping Smartcard Langsung (b) Tapping Smartcard dengan penghalang.....	32
Gambar 15 Diagram Jarak Baca Reader dengan Smartcard	33
Gambar 16 Pengujian Delay Scan Smartcard pada Reader	34
Gambar 17 Serial Monitor Pengujian Smartcard	34
Gambar 18 Pengujian Fingerprint Sensor	35
Gambar 19 Serial Monitor Pengujian Sensor Fingerprint.....	36
Gambar 20 Delay Sensor Fingerprint	37
Gambar 21 Pengujian Voice Recognition	37
Gambar 22 Serial Monitor Pengujian Sensor Suara	38
Gambar 23 Delay Voice Recognition.....	38
Gambar 24 Pengujian Face Recognition (a) mata terbuka (b) mata tertutup	40
Gambar 25 Delay Face Recognition	41
Gambar 26 Pengujian Delay Biometric Reader	41
Gambar 27 Delay Biometric Reader	42
Gambar 28 Pengujian jari yang tidak terdaftar dalam database.....	44
Gambar 29 Pengujian suara yang tidak terdaftar dalam database.....	44
Gambar 30 Pengujian Wajah yang tidak terdaftar dalam database	45
Gambar 31 Pengujian Jarak Jangkauan Sinyal Wifi pada Reader	46
Gambar 32 Login Interface	47
Gambar 33 User Inteface	48
Gambar 34 Halaman history user yang mengakses reader	49



DAFTAR LAMPIRAN

Lampiran 1 Tabel Jarak Baca Reader.....	56
Lampiran 2 Tabel Delay RFID.....	57
Lampiran 3 Tabel Delay Fingerprint.....	58
Lampiran 4 Tabel Delay Voice Recognition	59
Lampiran 5 Tabel Delay Face Recognition.....	60
Lampiran 6 Tabel Delay Biometric Reader.....	61
Lampiran 7 Program Index	62
Lampiran 8 Program <i>RFID</i>	64
Lampiran 9 Program Fingerprint	76
Lampiran 10 Program Voice Recognition.....	79
Lampiran 11 Program Face Recognition	82
Lampiran 12 Program LCD	83
Lampiran 13 Program Relay	88
Lampiran 14 Program Web Lock door.....	89
Lampiran 15 Program Variable	94



DAFTAR SINGKATAN DAN ARTI SIMBOL

Lambang/Singkatan	Arti dan Keterangan
°C	Satuan Suhu Celcius
AC	Address Counter
ADC	Analog to Digital Converter
AP	Access Point
ASCII	American Standard Code for Interchange Information
BaaS	Backend as a Service
BF	Busy Flag
BLE	Bluetooth Low Energy
BT	BlueTooth
CCTV	Closed Circuit Television
CGRAM	Character Generator Random Access Memory
CGROM	Character Generator Read Only Memory
CPU	Central Processing Unit
DAC	Digital to Analog Converter
DDRAM	Display Data Random Access Memory
DMIPS	Dynamic Microscopic Image Processing Scanner
DR	Data Register
EM	Electromagnetic
FOTA	Firmware Over-The-Air
GPS	Global Positioning System
Hz	Satuan Frekuensi Hertz
I/O	Input/ Output
I2C	Interface Inter Integrated Circuit
IDE	Integrated Development Environment
IEC	International Electrotechnical Commission
IFF	Identification Friend or Foe
IoT	Internet of Things
IR	Instruction Register
ISO	International Organization for Standardization
KB	KiloByte
LCD	Liquid Crystal Display
mA	Satuan Arus milliAmpere
MFA	Multi-Factor Authentication
mm	Satuan Panjang milliMeter
mV	Satuan Tegangan milliVolt
NUID	New User Identification
OS	Operating System
PCB	Printed Circuit Board
PSRAM	Pseudo-Static Random Access Memory
PWM	Pulse Width Modulation
RF	Radio Frequency
RFID	Radio Frequency Identification



ROM	Read Only Memory
SoC	System-on-Chip
SPI	Serial Peripheral
SRAM	Static Random Access Memory
STA	Station
TF	TransFlash
TSMC	Taiwan Semiconductor Manufacturing Company
UART	Universal Asynchronous Receiver-Transmitter
UID	User Identification
VDC	Satuan Tegangan Volt Listik Searah
WIFI	Wireless Fidelity



BAB I PENDAHULUAN

1.1 Latar Belakang

Seiring perkembangan zaman dan meningkatnya jumlah penduduk maka berpotensi memiliki dampak negatif berupa peningkatan kejahatan ditengah masyarakat. Jenis kejahatan pun menjadi lebih bervariasi, termasuk spesialisasi dalam pencurian. Sebagai contoh spesialis pencuri kendaraan dan spesialis pencurian rumah. (Henny Aprianty,dkk 2023).

Saat ini, kita telah berada dalam sebuah era yang sarat dengan teknologi komunikasi dan informasi. Teknologi telah memberikan sumber (*resources*) informasi dan komunikasi yang amat luas dari apa yang telah dimiliki manusia. Kebutuhan akan informasi dan komunikasi itu merupakan hal yang tidak kalah pentingnya dari kebutuhan sandang dan pangan manusia (Ahmad, 2012)

Berangkat dari kemajuan teknologi, dapat kita lihat bahwa perkembangan teknologi meningkatkan kebutuhan hidup masyarakat. Perkembangan teknologi memberikan kenyamanan kepada setiap masyarakat dalam melakukan pekerjaan. Selain teknologi efisiensi merupakan hal yang sangat penting dalam pengaruh perkembangan teknologi.

Teknologi memiliki banyak peran penting pada berbagai aspek kehidupan, salah satunya dengan memanfaatkan teknologi di bidang keamanan (*security*). Pengaman ruangan konvensional menggunakan kunci, memiliki kekurangan dalam penggunaannya. Salah satunya yaitu sifat manusia yang terkadang lupa tempat menyimpan kunci tersebut. Dengan menggunakan pengaman ruangan konvensional juga dapat meningkatkan pencurian. Salah satu solusi dari hal tersebut adalah penelitian dari Bahri, Saeful, dan Suhardiyanto yang membuat sistem keamanan ruang server menggunakan teknologi RFID dan password (Bahri & Suhardiyanto, 2018).

Keandalan sebuah sistem keamanan bergantung pada sistem autentikasi yang n. Autentikasi tetap menjadi perlindungan mendasar terhadap akses tidak rangkat atau aplikasi sensitive lainnya, baik *offline* maupun *online*. Pada hanya ada satu faktor yang digunakan untuk melakukan autentikasi pada



sebuah objek. Contohnya seperti diatas karya bahri, dan kawan kawan. Tapi ini merupakan level terendah dari autentikasi dengan membagikan password, seseorang langsung dapat mengakses akun tersebut. Oleh karena itu, autentikasi double-faktor diajukan untuk menyediakan keamanan dengan level yang lebih tinggi untuk melindungi perangkat dari akses yang tidak sah dengan menggunakan dua faktor pengenalan (Ometov dkk., 2018).

Hadis dkk (2018) membuat sistem penguncian yang dirancang dan dibangun menggunakan MAC Address sebagai kode akses. MAC Address tersimpan pada perangkat pengguna sehingga tidak perlu mengingat kode tersebut. Hal ini untuk mengatasi terjadi kelupaan.

Sedangkan Slamet Riyadi dan Rian Herianto (2017) memanfaatkan e-KTP sebagai media *smartcard* dengan SD card sebagai database yang terbung melalui media Bluetooth berisi data data e-KTP yang bertanggungjawab atas pengelolaan ruangan yang terdaftar. Dengan menempelkan *smartcard* pada reader, maka jika data sesuai dengan database ruangan akan terbuka secara otomatis, dan bila tidak sesuai dengan data yang ada maka ruangan tersebut tidak akan terbuka (Riyadi & Heriyanto, 2017).

Dengan penelitian yang serupa, Moch Iqbal Tawakkal, dan Yudi Ramdhani (2021) juga memanfaatkan e-KTP sebagai media *smartcard*. Yang menjadi perbedaan dengan penelitian sebelumnya, penelitian ini menggunakan menggunakan teknologi *Internet of Things*(IoT) dengan menggunakan *wireless* yang terhubung di aplikasi android (Tawakal & Ramdhani, 2021).

Verma & Tripathi, (2010) berhasil membuat dan mengimplementasikan sistem keamanan digital yaitu RFID sebagai penguncian pintu yang dapat bekerja secara *reeltime*. Sistem ini bekerja dengan menghubungkan atau mentag kartu pada reader yang dibangun kemudian informasi pengguna yang mengakses sistem tersebut akan di simpan di server utama.

Siswanto dkk (2019) telah berhasil membuat sistem keamanan ruangan dimana akses kunci pintu dan monitoring ruangan dapat dilakukan melalui android yang terpasang pada smartphone. Sistem ini juga dapat kan pesan peringatan bahaya yaitu seperti adanya kebocoran gas pada ersebut.



Pada penelitian Novita Hanafiah, dkk membuat kunci pintu *elektronik* dinamis, dimana kunci pintu dikendalikan oleh smartphone menggunakan kunci dinamis yang ditransfer melalui koneksi *Bluetooth Low Energi*. Pengembangan kunci dinamis menggunakan *cipher blok* metode enkripsi dan fusi (*artificial neural network*) (Hanafiah dkk., 2021).

Khozainuz Zuhri dan Ahmad Ikhwan (2021) merancang sistem keamanan ganda pada brankas berbasis telegram menggunakan mikrokontroler ESP32-CAM. Dimana upaya untuk mengamankan berupa notifikasi dan peringatan sistem jarak jauh melalui aplikasi telegram. Berdasarkan hal tersebut, peneliti mengusulkan suatu sistem pengamanan ruang brankas menggunakan kamera deteksi gerak berbasis esp32-cam dengan penyimpanan otomatis google drive dan telegram. Hasil dari penelitian adalah notifikasi telegram ke user untuk peringatan dini yaitu 5 detik. Selain itu, sistem mampu menerima sinyal sistem peringatan (*warning system*) hasil deteksi gerakan tergantung pada kekuatan jaringan internet (Zuhri & Ikhwan, 2020).

Abdi Darmawan membuat sistem pada kendaraan bermotor menggunakan kartu. Dengan memasukkan kartu sebagai input untuk mematikan sinyal alarm yang diterima dari input sinyal melalui sensor gerak (*switch*). Jika posisi stang roda dua berubah dari posisi awal, dan stang berubah dengan paksa maka akan memberikan input kepada mikrokontroler untuk menginformasikan sensor inframerah, jika kartu salah maka mikrokontroler akan mengaktifkan klakson (Darmawan, 2010).

Lagan & Ary (2021) membuat sistem kendali kunci pintu menggunakan voice command, dimana dapat di control jarak jauh menggunakan *smartphone* dengan perintah suara yang berfungsi untuk membuka dan mengunci pintu. Alat ini juga dilengkapi dengan sistem monitoring untuk mengetahui keadaan rumah atau sekitar rumah dengan mendeteksi pergerakan dan mengirim notifikasi ke *smartphone*, serta mengirim notifikasi dan membunyikan alarm *Buzzer* ada yang mencoba membobol pintu rumah.



1 & Budiyanto, (2020). Budiyanto membuat prototipe pengaman ruangan akan *voice recognition*. Dimana suara sebagai parameter agar pintu dapat

terbuka. Pada prototipe ini menggunakan sistem *Speech Recognition* sehingga jika kata kunci disebutkan oleh orang yang berbeda, maka pintu akan tetap terbuka

Cahaya Rezky Prihatmoko (2021) membuat *Smart hybrid Reader* yang beroperasi dengan dua mode yaitu menggunakan smart card dan aplikasi android pada *smartphone* untuk keamanan ruangan. *Smart Card* yang dibaca oleh modul RFID akan di kirimkan ke database untuk diverifikasi.

Muhammad Nurfauzi Naim (2022) membuat *Smart Key reader* dengan *multi-factor Authentication* dimana sistem keamanan terdapat beberapa lapis. Pertama menggunakan RFID ataupun aplikasi WEB, setelah itu pengguna akan diarahkan untuk mencocokkan sidik jari, selanjutnya mencocokkan wajah dengan metode *Face Recognition*. Setelah semua data sesuai maka akses ke ruangan akan terbuka.

Dari beberapa jurnal terkait maka pada penelitian ini dibuat Pengembangan *Smart Key Reader* dengan *Multi Biometric Authentication* yang menggabungkan teknologi *smartcard*, *web browser*, dan beberapa *biometric* yaitu *fingerprint*, *voice recognition* dan *face recognition*. Sistem dalam skripsi ini memiliki keunggulan dalam hal keamanan untuk ruangan yang membutuhkan Tingkat keamanan yang tinggi.

1.2 Rumusan Masalah

Berdasarkan uraian pada latar belakang, maka rumusan masalah pada penelitian ini adalah :

1. Bagaimana membuat sistem *Reader Multi Biometric Authentication* menggunakan *Face Recognition*, sidik jari, *RFID*, *Voice Recognition*, dan *Web Browser*?
2. Bagaimana unjuk kerja akses pintu menggunakan *Smart Key Reader* berbasis *Multi Biometric Authentication*?

1.3 Tujuan Penelitian



an yang ingin dicapai dalam penelitian ini adalah :

1. Membuat membuat sistem *Reader Multi Biometric Authentication* menggunakan *Face Recognition*, sidik jari, *RFID*, *Voice Recognition*, dan *Web Browser*.
2. Mengetahui dan mengimplementasikan unjuk kerja akses pintu menggunakan *Smart Key Reader* berbasis *Multi Biometric Authentication*.

1.4 Manfaat Penelitian

Manfaat dari penelitian ini di uraikan dalam beberapa poin di bawah :

1. Bagi masyarakat, mahasiswa, dan staf akademik penelitian ini diharapkan kedepannya dapat memberikan manfaat bagi siapa saja yang membutuhkan sistem keamanan ruangan yang tinggi.
2. Bagi institusi Universitas Hasanuddin, Departemen Teknik Elektro, dan pada bidang Teknologi Telekomunikasi dan Informasi, penelitian ini dapat berguna sebagai referensi ilmiah untuk pengembangan penelitian yang berhubungan dengan topik smart reader khususnya dalam pengembangan smart reader berbasis MFA dan teknologi *biometric*.
3. Bagi peneliti, penelitian ini memiliki manfaat untuk menambah wawasan dan kemampuan penulis, serta menjadi sumber data dalam *Smart Key Reader* dengan *Multi Biometric Authentication*.

1.5 Batasan Masalah

Dalam penelitian ini, perancangan yang akan di buat dibatasi pada hal-hal sebagai berikut :

1. Sistem Keamanan dengan *Multi Biometric Authentication* untuk ruangan dibuat menggunakan ESP32 CAM, ESP32, sensor sidik jari AS608, modul RFID, *Voice Recognition V3*, dan Elektromagnetik Lock Door.
2. Sistem keamanan diuji di Laboratorium Telekomunikasi, Radio, dan Gelombang Pendek.
3. Parameter kinerja yang dianalisis adalah respon Elektromagnetik Door lock terhadap data wajah, sidik jari, suara, dan *smartcard* yang diperoleh.



BAB II TINJAUAN PUSTAKA

2.1. Internet Of Things (IoT)

Internet of Things (IoT), juga disebut Internet Segalanya atau komputasi *Cloud* atau Industrial Internet, merupakan paradigma teknologi baru yang dibayangkan sebagai jaringan global IoT, mesin dan perangkat yang mampu berinteraksi satu sama lain. IoT diakui sebagai frekuensi Radio dan juga salah satu bidang terpenting dari teknologi masa depan dan mendapatkan perhatian luas dari berbagai industri. Nilai sebenarnya dari IoT untuk perusahaan dapat sepenuhnya terwujud ketika perangkat yang terhubung dapat saling berkomunikasi dan berintegrasi dengan sistem inventaris yang dikelola vendor, sistem dukungan pelanggan, aplikasi intelijen bisnis, dan analitik bisnis. Memperkirakan bahwa IoT akan mencapai 26 miliar unit pada tahun 2020, naik dari 0,9 miliar pada tahun 2009, dan akan berdampak pada informasi yang tersedia untuk mitra rantai pasokan dan bagaimana rantai pasokan beroperasi. Dari lini produksi dan pergudangan hingga pengiriman ritel dan rak toko, IoT mengubah proses bisnis dengan memberikan visibilitas yang lebih akurat dan real-time ke dalam aliran bahan dan produk. Perusahaan akan berinvestasi dalam IoT untuk mendesain ulang alur kerja pabrik, meningkatkan pelacakan bahan, dan mengoptimalkan biaya distribusi (Lee & Lee, 2015).

IoT merupakan segala aktifitas yang pelakunya saling berinteraksi dan dilakukan dengan memanfaatkan internet. Dalam penggunaannya IoT banyak ditemui dalam berbagai aktifitas, contohnya : banyaknya transportasi online, e-commerce, pemesanan tiket secara online, live streaming, e-learning dan lain-lain bahkan sampai alat-alat untuk membantu dibidang tertentu seperti remote temperature sensor, GPS *tracking*, and sebagainya yang menggunakan internet atau jaringan sebagai media untuk melakukannya. Dengan banyaknya manfaat dari IoT maka membuat segala sesuatunya lebih mudah, dalam bidang in IoT sangat diperlukan untuk melakukan segala aktifitas dengan akan sistem dan tertata serta sistem pengarsipan yang tepat (Sulaiman & 2017)



IoT dapat digambarkan sebagai penghubung benda-benda seperti telepon pintar, televisi Internet, sensor dan aktuator ke Internet dimana perangkat tersebut digabungkan menjadi bentuk baru yang memungkinkan adanya komunikasi antara seseorang dan benda tersebut. IoT memiliki konsep yang bertujuan untuk memperluas manfaat yang tersambung dalam koneksi Internet secara terus menerus (Amrullah dkk., 2018).

2.2. Multi-Factor Authentication (MFA)

Autentikasi adalah proses dimana “pengguna mengidentifikasi dirinya dengan mengirimkan x ke sistem; sistem mengautentikasi identitasnya dengan menghitung $F(x)$ dan memeriksa bahwa itu sama dengan nilai yang tersimpan y ”. Definisi ini tidak berubah secara signifikan dari waktu ke waktu meskipun fakta bahwa password sederhana tidak lagi menjadi satu-satunya faktor untuk memvalidasi pengguna dari perspektif teknologi informasi. Berikut adalah tiga tipe umum informasi yang tersedia untuk dijadikan faktor-faktor pada metode autentikasi:

1. *Knowledge* factor adalah sesuatu yang diketahui oleh user, seperti password atau “rahasia”;
2. *Ownership* factor adalah sesuatu yang dimiliki oleh user, seperti kartu atau smartphone;
3. *Biometric* factor adalah user itu sendiri, seperti data biometrik atau pola kebiasaan.

Multi-Factor Authentication (MFA) adalah metode autentikasi yang memerlukan user untuk menyediakan dua atau lebih faktor verifikasi untuk mendapatkan akses ke sebuah perangkat tertentu. Sebagian besar MFA berbasis pada biometrik, yang secara otomatis mengenali individu berdasarkan perilakunya dan karakteristik biologi. Metode ini menawarkan peningkatan level keamanan karena bergantung pada dua atau lebih faktor yang berbeda (Ometov dkk., 2018).



2.3. *Smart Key Reader*

Smart berasal dari bahasa Inggris yang berarti pintar. *Key Reader* adalah sebuah kunci pintu yang untuk pengoperasiannya dapat dilakukan dengan cara yang tidak biasa. Dalam hal ini pengoperasian dapat dilakukan dengan menggunakan sidik jari, wajah, suara, dengan menggunakan jaringan internet. Fungsi utama dari smart key reader adalah untuk membatasi orang yang dapat mengakses pintu sehingga hanya orang-orang tertentu yang mendapat ijin dan mendapat wewenang yang dapat mengakses pintu tersebut. Dengan *smart key reader* ini maka keamanan rumah dapat lebih terjamin (Imam,F,F 2018)

2.4. *Biometric Security*

Biometric merupakan sistem yang membaca bagian tubuh manusia untuk mengenali keaslian (authentication), dimana teknologi ini menggunakan bagian yang unik dan tetap dari tubuh manusia seperti sidik jari, wajah, maupun suara yang disimpan dalam database teknologi biometric. Mekanisme kerja dari teknologi ini adalah mencocokkan antara data yang diterima melalui biometric reader dengan apa yang ada dalam database sistem biometric atau dengan kata lain membandingkan data yang sudah didefinisikan (predifined data) dengan data sekarang (presented data). Dari perspektif dana investasi, teknologi biometric security tidak lagi tergolong investasi yang mahal, karena harga aplikasi biometric sudah mulai terjangkau oleh hampir semua lapisan organisasi, jika dibandingkan beberapa tahun sebelumnya, sehingga dalam hal ini teknologi biometric security dapat dipertimbangkan sebagai salah satu alternatif sebagai pengendalian dalam sistem informasi akuntansi (Josua,2004).

2.5. *Penguncian Cerdas*

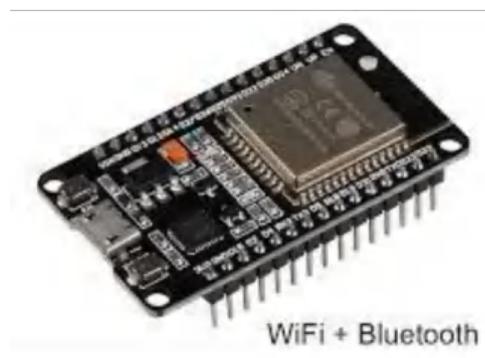
Penguncian cerdas merupakan tambahan atau bahkan pengganti penguncian konvensional dikarenakan sistem ini dapat mengatasi kelemahan memberikan kemudahan yang lebih baik dibandingkan penguncian konvensional. Fitur yang diberikan penguncian cerdas seperti memberikan berupa alarm ketika penguncian berusaha dibobol, dapat melacak siapa masuk dan keluar dari suatu wilayah atau area serta peningkatan



pengontrolan sehingga pengguna dapat menutup dan membuka akses dari jarak jauh. Hal ini membuat sistem penguncian cerdas merupakan hal yang diminati untuk diteliti lebih lanjut demi perkembangan sistem penguncian cerdas. Penguncian cerdas merupakan salah satu produk dari rumah cerdas yang dimana masih pada tahap masa remaja, masih banyak perlu dikembangkan untuk mengatasi kelemahan yang ada seperti kurang responsif dalam mengontrol, permasalahan daya yang digunakan dan sebagainya (Hadis dkk., 2018).

2.6. ESP32

ESP32 dikenalkan oleh *Espressif System* yang merupakan penerus dari mikrokontroler ESP8266. Mikrokontroler ESP32 memiliki keunggulan yaitu sistem berbiaya rendah, dan juga berdaya rendah dengan modul WiFi yang terintegrasi dengan *chip mikrokontroler* serta memiliki bluetooth dengan mode ganda dan fitur hemat daya menjadikannya lebih fleksibel. ESP32 kompatibel dengan perangkat seluler dan aplikasi IoT (*Internet of Things*). Mikrokontroler ini dapat digunakan sebagai sistem mandiri yang lengkap atau dapat dioperasikan sebagai perangkat pendukung *mikrokontroler host*.



Gambar 1 ESP32

ESP32 yang diperlihatkan pada gambar 1 adalah *chip combo* 2,4 GHz WiFi dan *Bluetooth* tunggal yang dirancang dengan daya ultra rendah TSMC 40 nm. Perangkat ini dirancang untuk mencapai daya dan kinerja RF yang terbaik, dengan ketahanan, keserbagunaan dan keandalan dalam berbagai macam dan skenario daya (Gunarjati, 2019)



2.7. ESP32-CAM

ESP32-CAM adalah papan pengembangan mode ganda WIFI + *bluetooth* yang menggunakan antena dan inti papan PCB berbasis *chip* ESP32. Modul ini dapat bekerja secara independen sebagai sistem minimum. Modul ini merupakan sebuah modul WiFi yang sudah dilengkapi dengan kamera ov2640. Dari modul ini bisa digunakan untuk berbagai keperluan, contoh untuk CCTV, mengambil gambar dan sebagainya. Fitur lain yaitu kita bisa mendeteksi wajah (*face detection*) dan pengenalan wajah (*face recognition*). Maka demikian, modul ESP32-CAM ini dapat digunakan untuk mengambil gambar, dan juga dapat digunakan sebagai modul WiFi untuk mengirim data (Y.Fauzan, 2020).



Gambar 2 ESP32-CAM

Fitur dari modul ESP32-CAM adalah:

- a. Modul *Ultra-small* 802.11b / g / n WiFi + BT / BLE SoC
- b. Daya rendah *dual-core* 32-bit CPU untuk prosesor aplikasi 13
- c. Hingga 240MHz, hingga 600 DMIPS
- d. Built-in 520 KB SRAM, eksternal 4M PSRAM
- e. Mendukung antarmuka seperti UART / SPI / I2C / PWM / ADC / DAC
- f. Mendukung kamera OV2640 dan OV 7670 dengan flash built-in
- g. Dukungan untuk upload gambar WiFi
- h. Dukungan kartu TF



Mendukung beberapa mode tidur

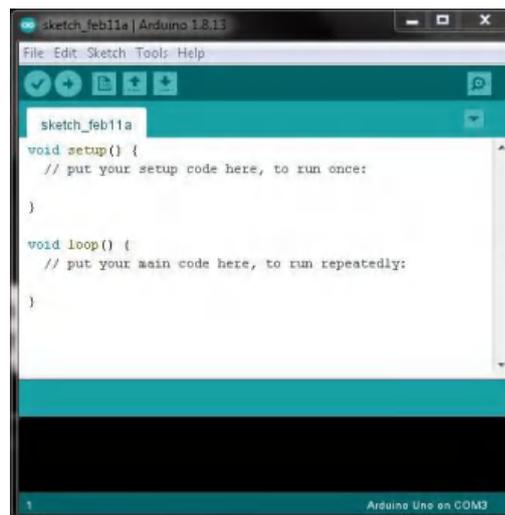
Mertanam Lwip dan FreeRTOS

Mendukung mode kerja STA / AP / STA + AP

- l. Dukungan smart config / AirKiss jaringan distribusi sekali klik
- m. Dukungan untuk peningkatan lokal serial dan peningkatan firmware jarak jauh (FOTA)
- n. Mendukung pengembangan sekunder.

2.8. Software Arduino IDE (Integrated Development Environment)

Arduino memakai *Software processing* untuk diaplikasikan dalam menulis program kedalam *Arduino processing* ini sendiri merupakan penggabungan antara bahasa C++ dan bahasa Java. *Software Arduino* dapat di *install* di berbagai *operating sistem (OS)* 9 *Linux, Mac OS* dan *Windows*. *Software arduino* yang biasa digunakan adalah *software IDE* yang tampilannya dapat dilihat pada gambar 3.



Gambar 3 Software Arduino IDE (Integrated Development Environment)

IDE *Arduino* adalah *software* yang sangat canggih dan dapat di program menggunakan *Java*. IDE *Arduino* terdiri dari (D.Wahyuni,2019):

1. *Editor program* adalah jendela yang memungkinkan pengguna untuk menulis dan mengedit program dalam Bahasa *Processing*.
2. *Compiler* adalah fitur untuk mengubah kode program menjadi kode biner. *Compiler* perlu dilakukan dalam hal ini. Karena sebuah *mikrokontroler* tidak bisa memahami Bahasa *Processing*.



3. *Uploader* adalah fitur untuk memuat kode *biner* dari komputer yang diteruskan ke memori pada board *Arduino*.

2.9. LCD

LCD (*Liquid Crystal Display*) adalah suatu jenis media tampilan yang menggunakan kristal cair sebagai penampil utama, LCD *dot matrix* berfungsi untuk menampilkan tulisan berupa angka, huruf, dan grafik sesuai dengan yang diinginkan (sesuai dengan program yang digunakan untuk mengontrolnya). Pada tugas akhir ini menggunakan LCD dot matrix dengan karakter 20x4, yang kakinya berjumlah 20 pin, seperti yang terlihat pada gambar 4



Gambar 4 LCD (*Liquid Crystal Display*)

LCD adalah suatu jenis media tampilan yang menggunakan kristal cair sebagai penampil utama. LCD terdiri dari lapisan-lapisan cairan kristal diantara dua pelat kaca. Film transparan yang dapat menghantarkan listrik atau *back plane*, diletakkan pada lembaran belakang kaca kemudian bagian trasparan dari film yang dapat menghantarkan arus listrik pada bagian luar dari karakter yang diinginkan dilapiskan pada pelat bagian depan. Pada saat terdapat tegangan antara segmen dan *back plane*, bagian yang berarus listrik ini mengubah transmisi cahaya melalui daerah di bawah segmen film. Berdasarkan jenis tampilan, LCD dapat dikelompokkan menjadi beberapa jenis, yaitu:

1. Segment LCD jenis ini terbentuk dari beberapa seven-segment display atau sixteen segment display, tetapi ada juga yang menggunakan gabungan dari keduanya. LCD jenis ini sering dipakai pada jam digital dan alat ukur digital.



2. *Dot Matrix Character* LCD LCD jenis ini terbentuk dari beberapa *dot matrix* display berukuran 5x7 atau 5x9, yang membentuk sebuah matriks yang lebih besar dengan berbagai kombinasi jumlah kolom dan baris. Kombinasi ini menentukan jumlah karakter yang dapat ditampilkan oleh LCD tersebut, seperti 2 baris x 20 karakter atau 4 baris x 20 karakter.
3. *Graphic* LCD LCD jenis ini masih terus berkembang sampai saat ini. Resolusi LCD jenis ini bervariasi, diantaranya 128x64, 128x128, 240x64, 240x128. Sekarang ini, *graphic* LCD banyak dipakai pada handycam, laptop, telepon selular (*cellphone*), monitor komputer, dan lain-lain.

Adapun register-register yang terdapat dalam LCD adalah sebagai berikut:

1. IR (*Instruction Register*), digunakan untuk menentukan fungsi yang harus dikerjakan oleh LCD serta pengalamatan DDRAM atau CGRAM.
2. DR (data register), digunakan sebagai tempat data DDRAM atau CGRAM yang akan dituliskan ke atau dibaca oleh komputer atau sistem minimum.
3. BF (*Busy Flag*), digunakan untuk memberi tanda bahwa LCD dalam keadaan siap atau sibuk. Apabila LCD sedang melakukan operasi internal, BF di-set menjadi 1, sehingga tidak akan menerima perintah dari luar. Jadi, BF harus dicek apakah telah direset menjadi 0 ketika akan menulis LCD (memberi data pada LCD). Cara untuk menulis LCD adalah dengan mengeset RS menjadi 0 dan mengeset R/W menjadi 1.
4. AC (*address counter*), digunakan untuk menunjuk alamat pada DDRAM atau CGRAM dibaca atau ditulis, maka AC secara otomatis menunjukkan alamat berikutnya. Alamat yang disimpan AC dapat dibaca bersamaan dengan BF.
5. DDRAM (*Display Data Random Access Memory*), digunakan sebagai tempat penyimpanan data sebesar 80 byte. AC menunjukkan alamat karakter yang sedang ditampilkan.



6. CGROM (*Character Generator Read Only Memory*), pada LCD telah terdapat ROM untuk menyimpan karakter-karakter ASCII (*American Standard Code for Interchange Information*), sehingga cukup memasukan kode ASCII untuk menampilkannya.
7. CGRAM (*Character Generator Random Access Memory*), sebagai data storage untuk merancang karakter yang dikehendaki. Untuk CGRAM terletak pada kode ASCII dari 00h sampai 0Fh, tetapi hanya delapan karakter yang disediakan. Alamat CGRAM hanya 6 bit, 3 bit untuk mengatur tinggi karakter dan 3 bit tinggi menjadi 3 bit rendah DDRAM yang menunjukkan karakter, sedangkan 3 bit rendah sebagai posisi data CGRAM untuk membuat tampilan satu baris dalam dot matrix 5x7 karakter tersebut dimulai dari atas, sehingga 25 karakter untuk kode ASCII 00h sama dengan 09h sampai 07h dengan 0Fh. Oleh karena itu untuk perancangan satu karakter memerlukan penulisan data ke CGRAM sampai delapan kali (Nataliana dkk., 2014).

2.10. Smartcard

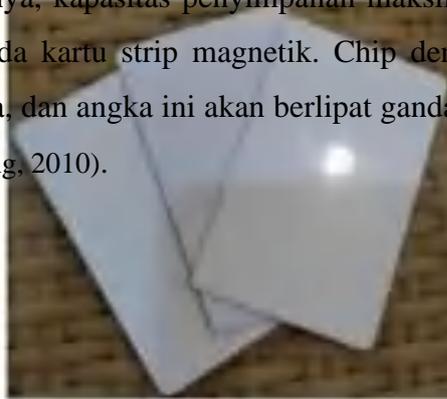


Gambar 5 Arsitektur Smartcard

Smartcard adalah anggota termuda dan terpandai dari keluarga kartu identitas dalam format ID-1. Fitur karakteristiknya adalah sirkuit terintegrasi yang dalam kartu, yang memiliki komponen untuk mentransmisikan, an, dan memproses data. Data dapat ditransmisikan menggunakan ida permukaan kartu atau medan elektromagnetik, tanpa kontak apa pun.



Smartcard menawarkan beberapa keunggulan dibandingkan dengan kartu magnetic-stripe. Misalnya, kapasitas penyimpanan maksimum smartcard berkali-kali lebih besar daripada kartu strip magnetik. Chip dengan lebih dari 256 kB memori saat ini tersedia, dan angka ini akan berlipat ganda dengan setiap generasi chip baru (Rankl & Effing, 2010).



Gambar 6 Tag Mifare Classic 1K.

Sistem *smarrtcard* terdiri dari *hardware*, *software*, dan *protokol smartcard*. *Protokol smart card* meliputi *Key Management System (KMS)* dan *Card Management System (CMS)* yang diimplementasikan ke dalam *Operating System (OS) smartcard*. Semua komponen tersebut bekerja dengan komponen pendukung lainnya, seperti internet dan komputer, menjadi sistem *smartcard*.

Komponen hardware terdiri dari *smartcard reader*, *PC*, *server*, dan *network*. *Software* berupa *Host Application*, *Network Application* dan *Back End Services*. Protokol komunikasi berupa komunikasi antara *smart card* dengan *reader*, *reader* dengan *PC*, lalu *PC* dengan *server*. Hal ini sebagaimana digambarkan pada gambar 6. (Areni dkk., 2019).

Adapun smartcard yang dikembangkan oleh NXP Semiconductors, Mifare Classic EV1 yang ditunjukkan pada gambar 6 merupakan contactless smart card berbasis ISO/IEC 14443 Type A. Mifare Classic EV1 yang digunakan adalah dengan memori (Adhitama & Putra, 2019).



keunggulan:

Transmisi data dan suplay energi *contactless*.

- b. Jarak pengoperasian mencapai 100 mm, tergantung dari geometri antenna dan konfigurasi reader.
- c. Bekerja pada frekuensi 13.56 MHz.
- d. Transfer data 106 kbit/s.
- e. Data *integrity* of 16-bit CRC, *parity*, *bit coding*, *bit counting*.
- f. *Anticollision*.
- g. Tipikal waktu transaksi tiket < 100 ms (termasuk *backup management*).
- h. 7 Byte UID atau 4 Byte NUID.
- i. Mendukung *Random ID* (7 Byte UID version).

2.11. Radio Frequency Identification (RFID)

Radio Frequency Identification (RFID) adalah sebuah teknologi yang menggunakan frekuensi radio untuk mengidentifikasi suatu barang atau manusia. Sejarah perkembangan *radio frequency identification* dimulai sejak tahun 1920, tetapi berkembang menjadi *IFF transponder* pada tahun 1939, dapat dilihat pada gambar 7.



Gambar 7 Radio Frequency Identification (RFID)

Yang waktu itu berfungsi sebagai alat identifikasi pesawat musuh, Dipakai oleh militer Inggris pada perang dunia II. Sejak tahun 1945 beberapa orang berfikir bahwa perangkat pertama RFID ditemukan oleh Leon Theremin sebagai alat untuk pemerintahan Rusia. Sistem RFID terbagi menjadi 3 bagian, yaitu: RFID Tag, RFID Terminal Reader, dan Middleware. Sedangkan



untuk jenisnya RFID terbagi, berdasarkan frekuensi, berdasarkan sumber energi, dan berdasarkan bentuk (T.Santoso, 2019).

Identifikasi data pada RFID tag dilakukan melalui frekuensi radio yang merambat melalui media udara pada jangkauan tertentu sesuai dengan fitur yang dimiliki oleh setiap modul RFID (terdiri dari RFID *Reader* dan RFID tag) yang digunakan. Pada umumnya, data RFID tag yang bersifat unik tersimpan atau tertanam dalam sebuah kartu chip sehingga pengaruh kondisi alam seperti debu, kotoran ataupun temperature udara tidak akan mengurangi kualitas komunikasi data yang terjadi. Fitur-fitur yang dimiliki oleh teknologi RFID ini menjadi keunggulan dari teknologi RFID. Namun keunggulan ini akan bersifat relatif karena akan tergantung dari pemanfaatan suatu teknologi identifikasi pada suatu aplikasi yang akan diimplementasikan. Teknologi ini telah dimanfaatkan pada berbagai aplikasi yang berhubungan dengan sistem identifikasi objek pada beberapa penelitian sebelumnya, seperti membuka pintu, mengakses *computer*, menyalakan sepeda motor, serta mengontrol peralatan di ruangan kantor seperti lampu, *computer* dan lampu penerangan (Addres, t.t.).

2.12. Sensor *Fingerprint AS608*

Fingerprint adalah sebuah alat elektronik yang menerapkan sensor scanning untuk mengetahui sidik jari seseorang guna keperluan verifikasi identitas. Sensor 15 fingerprint seperti ini digunakan pada beberapa peralatan elektronik seperti smartphone, pintu masuk, alat absensi karyawan dan berbagai macam peralatan elektronik yang membutuhkan tingkat keamanan yang tinggi, dan hanya bisa di akses oleh orang - orang tertentu saja (Wijaya dkk., 2020).

Sensor fingerprint merupakan sensor yang digunakan untuk mendeteksi sidik jari dengan menggunakan sistem optik. Deteksi dilakukan dengan membaca kontur (tinggi dan rendah permukaan) sidik jari dan listrik statis tubuh. Hal ini menghasilkan tingkat keamanan yang tinggi karena tidak bisa dipalsukan dengan foto atau sidik jari ataupun sidik jari palsu. Sensor ini memiliki lapisan kaca yang na dan juga memiliki sensor gerak, yaitu jika jari ditempelkan pada maka sensor akan langsung menyala untuk mengambil sidik jari (U. 2020).



Spesifikasi dari modul AS608:

- *Supply Voltage*: 3.6-6.0 VDC
- *Operating Current*: 120mA max
- *Delay system* <1ms
- *Peak Current*: 150mA max
- *Fingerprint Imaging Time*

2.13. Voice Recognition V3

Voice Recognition atau pengenalan ucapan / suara adalah suatu sistem yang dapat mengidentifikasi seseorang melalui suaranya. Modul pengenalan suara atau *Voice Recognition* ini dapat digunakan pada banyak aplikasi pengontrolan yang membutuhkan pendeteksian bukan hanya suara melainkan percakapan seperti home automation (dimana user dapat mengontrol nyala lampu, kunci pintu, televisi, atau perangkat lainnya) atau sebagai modul pelengkap sensor pendengaran pada robot. *Voice Recognition* ini merupakan suatu teknik yang memungkinkan sistem komputer untuk menerima input berupa kata yang diucapkan (Rahayu & Masdi, 2020).

2.14. Teknologi Wi-Fi

Hotspot (WiFi) adalah satu standar *Wireless Networking* tanpa kabel, hanya dengan komponen yang sesuai dapat terkoneksi ke jaringan. (Priyambodo, 2005: 1). Wi-Fi merupakan singkatan dari *Wireless Fidelity* yaitu sebuah media penghantar komunikasi data tanpa kabel yang bisa digunakan untuk komunikasi atau mentransfer program dan data dengan kemampuan yang sangat cepat. Wi-Fi juga dapat diartikan teknologi yang memanfaatkan peralatan elektronik untuk bertukar data dengan menggunakan gelombang radio (nirkabel) melalui sebuah jaringan komputer, termasuk koneksi internet berkecepatan tinggi. Istilah Wi-Fi banyak dikenal oleh masyarakat sebagai media untuk internet saja, namun sebenarnya bisa juga difungsikan sebagai jaringan tanpa kabel (nirkabel)



di perusahaan-perusahaan besar dan juga di warnet. Jaringan nirkabel biasa diistilahkan dengan LAN (*local area network*). Sehingga antara dilokasi satu bisa saling berhubungan dengan komputer lain yang

letaknya berbeda. Sedangkan untuk penggunaan internet, Wi-Fi memerlukan sebuah titik akses yang biasa disebut dengan hotspot untuk menghubungkan dan mengontrol antara pengguna Wi-Fi dengan jaringan internet pusat. Sebuah hotspot pada umumnya dilengkapi dengan password yang bisa meminimalisasi siapa saja yang bisa menggunakan fasilitas tersebut. Ini sering digunakan oleh pengguna rumahan, restoran, swalayan, *café*, dan hotel (Karim dkk., 2016).

2.15. Delay

Delay atau *latency* merupakan salah satu parameter dari *Qualitas of Service* (QoS) yaitu waktu yang dibutuhkan data untuk menempuh jarak dari asal ke tujuan. Delay dapat dipengaruhi oleh jarak, media fisik, kongesti atau juga waktu proses yang lama. Menurut versi *Telecommunications and Internet Protocol Harmonization Over Networks* (TIPHON) standarisasi nilai *latency/delay* sebagai berikut (J. Oliver, 2019) :

Tabel 1 Kategori *delay* versi THYPON

Kategori Delay	Besar Delay
Sangat Bagus	< 150 ms
Bagus	150 s/d 300 ms
Sedang	300 s/d 450 ms
Jelek	> 450 ms

Sedangkan menurut *International Telecommunication Union Telecommunication* (ITU-T) standarisasi nilai *delay* sebagai berikut :

Tabel 2 Kategori *delay* versi ITU-T

Kategori Delay	Besar Delay
Baik	<150 ms
Cukup	150 s/d 400 ms
Buruk	>450 ms

