TUGAS AKHIR

SISTEM PENGUNCIAN MULTI FAKTOR BERBASIS RFID DAN VOICE RECOGNITION UNTUK PENGAMANAN 2 LANGKAH

Diajukan Untuk Memenuhi Syarat Memperoleh Gelar Sarjana Teknik Elektro Pada Fakultas Teknik Universitas Muhammadiyah Sumatera Utara

Disusun Oleh:

FARIZ HANDICHA
2301220121P

UMSU
Unggul | Cerdas | Terpercaya

PROGRAM STUDI TEKNIK ELEKTRO
FAKULTAS TEKNIK
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
MEDAN
2025

SURAT PERNYATAAN KEASLIAN TUGAS AKHIR

Saya yang bertanda tangan di bawah ini:

Nama Lengkap	: Fariz Handicha
Tempat / Tanggal lahir	: Medan / 26 Juli 2003
NPM	: 2307220121P
Fakultas	: Teknik
Program Studi	: Teknik Elektro

Menyatakan dengan sesungguhnya dan sejujurnya, bahwa laporan Tugas Akhir saya yang berjudul:

"Sistem Penguncian Multi Faktor Berbasis RFID dan Voice Recognition Untuk Pengamanan 2 Langkah",

Bukan merupakan plagiarisme, pencurian hasil karya milik orang lain, hasil kerja orang lain untuk kepentingan saya karena hubungan material dan non-material, ataupun segala kemungkinan lain, yang pada hakekatnya bukan merupakan karya tulis Tugas Akhir saya secara orisinil dan otentik.

Bila kemudian hari diduga kuat ada ketidaksesuaian antara fakta dengan kenyataan ini, saya bersedia diproses oleh Tim Fakultas yang dibentuk untuk melakukan verifikasi, dengan sanksi terberat berupa pembatalan kelulusan/ kesarjanaan saya.

Demikian Surat Pernyataan ini saya buat dengan kesadaran sendiri dan tidak atas tekanan ataupun paksaan dari pihak manapun demi menegakkan integritas akademik di Program Studi Teknik Elektro, Fakultas Teknik, Universitas Muhammadiyah Sumatera Utara.

Medan, 19 Agustus 2025

Saya yang menyatakan.

Fariz Handicha

HALAMAN PENGESAHAN

Tugas Akhir ini diajukan oleh:

Nama	: Fariz Handicha
NPM	: 2307220121P
Program Studi	: Teknik Elektro
Judul Skripsi	: Sistem Penguncian Multi Faktor Berbasis RFID dan Voice Recognition Untuk Pengamanan 2 Langkah
Bidang Ilmu	: Sistem Kendali

Telah berhasil dipertahankan di hadapan Tim Penguji dan diterima sebagai salah satu syarat yang diperlukan untuk memperoleh gelar Sarjana Teknik pada Program Studi Teknik Elektro, Fakultas Teknik, Universitas Muhammadiyah Sumatera Utara.

Medan, 19 Agustus 2025

Mengetahui dan menyetujui:
Dosen Pembimbing I

Dr. Rimbawati, S.T., M.T

Dosen Pembanding I / Penguji	Dosen Pembanding II / Penguji
Partaonan Harahap, S.T,. M.T	Faisal Irsan Pasaribu, S.T,. M.T

Program Studi Teknik Elektro
Ketua,

Dr. Elvy Sahnur Nasution, S.T., M.Pd

ABSTRAK

Sistem penguncian pintu berbasis autentikasi tunggal memiliki potensi kerentanan yang cukup tinggi terhadap manipulasi atau akses tidak sah. Untuk mengatasi hal tersebut, dibutuhkan sistem penguncian yang lebih tangguh namun tetap efisien dalam implementasinya. Penelitian ini bertujuan untuk merancang dan mengembangkan Sistem Penguncian Multi Faktor Berbasis RFID dan Voice Recognition Untuk Pengamanan Dua Langkah. Sistem ini ditujukan untuk meningkatkan efektivitas dan keandalan kontrol akses pada ruang terbatas maupun lingkungan hunian. Metode yang digunakan melibatkan integrasi antara modul RFID RC522 dan Voice Recognition V3 Elechouse, dengan mikrokontroler Arduino Uno sebagai pusat kendali. Proses autentikasi dilakukan secara berurutan, dimulai dari pemindaian kartu RFID yang valid, dilanjutkan dengan pengenalan suara. Sistem juga dilengkapi dengan LCD, buzzer, LED, serta tombol buka dari sisi dalam sebagai fitur darurat. Hasil pengujian menunjukkan bahwa sistem mampu beroperasi secara stabil selama lebih dari satu jam tanpa mengalami gangguan, dengan tingkat keberhasilan autentikasi 25 dari 30 percobaan (83,3%). Kegagalan sebanyak 5 percobaan (16,7%) terdiri atas tiga kali akibat gangguan noise lingkungan dan dua kali karena perbedaan intonasi pengguna. Selain itu, sistem menolak seluruh 20 kali uji dengan rekaman suara, sehingga terbukti tahan terhadap upaya spoofing berbasis audio. Berdasarkan hasil tersebut, sistem autentikasi dua langkah yang dikembangkan dinyatakan layak untuk diterapkan pada kebutuhan rumah tangga maupun ruang terbatas lainnya, dengan biaya yang terukur dan kinerja yang dapat diandalkan. Penelitian ini juga membuka peluang pengembangan lebih lanjut pada sistem penguncian berbasis autentikasi berlapis di sektor publik maupun privat.

Kata Kunci**: Multi Faktor, RFID, Voice Recognition, Penguncian**

ABSTRACT

A single authentication-based door locking system has a high potential vulnerability to manipulation or unauthorized access. To overcome this, a more robust locking system is needed but remains efficient in its implementation. This study aims to design and develop a Multi-Factor Locking System Based on RFID and Voice Recognition for Two-Step Security. This system is intended to improve the effectiveness and reliability of access control in confined spaces and residential environments. The method used involves the integration of the RFID RC522 module and Voice Recognition V3 Elechouse, with the Arduino Uno microcontroller as the control center. The authentication process is carried out sequentially, starting from scanning a valid RFID card, followed by voice recognition. The system is also equipped with an LCD, buzzer, LED, and an open button from the inside as an emergency feature. The test results show that the system is able to operate stably for more than an hour without experiencing any interference, with an authentication success rate of 25 out of 30 trials (83.3%). The failure of 5 trials (16.7%) consists of three times due to environmental noise interference and two times due to differences in user intonation. Furthermore, the system resisted all 20 voice recording tests, proving its resilience against audio-based spoofing attempts. Based on these results, the developed two-factor authentication system is deemed feasible for use in households and other confined spaces, with measurable costs and reliable performance. This research also opens up opportunities for further development of multi-layered authentication-based locking systems in both the public and private sectors.

Keywords: ***Multi Factor, RFID, Voice Recognition, Locking***

KATA PENGANTAR

Dengan nama Allah Yang Maha Pengasih lagi Maha Penyayang. Segala puji dan syukur penulis ucapkan kehadirat Allah SWT yang telah memberikan karunia dan nikmat yang tiada terkira. Salah satu dari nikmat tersebut adalah keberhasilan penulis dalam menyelesaikan laporan Tugas Akhir ini yang berjudul "Sistem Penguncian Multi Faktor Berbasis RFID Dan Voice Recognition Untuk Pengamanan 2 Langkah" sebagai syarat untuk meraih gelar akademik Sarjana Teknik pada Program Studi Teknik Elektro, Fakultas Teknik, Universitas Muhammadiyah Sumatera Utara (UMSU), Medan.

Banyak pihak telah membantu dalam menyelesaikan laporan Tugas Akhir ini, untuk itu penulis menghaturkan rasa terimakasih yang tulus dan dalam kepada:

1. Ibu Dr. Rimbawati, ST, MT, Dosen Pembimbing I dan Penguji yang telah banyak membimbing dan mengarahkan penulis dalam menyelesaikan Tugas Akhir ini.
2. Bapak Partaonan Harahap, ST, MT, selaku Dosen Pembanding I dan Penguji yang telah banyak memberikan koreksi dan masukan kepada penulis dalam menyelesaikan Tugas Akhir ini.
3. Bapak Faisal Irsan Pasaribu, ST, MT, selaku Dosen Pembanding II dan Penguji yang telah banyak memberikan koreksi dan masukan kepada penulis dalam menyelesaikan Tugas Akhir ini.
4. Ibu Elvy Sahnur Nasution, ST, MPd, yang telah banyak memberikan koreksi dan masukan kepada penulis dalam menyelesaikan Tugas Akhir ini, sekaligus sebagai Ketua Program Studi Teknik Elektro, Universitas Muhammadiyah Sumatera Utara.
5. Bapak Dr. Munawar Alfansury Siregar, ST, MT selaku Dekan Fakultas Teknik, Universitas Muhammadiyah Sumatera Utara.
6. Seluruh Bapak/Ibu Dosen di Program Studi Teknik Elektro, Universitas Muhammadiyah Sumatera Utara yang telah banyak memberikan ilmu keteknikelektroan kepada penulis.
7. Orang tua penulis: M. Yusni dan Nuraini, yang telah bersusah payah membesarkan dan membiayai studi penulis.

8. Bapak/Ibu Staf Administrasi di Biro Fakultas Teknik, Universitas Muhammadiyah Sumatera Utara.
9. Teman-teman penulis: Ade Naufal Nufairi, Mhd Iqbal, Tengku Alif Bima Yudha Mahesa, dan lainnya yang tidak mungkin namanya disebut satu per satu, terima kasih atas dukungan dan motivasi yang telah kalian berikan. Kalian membuat perjalanan ini tidak terasa sendirian.
10. Adik Online penulis: Yuke Yulia Elvan, selalu memberikan dukungan tanpa henti. Kehadiranmu telah menjadi motivasi yang luar biasa, mengisi kekosongan dan membuat perjalanan penulisan ini terasa jauh lebih ringan dan bermakna.

Laporan Tugas Akhir ini tentunya masih jauh dari kesempurnaan, untuk itu penulis berharap kritik dan masukan yang konstruktif untuk menjadi bahan pembelajaran berkesinambungan penulis di masa depan. Semoga laporan Tugas Akhir ini dapat bermanfaat bagi dunia konstruksi Teknik Elektro.

Medan, 19 Agustus 2025

Fariz Handicha

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB 1
PENDAHULUAN

1.1 Latar Belakang

Dalam hal keamanan rumah, pintu masuk merupakan salah satu dari banyak lokasi yang sering menjadi sasaran tindak kejahatan. Karena masih banyak yang menggunakan kunci mekanis klasik yang mudah dibuka paksa atau dibobol dengan kunci palsu, pintu merupakan salah satu lokasi yang sering menjadi incaran para penjahat.

Keamanan tempat tinggal menjadi kebutuhan yang tidak bisa diabaikan, terutama dengan meningkatnya kasus pencurian dan pembobolan rumah dalam beberapa tahun terakhir. Di banyak daerah, pintu rumah sering menjadi titik rawan karena masih menggunakan sistem penguncian manual yang mudah dibuka paksa. Sementara teknologi keamanan sudah berkembang pesat, akses terhadap sistem canggih tersebut belum merata.

Banyak sistem penguncian digital seperti *smart lock* dan pengenalan wajah memerlukan biaya pemasangan yang mahal dan integrasi dengan internet. Kondisi ini tentu menjadi tantangan tersendiri, khususnya bagi masyarakat kalangan menengah ke bawah. Di sisi lain, teknologi sederhana seperti RFID dan Voice Recognition kini semakin mudah diakses, murah, dan dapat digunakan untuk membangun sistem penguncian yang fungsional tanpa koneksi internet.

Penulis mengamati bahwa penggunaan satu metode autentikasi saja, seperti kartu RFID, masih menyimpan celah keamanan. Hal ini mendorong kebutuhan akan sistem autentikasi dua langkah *(two-factor authentication)* yang dapat meningkatkan proteksi secara signifikan. Namun, solusi semacam ini belum banyak dikembangkan dalam skala kecil yang bisa dijangkau secara luas.

Melalui tugas akhir ini, penulis merancang dan membangun prototipe sistem penguncian dua langkah berbasis RFID dan Voice Recognition, yang dikendalikan oleh mikrokontroler Arduino Uno. Pengguna diharuskan melewati dua tahap verifikasi secara berurutan untuk membuka pengunci pintu otomatis berbasis solenoid. Semua komponen yang digunakan dipilih karena harganya terjangkau, mudah didapat, dan telah terbukti stabil dalam pengujian.

Dengan pendekatan ini, sistem yang dirancang tidak hanya meningkatkan keamanan secara teknis, tetapi juga menyampaikan pesan bahwa sistem pengamanan tidak harus mahal untuk bisa efektif. Penulis berharap karya ini dapat menjadi alternatif yang relevan bagi rumah tinggal, pos keamanan, atau ruang privat lain yang membutuhkan solusi praktis dan terjangkau.

Sebagai kontribusi terhadap solusi tersebut, tugas akhir ini berjudul "Sistem penguncian Multi Faktor Berbasis RFID dan Voice Recognition untuk Pengamanan 2 Langkah", yang difokuskan pada perancangan, integrasi, dan analisis sistem pengamanan dua tahap dengan biaya rendah dan keandalan tinggi.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan, penelitian ini dilakukan untuk menjawab beberapa pertanyaan berikut:

1. Bagaimana sistem interkoneksi RFID dan Voice Recognition sebagai sistem penguncian Multi-Faktor.
2. Bagaimana cara mengintegrasikan kedua metode autentikasi tersebut agar dapat dikendalikan secara berurutan menggunakan mikrokontroler Arduino?
3. Seberapa efektif sistem ini dalam meningkatkan keamanan akses dibandingkan sistem dengan satu metode autentikasi saja?

1.3 Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah sebagai berikut:

1. Membangun sistem autentikasi dua langkah berbasis RFID dan Voice Recognition sebagai prototipe sistem penguncian pintu.
2. Mengintegrasikan modul RFID dan Voice Recognition agar dapat dikendalikan secara berurutan menggunakan mikrokontroler Arduino Uno.
3. Mengevaluasi efektivitas sistem dalam meningkatkan keamanan akses dibandingkan sistem dengan autentikasi tunggal.

1.4 Batasan Penelitian

Ruang lingkup penelitian ini mencakup aspek-aspek yang secara khusus menjadi fokus kajian, sehingga pembahasan tetap terarah dan sesuai dengan tujuan penelitian. Adapun cakupan penelitian ini adalah sebagai berikut:

1. Sistem autentikasi yang dikembangkan memanfaatkan dua metode verifikasi, yaitu *Radio Frequency Identification* (RFID) dan *Voice Recognition*, tanpa melibatkan metode autentikasi biometrik lainnya seperti sidik jari (*fingerprint*) atau pemindaian wajah (*facial recognition*).
2. Prototipe sistem dirancang dalam skala mini dan tidak merepresentasikan ukuran fisik pintu sesungguhnya. Seluruh pengujian dilakukan pada kondisi lingkungan *indoor* untuk memastikan kestabilan dan konsistensi pengukuran.
3. Sistem direalisasikan sebagai perangkat mandiri (*stand-alone*) tanpa konektivitas internet serta tidak diintegrasikan dengan platform *Internet of Things* (IoT) maupun layanan *cloud computing*.
4. Sistem dirancang menggunakan komponen yang terjangkau secara ekonomis, dengan estimasi total biaya realisasi berada pada kisaran Rp900.000 hingga Rp1.000.000. Perhitungan estimasi ini didasarkan pada harga pasar komponen yang digunakan serta mempertimbangkan biaya tak terduga yang mungkin muncul selama proses perancangan dan perakitan.

1.5 Manfaat Penelitian

Adapun manfaat dari melakukan penelitian untuk tugas akhir ini yaitu sebagai berikut:

1. Memberikan kontribusi terhadap pengembangan sistem penguncian yang lebih inklusif dan terjangkau, tanpa bergantung pada konektivitas internet atau biaya tinggi.
2. Menunjukkan bahwa sistem autentikasi dua langkah dapat dibangun menggunakan komponen berbiaya rendah, tanpa mengorbankan fungsi dasar dan keandalan sistem.
3. Memperkuat pemahaman teknis mengenai integrasi dua metode autentikasi dalam satu sistem kontrol akses berbasis mikrokontroler.

4. Menjadi dasar pengembangan sistem penguncian praktis dan mandiri, yang dapat diterapkan pada berbagai kebutuhan ruang akses terbatas secara ekonomis.

1.6 Sistematika Penulisan

Untuk memperoleh pemahaman yang lebih mendalam mengenai penelitian ini, materi-materi yang dibahas dalam skripsi ini akan dikelompokkan ke dalam beberapa bab dengan penyusunan yang sistematis sebagai berikut:

1. BAB I PENDAHULUAN

   Bab ini bertindak sebagai pengantar yang menyajikan gambaran umum tentang latar belakang, rumusan masalah, tujuan, manfaat, serta sistematika penulisan dalam penelitian ini.

2. BAB II TINJAUAN PUSTAKA

   Bab ini memuat pembahasan teori dan referensi ilmiah yang berkaitan dengan topik penelitian, serta menjelaskan landasan ilmiah yang menjadi dasar penelitian. Dalam tinjauan pustaka, peneliti akan mengkaji berbagai literatur dari berbagai sumber untuk memperkuat argumen dan pemahaman mengenai masalah yang dibahas.

3. BAB III METODOLOGI PENELITIAN

   Bab ini menguraikan metode yang diterapkan dalam penelitian, termasuk tahapan yang diambil untuk mencapai tujuan penelitian. Metodologi penelitian meliputi pendekatan, teknik, dan prosedur yang digunakan dalam proses pengumpulan dan analisis data, sehingga hasil yang diperoleh dapat dipertanggungjawabkan secara ilmiah.

4. BAB IV HASIL DAN PEMBAHASAN

   Bab ini menyajikan hasil-hasil penelitian yang diperoleh melalui analisis data, kemudian mengulas temuan tersebut secara mendetail untuk menjawab rumusan masalah dan mencapai tujuan penelitian.

5. BAB V PENUTUP

   Bab ini adalah bagian penutup dari skripsi yang menyajikan kesimpulan dan rekomendasi berdasarkan hasil penelitian yang telah dilaksanakan. Selain itu,

bab ini juga merangkum temuan utama dan memberikan saran untuk penelitian di masa depan atau penerapan praktis.

6. DAFTAR PUSTAKA

BAB 2
TINJAUAN PUSTAKA

2.1 Tinjauan Pustaka Relevan

Untuk memperkuat landasan penelitian ini, penulis mengkaji berbagai karya terdahulu yang relevan dengan topik sistem penguncian berbasis autentikasi ganda, khususnya yang menggunakan teknologi RFID, Voice Recognition, serta mikrokontroler Arduino. Tinjauan ini bertujuan untuk memahami pendekatan yang telah dilakukan oleh peneliti sebelumnya, sekaligus menilai celah atau kekurangan yang bisa diperbaiki dalam sistem yang dikembangkan saat ini.

Dalam pengembangan sistem penguncian elektronik, saya menemukan bahwa penggunaan teknologi *Radio Frequency Identification* (RFID) menjadi salah satu pendekatan yang cukup luas digunakan di industri, khususnya dalam hal pelacakan, penyimpanan, dan distribusi data yang berkaitan dengan pergerakan barang dan aset. Tidak hanya itu, RFID juga memiliki potensi dalam aspek keamanan karena mampu melindungi data dari pencurian atau kehilangan informasi fisik di lingkungan operasional yang rawan. Temuan ini sejalan dengan pemaparan [1] yang menyebutkan bahwa RFID merupakan teknik pengumpulan data yang efektif, yang dapat digunakan untuk melacak produksi, inventaris, serta menjaga keamanan informasi dalam rantai pasok industri.

Dalam perancangan sistem penguncian dua langkah ini, penulis secara khusus mempertimbangkan penggunaan RFID karena karakteristik teknis dan praktisnya yang mendukung kebutuhan autentikasi tanpa kontak fisik. Teknologi RFID telah digunakan secara luas dalam pengenalan aktivitas manusia (*Human Activity Recognition*/HAR) karena keunggulannya yang bersifat tidak mengganggu dan tetap menjaga privasi pengguna. Penelitian oleh [2] menjelaskan bahwa sistem pengenalan berbasis RFID menjadi populer karena mampu bekerja tanpa intervensi aktif dari pengguna, sehingga menjadikannya ideal untuk aplikasi yang mengutamakan efisiensi dan kenyamanan. Selain itu, ketika seseorang bergerak dalam jangkauan pembaca RFID, sinyal yang dipantulkan dan dibiaskan akan menghasilkan pola perubahan yang khas. Pola ini memungkinkan sistem untuk mengenali kehadiran atau aktivitas berdasarkan fluktuasi sinyal yang terekam. Hal

ini memperkuat keyakinan penulis bahwa RFID bukan hanya alat identifikasi, tetapi juga memiliki potensi dalam mendeteksi perilaku atau pola akses tertentu secara pasif. Masih dari studi yang sama, RFID juga dikonfirmasi mampu melakukan proses deteksi secara alami tanpa mengganggu aktivitas pengguna, menjadikannya sebagai salah satu solusi autentikasi yang efisien dan layak diterapkan pada sistem penguncian yang berdiri sendiri dan terjangkau.

Sebagai bagian dari pengembangan sistem penguncian berbasis RFID, penulis merasa penting untuk memahami bagaimana teknologi ini didorong oleh berbagai institusi profesional di bidang teknik. Salah satu entitas yang berperan besar adalah IEEE melalui *Council on RFID* (CRFID), yang menjadi pusat kolaborasi antara berbagai Society teknis yang memiliki kepentingan di bidang elektromagnetik, komunikasi nirkabel, dan sistem identifikasi frekuensi radio. Dalam struktur IEEE sendiri, RFID menjadi bagian dari ekosistem teknis *Division IV*, yang menaungi berbagai *Society* seperti *Microwave Theory and Technology Society* (MTT-S), *Antennas and Propagation Society* (AP-S), serta *Electromagnetic Compatibility Society*. Pengetahuan ini memberikan gambaran bahwa RFID bukan sekadar teknologi terapan, melainkan juga merupakan hasil dari sinergi antardisiplin teknik yang terus dikembangkan oleh komunitas ilmiah global [3].

Perkembangan RFID sebagai teknologi identifikasi tanpa kontak telah memberikan pengaruh besar terhadap sistem penguncian modern. Dalam pengalaman penulis, kemudahan integrasi serta kecepatan pembacaan data menjadi dua alasan utama mengapa RFID layak digunakan dalam sistem pengamanan dua langkah. Teknologi ini memungkinkan proses identifikasi berlangsung secara otomatis dan andal, tanpa memerlukan input manual dari pengguna. Sesuai dengan temuan dalam studi oleh [4], RFID telah merevolusi sistem identifikasi dengan pendekatan yang lebih cepat, aman, dan dapat diandalkan. Tidak hanya digunakan dalam pelacakan logistik, RFID juga telah banyak diterapkan pada sistem kontrol akses, menjadikannya teknologi yang sangat relevan untuk diaplikasikan dalam konteks proteksi fisik dan digital.

Dalam konteks keamanan ruang atau akses pintu, penelitian oleh [5] menyoroti bahwa sistem penguncian konvensional masih banyak digunakan masyarakat, namun memiliki kelemahan serius karena rentan terhadap tindakan perusakan atau

pembobolan. Mereka menekankan pentingnya peningkatan keamanan akses, terutama pada area yang menyimpan barang atau aset bernilai. Hal ini menunjukkan urgensi penggunaan teknologi seperti RFID untuk menggantikan sistem manual yang tidak lagi cukup aman. Temuan ini mendukung dasar pemikiran penulis dalam memilih autentikasi berbasis RFID sebagai salah satu komponen penting dalam sistem penguncian dua langkah yang sedang dikembangkan.

Penelitian oleh [6] menekankan bahwa sistem yang memanfaatkan RF sensing seperti RFID memiliki sejumlah kerentanan kritis terhadap serangan spoofing, pemalsuan sinyal, hingga penyadapan data. Dalam konteks tersebut, penulis menilai bahwa penerapan autentikasi dua langkah menjadi semakin relevan, karena menambahkan lapisan verifikasi suara dapat mengurangi potensi eksploitasi dari celah yang disebutkan. Temuan ini memperkuat pendekatan sistem yang dikembangkan, yaitu dengan memadukan RFID dan Voice Recognition untuk memastikan integritas dan keamanan akses secara lebih menyeluruh.

Penelitian oleh [7] membahas tentang penerapan autentikasi multi-faktor dengan menggabungkan pengenalan wajah dan teknologi FIDO (*Fast Identity Online*) untuk meningkatkan keamanan sistem informasi. Dalam kajiannya, mereka menekankan pentingnya penggunaan lebih dari satu metode verifikasi untuk meminimalisir risiko akses ilegal. Autentikasi multi-faktor dianggap lebih aman karena tetap dapat memberikan perlindungan bahkan ketika salah satu faktor verifikasi bocor. Meskipun teknologi yang digunakan berbeda, prinsip dasar pengamanan melalui kombinasi dua metode verifikasi sangat sejalan dengan pendekatan yang digunakan dalam penelitian ini, yaitu menggabungkan RFID dan Voice Recognition sebagai bentuk autentikasi dua langkah yang hemat biaya namun tetap aman dan andal.

Salah satu pendekatan efektif dalam membangun sistem kontrol akses adalah dengan menggunakan mikrokontroler Arduino Uno. Penelitian oleh [8] menunjukkan bahwa Arduino Uno dapat dimanfaatkan untuk membuat sistem kontrol pintu otomatis yang tidak hanya sederhana tetapi juga cukup andal dalam meningkatkan keamanan ruangan. Teknologi ini memberikan kemudahan dalam pengaturan akses pengguna ke ruangan tertentu, serta dapat dimanfaatkan untuk

mengoptimalkan pemanfaatan waktu dan ruang kerja secara efisien tanpa mengurangi aspek pengawasan.

Di sisi lain, teknologi pengenalan suara juga mengalami kemajuan signifikan dan menjadi bagian dari inovasi kecerdasan buatan yang semakin relevan untuk diaplikasikan dalam sistem penguncian. Seiring dengan perkembangannya, pengenalan suara kini telah berevolusi dari sekadar eksperimen laboratorium menjadi teknologi praktis yang terintegrasi dalam perangkat sehari-hari seperti smartphone, komputer, hingga asisten digital. Menurut [9], teknologi ini memungkinkan komputer untuk mengenali dan menginterpretasi suara manusia secara otomatis, sehingga sangat potensial untuk diterapkan sebagai salah satu metode autentikasi dalam sistem penguncian berbasis suara.

Teknologi pengenalan suara yang diimplementasikan dalam *artificially intelligent interactive voice assistants* (AIIVAs) menunjukkan bahwa kecanggihan sistem ini tidak hanya terletak pada kemampuan pemrosesan bahasa alami dan pembelajaran mesin, tetapi juga pada fitur antropomorfiknya seperti suara manusia. Karakteristik ini memungkinkan pengguna membangun persepsi seolah-olah sedang berinteraksi dengan entitas yang memiliki dimensi sosial dan emosional, bukan sekadar perangkat elektronik. Hal ini menjadikan Voice Recognition bukan hanya sebagai media input, tetapi juga sebagai penguat interaktivitas dan penerimaan pengguna terhadap sistem penguncian berbasis suara [10].

Penelitian oleh [11] menunjukkan bahwa sensor berbasis $PdSe_2$ mampu mendeteksi getaran pita suara ketika ditempatkan di area leher pengguna. Sensor ini menunjukkan respons yang konsisten saat pengguna mengucapkan huruf vokal seperti "U", "E", "S", "T", dan "C", yang menandakan potensi kuatnya dalam aplikasi Voice Recognition. Temuan ini memberikan kontribusi penting dalam konteks sistem penguncian dua langkah berbasis suara, karena menggarisbawahi bahwa kualitas pengenalan suara tidak hanya dipengaruhi oleh perangkat lunak, tetapi juga oleh sensitivitas perangkat keras yang mampu menangkap ciri khas getaran vokal secara akurat.

Penelitian yang dilakukan oleh [12] menyoroti bagaimana media sosial telah memungkinkan ekspresi diri yang lebih luas, terutama bagi kelompok disabilitas. Ketersediaan format ekspresi yang beragam seperti audio, teks, dan video

menciptakan ruang bersama yang mendukung dokumentasi dan koneksi antarindividu. Dalam konteks sistem penguncian berbasis pengenalan suara, hal ini menunjukkan bahwa format suara sebagai media digital tidak hanya inklusif, tetapi juga fungsional sebagai sarana identifikasi personal yang efektif. Dengan demikian, penggunaan suara dalam autentikasi dua langkah memperkuat peran teknologi sebagai alat aksesibilitas sekaligus keamanan.

Menurut *conclusion* pada penelitian yang dilakukan oleh [13], perubahan karakteristik suara akibat kelelahan vokal dapat terjadi bahkan pada pengguna dengan suara yang sehat. Penelitian tersebut mengeksplorasi kelelahan vokal dari sudut pandang subjektif, klinis, dan teknis, serta menunjukkan bahwa sistem pengenalan suara memerlukan pendekatan yang bersifat personal untuk menjaga akurasi.

Temuan ini mendukung pendekatan yang digunakan dalam sistem ini, yaitu membatasi perintah suara hanya pada dua perintah dasar ('BUKA' dan 'TUTUP') serta menggunakan satu pengguna utama untuk proses pelatihan suara. Hal ini dimaksudkan untuk menjaga akurasi pengenalan, mengurangi risiko kesalahan akibat perubahan suara, serta menyederhanakan implementasi pada perangkat keras dengan keterbatasan sumber daya.

Menurut *conclusion* dalam penelitian yang dilakukan oleh [14], sistem pengenalan suara berbasis digital dapat diimplementasikan secara efisien dan ekonomis dalam skala besar, bahkan oleh pengguna non-profesional. Penelitian tersebut menunjukkan bahwa sistem Voice Recognition yang dioptimalkan mampu bekerja dengan baik di tengah keragaman bahasa dan tingkat pendidikan pengguna. Temuan ini memperkuat pendekatan yang digunakan dalam penelitian ini, yaitu menyederhanakan sistem menjadi dua perintah suara ('BUKA' dan 'TUTUP') untuk menjaga tingkat akurasi serta menjangkau pengguna dari berbagai latar belakang teknis.

Penelitian oleh [15] menunjukkan bahwa performa sistem pengenalan suara sangat dipengaruhi oleh kondisi spesifik seperti durasi dan jumlah kata, serta pentingnya validasi pada data yang sesuai dengan konteks pengguna. Hal ini sejalan dengan pendekatan sistem yang dirancang dalam penelitian ini, di mana pengenalan suara dibatasi pada dua perintah utama yang dilatih secara langsung oleh pengguna,

untuk memastikan tingkat akurasi yang dapat diandalkan meskipun tanpa algoritma normalisasi atau pembelajaran lanjutan.

Salah satu tantangan dalam pengembangan sistem penguncian berbasis pengenalan suara adalah potensi serangan spoofing melalui teknologi *voice conversion* atau *deepfake* yang semakin canggih. Penelitian terbaru menunjukkan bahwa sistem verifikasi suara otomatis (ASV) masih rentan terhadap serangan yang memanfaatkan model *deep neural network* (DNN), termasuk teknik *generative adversarial networks* (GANs) yang mampu merekayasa suara sedemikian rupa sehingga menyerupai pengguna asli [16]. Temuan ini menjadi alasan penting mengapa pengamanan dua langkah yang saya bangun membatasi perintah suara hanya pada dua instruksi dasar, serta mengandalkan pelatihan suara secara lokal dan spesifik untuk satu pengguna tetap. Pendekatan ini tidak hanya menyederhanakan sistem, tetapi juga meningkatkan keandalan dalam menghadapi risiko penyalahgunaan teknologi suara sintetis.

Dalam perancangan sistem ini, saya menggunakan modul Voice Recognition Elechouse V3, yang terbukti mampu menyimpan dan mencocokkan pola suara secara langsung dari hasil rekaman. Modul ini dipilih karena telah terbukti efektif digunakan dalam berbagai penelitian, salah satunya oleh Purwitasari et al. yang berhasil menerapkannya dalam sistem pengunci pintu otomatis berbasis suara. Dengan kemampuan mengenali perintah tertentu seperti kata "Buka", Elechouse V3 menjadi pilihan ideal dalam pengamanan dua langkah yang membutuhkan autentikasi suara secara real-time [17].

Penelitian oleh [18] menunjukkan bahwa penerapan teknologi biometrik, termasuk pengenalan wajah, memunculkan konflik etis antara nilai-nilai dasar demokrasi liberal seperti keamanan, privasi individu, otonomi, dan akuntabilitas demokratis. Temuan ini memperkuat pentingnya desain sistem penguncian yang tidak hanya mengedepankan efisiensi teknis, tetapi juga mempertimbangkan hak-hak pengguna, terutama ketika sistem tersebut melibatkan data biometrik seperti suara atau wajah untuk autentikasi.

Namun, meskipun teknologi RFID dan Voice Recognition masing-masing menawarkan efisiensi, kecepatan, dan kenyamanan dalam sistem penguncian modern, keduanya juga memiliki tantangan keamanan yang tidak dapat diabaikan.

Penelitian [6] mengungkap bahwa sistem berbasis RFID rentan terhadap serangan seperti spoofing, penyadapan sinyal, dan pemalsuan identitas digital. Sementara itu, sistem pengenalan suara juga menghadapi ancaman yang semakin kompleks, terutama dari rekayasa suara sintetis berbasis *deep learning* dan *generative adversarial networks* (GANs) yang dapat digunakan untuk melakukan serangan spoofing berbasis suara, seperti ditunjukkan dalam penelitian [16].

Untuk merancang sistem yang tidak hanya fungsional tetapi juga aman dari sisi keamanan siber, penting untuk memahami dan mengantisipasi berbagai potensi kerentanannya. Potensi eksploitasi seperti spoofing, penyadapan sinyal, atau manipulasi identitas dapat secara langsung memengaruhi keandalan sistem, khususnya jika hanya mengandalkan satu metode autentikasi. Oleh karena itu, penerapan autentikasi berlapis melalui kombinasi RFID dan Voice Recognition menjadi pendekatan yang semakin relevan. Sistem dua langkah ini tidak hanya memberikan perlindungan ganda, tetapi juga menurunkan risiko keberhasilan serangan seperti *denial of service* (*DoS*) maupun akses ilegal akibat manipulasi salah satu komponen. Dengan membatasi perintah suara pada dua instruksi sederhana dan melatihnya secara lokal hanya pada satu pengguna tetap, serta menjaga integritas koneksi RFID secara optimal, sistem yang dikembangkan dalam penelitian ini dirancang agar lebih tahan terhadap serangan berbasis perangkat keras maupun perangkat lunak. Pendekatan ini menjadikan sistem penguncian tidak hanya fungsional, tetapi juga adaptif terhadap dinamika ancaman siber yang terus berkembang.

2.2 Landasan Teori

Penelitian oleh [19] mengangkat isu bahwa di era digital saat ini, kebutuhan akan pengamanan bukan lagi hal tambahan, melainkan kebutuhan dasar. Perkembangan teknologi di satu sisi memang membantu kehidupan, namun di sisi lain juga memunculkan ancaman baru seperti maraknya pencurian rumah kosong. Kondisi ini menunjukkan bahwa masyarakat membutuhkan keamanan yang mampu beradaptasi dengan tantangan zaman, termasuk sistem yang bisa bekerja secara otomatis dan mandiri tanpa harus bergantung pada pengawasan manusia sepanjang waktu. Relevansi ini mendasari pentingnya sistem penguncian dua langkah yang

dirancang dalam penelitian ini sebagai respons terhadap kebutuhan masyarakat akan solusi yang praktis dan canggih.

[20] menyatakan bahwa sistem pengamanan konvensional seperti penjaga keamanan dan CCTV mulai dianggap kurang memadai, terutama untuk menjaga objek penting yang memiliki risiko tinggi. Mereka menekankan bahwa sistem pengamanan modern perlu mengandalkan pendekatan yang lebih struktural dan presisi, yang tidak hanya mampu membatasi akses, tetapi juga secara aktif memantau aktivitas pengguna. Gagasan ini sejalan dengan pendekatan yang penulis gunakan dalam membangun sistem autentikasi dua langkah, di mana proses verifikasi dilakukan secara bertingkat untuk memastikan hanya pengguna sah yang bisa mengakses area tertentu, tanpa mengorbankan efisiensi dan kepraktisan sistem.

Penelitian oleh dosen saya [21] mengenai perancangan sistem kontrol penstabil tegangan pada PLTMH Bintang Asih menggunakan PLC M221 menunjukkan bahwa pengembangan sistem berbasis kontrol otomatis membutuhkan perancangan perangkat keras, pemrograman logika, dan pengujian langsung untuk memastikan kestabilan fungsi sistem. Pendekatan ini relevan sebagai referensi dalam membangun sistem penguncian dua langkah berbasis mikrokontroler, karena menekankan pentingnya respon sistem yang cepat dan keandalan fungsi dalam situasi nyata.

Lalu [22] mengenai perancangan PLTS on-grid menggunakan micro inverter menunjukkan pentingnya sistem monitoring berbasis mikrokontroler untuk mendeteksi parameter kelistrikan secara real-time. Dalam penelitian tersebut, mikrokontroler digunakan sebagai pusat pengontrol yang memastikan kestabilan dan efisiensi sistem kelistrikan yang terhubung langsung ke jaringan. Konsep ini relevan dalam pengembangan sistem penguncian dua langkah yang dirancang penulis, karena menekankan pentingnya integrasi antara perangkat keras dan logika kontrol dalam menjamin keandalan sistem yang bekerja secara otomatis dan mandiri.

Dalam konteks kebutuhan autentikasi yang aman dan bermakna, sistem formal sering kali gagal memenuhi rasa keadilan pengguna ketika akses atau perlindungan tidak berjalan sebagaimana mestinya. Seperti yang ditunjukkan oleh [23], pencarian keadilan melalui mekanisme formal kerap menciptakan ketidakadilan baru, yang

kemudian mendorong individu untuk mencari sistem alternatif yang lebih personal dan dapat dipercaya. Temuan ini memberikan dasar penting bagi pengembangan sistem autentikasi berbasis teknologi, seperti pengenalan suara dan RFID, yang harus dirancang tidak hanya untuk mengamankan akses, tetapi juga untuk mengembalikan rasa kendali, validasi, dan kenyamanan bagi pengguna dalam proses interaksinya dengan sistem penguncian.

Era digitalisasi telah mendorong lahirnya berbagai pendekatan autentikasi yang lebih kuat, salah satunya adalah *Multi-Factor Authentication* (MFA). Pendekatan ini menggabungkan dua atau lebih metode verifikasi, seperti sesuatu yang dimiliki pengguna (misalnya kartu RFID) dan sesuatu yang melekat pada pengguna (seperti suara). Menurut [24], MFA memberikan tingkat keamanan yang lebih tinggi dibanding autentikasi tunggal, karena mempersulit upaya penyusupan oleh pihak yang tidak berwenang. Pendekatan ini menjadi dasar penting dalam pengembangan sistem penguncian dua langkah yang dirancang penulis.

Teknologi RFID menjadi salah satu solusi autentikasi yang banyak digunakan karena kemampuannya mengidentifikasi objek secara otomatis menggunakan gelombang radio. Dalam sistem ini, proses identifikasi melibatkan interaksi antara tag, reader, dan basis data, dengan protokol komunikasi yang dirancang untuk menjaga keamanan dan keaslian data yang dikirim. [25] menjelaskan bahwa sistem RFID mampu memastikan bahwa entitas yang berkomunikasi adalah entitas yang sah, menjadikannya cocok untuk kebutuhan autentikasi di pengamanan modern yang membutuhkan verifikasi cepat dan akurat.

Autentikasi merupakan proses elektronik yang digunakan untuk memverifikasi dan memastikan keaslian identitas pengguna, sekaligus mencegah akses dari pihak yang tidak berwenang. [26] menekankan bahwa autentikasi berperan penting dalam menjaga integritas akses sistem, terutama dalam lingkungan digital yang menuntut validasi identitas secara *real-time*. Selain itu, menurut [27], autentikasi tidak hanya memastikan siapa pengguna yang mengakses sistem, tetapi juga menjamin integritas dan keandalan data yang berinteraksi di dalamnya.

Teknologi RFID juga telah digunakan dalam sistem e-voting sebagai metode autentikasi berbasis identifikasi tanpa kontak. Dalam implementasinya, pemilih membawa tag RFID yang menyimpan ID unik, lalu mendekatkannya ke reader

RFID yang terpasang di masing-masing komputer pemungutan suara. Gelombang radio digunakan untuk mentransmisikan ID tersebut ke sistem, yang kemudian melakukan proses verifikasi terhadap identitas pemilih secara otomatis [26]. Pendekatan ini menunjukkan bagaimana RFID dapat berfungsi sebagai komponen autentikasi yang cepat dan efisien dalam sistem yang membutuhkan keakuratan tinggi.

Seiring meningkatnya risiko terhadap sistem informasi, autentikasi kini memegang peran yang semakin sentral dalam menjamin keamanan digital. Tantangan utama dalam era digital bukan hanya berasal dari serangan langsung, tetapi juga dari kebutuhan akses jarak jauh yang semakin luas. Hal ini mendorong transisi dari sistem autentikasi tunggal ke pendekatan yang lebih kompleks seperti *Two-Factor Authentication* (2FA) dan *Multi-Factor Authentication* (MFA). Menurut [28], autentikasi multifaktor telah menjadi fokus utama dalam penelitian keamanan digital karena kemampuannya dalam meningkatkan kepercayaan sistem, meskipun masih diperlukan pengembangan lebih lanjut dalam pemahaman dan penerapan berbagai pendekatannya di dunia nyata.

Teknologi RFID juga menunjukkan kontribusi yang signifikan dalam pengembangan sistem autentikasi fisik. Dalam konteks sistem akses ruangan, RFID berfungsi sebagai identifikasi pribadi yang mampu membatasi akses ke area tertentu. [29] menekankan bahwa evaluasi jarak baca dan posisi optimal tag RFID menjadi faktor penting dalam merancang sistem yang efisien. Mereka juga mengkaji penggunaan kunci elektrik berbasis solenoid sebagai aktuator pengunci, yang jika dirancang secara tepat dapat meningkatkan kenyamanan dan efektivitas pengamanan. Temuan ini memberikan wawasan teknis yang relevan dalam merancang sistem autentikasi dua langkah berbasis RFID yang responsif dan mudah digunakan.

Selain kepraktisannya, sistem RFID juga dikenal karena ketahanan fisik dari RFID Tag Card yang digunakan. Tag ini memiliki daya tahan tinggi terhadap berbagai kondisi lingkungan seperti udara terbuka, pencahayaan ekstrem, debu, dan suhu tinggi, menjadikannya sangat cocok untuk aplikasi keamanan di luar ruang maupun dalam ruang tertutup. Keandalan ini diperkuat dengan struktur casing pelindung dan sistem injeksi data yang membuat informasi di dalamnya tidak

mudah rusak atau hilang. Keunikan setiap tag dalam bentuk kode identitas juga menjadikan RFID sebagai salah satu metode identifikasi yang aman dan sulit dipalsukan, sebagaimana dijelaskan oleh [30].

Pemanfaatan RFID dalam pengamanan sering kali dikombinasikan dengan mikrokontroler untuk membangun perangkat yang cerdas dan responsif. Penelitian oleh [31] menunjukkan bahwa mikrokontroler Arduino menjadi pilihan populer karena sifatnya yang *open-source*, mudah diprogram, dan cocok untuk integrasi dengan berbagai sensor, termasuk RFID. Fleksibilitas Arduino inilah yang membuatnya relevan dalam pengembangan sistem autentikasi dua langkah, seperti yang penulis kembangkan, di mana kendali otomatis dan kemudahan integrasi menjadi faktor utama.

Dalam sistem ini, Arduino Uno berperan sebagai otak pengendali utama yang memproses data dari sensor sidik jari maupun koneksi smartphone melalui Bluetooth. Peran sentral Arduino tidak hanya terbatas pada logika kontrol, tetapi juga menghubungkan berbagai aktuator seperti LED, buzzer, dan relay yang terhubung ke solenoid kunci pintu. Pendekatan ini memperkuat validitas penggunaan Arduino dalam rancangan sistem pengamanan rumah berbasis mikrokontroler karena kemampuannya dalam mengelola integrasi beberapa perangkat input dan output secara real-time [32].

Arduino Uno digunakan sebagai inti kendali sistem karena kesederhanaannya dalam pemrograman dan kelengkapan fitur dasarnya. Papan ini berbasis mikrokontroler ATmega328 dan memiliki 14 pin digital input/output serta input analog, yang sangat cukup untuk menangani interkoneksi antara RFID, modul voice recognition, relay, buzzer, LED, dan LCD. Fleksibilitas koneksi melalui USB maupun catu daya eksternal membuatnya ideal untuk kebutuhan prototipe pengamanan dua langkah ini. Penjelasan mengenai Arduino Uno sebagai papan pengendali juga telah disampaikan dalam penelitian oleh [33], yang menekankan kemudahan integrasi dan kelengkapan fitur perangkat kerasnya dalam membangun sistem otomatisasi berbasis mikrokontroler.

Penggunaan *Arduino Uno* dalam pengamanan berbasis autentikasi dua langkah ini mengadopsi prinsip fleksibilitas dan kendali presisi yang juga telah terbukti dalam berbagai bidang otomasi, termasuk pengendalian temperatur oven listrik.

Seperti yang dijelaskan oleh [34], Arduino Uno dapat diandalkan dalam menerima input, memproses logika kontrol, dan mengatur keluaran ke aktuator seperti *relay* maupun *display* informasi melalui LCD. Dalam konteks penelitian ini, prinsip serupa diterapkan dengan Arduino Uno yang mengatur sistem kerja relay berdasarkan hasil verifikasi data RFID dan perintah suara, serta memberikan umpan balik melalui indikator visual dan suara. Pendekatan ini mendukung keandalan sistem dan kemudahan dalam pengembangan prototipe yang terjangkau dan efisien.

Penggunaan *Arduino Uno* dalam pengembangan sistem otomatis telah diterapkan secara luas dalam berbagai konteks, salah satunya adalah pengontrolan ketinggian air pada media tanam hidroponik seperti yang dirancang oleh [35]. Dalam penelitian tersebut, Arduino Uno digunakan sebagai pusat kontrol untuk memproses data dari sensor ketinggian air dan mengatur kerja motor DC secara otomatis. Penerapan ini menunjukkan bagaimana Arduino dapat menjalankan proses kendali berbasis logika sederhana namun efektif dengan membaca sensor, memutuskan tindakan, dan mengaktifkan aktuator.

Dalam konteks sistem penguncian untuk pengamanan dua langkah berbasis RFID dan *voice recognition* yang saya kembangkan, prinsip kerja serupa diterapkan. Arduino Uno bertugas membaca dua jenis input berbeda (data kartu RFID dan data suara pengguna), lalu mengolahnya secara berurutan sebelum memberikan output kendali kepada relay dan aktuator fisik lainnya. Pendekatan ini menegaskan fleksibilitas Arduino sebagai *core controller* dalam sistem berbasis mikrokontroler untuk berbagai kebutuhan kontrol otomatis.

Penelitian oleh [36] menunjukkan bahwa Arduino Uno dapat diandalkan sebagai pusat kendali dalam sistem penguncian otomatis berbasis biometrik. Dalam konteks pengamanan kendaraan bermotor, Arduino digunakan untuk memproses input dari sensor sidik jari, kemudian mengatur aktuator seperti motor servo dan relay untuk mengunci atau membuka sistem pengaman. Temuan ini menguatkan bahwa Arduino tidak hanya fleksibel dalam pemrograman, tetapi juga cukup efisien untuk mengelola alur autentikasi pengguna secara real-time. Relevansi penelitian ini sangat terasa dalam pengembangan sistem penguncian untuk pengamanan dua langkah yang saya bangun, karena membuktikan bahwa mikrokontroler Arduino

mampu menghadirkan solusi autentikasi yang praktis dan responsif dalam konteks dunia nyata.

Penerapan sistem penguncian dua langkah menggunakan teknologi RFID dan pengenalan suara berbasis Arduino terbukti mampu meningkatkan perlindungan akses secara signifikan. Dengan menggabungkan autentikasi berbasis kepemilikan (melalui tag RFID) dan identifikasi biometrik (melalui suara pengguna), sistem ini menghadirkan lapisan proteksi tambahan yang lebih sulit untuk ditembus dibandingkan sistem autentikasi tunggal. Arduino berperan sebagai pusat kendali yang mengoordinasikan kedua metode autentikasi ini agar berjalan berurutan, responsif, dan efisien dengan waktu respon rata-rata di bawah tiga detik.

Keunggulan utama dari pendekatan ini terletak pada metode autentikasi berlapis, yaitu:

1. Verifikasi dua tahap: Proses autentikasi dimulai dengan pembacaan ID unik pada kartu RFID, kemudian dilanjutkan dengan pencocokan pola suara yang bersifat individual dan sulit untuk ditiru.
2. Perlindungan ganda: Sistem dilengkapi dengan deteksi keaslian suara serta pengaturan jarak baca RFID yang terbatas, guna menghindari pembacaan tidak sah atau penyadapan data.

Dibandingkan dengan sistem satu faktor, rancangan ini mampu mengurangi risiko keamanan seperti duplikasi kartu RFID atau kesalahan identifikasi suara secara signifikan. Selain itu, sistem ini masih tergolong hemat biaya jika dibandingkan dengan solusi komersial yang memiliki fitur serupa.

Meski demikian, pengembangan lebih lanjut tetap diperlukan. Peningkatan skalabilitas sistem, perlindungan terhadap serangan spoofing, serta integrasi dengan *Internet of Things* (IoT) untuk pemantauan jarak jauh adalah langkah strategis ke depan. Penggunaan algoritma pembelajaran mesin (*machine learning*) juga berpotensi memperkuat akurasi dan ketahanan sistem terhadap anomali.

Dengan semua keunggulan tersebut, integrasi RFID, Voice Recognition, dan Arduino dapat menjadi salah satu solusi keamanan yang tidak hanya praktis dan terjangkau, tetapi juga menjadi pondasi kuat bagi sistem akses modern yang lebih adaptif dan cerdas di masa depan.

Teknologi pengenalan suara semakin banyak dimanfaatkan dalam bidang pendidikan, terutama dalam pembelajaran bahasa asing. Salah satu studi oleh [37] mengeksplorasi penggunaan perangkat seperti Alexa dan menunjukkan bahwa teknologi ini tidak hanya meningkatkan kenyamanan dalam berinteraksi, tetapi juga berpotensi besar dalam mendukung praktik pembelajaran yang lebih interaktif dan personal. Penerapan pengenalan suara dalam lingkungan laboratorium bahasa memungkinkan siswa untuk melatih kemampuan berbicara dalam suasana yang lebih natural dan tanpa tekanan sosial, yang umumnya terjadi pada interaksi antarmanusia. Studi tersebut menyoroti bagaimana perangkat berbasis NLP seperti Alexa dapat memberikan pengalaman belajar yang menyenangkan, mudah diakses, dan mendukung pelatihan bahasa secara berkelanjutan.

Teknologi pengenalan suara tidak hanya terbatas pada pengenalan identitas pembicara, namun juga telah berkembang ke arah deteksi emosi yang terkandung dalam ucapan. Salah satu pendekatan yang menunjukkan efektivitas tinggi dalam bidang ini adalah penggunaan arsitektur *Convolutional Neural Network* (CNN), khususnya tipe 1D-CNN. CNN mampu memproses sinyal suara secara satu dimensi untuk mengekstraksi atribut akustik lokal, kemudian melakukan penyaringan (pooling) guna mengenali fitur yang paling signifikan. Dalam konteks sistem penguncian berbasis suara, pendekatan ini memberikan peluang untuk menambahkan lapisan analisis emosional yang dapat mendukung validasi identitas dengan pendekatan biometrik yang lebih manusiawi dan responsif [38].

Selain itu keamanan merupakan suatu kondisi atau situasi di mana individu, organisasi, atau sistem terlindungi dari berbagai risiko, ancaman, atau bahaya yang mungkin timbul. Konsep ini mencakup upaya proaktif dan preventif untuk mendeteksi, mencegah, mengurangi, atau mengatasi potensi ancaman terhadap aset atau kepentingan yang berharga [39]. Melalui penelusuran berbagai literatur, dapat disimpulkan bahwa tingkat keamanan dapat ditingkatkan secara signifikan dengan beberapa pendekatan strategis. Salah satu metode yang paling efektif adalah dengan menerapkan lapisan keamanan tambahan melalui penerapan sistem autentikasi multi-faktor (MFA). Penerapan MFA terbukti dapat meningkatkan tingkat keamanan secara substansial dibandingkan dengan sistem pengamanan konvensional yang hanya mengandalkan satu faktor verifikasi.

MFA (*Multi-Factor Authentication*) merupakan paradigma keamanan komprehensif yang mengharuskan pengguna untuk memberikan dua atau lebih faktor verifikasi independen dari kategori yang berbeda untuk mengonfirmasi identitas mereka sebelum mendapatkan akses ke sistem, aplikasi, atau data sensitif. Tujuan utama dari pendekatan ini adalah untuk memperkuat keamanan secara signifikan dengan meminimalkan risiko akses yang tidak sah, bahkan dalam skenario di mana salah satu faktor keamanan telah dikompromikan. MFA secara efektif mengintegrasikan beberapa lapisan verifikasi yang terdiri dari: sesuatu yang Anda ketahui (seperti kata sandi, PIN, pola, atau frasa sandi), sesuatu yang Anda miliki (seperti token keamanan, ponsel dengan aplikasi login, kartu pintar, atau perangkat keras khusus), dan sesuatu tentang Anda (seperti data biometrik seperti sidik jari, pengenalan wajah, pemindaian retina, analisis suara, atau pola perilaku unik).

Dengan mengintegrasikan berbagai elemen verifikasi, sistem autentikasi multifaktor membentuk perlindungan berlapis yang sulit ditembus oleh pihak jahat, karena mereka harus mengatasi beberapa komponen keamanan sekaligus proses yang melibatkan kendala teknis dan logistik yang rumit. Selain meningkatkan perlindungan, penerapan MFA juga merupakan solusi untuk memenuhi standar regulasi privasi data seperti GDPR, HIPAA, PCI DSS, NIST Cybersecurity Framework, dan ISO 27001, aspek-aspek yang krusial dalam ekosistem digital kontemporer.

Penerapan MFA dirancang untuk menciptakan keselarasan antara perlindungan optimal dan aksesibilitas yang mudah bagi pengguna, dengan fleksibilitas memilih metode autentikasi sesuai dengan preferensi individu dan tingkat ancaman yang dihadapi. Fondasi teknologi di balik MFA mencakup protokol kriptografi tingkat lanjut, algoritma pengenalan biometrik tingkat lanjut, mekanisme verifikasi token dinamis, dan analisis berbasis Kecerdasan Buatan (AI) dan Pembelajaran Mesin (ML) yang terus berkembang untuk menghadapi potensi risiko keamanan yang semakin canggih dan adaptif. Penerapan sistem MFA yang efisien memerlukan pemahaman kontekstual yang mendalam tentang lingkungan keamanan tertentu, penilaian risiko menyeluruh, dan pelaksanaan yang cermat untuk memastikan perlindungan aset berharga secara maksimal.

2.3 RFID

RFID merupakan bagian dari teknologi Auto-ID (*Automatic Identification*), yang mencakup berbagai metode seperti barcode, pembaca karakter optis, dan teknologi biometri. Menurut [40], perbedaan utama antara RFID dan teknologi Auto-ID lainnya adalah bahwa metode identifikasi konvensional masih memerlukan campur tangan manusia, meskipun dalam batas tertentu, untuk menangkap data identitas. Berbeda dengan itu, teknologi RFID (*Radio Frequency Identification*) adalah sistem identifikasi nirkabel yang menggunakan gelombang radio untuk membaca, mengirim, dan menyimpan data secara elektronik pada tag atau transponder tanpa memerlukan intervensi manusia.

Keunggulan utama RFID terletak pada kemampuannya untuk melakukan identifikasi objek atau individu secara otomatis tanpa memerlukan kontak fisik atau garis pandang langsung. Dengan kemampuan ini, RFID menawarkan kecepatan, efisiensi, dan fleksibilitas yang lebih tinggi dibandingkan metode identifikasi visual seperti barcode atau QR code. Selain itu, RFID dapat beroperasi dalam berbagai kondisi lingkungan yang mungkin tidak ideal bagi teknologi identifikasi lainnya, yang menjadikannya sebagai solusi yang lebih efektif dan andal untuk aplikasi yang memerlukan otomatisasi dan kinerja tinggi.

Dalam perkembangan inovasi teknologi, RFID telah mengubah cara kita mengidentifikasi, melacak, dan mengelola objek dalam berbagai industri. Berbeda dengan teknologi identifikasi lainnya, RFID memungkinkan identifikasi tanpa kontak langsung dan dapat membaca beberapa tag secara bersamaan, menghadirkan efisiensi dan kemudahan yang belum pernah ada sebelumnya. Teknik RFID pada dasarnya merupakan teknologi yang berbasis pancaran gelombang radio untuk transmisi data identifikasi, menjadikannya pilihan ideal untuk sistem otomatisasi identifikasi yang memerlukan kecepatan, akurasi, dan operasi tanpa intervensi manusia.

2.3.1 Perkembangan Teknologi RFID

Teknologi *Radio Frequency Identification* (RFID) telah mengalami evolusi yang menakjubkan sepanjang sejarahnya, bertransformasi dari alat bantu militer

menjadi komponen integral dalam berbagai aspek kehidupan modern. Perjalanan panjang teknologi ini mencerminkan bagaimana inovasi dapat beradaptasi dan berkembang untuk memenuhi kebutuhan yang terus berubah dalam masyarakat, membawa dampak signifikan pada efisiensi dan otomatisasi di berbagai sektor.

A. Sejarah Perkembangan

Cikal bakal teknologi RFID dapat ditelusuri kembali ke masa-masa peperangan saat dunia sedang mencari solusi inovatif untuk kebutuhan militer. Pada era yang dipenuhi ketegangan politik dan konflik bersenjata, teknologi identifikasi yang cepat dan akurat menjadi kebutuhan yang krusial di medan perang. Penemuan dan pengembangan gelombang radio pada masa ini tidak hanya mengubah lanskap komunikasi tetapi juga membuka jalan bagi sistem identifikasi yang lebih canggih dan efisien.

Teknologi pancaran gelombang elektromagnetik sudah berkembang dan digunakan sejak Perang Dunia II:

- Jepang, Amerika, dan Jerman menggunakan teknologi radar dengan gelombang radio sebagai alat bantu perang.
- Watson-Watt dalam proyek rahasianya di Inggris membangun *active identity friend or foe* (IFF) yang dipasang pada setiap pesawat Inggris.
- Ketika pesawat Inggris tertangkap radar, pesawat tersebut memancarkan sinyal ke radar untuk mengidentifikasi bahwa pesawat tersebut adalah "teman".
- IFF ini menggunakan prinsip dasar yang sama dengan teknologi RFID.

B. Perkembangan Modern

Setelah perang berakhir, terobosan dalam teknologi RFID terus berlanjut dengan kecepatan yang mengesankan. Dari laboratorium penelitian hingga aplikasi komersial, perjalanan RFID dalam beberapa dekade menunjukkan bagaimana sebuah inovasi dapat berkembang dan beradaptasi dengan kebutuhan masyarakat modern. Kemajuan signifikan dalam miniaturisasi komponen elektronik, peningkatan jangkauan transmisi, dan penurunan biaya produksi telah membuka pintu bagi adopsi teknologi RFID secara luas di berbagai sektor industri, mengubah cara kita mengelola rantai pasokan, inventaris, dan bahkan interaksi sehari-hari dengan lingkungan sekitar.

- 1950-1960: Para ilmuwan meneliti penggunaan frekuensi radio sebagai pembangkit dan pengirim identitas.
- Hasil penelitian tersebut melahirkan anti-theft system yang digunakan di toko swalayan untuk mendeteksi status pembayaran barang.
- 1973: Sistem RFID yang dapat diisi dengan data secara berulang mulai ditemukan di Amerika.
- 1983: Paten pertama yang menggunakan kata RFID diberikan kepada Charles Walton dengan nomor paten Amerika Serikat 4.384.288.
- 1990: IBM mengembangkan sistem RFID menggunakan gelombang UHF yang mampu memancarkan sinyal lebih jauh dan lebih cepat.
- 1999-2003: RFID diadopsi secara luas oleh lebih dari 100 perusahaan besar di dunia dan diterapkan dalam berbagai bidang seperti personalia, inventarisasi aset, dan sebagainya.

2.3.2 Komponen Utama RFID

Sistem RFID (*Radio Frequency Identification*) terdiri dari beberapa komponen utama yang bekerja bersama untuk mengidentifikasi dan melacak objek menggunakan gelombang radio. Berikut adalah komponen-komponen utama tersebut:

1. Tag RFID (Transponder)

Tag RFID adalah komponen kecil yang ditempelkan pada objek untuk diidentifikasi. Komponen ini terdiri dari chip mikro yang menyimpan informasi identifikasi unik dan antena yang mengirimkan serta menerima sinyal radio. Tag RFID dapat bersifat aktif, yang berarti memiliki sumber daya baterai sendiri untuk mengirimkan sinyal, atau pasif, yang berarti mendapatkan energi dari pembaca RFID. Informasi yang tersimpan dalam chip mikro dapat berupa nomor seri, data produk, atau informasi lain yang relevan.

Tag RFID atau transponder adalah komponen kunci dalam sistem identifikasi frekuensi radio. Berikut adalah proses kerja atau cara bagaimana tag RFID beroperasi:

A. Proses Kerja Tag RFID Aktif

- Penyediaan Energi:

Tag RFID aktif memiliki sumber daya baterai sendiri, sehingga tidak bergantung pada pembaca untuk energi. Baterai ini memungkinkan tag untuk secara aktif mengirimkan sinyal radio. Hal ini memberikan keunggulan dalam hal jangkauan pembacaan yang lebih luas dan kemampuan untuk mengirimkan data secara berkala tanpa interogasi dari pembaca.

- Transmisi Data:

  Tag RFID aktif dapat secara mandiri memancarkan sinyal radio yang berisi data yang tersimpan di chip mikro. Ketika pembaca RFID berada dalam jangkauan, tag aktif dapat merespons dengan sinyal yang lebih kuat dan stabil. Selain itu, beberapa tag aktif dapat diprogram untuk mengirimkan data secara berkala, memungkinkan pelacakan real-time tanpa perlu interogasi terus-menerus dari pembaca.

B. Proses Kerja Tag RFID Pasif:

- Penerimaan Energi:

  Ketika pembaca RFID memancarkan gelombang radio, antena pada tag RFID pasif menangkap energi dari gelombang radio tersebut. Energi ini kemudian digunakan untuk mengaktifkan chip mikro yang terdapat di dalam tag. Karena tag pasif tidak memiliki sumber daya baterai sendiri, ia sepenuhnya bergantung pada energi yang diterima dari pembaca. Proses ini terjadi secara instan ketika tag berada dalam jangkauan medan elektromagnetik yang dihasilkan oleh pembaca.

- Transmisi Data:

  Setelah chip mikro pada tag diaktifkan oleh energi yang diterima, ia mengambil data yang tersimpan di dalamnya. Kemudian, antena tag mengirimkan data ini kembali ke pembaca RFID melalui gelombang radio. Respons ini adalah sinyal yang diubah yang berisi informasi yang disimpan dalam chip. Proses transmisi ini terjadi dengan cepat setelah tag menerima energi yang cukup untuk mengaktifkan chip mikro, memungkinkan pembaca untuk menerima data yang diperlukan secara efisien.

Gambar 2. 1 Tag RFID
Sumber: amazon.in

2. Pembaca RFID (*RFID Reader*)

Pembaca RFID adalah perangkat yang mengirimkan gelombang radio untuk mengaktifkan dan membaca informasi dari tag RFID. Pembaca ini memiliki antena yang memancarkan gelombang radio dan menerima respons dari tag. Data yang diterima kemudian diteruskan ke sistem komputer untuk diproses lebih lanjut. Pembaca RFID dapat berupa perangkat genggam, perangkat tetap yang dipasang di pintu atau lorong, atau perangkat.

Pembaca RFID (*RFID Reader*) bertindak sebagai pusat komunikasi dalam sistem RFID, yang bertanggung jawab untuk mengirimkan sinyal interogasi dan menerima respons dari tag. Berikut adalah proses kerja atau cara bagaimana pembaca RFID (*RFID Reader*) beroperasi:

- Pengiriman Sinyal Interogasi:

  Pembaca RFID memancarkan gelombang radio melalui antenanya, menciptakan medan elektromagnetik di sekitarnya. Sinyal ini berfungsi sebagai "panggilan" atau permintaan informasi dari tag RFID. Medan elektromagnetik yang dihasilkan ini juga berfungsi sebagai sumber energi untuk tag RFID pasif, yang tidak memiliki sumber daya baterai sendiri. Dengan mengirimkan sinyal ini, pembaca memulai proses identifikasi dan komunikasi dengan tag RFID yang berada dalam jangkauannya.

- Penerimaan Respons dari Tag:

  Ketika tag RFID berada dalam jangkauan medan elektromagnetik yang dipancarkan oleh pembaca, tag tersebut merespons dengan mengirimkan sinyal yang berisi data yang tersimpan di dalamnya. Antena pada pembaca RFID menerima sinyal respons ini. Sinyal ini kemudian diteruskan ke bagian penerima pada pembaca untuk diproses lebih lanjut. Proses ini terjadi dengan sangat cepat, memungkinkan pembaca untuk mengumpulkan data dari tag RFID secara efisien.
- Dekode dan Pemrosesan Data:

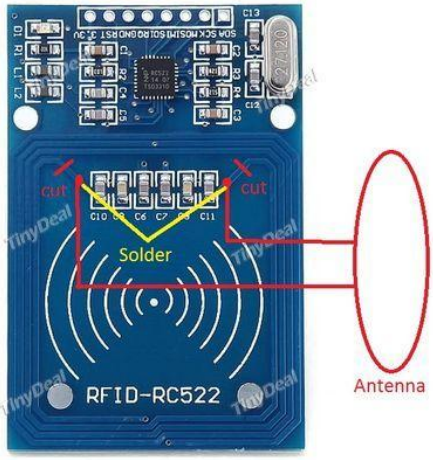
  Setelah menerima sinyal respons dari tag, pembaca RFID mendekode sinyal tersebut menjadi data digital yang dapat dipahami oleh sistem komputer. Proses dekode ini melibatkan konversi sinyal radio menjadi format data yang sesuai. Data digital ini kemudian diproses oleh pengontrol yang terdapat di dalam pembaca. Pengontrol ini melakukan berbagai tugas, seperti memeriksa integritas data, memfilter data yang tidak relevan, dan mempersiapkan data untuk dikirim ke sistem komputer atau perangkat lunak aplikasi.

Gambar 2. 2 Modul RFID RC255

Sumber: electronics-lab.com

3. Antena

Antena dalam sistem RFID berfungsi untuk mengirim dan menerima gelombang radio antara pembaca dan tag. Antena pembaca memancarkan gelombang radio untuk mengaktifkan tag, sementara antena tag merespons dengan mengirimkan informasi yang tersimpan di chip mikro. Antena dapat dirancang untuk berbagai frekuensi dan jangkauan, tergantung pada aplikasi dan kebutuhan spesifik.



Gambar 2. 3 Antena RFID

Sumber: id.pinterest.com

Antena adalah penghubung tak terlihat dalam sistem RFID, yang memungkinkan transmisi dan penerimaan sinyal radio antara pembaca dan tag. Berikut adalah proses kerja atau cara bagaimana antena beroperasi:

- Pemancaran Sinyal Interogasi (Pembaca):

  Antena pada pembaca RFID memancarkan gelombang radio yang berfungsi sebagai sinyal interogasi. Gelombang ini menciptakan medan elektromagnetik yang mencakup area tertentu. Fungsinya tidak hanya mengirimkan sinyal, tetapi juga menyediakan energi yang diperlukan oleh tag RFID pasif untuk beroperasi.
- Penerimaan Respons dari Tag:

  Antena pada pembaca juga berfungsi untuk menerima sinyal respons yang dikirimkan oleh tag RFID. Sinyal ini membawa informasi yang tersimpan di

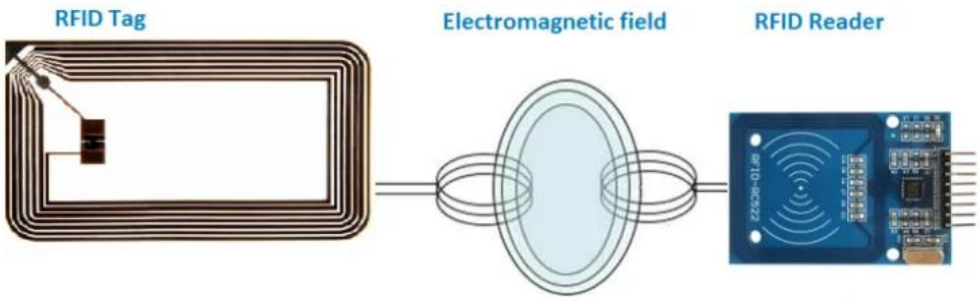
dalam chip mikro tag. Antena harus dirancang untuk sensitif terhadap sinyal lemah yang dikirimkan oleh tag, terutama dalam kasus tag pasif.

- Pengiriman Respons (Tag Aktif):

  Pada tag aktif, antena berfungsi untuk mengirimkan sinyal balik ke *reader* RFID. Sinyal ini berasal dari daya yang di miliki oleh tag itu sendiri.

- Penerimaan Energi dan Pengiriman Respons (Tag Pasif):

  Pada tag pasif, antena memiliki peran ganda. Pertama, antena menangkap energi dari medan elektromagnetik yang dipancarkan oleh pembaca. Energi ini digunakan untuk mengaktifkan chip mikro pada tag. Kedua, setelah chip mikro aktif, antena mengirimkan sinyal respons yang berisi data yang tersimpan kembali ke pembaca.



Gambar 2. 4 Diagram Proses Kerja Sistem RFID
Sumber: elementzonline.com

2.3.3 Prinsip Dasar Operasi RFID

RFID beroperasi dengan memanfaatkan prinsip dasar elektromagnetisme. Sistem RFID terdiri dari dua komponen utama:

1. Tag RFID: Sebuah chip mikro yang dilengkapi dengan antena. Tag ini menyimpan informasi identifikasi unik dan dapat dipasifkan (tanpa sumber daya sendiri) atau diaktifkan (dengan baterai).
2. Pembaca RFID (*Reader*): Perangkat yang memancarkan gelombang radio untuk mengaktifkan dan membaca data dari tag RFID. Pembaca ini terhubung ke sistem komputer untuk memproses dan menyimpan informasi yang diperoleh.

Ketika tag RFID memasuki medan elektromagnetik yang dipancarkan oleh pembaca, energi dari gelombang radio mengaktifkan tag. Tag kemudian mengirimkan data identifikasi yang tersimpan kembali ke pembaca. Data ini kemudian diproses oleh sistem komputer untuk berbagai aplikasi, seperti pelacakan inventaris, kontrol akses, pembayaran tanpa kontak, dan banyak lagi.

2.3.4 Proses Komunkasi RFID

Sistem RFID (Radio Frequency Identification) beroperasi melalui serangkaian proses komunikasi yang kompleks namun terorganisir dengan baik antara berbagai komponennya. Berikut adalah penjelasan mendalam tentang mekanisme komunikasi dalam sistem RFID:

A. *Reader* memancarkan gelombang radio melalui antena.
   - *Reader*, yang berfungsi sebagai inisiator komunikasi, menghasilkan sinyal elektromagnetik pada frekuensi spesifik.
   - Sinyal ini dipancarkan melalui antena *reader* yang membentuk zona interogasi (*interrogation zone*) atau medan elektromagnetik dengan jangkauan tertentu sesuai dengan spesifikasi sistem.
   - Modulasi sinyal pada fase ini mengikuti protokol komunikasi tertentu seperti ISO 14443, ISO 15693, atau EPC Gen2, yang mengatur bagaimana data dikirimkan dan diterima.

B. Tag RFID yang berada dalam jangkauan menerima energi dari sinyal *reader* (untuk tag pasif) atau menggunakan baterai internal (tag aktif).
   - Untuk tag pasif, antena tag menangkap gelombang elektromagnetik dari *reader* dan mengubahnya menjadi energi listrik melalui prinsip induksi elektromagnetik (untuk frekuensi rendah dan tinggi) atau coupling elektromagnetik (untuk UHF dan gelombang mikro).
   - Kapasitor dalam sirkuit tag menyimpan energi yang cukup untuk mengaktifkan chip mikrokontroler embedded yang berisi data identifikasi dan logika pemrosesan.
   - Pada tag semi-pasif, baterai internal hanya mendukung operasi sirkuit mikrokontroler, sementara komunikasi masih bergantung pada energi dari *reader*.

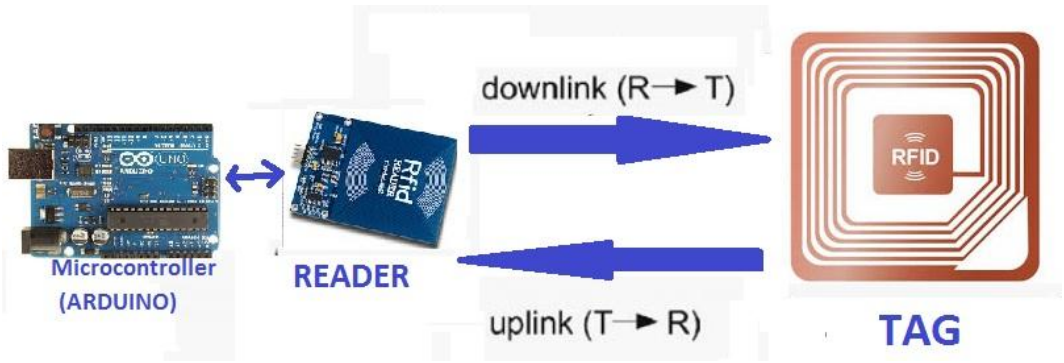
- Tag aktif, dengan sumber dayanya sendiri, memiliki kemampuan untuk memperkuat sinyal respons, sehingga dapat berkomunikasi pada jarak yang lebih jauh (hingga 100 meter atau lebih) dan bahkan dapat menginisiasi komunikasi tanpa terlebih dahulu diaktifkan oleh *reader*.

C. Tag mengirimkan data (misal: ID unik) kembali ke *reader* melalui gelombang radio.
   - Setelah menerima energi yang cukup, mikrokontroler dalam tag memproses sinyal permintaan dari *reader* dan mempersiapkan respons.
   - Tag menggunakan teknik modulasi beban (*load modulation*) untuk tag pasif di frekuensi rendah/tinggi atau *backscatter modulation* untuk tag pasif UHF, di mana tag memodifikasi impedansi antenanya untuk memantulkan kembali sinyal dengan karakteristik yang berbeda.
   - Data yang dikirimkan biasanya mencakup *Unique Identifier* (UID) yang tersimpan dalam memori tag, serta informasi tambahan seperti data pengguna atau status sensor jika tersedia.
   - Proses transmisi data mengikuti protokol *anti-collision* yang memungkinkan multiple tag untuk berkomunikasi dengan *reader* secara simultan tanpa interferensi, menggunakan algoritma seperti ALOHA, *binary tree*, atau *query tree*.

D. *Reader* menerjemahkan data dan meneruskannya ke sistem komputer untuk diproses.
   - Antena *reader* menangkap sinyal yang dipancarkan atau dipantulkan kembali oleh tag.
   - Sirkuit demodulator dalam *reader* mengekstrak data dari sinyal yang diterima, sementara decoder mengkonversi sinyal ini menjadi format digital yang dapat diproses.
   - Mikroprosesor dalam *reader* melakukan verifikasi data yang diterima melalui algoritma *error-checking* seperti CRC (*Cyclic Redundancy Check*) untuk memastikan integritas data.
   - Data yang sudah diverifikasi kemudian diteruskan ke host system (komputer atau server) melalui antarmuka komunikasi seperti RS-232, RS-485, USB, Ethernet, atau koneksi nirkabel seperti Wi-Fi atau Bluetooth.

- *Middleware* RFID pada host system memproses data lebih lanjut, melakukan filtering, agregasi, dan routing ke aplikasi yang sesuai seperti sistem manajemen inventaris, kontrol akses, atau sistem penguncian untuk pengamanan.

Proses komunikasi ini terjadi dalam hitungan milidetik dan memberikan kemampuan bagi sistem RFID untuk mengidentifikasi dan melacak objek secara real-time dengan tingkat akurasi yang tinggi. Kemampuan komunikasi nirkabel tanpa garis pandang (*line-of-sight*) ini membedakan RFID dari teknologi identifikasi lainnya dan memungkinkan implementasinya dalam berbagai aplikasi di bidang rantai pasok, logistik, keamanan, dan berbagai industri lainnya.



Gambar 2. 5 Cara Kerja RFID

Sumber: Jurnal Repositori Universitas Dinamika

2.3.5 Pengaplikasian Teknologi RFID

Pengaplikasian teknologi RFID dalam berbagai sector untuk meningkatkan efisiensi, keamanan, dan akurasi dalam proses tertentu. Berikut adalah ringkasan dari masing-masing poin sebagai pengaplikasian teknologi RFID :

1. Kontrol Akses: Penggunaan RFID dalam sistem penguncian untuk memberikan akses ke gedung atau area tertentu, seperti kartu akses dan sistem parkir otomatis.
2. Manajemen Inventaris: Penerapan RFID untuk pelacakan stok barang di gudang secara real-time, yang membantu dalam pengelolaan inventaris dan mengurangi kesalahan.

3. Ritel: Penggunaan RFID untuk mencegah pencurian (EAS) dan memfasilitasi pembayaran tanpa kontak, yang meningkatkan pengalaman belanja dan efisiensi operasional.
4. Kesehatan: Aplikasi RFID dalam pelacakan alat medis dan rekam jejak pasien, yang meningkatkan pengelolaan peralatan dan keamanan data pasien.
5. Transportasi: Penerapan RFID dalam sistem e-toll dan tiket transportasi umum, yang mempercepat proses pembayaran dan meningkatkan alur lalu lintas.

2.3.6 Kelebihan Teknologi RFID

Teknologi Radio Frequency Identification (RFID) menawarkan serangkaian keunggulan signifikan dibandingkan dengan sistem identifikasi konvensional. Sistem RFID memungkinkan identifikasi dan pelacakan objek secara nirkabel tanpa memerlukan garis pandang langsung, yang secara drastis meningkatkan efisiensi operasional dalam berbagai lingkungan. Dibandingkan dengan teknologi barcode tradisional, RFID menawarkan kecepatan pemrosesan yang lebih tinggi, ketahanan yang lebih baik terhadap kondisi lingkungan yang keras, serta kemampuan untuk membaca banyak tag secara simultan.

Beberapa keunggulan utama teknologi RFID meliputi:

1) Kemampuan pembacaan tanpa kontak langsung dan *line-of-sight*, yang memungkinkan pemindaian objek bahkan ketika tertutup oleh material lain.
2) Durabilitas superior, karena tag RFID lebih tahan terhadap kelembaban, suhu ekstrem, dan kontaminan dibandingkan label barcode.
3) Kapasitas penyimpanan data yang lebih besar, memungkinkan penyimpanan informasi lebih detail tentang produk atau asset.
4) Kemampuan multi-read, di mana ratusan tag dapat dibaca secara bersamaan dalam waktu singkat.
5) Fitur keamanan yang lebih baik, termasuk enkripsi data dan proteksi terhadap pemalsuan.
6) Kemampuan untuk memperbarui informasi secara dinamis pada tag RFID yang dapat ditulis ulang.
7) Jangkauan pembacaan yang fleksibel, mulai dari beberapa sentimeter hingga puluhan meter tergantung pada jenis tag dan *reader*.

8) Otomatisasi proses, mengurangi intervensi manual dan meningkatkan akurasi data.
9) Pelacakan real-time, yang memungkinkan visibilitas aset secara instan.
10) Ketahanan jangka panjang, dengan tag yang dapat berfungsi selama bertahun-tahun tanpa degradasi kinerja.

Dengan kombinasi keunggulan tersebut, teknologi RFID telah menjadi pilihan optimal untuk berbagai aplikasi yang membutuhkan identifikasi objek yang cepat, akurat, dan efisien. Keunggulan-keunggulan ini telah mendorong adopsi RFID secara luas di berbagai sektor industri, mulai dari manajemen rantai pasok dan logistik hingga keamanan akses dan pelacakan aset. Kemampuan RFID untuk mengotomatisasi dan mengoptimalkan proses bisnis tidak hanya menghasilkan penghematan biaya yang signifikan tetapi juga memberikan keunggulan kompetitif bagi organisasi yang mengimplementasikannya, membuktikan bahwa teknologi ini merupakan komponen esensial dalam ekosistem teknologi identifikasi modern yang terus berkembang.

2.3.7 Analisis Pemilihan RFID RC522

Sistem penguncian dua langkah yang saya rancang menempatkan kartu *RFID* sebagai metode autentikasi pertama sebelum dilanjutkan dengan pengenalan suara. Karena itu, pemilihan modul *RFID* menjadi tahap penting yang harus dipertimbangkan secara matang sejak awal. Modul yang dipilih harus tidak hanya kompatibel dengan mikrokontroler yang digunakan (dalam hal ini Arduino Uno), tetapi juga andal, efisien dari sisi daya, serta terjangkau secara biaya.

Setelah melalui proses pengujian awal dan membandingkan beberapa alternatif, saya memutuskan menggunakan modul RC522. Alasan utama pemilihan ini didasarkan pada kemudahan integrasi, dukungan library yang luas, dokumentasi teknis yang mudah diakses, serta harga yang relatif rendah di pasaran lokal Indonesia. Selain itu, RC522 mendukung berbagai protokol komunikasi seperti SPI, I2C, dan UART, yang membuatnya fleksibel untuk diintegrasikan dalam berbagai konfigurasi sistem.

Agar keputusan ini tidak bersifat subjektif, saya juga melakukan perbandingan terhadap beberapa modul lain yang sempat dipertimbangkan. Tabel berikut

menyajikan hasil analisis perbandingan berdasarkan spesifikasi teknis, kemudahan pemakaian, dan pertimbangan praktis lainnya:

Tabel 2. 1 Perbandingan Beberapa Modul *RFID Reader*

Nama Module	Harga	Protokol	Jarak Baca	Frekuensi	Kelebihan	Kekurangan
RC522	Rp15.000-Rp40.000	SPI/I2C/UART	2-5 cm	13.56 Mhz	Murah, kompatibel Arduino, dokumentasi luas	Rentan terhadap gangguan kabel
PN532	Rp50.000-Rp130.000	SPI/I2C/UART	5-7 cm	13.56 MHz (NFC)	Mendukung NFC, jarak lebih jauh	Harga relatif mahal, library lebih kompleks
RDM6300	Rp33.000-Rp75.000	UART	3-8 cm	125 kHz	Mudah digunakan, frekuensi rendah tahan noise	Tidak mendukung kartu MIFARE

Berdasarkan hasil evaluasi tersebut, RC522 terbukti menjadi pilihan paling tepat dalam konteks sistem yang saya rancang. Walaupun tidak memiliki jarak baca sejauh PN532 dan tidak sekuat RDM6300 terhadap gangguan, RC522 memiliki keseimbangan antara performa, kemudahan pemakaian, dan efisiensi biaya. Tantangan terbesar justru berasal dari penggunaan kabel jumper berkualitas rendah yang menyebabkan gangguan komunikasi. Namun, setelah kabel diganti, performa RC522 kembali stabil dan dapat diandalkan.

Dengan pertimbangan teknis dan praktis tersebut, saya menilai RC522 adalah modul *RFID* yang paling sesuai untuk kebutuhan sistem autentikasi awal, terutama dalam prototipe yang berorientasi pada efisiensi dan keterjangkauan.

2.4 Teknologi Voice Recognition (Voice Recognition)

Teknologi Voice Recognition (Pengenalan Suara) merupakan sistem identifikasi dan autentikasi yang memanfaatkan keunikan karakteristik voiceprint pada setiap individu, yang terdiri dari pola frekuensi, intonasi, timbre, dan spektrum suara yang membentuk identitas akustik khas yang berbeda bahkan pada individu dengan suara yang terdengar serupa. Teknologi ini telah mendapatkan adopsi luas di berbagai sektor karena tingkat akurasi dan kemudahan implementasinya yang

tinggi, serta konsistensi pola suara yang relatif stabil meskipun dapat mengalami perubahan minor akibat kondisi kesehatan atau usia. Implementasinya mencakup berbagai aplikasi mulai dari pengamanan smart home, autentikasi perbankan digital, asisten virtual, kontrol akses kendaraan, hingga identifikasi dalam sistem call center dan layanan pelanggan. Kemajuan dalam teknologi pemrosesan sinyal digital dan algoritma machine learning telah meningkatkan kecepatan dan ketepatan proses pengenalan suara, sementara pengembangan mikroprosesor yang lebih canggih memungkinkan analisis real-time yang lebih akurat bahkan dalam kondisi yang menantang seperti lingkungan dengan noise tinggi atau variasi aksen. Selain itu, integrasi teknologi Voice Recognition dengan neural networks dan deep learning telah membuka peluang baru untuk peningkatan adaptabilitas sistem terhadap variasi bahasa, dialek, dan kondisi lingkungan dalam proses autentikasi suara.

2.4.1 Komponen Utama dan Cara kerja Sistem Voice Recognition:

Dalam sebuah sistem Voice Recognition yang canggih, titik awal dari proses identifikasi terletak pada kemampuan untuk menangkap data suara dengan akurat. Inilah peran krusial yang dimainkan oleh komponen utama, yaitu:

1. Sensor Audio/Mikropon (Hardware)

Gambar 2. 6 Mic Modul Voice Recognition V3

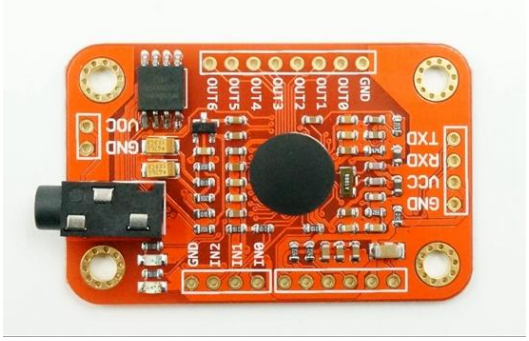
Sumber: robolabs.lk

Sensor audio atau mikropon merupakan komponen perangkat keras yang memiliki fungsi utama untuk menangkap sinyal suara atau data voiceprint seseorang. Dalam menjalankan tugasnya, terdapat beberapa jenis mikropon yang umum digunakan, masing-masing dengan cara kerja yang berbeda.

- Mikropon Kondensor: Menggunakan perubahan kapasitansi untuk mengonversi gelombang suara menjadi sinyal listrik. Mikropon ini sangat sensitif dan mampu menangkap detail frekuensi suara dengan presisi tinggi.
- Mikropon Dinamis: Menggunakan prinsip elektromagnetik di mana diafragma bergerak dalam medan magnet untuk menghasilkan sinyal listrik. Sensor ini tahan terhadap interferensi dan cocok untuk lingkungan dengan noise tinggi.
- Mikropon MEMS: Menggunakan teknologi mikroelektromekanikal yang sangat kecil dan efisien dalam menangkap gelombang suara. Teknologi ini sangat efektif dalam menangkap detail voiceprint, bahkan dalam kondisi yang menantang seperti lingkungan dengan gema atau gangguan akustik.

Sensor ini harus mampu menangkap karakteristik suara dengan akurat agar sistem dapat bekerja dengan baik. Akurasi sensor sangat penting untuk memastikan bahwa sistem dapat membedakan antara voiceprint yang berbeda.

2. Modul Pemrosesan Sinyal Audio (Audio Signal Processing Module)



Gambar 2. 7 Modul Voice Recognition V3 Elechouse

Sumber: edukasielektronika.com

Modul Pemrosesan Sinyal Audio merupakan perangkat lunak yang memiliki peran penting dalam menganalisis sinyal suara yang ditangkap oleh mikropon.

Tugas utamanya adalah menyaring noise dan gangguan yang tidak relevan serta memfokuskan pada karakteristik suara yang membedakan setiap individu. Dalam proses ini, modul tersebut mengekstrak fitur-fitur unik dari voiceprint, seperti:

- Spektral Features: Karakteristik frekuensi dasar (fundamental frequency) dan harmonik yang mencerminkan struktur pita suara individu.
- Prosodic Features: Pola intonasi, ritme bicara, dan tekanan suara yang mencerminkan gaya komunikasi personal.

Fitur-fitur ini kemudian diubah menjadi template digital, yaitu representasi matematis dari voiceprint yang ringkas dan efisien. Template ini akan digunakan untuk proses pencocokan selanjutnya.

3. Basis Data Voiceprint (Voice Database)

   Dalam sebuah sistem Voice Recognition yang efektif, penyimpanan dan pengelolaan data voiceprint yang aman dan terorganisir adalah hal yang sangat penting.

   Basis Data Voiceprint berfungsi sebagai tempat penyimpanan template digital voiceprint yang telah terdaftar, dengan tujuan utama untuk menyimpan data tersebut secara aman dan terorganisir. Hal ini memungkinkan sistem untuk melakukan pencarian dan pencocokan voiceprint dengan cepat dan akurat. Dalam pengelolaan basis data ini, aspek keamanan dan privasi menjadi sangat krusial. Keamanan data voiceprint harus dijamin melalui enkripsi yang kuat dan kontrol akses yang ketat, sementara privasi pengguna harus dihormati dengan mematuhi peraturan yang berlaku dan memastikan transparansi dalam penggunaan data.

4. Modul Pengenalan dan Pencocokan (Recognition and Matching Module)

   Setelah template digital voiceprint berhasil diekstraksi dan disimpan dalam basis data, langkah krusial berikutnya adalah membandingkan template tersebut dengan voiceprint yang baru direkam.

   Modul Pengenalan dan Pencocokan merupakan komponen perangkat lunak yang krusial dalam sistem Voice Recognition, bertugas membandingkan template digital voiceprint yang baru diekstraksi dari rekaman langsung dengan template yang tersimpan di basis data. Fungsi utamanya adalah menentukan

tingkat kecocokan antara kedua template tersebut, dan berdasarkan hasil perbandingan, memutuskan apakah identitas seseorang dapat diverifikasi. Akurasi dari proses pencocokan ini sangat bergantung pada algoritma yang digunakan, di mana algoritma yang efisien dan andal akan menghasilkan tingkat penerimaan palsu (FAR) dan tingkat penolakan palsu (FRR) yang rendah.

5. Sistem Kontrol dan Interface (Control System and Interface)

   Dalam sebuah sistem Voice Recognition yang kompleks, koordinasi dan pengelolaan seluruh komponen sangatlah penting untuk memastikan sistem berfungsi dengan lancar dan efisien.

   Sistem Kontrol dan Interface berperan sebagai komponen utama yang mengatur keseluruhan alur kerja dalam sistem Voice Recognition. Sebagai 'otak' dari sistem, fungsinya mencakup pengelolaan interaksi dengan pengguna melalui antarmuka suara, pengelolaan basis data voiceprint, dan komunikasi dengan sistem lain yang terintegrasi. Sistem ini memastikan bahwa semua komponen bekerja secara terkoordinasi, mulai dari proses perekaman suara hingga verifikasi identitas, serta memberikan feedback audio atau visual kepada pengguna mengenai status autentikasi.

2.4.2 Kelebihan Teknologi Sistem Voice Recognition

Sistem Voice Recognition (pengenalan suara) merupakan teknologi otentikasi yang memanfaatkan karakteristik unik dari pola voiceprint setiap individu untuk verifikasi identitas. Keunggulan utama sistem ini terletak pada kombinasi antara keamanan tinggi dan aksesibilitas yang luar biasa yang tidak ditemukan pada metode otentikasi konvensional. Tidak seperti kata sandi atau kartu identifikasi yang dapat hilang, dicuri, atau dilupakan, voiceprint selalu melekat pada individu dan dapat diakses tanpa kontak fisik, menjadikannya metode verifikasi yang sangat andal dan praktis untuk berbagai aplikasi keamanan, dari kontrol akses jarak jauh hingga autentikasi sistem perbankan digital. Beberapa keunggulan spesifik dari sistem Voice Recognition meliputi:

1) Keunikan akustik yang sangat tinggi**,** karena tidak ada dua individu yang memiliki karakteristik voiceprint identik, bahkan pada kembar identik

sekalipun, berkat perbedaan struktur anatomi pita suara dan rongga resonansi.

2) Kemudahan akses tanpa kontak, di mana pengguna tidak perlu menyentuh perangkat apapun atau membawa token fisik, cukup dengan berbicara pada jarak tertentu.
3) Kecepatan autentikasi real-time, dengan identifikasi yang biasanya selesai dalam hitungan detik melalui analisis spektral langsung.
4) Tingkat keamanan adaptif yang lebih tinggi dibandingkan metode tradisional, dengan kemampuan deteksi suara hidup (*voice liveness detection*) untuk mencegah spoofing dari rekaman.
5) Fleksibilitas implementasi jarak jauh, karena sistem dapat beroperasi melalui saluran komunikasi seperti telepon atau aplikasi digital tanpa kehadiran fisik.
6) Skalabilitas sistem enterprise yang memungkinkan penerapan dari skala personal hingga sistem call center besar dengan ribuan pengguna.
7) Integrasi multi-platform yang mudah dengan pengamanan lain, aplikasi mobile, dan layanan cloud sebagai bagian dari solusi omnichannel.
8) Audit trail yang komprehensif dan tidak dapat disangkal untuk keperluan forensik, compliance, dan monitoring keamanan administrative.
9) Efisiensi biaya operasional yang rendah setelah investasi awal, tanpa kebutuhan hardware khusus atau maintenance fisik berkelanjutan.
10) Adaptabilitas lingkungan yang superior untuk beroperasi dalam berbagai kondisi akustik dengan algoritma noise cancellation dan filter adaptif modern.

Dengan mempertimbangkan semua keunggulan tersebut, sistem Voice Recognition telah menjadi solusi otentikasi terdepan di berbagai sektor digital dan tradisional. Kombinasi keamanan tingkat tinggi, efisiensi operasional, dan pengalaman pengguna yang seamless membuat teknologi ini menjadi pilihan optimal untuk lingkungan yang membutuhkan verifikasi identitas yang andal namun user-friendly. Kemajuan dalam algoritma machine learning dan teknologi pemrosesan sinyal digital terus meningkatkan akurasi dan kecepatan sistem ini, memperluas kemungkinan implementasinya dari smart home automation dan

virtual assistant hingga secure banking dan customer service authentication. Sebagai teknologi yang telah terbukti kehandalannya di era digital, sistem Voice Recognition memainkan peran penting dalam lanskap keamanan modern, menawarkan keseimbangan ideal antara security, convenience, dan accessibility yang sulit dicapai oleh metode otentikasi konvensional.

2.4.3 Aplikasi di Dunia Nyata

Dalam era digital yang terus berkembang, teknologi Voice Recognition telah menjadi bagian integral dari kehidupan sehari-hari. Keandalan dan aksesibilitasnya telah mendorong adopsi luas di berbagai sektor. Berikut adalah beberapa contoh aplikasi nyata:

1. Smart Home dan IoT
    - Asisten Virtual

      Voice Recognition telah menjadi inti dari asisten virtual seperti Amazon Alexa, Google Assistant, dan Apple Siri, menawarkan kontrol hands-free untuk berbagai perangkat rumah pintar dan memberikan pengalaman interaksi yang lebih natural.
    - Kontrol Perangkat Rumah

      Sistem smart home menggunakan Voice Recognition untuk mengoperasikan lampu, AC, sistem penguncian , dan perangkat elektronik lainnya, memungkinkan pengendalian lingkungan rumah tanpa perlu menyentuh panel kontrol.
2. Sektor Perbankan dan Keuangan
    - Phone Banking Authentication

      Bank-bank besar menggunakan Voice Recognition untuk memverifikasi identitas nasabah saat melakukan transaksi telepon, menggantikan PIN dan pertanyaan keamanan tradisional yang rentan terhadap social engineering.
    - Fraud Detection

      Sistem Voice Recognition diintegrasikan dengan sistem deteksi penipuan untuk mengidentifikasi pola suara yang mencurigakan dan mencegah transaksi unauthorized melalui saluran voice banking.
3. Layanan Pelanggan dan Call Center

- Customer Authentication

  Perusahaan telekomunikasi dan layanan finansial menggunakan Voice Recognition untuk autentikasi otomatis nasabah, mengurangi waktu verifikasi identitas dan meningkatkan efisiensi layanan customer service.

- Personalisasi Layanan

  Voice Recognition memungkinkan sistem untuk mengenali pelanggan secara otomatis dan menyediakan layanan yang dipersonalisasi berdasarkan profil dan riwayat interaksi sebelumnya.

4. Otomotif dan Transportasi
   - Vehicle Access Control

     Kendaraan modern mengintegrasikan Voice Recognition untuk membuka kunci mobil, menyalakan mesin, dan mengakses fitur-fitur kendaraan tanpa memerlukan kunci fisik atau remote control.

   - In-Car Entertainment

     Sistem infotainment kendaraan menggunakan Voice Recognition untuk kontrol hands-free terhadap musik, navigasi, dan komunikasi, meningkatkan keselamatan berkendara dengan mengurangi distraksi visual.

5. Healthcare dan Telemedicine
   - Patient Identification

     Rumah sakit dan klinik menggunakan Voice Recognition untuk mengidentifikasi pasien secara akurat, mengurangi kesalahan medical record dan meningkatkan patient safety.

   - Telemedicine Authentication

     Platform konsultasi online menggunakan Voice Recognition untuk memverifikasi identitas pasien dan dokter, memastikan keamanan dan privasi dalam layanan kesehatan jarak jauh.

Dengan demikian, aplikasi Voice Recognition telah terbukti sangat berguna di berbagai bidang, tidak hanya meningkatkan keamanan, efisiensi, dan aksesibilitas, tetapi juga membawa perubahan transformatif dalam cara kita berinteraksi dengan teknologi dan lingkungan digital. Dalam sektor keamanan, Voice Recognition telah memperkuat sistem autentikasi remote, mengurangi risiko identity fraud, dan meningkatkan user experience dengan eliminasi kebutuhan physical contact atau

memorization. Teknologi ini terus berkembang dengan integrasi artificial intelligence dan machine learning, membuka peluang aplikasi baru dalam Internet of Things, smart cities, dan digital transformation yang akan semakin mengubah landscape interaksi manusia-teknologi di masa depan.

2.4.4 Pandangan Masa Depan Sistem Voice Recognition

Perkembangan teknologi Voice Recognition diprediksi akan semakin transformatif, didorong oleh inovasi di bidang *natural language processing* (NLP), *artificial intelligence* (AI), dan integrasi sistem *conversational multimodal*. Algoritma generasi mendatang akan memiliki kemampuan *deep learning* ultra-canggih dan *real-time voice liveness detection* untuk mengidentifikasi synthetic voice atau deepfake audio dengan akurasi hampir sempurna. Integrasi AI akan memungkinkan sistem belajar dari pola komunikasi individual, meningkatkan kecepatan pengenalan dan adaptasi terhadap perubahan voiceprint alami, seperti perubahan suara akibat usia, kondisi kesehatan, atau emosi. Di sisi keamanan data, teknologi *blockchain* akan diterapkan untuk menyimpan template voiceprint secara terdesentralisasi, meminimalkan risiko kebocoran atau penyalahgunaan data biometrik suara. Tren *multimodal conversational AI* seperti menggabungkan Voice Recognition dengan analisis sentimen, gesture recognition, atau biometric fusion akan menjadi standar baru, menciptakan lapisan interaksi yang lebih natural dan aman. Aplikasinya pun akan meluas ke sektor *smart ecosystem*, seperti ambient computing dalam smart cities, *voice-first commerce*, *telepresence authentication*, hingga *neural interface* dalam layanan healthcare dan digital government. Tantangan utama tetap pada perlindungan privasi dan *voice* spoofing, yang memerlukan regulasi ketat dan enkripsi *end-to-end* untuk data voiceprint. Dengan kolaborasi antara kemajuan teknologi AI dan kebijakan yang responsif, sistem Voice Recognition akan menjadi tulang punggung interaksi manusia-teknologi yang seamless, intelligent, serta privacy-preserving dalam era *ambient intelligence*.

2.4.5 Analisis Pemilihan Voice Recognition V3 Elechouse

Sebelum menentukan modul voice recognition yang akan digunakan dalam sistem ini, saya melakukan pencarian dari berbagai sumber, termasuk platform

video seperti YouTube. Tujuannya adalah untuk melihat bagaimana modul-modul yang tersedia bekerja dalam praktik sebenarnya, bukan hanya berdasarkan spesifikasi teknis di atas kertas. Dari hasil penelusuran tersebut, saya menemukan bahwa Voice Recognition V3 buatan Elechouse merupakan modul yang paling banyak digunakan dalam proyek-proyek Arduino untuk sistem pengenalan suara secara offline.

Modul ini mampu mengenali suara pengguna berdasarkan pelatihan langsung, memiliki dukungan pustaka Arduino yang relatif stabil, serta dapat bekerja secara mandiri tanpa koneksi internet. Ini menjadi sangat relevan untuk pengamanan lokal yang tidak selalu terhubung dengan jaringan.

Beberapa modul lain memang disebut-sebut dalam forum atau dokumentasi teknis, namun berdasarkan pencarian saya, sebagian besar dari modul-modul tersebut:

- Tidak lagi tersedia di pasaran
- Tidak dijual dalam bentuk modul siap pakai
- Atau memiliki dokumentasi dan dukungan komunitas yang sangat terbatas.

Di sisi lain, Voice Recognition V3 masih bisa ditemukan dengan mudah di berbagai marketplace seperti Shopee, Tokopedia, maupun situs internasional seperti AliExpress. Harga pasarannya memang cukup tinggi dibandingkan modul sensor lain, yaitu sekitar Rp400.000 hingga Rp500.000 (setara dengan ±28 USD)**,** namun hal tersebut sebanding dengan kemampuannya dalam menyediakan autentikasi suara tanpa bergantung pada cloud atau layanan pihak ketiga.

Melalui berbagai pertimbangan di atas mulai dari ketersediaan modul, kemudahan integrasi, kestabilan dalam implementasi proyek-proyek sejenis, hingga pengalaman pengguna lain di YouTube saya menyimpulkan bahwa Voice Recognition V3 Elechouse adalah pilihan paling relevan dan layak untuk digunakan dalam sistem autentikasi dua langkah yang saya bangun.

2.5 Konsep Keamanan Akses

Keamanan akses merupakan serangkaian kebijakan, prosedur, dan kontrol teknis yang dirancang untuk melindungi sistem, data, dan sumber daya dari akses yang tidak sah atau berbahaya. Konsep ini mencakup berbagai aspek mulai dari

autentikasi (memverifikasi identitas pengguna), otorisasi (menentukan hak akses pengguna), hingga pencatatan aktivitas (audit trail). Dalam implementasinya, keamanan akses menerapkan prinsip "*least privilege*" di mana pengguna hanya diberikan akses minimal yang diperlukan untuk menjalankan tugas mereka. Sistem penguncian akses modern juga menggunakan berbagai mekanisme seperti kata sandi yang kuat, autentikasi multi-faktor, enkripsi data, firewall, dan sistem deteksi intrusi. Selain aspek teknis, keamanan akses juga melibatkan faktor manusia melalui pelatihan kesadaran keamanan, kebijakan penggunaan yang dapat diterima, dan prosedur penanganan insiden. Pemantauan dan evaluasi berkelanjutan terhadap kontrol akses sangat penting untuk memastikan efektivitasnya dalam menghadapi ancaman keamanan yang terus berkembang. Keamanan akses yang baik harus menyeimbangkan antara perlindungan aset informasi dengan kemudahan penggunaan sistem, sehingga tidak menghambat produktivitas pengguna yang sah.

2.6 Konsep Keamanan Akses Dengan Integrasi Teknologi RFID

Konsep keamanan akses adalah kerangka yang bertujuan melindungi sumber daya digital dan fisik dari akses ilegal melalui kombinasi autentikasi, otorisasi, dan pengawasan. Dalam perkembangannya, teknologi RFID (Radio-Frequency Identification) menjadi komponen krusial untuk memperkuat sistem ini, terutama dalam lingkungan yang membutuhkan kecepatan, akurasi, dan skalabilitas. RFID bekerja dengan memanfaatkan gelombang radio untuk mengidentifikasi dan memverifikasi objek atau pengguna melalui tag atau kartu yang tertanam chip. Ketika diintegrasikan ke dalam sistem penguncian akses, teknologi ini tidak hanya meningkatkan efisiensi tetapi juga menambahkan lapisan keamanan fisik yang sulit dipalsukan.

Sistem penguncian berbasis RFID umumnya digunakan untuk mengontrol akses fisik, seperti pintu gedung, parkiran, atau ruang server, serta akses logis ke jaringan dan database. Proses autentikasinya dimulai ketika pengguna mendekatkan kartu RFID ke pembaca. Chip pada kartu mengirimkan data unik yang terenkripsi ke sistem, yang kemudian memvalidasi apakah identitas tersebut terdaftar dan memiliki izin. Untuk mencegah cloning atau penyadapan, RFID modern menggunakan protokol keamanan seperti AES-256 atau Dynamic ID yang

mengubah kode identifikasi secara berkala. Namun, RFID jarang berdiri sendiri—ia sering dipasangkan dengan faktor autentikasi tambahan, seperti biometrik (sidik jari, pengenalan wajah) atau PIN, membentuk sistem Multi-Factor Authentication (MFA) yang lebih tangguh.

Kelebihan utama RFID terletak pada kemudahan penggunaan dan kemampuannya bekerja tanpa kontak fisik, mengurangi keausan perangkat. Di sisi keamanan, integrasi dengan prinsip *Zero Trust* memastikan setiap akses divalidasi ulang, bahkan bagi pengguna yang sudah berada di dalam jaringan. Misalnya, di bandara, petugas keamanan mungkin memerlukan kartu RFID dan verifikasi biometrik untuk memasuki area restriksi. Namun, tantangan tetap ada, seperti risiko skimming (pencurian data RFID melalui perangkat ilegal) atau kehilangan kartu. Untuk mengatasinya, organisasi menerapkan kebijakan seperti RFID blocking (menggunakan bahan pelindung untuk kartu), geofencing (membatasi area penggunaan), atau menggabungkan RFID dengan autentikasi berbasis lokasi.

Dalam skala yang lebih luas, RFID juga mendukung manajemen akses yang terpusat. Sistem seperti PACS (Physical Access Control System) memungkinkan administrator memantau dan memperbarui izin akses secara real-time, mencabut hak pengguna yang kartunya hilang, atau melacak riwayat masuk/keluar untuk keperluan audit. Contoh penerapannya bisa dilihat di rumah sakit, di mana staf menggunakan badge RFID untuk membuka pintu ruang operasi sekaligus mengakses data pasien, dengan tambahan verifikasi sidik jari untuk memastikan hanya personel berwenang yang masuk. Di sektor logistik, RFID digunakan untuk melindungi gudang—kontainer atau dokumen penting hanya bisa dibuka setelah pemindaian kartu dan otorisasi dari sistem ERP.

Dengan menggabungkan RFID ke dalam kerangka keamanan akses, organisasi tidak hanya meningkatkan pertahanan terhadap ancaman eksternal tetapi juga mengoptimalkan operasional sehari-hari. Teknologi ini menjadi tulang punggung dalam lingkungan yang memerlukan keseimbangan antara keamanan ketat dan efisiensi, seperti fasilitas pemerintah, pusat data, atau rantai pasok global. Namun, kesuksesan implementasinya bergantung pada desain sistem yang matang, pelatihan pengguna, dan pemeliharaan berkala untuk memastikan bahwa kelemahan teknologi tidak dieksploitasi oleh pihak yang tidak bertanggung jawab.

2.7 Konsep Keamanan Akses Dengan Integrasi Teknologi Voice recognition (Voice Recognition)

Konsep keamanan akses dengan integrasi teknologi Voice Recognition adalah kerangka sistem penguncian yang menggabungkan mekanisme kontrol akses dengan teknologi pengenalan suara dan ucapan untuk melindungi sumber daya baik digital maupun fisik dari akses tidak sah. Sistem ini mengutamakan autentikasi berbasis karakteristik vokal yang unik dan sulit dipalsukan, termasuk pola bicara, intonasi, frekuensi suara, dan struktur vokal individual.

Sistem penguncian berbasis Voice Recognition umumnya digunakan untuk mengontrol akses fisik seperti pintu gedung, ruang server, atau area terbatas, serta akses logis ke perangkat elektronik, aplikasi mobile, dan database. Proses autentikasi dimulai ketika pengguna mengucapkan passphrase atau perintah suara yang telah ditentukan ke mikrofon sistem. Sistem kemudian menganalisis karakteristik unik suara tersebut menggunakan algoritma machine learning dan membandingkannya dengan voiceprint yang tersimpan dalam database.

Untuk meningkatkan keamanan, teknologi modern menggunakan sensor audio berkualitas tinggi dengan noise cancellation dan algoritma AI berbasis deep learning untuk mendeteksi upaya pemalsuan suara atau voice spoofing. Sistem canggih juga dapat membedakan antara suara asli dengan rekaman atau suara sintetis yang dihasilkan oleh teknologi voice cloning.

Kelebihan utama sistem biometrik Voice Recognition adalah tingkat keamanan yang tinggi karena voiceprint bersifat unik untuk setiap individu dan mencakup karakteristik fisik yang sulit diduplikasi seperti bentuk pita suara, rongga mulut, dan saluran pernapasan. Di sisi pengguna, sistem ini menawarkan kenyamanan luar biasa karena tidak memerlukan kontak fisik, tidak perlu mengingat password kompleks, atau membawa kartu akses fisik. Pengguna cukup berbicara secara natural untuk mendapatkan akses.

Dalam implementasi Zero Trust, setiap akses dapat divalidasi ulang secara real-time dengan continuous authentication, bahkan untuk pengguna yang sudah terverifikasi sebelumnya. Sistem dapat memantau pola bicara selama sesi aktif untuk memastikan konsistensi identitas pengguna.

Integrasi Voice Recognition dalam sistem penguncian akses sering dikombinasikan dengan metode autentikasi lain seperti PIN, kartu RFID, atau biometrik visual untuk membentuk sistem Multi-Factor Authentication (MFA). Misalnya, di fasilitas penelitian sensitif, pegawai mungkin perlu mengucapkan passphrase khusus dan memindai kartu akses untuk mengakses laboratorium. Sistem juga dapat mengimplementasikan dynamic passphrase yang berubah secara berkala untuk meningkatkan keamanan.

Tantangan implementasi meliputi kebutuhan akan mikrofon berkualitas tinggi dengan noise reduction, pemeliharaan database voiceprint yang aman dan terenkripsi, serta antisipasi terhadap kondisi yang dapat mempengaruhi kualitas pengenalan suara seperti sakit tenggorokan, perubahan suara karena usia, lingkungan bising, atau gangguan emosional. Sistem harus mampu beradaptasi dengan variasi natural dalam suara pengguna sambil tetap menolak upaya imitasi.

Dalam manajemen akses terpusat, teknologi Voice Recognition mendukung pemantauan dan kontrol yang lebih efektif. Administrator dapat dengan mudah mengelola hak akses berbasis voice profile, melacak aktivitas pengguna dengan timestamp audio, dan menghasilkan laporan audit yang detail termasuk analisis pola penggunaan suara. Sistem dapat pula mengintegrasikan natural language processing untuk memahami perintah suara yang kompleks dan kontekstual.

Contoh penerapannya dapat dilihat di bank, dimana karyawan menggunakan voice command untuk mengakses brankas digital sekaligus mencatat waktu akses dan transkrip audio untuk keperluan audit dan compliance. Dalam call center, teknologi ini memungkinkan verifikasi identitas pelanggan secara real-time selama percakapan telepon.

Keberhasilan implementasi sistem penguncian Voice Recognition bergantung pada beberapa faktor kunci:

1) Kualitas perangkat keras (mikrofon array dan processor audio) serta perangkat lunak (algoritma machine learning dan neural networks).
2) Prosedur enrollment voiceprint yang komprehensif dengan multiple sample recordings dalam berbagai kondisi.
3) Pelatihan pengguna tentang teknik bicara yang optimal dan sosialisasi kebijakan keamanan suara.

4) Pemeliharaan berkala sistem dengan update model *AI* dan *re-training* algoritma pengenalan.
5) Integrasi dengan sistem penguncian *existing* dan *backup procedures* untuk situasi darurat atau kegagalan sistem.
6) Penanganan *privacy* dan *compliance* terhadap regulasi perlindungan data biometrik dan *recording audio*.
7) *Disaster recovery planning* untuk *backup* akses ketika sistem Voice Recognition mengalami gangguan.

Dengan menggabungkan teknologi Voice Recognition ke dalam kerangka keamanan akses, organisasi dapat menciptakan sistem perlindungan yang lebih kuat sekaligus meningkatkan efisiensi operasional dan user experience. Pendekatan ini sangat cocok untuk lingkungan yang membutuhkan tingkat keamanan tinggi seperti fasilitas militer, pusat data, atau laboratorium penelitian, dimana verifikasi identitas yang akurat, contactless, dan dapat diandalkan menjadi prioritas utama, terutama dalam era post-pandemic yang mengutamakan teknologi hands-free.

2.8 Sistem Penguncian 2 Langkah

Sistem Penguncian 2 Langkah (Two-Factor Authentication/2FA) adalah metode keamanan yang menggunakan dua bentuk verifikasi berbeda untuk memastikan identitas pengguna sebelum memberikan akses. Sistem ini dirancang untuk meningkatkan keamanan dengan menambahkan lapisan perlindungan tambahan, sehingga meminimalkan risiko akses tidak sah meskipun salah satu faktor berhasil dibobol.

2.8.1 Cara Kerja Sistem 2 Langkah

1. Proses keamanan dimulai dengan autentikasi awal, di mana pengguna memasukkan faktor pertama, biasanya berupa kata sandi atau PIN yang mereka ketahui. Sistem kemudian memverifikasi validitas informasi ini dengan membandingkannya dengan data yang tersimpan. Jika faktor pertama cocok, sistem melanjutkan ke tahap berikutnya. Namun, untuk meningkatkan keamanan, sistem meminta verifikasi sekunder. Pada tahap ini, pengguna diminta untuk memberikan faktor kedua, yang bisa berupa kode unik yang

dikirim ke ponsel mereka, sidik jari, atau bentuk identifikasi lain yang mereka miliki. Sistem melakukan verifikasi tambahan untuk memastikan bahwa faktor kedua ini juga valid. Hanya jika kedua faktor terverifikasi, akses akan diberikan.

2. Setelah pengguna berhasil melewati dua tahap verifikasi yang berbeda, sistem akan melanjutkan ke tahap akhir, yaitu pemberian akses. Tahap ini sangat penting untuk memastikan bahwa hanya pengguna yang sah yang dapat mengakses akun atau sistem yang dilindungi.

   Sesuai dengan prinsip dasar dari sistem penguncian 2 langkah (2FA):

   - Hanya jika pengguna berhasil melewati kedua langkah autentikasi, sistem akan memberikan akses ke akun atau sistem yang dilindungi.
   - Yang berarti bahwa sistem telah memverifikasi identitas pengguna dengan dua cara yang berbeda, yang secara signifikan mengurangi risiko akses yang tidak sah

   Inti dari keamanan 2 langkah terletak pada perlindungan tambahan yang diberikan. Bahkan jika seorang penyerang berhasil memperoleh kata sandi pengguna, mereka tetap tidak dapat mengakses akun tanpa faktor kedua, seperti kode SMS atau sidik jari.

2.8.2 Implementasi dalam Kehidupan Sehari-hari

Sistem penguncian 2 langkah telah menjadi standar dalam berbagai aspek kehidupan digital dan fisik kita. Tujuannya adalah untuk memberikan lapisan perlindungan tambahan dengan mewajibkan dua bentuk identifikasi yang berbeda. Berikut adalah beberapa contoh implementasinya:

1. Layanan Perbankan
   - Password + OTP via SMS/email

     Ini adalah implementasi yang sangat umum dalam perbankan online. Setelah memasukkan kata sandi, pengguna akan menerima kode OTP (One-Time Password) melalui SMS atau email. Kode ini harus dimasukkan untuk menyelesaikan proses login atau transaksi.
   - Kartu ATM + PIN

Saat menggunakan ATM, pengguna harus memasukkan kartu ATM (sesuatu yang dimiliki) dan PIN (sesuatu yang diketahui) adalah contoh 2FA dalam dunia nyata.

2. Sistem Penguncian Fisik
   - Kartu Akses + Sidik Jari

     Di banyak gedung perkantoran atau fasilitas yang aman, karyawan harus menggunakan kartu akses (sesuatu yang dimiliki) dan memindai sidik jari (sesuatu yang merupakan bagian dari diri mereka) untuk mendapatkan akses.
   - Badge ID + PIN

     Beberapa sistem Penguncian fisik mengharuskan karyawan untuk menggunakan badge ID (sesuatu yang dimiliki) dan memasukkan PIN (sesuatu yang diketahui) untuk mengakses area tertentu.
3. Layanan Online
   - Password + Authenticator App

     Banyak layanan online kini menawarkan opsi keamanan 2 langkah dengan menggunakan aplikasi autentikator. Setelah memasukkan kata sandi, pengguna akan diminta untuk membuka aplikasi autentikator yang terpasang di ponsel mereka.
   - Email + Kode Verifikasi

     Metode keamanan lain yang sering digunakan adalah verifikasi melalui email. Setelah pengguna memasukkan kata sandi, sistem akan mengirimkan kode verifikasi unik ke alamat email yang terdaftar. Pengguna kemudian harus membuka email tersebut dan memasukkan kode yang diterima untuk menyelesaikan proses login.

2.8.3 Keunggulan Sistem

Dalam menghadapi ancaman keamanan digital yang semakin kompleks, sistem penguncian 2 langkah (2FA) menawarkan sejumlah keunggulan yang signifikan. Keunggulan-keunggulan ini menjadikan 2FA sebagai lapisan perlindungan yang penting dalam berbagai aplikasi dan layanan. Berikut adalah penjelasan lebih lanjut:

1. Keamanan Berlapis
    - Proteksi Ganda Terhadap Akses Tidak Sah

      Sistem autentikasi dua faktor (2FA) menyediakan lapisan perlindungan tambahan dengan mengharuskan pengguna memverifikasi identitas mereka melalui dua bentuk identifikasi yang berbeda dan independen. Konsekuensinya, meskipun pihak tidak bertanggung jawab berhasil mengompromikan satu faktor (misalnya memperoleh kata sandi), mereka tetap tidak dapat mengakses sistem tanpa memiliki faktor kedua yang diperlukan untuk validasi lengkap.
    - Mengurangi Resiko Pembobolan

      Dengan mengimplementasikan proteksi berlapis, 2FA secara substansial mengurangi kemungkinan terjadinya intrusi tidak sah ke dalam akun atau sistem. Pendekatan ini terbukti sangat efektif dalam menangkal berbagai jenis serangan siber, termasuk phishing, pencurian kredensial, serangan brute force, dan metode peretasan lainnya yang umumnya menargetkan sistem dengan autentikasi tunggal.
2. Fleksibilitas
    - Variasi Opsi Faktor Kedua

      Pengguna dapat memilih dari beragam alternatif faktor kedua yang paling sesuai dengan preferensi pribadi dan kebutuhan spesifik mereka. Fleksibilitas ini meningkatkan kenyamanan penggunaan sekaligus mempertahankan tingkat keamanan yang tinggi. Opsi yang tersedia dapat mencakup aplikasi autentikator, token fisik, biometrik, atau notifikasi perangkat.
    - Kostumisasi Sesuai Kebutuhan

      Sistem 2FA dapat dikonfigurasi dengan berbagai konfigurasi yang disesuaikan dengan karakteristik khusus aplikasi atau layanan yang dilindungi. Beberapa implementasi mengoptimalkan penggunaan kode sekali pakai (OTP) melalui pesan teks, sementara sistem lain memanfaatkan aplikasi autentikator khusus, verifikasi biometrik (seperti sidik jari atau pengenalan wajah), atau perangkat keras keamanan seperti YubiKey untuk memaksimalkan keamanan.

3. Kemudahan Manajemen
    - Rekan Jejak Audit Konprehensif

      Implementasi 2FA secara otomatis menciptakan dokumentasi terperinci yang merekam setiap aktivitas akses dan tindakan pengguna dalam sistem. Catatan kronologis ini sangat berharga untuk keperluan audit keamanan, investigasi insiden, dan untuk mengidentifikasi pola aktivitas yang mencurigakan atau anomali yang mungkin mengindikasikan upaya pelanggaran keamanan.
    - Pemantauan Akses Terpusat

      Infrastruktur 2FA modern dilengkapi dengan kemampuan monitoring terpusat yang memungkinkan administrator keamanan untuk mengawasi aktivitas autentikasi secara real-time, menganalisis pola penggunaan, dan dengan cepat mengidentifikasi percobaan akses yang tidak biasa atau mencurigakan. Fitur ini mempercepat respons terhadap potensi insiden keamanan dan memungkinkan penerapan tindakan preventif sebelum terjadi pelanggaran yang serius.

2.8.4 Tantangan dan Solusi

Meskipun sistem penguncian 2 langkah (2FA) menawarkan banyak keunggulan, implementasinya tidak selalu mudah. Terdapat beberapa tantangan yang perlu diatasi untuk memastikan keberhasilan penerapan 2FA. Berikut adalah penjelasan lebih lanjut:

1. Tantangan
    - Biaya Implementasi

      Penerapan sistem autentikasi dua faktor sering membutuhkan alokasi sumber daya finansial yang signifikan untuk pengadaan infrastruktur pendukung, termasuk perangkat keras khusus, lisensi perangkat lunak, dan program pelatihan komprehensif bagi staf teknis dan pengguna akhir. Investasi awal ini dapat menjadi pertimbangan krusial, terutama bagi organisasi dengan keterbatasan anggaran keamanan.
    - Kompleksitas Sistem

Integrasi sistem 2FA dengan infrastruktur teknologi yang sudah ada berpotensi menimbulkan tantangan teknis yang signifikan. Proses ini sering memerlukan modifikasi arsitektur sistem, penyesuaian protokol keamanan, dan pengembangan antarmuka penghubung yang dapat mengakomodasi berbagai platform dan lingkungan operasional tanpa mengganggu fungsionalitas sistem yang telah berjalan.

- Resistensi Pengguna

  Penerapan lapisan keamanan tambahan seringkali menghadapi hambatan psikologis dari pengguna yang memprioritaskan kenyamanan dan efisiensi dalam interaksi digital mereka. Banyak pengguna menganggap prosedur autentikasi tambahan sebagai beban operasional yang menghambat produktivitas, sehingga menimbulkan keengganan untuk mengadopsi teknologi 2FA meskipun manfaat keamanannya telah dibuktikan.

2. Solusi Strategis

   - Pilihan Teknologi Terjangkau

     Kemajuan dalam industri keamanan siber telah menghasilkan beragam solusi 2FA dengan berbagai tingkat investasi. Organisasi dapat memilih opsi yang sesuai dengan anggaran mereka, seperti aplikasi autentikator berbasis perangkat mobile yang tidak memerlukan perangkat khusus, sistem pengiriman kode verifikasi melalui SMS, atau solusi berbasis email yang dapat diimplementasikan dengan biaya minimal namun tetap memberikan peningkatan keamanan yang substansial.

   - Antarmuka *User-Friendly*

     Pengembangan antarmuka yang intuitif dan sederhana dapat secara signifikan mengurangi kompleksitas operasional yang dirasakan pengguna. Desain yang berfokus pada pengalaman pengguna memungkinkan proses autentikasi yang lancar dengan langkah-langkah yang jelas, mengurangi gesekan dalam proses login, dan meminimalkan hambatan kognitif yang dapat menimbulkan frustrasi dan penolakan terhadap sistem.

   - Edukasi Pengguna

     Program edukasi komprehensif yang menjelaskan manfaat keamanan 2FA, risiko keamanan digital kontemporer, dan potensi konsekuensi dari

pelanggaran keamanan dapat secara efektif mengatasi resistensi pengguna. Pelatihan praktis yang dilengkapi dengan demonstrasi langsung dan materi pendukung membantu pengguna memahami nilai perlindungan tambahan yang ditawarkan 2FA, sehingga meningkatkan tingkat adopsi dan kepatuhan terhadap protokol keamanan.

Sistem autentikasi dua faktor merepresentasikan keseimbangan optimal antara perlindungan keamanan tingkat tinggi dan pengalaman pengguna yang praktis dalam ekosistem digital kontemporer. Dengan mengkombinasikan dua mekanisme verifikasi identitas yang berbeda, sistem ini menawarkan proteksi yang jauh lebih kokoh dibandingkan pendekatan autentikasi tradisional. Perkembangan berkelanjutan dalam teknologi biometrik, aplikasi mobile, dan metodologi autentikasi kontekstual terus meningkatkan efektivitas, aksesibilitas, dan keamanan platform 2FA, menegaskan posisinya sebagai komponen fundamental dalam strategi keamanan komprehensif untuk melindungi aset digital maupun fisik di era transformasi digital yang semakin kompleks.

BAB 3
METODOLOGI PENELITIAN

3.1 Tempat Penelitian

Lokasi penelitian ini adalah lingkungan Rumah Jl. Mesjid Lk VI P. Rambai. Untuk memenuhi tugas akhir dengan mengobservasi lingkungan sekitar.

3.2 Alat dan Bahan Penelitian

Berikut merupakan alat dan bahan yang dibutuhkan dalam melakukan penelitian yang diuraikan dalam tabel 3.1 dan tabel 3.2.

Tabel 3. 1 Bahan Penelitian

No	Komponen/ Bahan	Spesifikasi	Fungsi
1	Arduino Uno R3	- Mikrokontroler: ATmega328P - Tegangan operasi: 5V - Digital I/O Pins: 14 (6 di antaranya dapat digunakan sebagai output PWM) - Input analog: 6 channel - Memory: 32 KB Flash (0.5 KB digunakan untuk bootloader) - Clock speed: 16 MHz	Memiliki kapasitas memori dan jumlah pin yang memadai untuk sistem yang kompleks ini
2	RFID-RC522	- Frekuensi kerja: 13.56 MHz - Jarak pembacaan: 0-5 cm - Protokol: SPI - Tegangan operasi: 3.3V - Chip: MFRC522	Membaca kartu RFID standar yang umum digunakan, dengan kemampuan kriptografi untuk keamanan tambahan
3	Voice Recognition V3 Module (Elechouse)	- Interface: UART - Tegangan operasi: 4.4V - 5.5V - Arus operasi: < 40 mA (standby), < 150 mA (recognition) - Jumlah voice commands: Hingga 80 perintah suara - Group commands: 7 grup, masing-masing 5 perintah - Waktu respons: < 300ms - Jarak deteksi: 0.5 - 1.5 meter	Dilengkapi dengan algoritma pengenalan suara yang canggih dan dapat mengenali perintah suara yang telah dilatih sebelumnya. Modul ini memiliki fitur anti-noise dan dapat bekerja dalam lingkungan dengan tingkat kebisingan sedang.

No	Komponen/ Bahan	Spesifikasi	Fungsi
		- Mikrofon: On-board high-sensitivity microphone - Training mode: Voice recording dan training terintegrasi - Memory: Non-volatile storage untuk voice templates	
4	Selenoid Electric Door Lock	- Tegangan operasi: 12V DC - Arus: 1A (saat aktif) - Tipe: Normally Closed (NC) - terkunci saat tidak dialiri listrik - Dimensi: 90mm × 25mm × 28mm - Daya tahan: >500,000 siklus operasi - Waktu respons: < 0.5 detik	Dirancang untuk dipasang pada pintu sungguhan dengan kekuatan yang cukup untuk menahan dorongan normal.
5	Relay Module 1-Channel	- Tegangan kontrol: 5V DC - Tegangan switching: hingga 250V AC atau 30V DC - Arus maksimum: 10A - Dengan optocoupler untuk isolasi - LED indikator status	Relay diperlukan karena solenoid membutuhkan arus yang lebih besar daripada yang dapat disediakan langsung oleh Arduino.
6	LCD I2C 16x2	- Jenis LCD: Alphanumeric 16×2 (16 karakter, 2 baris) - Interface: I2C - Tegangan operasi: 5V - Backlight: Biru dengan teks putih	LCD akan menampilkan instruksi pengguna dan status sistem
7	LED Indikator dan Buzzer	- LED Merah: Untuk indikasi akses ditolak - LED Hijau: Untuk indikasi akses diterima - Buzzer Aktif 5V: Untuk umpan balik audio - Resistor 220 ohm: Untuk LED	Indikator visual dan audio membantu pengguna memahami respons sistem tanpa harus membaca LCD
8	Adaptor 12V 2A	- Input: 100-240V AC - Output: 12V DC, 2A - Connector: 5.5mm × 2.1mm barrel jack	Diperlukan untuk mengakomodasi kebutuhan solenoid lock

No	Komponen/ Bahan	Spesifikasi	Fungsi
9	Dioda 1N4007	- Arus Maksimum (Forward Current): 1 A - Tegangan Balik Maksimum (Peak Inverse Voltage/PIV): 1000 V - Tegangan Maju (Forward Voltage Drop): sekitar 0.7V - 1.1V - Jenis: Dioda penyearah silikon - Ukuran Fisik: DO-41 - Aplikasi: Power supply, inverter, converter, freewheeling diode, dan aplikasi penyearah lainnya.	sebagai pelindung terhadap tegangan balik (back EMF) yang dihasilkan oleh solenoid saat relay memutus arus. Ketika arus dihentikan secara tiba-tiba, solenoid sebagai beban induktif akan melepaskan energi dalam bentuk lonjakan tegangan yang dapat mengganggu atau merusak komponen lain seperti LCD atau mikrokontroler. Dengan dipasang secara paralel dan berlawanan arah terhadap suplai solenoid, dioda ini memberikan jalur aman bagi arus induktif untuk mengalir kembali ke kumparan, sehingga mencegah gangguan tegangan dan menjaga kestabilan sistem.
10	Resistor 220 Ohm	- 220 ohm (Ω) - Umumnya 1/4 Watt (0.25W), tetapi bisa juga ditemukan dalam nilai daya yang lebih tinggi seperti 1/2 Watt (0.5W) atau lebih. - Biasanya ±5%, yang berarti nilai resistansi sebenarnya bisa sedikit berbeda dari 220 ohm (misalnya, antara 209 ohm dan 231 ohm). - Tersedia dalam berbagai bentuk, seperti resistor film karbon (carbon film) atau resistor film logam (metal film).	untuk membatasi arus listrik yang mengalir ke LED agar tidak melebihi batas toleransi yang dapat menyebabkan LED rusak atau terbakar. LED adalah komponen yang sangat sensitif terhadap arus, dan tanpa resistor pembatas, arus yang terlalu besar dari sumber tegangan dapat langsung melewati LED sehingga memperpendek umur atau bahkan langsung merusaknya. Dengan menghitung nilai resistor yang sesuai berdasarkan tegangan sumber dan tegangan kerja LED, resistor memastikan LED menyala dengan terang yang stabil dan aman dalam jangka waktu panjang.
11	LM2596 DC-DC	- Tegangan Input: 3V - 40V DC (minimal 1.5V lebih tinggi dari tegangan output) - Tegangan Output: 1.25V - 35V DC yang dapat disesuaikan (dengan potensiometer)	Untuk menurunkan tegangan dc dari adaptor 12 volt menjadi 5 volt untuk ke beban dan memberi daya pada arduino

No	Komponen/ Bahan	Spesifikasi	Fungsi
		- Arus Output: 3A (maksimal, disarankan penggunaan di bawah 2A) - Efisiensi: Hingga 92% - Frekuensi Switching: 150kHz - Ukuran: Umumnya sekitar 43mm x 21mm x 14mm - Ripple Output: 200mV	
12	Jack Male	- Plug Type: 2.1 x 5.5mm Female - -Material: Plastic, Electric Parts	Dipasang pada adaptor sebagai dc konektor yang akan langsung turun menuju beban
11	Push button	- Untuk berfungsi sebagai saklar/tombol	Dipasang pada pin digital untuk membuka pintu dari dalam ruang

Dalam menghubungkan setiap komponen dari bahan yang akan digunakan tetap harus menggunakan alat, berikut adalah alat yang akan digunakan dalam penelitian tertera pada tabel 3.2.

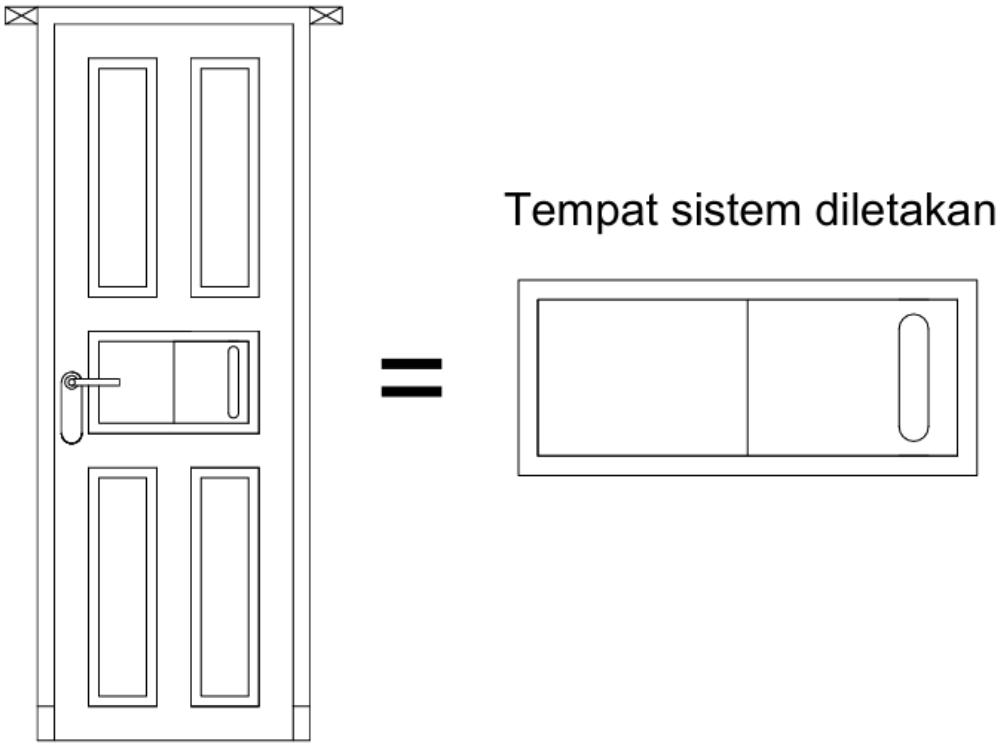
Tabel 3. 2 Alat Penelitian

No	Nama Alat	Spesifikasi	Fungsi
1	Obeng Set	- Ukuran: Philips + slot	Pemasangan komponen fisik
2	Multimeter Digital	- Pengukuran: Tegangan, arus, resistansi	Memeriksa koneksi dan tegangan
3	Soldering Iron	- Daya: 40W–60W	Penyolderan kabel/PCB
4	Tang Potong	- Ukuran: 6 inci	Memotong kabel
5	Kabel USB	- Panjang: 1m	Upload kode ke mikrokontroler
6	Komputer/Laptop	- OS: Windows	Pemrograman dan konfigurasi sistem
7	Isolasi Listrik	- Lebar: 1.8 cm	Mengamankan sambungan kabel

Alat yang digunakan dalam tabel akan membantu pemasangan setiap komponen dengan lancar dan cepat.

3.3 Desain Penelitian

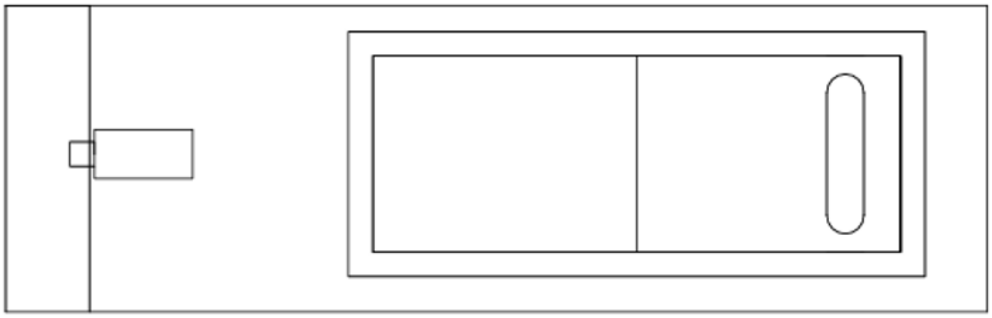
Dalam membuat alat sistem penguncian, penulis perlu mendesain bentuk alat sistem yang akan dibuat. Berikut adalah desain yang dibuatkan oleh penulis sendiri.

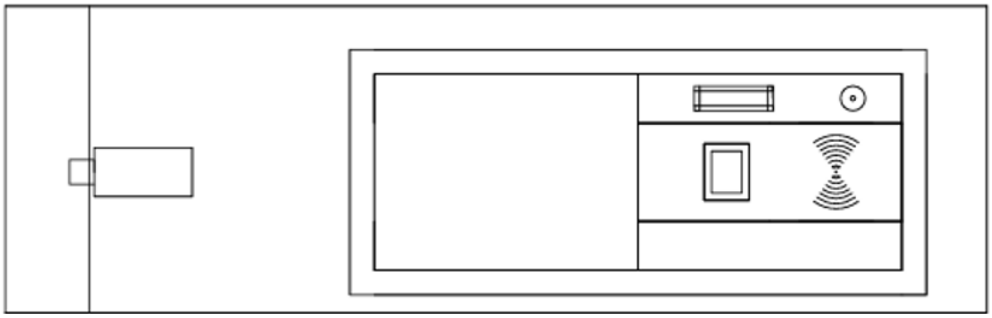


Gambar 3. 1 Posisi Peletakan Alat

Tempat sistem diletakkan adalah bentuk fisik atau tampak luar yang di dalamnya terdapat sistem operasi dari sistem penguncian multi-faktor yang penulis buat.

Bagian autentikasi sistem ditutup sebelum digunakan





Bagian autentikasi sistem dibuka untuk digunakan

Gambar 3. 2 Bentuk Alat

Alat dibuat dengan pelindung yang akan melindungi Voice Recognition, RFID, Buzzer, dan komponen lain dari sentuhan fisik yang tidak diperlukan.

3.4 Desain Software

Untuk mewujudkan sistem autentikasi dua langkah berbasis RFID dan pengenalan suara, diperlukan rancangan perangkat lunak yang mampu mengatur logika kontrol secara efisien dan responsif. Bagian ini menyajikan implementasi kode program yang mengintegrasikan berbagai perangkat seperti RFID reader, modul voice recognition, LCD I2C, relay, dan tombol fisik, guna mengelola alur autentikasi dan respon sistem secara berlapis.

```
#include <SPI.h>
#include <MFRC522.h>
#include <SoftwareSerial.h>
#include "VoiceRecognitionV3.h"
#include <Wire.h>
#include <LiquidCrystal_I2C.h>

#define SS_PIN 10
#define RST_PIN 9
MFRC522 mfrc522(SS_PIN, RST_PIN);

#define RELAY_PIN       6
#define LED_HIJAU2      5
#define LED_MERAH       7
#define BUZZER_PIN      8
#define TOMBOL_BUKA_PIN 4

#define CMD_NYALA_3DTK  0
#define CMD_MATI        1
#define CMD_NYALA_5DTK  2

VR myVR(2, 3);
uint8_t records[] = {0, 1, 2};
uint8_t buf[64];

byte authorizedUID[4] = {0x8D, 0xEC, 0xC4, 0x23};  // Ganti dengan
UID milikmu
```

```
LiquidCrystal_I2C lcd(0x27, 16, 2);

int voiceCommand = -1;
bool waitingForVoice = false;
bool voiceCanceled = false;
bool voiceInitialized = false;

unsigned long voiceStartTime = 0;
unsigned long relayOnTime = 0;
unsigned long relayDuration = 0;
bool relayOn = false;

void setup() {
  SPI.begin();
  mfrc522.PCD_Init();

  pinMode(RELAY_PIN, OUTPUT);
  pinMode(LED_HIJAU2, OUTPUT);
  pinMode(LED_MERAH, OUTPUT);
  pinMode(BUZZER_PIN, OUTPUT);
  pinMode(TOMBOL_BUKA_PIN, INPUT_PULLUP);

  digitalWrite(RELAY_PIN, HIGH);
  digitalWrite(LED_HIJAU2, LOW);
  digitalWrite(LED_MERAH, LOW);
  digitalWrite(BUZZER_PIN, LOW);

  lcd.init();
  lcd.backlight();
  showLCD("SISTEM AKTIF", "Scan kartu anda");
}

void loop() {
  if (digitalRead(TOMBOL_BUKA_PIN) == LOW && !relayOn) {
    showLCD("TOMBOL DITEKAN", "BUKA PINTU");
    aktifkanRelay(3000);
```

```
  delay(500);

  if (waitingForVoice) {
    waitingForVoice = false;
    voiceCanceled = true;
    myVR.clear();           // Stop pengenalan suara
    resetSystem();          // Reset tampilan & logika
  }

  return;
}

if (relayOn) {
  unsigned long elapsed = millis() - relayOnTime;
  int remaining = (relayDuration / 1000) - (elapsed / 1000);
  if (elapsed >= relayDuration) {
    matikanRelay();
  } else {
    lcd.setCursor(0, 0);
    lcd.print("RELAY AKTIF     ");
    lcd.setCursor(0, 1);
    lcd.print("Sisa: ");
    lcd.print(remaining);
    lcd.print(" detik   ");
  }
}

if (waitingForVoice) {
  if (!voiceInitialized) {
    myVR.begin(9600);
    if (myVR.load(records, 3) < 0) {
      showLCD("GAGAL", "Load voice");
      delay(1500);
      resetSystem();
      return;
    }
```

```
      voiceInitialized = true;
    }

    unsigned long elapsed = millis() - voiceStartTime;
    int remaining = 10 - (elapsed / 1000);
    if (elapsed >= 10000) {
      showLCD("TIDAK ADA SUARA", "RESET...");
      for (int i = 0; i < 5; i++) {
        digitalWrite(LED_MERAH, HIGH);
        tone(BUZZER_PIN, 1000, 200);
        delay(1000);
        digitalWrite(LED_MERAH, LOW);
        delay(200);
      }
      waitingForVoice = false;
      voiceInitialized = false;
      resetSystem();
      return;
    }

    lcd.setCursor(0, 0);
    lcd.print("MENUNGGU SUARA ");
    lcd.setCursor(0, 1);
    lcd.print("Sisa: ");
    lcd.print(remaining);
    lcd.print(" detik  ");

    int ret = myVR.recognize(buf, 50);
    if (ret > 0) {
      voiceCommand = buf[1];
      tone(BUZZER_PIN, 1500, 100);

      if (voiceCommand == CMD_NYALA_3DTK || voiceCommand ==
CMD_NYALA_5DTK) {
        int duration = (voiceCommand == CMD_NYALA_3DTK) ? 3 : 5;
        showLCD("HALO FARIZ", String(duration) + " Detik");
```

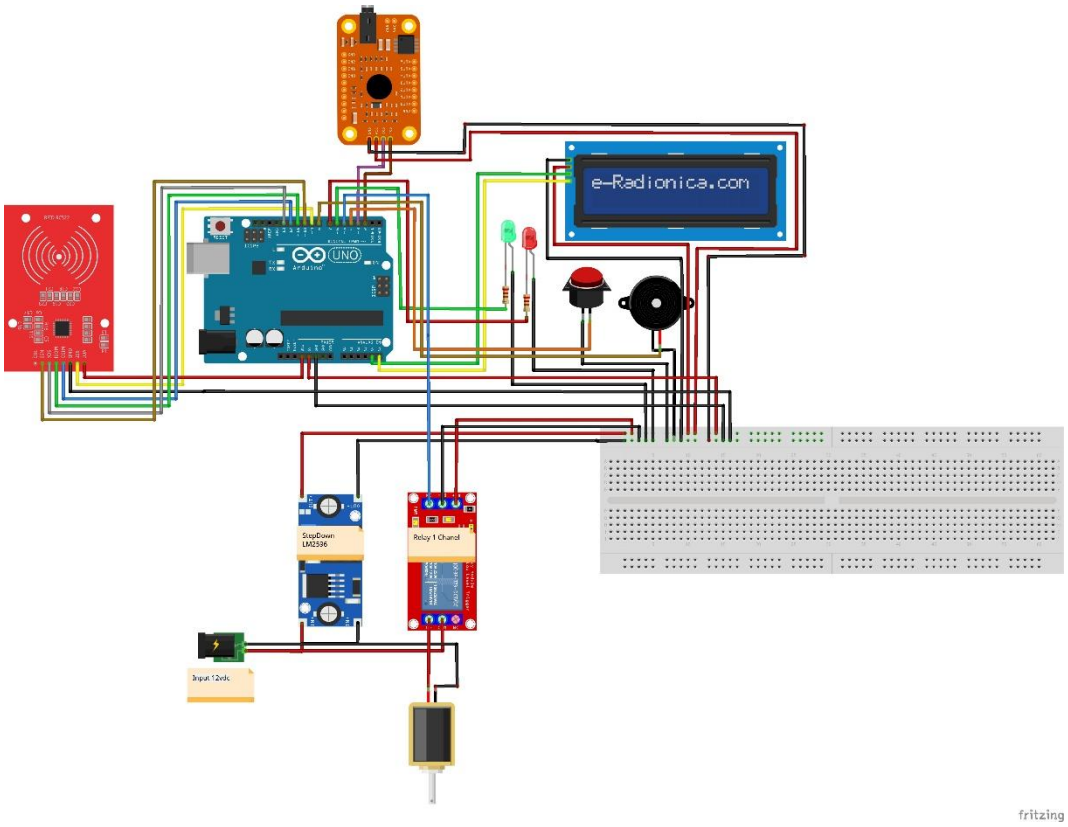
```
        delay(1000);
        aktifkanRelay(duration * 1000);
      } else if (voiceCommand == CMD_MATI) {
        matikanRelay();
      } else {
        showLCD("SUARA TDK DIKENAL", "RESET...");
        for (int i = 0; i < 5; i++) {
          digitalWrite(LED_MERAH, HIGH);
          tone(BUZZER_PIN, 1000, 200);
          delay(1000);
          digitalWrite(LED_MERAH, LOW);
          delay(200);
        }
        resetSystem();
      }

      waitingForVoice = false;
      voiceInitialized = false;
    }
    return;
  }

  if (mfrc522.PICC_IsNewCardPresent() &&
mfrc522.PICC_ReadCardSerial()) {
    if (isAuthorizedCard(mfrc522.uid.uidByte)) {
      showLCD("KARTU DITERIMA", "MENUNGGU SUARA");
      digitalWrite(LED_MERAH, LOW);
      waitingForVoice = true;
      voiceCanceled = false;
      voiceInitialized = false;
      voiceStartTime = millis();
    } else {
      showLCD("KARTU DITOLAK", "COBA LAGI");
      digitalWrite(LED_MERAH, HIGH);
      tone(BUZZER_PIN, 600, 400);
      delay(1500);
```

```
      resetSystem();
    }
    mfrc522.PICC_HaltA();
  }
}

bool isAuthorizedCard(byte *uid) {
  for (byte i = 0; i < 4; i++) {
    if (uid[i] != authorizedUID[i]) return false;
  }
  return true;
}

void showLCD(String baris1, String baris2) {
  lcd.clear();
  lcd.setCursor(0, 0);
  lcd.print(baris1);
  lcd.setCursor(0, 1);
  lcd.print(baris2);
}

void resetSystem() {
  digitalWrite(LED_HIJAU2, LOW);
  digitalWrite(LED_MERAH, LOW);
  showLCD("SISTEM AKTIF", "Scan kartu anda");
}

void aktifkanRelay(unsigned long durasi) {
  digitalWrite(RELAY_PIN, LOW);
  digitalWrite(LED_HIJAU2, HIGH);
  digitalWrite(LED_MERAH, LOW);
  relayOn = true;
  relayDuration = durasi;
  relayOnTime = millis();
}
```

```
void matikanRelay() {
  digitalWrite(RELAY_PIN, HIGH);
  digitalWrite(LED_HIJAU2, LOW);
  relayOn = false;
  showLCD("RELAY OFF", "Selesai");
  delay(1500);
  showLCD("SISTEM AKTIF", "Scan kartu anda");
}
```

Kode program di atas menunjukkan bagaimana mikrokontroler digunakan sebagai pusat kendali untuk mengelola autentikasi kartu RFID dan perintah suara secara berurutan, sekaligus mengatur keluaran berupa aktuator, indikator, dan tampilan LCD. Pendekatan ini memastikan sistem bekerja secara stabil, hemat energi, dan mampu merespons berbagai kondisi operasional maupun kesalahan pengguna dengan logika yang terstruktur.

3.5 Desain Rangkaian



Gambar 3. 3 Rangkaian Sistem

Gambar di atas menunjukkan rangkaian keseluruhan sistem yang menjadi acuan dalam pembuatan alat. Berikut adalah penjelasan alur kerja berdasarkan gambar tersebut:

Alur Kerja Sistem Kontrol:

A. Koneksi perangkat input

RFID reader (RC522) terhubung ke Arduino Uno melalui protokol SPI (*Serial Peripheral Interface*), menggunakan pin MOSI, MISO, SCK, SS, RST, dan GND.

Modul voice recognition V3 terhubung ke Arduino melalui komunikasi UART menggunakan pin TX dan RX (pin 2 dan 3). Mikrofon internal pada modul ini mendeteksi perintah suara dari jarak sekitar 0,5–1,5 meter. Modul tersebut mendukung komunikasi dua arah untuk pelatihan dan pengenalan perintah suara.

Push button (tombol darurat dari dalam ruangan) dihubungkan ke salah satu pin digital Arduino dan dikonfigurasi dengan resistor pull-up internal (INPUT_PULLUP) untuk membaca status logika ketika ditekan.

B. Koneksi perangkat output

Modul relay satu channel dikendalikan oleh Arduino melalui salah satu pin digital. Relay ini bertugas menghubungkan dan memutuskan suplai 12 volt ke solenoid doorlock ketika autentikasi valid berhasil.

LCD 16x2 dengan antarmuka I2C terhubung ke pin SDA dan SCL (A4 dan A5 pada Arduino Uno) untuk menampilkan status sistem, petunjuk akses, atau hasil validasi pengguna.

LED indikator dan buzzer masing-masing terhubung ke pin digital berbeda pada Arduino. LED hijau menyala saat akses diizinkan, sedangkan LED merah menyala saat akses ditolak. Buzzer akan berbunyi singkat sebagai notifikasi suara.

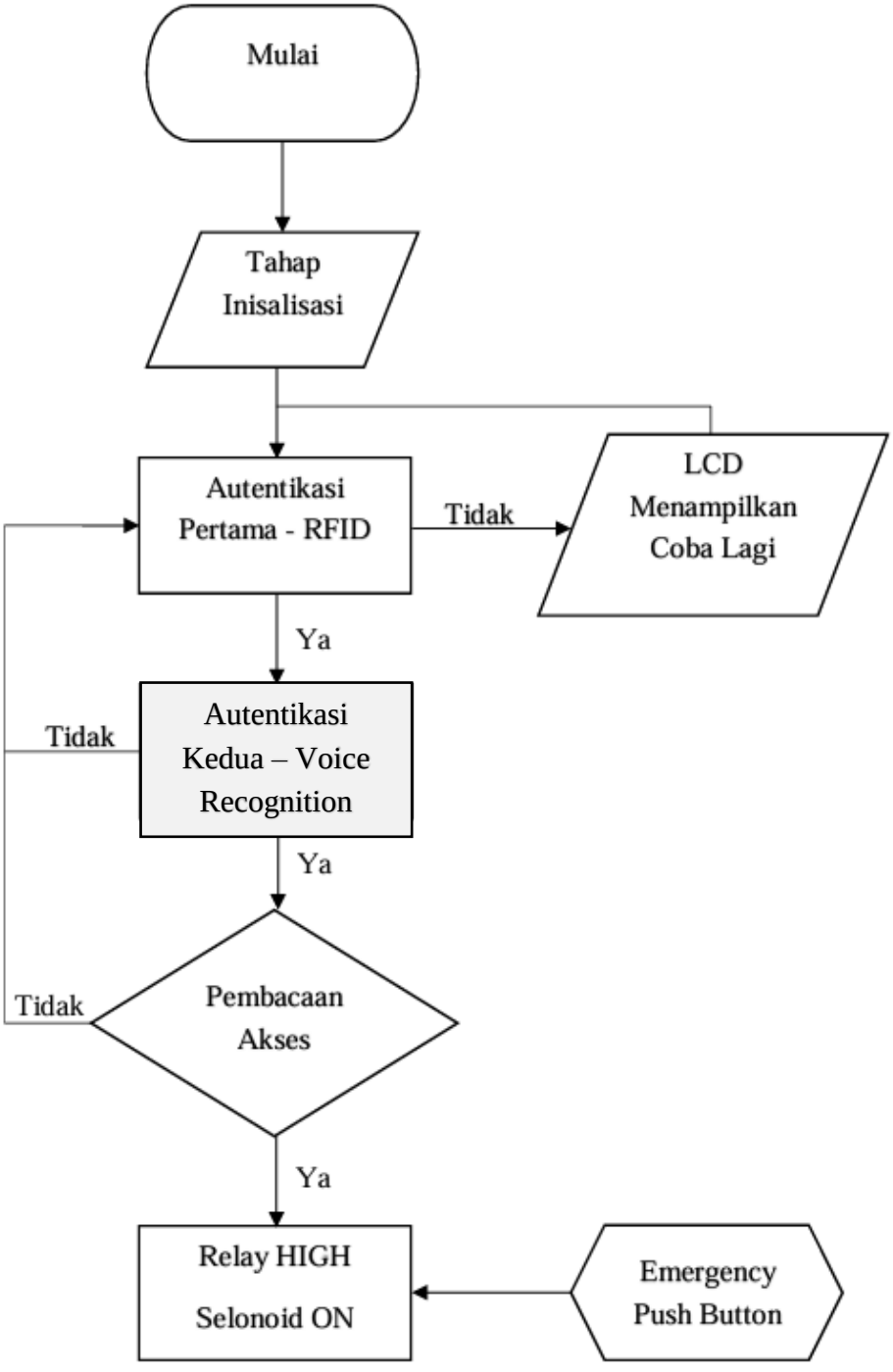
C. Power supply

Catu daya utama berasal dari adaptor 12 volt DC. Tegangan ini diturunkan oleh modul step-down LM2596 menjadi 5 volt DC untuk memberi daya pada Arduino Uno dan seluruh komponen lainnya seperti RFID, voice recognition, dan LCD. Penggunaan LM2596 dipilih karena efisiensinya yang tinggi dalam menurunkan tegangan tanpa menghasilkan panas berlebih, tidak seperti regulator linier seperti LM7805.

Sementara itu, solenoid tetap mendapatkan suplai 12 volt penuh dari adaptor melalui kendali relay, karena solenoid membutuhkan arus dan tegangan yang relatif besar agar dapat bekerja secara mekanis menarik dan melepaskan kunci pintu.

Dengan susunan ini, Arduino Uno berfungsi sebagai pusat kontrol sistem. Ketika kartu RFID valid dan perintah suara sesuai diterima secara berurutan, maka Arduino akan mengaktifkan relay sehingga solenoid terbuka. Seluruh proses disertai umpan balik melalui LCD, LED, dan buzzer. Sistem ini tidak dilengkapi baterai cadangan, sehingga bergantung sepenuhnya pada ketersediaan sumber listrik eksternal.

3.6 Flowchat



Gambar 3. 4 Flowchart

Flowchart sistem kontrol akses ini menggambarkan alur kerja yang dimulai dari tahap inisialisasi, di mana Arduino menyiapkan seluruh perangkat termasuk RFID Reader RC522 melalui protokol SPI, Voice Recognition V3 Module melalui komunikasi UART, serta konfigurasi pin-pin digital untuk relay, LED, buzzer, tombol darurat, dan LCD 16x2 dengan modul I2C. Setelah semua perangkat siap, LCD akan menampilkan pesan "SISTEM AKTIF - Scan kartu anda" sebagai tanda bahwa sistem masuk ke mode standby dan siap menerima input.

Tahap autentikasi pertama dimulai dengan memindai kartu RFID. Jika UID kartu cocok dengan UID yang telah diprogram (hardcoded) di dalam kode, maka sistem akan menampilkan pesan "KARTU DITERIMA - MENUNGGU SUARA", mematikan LED merah jika sebelumnya menyala, dan masuk ke tahap kedua. Jika kartu tidak valid, maka sistem menampilkan "KARTU DITOLAK - COBA LAGI", mengaktifkan LED merah, membunyikan buzzer, dan mengulang proses dari awal.

Setelah kartu valid, sistem masuk ke tahap pengenalan suara. Voice Recognition Module akan aktif selama 10 detik dan menunggu perintah suara yang telah dilatih sebelumnya. LCD akan menampilkan countdown waktu yang tersisa untuk input suara. Jika tidak ada suara valid yang dikenali dalam waktu tersebut, atau suara yang diterima tidak cocok dengan command yang telah diload (0, 1, atau 2), maka sistem akan menampilkan "SUARA TDK DIKENAL - ULANGI DARI RFID", LED merah menyala, buzzer berbunyi, dan sistem kembali ke tahap awal.

Jika perintah suara dikenali dan cocok, maka sistem mengeksekusi perintah tersebut. Jika perintah adalah "nyala 3 detik" atau "nyala 5 detik", relay akan aktif selama durasi tersebut dan membuka solenoid lock. LCD akan menampilkan nama pengguna dan durasi akses. Jika perintah suara adalah "mati", maka relay akan segera dimatikan. Setelah durasi habis, relay akan otomatis dimatikan dan LCD kembali menampilkan pesan awal untuk pengguna berikutnya.

Sistem juga memiliki fitur tombol darurat (emergency button) yang terhubung ke pin digital dengan konfigurasi INPUT_PULLUP. Jika tombol ditekan, dan tidak ada proses aktif lainnya, sistem akan langsung mengaktifkan relay selama 3 detik untuk membuka pintu, menampilkan pesan "TOMBOL DITEKAN - BUKA PINTU", dan kembali ke mode standby setelah selesai.

DAFTAR PUSTAKA

[1] P. R. C. Gopal, N. P. Rana, T. V. Krishna, and M. Ramkumar, "Impact of big data analytics on supply chain performance: an analysis of influencing factors," *Ann. Oper. Res.*, vol. 333, no. 2–3, 2024, doi: 10.1007/s10479-022-04749-6.

[2] Y. Liu *et al.*, "TransTM: A device-free method based on time-streaming multiscale transformer for human activity recognition," *Def. Technol.*, vol. 32, 2024, doi: 10.1016/j.dt.2023.02.021.

[3] F. Schindler, "The IEEE Microwave Theory and Technology Society and IEEE [MicroBusiness]," 2024. doi: 10.1109/MMM.2023.3321224.

[4] J. Nolan, K. Qian, and X. Zhang, "KeyStub: A Passive RFID-based Keypad Interface Using Resonant Stubs," *Proc. ACM Interactive, Mobile, Wearable Ubiquitous Technol.*, vol. 7, no. 4, 2024, doi: 10.1145/3631442.

[5] I. P. Sari, A. H. Hazidar, M. Basri, F. Ramadhani, and A. A. Manurung, "Penerapan Palang Pintu Otomatis Jarak Jauh Berbasis RFID di Perumahan," *Blend Sains J. Tek.*, vol. 2, no. 1, 2023, doi: 10.56211/blendsains.v2i1.246.

[6] M. Han *et al.*, "RF Sensing Security and Malicious Exploitation: A Comprehensive Survey," vol. 14, no. 8, pp. 1–51, 2025.

[7] R. Atmawijaya and U. Radiyah, "Perancangan Autentikasi Multi Faktor Dengan Pengenalan Wajah Dan Fido (Fast Identity Online)," *INTI Nusa Mandiri*, vol. 19, no. 1, pp. 46–53, 2024, doi: 10.33480/inti.v19i1.5263.

[8] A. H. Nugroho, A.-B. Bin Ladjamudin, and S. Bariroh, "Prototipe Pengontrol Kunci Pintu Berbasis Arduino Uno Menggunakan RFID Studi Pada Smks Kesehatan Utama Insani," *J. Tek. Inform. UNIS*, vol. 7, no. 2, 2020, doi: 10.33592/jutis.v7i2.390.

[9] D. Jollyta, D. Oktarina, and J. Johan, "Tinjauan Kasus Model Speech Recognition: Hidden Markov Model," *J. Edukasi dan Penelit. Inform.*, vol. 6, no. 2, 2020, doi: 10.26418/jp.v6i2.39231.

[10] P. K. Sattarapu, D. Wadera, N. P. Nguyen, J. Kaur, S. Kaur, and E. Mogaji, "Tomeito or Tomahto: Exploring consumer's accent and their engagement

with artificially intelligent interactive voice assistants," *J. Consum. Behav.*, vol. 23, no. 2, 2024, doi: 10.1002/cb.2195.

[11] R. Zhang *et al.*, "High-performance piezoresistive sensors based on transfer-free large-area PdSe2 films for human motion and health care monitoring," *InfoMat*, vol. 6, no. 1, 2024, doi: 10.1002/inf2.12484.

[12] A. Pearson, M. Griffith, B. Rakoska, C. Harrison, K. Schuitema, and E. Taşcıoğlu, "Breaking out of the box: increasing the representation of disability within archive science," *Arch. Sci.*, vol. 24, no. 1, 2024, doi: 10.1007/s10502-023-09429-3.

[13] F. B. Pokorny *et al.*, "VocDoc, what happened to my voice? Towards automatically capturing vocal fatigue in the wild," *Biomed. Signal Process. Control*, vol. 88, 2024, doi: 10.1016/j.bspc.2023.105595.

[14] X. Zhao *et al.*, "Validity, feasibility, and effectiveness of a voice-recognition based digital cognitive screener for dementia and mild cognitive impairment in community-dwelling older Chinese adults: A large-scale implementation study," *Alzheimer's Dement.*, vol. 20, no. 4, 2024, doi: 10.1002/alz.13668.

[15] F. Sigona and M. Grimaldi, "Validation of an ECAPA-TDNN system for Forensic Automatic Speaker Recognition under case work conditions," *Speech Commun.*, vol. 158, 2024, doi: 10.1016/j.specom.2024.103045.

[16] P. Gupta, H. A. Patil, and R. C. Guido, "Vulnerability issues in Automatic Speaker Verification (ASV) systems," *Eurasip J. Audio, Speech, Music Process.*, vol. 2024, no. 1, 2024, doi: 10.1186/s13636-024-00328-8.

[17] I. P. Ihsan, S. Buwarda, H. Novianty, and I. A. Putra, "Voice Recognition Untuk Otomatisasi Sistem Pengakses Pintu," *JSAI (Journal Sci. Appl. Informatics)*, vol. 4, no. 1, pp. 116–125, 2021, doi: 10.36085/jsai.v4i1.1318.

[18] M. Smith and S. Miller, "The ethical application of biometric facial recognition technology," *AI Soc.*, vol. 37, no. 1, 2022, doi: 10.1007/s00146-021-01199-9.

[19] F. Ramadhan and N. Komariah, "PURWARUPA SISTEM NOTIFIKASI KEAMANAN RUMAH MENGGUNAKAN RFID DAN SENSOR PIR BERBASIS NODE MCU," *J. Inform. dan Komputasi Media Bahasan, Anal. dan Apl.*, vol. 16, no. 02, 2022, doi: 10.56956/jiki.v16i02.114.

[20] K. Diantoro and F. Rohmatullahama, “Rancang Bangun Sistem Keamanan Akses Terbatas dengan Teknologi RFID pada PJB Muara Tawar,” *remik*, vol. 7, no. 1, 2023, doi: 10.33395/remik.v7i1.11932.

[21] Rimbawati, Cholish, E. Saputro, and P. Harahap, “Perancangan Sistem Kontrol Penstabil Tegangan Menggunakan PLC M221 Pada PLTMH Bintang Asih,” *J. Tek. Elektro*, vol. 3, no. 2, pp. 62–70, 2021, [Online]. Available: https://jurnal.umsu.ac.id/index.php/RELE/article/view/v3i2.6482

[22] P. Harahap, Rimbawati, and C. A. Siregar, “Perancangan Plts on-Grid Berbasis Micro Inverter 500 Watt,” *RELE (Rekayasa Elektr. dan Energi) J. Tek. Elektro*, vol. 6, no. 2, pp. 120–127, 2024, doi: 10.30596/rele.v6i2.17688.

[23] B. Yalcinoz-Ucan and H. Eslen-Ziya, “Online disclosure, a mechanism for seeking informal justice?,” *Crime, Media, Cult.*, vol. 20, no. 1, 2024, doi: 10.1177/17416590231153077.

[24] A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen, and Y. Koucheryavy, “Multi-factor authentication: A survey,” *Cryptography*, vol. 2, no. 1, 2018, doi: 10.3390/cryptography2010001.

[25] D. Putri and A. Dini, “Analisis Formal Lightweight Mutual Authentication RFID Protocol Menggunakan Scyther,” *Info Kripto*, vol. 16, no. 1, 2022, doi: 10.56706/ik.v16i1.42.

[26] A. S. Indrawanti, A. W. Azinar, and M. A. Firdiansyah, “SECURE E-VOTING MENGGUNAKAN METODE RSA DAN AUTENTIKASI RFID,” *Netw. Eng. Res. Oper.*, vol. 4, no. 1, 2018, doi: 10.21107/nero.v4i1.113.

[27] M. Anwar Fauzi, A. Id Hadiana, and F. Rakhmat Umbara, “PENAMBAHAN FITUR MULTI-FACTOR AUTHENTICATION DALAM STUDI KASUS SISTEM INFORMASI REKAM MEDIS RUMAH SAKIT,” *JATI (Jurnal Mhs. Tek. Inform.*, vol. 7, no. 4, 2024, doi: 10.36040/jati.v7i4.7305.

[28] R. M. Saqib *et al.*, “Analysis and Intellectual Structure of the Multi-Factor Authentication in Information Security,” *Intell. Autom. Soft Comput.*, vol. 32, no. 3, 2022, doi: 10.32604/IASC.2022.021786.

[29] H. H. RACHMAT and G. A. HUTABARAT, “Pemanfaatan Sistem RFID

sebagai Pembatas Akses Ruangan," *ELKOMIKA J. Tek. Energi Elektr. Tek. Telekomun. Tek. Elektron.*, vol. 2, no. 1, 2014, doi: 10.26760/elkomika.v2i1.27.

[30] K. Wirawibawa, R. Susana, and H. H. Rachmat, "Evaluasi Keandalan Identifikasi RFID MFRC522 dengan Barrier Berbahan Dasar Plastik Berbasis Sistem Mikrokontroler," *JEECOM J. Electr. Eng. Comput.*, vol. 4, no. 1, 2022, doi: 10.33650/jeecom.v4i1.2930.

[31] S. Sutarti, T. Triyatna, and S. Ardiansyah, "Prototype Sistem Absensi Siswa/I Dengan Menggunakan Sensor Rfid Berbasis Arduino Uno," *PROSISKO J. Pengemb. Ris. dan Obs. Sist. Komput.*, vol. 9, no. 1, pp. 76–85, 2022, doi: 10.30656/prosisko.v9i1.4744.

[32] T. Sutikno, M. A. Faqih Ubaidillah, W. Arsadiando, and H. S. Purnama, "Fingerprint based smart door lock system using Arduino and smartphone application," *Comput. Sci. Inf. Technol.*, vol. 5, no. 1, 2024, doi: 10.11591/csit.v5i1.p85-92.

[33] F. I. Pasaribu and M. Marcopolo, "Perancangan Prototype Alat Pemilah Sampah Otomatis," *RELE (Rekayasa Elektr. dan Energi) J. Tek. Elektro*, vol. 2, no. 1, pp. 22–29, 2019, doi: 10.30596/rele.v2i1.3645.

[34] N. Evalina, F. I. Pasaribu, A. A. H, and A. Sary, "Penggunaan Arduino Uno Untuk Mengatur Temperatur Pada Oven," *RELE (Rekayasa Elektr. dan Energi) J. Tek. Elektro*, vol. 4, no. 2, pp. 122–128, 2022, doi: 10.30596/rele.v4i2.9559.

[35] N. Evalina, D. J. Maulana, M. Putri, F. I. Pasaribu, and P. Harahap, "Perancangan Sistem Kontrol Ketinggian Air Pada Media Tanam Hidroponik," *RELE (Rekayasa Elektr. dan Energi) J. Tek. Elektro*, vol. 6, no. 1, pp. 36–41, 2023, doi: 10.30596/rele.v6i1.15457.

[36] J. E. C. Candra and M. F. E. Prasetyo, "Pemanfaatan Sensor Fingerprint Untuk Kendali dan Keamanan Sepeda Motor Berbasis Arduino," *J. Desain Dan Anal. Teknol.*, vol. 2, no. 1, pp. 66–74, 2023, doi: 10.58520/jddat.v2i1.22.

[37] I. Oraif, "Natural Language Processing (NLP) and EFL Learning: A Case Study Based on Deep Learning," *J. Lang. Teach. Res.*, vol. 15, no. 1, 2024,

doi: 10.17507/jltr.1501.22.

[38] T. M. Taha, Z. Ben Messaoud, and M. Frikha, “Convolutional Neural Network Architectures for Gender, Emotional Detection from Speech and Speaker Diarization,” *Int. J. Interact. Mob. Technol.*, vol. 18, no. 3, 2024, doi: 10.3991/ijim.v18i03.43013.

[39] F. Azhari *et al.*, “Penerapan Manajemen Sekuriti Dalam Meningkatkan Keamanan Pengguna Pada Transaksi E-wallet,” *J. Kewirausahaan dan Multi Talent.*, vol. 2, no. 2, pp. 138–147, 2024, [Online]. Available: https://creativecommons.org/licenses/by/4.0/

[40] H. Djamal, “Radio Frequency Identification (RFID) Dan Aplikasinya,” *TESLA J. Tek. Elektro*, vol. 16, no. 1, pp. 45–55, 2014.