

BAB I USULAN GAGASAN

1.1. Latar Belakang Masalah

Pada bagian ini, akan diawali dengan data statistik yang diambil dari artikel *goodstats.id* terkait masalah yang diangkat yakni kasus kejahatan yang terjadi di Indonesia selama periode Januari hingga April 2023 [1]. Grafik yang disajikan akan memberikan gambaran mengenai jenis-jenis kejahatan yang paling banyak tercatat dan frekuensinya. Informasi ini bermanfaat untuk memahami tren kejahatan yang terjadi, yang dapat membantu dalam penyusunan strategi pencegahan dan penanggulangan kejahatan.



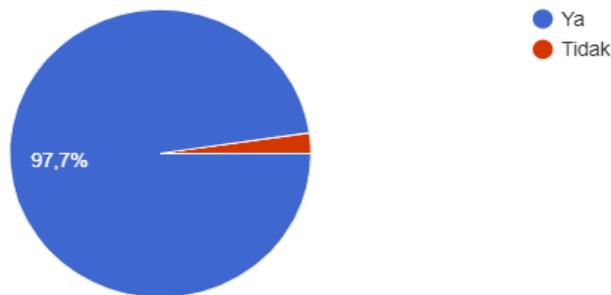
Gambar 1.1 Sepuluh Kasus Kejahatan yang Paling Banyak Terjadi di Indonesia Selama Kuartal Pertama Tahun 2023 [1]

Berdasarkan jenisnya, Pada gambar 1.1 mayoritas kasus kejahatan yang terjadi di Indonesia pada kuartal pertama tahun 2023 berupa pencurian dengan pemberatan (curat), yaitu 30.019 kasus. Mengacu pada UU Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (KUHP), curat adalah pencurian yang dilakukan dalam keadaan tertentu sehingga hukumannya menjadi lebih berat. Kemudian pada urutan kedua yakni kejahatan pencurian biasa dengan jumlah kasus sebanyak 20.043 kasus. Rumah merupakan salah satu target pencurian. Berikut di

bawah ini merupakan gambar survei mengenai penggunaan kunci pintu yang telah dilakukan melalui kuisisioner Google *form* dengan *link* <https://bit.ly/KuisisionerKunciManual>.

Apakah pintu Anda saat ini masih menggunakan kunci manual yang biasa?

43 jawaban

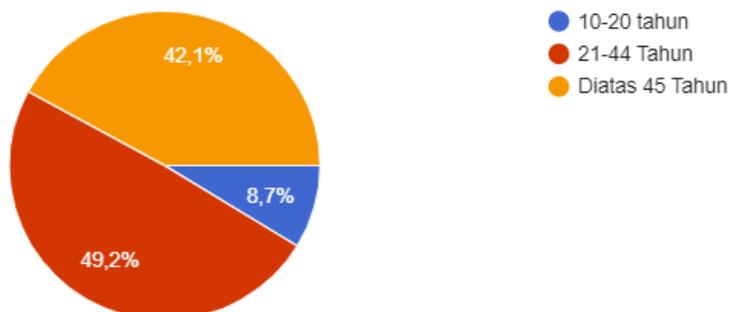


Gambar 1.2 Survei Banyaknya Penggunaan Kunci Manual Pada Masyarakat

Menghubungkan gambar 1.2 di atas dengan gambar 1.1 sebelumnya tentang kasus kejahatan di Indonesia, bahwa mayoritas rumah yang menjadi target pencurian kemungkinan besar masih menggunakan kunci manual. Ini mengindikasikan pentingnya meningkatkan kesadaran akan keamanan yang dapat memberikan perlindungan lebih baik terhadap pencurian. Berikut di bawah ini merupakan gambar survei mengenai mayoritas responden dalam rentang usia.

Berapa rentang umur anda?

126 jawaban

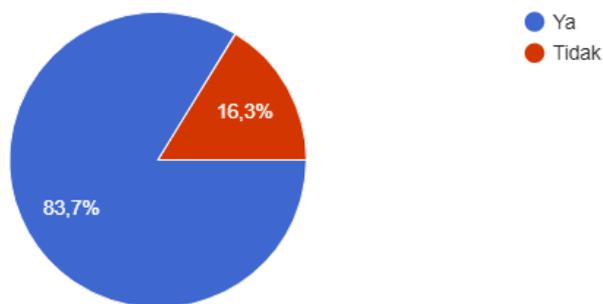


Gambar 1.3 Survei Mayoritas Responden Dalam Rentang Usia

Gambar di atas menunjukkan usia yang lebih condong ke kelompok umur dewasa dan lanjut usia, dengan rentang umur 21-44 tahun sebesar 49.2%. Kemudian, untuk umur di atas 45 tahun sebesar 42.1%. Berikut di bawah ini merupakan gambar survei mengenai masalah-masalah yang pernah terjadi dalam penggunaan kunci manual.

Pernahkah anda lupa sudah mengunci pintu atau belum, ketika sedang berpergian?

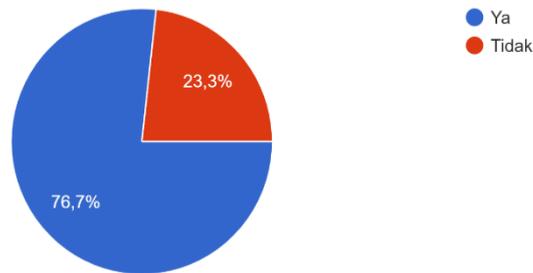
43 jawaban



Gambar 1.4 Survei Banyaknya Pengguna yang Lupa Dengan Kondisi Pintu Ketika Sedang Berpergian

Gambar di atas menampilkan hasil survei tentang pengguna yang lupa dengan kondisi pintu ketika sedang berpergian, dengan 43 responden yang berpartisipasi. Dari survei tersebut, 83.7% responden mengakui bahwa mereka pernah lupa mengunci pintu saat hendak berpergian, sementara 16.3% responden menyatakan bahwa mereka tidak pernah lupa. Menghubungkan ini dengan data kejahatan di Indonesia yang sebelumnya dijelaskan, lupa terhadap kondisi pintu dapat menjadi risiko yang signifikan dalam kasus pencurian. Berikut di bawah ini merupakan gambar survei selanjutnya.

Pernahkah Anda menghadapi masalah kunci yang tertinggal sehingga tidak bisa membuka pintu?
43 jawaban

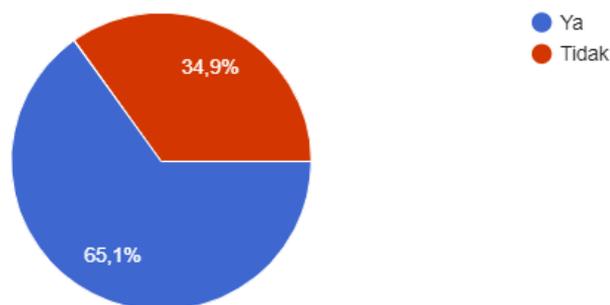


Gambar 1.5 Survei banyaknya pengguna yang pernah tertinggal kunci

Gambar di atas menunjukkan hasil survei yang melibatkan 43 responden tentang pernah tidaknya mereka menghadapi masalah kunci yang tertinggal sehingga tidak bisa membuka pintu. Dari survei tersebut, 76.7% responden mengatakan bahwa mereka pernah mengalami masalah ini, sementara 23.3% responden tidak pernah mengalaminya. Berikut di bawah ini merupakan gambar survei selanjutnya.

Pernahkah Anda menghadapi masalah kunci yang tertukar-tukar karena banyaknya kunci manual yang harus Anda bawa?

43 jawaban



Gambar 1.6 Survei banyaknya pengguna yang pernah tertukar-tukar kunci karena banyaknya kunci manual yang harus dibawa

Dari gambar survei di atas terlihat, sebanyak 65.1% responden mengatakan mereka pernah menghadapi masalah kunci yang tertukar-tukar karena banyaknya kunci manual yang harus mereka bawa, sementara 34.9% responden tidak pernah

mengalami masalah tersebut. Masalah ini menekankan tantangan yang mungkin dihadapi pengguna kunci manual. Mengelola banyak kunci bisa menyebabkan kebingungan dan kesulitan, terutama dalam situasi yang membutuhkan akses cepat atau dalam keadaan darurat. Ini menggarisbawahi pentingnya sistem kunci yang lebih efisien dan mudah digunakan.

Berdasarkan permasalahan tersebut, kunci manual mendapatkan respons terhadap sejumlah masalah yang dialami dari kalangan masyarakat. Kunci manual seringkali rentan terhadap pencurian, kehilangan, dan kesulitan pengelolaan akses. Masalah ini meliputi risiko keamanan yang meningkat, resiko kehilangan atau lupa kunci, serta kendala dalam pengelolaan akses, terutama dalam rumah tangga. Selain itu, mengganti kunci manual, pemantauan akses, dan kontrol jarak jauh adalah tantangan yang sulit di atasi dengan sistem kunci manual. Dengan begitu, dibutuhkan langkah penting dalam menangani beberapa masalah yang sering terjadi dengan sistem kunci manual.

Oleh karena itu, di dalam penelitian ini diusulkan salah satu alternatif solusi yang bisa mengatasi masalah itu semua yaitu alat kunci pintu digital atau *smart lock*. Alat *smart lock* hadir untuk mengatasi risiko-risiko di atas. Alat *smart lock* hadir sebagai solusi komprehensif untuk mengatasi masalah keamanan yang dihadapi oleh sistem kunci konvensional. *Smart lock* dapat menggantikan kunci fisik dengan metode otentikasi yang lebih canggih, seperti menggunakan PIN, kartu, atau pengendalian jarak jauh melalui *smartphone* yang memberikan perlindungan keamanan lebih kuat terhadap risiko pencurian. Dalam hal pengelolaan akses, alat *smart lock* menghilangkan kerumitan berbagi kunci fisik, memungkinkan pengguna untuk dengan mudah memberikan akses kepada individu yang diinginkan dan mengubah izin akses secara dinamis. Ini menjadikan manajemen akses lebih efisien dan mengurangi resiko kehilangan kunci atau tertukar. Terakhir, dari perspektif kemudahan, alat *smart lock* memberikan kenyamanan dengan pemantauan akses dan pengendalian pintu dari jarak jauh, serta memungkinkan pembukaan pintu tanpa kunci fisik, seperti menggunakan *smartphone* atau PIN, yang membuat pengalaman pengguna lebih nyaman dalam kehidupan sehari-hari.

1.2. Analisis Masalah

Pada bagian ini, dijelaskan masalah yang dianalisis dari berbagai aspek, di antaranya aspek ekonomi, aspek teknis, aspek keamanan, dan aspek kemudahan. Dengan menjabarkan aspek-aspek di atas, diharapkan dapat menemukan masalah dari setiap aspek tersebut.

1.2.1 Aspek Ekonomi

Dalam kasus masalah ini, untuk membangun sebuah sistem *smart lock* ini ada tiga metode yaitu Biometrik, RFID dan *Remote* yang kekurangannya itu sendiri membutuhkan alat-alat yang salah satunya memerlukan biaya yang tinggi untuk satu alatnya. Selain itu juga, diperlukan pemeliharaan berkala dan pembaruan perangkat lunak, yang dapat mengakibatkan adanya biaya tambahan. Dalam jangka panjang, efisiensi dan manajemen akses yang lebih baik dapat mengurangi biaya penggantian kunci fisik yang sering terjadi pada sistem konvensional. Selain itu, efisiensi energi yang terkait dengan *smart lock* dapat mengurangi pengeluaran bulanan. Oleh karena itu, analisis ekonomi menyeluruh perlu dipertimbangkan untuk menilai keuntungan jangka panjang dari penggunaan alat *smart lock door* dan dampaknya terhadap keuangan pribadi dan properti.

1.2.2 Aspek Teknis

Banyak hal teknis yang menjadi aspek penting untuk ditinjau dalam *smart lock door*. salah satunya ada penggunaan daya. *Smart lock* pintu bergantung pada daya listrik untuk mengaksesnya. Jika tidak ada daya listrik, pintu tidak dapat dibuka, yang dapat mengganggu akses ke rumah. Sebaiknya ada perangkat penyimpanan energi seperti baterai karena jika terjadi pemadaman listrik maka dapat menggunakan baterai untuk daya listrik sementara.

Selain itu, penggunaan daya yang efisien dan masa pakai baterai yang cukup lama menjadi faktor kunci dalam memastikan kinerja yang baik. Oleh karena itu, ketika mempertimbangkan pembuatan alat *smart lock door*, perlu ada pemahaman yang baik tentang aspek teknisnya dan langkah-langkah yang diperlukan untuk menjaga kinerja yang optimal dan mengatasi potensi masalah teknis.

1.2.3 Aspek Keamanan

Penggunaan *smart door smart locks* membawa sejumlah masalah keamanan yang perlu diperhatikan. Pertama, kerentanan terhadap peretasan elektronik menjadi ancaman utama, karena peretas yang cakap dapat meretas sistem ini untuk membuka pintu tanpa izin. Selain itu, koneksi ke internet juga membuat *smart locks* rentan terhadap serangan siber, seperti serangan *phishing* atau *brute force* pada kata sandi. Kerentan tersebut dapat membahayakan keamanan fisik rumah. Untuk menghindari ini, ketika pembuatan harus dipastikan bahwa alat *smart locks* harus dilengkapi dengan lapisan keamanan dan enkripsi yang kuat. Selain itu, pembaruan perangkat lunak dan perangkat keras berkala harus dijalankan untuk mengatasi kerentanan yang mungkin muncul dari waktu ke waktu.

Kedua, masalah terkait dengan privasi dan keamanan data juga perlu diperhatikan. Data yang dikumpulkan oleh *smart locks*, termasuk catatan akses, dapat menjadi target peretasan atau penyalahgunaan privasi jika tidak dijamin dengan baik. Oleh karena itu, untuk menghindari hal tersebut alat *smart locks* harus memiliki kebijakan privasi yang ketat dan melindungi data akses dengan baik. Salah satunya dengan membuat fitur otentikasi dua faktor. Selain itu, pengguna juga harus mengamankan jaringan *WiFi* mereka dengan kata sandi yang kuat dan enkripsi yang solid untuk mencegah serangan siber terhadap perangkat *smart lock*.

1.2.4 Aspek Kemudahan

Dari segi pembuatan, pembuatan alat *smart lock door* mungkin memerlukan teknologi dan bahan yang lebih canggih, yang pada gilirannya dapat meningkatkan biaya produksi. Selain itu, pengembangan perangkat lunak yang diperlukan untuk mengendalikan dan mengintegrasikan *smart lock door* juga memerlukan sumber daya yang cukup besar. Ini dapat menjadi kendala pada tahap pembuatan alat karena banyaknya perangkat yang kompleks.

Dari sudut pandang pengguna, masalah yang mungkin muncul adalah terkait dengan kerumitan penggunaan dan kompatibilitas. Pengguna harus memahami cara mengoperasikan *smart lock door*, dan dalam beberapa kasus, ini dapat menjadi tugas yang menantang, terutama bagi orang-orang yang kurang

berpengalaman dalam teknologi atau orang lansia. Selain itu, kompatibilitas dengan perangkat rumah pintar yang ada dapat menjadi masalah, terutama jika pengguna harus menghadapi banyak antarmuka dan aplikasi yang berbeda.

Untuk mengatasi masalah ini, pembuatan alat *smart lock door* perlu mengembangkan teknologi produksi yang lebih efisien untuk menjaga agar tetap mudah ketika pembuatan dan juga ketika digunakan pengguna. Selain itu, pelatihan dan panduan pengguna yang baik dapat membantu mengurangi kerumitan bagi pengguna dan memastikan penggunaan alat ini yang lebih lancar. Pengintegrasian yang lebih baik dengan sistem rumah pintar yang ada juga dapat meningkatkan kemudahan penggunaan. Dengan demikian, kendala dalam hal pembuatan alat dan kemudahan penggunaan dapat diatasi dengan pendekatan yang benar dalam pengembangan dan penyebaran *smart lock door*.

1.3 Analisis Solusi yang Ada

Pada bagian ini, dijelaskan mengenai solusi dari berbagai tipe autentikasi, di antaranya biometrik, RFID, dan *remote*. Tipe autentikasi merupakan cara untuk mengakses pintu.

1.3.1 Biometrik

Berikut pada bagian ini berisi analisis dari penelitian-penelitian sebelumnya yang telah dibuat dari tipe autentikasi menggunakan biometrik, di antaranya pengenalan wajah, sidik jari, dan pengenalan suara. Biometrik digunakan untuk mengidentifikasi dan memverifikasi identitas seseorang berdasarkan karakteristik fisik atau perilaku yang unik.

A. Sistem Pengenalan Kunci Otomatis Menggunakan Pengenalan Wajah

Penelitian yang dibuat adalah untuk membuat sistem kunci pintu otomatis menggunakan pengenalan wajah untuk tujuan keamanan. Alat ini menggunakan Raspberry Pi sebagai platform utama, lalu terdapat kamera Pi untuk merekam gambar, Relay untuk menggerakkan motor DC agar pintu dapat dibuka setelah proses pengenalan wajah berhasil, LED digunakan sebagai indikator status pintu, dan modul GSM untuk pengiriman pesan ke nomor ponsel terdaftar jika gambar yang ditangkap oleh kamera tidak cocok dengan gambar yang ada dalam basisdata.

Untuk cara kerjanya adalah sistem akan dirancang untuk mengenali wajah orang di dekat pintu dan membandingkannya dengan wajah yang diunggah yang tersimpan dalam *database*. Jika orang tersebut terdeteksi, maka pintu akan terbuka dan menyambut mereka. Jika ada orang yang tidak dikenal masuk, pemilik rumah akan diberitahu melalui pesan dan surat dengan gambar penyusup. Untuk mendeteksi pengenalan wajah menggunakan algoritma Haar Cascade Classifier dan di program menggunakan bahasa Python melalui OpenCV *Libraries*. Kelebihan dari proyek ini adalah secara keamanan sangat bagus karena dapat memantau apakah ada orang yang tidak dikenal memasuki pintu menggunakan pendekatan deteksi pengenalan wajah. Lalu, penggunaan algoritma Haar Cascade Classifier memiliki akurasi dan kecepatan yang tinggi dalam mendeteksi wajah. Kemudian, alat ini cocok untuk orang dewasa yang tinggal sendiri dan untuk orang yang tidak dapat berjalan karena sistem yang digunakan praktis dan mudah dilacak. Kekurangannya adalah, penggunaan pengiriman pesan pada ponsel yang sebagian orang mungkin masih belum mengerti. Kemudian, untuk sistem menangkap gambar wajah orang yang ingin memasuki pintu, ini dapat menimbulkan masalah privasi bagi sebagian orang [2].

B. Perancangan Pengaman Pintu Rumah Berbasis Sidik Jari

Tujuan dari penelitian ini yaitu menggantikan kunci konvensional biasa menjadi *smart lock* yang menggunakan sensor sidik jari. Penelitian ini menggunakan mikrokontroler ATmega328P, sensor sidik jari C3, aktuator, solenoid untuk sebagai penggerak aktuator, *SD card* untuk *logging*, dan 16 x 02 serial LCD. Cara kerja secara garis besar pada alat ini yaitu identifikasi sidik jari sebagai input dari sensor sidik jari. Setelah itu sidik jari dicocokkan dengan *database* yang sudah disimpan. Jika sidik jari tidak cocok dengan *database* maka solenoid tidak akan menggerakkan aktuator yang berarti pintu tidak terbuka. Jika sidik jari cocok dengan *database* maka solenoid akan menggerakkan aktuator yang membuat pintu terbuka. Dari perancangan ini dapat digunakan untuk melanjutkan pada tingkat yang lebih tinggi lagi yaitu dalam tahap pembuatan, karena penggunaan kunci konvensional rentan terhadap kehilangan atau kelupaan. Ini menjadi suatu prospek yang baik untuk mengedepankan kebutuhan teknologi dan informasi [3].

C. Perancangan *Smart Door Lock* Menggunakan Pengenalan Suara

Masalah pada penelitian ini adalah penggunaan kunci konvensional untuk mengunci dan membuka kunci pintu ruang *server*. Hal ini mengharuskan staf untuk mencari kunci dan membuka kunci pintu secara manual. Untuk mengatasi masalah ini, penelitian ini mengusulkan sistem *Smart Door Lock* yang menggunakan pengenalan suara untuk mengunci dan membuka kunci pintu. Perancangan alat ini dibuat dengan menggunakan Raspberry pi 3 sebagai pusat pemrosesannya dan ULN2803 sebagai IC untuk menaikkan tegangan sehingga dapat menggerakkan solenoid yang berfungsi untuk menggerakkan pengunci pintu. Cara kerja dari sistem ini menggunakan aplikasi *smartphone* yang terhubung dengan *Bluetooth* dan internet. Aplikasi tersebut mengirimkan perintah suara ke Raspberry Pi 3, yang akan memproses perintah tersebut dan mengirimkan data ke *ULN2803* untuk menaikkan tegangan dan mengaktifkan solenoid *door lock*. Raspberry Pi 3 juga mengirimkan perintah ke servo motor untuk membuka atau menutup pintu. Sistem *Smart Door Lock* dirancang untuk membatasi akses hanya untuk personil yang berwenang, dan hanya dapat dioperasikan oleh staf yang telah mendaftarkan ID dan kata sandi. Sistem ini dilengkapi dengan dashboard bagi admin untuk mengelola data pengguna. Sistem akan diuji dengan menggunakan pengujian *black box* untuk *login*, solenoid, dan motor servo. Prototipe sistem dirancang untuk mempermudah proses penguncian dan pembukaan kunci pintu ruang *server* dengan menghilangkan kebutuhan akan kunci konvensional dan menggantinya dengan teknologi pengenalan suara. Kelebihan dari proyek ini adalah menggunakan teknologi pengenalan suara yang memberikan tingkat keamanan dan akses yang lebih terkomputerisasi. Kemudian, sistem ini dirancang untuk membatasi akses hanya untuk personil yang berwenang, dan hanya dapat dioperasikan oleh staf yang telah mendaftarkan ID dan kata sandi. Keterbatasannya adalah, sistem akan susah mendeteksi suara di lingkungan yang bising atau saat pengguna sedang pilek atau sakit tenggorokan. Lalu, sistem juga akan sulit mendeteksi apabila suara orang yang memiliki hambatan bicara atau aksen, dan dalam mengenali suara orang yang tidak terdaftar dalam sistem [4].

D. Desain Sistem Keamanan Pintu Menggunakan Pengenalan Wajah

Penelitian ini adalah untuk pengembangan dan pengujian sistem keamanan pintu menggunakan pengenalan wajah. Sistem ini bertujuan untuk mencegah akses yang tidak sah ke sebuah rumah dengan mendeteksi dan mengenali wajah orang yang mencoba masuk. Sistem ini memberikan solusi keamanan yang komprehensif dengan mengintegrasikan deteksi wajah dan langkah-langkah keamanan berbasis keypad. Alat mikrokontroler yang dibuat pada sistem ini adalah menggunakan Arduino Uno dan ESP 32 - CAM. Sistem ini menggunakan kamera internal pada ESP 32 - CAM untuk menangkap gambar wajah dan mengenali individu yang berwenang. Sistem ini terintegrasi dengan kerangka kerja IoT, memungkinkan pemantauan dan pemberitahuan jarak jauh melalui aplikasi Telegram. ESP 32 - CAM berfungsi sebagai pengontrol untuk sistem IoT, memungkinkan komunikasi dan transmisi data yang lancar. Tujuannya adalah untuk mengendalikan berbagai komponen sistem, seperti kunci pintu solenoid, *keypad*, dan layar LCD. Sistem ini menggunakan kunci pintu solenoid sebagai aktuator untuk membuka dan menutup pintu. *Keypad* digunakan untuk memasukkan kata sandi secara manual, dan memberikan lapisan keamanan tambahan. Layar LCD digunakan untuk memberikan informasi berupa tulisan ketika pintu dapat dibuka atau *card* yang digunakan untuk membuka pintu adalah salah. Kelebihan dari proyek ini adalah memberikan tingkat keamanan yang lebih tinggi dengan memanfaatkan teknologi pendeteksi wajah untuk mengenali individu yang berwenang dan mengirimkan peringatan keamanan ketika individu yang tidak berwenang terdeteksi. Kemudian, untuk integrasi aplikasi Telegram memungkinkan pemberitahuan keamanan jarak jauh, sehingga pemilik rumah dapat menerima peringatan dan mengambil tindakan yang diperlukan meskipun mereka berada jauh dari lokasi. Kekurangan dari proyek ini adalah penundaan dalam pengenalan wajah, dengan penundaan rata-rata 11,60 detik. Penundaan ini dapat dianggap sebagai kelemahan, terutama dalam situasi yang membutuhkan akses atau respons yang cepat. Kemudian, meskipun sistem menunjukkan kemampuan pengenalan wajah yang andal, mungkin ada skenario di mana sistem dapat menghadapi tantangan, seperti variasi kondisi pencahayaan, penghalang wajah, atau perubahan penampilan wajah karena faktor-faktor seperti rambut atau aksesoris wajah [5].

E. Pengenalan Individu Melalui Identifikasi Wajah Menggunakan Metode *You Only Look Once (YOLOv5)*

Jurnal ini membahas tentang teknologi biometrika yang memanfaatkan identifikasi wajah untuk mengenali individu menggunakan metode YOLOv5. YOLOv5 adalah sistem deteksi objek yang mampu mendeteksi objek secara *real time* dan tidak memerlukan memori besar, sehingga memudahkan instalasi dan integrasi pada perangkat IoT. Penelitian ini diawali dengan pengumpulan data dari video rekaman CCTV di Laboratorium *Machine Learning* dan *Big Data* Departemen Matematika ITS. Data video tersebut kemudian diproses menjadi *frame-frame* citra gambar yang disortir dan dianotasi untuk mendeteksi objek wajah mahasiswa. Model YOLOv5 dilatih menggunakan data latih dan data validasi yang telah dianotasi, melalui proses konversi ukuran citra gambar, pendeteksian pada beberapa skala, dan penghitungan *loss function* untuk meningkatkan akurasi prediksi. Hasil penelitian menunjukkan bahwa model YOLOv5 dapat mengidentifikasi wajah individu dengan akurasi rata-rata 99.88% pada video dengan satu mahasiswa dan tingkat kecerahan normal. Penelitian ini menekankan bahwa metode YOLOv5 efektif dalam mengidentifikasi wajah individu secara *real time*, serta memberikan kontribusi dalam pengembangan sistem deteksi individu untuk keperluan identitas atau keamanan [6].

1.4.2 RFID

Berikut pada bagian ini berisi analisa dari penelitian sebelumnya yang telah dibuat dari tipe autentikasi menggunakan kartu RFID. Kartu RFID digunakan untuk mengakses pintu dengan menempelkan kartu ke sensor.

A. RFID Based Smart Door Lock Security System

Tujuan dari membuat sensor pada rak *server* ini bertujuan untuk meningkatkan keamanan secara fisik pada sebuah perangkat *server data center*. Sehingga selain teknisi yang mengoperasikan *data center* ini tidak akan dapat mengakses rak *data center*. PT Cybertechtonic Pratama pada ruangan rak *data center* masih menggunakan kunci fisik. Oleh karena itu peneliti ingin membuat sistem *Door Lock* yang menerapkan (IOT) *Internet of Things* untuk menambah keamanan dalam pemeliharaan perangkat fisik *data center*. Pada Tugas Akhir ini,

dilakukan perancangan alat *Door Lock* menggunakan mikrokontroler NodeMCU yang akan terhubung dengan aplikasi Blynk menggunakan ESP8266. Dengan adanya RFID *Door Lock* pada perangkat *data center* para teknisi nantinya tidak perlu lagi repot untuk membuka kunci rak *server* secara manual. Kunci tersebut dapat dibuka melalui Kartu Mifare yang akan di *tapping* ke alat RFID. Nantinya *smartphone* pada dapat menerima notifikasi ketika ada yang membuka kunci pada aplikasi Blynk. Jurnal ini mengharapkan jika penerapan *prototype door lock* dengan metode PPDIIO yang dapat dikembangkan kembali pada penelitian yang berikutnya untuk mencapai keamanan yang lebih baik untuk membuat perangkat rak *server* pada *data center* terjaga [7].

1.4.3 Remote

Berikut pada bagian ini berisi analisa dari penelitian sebelumnya yang telah dibuat dari tipe autentikasi menggunakan *Remote*. *Remote* digunakan untuk mengakses pintu dari jarak jauh.

A. Remotely Accessible Smart Lock Security System with Essential Features

Sistem ini dapat dengan mudah diintegrasikan dengan perangkat IoT lainnya. Integrasi ini akan memperluas kemampuan sistem dan memungkinkan pengendalian dan pemantauan yang mulus dari berbagai perangkat pintar di rumah. Sistem dapat ditingkatkan dengan mengeksplorasi mekanisme transmisi alternatif seperti biometrik atau pengenalan gerakan. Mekanisme ini akan memberikan cara yang lebih aman dan nyaman bagi pemilik untuk mengotentikasi diri mereka dan memberikan akses kepada individu yang diotorisasi. Integrasi ini akan memungkinkan pengendalian dan otomatisasi berbagai perangkat rumah, meningkatkan kenyamanan dan efisiensi. Sistem diperkuat dengan integrasi perangkat lunak *computer vision* seperti *OpenCV* untuk ekstraksi dan analisis fitur wajah. Hal ini akan memungkinkan pemilik untuk menilai niat pengunjung sebelum memberikan akses, meningkatkan keamanan. Dengan menerapkan perbaikan di atasnya, sistem akan menjadi lebih canggih, aman, dan ramah pengguna, menyediakan solusi komprehensif untuk akses jarak jauh dan keamanan di rumah pintar.

Sistem keamanan kunci pintar yang dapat diakses dari jarak jauh bekerja dengan menggunakan Raspberry Pi dengan kamera HD yang terpasang di pintu. Ketika seorang pengunjung menekan bel panggilan, Raspberry Pi menyalakan dan mengirimkan pemberitahuan ke ponsel pintar pemiliknya. Pemilik kemudian dapat melihat siaran langsung identitas pengunjung di ponsel pintar mereka. Jika pemilik ingin memberikan akses, mereka dapat membuka pintu dari jarak jauh dengan memasukkan kata sandi yang telah ditetapkan pada ponsel mereka. Selain itu, pemilik dapat meninggalkan pesan suara untuk pengunjung dengan memasukkan teks yang sesuai dalam aplikasi ponsel mereka. Sistem ini menggunakan arsitektur sederhana dan efisien untuk mengatasi keterbatasan sistem kunci fisik tradisional dan solusi digital. Hal ini memberikan akses jarak jauh ke rumah, siaran langsung, kemampuan pesan suara, peningkatan keamanan, dan konsumsi daya yang optimal. Sistem ini juga dapat dengan mudah diintegrasikan dengan perangkat IoT lainnya dan dapat digabungkan untuk menyatukan dan mengendalikan beberapa kunci dengan otentikasi unik untuk masing-masing dari mereka. Konfigurasi perangkat keras mencakup Raspberry Pi, kamera HD, modul konverter logika, dan saklar dengan resistor *pull-up*. Sistem ini diprogram dalam bahasa Python untuk mengendalikan mekanisme kunci dan menangani komunikasi antara Raspberry Pi dan ponsel pintar pemiliknya. Secara keseluruhan, sistem ini memberikan akses jarak jauh secara *real time* dan fitur interaktif bagi pemilik, meningkatkan keamanan dan kenyamanan [8].

B. Door lock system based on internet of things and Bluetooth by using Raspberry Pi

Sistem keamanan kunci pintar yang dapat diakses dari jarak jauh yang dijelaskan dalam makalah ini bekerja dengan memanfaatkan teknologi *Internet of Things (IoT)* dan perangkat elektronik portabel *Bluetooth*, seperti ponsel pintar. Sistem ini menggunakan alamat kontrol media *Bluetooth (MAC)* dari perangkat *Bluetooth* sebagai kunci, dan IoT untuk pemantauan. Admin dapat mendaftarkan pengguna menggunakan aplikasi yang bekerja pada Android dan iOS. Admin juga dapat membuka pintu dari jarak jauh dengan melihat gambar pengunjung di pintu dan membukanya secara *remote* melalui aplikasi. Ini memungkinkan admin untuk

mengelola akses pintu tanpa harus berada di dekat pintu secara fisik. Sistem menyediakan fitur bagi admin untuk mengelola pengguna dan membuka pintu dari jarak jauh melalui sebuah aplikasi. Admin dapat mendaftarkan pengguna menggunakan aplikasi yang bekerja pada Android dan iOS. Admin juga dapat membuka pintu dari jarak jauh dengan melihat gambar pengunjung di pintu dan membukanya secara *remote* melalui aplikasi. Ini memungkinkan admin untuk mengelola akses pintu tanpa harus berada di dekat pintu secara fisik. Menggunakan teknologi *Internet of Things* (IoT) dan perangkat elektronik portabel *Bluetooth*, seperti ponsel pintar, sebagai kunci. Admin dapat mendaftarkan pengguna menggunakan aplikasi yang bekerja pada Android dan iOS. Admin dapat membuka pintu dari jarak jauh dengan melihat gambar pengunjung di pintu dan membukanya secara *remote* melalui aplikasi. Untuk meningkatkan keamanan sistem ini, dapat dilakukan dengan integrasi teknologi lain seperti pengenalan wajah, sensor sidik jari, dan teknologi pengenalan suara. Integrasi teknologi-teknologi ini dapat memberikan opsi tambahan untuk otentikasi pengguna, sehingga meningkatkan tingkat keamanan [9].

1.4 Analisis dari Jurnal yang Sudah Ada

Pada bagian ini, solusi yang sudah dijabarkan sebelumnya selanjutnya akan dianalisis kelebihan dan juga kekurangannya. Berikut di bawah ini merupakan tabel yang berisi kelebihan dan kekurangan dari setiap solusi.

Tabel 1.1 Analisis dari Jurnal yang Sudah Ada

Nama Solusi	Kelebihan	Kekurangan
(Biometrik) Pengenalan Wajah menggunakan algoritma Haar Cascade Classifier, dan bahasa Python OpenCV Libraries dengan aktuator Motor DC.	Algoritma Haar Cascade Classifier lebih akurat dan cepat dalam mendeteksi wajah. Cocok untuk orang dewasa dan yang tidak dapat berjalan. Karena	Sistem terkadang gagal mengenali wajah orang yang berwenang, yang dapat menyebabkan ketidaknyamanan. Motor DC dari segi keamanan fisik tidak

Nama Solusi	Kelebihan	Kekurangan
	<p>sistem praktis dan mudah dilacak.</p> <p>Motor DC memiliki kecepatan untuk mengoptimalkan waktu penguncian atau pembukaan pintu. Kemudian, relatif efisien dari segi energi, yang berarti bahwa mereka dapat menggerakkan mekanisme penguncian dengan menggunakan daya yang relatif sedikit.</p>	<p>memiliki kemampuan untuk keamanan pintu secara langsung.</p> <p>Dibutuhkan pintu yang terbuat dari bahan yang kokoh dan berkualitas tinggi, dan sistem penguncian harus dirancang dengan baik.</p> <p>Sistem harus dirancang agar terhindar dari pemutusan daya listrik atau manipulasi mekanisme penguncian.</p>
<p>(Biometrik) Pengenalan individu melalui identifikasi wajah menggunakan metode YOLOv5</p>	<p>Mampu mendeteksi objek secara <i>real time</i>, tidak memerlukan memori besar, akurasi rata-rata sangat tinggi, efektif dalam identifikasi wajah individu, kontribusi dalam pengembangan sistem deteksi individu.</p>	<p>Belum disebutkan performa pada kondisi pencahayaan yang buruk, hasil penelitian terbatas pada satu atau dua individu, dataset terbatas dari satu sumber, belum diuraikan waktu pemrosesan secara detail.</p>
<p>(Biometrik) Sensor Sidik jari menggunakan metode UML</p>	<p>Metode UML disini sebagai metode pengambilan suatu keputusan yang jelas dengan gambaran desain keseluruhan.</p>	<p>Penggunaan solenoid yang berupa barang elektronik dapat mengalami keausan. oleh karena itu, diharuskan pemeliharaan rutin.</p>

Nama Solusi	Kelebihan	Kekurangan
		<p>Sistem ini belum ada cadangan daya bila <i>power supply</i> tidak bekerja. Jadi diharuskan cadangan daya alternatif</p>
<p>(Biometrik) Pengenalan Suara menggunakan aktuator solenoid dan motor servo.</p>	<p>Menggunakan teknologi pengenalan suara yang memberikan tingkat keamanan dan akses yang lebih terkompuserisasi.</p> <p>Pembatasan akses hanya untuk personil yang berwenang, dan hanya dapat dioperasikan oleh staf yang telah mendaftarkan ID dan kata sandi.</p> <p>Solenoid cocok untuk aplikasi yang membutuhkan tindakan cepat, seperti membuka/menutup kunci pintu.</p> <p>Solenoid memiliki umur panjang dan tahan terhadap keausan yang</p>	<p>Tidak cocok apabila di tempat rumah yang bising (misalnya rumah di pinggir jalan raya banyak mobil motor lewat).</p> <p>Solenoid memerlukan pemeliharaan rutin untuk memastikan operasi yang lancar dan keamanan yang berkelanjutan.</p> <p>Solenoid harus dipastikan penggunaanya dengan tepat, karena jika digunakan dengan tidak benar, dapat menyebabkan pintu terkunci atau terbuka saat tidak seharusnya.</p> <p>Motor servo cenderung lebih mahal yang dapat mempengaruhi biaya</p>

Nama Solusi	Kelebihan	Kekurangan
	<p>berarti bahwa mereka dapat digunakan dalam jangka waktu yang lama.</p> <p>Kecepatan motor servo dapat diatur sesuai dengan kebutuhan, sehingga Anda dapat mengontrol sejauh mana pintu dibuka atau ditutup dengan presisi.</p> <p>Motor servo dapat dikendalikan dengan sangat akurat melalui perangkat elektronik, sehingga memungkinkan penggunaan berbagai metode otentikasi seperti kode PIN, kartu akses, atau pemindaian biometrik.</p>	<p>keseluruhan proyek pintu pintar.</p> <p>Motor servo lebih kompleks dalam hal perancangan dan penggunaan.</p>
<p>(Biometrik) Deteksi Wajah dengan solenoid sebagai aktuator</p>	<p>Solenoid cocok untuk aplikasi yang membutuhkan tindakan cepat, seperti membuka/menutup kunci pintu.</p> <p>Solenoid memiliki umur panjang dan tahan</p>	<p>Solenoid memerlukan pemeliharaan rutin untuk memastikan operasi yang lancar dan keamanan yang berkelanjutan.</p> <p>Solenoid harus dipastikan penggunaannya dengan tepat, karena jika</p>

Nama Solusi	Kelebihan	Kekurangan
	terhadap keausan yang berarti bahwa mereka dapat digunakan dalam jangka waktu yang lama.	digunakan dengan tidak benar, dapat menyebabkan pintu terkunci atau terbuka saat tidak seharusnya.
Solusi 2 (RFID)	Manfaat dari adanya RFID <i>Door Lock</i> ini adalah pengamanan secara fisik perangkat <i>data center</i> ini dilakukan secara menggunakan <i>smartphone</i> sehingga tidak perlu lagi membutuhkan kunci fisik untuk mengaksesnya. Dan juga untuk pengamanan pada <i>data center</i> ketika hendak dibuka.	Sistem kunci dan kunci, tanpa keraguan, adalah yang termurah di antara sistem keamanan dan tersedia untuk semua pengguna. Pembaca dan tag RFID sedikit lebih mahal namun juga memberikan keamanan yang cukup dibandingkan dengan sistem kunci dan kunci. Sebenarnya, biaya RFID tidak terlalu mahal jika harga kunci berkualitas baik diperhitungkan. Tetapi proyek ini, karena terdiri dari berbagai komponen, cukup lebih mahal daripada alternatif tradisional.
Solusi 3 (<i>Remote Bluetooth (MAC) and WiFi</i>)	<i>Bluetooth (MAC)</i> memungkinkan pengguna untuk membuka pintu dari	<i>Bluetooth (MAC)</i> , seperti jarak operasi yang terbatas dan rentan terhadap interferensi,

Nama Solusi	Kelebihan	Kekurangan
	<p>jarak jauh melalui aplikasi yang bekerja pada Android dan iOS. Admin dapat membuka pintu dengan melihat gambar pengunjung di pintu dan membukanya secara <i>remote</i> melalui aplikasi, tanpa harus berada di dekat pintu secara fisik.</p> <p><i>WiFi</i> memungkinkan Raspberry Pi untuk terhubung ke internet dan memberikan akses jarak jauh ke pemilik rumah melalui aplikasi <i>smartphone</i>. Ini memungkinkan sistem untuk memberikan akses <i>real time</i> dan fitur interaktif bagi pemilik, meningkatkan keamanan dan kenyamanan.</p>	<p>mungkin juga berlaku dalam konteks sistem ini. Selain itu, keamanan <i>Bluetooth</i> juga dapat menjadi perhatian, terutama terkait dengan kerentanan terhadap serangan peretasan. Oleh karena itu, perlu dilakukan evaluasi lebih lanjut terkait keamanan dan kehandalan teknologi <i>Bluetooth</i> dalam konteks implementasi sistem kunci pintar ini.</p> <p><i>WiFi</i> rentan terhadap interferensi, keterbatasan jangkauan sinyal, dan potensi kerentanan keamanan jika tidak diamankan dengan benar. Selain itu, ketergantungan pada <i>WiFi</i> untuk akses jarak jauh dapat menimbulkan tantangan di lingkungan dengan konektivitas <i>WiFi</i> yang tidak dapat diandalkan atau terbatas.</p>

Nama Solusi	Kelebihan	Kekurangan
		<p>Faktor-faktor ini berpotensi mempengaruhi keandalan dan aksesibilitas sistem kunci pintar. Penelitian dan pengembangan lebih lanjut mungkin diperlukan untuk mengatasi potensi keterbatasan ini dan memastikan ketahanan sistem dalam berbagai kondisi jaringan <i>WiFi</i>.</p>

1.5 Kesimpulan dan Ringkasan CD-1

Masalah yang dihadapi melibatkan beberapa aspek yang perlu dipertimbangkan dengan serius. Urgensi masalah terkait dengan keamanan dan privasi rumah membuat pengembangan dan penerapan teknologi ini menjadi penting. Selain itu, kompleksitas dalam pembuatan alat dan tantangan dalam kemudahan penggunaan juga harus diatasi. Dalam mempertimbangkan keterbatasan masalah yang sudah ada, solusi *smart lock door* menawarkan potensi yang signifikan untuk memenuhi kebutuhan pengguna, tetapi perlu pendekatan yang hati-hati dalam mengatasi hambatan teknis, ekonomi, dan penggunaan agar teknologi ini dapat memberikan manfaat maksimal dengan tanpa mengorbankan keamanan, kemudahan dan kenyamanan pengguna. Oleh karena itu, kesimpulannya adalah bahwa masalah ini sangat penting dan perlu penanganan yang cermat untuk memaksimalkan potensi solusi *smart lock door*.