

BAB II

TINJAUAN PUSTAKA

Seiring Perkembangan sistem keamanan rumah, kantor, dan fasilitas publik terus mengalami inovasi seiring kebutuhan akan akses pintu otomatis yang lebih praktis dan aman. Berbagai penelitian telah mengusulkan solusi berbasis teknologi *Internet of Things (IoT)*, *face recognition*, *RFID*, dan *push button* untuk membangun sistem *smart door lock* yang andal dan mudah diimplementasikan.

Setiawan et al. mengembangkan *prototipe* sistem keamanan rumah dengan *face recognition* berbasis *Raspberry Pi 4*, kamera, serta *library face_recognition* [1]. Sistem ini dapat mengenali wajah pengguna terdaftar secara *real-time* dan membuka pintu otomatis, menunjukkan keandalan serta efisiensi proses autentikasi pada perangkat *embedded*. Sutarti et al. juga merancang sistem keamanan rumah melalui pengenalan wajah menggunakan *webcam* dan *OpenCV* pada *Raspberry Pi*, menekankan pentingnya integrasi perangkat keras dan pustaka deteksi wajah agar sistem mampu memverifikasi identitas secara cepat dan akurat [2].

Boxey et al. memanfaatkan algoritma *deep learning* pada *face_recognition* untuk mengekstraksi fitur wajah, lalu membandingkan *encoding* wajah pengguna dengan *database*, sehingga hanya pengguna yang dikenali yang dapat membuka pintu otomatis [3]. Penelitian oleh Balogh et al. menggabungkan deteksi gerakan dan pengenalan wajah dalam ekosistem *IoT* dengan *Raspberry Pi* untuk menangkap video, mendeteksi pergerakan, dan mengenali wajah, menggunakan *Local Binary Pattern Histogram (LBPH)*, agar sistem tetap dapat mengenali pengguna meski dalam berbagai kondisi Cahaya [4]. Krishna et al. merancang sistem kunci pintu otomatis dengan *face recognition* berbasis *Raspberry Pi*, *relay*, dan notifikasi, di mana pintu hanya akan terbuka jika wajah terverifikasi valid [5]. Sistem ini terbukti

mampu meningkatkan keamanan dan meminimalisir potensi akses tidak sah.

Di sisi lain, penelitian terkait *push button* sebagai metode akses manual juga penting sebagai fitur cadangan pada *smart door lock*. Putra et al. membangun sistem keamanan pintu berbasis *IoT* dengan *Raspberry Pi*, *push button*, dan *relay* untuk membuka pintu secara otomatis [6]. Sistem ini juga dilengkapi notifikasi ke *telegram admin* setiap ada aktivitas akses, sehingga pengelola dapat memantau status pintu secara *real-time*. Kombinasi *push button* dan sistem notifikasi *telegram* terbukti memberikan kemudahan serta menambah aspek keamanan.

Teknologi *RFID* telah banyak digunakan untuk autentikasi akses pintu karena kecepatan dan kemudahannya. Soni et al. mengembangkan digital *door locking system* berbasis *RFID* dengan *Raspberry Pi* dan *RC522*, di mana *UID* kartu *RFID* berperan sebagai kunci utama [7]. Sistem memberikan kemudahan pengelolaan *user* dan mempercepat proses akses. Gindi et al. merancang *smart lock system* menggunakan *RFID* yang terintegrasi dengan indikator *LCD* dan *buzzer* untuk status akses, membuktikan efektivitas *RFID* dalam memproteksi akses pintu dan memudahkan *monitoring* [8]. Penelitian Hasan et al. memperkuat keamanan sistem *RFID* dengan menambah *push button* dan autentikasi berlapis menggunakan *Arduino Mega*, serta menyimpan data pengguna pada *server* agar lebih aman [9]. Evaluasi performa *RFID+IoT* juga dibahas Perdana et al. yang menegaskan bahwa sistem berbasis *RFID* mampu memberikan efisiensi dan kecepatan dalam otentikasi akses pintu pada *prototipe* keamanan [10].

Penelitian Rahman et al., Reddi et al., dan Taryudi et al. mendesain sistem keamanan rumah berbasis *IoT* yang mengintegrasikan *multi-sensor* seperti *face recognition*, *RFID*, *relay*, serta sistem *monitoring* dan pencatatan aktivitas akses. Pengiriman log

secara otomatis ke *server* atau *email*, serta penggunaan *relay* sebagai aktuator kunci pintu, menjadi fitur utama yang mendukung keamanan, fleksibilitas, dan transparansi system [11][12][13]. Hal serupa juga disampaikan oleh Osman et al. yang mengimplementasikan sistem notifikasi *real-time* menggunakan *telegram bot* dan *email* untuk mengawasi akses secara jarak jauh, dengan biaya murah dan integrasi yang mudah pada perangkat *IoT* [14].

Osman et al. dan Halim et al. meski meneliti sistem notifikasi berbasis *IoT* untuk kasus deteksi kebakaran dan *monitoring* sungai, namun menegaskan bahwa teknologi *telegram bot API* sangat efektif sebagai media pengiriman pesan instan ke pengguna karena memiliki *delay* yang sangat singkat, sangat cocok juga diterapkan pada sistem keamanan rumah atau *smart lock* [15][16]. Shingala dan Patel serta Fatima dan Gadgay juga membahas pentingnya sistem notifikasi berbasis *SMS*, *email*, dan *IoT* untuk meningkatkan keamanan dan respons terhadap aktivitas akses [17][18].

Dari sisi otentikasi *multi-faktor*, Rivera et al. serta Desai et al. mengembangkan sistem kunci pintu otomatis berbasis *Arduino* dan *IoT* yang menggabungkan beberapa metode autentikasi (seperti *face recognition*, *RFID*, *password*, atau *OTP*), dan menyoroti peningkatan keamanan dengan pendekatan tersebut [19][20]. Veijalainen dan Karlsson secara khusus mengevaluasi aspek keamanan dan reliabilitas pada *smart door lock*, menekankan pentingnya integrasi log aktivitas, notifikasi, dan audit sistem untuk mengurangi potensi risiko keamanan [21].

Studi oleh Derbali menegaskan pentingnya pengembangan *smart door lock* dengan integrasi *multi*-autentikasi, sistem log otomatis, *monitoring real-time*, serta efisiensi biaya dan kemudahan pemasangan pada perangkat *IoT* [22]. Kesimpulan penelitian tersebut mendukung temuan-temuan sebelumnya bahwa kombinasi *face recognition*, *RFID*,

push button, *relay*, notifikasi, dan *logging* otomatis pada *Raspberry Pi* dapat membentuk sistem *smart door lock* yang aman, efisien, dan mudah diadopsi pada berbagai skenario penggunaan, baik skala rumah, kost, maupun institusi pendidikan.

Seiring berkembangnya tantangan keamanan pada sistem *IoT*, beberapa studi terbaru mulai menekankan pentingnya perlindungan data biometrik dan *RFID* melalui teknik enkripsi. Wang et al. membahas secara mendalam peran enkripsi pada penyimpanan dan transmisi *template* biometrik (seperti *face encoding*) dalam sistem *smart door lock*, yang terbukti efektif untuk mencegah penyalahgunaan data pengguna [23]. Selain itu, Liu et al. mengembangkan protokol otentikasi *RFID* modern berbasis algoritma enkripsi matriks variabel, yang mampu meningkatkan keamanan dan efisiensi penyimpanan data pada lingkungan *IoT* [24]. Penambahan mekanisme enkripsi ini menjadi salah satu aspek penting dalam mendukung perlindungan data sensitif pada sistem keamanan akses fisik.

Secara keseluruhan, penelitian-penelitian di atas menjadi landasan penting bagi pengembangan sistem *smart door lock* pada tugas akhir ini, dan membuktikan bahwa integrasi teknologi *face recognition*, *RFID*, *push button*, *relay*, notifikasi *telegram/email*, serta *logging* akses otomatis merupakan *best practice* yang dapat diimplementasikan untuk menciptakan solusi keamanan akses fisik yang modern, efektif, dan terjangkau.

Berikut merupakan tabel perbandingan dengan penelitian-penelitian terdahulu:

Tabel 2. 1 Tabel Perbandingan

No	Penulis	Metode Autentikasi	Platform	Notifikasi	Log Akses	Kelebihan	Kekurangan
1	Setiawan et al.	<i>Face Recognition</i>	<i>RPi</i>	Tidak	Tidak	Implementasi lokal <i>face recog</i>	Tidak ada notifikasi/log
2	Putra et al.	<i>Push Button</i> (manual)	<i>RPi + IoT</i>	Tidak	Tidak	Kontrol <i>IoT</i> sederhana	Tidak aman dan konvensional
3	Sutarti et al.	<i>Face Recognition</i>	<i>RPi + OpenCV</i>	Tidak	Tidak	<i>OpenCV & webcam</i>	Tanpa sistem log/notif
4	Boxey et al.	<i>Face Recognition</i>	<i>RPi + Python</i>	Tidak	Tidak	Implementasi <i>real-time</i> sederhana	Tanpa sistem log
5	Balogh et al.	<i>Face Recognition</i>	<i>RPi + IoT</i>	Tidak	Tidak	Integrasi dengan <i>IoT</i>	Fokus ke <i>framework</i> , bukan sistem
6	Bhoite & Patil	<i>Face Recognition</i>	<i>RPi</i>	Tidak	Tidak	Penguncian otomatis	Tidak ada fitur tambahan
7	Soni et al.	<i>RFID</i>	<i>Arduino</i>	Tidak	Tidak	<i>RFID</i> cepat dan efisien	Tanpa biometrik/notifikasi
8	Gindi et al.	<i>RFID</i>	<i>RPi</i>	Tidak	Tidak	<i>Smart lock RFID</i>	Tidak <i>real-time</i> /log
9	Hasan et al.	<i>RFID</i>	Polsri + <i>RPi</i>	Tidak	Tidak	<i>RFID</i> otomatisasi	Tidak ada notifikasi/log
10	Rahman et al.	Sensor <i>IoT</i>	<i>IoT</i> (ESP)	Tidak	Tidak	Otomatisasi berbasis <i>IoT</i>	Tidak autentikasi spesifik
11	Kousalya et al.	Sensor <i>IoT</i>	<i>IoT</i>	Tidak	Tidak	<i>Smart home</i>	Tidak autentikasi pengguna
12	Taryudi et al.	<i>IoT</i>	<i>RPi</i>	Tidak	Tidak	<i>Monitoring</i> sistem	Tidak berbasis autentikasi pengguna
13	Osman et al.	<i>IoT + telegram</i>	ESP	Ya	Tidak	Notifikasi <i>telegram</i>	Tidak autentikasi pengguna
14	Halim et al.	Sensor + <i>telegram</i>	<i>IoT</i>	Ya	Tidak	<i>Monitoring</i> sungai via <i>telegram</i>	Bukan sistem keamanan pintu

No	Penulis	Metode Autentikasi	Platform	Notifikasi	Log Akses	Kelebihan	Kekurangan
15	Prasad et al.	Sensor + <i>telegram</i>	<i>IoT</i>	Ya	Tidak	Fire notif via <i>telegram</i>	Bukan sistem akses
16	Shingala & Patel	<i>RFID</i> + <i>Email</i>	<i>IoT</i>	Ya (<i>Email</i>)	Tidak	Sistem alert <i>email</i>	Tidak <i>real-time</i> /notif langsung
17	Fatima & Gadgay	<i>IoT</i> + <i>SMS/Email</i>	<i>IoT</i>	Ya	Tidak	Sistem interaktif	Tidak autentikasi pengguna
18	Rivera et al.	<i>Face</i> + <i>RFID</i> (MFA)	<i>Arduino</i>	Tidak	Tidak	Multi-Factor	Kompleks dan mahal
19	Desai et al.	<i>Face</i> + <i>RFID</i> (Multi-Modal)	<i>Keyless</i>	Tidak	Tidak	Multi-modal authentication	Tidak <i>real-time</i>
20	Veijalainen & Karlsson	Evaluasi Keamanan	<i>Smart Lock IoT</i>	Ya	Tidak	Uji STRIDE/DREAD	Tidak ada implementasi
21	Perdana et al.	<i>RFID</i>	<i>IoT</i>	Tidak	Tidak	Uji performa sistem <i>RFID</i>	Tidak biometrik/notif/log
22	Derbali	<i>RFID</i> , PIN Keypad, <i>Bluetooth</i> , 2FA, Web	<i>RPi</i> + <i>IoT</i>	Ya	Ya	Multi-autentikasi, remote <i>unlock</i> via <i>web</i> , UI <i>web</i> , log akses, <i>user</i> management	Tidak ada biometrik, <i>OTP</i> terbatas, butuh daya tambahan
23	Penelitian ini	<i>Face</i> / <i>RFID</i> (alternatif)	<i>RPi</i> + <i>SQLite</i>	Ya	Ya	<i>Real-time</i> , <i>telegram</i> , <i>Email</i> , log otomatis	Belum ada enkripsi data

Berdasarkan hasil tinjauan pustaka, kebaruan utama dari penelitian ini terletak pada integrasi tiga metode autentikasi, yaitu *face recognition* berbasis *deep learning*, *RFID*, dan *push button* sebagai manual *override*, yang diimplementasikan secara lokal pada platform *Raspberry Pi*. Selain itu, sistem yang dikembangkan telah dilengkapi dengan fitur notifikasi *real-time* melalui

Telegram dan pengiriman log aktivitas otomatis ke *email admin*, sehingga *monitoring* akses dapat dilakukan dengan lebih efisien. Penerapan enkripsi pada *database* biometrik (*face encoding*) dan data *RFID* juga menjadi pembeda penting, karena mampu meningkatkan perlindungan data pengguna dari risiko penyalahgunaan. Kombinasi fitur-fitur ini belum ditemukan secara lengkap pada penelitian terdahulu, sehingga sistem *Smart Door Lock* yang dibangun pada penelitian ini memiliki keunggulan dari sisi keamanan, fleksibilitas, dan kemudahan *monitoring* akses pintu secara praktis dan modern.

