

BAB I

PENDAHULUAN

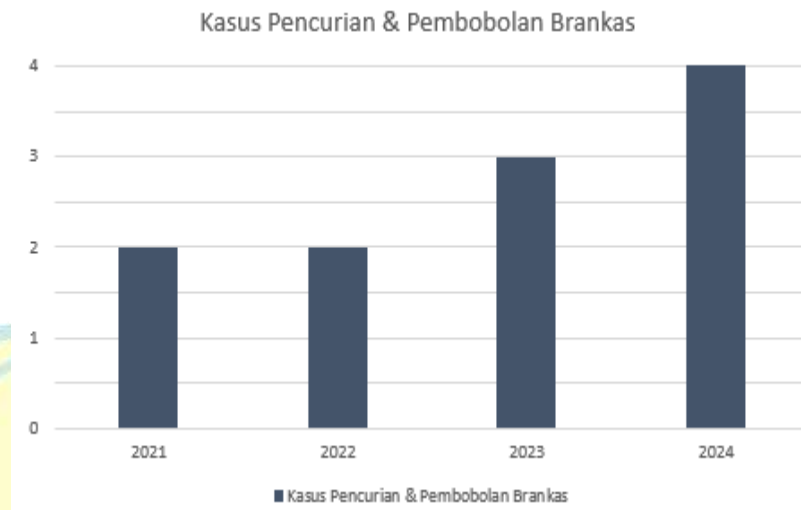
1.1. Latar Belakang Masalah

Kemajuan teknologi digital telah berkembang sangat pesat dan memberikan dampak pada berbagai aspek kehidupan, termasuk dalam bidang sistem keamanan. Perkembangan tersebut mendorong meningkatnya kebutuhan masyarakat terhadap perlindungan data maupun barang berharga agar terhindar dari tindakan penyalahgunaan oleh pihak yang tidak bertanggung jawab (Junaedi, 2025). Salah satu media penyimpanan yang banyak digunakan masyarakat untuk menyimpan uang, dokumen penting, perhiasan, maupun barang berharga lainnya adalah brankas karena dinilai memiliki tingkat keamanan yang baik serta tidak memerlukan ruang penyimpanan yang besar Lumbanraja *et al.* (2023). Lumbanraja *et al.* (2023) menjelaskan bahwa brankas yang masih menggunakan sistem penguncian konvensional masih memiliki keterbatasan pada mekanisme autentikasi sehingga memerlukan sistem keamanan tambahan pada sisi akses elektronik.

Menurut Suradi *et al.* (2024), sebagian besar brankas konvensional masih menggunakan sistem penguncian mekanik, kombinasi angka, maupun satu metode autentikasi sebagai mekanisme pembukaan pintu. Sistem tersebut dinilai kurang praktis karena belum menerapkan autentikasi berlapis maupun pemantauan akses secara jarak jauh. Oleh karena itu, diperlukan pengembangan sistem keamanan tambahan yang mampu meningkatkan keamanan proses akses tanpa mengubah mekanisme maupun ketahanan fisik brankas itu sendiri.

Selain faktor keamanan, kondisi sosial dan ekonomi juga dapat menjadi salah satu penyebab meningkatnya tindak kriminalitas, termasuk pencurian (Wilfred, 2025). Namun demikian, penelitian ini tidak berfokus pada faktor penyebab kriminalitas, melainkan pada

pengembangan sistem keamanan tambahan pada sisi akses elektronik brankas melalui autentikasi berlapis dan pemantauan berbasis *Internet of Things* (IoT).



Gambar 1.1. Grafik kasus pencurian dan pembobolan Brankas

Berdasarkan dari berbagai rekap kasus kumpulan berita, yang dikutip dari (Kurniati, 2021), (Debora, 2021), (Susanti, 2022), (Bernardi, 2022), (Polres Jogja, 2023), (Pasaribu, 2023), (NusaBali, 2024), (Amaludin, 2024), dan (Maulana, 2024).

Gambar 1.1 menunjukkan rekap kasus pencurian dan pembobolan brankas yang dihimpun dari berbagai sumber pemberitaan di Indonesia, yaitu (Kurniati, 2021), (Debora, 2021), (Susanti, 2022), (Bernardi, 2022), (Polres Jogja, 2023), (Pasaribu, 2023), (NusaBali, 2024), (Amaludin, 2024), dan (Maulana, 2024). Rekap tersebut bukan merupakan data statistik resmi nasional, melainkan gambaran bahwa kasus pencurian dan pembobolan brankas masih sering diberitakan pada beberapa tahun terakhir sehingga keamanan akses terhadap brankas masih menjadi perhatian.

Berdasarkan berbagai kasus tersebut diketahui bahwa pelaku pencurian tidak selalu berasal dari orang yang tidak dikenal, tetapi juga dapat dilakukan oleh orang yang telah memahami kondisi lingkungan maupun mekanisme penggunaan brankas. Kondisi tersebut memungkinkan pelaku memperoleh informasi mengenai sistem penguncian sehingga proses pembobolan menjadi lebih mudah

dilakukan. Selain itu, sebagian besar brankas konvensional belum memiliki dokumentasi visual maupun sistem pemantauan ketika proses pembukaan brankas berlangsung, sehingga pemilik tidak memperoleh informasi mengenai aktivitas akses terhadap brankas.

Perkembangan teknologi elektronika dan mikrokontroler telah mendorong lahirnya berbagai inovasi sistem keamanan yang mampu meningkatkan perlindungan terhadap barang berharga. Pemanfaatan teknologi modern memungkinkan pengguna memperoleh kemudahan dalam melakukan pengendalian akses serta pemantauan kondisi brankas secara lebih fleksibel. Oleh karena itu, penerapan sistem keamanan berbasis mikrokontroler dan *Internet of Things* menjadi salah satu alternatif untuk mendukung mekanisme penguncian elektronik pada brankas (Ashar & Saputra, 2021).

Zurairah *et al.* (2022) mengembangkan sistem keamanan brankas menggunakan metode *One Time Password* (OTP). Hasil penelitian menunjukkan bahwa penggunaan OTP lebih aman dibandingkan kombinasi angka mekanik karena data autentikasi disimpan pada mikrokontroler. Akan tetapi, sistem tersebut masih menggunakan satu metode autentikasi sehingga *password* tetap berpotensi diketahui oleh pihak lain.

Tata *et al.* (2025) mengembangkan sistem keamanan brankas menggunakan autentikasi sidik jari (*fingerprint*). Hasil penelitian menunjukkan bahwa hanya sidik jari yang telah terdaftar yang dapat membuka brankas. Namun demikian, sensor sidik jari masih memiliki keterbatasan ketika kondisi kulit pengguna mengalami perubahan, seperti terkelupas atau berganti kulit, sehingga proses autentikasi dapat mengalami kegagalan.

Rizaldi (2022) mengembangkan sistem keamanan brankas berbasis *Internet of Things* dengan autentikasi sidik jari dan pemantauan melalui jaringan *internet*. Sistem mampu mengirimkan informasi kondisi brankas melalui media berbasis *web*. Akan tetapi, autentikasi masih bergantung pada sensor sidik jari, sedangkan

Internet of Things hanya dimanfaatkan sebagai media pemantauan kondisi brankas.

Berdasarkan penelitian-penelitian terdahulu, dapat diketahui bahwa sistem keamanan brankas telah dikembangkan menggunakan password, sidik jari, RFID tunggal, maupun *Internet of Things* sebagai media pemantauan. Namun demikian, penelitian-penelitian tersebut umumnya masih menggunakan satu metode autentikasi utama atau belum mengintegrasikan autentikasi dengan dokumentasi visual dan pemantauan secara terpadu. Belum adanya penelitian yang menggabungkan autentikasi menggunakan kartu MIFARE, autentikasi perintah suara, pengambilan gambar pengguna, pengiriman notifikasi melalui Bot Telegram, serta pengendalian *solenoid door lock* dalam satu sistem autentikasi berlapis. Kondisi tersebut menjadi dasar dilakukannya penelitian ini.

Penelitian ini mengusulkan pengembangan prototipe sistem keamanan tambahan pada brankas mini berbasis *Internet of Things* (IoT) dengan menerapkan autentikasi berlapis. Tahap autentikasi pertama dilakukan menggunakan modul PN532 berbasis *Near Field Communication* (NFC). Pada proses autentikasi, modul PN532 membaca UID kartu MIFARE sebagai identitas kartu serta membaca data autentikasi yang tersimpan pada Blok 4 kartu MIFARE. Selanjutnya, Arduino Mega 2560 melakukan proses dekripsi sederhana menggunakan algoritma XOR terhadap data autentikasi tersebut dan mencocokkannya dengan data autentikasi yang tersimpan pada sistem. Keberhasilan proses pencocokan data autentikasi menjadi dasar autentikasi pertama, sedangkan UID hanya digunakan sebagai informasi identitas kartu pada proses pembacaan dan tidak digunakan sebagai dasar pembukaan brankas.

Setelah Arduino Mega 2560 berhasil memverifikasi data autentikasi kartu, sistem mengaktifkan ESP32-CAM untuk mengambil gambar pengguna dan mengirimkan gambar beserta status akses melalui Bot Telegram sebagai dokumentasi aktivitas akses

secara jarak jauh. Setelah proses dokumentasi selesai, sistem mengaktifkan modul *Voice Recognition V3* untuk mengenali perintah suara yang telah didaftarkan sebagai autentikasi kedua. Relay akan diaktifkan sehingga *solenoid door lock* membuka pintu brankas hanya apabila autentikasi kartu dan autentikasi perintah suara berhasil dilakukan.

Penerapan autentikasi berlapis pada penelitian ini tidak dimaksudkan untuk menyatakan bahwa sistem mampu mencegah atau mengurangi kasus pembobolan brankas secara umum, melainkan berpotensi menjadi sistem keamanan tambahan pada brankas mini melalui kombinasi autentikasi kartu MIFARE, pengenalan perintah suara terdaftar, dokumentasi visual menggunakan ESP32-CAM, serta pengiriman notifikasi melalui Bot Telegram. Penelitian ini hanya berfokus pada pengujian kinerja sistem penguncian elektronik dan pemantauan akses, bukan pada pengujian ketahanan fisik brankas terhadap pembobolan secara paksa.

Berdasarkan uraian latar belakang tersebut, penelitian ini dilakukan untuk mengembangkan prototipe sistem pengunci brankas mini berbasis *Internet of Things (IoT)* yang menerapkan autentikasi berlapis sebagai sistem keamanan tambahan. Prototipe ini mengintegrasikan modul PN532 sebagai pembaca kartu MIFARE, Arduino Mega 2560 sebagai pengendali utama sekaligus pelaksana dekripsi XOR sederhana dan pencocokan data autentikasi, *Voice Recognition V3* sebagai pengenalan perintah suara terdaftar, ESP32-CAM sebagai perangkat dokumentasi akses, Bot Telegram sebagai media pengiriman notifikasi, serta *solenoid door lock* sebagai aktuator pengunci elektronik. Pada implementasi program yang dikembangkan, proses pengambilan gambar dan pengiriman notifikasi hanya dilakukan ketika ESP32-CAM berhasil terhubung ke jaringan *internet*.

Apabila koneksi *internet* terputus, autentikasi lokal tetap dapat dilakukan sehingga brankas tetap dapat diakses sesuai hak pengguna,

namun fungsi dokumentasi dan monitoring melalui Bot Telegram tidak berjalan. Kondisi tersebut merupakan keterbatasan dari rancangan program pada penelitian ini. Selanjutnya, penelitian ini berfokus pada pengujian kinerja setiap modul dan integrasi sistem secara keseluruhan untuk mengetahui kemampuan sistem dalam menjalankan autentikasi, penguncian elektronik, dokumentasi akses, serta pengiriman notifikasi sesuai dengan rancangan yang telah ditetapkan.

1.2. Identifikasi Masalah

Berdasarkan latar belakang masalah yang telah dijelaskan serta diuraikan di atas, maka dapat diidentifikasi permasalahan sebagai berikut:

1. Sistem keamanan brankas konvensional belum dilengkapi dengan autentikasi berlapis sebagai mekanisme verifikasi pengguna sebelum proses pembukaan brankas dilakukan.
2. Sistem keamanan brankas konvensional belum memanfaatkan teknologi *Internet of Things* sebagai pemantauan jarak jauh dengan memberikan notifikasi atau dokumentasi gambar ketika ada akses.
3. Sistem penguncian brankas yang menggunakan kunci manual, kode, atau *keypad* masih berisiko diketahui, dipinjam, atau disalahgunakan oleh pihak lain.
4. Belum diketahui kinerja integrasi modul PN532, *Voice Recognition V3*, ESP32-CAM, Telegram, dan *solenoid door lock* ketika diimplementasikan dalam satu prototipe sistem pengunci brankas mini berbasis *Internet of Things* (IoT).

1.3. Pembatasan Masalah

Penelitian, dibatasi dalam lingkup sebagai berikut:

1. Penelitian hanya dilakukan pada prototipe sistem pengunci brankas mini berbasis *Internet of Things* (IoT) dengan ukuran 0.20 m × 0.20 m × 0.31 m.
2. Sistem menggunakan *power supply* DC sebagai sumber catu daya utama untuk menyuplai seluruh modul elektronik dan belum dilengkapi dengan

baterai cadangan (*backup power supply*) sebagai sumber daya ketika terjadi pemadaman listrik.

3. Penelitian belum menguji secara mendalam kinerja sistem pada kondisi kehilangan sumber listrik, seperti saat terjadi pemadaman listrik atau ketika kabel *power supply* dilepas, sehingga aspek kontinuitas operasi sistem di luar kondisi pengujian tidak dibahas.
4. Modul *Voice Recognition V3* hanya digunakan untuk mengenali satu perintah suara yang telah direkam (*voice command*) sebagai syarat autentikasi, bukan untuk melakukan identifikasi biometrik atau verifikasi identitas pengguna berdasarkan karakteristik suara.
5. Pengujian modul *Voice Recognition V3* dilakukan pada kondisi lingkungan dengan tingkat kebisingan (*noise*) rendah dan tinggi sesuai skenario pengujian pada Bab III dan Bab IV.
6. Modul ESP32-CAM hanya digunakan untuk mengambil gambar saat proses akses brankas dan mengirimkan gambar tersebut melalui Telegram, bukan untuk melakukan pengenalan wajah (*face recognition*) maupun verifikasi identitas pengguna secara otomatis.
7. Aplikasi Telegram hanya digunakan sebagai media pengiriman notifikasi dan dokumentasi gambar hasil akses brankas, bukan sebagai sistem pengendali utama maupun basis data (*cloud database*).
8. Pada penelitian ini, sesuai dengan implementasi program yang dikembangkan, ESP32-CAM hanya menjalankan proses pengambilan gambar, dokumentasi akses, dan pengiriman notifikasi ke Bot Telegram ketika telah berhasil terhubung ke jaringan *internet*. Oleh karena itu, apabila koneksi *internet* terputus atau tidak tersedia, sistem tetap dapat melakukan autentikasi lokal dan membuka brankas sesuai hasil autentikasi, namun fungsi pengambilan gambar, dokumentasi akses, dan *monitoring* melalui Bot Telegram tidak dijalankan. Kondisi tersebut merupakan batasan implementasi program, bukan keterbatasan perangkat ESP32-CAM.
9. Penelitian menggunakan *solenoid door lock* bawaan pada brankas mini dengan tipe *Normally Locked* sebagai aktuator elektronik untuk membuka

dan mengunci pintu berdasarkan hasil autentikasi sistem. Penelitian ini hanya menguji fungsi buka dan kunci *solenoid* sebagai bagian dari integrasi sistem, bukan menganalisis karakteristik maupun performa mekanik *solenoid* secara khusus, serta tidak menguji ketahanan fisik brankas terhadap pembobolan secara paksa.

10. Penelitian ini tidak membahas aspek keamanan siber, seperti pengamanan token Telegram, maupun enkripsi komunikasi data secara mendalam.
11. Pengujian penelitian difokuskan pada kinerja setiap modul serta integrasi sistem secara keseluruhan dalam menjalankan proses autentikasi, penguncian elektronik, dokumentasi akses, dan pengiriman notifikasi.

1.4. Perumusan Masalah

Berdasarkan penjelasan latar belakang, identifikasi masalah, dan batasan masalah yang telah diuraikan maka didapatkan rumusan masalah yaitu:

Bagaimana mengembangkan prototipe *smart* sistem brankas mini berbasis *Internet of Things* dengan autentikasi berlapis menggunakan kartu MIFARE dan *Voice Recognition V3* sebagai sistem keamanan tambahan?

1.5. Tujuan Penelitian

Berdasarkan rumusan masalah yang telah ditetapkan, tujuan penelitian ini adalah sebagai berikut:

1. Mengembangkan prototipe sistem pengunci brankas mini berbasis *Internet of Things* (IoT) yang menerapkan autentikasi berlapis, menggunakan modul PN532, *Voice Recognition V3*, ESP32-CAM, Telegram, dan *solenoid door lock*.
2. Menguji kinerja prototipe, secara keseluruhan untuk mengetahui kemampuan sistem dalam menjalankan proses autentikasi, penguncian elektronik, dokumentasi akses, dan pengiriman notifikasi sesuai dengan rancangan yang telah ditetapkan.

1.6. Manfaat Penelitian

Penelitian diharapkan dapat bermanfaat secara teoretis maupun praktis sebagai berikut:

1. Manfaat teoretis

Hasil penelitian ini diharapkan dapat menjadi referensi ilmiah dalam pengembangan sistem pengunci brankas mini berbasis *Internet of Things* (IoT) dengan menerapkan autentikasi berlapis. Selain itu, penelitian ini diharapkan dapat memberikan kontribusi terhadap pengembangan ilmu pengetahuan di bidang sistem tertanam (*embedded system*), mikrokontroler, sensor, aktuator, dan teknologi *Internet of Things*.

2. Manfaat Praktis

a. Bagi Pengguna

Penelitian ini diharapkan dapat menjadi alternatif sistem keamanan tambahan pada brankas mini melalui penerapan autentikasi berlapis, dokumentasi akses menggunakan ESP32-CAM, serta pengiriman notifikasi melalui Telegram.

b. Bagi Mahasiswa atau Peneliti

Penelitian ini diharapkan dapat menjadi sarana penerapan dan pengembangan ilmu pengetahuan di bidang mikrokontroler, komunikasi serial, sensor, aktuator, serta teknologi *Internet of Things* dalam membangun suatu sistem keamanan elektronik.

c. Bagi Program Studi

Penelitian ini diharapkan dapat menjadi referensi pembelajaran maupun bahan pengembangan proyek elektronika berbasis sistem tertanam (*embedded system*), khususnya pada mata kuliah atau penelitian yang berkaitan dengan mikrokontroler dan *Internet of Things*.

d. Bagi Penelitian Selanjutnya

Hasil penelitian ini diharapkan dapat menjadi dasar pengembangan penelitian berikutnya, seperti penerapan teknologi pengenalan wajah (*face recognition*), sistem pencatatan riwayat akses (*access log*), integrasi basis data, penggunaan catu daya cadangan (*backup power supply*), penggunaan sensor getar, *alarm*, dan algoritma enkripsi yang lebih kuat, serta peningkatan aspek keamanan jaringan dan komunikasi data.