

## Sistem Pengunci Brankas Digital dengan Password Otomatis Menggunakan Proteus

Muhammad Agil Wahyudy <sup>1\*</sup>, Dwi Titi Maesaroh <sup>2</sup>, Rihartanto <sup>3</sup>

<sup>1,2,3</sup>Teknologi Informasi, Politeknik Negeri Samarinda

Jl. DR. Ciptomangunkusumo, Kampus Gunung Lipan, Samarinda, Kalimantan Timur, Indonesia  
75131

email : [infinityblame759@gmail.com](mailto:infinityblame759@gmail.com) <sup>1</sup>, [dwititi.maesaroh@polnes.ac.id](mailto:dwititi.maesaroh@polnes.ac.id) <sup>2</sup>, [rihartanto@polnes.ac.id](mailto:rihartanto@polnes.ac.id) <sup>3</sup>

\*Penulis Korespondensi: Muhammad Agil Wahyudy

**Abstract:** Safe security is an important aspect in protecting valuable items from theft and unauthorized access. Conventional locking systems that still use mechanical keys have several weaknesses, such as being easily duplicated and vulnerable to damage, therefore a more effective and modern security system is needed. This study aims to design and simulate a digital safe locking system with an automatic password using Proteus software based on the ATmega8535 microcontroller. The system is designed using a 4×4 matrix keypad as a password input device, a 16×2 LCD as an information display, LED and speaker as system status indicators, and ATmega8535 as the main controller for the password authentication process. The research method includes circuit design, microcontroller programming, system simulation using Proteus, and functional testing of input and output devices. The test results show that the system is able to read password input through the keypad, display information on the LCD, and provide automatic responses in the form of access granted when the password is correct and warnings when incorrect passwords are entered. The system also works stably in the authentication and output control processes. Based on the results, the designed digital safe locking system can be used as a more practical, automatic, and effective digital security solution compared to conventional locking systems.

**Keywords:** safe lock; ATmega8535; 4×4 matrix keypad; 16×2 LCD; Proteus; automatic security system

**Abstrak:** Keamanan brankas merupakan salah satu aspek penting dalam melindungi barang berharga dari risiko pencurian maupun akses oleh pihak yang tidak berwenang. Sistem pengunci konvensional yang masih menggunakan kunci mekanik memiliki kelemahan seperti mudah diduplikasi dan rentan terhadap kerusakan, sehingga diperlukan sistem pengamanan yang lebih efektif dan modern. Penelitian ini bertujuan untuk merancang dan mensimulasikan sistem pengunci brankas digital dengan password otomatis menggunakan aplikasi Proteus berbasis mikrokontroler ATmega8535. Sistem dirancang menggunakan keypad matriks 4×4 sebagai media input password, LCD 16×2 sebagai media tampilan informasi, LED dan *speaker* sebagai indikator status sistem, serta ATmega8535 sebagai pusat pengendali proses autentikasi password. Metode penelitian dilakukan melalui tahap perancangan rangkaian, pemrograman mikrokontroler, simulasi sistem pada Proteus, serta pengujian fungsi input dan output perangkat. Hasil pengujian menunjukkan bahwa sistem mampu membaca input password melalui keypad, menampilkan informasi pada LCD, serta memberikan respon otomatis berupa akses terbuka ketika password benar dan peringatan ketika password salah dimasukkan. Sistem juga mampu bekerja secara stabil dalam proses autentikasi dan pengendalian output. Berdasarkan hasil penelitian, sistem pengunci brankas digital yang dirancang dapat menjadi solusi keamanan berbasis digital yang lebih praktis, otomatis, dan efektif dibandingkan sistem pengunci konvensional.

**Kata kunci:** pengunci brankas; ATmega8535; keypad matriks 4×4; LCD 16×2; Proteus; sistem keamanan otomatis

Diterima: 12 Mei 2026

Direvisi: 20 Mei 2026

Diterima: 25 Mei 2026

Diterbitkan: 31 Mei 2026

Versi sekarang: Mei 2026



Hak cipta: © 2025 oleh penulis.  
Diserahkan untuk kemungkinan  
publikasi akses terbuka  
berdasarkan syarat dan ketentuan  
lisensi Creative Commons  
Attribution (CC BY SA) (  
<https://creativecommons.org/licenses/by-sa/4.0/>)

## 1. Pendahuluan

Perkembangan teknologi digital mendorong meningkatnya kebutuhan masyarakat terhadap sistem keamanan yang lebih modern dan efisien, khususnya pada media penyimpanan seperti brankas. Sistem penguncian mekanik konvensional yang masih menggunakan kunci fisik memiliki kelemahan, seperti mudah diduplikasi, berisiko hilang, serta rentan dibobol menggunakan teknik tertentu. Berdasarkan penelitian Khairul Agus Rizal dkk., sistem keamanan brankas digital dapat ditingkatkan dengan memanfaatkan mikrokontroler ATmega16 sebagai pusat pengendali yang terhubung dengan keypad 4x4 sebagai input password, LCD sebagai media tampilan, sensor *fingerprint* untuk autentikasi sidik jari, serta solenoid sebagai pengunci otomatis pintu brankas. Sistem bekerja dengan proses verifikasi password 4 digit dan sidik jari yang telah didaftarkan sebelumnya sehingga akses hanya dapat dilakukan oleh pengguna yang terotorisasi. Selain itu, penelitian tersebut menjelaskan bahwa penggunaan sensor *fingerprint* memiliki tingkat keberhasilan pembacaan sebesar 80% dari 10 kali pengujian, sedangkan kesalahan pembacaan terjadi akibat posisi jari yang kurang tepat saat proses *scanning* [1]. Oleh karena itu, penelitian “Sistem Pengunci Brankas Digital dengan Password Otomatis Menggunakan Proteus” dilakukan untuk merancang sistem keamanan berbasis simulasi Proteus yang mampu meningkatkan keamanan dan efektivitas penguncian brankas secara digital menggunakan kombinasi password otomatis dan mikrokontroler.

Mikrokontroler merupakan teknologi yang banyak digunakan dalam sistem otomatisasi dan keamanan karena mampu mengendalikan proses input dan output secara terprogram. Pada penelitian ini, digunakan mikrokontroler ATmega8535 sebagai pusat pengendali utama sistem keamanan brankas digital. Mikrokontroler ini dipilih karena memiliki kemampuan pemrosesan data yang stabil, mudah diprogram, serta mendukung integrasi dengan berbagai perangkat input dan output. Sistem dirancang menggunakan keypad matriks 4x4 sebagai media input password untuk proses autentikasi pengguna, sedangkan LCD 16x2 digunakan untuk menampilkan status sistem dan informasi akses. LED digunakan sebagai indikator kondisi sistem, sementara *speaker* atau *buzzer* berfungsi sebagai alarm ketika password yang dimasukkan salah [2]. Konsep keamanan digital ini sejalan dengan penelitian yang dilakukan oleh Sri Hartanto, dan rekan-rekannya yang menjelaskan bahwa sistem keamanan brankas berbasis mikrokontroler mampu meningkatkan keamanan akses dibandingkan kunci mekanik konvensional karena proses autentikasi dilakukan secara digital dan hanya pengguna tertentu yang dapat membuka brankas. Penelitian tersebut juga menjelaskan bahwa sistem keamanan modern dapat meningkatkan efisiensi serta meminimalkan risiko akses ilegal melalui penggunaan teknologi elektronik dan otomatisasi pada sistem pengunci brankas.

Perancangan sistem pengunci brankas digital pada penelitian ini, dilakukan menggunakan aplikasi Proteus sebagai media simulasi rangkaian elektronika dan pengujian program mikrokontroler sebelum diterapkan pada perangkat keras nyata. Penggunaan simulasi ini bertujuan untuk mempermudah proses perancangan, pengujian fungsi komponen, serta analisis kerja sistem keamanan secara keseluruhan. Melalui simulasi Proteus, komponen seperti mikrokontroler ATmega8535, keypad matriks 4x4, LCD 16x2, LED, dan *speaker* dapat diintegrasikan dalam satu rangkaian virtual sehingga proses pengujian sistem menjadi lebih efektif dan efisien. Sistem dirancang agar mampu membaca input password dari keypad, memproses data autentikasi menggunakan mikrokontroler, kemudian memberikan respon otomatis sesuai kondisi password yang dimasukkan pengguna. Jika password benar maka akses brankas akan terbuka, sedangkan jika password salah maka sistem memberikan peringatan melalui LED dan *speaker* sebagai indikator keamanan [3]. Konsep sistem keamanan digital ini didukung oleh penelitian Zoggy Adam Pangaribuan yang menjelaskan bahwa sistem keamanan brankas berbasis mikrokontroler mampu meningkatkan keamanan akses melalui proses autentikasi digital dan pemberian notifikasi otomatis pada sistem keamanan modern. Selain itu, penggunaan simulasi sebelum implementasi perangkat keras dapat membantu meminimalkan kesalahan perancangan dan meningkatkan efisiensi pengembangan sistem keamanan berbasis digital.

Penelitian ini memiliki kontribusi dalam pengembangan sistem pengunci brankas digital berbasis mikrokontroler ATmega8535 yang dirancang dan diuji melalui simulasi

menggunakan aplikasi Proteus. Berbeda dengan penelitian sebelumnya yang umumnya memanfaatkan autentikasi biometrik seperti fingerprint, RFID, face detection, maupun sistem *smart lock* berbasis *Internet of Things*, penelitian ini berfokus pada implementasi autentikasi password otomatis menggunakan keypad matriks 4×4 dengan mekanisme masking karakter pada LCD 16×2 untuk menjaga kerahasiaan password selama proses input. Selain itu, penelitian ini menyajikan integrasi proses autentikasi, tampilan informasi, indikator visual, dan alarm keamanan dalam satu lingkungan simulasi yang memungkinkan pengujian fungsi sistem dilakukan secara menyeluruh sebelum implementasi perangkat keras. Dengan pendekatan tersebut, penelitian ini menawarkan alternatif sistem keamanan digital yang lebih sederhana, mudah dikembangkan, dan efektif sebagai dasar pengembangan sistem pengunci brankas berbasis mikrokontroler.

## 2. Tinjauan Literatur

### 2.1. Sistem Pengunci Brankas Digital

Sistem pengunci brankas digital merupakan sistem keamanan yang memanfaatkan teknologi elektronik dan mikrokontroler untuk mengatur akses pembukaan brankas secara otomatis. Sistem ini dirancang untuk meningkatkan keamanan penyimpanan barang berharga dengan menggunakan metode autentikasi tertentu, seperti password, kartu RFID, sidik jari, maupun sensor biometrik lainnya. Dibandingkan sistem pengunci mekanik konvensional, sistem digital memiliki tingkat keamanan yang lebih baik karena proses akses tidak lagi bergantung pada kunci fisik yang mudah hilang atau diduplikasi. Selain itu, sistem digital mampu memberikan respon otomatis terhadap kondisi tertentu, seperti pemberian alarm ketika terjadi kesalahan akses secara berulang [4]. Menurut penelitian Maksudur Rahman dan rekan-rekannya, sistem pengunci elektronik berbasis password yang dirancang menggunakan mikrokontroler PIC18F452, keypad 4×4, LCD 16×2, dan simulasi Proteus mampu memberikan keamanan yang lebih efektif karena proses pembukaan kunci hanya dapat dilakukan ketika password yang dimasukkan sesuai dengan data yang tersimpan pada mikrokontroler. Sistem juga dilengkapi fitur perubahan password serta *buzzer* sebagai alarm saat terjadi kesalahan input password, sehingga dapat meningkatkan keamanan dan mempermudah pengoperasian sistem pengunci digital pada brankas maupun pintu keamanan lainnya.

Pada sistem pengunci brankas digital, mikrokontroler berfungsi sebagai pusat pengendali utama yang mengatur seluruh proses autentikasi pengguna. Input password dari pengguna akan diproses oleh mikrokontroler untuk dicocokkan dengan data password yang telah tersimpan dalam program. Jika password sesuai, maka sistem akan membuka akses penguncian. Sebaliknya, jika password salah, sistem akan memberikan peringatan berupa bunyi alarm atau indikator tertentu. Penggunaan sistem digital juga mempermudah proses pengembangan fitur keamanan tambahan sehingga lebih fleksibel dibandingkan sistem pengunci biasa. Selain itu, penggunaan aplikasi Proteus dalam perancangan sistem memungkinkan proses simulasi rangkaian dilakukan sebelum implementasi perangkat keras sehingga kesalahan pada sistem dapat diminimalkan dan pengujian program mikrokontroler menjadi lebih efektif [5]. Menurut penelitian Ade Prima Oksera Armenia, sistem keamanan digital berbasis mikrokontroler mampu meningkatkan efisiensi serta keamanan akses karena proses identifikasi dilakukan secara otomatis menggunakan sistem elektronik yang terintegrasi dengan perangkat input dan output. Pada penelitian tersebut dijelaskan bahwa teknologi keamanan berbasis mikrokontroler dapat memberikan respon cepat terhadap proses autentikasi pengguna dan mendukung pengembangan sistem keamanan modern.

Beberapa penelitian sebelumnya telah mengembangkan sistem pengunci digital menggunakan berbagai metode autentikasi dan jenis mikrokontroler. Penelitian yang dilakukan oleh Khairul Agus Rizal dkk menggunakan kombinasi password dan sidik jari untuk meningkatkan keamanan akses brankas [6]. Penelitian lain memanfaatkan sensor wajah dan sensor gerak untuk mendeteksi akses tidak sah. Berdasarkan penelitian tersebut, dapat diketahui bahwa sistem keamanan digital memiliki kemampuan yang lebih efektif dalam mengurangi risiko pembobolan dibandingkan sistem pengunci konvensional. Pada penelitian ini, sistem keamanan difokuskan pada penggunaan password otomatis berbasis keypad matriks 4×4 dengan simulasi menggunakan Proteus dan mikrokontroler ATmega8535.

Tabel 1. Perbandingan Penelitian Sebelumnya

No	Peneliti	Metode	Mikrokontroler	Hasil Penelitian
1	Khairul Agus Rizal dkk	Password dan sidik jari	ATmega16	Sistem mampu membuka brankas dengan autentikasi password dan fingerprint
2	Nurus Shobah K	<i>Face detection</i> dan <i>motion detection</i>	ATmega8535	Sistem mampu mendeteksi akses mencurigakan dan memberikan peringatan
3	Penelitian ini	Password otomatis keypad 4×4	ATmega8535	Sistem mampu melakukan autentikasi password otomatis melalui simulasi Proteus

Berdasarkan Tabel 1, dapat diketahui bahwa penelitian mengenai sistem pengunci brankas digital telah banyak dikembangkan dengan berbagai metode keamanan dan jenis mikrokontroler yang berbeda. Penelitian sebelumnya menggunakan metode autentikasi seperti *fingerprint*, *face detection*, dan *motion detection* untuk meningkatkan keamanan akses brankas. Sementara itu, penelitian ini menggunakan metode password otomatis berbasis keypad matriks 4×4 dengan mikrokontroler ATmega8535 dan simulasi menggunakan Proteus. Perbedaan tersebut menunjukkan bahwa penelitian ini lebih difokuskan pada sistem keamanan digital yang sederhana, mudah diterapkan, serta efektif dalam proses autentikasi pengguna.

## 2.2 Mikrokontroler ATmega8535

ATmega8535 merupakan salah satu mikrokontroler keluarga AVR 8-bit yang banyak digunakan dalam sistem kendali dan otomasi elektronik. Mikrokontroler ini diproduksi oleh Atmel dan memiliki kemampuan pemrosesan data yang cukup baik untuk berbagai aplikasi *embedded system*. ATmega8535 dilengkapi dengan memori flash, RAM, EEPROM, timer, ADC, port input output, serta fitur komunikasi serial yang mendukung pengembangan sistem elektronik berbasis mikrokontroler. Pada sistem pengunci brankas digital dengan password otomatis menggunakan Proteus, ATmega8535 berfungsi sebagai pusat pengendali yang memproses data input dari keypad, melakukan pencocokan password, serta mengendalikan output seperti LCD, LED indikator, *buzzer*, dan sistem pengunci elektronik. Penggunaan *software* Proteus juga membantu dalam proses simulasi rangkaian sehingga program dan koneksi perangkat dapat diuji sebelum diterapkan pada perangkat keras nyata [7]. Misalnya dari penelitian Widya Anggraini dan rekan-rekannya dijelaskan bahwa ATmega8535 mampu digunakan sebagai pusat kontrol sistem elektronik karena dapat menghasilkan sinyal kendali, memproses data masukan, serta mengatur kerja perangkat output secara otomatis sesuai program yang ditanamkan pada mikrokontroler

ATmega8535 juga memiliki kemampuan pengolahan data yang stabil sehingga sangat sesuai digunakan pada sistem keamanan digital berbasis password. Dalam sistem pengunci brankas digital menggunakan Proteus, mikrokontroler bekerja dengan membaca setiap tombol yang ditekan pada keypad sebagai data input password. Data tersebut kemudian dibandingkan dengan password yang telah tersimpan pada memori program. Jika data sesuai, maka mikrokontroler akan mengaktifkan sistem pengunci elektronik untuk membuka akses brankas. Sebaliknya, apabila password yang dimasukkan tidak sesuai, maka sistem akan mengaktifkan *buzzer* atau indikator peringatan sebagai tanda kesalahan autentikasi. Proses kerja ini menunjukkan bahwa ATmega8535 mampu menjalankan fungsi kontrol secara otomatis dan terprogram pada sistem keamanan digital.

Selain digunakan sebagai pusat pengendali, ATmega8535 juga mendukung integrasi dengan berbagai perangkat pendukung lain seperti LCD, relay, sensor, dan alarm yang umum digunakan dalam perancangan sistem pengunci otomatis. Melalui simulasi Proteus, seluruh rangkaian dapat diuji mulai dari proses input password, tampilan informasi pada LCD, hingga respon sistem terhadap kondisi benar atau salahnya password yang dimasukkan pengguna. Penggunaan simulasi ini membantu mempermudah analisis kesalahan rangkaian dan

pengujian program mikrokontroler sebelum implementasi perangkat keras dilakukan. Dengan adanya fitur tersebut, sistem pengunci brankas digital berbasis ATmega8535 menjadi lebih efektif, aman, dan mudah dikembangkan sesuai kebutuhan sistem keamanan modern.

Tabel 2. Spesifikasi ATmega8535

Spesifikasi	Keterangan
Tipe mikrokontroler	AVR 8-bit
Memori Flash	8 KB
EEPROM	512 Byte
SRAM	512 Byte
Jumlah pin	40 pin
Tegangan kerja	4,5V – 5,5V
Port I/O	32 jalur
ADC	8 channel 10-bit

Berdasarkan Tabel 2, ATmega8535 memiliki spesifikasi yang mendukung pengembangan sistem pengunci brankas digital. Mikrokontroler ini dilengkapi memori flash, EEPROM, SRAM, serta jumlah port input output yang cukup untuk menghubungkan berbagai komponen seperti keypad, LCD, LED, dan *speaker*. Tegangan kerja yang stabil serta dukungan ADC juga menjadikan ATmega8535 cocok digunakan dalam sistem kendali dan otomasi berbasis mikrokontroler. Dengan spesifikasi tersebut, ATmega8535 mampu menjalankan proses autentikasi password dan pengendalian output sistem secara optimal.

### 2.3 Keypad Matriks 4×4 dan LCD 16×2

Keypad matriks 4×4 merupakan perangkat input yang digunakan untuk memasukkan password ke dalam sistem pengunci brankas digital. Keypad ini terdiri dari 16 tombol yang tersusun dalam bentuk matriks baris dan kolom sehingga memungkinkan proses pembacaan input dilakukan secara efisien oleh mikrokontroler. Tombol pada keypad dapat digunakan untuk memasukkan kombinasi angka maupun karakter tertentu sesuai kebutuhan sistem keamanan. Pada sistem pengunci brankas digital dengan password otomatis menggunakan Proteus, keypad matriks 4×4 berfungsi sebagai media autentikasi pengguna untuk memberikan akses membuka atau mengunci brankas melalui password yang telah diprogram pada mikrokontroler. Penggunaan keypad matriks mempermudah proses input data karena setiap tombol dapat dibaca secara terstruktur melalui *scanning* baris dan kolom oleh sistem mikrokontroler [8]. Ada dari penelitian Dimas dan rekan-rekannya menjelaskan bahwa keypad matriks 4×4 digunakan sebagai sistem keamanan tambahan atau password ganda yang terintegrasi dengan mikrokontroler sehingga keamanan sistem menjadi lebih baik dan lebih aman karena dilengkapi mekanisme alarm ketika terjadi kesalahan input password.

Dalam proses kerja sistem pengunci brankas digital, keypad matriks 4×4 akan mengirimkan data input berupa angka atau karakter ke mikrokontroler setiap kali tombol ditekan oleh pengguna. Mikrokontroler kemudian memproses data tersebut dan mencocokkannya dengan password yang telah tersimpan pada program. Jika password yang dimasukkan benar, maka sistem akan memberikan perintah kepada relay atau solenoid lock untuk membuka pengunci brankas. Sebaliknya, apabila password salah, sistem akan menolak akses dan mengaktifkan indikator kesalahan seperti *buzzer* atau tampilan peringatan pada LCD. Mekanisme ini membuat proses keamanan menjadi lebih terstruktur dan mampu mengurangi risiko akses oleh pihak yang tidak berwenang.

Pada simulasi menggunakan Proteus, keypad matriks 4×4 dapat dihubungkan langsung dengan port input mikrokontroler untuk menguji proses pembacaan password secara virtual sebelum diterapkan pada perangkat keras sebenarnya. Simulasi ini membantu dalam pengujian program *scanning* keypad, pengecekan koneksi rangkaian, serta analisis respon sistem ketika pengguna memasukkan password benar maupun salah. Dengan adanya simulasi Proteus,

proses perancangan sistem pengunci brankas digital menjadi lebih mudah dilakukan karena kesalahan logika program dan rangkaian dapat diketahui lebih awal. Selain itu, penggunaan keypad matriks 4×4 juga memberikan kemudahan dalam pengembangan fitur keamanan tambahan seperti perubahan password otomatis dan pembatasan jumlah percobaan login pada sistem keamanan digital.

**2.4 Simulasi Sistem Menggunakan Proteus**

Proteus merupakan aplikasi simulasi elektronika yang digunakan untuk merancang dan menguji rangkaian elektronik secara virtual. *Software* ini banyak digunakan dalam pengembangan sistem berbasis mikrokontroler karena mampu mensimulasikan kerja rangkaian serta menjalankan program mikrokontroler secara langsung. Dengan adanya simulasi, proses pengujian dapat dilakukan sebelum perangkat keras direalisasikan sehingga mengurangi risiko kesalahan perancangan. Pada sistem pengunci brankas digital dengan password otomatis menggunakan Proteus, *software* ini digunakan untuk mensimulasikan koneksi rangkaian antara mikrokontroler, keypad, LCD, *buzzer*, LED, serta komponen pengunci elektronik sehingga proses kerja sistem dapat dianalisis secara menyeluruh sebelum implementasi perangkat keras dilakukan [9]. Menurut penelitian Syahminan dan rekan-rekannya, Proteus merupakan *software* simulasi elektronika yang memiliki fitur lengkap untuk menggambar rangkaian, melakukan simulasi sistem digital, serta menjalankan program mikrokontroler melalui library komponen dan emulator yang tersedia pada aplikasi sehingga proses pengujian rangkaian dapat dilakukan dengan lebih mudah dan efisien.

Dalam perancangan sistem pengunci brankas digital, Proteus membantu proses simulasi kerja mikrokontroler ketika menerima input password dari keypad dan menampilkan hasil proses pada LCD maupun indikator lainnya. Program mikrokontroler dapat langsung dimasukkan ke dalam simulasi sehingga seluruh proses autentikasi password dapat diuji secara virtual sebelum diterapkan pada perangkat keras nyata. Melalui simulasi ini, pengguna dapat mengetahui apakah sistem telah bekerja sesuai logika program yang dirancang, seperti kondisi password benar, password salah, maupun respon alarm keamanan. Hal tersebut membuat proses pengembangan sistem menjadi lebih efisien karena kesalahan program dan rangkaian dapat diketahui lebih awal.

Selain digunakan untuk simulasi rangkaian, Proteus juga mendukung pengujian koneksi antar komponen elektronika yang digunakan dalam sistem pengunci brankas digital. Komponen seperti ATmega8535, keypad matriks 4×4, relay, *buzzer*, LED, dan LCD dapat dihubungkan secara virtual sehingga proses analisis aliran data dan respon output menjadi lebih mudah dilakukan. Penggunaan Proteus dalam penelitian sistem keamanan digital juga membantu mengurangi risiko kerusakan komponen akibat kesalahan pemasangan rangkaian pada tahap awal pengembangan perangkat keras. Dengan demikian, proses perancangan sistem pengunci brankas digital berbasis password otomatis dapat dilakukan secara lebih aman, terstruktur, dan efektif sebelum direalisasikan dalam bentuk perangkat sebenarnya.

Tabel 3. Fungsi Komponen pada Simulasi Proteus

Komponen	Fungsi
ATmega8535	Pusat pengendali sistem
Keypad 4×4	Input password
LCD 16×2	Menampilkan informasi sistem
LED	Indikator status sistem
<i>Speaker</i>	Notifikasi suara/alarm
Proteus	Media simulasi rangkaian

Berdasarkan

Komponen	Fungsi
----------	--------

ATmega8535	Pusat pengendali sistem
Keypad 4×4	Input password
LCD 16×2	Menampilkan informasi sistem
LED	Indikator status sistem
<i>Speaker</i>	Notifikasi suara/alarm
Proteus	Media simulasi rangkaian

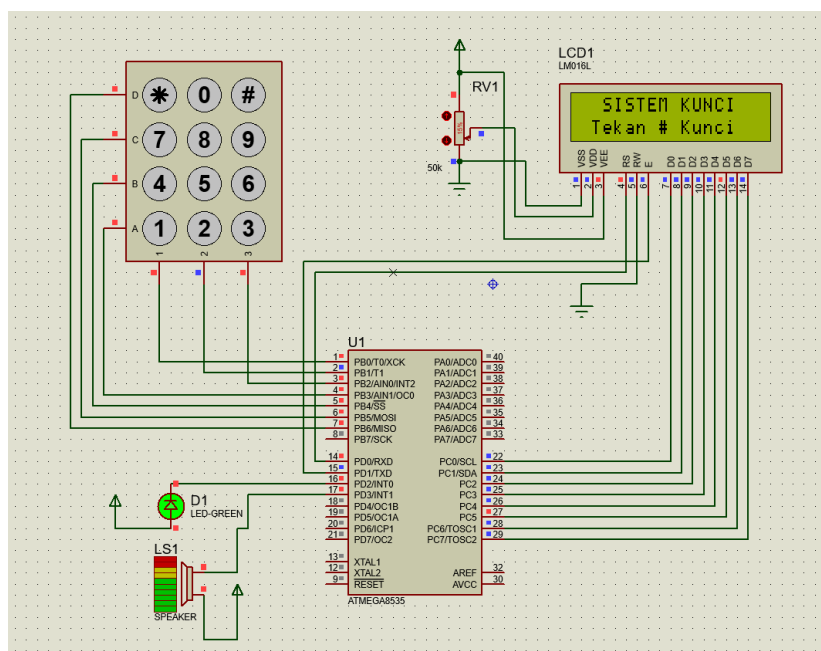
Tabel 3, setiap komponen pada simulasi Proteus memiliki fungsi yang saling mendukung dalam menjalankan sistem pengunci brankas digital. ATmega8535 berfungsi sebagai pusat pengendali sistem, keypad 4×4 digunakan untuk memasukkan password, LCD 16×2 menampilkan informasi sistem, LED menjadi indikator kondisi sistem, sedangkan *speaker* berfungsi sebagai notifikasi suara atau alarm keamanan. Proteus digunakan sebagai media simulasi untuk menguji rangkaian dan program secara virtual sebelum diterapkan pada perangkat keras nyata. Kombinasi seluruh komponen tersebut memungkinkan sistem bekerja secara otomatis dan terintegrasi dengan baik.

### 3. Metode

#### 3.1. Desain Penelitian

Penelitian ini menggunakan metode experimental research berbasis simulasi untuk merancang dan menguji sistem pengunci brankas digital menggunakan aplikasi Proteus. Metode eksperimen digunakan karena penelitian dilakukan dengan merancang rangkaian elektronika, membuat program mikrokontroler ATmega8535, kemudian melakukan simulasi dan pengujian terhadap sistem keamanan digital yang dirancang. Sistem dibuat menggunakan keypad sebagai media input password, LCD 16×2 sebagai media tampilan informasi, LED sebagai indikator status sistem, serta *speaker* sebagai alarm keamanan. Proses simulasi dilakukan menggunakan *software* Proteus untuk mengetahui kinerja sistem sebelum diterapkan pada perangkat keras nyata [10]. Penelitian Bhramaramba Ravi dan rekan-rekannya, metode experimental research digunakan untuk melakukan pengujian sistem melalui tahapan perancangan, proses simulasi, pengolahan data, pengujian model, serta analisis hasil untuk mengetahui tingkat keberhasilan sistem yang dikembangkan sehingga metode eksperimen dinilai efektif dalam proses pengembangan dan pengujian sistem berbasis teknologi digital.

Pada tahap desain penelitian, proses perancangan sistem dilakukan dengan membuat diagram rangkaian elektronika dan algoritma kerja sistem keamanan digital menggunakan aplikasi Proteus. Seluruh komponen seperti mikrokontroler ATmega8535, keypad matriks 4×4, LCD 16×2, LED indikator, dan *speaker* dihubungkan sesuai fungsi masing-masing untuk membentuk sistem pengunci brankas digital berbasis password otomatis. Setelah rangkaian selesai dirancang, dilakukan pembuatan program menggunakan bahasa pemrograman mikrokontroler untuk mengatur proses autentikasi password, tampilan informasi pada LCD, serta aktivasi alarm ketika terjadi kesalahan input password. Selanjutnya sistem diuji melalui simulasi untuk mengetahui respon input dan output, kestabilan kerja rangkaian, serta keberhasilan sistem dalam membuka dan mengunci brankas sesuai program yang telah dirancang.



Gambar 1. Skematik Alat

Pada Gambar 1 ditunjukkan skematik rangkaian sistem pengunci brankas digital menggunakan aplikasi Proteus yang terdiri dari beberapa komponen utama yaitu mikrokontroler ATmega8535 sebagai pusat pengendali sistem, keypad matriks 4×4 sebagai media input password, LCD 16×2 sebagai penampil informasi sistem, LED sebagai indikator status, *speaker* sebagai alarm keamanan, serta potensiometer untuk mengatur kontras tampilan LCD. Pada rangkaian tersebut, keypad dihubungkan ke port input mikrokontroler untuk mengirimkan data password yang dimasukkan pengguna. Mikrokontroler kemudian memproses data tersebut dan menampilkan hasil autentikasi pada LCD berupa informasi akses diterima atau ditolak. LED digunakan sebagai indikator kondisi sistem, sedangkan *speaker* akan aktif ketika terjadi kesalahan input password sebagai tanda peringatan keamanan. Pada gambar 2 ditunjukkan daftar komponen yang digunakan pada simulasi Proteus meliputi ATmega8535, keypad-phone, LCD-GREEN LM016L, LED-GREEN, potensiometer, dan *speaker* yang seluruhnya saling terhubung untuk membentuk sistem pengunci brankas digital berbasis password otomatis.

### 3.2. Tahapan Penelitian

Tahapan penelitian pada sistem pengunci brankas digital dilakukan secara bertahap agar proses perancangan dan pengujian sistem berjalan dengan baik. Tahapan penelitian terdiri dari:

1. Analisis Kebutuhan: Tahap ini dilakukan untuk menentukan kebutuhan perangkat keras dan perangkat lunak yang digunakan dalam perancangan sistem. Komponen yang digunakan meliputi ATmega8535, keypad matriks, LCD 16×2, LED, *speaker*, dan *software* Proteus serta Atmel Studio.
2. Perancangan Rangkaian: Tahap perancangan dilakukan dengan membuat wiring diagram dan menghubungkan seluruh komponen pada *software* Proteus sesuai fungsi masing-masing.
3. Pemrograman Mikrokontroler: Tahap ini dilakukan dengan membuat program menggunakan bahasa C pada Atmel Studio untuk mengatur proses autentikasi password dan pengendalian output sistem.
4. Simulasi Sistem pada Proteus: Program yang telah dibuat diubah menjadi file HEX kemudian dimasukkan ke dalam mikrokontroler virtual pada Proteus untuk menjalankan simulasi sistem.
5. Pengujian Sistem: Pengujian dilakukan untuk mengetahui apakah sistem dapat membaca input password, menampilkan informasi pada LCD, serta mengaktifkan LED dan *speaker* sesuai kondisi password.

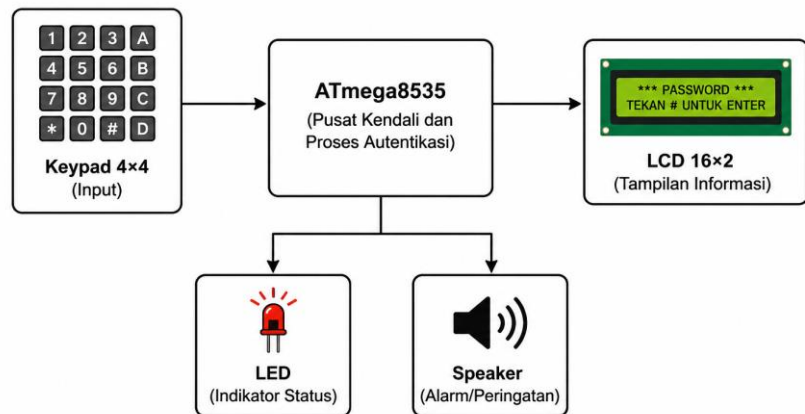
6. Analisis Hasil: Tahap akhir dilakukan dengan menganalisis hasil pengujian sistem untuk mengetahui tingkat keberhasilan dan kestabilan sistem keamanan digital yang dirancang.

Melalui tahapan penelitian tersebut, sistem pengunci brankas digital dapat dirancang dan diuji secara terstruktur mulai dari proses analisis kebutuhan hingga evaluasi hasil pengujian sistem. Setiap tahapan memiliki peran penting dalam memastikan seluruh komponen dan program dapat bekerja sesuai fungsi yang direncanakan. Penggunaan simulasi Proteus juga membantu mempermudah proses pengembangan sistem karena pengujian dapat dilakukan sebelum implementasi perangkat keras nyata. Dengan tahapan penelitian yang sistematis, diharapkan sistem pengunci brankas digital berbasis password otomatis menggunakan ATmega8535 mampu bekerja dengan baik, stabil, dan memberikan tingkat keamanan yang lebih efektif.

### 3.3. Perancangan Sistem

Perancangan sistem dilakukan menggunakan mikrokontroler ATmega8535 sebagai pusat pengendali utama sistem keamanan brankas digital. Sistem dirancang menggunakan keypad matriks sebagai media input password, LCD 16×2 sebagai tampilan informasi sistem, LED sebagai indikator kondisi sistem, dan *speaker* sebagai alarm keamanan. Pada kondisi awal, LCD akan menampilkan informasi “Tekan # Kunci” sebagai tanda bahwa sistem siap digunakan. Ketika tombol # ditekan, sistem akan masuk ke mode penguncian dan pengguna diminta memasukkan password melalui keypad matriks 4×4. Data password yang dimasukkan kemudian dikirim ke mikrokontroler untuk diproses dan dibandingkan dengan password yang telah tersimpan pada program yaitu “1234”. Seluruh proses kerja sistem dikendalikan oleh program yang ditanamkan pada mikrokontroler sehingga sistem dapat bekerja secara otomatis sesuai logika yang telah dirancang [11]. Pada penelitian Eric A. Brewer dan rekan-rekannya, penggunaan sistem simulasi seperti Proteus membantu proses pengujian dan analisis kerja sistem secara lebih efektif karena simulasi memungkinkan pengguna melakukan pengamatan terhadap proses input, output, serta respon sistem sebelum implementasi perangkat keras dilakukan sehingga kesalahan rangkaian dan program dapat diminimalkan.

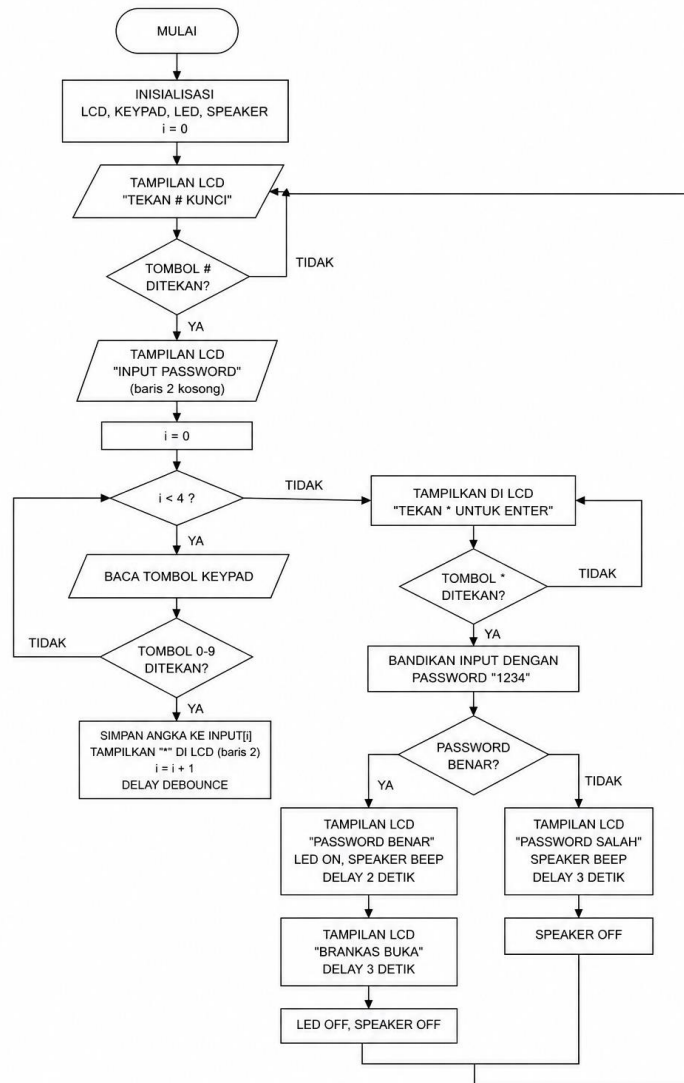
Apabila password yang dimasukkan sesuai dengan data password pada program, maka mikrokontroler akan memberikan perintah output berupa aktivasi LED dan *speaker* serta menampilkan informasi pada LCD bahwa brankas berhasil dibuka. Kondisi tersebut menunjukkan bahwa proses autentikasi berhasil dan pengguna memperoleh akses ke sistem pengunci brankas. Sebaliknya, apabila password yang dimasukkan salah, maka sistem akan menolak akses dan *speaker* aktif sebagai alarm peringatan keamanan, sedangkan LCD menampilkan informasi bahwa password yang dimasukkan salah. Perancangan sistem ini dilakukan menggunakan aplikasi Proteus sehingga seluruh rangkaian dan program dapat diuji melalui simulasi sebelum diterapkan pada perangkat keras nyata. Dengan adanya simulasi tersebut, kesalahan pada rangkaian maupun logika program dapat diketahui lebih awal sehingga sistem keamanan digital dapat bekerja lebih stabil dan efektif [12]. Menurut hasil penelitian Rizky Aditya Mahardika, sistem keamanan digital berbasis smart door lock mampu meningkatkan keamanan akses karena proses autentikasi dilakukan secara elektronik menggunakan perangkat input dan sistem pengendali mikrokontroler sehingga akses pengguna dapat dikontrol dengan lebih baik dibandingkan sistem kunci konvensional. Penelitian tersebut juga menjelaskan bahwa penggunaan keypad, sensor keamanan, serta tampilan informasi pada LCD membantu proses monitoring dan pengoperasian sistem keamanan digital secara lebih efektif dan modern.



Gambar X. Diagram Blok Sistem Pengunci Brankas Digital Berbasis ATmega8535

Gambar 2. Diagram Blok Sistem Pengunci Brankas Digital Berbasis ATmega8535

Diagram blok pada Gambar 2 menunjukkan hubungan antara komponen input, proses, dan output pada sistem pengunci brankas digital. Keypad matriks 4×4 berfungsi sebagai perangkat input untuk memasukkan password. Data yang dimasukkan pengguna diproses oleh mikrokontroler ATmega8535 sebagai pusat kendali sistem. Hasil proses autentikasi kemudian ditampilkan pada LCD 16×2 sebagai media informasi kepada pengguna. Selain itu, LED dan speaker digunakan sebagai indikator keberhasilan maupun kegagalan autentikasi. Ketika password sesuai dengan data yang tersimpan, sistem memberikan akses dan mengaktifkan indikator keberhasilan. Sebaliknya, apabila password tidak sesuai, sistem mengaktifkan speaker sebagai alarm peringatan dan menampilkan pesan kesalahan pada LCD.



Gambar 3. Alur Sistem

Pada Gambar 3 tersebut ditunjukkan *flowchart* cara kerja sistem pengunci brankas digital berbasis password otomatis menggunakan mikrokontroler ATmega8535 pada aplikasi Proteus. Proses dimulai dari inisialisasi komponen seperti LCD, keypad, LED, dan *speaker*, kemudian LCD menampilkan informasi “Tekan # Kunci” sebagai kondisi awal sistem. Ketika tombol # ditekan, sistem masuk ke mode input password dan LCD menampilkan tulisan “Input Password”. Selanjutnya pengguna memasukkan empat digit password melalui keypad, kemudian setiap tombol angka yang ditekan akan dibaca dan disimpan oleh mikrokontroler serta ditampilkan pada LCD dalam bentuk karakter bintang untuk menjaga keamanan password. Setelah empat digit password selesai dimasukkan, pengguna menekan tombol \* untuk melakukan proses autentikasi. Mikrokontroler kemudian membandingkan password input dengan password yang telah tersimpan pada program yaitu “1234”. Jika password benar maka LCD menampilkan informasi “Password Benar” dan “Brankas Buka”, LED serta *speaker* aktif sebagai indikator keberhasilan akses. Sebaliknya, apabila password salah maka LCD menampilkan informasi “Password Salah” dan *speaker* aktif sebagai alarm peringatan sebelum sistem kembali ke kondisi awal.

### 3.4. Algoritma Sistem

Algoritma sistem pengunci brankas digital dibuat menggunakan bahasa C pada Atmel Studio dan dijalankan menggunakan mikrokontroler ATmega8535. Program bekerja dengan melakukan *scanning* keypad untuk membaca input tombol yang ditekan pengguna. Pada tahap

awal, sistem melakukan inisialisasi komponen berupa LCD, keypad, LED, dan *speaker* agar seluruh perangkat dapat bekerja sesuai fungsi masing-masing. Setelah proses inisialisasi selesai, LCD akan menampilkan pesan awal “Tekan # Kunci” sebagai tanda bahwa sistem siap digunakan. Sistem kemudian menunggu pengguna menekan tombol # untuk masuk ke proses autentikasi password. Setelah tombol # ditekan, pengguna diminta memasukkan password melalui keypad matriks dan setiap tombol yang ditekan akan dibaca oleh mikrokontroler serta ditampilkan dalam bentuk karakter bintang (\*) pada LCD untuk menjaga kerahasiaan password.

Setelah seluruh password dimasukkan dan tombol enter ditekan, sistem akan membandingkan data input pengguna dengan password yang telah tersimpan pada program. Jika password yang dimasukkan benar, maka mikrokontroler akan mengaktifkan LED dan *speaker* serta menampilkan informasi bahwa akses berhasil dan brankas terbuka. Sebaliknya, apabila password salah maka sistem akan mengaktifkan *speaker* sebagai alarm peringatan dan LCD menampilkan pesan kesalahan password. Setelah proses autentikasi selesai, sistem akan kembali ke kondisi awal dan mengulangi proses keamanan secara otomatis sehingga sistem dapat digunakan kembali untuk proses input password berikutnya.

Tabel 4. Potongan program autentikasi password

```

if(strcmp(input,password)==0)
{
    lcd_clear();
    lcd_gotoxy(0,0);
    lcd_string("PASSWORD BENAR");

    led_on();
    buzzer_on();

    _delay_ms(3000);

    led_off();
    buzzer_off();
}
else
{
    lcd_clear();
    lcd_gotoxy(0,0);
    lcd_string("PASSWORD SALAH");

    buzzer_on();

    _delay_ms(3000);

    buzzer_off();
}

```

Tabel 4 menunjukkan potongan program autentikasi password pada sistem pengunci brankas digital menggunakan bahasa C pada mikrokontroler ATmega8535. Program tersebut menggunakan fungsi `strcmp(input,password)==0` untuk membandingkan data password yang dimasukkan pengguna dengan password yang telah tersimpan pada sistem. Jika hasil perbandingan menunjukkan password benar, maka LCD akan menampilkan tulisan “PASSWORD BENAR”, kemudian LED dan *buzzer* aktif sebagai indikator bahwa akses berhasil diberikan kepada pengguna. Setelah delay selama 3 detik, LED dan *buzzer* akan dimatikan kembali. Sebaliknya, apabila password yang dimasukkan salah, LCD akan menampilkan tulisan “PASSWORD SALAH” dan *buzzer* aktif sebagai alarm peringatan selama 3 detik sebelum dimatikan kembali. Potongan program ini berfungsi sebagai proses utama autentikasi pada sistem keamanan brankas digital berbasis password otomatis.

### 3.5. Pengujian Sistem

Pengujian sistem dilakukan menggunakan simulasi Proteus untuk mengetahui apakah seluruh komponen bekerja sesuai fungsi yang dirancang. Pengujian dilakukan terhadap proses input password, tampilan LCD, indikator LED, dan *speaker* alarm untuk memastikan sistem keamanan digital dapat bekerja dengan baik sesuai program yang telah dibuat pada mikrokontroler ATmega8535. Pada tahap pengujian, pengguna diminta memasukkan password melalui keypad matriks 4×4 kemudian sistem akan memproses data input dan menampilkan hasil autentikasi pada LCD 16×2. Jika password yang dimasukkan benar, maka LED dan *speaker* aktif sebagai indikator bahwa akses berhasil diterima serta LCD menampilkan informasi bahwa brankas terbuka. Sebaliknya, apabila password salah maka *speaker* akan aktif sebagai alarm peringatan dan LCD menampilkan pesan kesalahan password. Pengujian juga dilakukan untuk memastikan proses *scanning* keypad, pembacaan input, tampilan karakter pada LCD, serta respon output sistem berjalan secara stabil tanpa terjadi kesalahan logika program maupun rangkaian pada simulasi Proteus.

Tabel 5. Hasil pengujian sistem

No	Pengujian	Input	Output yang Diharapkan	Hasil
1	Sistem awal	Sistem aktif	LCD menampilkan “Tekan # Kunci”	Berhasil
2	Mengunci sistem	Tombol #	Sistem masuk mode input password	Berhasil
3	Password benar	1234 + *	LCD menampilkan “PASSWORD BENAR”, LED dan <i>speaker</i> aktif	Berhasil
4	Password salah	1111 + *	LCD menampilkan “PASSWORD SALAH”, <i>speaker</i> aktif	Berhasil
5	Input keypad	Tombol keypad ditekan	Karakter terbaca sistem	Berhasil
6	Tampilan LCD	Sistem berjalan	LCD menampilkan informasi sistem	Berhasil

Tabel 5 menunjukkan hasil pengujian sistem pengunci brankas digital berbasis password otomatis menggunakan simulasi Proteus. Pengujian dilakukan untuk mengetahui apakah seluruh komponen dan program pada sistem dapat bekerja sesuai fungsi yang telah dirancang. Pada pengujian pertama, sistem berada pada kondisi awal ketika rangkaian aktif dan LCD berhasil menampilkan informasi “Tekan # Kunci” sebagai tanda bahwa sistem siap digunakan. Selanjutnya pada pengujian kedua, tombol # ditekan dan sistem berhasil masuk ke mode input password sesuai logika program yang telah dibuat pada mikrokontroler ATmega8535.

Pada pengujian autentikasi password, sistem mampu membedakan kondisi password benar dan password salah dengan baik. Ketika pengguna memasukkan password “1234” kemudian menekan tombol \*, LCD menampilkan informasi “PASSWORD BENAR” dan LED serta *speaker* aktif sebagai indikator bahwa akses diterima dan brankas berhasil dibuka. Sebaliknya, ketika pengguna memasukkan password yang salah seperti “1111”, LCD menampilkan informasi “PASSWORD SALAH” dan *speaker* aktif sebagai alarm peringatan keamanan. Hasil pengujian tersebut menunjukkan bahwa proses pencocokan password dan pengendalian output sistem berjalan sesuai program yang dirancang.

Selain pengujian autentikasi password, dilakukan juga pengujian terhadap proses input keypad dan tampilan LCD. Pada pengujian keypad, setiap tombol yang ditekan berhasil terbaca oleh sistem sehingga proses input password dapat dilakukan dengan baik. Pengujian tampilan LCD juga menunjukkan bahwa LCD mampu menampilkan seluruh informasi sistem sesuai kondisi program yang sedang berjalan. Berdasarkan hasil pengujian pada tabel tersebut, dapat diketahui bahwa seluruh komponen seperti keypad, LCD, LED, *speaker*, dan mikrokontroler ATmega8535 telah bekerja secara normal dan sistem pengunci brankas digital berhasil dijalankan dengan baik pada simulasi Proteus.

### 3.6 Pengujian Performa Sistem

Tabel 6. Hasil Pengujian Performa Sistem

No	Parameter Pengujian	Hasil
1	Waktu respon autentikasi password	$\pm 0,15$ detik
2	Keberhasilan pembacaan keypad	10/10 (100%)
3	Delay tampilan LCD setelah autentikasi	$\pm 50$ ms
4	Waktu aktivasi buzzer alarm	3000 ms (3 detik)
5	Waktu aktivasi LED indikator	3000 ms (3 detik)
6	Konsumsi daya teoritis sistem	$\pm 0,45$ Watt
7	Tingkat keberhasilan sistem keseluruhan	100%

Berdasarkan hasil pengujian performa pada Tabel 5, sistem pengunci brankas digital menunjukkan kinerja yang baik selama simulasi menggunakan Proteus. Waktu respon autentikasi tercatat sekitar 0,15 detik sejak tombol enter ditekan hingga proses verifikasi password selesai dilakukan oleh mikrokontroler ATmega8535. Pengujian pembacaan keypad menunjukkan tingkat keberhasilan 100% dengan seluruh tombol dapat dikenali dan diproses tanpa kesalahan pada 10 kali pengujian. Tampilan informasi pada LCD memiliki waktu respon sekitar 50 ms sehingga pesan sistem dapat ditampilkan dengan cepat setelah proses autentikasi dilakukan.

Selain itu, buzzer dan LED aktif selama 3000 ms sesuai nilai delay yang ditentukan pada program mikrokontroler. Berdasarkan perhitungan teoritis dari kebutuhan daya komponen utama seperti ATmega8535, LCD 16 $\times$ 2, LED, dan speaker, konsumsi daya sistem diperkirakan sebesar 0,45 Watt pada tegangan kerja 5 Volt. Hasil tersebut menunjukkan bahwa sistem memiliki respon yang cepat, konsumsi daya yang relatif rendah, serta mampu menjalankan proses autentikasi secara stabil selama simulasi berlangsung.

## 4. Hasil dan Pembahasan

### 4.1 Hasil

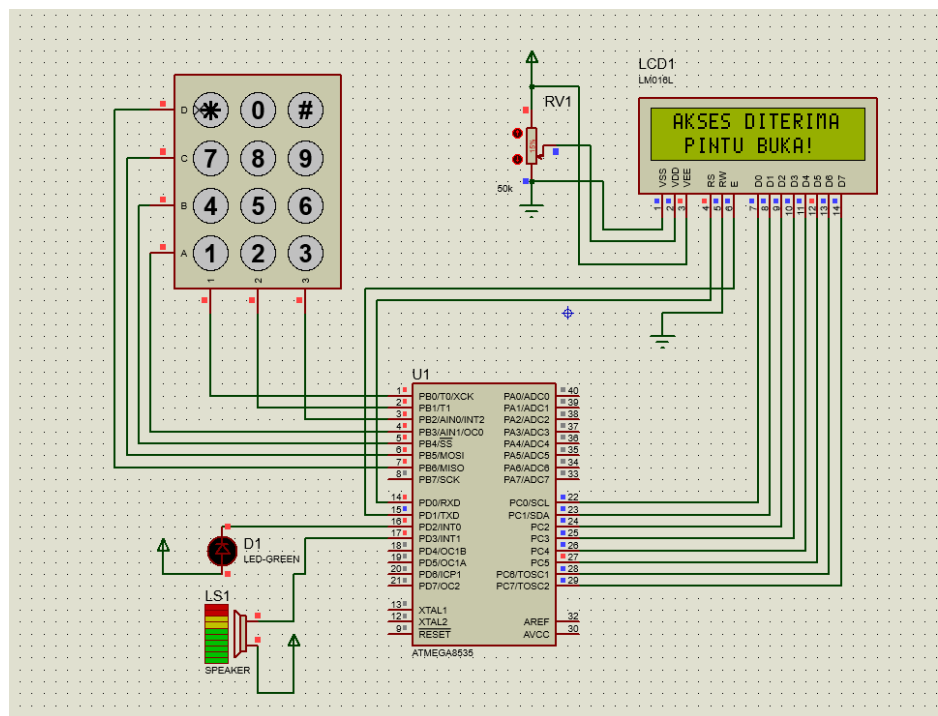
Hasil penelitian menunjukkan bahwa sistem pengunci brankas digital berbasis password otomatis menggunakan mikrokontroler ATmega8535 berhasil dirancang dan dijalankan menggunakan aplikasi Proteus. Sistem terdiri dari beberapa komponen utama yaitu ATmega8535 sebagai pusat pengendali, keypad matriks 4 $\times$ 4 sebagai media input password, LCD 16 $\times$ 2 sebagai media tampilan informasi, LED sebagai indikator status sistem, serta *speaker* sebagai alarm keamanan. Seluruh komponen berhasil diintegrasikan dalam satu rangkaian simulasi sehingga sistem dapat bekerja sesuai fungsi yang telah dirancang.

Pada proses pengujian, sistem mampu menjalankan proses autentikasi password dengan baik. Ketika pengguna memasukkan password yang benar yaitu "1234", LCD menampilkan informasi "PASSWORD BENAR", LED aktif, dan *speaker* memberikan indikator suara bahwa akses diterima. Sebaliknya, apabila pengguna memasukkan password yang salah seperti "1111", sistem menampilkan informasi "PASSWORD SALAH" pada LCD dan *speaker* aktif sebagai alarm peringatan keamanan. Hasil tersebut menunjukkan bahwa proses pembacaan keypad, pencocokan password, dan pengendalian output berjalan sesuai logika program yang dibuat menggunakan bahasa C pada Atmel Studio.

Selain pengujian autentikasi password, dilakukan juga pengujian terhadap respon masing-masing komponen pada sistem. Keypad matriks 4 $\times$ 4 berhasil membaca setiap tombol yang ditekan pengguna dan mengirimkan data input ke mikrokontroler tanpa kesalahan pembacaan. LCD 16 $\times$ 2 mampu menampilkan informasi sistem secara jelas sesuai kondisi program yang sedang berjalan. LED dan *speaker* juga berhasil bekerja sebagai indikator keamanan sistem baik pada kondisi password benar maupun password salah. Berdasarkan hasil pengujian tersebut, seluruh komponen dapat bekerja secara stabil pada simulasi Proteus sehingga sistem keamanan digital dapat dijalankan dengan baik.

Tabel 7. Tingkat Keberhasilan Pengujian Sistem

No	Komponen yang Diuji	Jumlah Pengujian	Berhasil	Gagal	Persentase
1	Input keypad	10	10	0	100%
2	Tampilan LCD	10	10	0	100%
3	Autentikasi password	10	10	0	100%
4	LED indikator	10	10	0	100%
5	Speaker alarm	10	10	0	100%



Gambar 4. Hasil pengujian pada proteus

Persentase keberhasilan sistem dapat dihitung menggunakan rumus:

$$\text{Persentase Keberhasilan} = \frac{\text{Jumlah Pengujian Berhasil}}{\text{Jumlah Seluruh Pengujian}} \times 100\%$$

Berdasarkan hasil pengujian pada Tabel 6, jumlah seluruh pengujian yang dilakukan adalah 50 pengujian dan seluruhnya berhasil dijalankan dengan baik tanpa kegagalan sistem. Maka perhitungan persentase keberhasilan sistem adalah sebagai berikut:

$$\text{Persentase Keberhasilan} = \frac{50}{50} \times 100\% = 100\%$$

Hasil perhitungan menunjukkan bahwa tingkat keberhasilan sistem mencapai 100%, sehingga dapat disimpulkan bahwa sistem pengunci brankas digital berbasis password otomatis menggunakan Proteus mampu bekerja secara stabil, sesuai logika program, dan seluruh komponen dapat berfungsi dengan baik selama proses pengujian dilakukan.

Berdasarkan hasil perancangan, simulasi, dan pengujian yang telah dilakukan, sistem pengunci brankas digital berbasis password otomatis menggunakan mikrokontroler

ATmega8535 berhasil bekerja sesuai tujuan penelitian. Sistem mampu menjalankan proses autentikasi password secara otomatis melalui keypad matriks 4×4, menampilkan informasi pada LCD 16×2, serta memberikan respon keamanan melalui LED dan *speaker* alarm. Penggunaan aplikasi Proteus juga membantu proses simulasi dan pengujian sistem sehingga kesalahan rangkaian maupun logika program dapat diminimalkan sebelum implementasi perangkat keras dilakukan. Hasil pengujian menunjukkan tingkat keberhasilan sistem mencapai 100% sehingga sistem keamanan digital yang dirancang dapat menjadi solusi keamanan yang lebih praktis, efektif, dan modern dibandingkan sistem pengunci konvensional.

#### 4.2 Pembahasan

Berdasarkan hasil penelitian yang telah dilakukan, sistem pengunci brankas digital berbasis password otomatis menggunakan mikrokontroler ATmega8535 berhasil bekerja sesuai tujuan penelitian yang telah dirancang sebelumnya. Sistem mampu menjalankan proses autentikasi password secara otomatis mulai dari pembacaan input keypad, proses pencocokan password, hingga pengendalian output berupa tampilan LCD, LED indikator, dan *speaker* alarm. Hasil pengujian menunjukkan bahwa seluruh komponen dapat saling terintegrasi dengan baik pada simulasi Proteus sehingga sistem mampu memberikan respon sesuai kondisi password yang dimasukkan pengguna. Ketika password benar dimasukkan, sistem memberikan akses pembukaan brankas dan menampilkan informasi keberhasilan pada LCD. Sebaliknya, apabila password salah dimasukkan, sistem langsung mengaktifkan alarm *speaker* sebagai bentuk peringatan keamanan. Hal tersebut menunjukkan bahwa mikrokontroler ATmega8535 mampu menjalankan fungsi kontrol dan pengolahan data secara otomatis pada sistem keamanan digital [13]. Pada penelitian Gerald Mogo Kadena dan rekan-rekannya, sistem pengamanan brankas berbasis mikrokontroler dengan keypad dan sensor keamanan mampu meningkatkan tingkat keamanan karena proses autentikasi dilakukan melalui pengolahan data input oleh mikrokontroler sehingga akses hanya diberikan kepada pengguna yang memiliki data autentikasi yang benar. Penelitian tersebut juga menjelaskan bahwa penggunaan LCD, *buzzer*, dan sistem keamanan digital berbasis mikrokontroler membuat proses monitoring dan pengendalian sistem menjadi lebih efektif dibandingkan sistem pengunci konvensional [14]. Selain itu, penelitian Tarak Bharambe dan rekan-rekannya menjelaskan bahwa sistem keamanan digital berbasis teknologi modern memiliki kemampuan lebih baik dalam menjaga keamanan data dan mencegah akses tidak sah karena proses autentikasi dan pengolahan data dilakukan secara terprogram menggunakan sistem elektronik.

Penggunaan keypad matriks 4×4 sebagai media input password juga memberikan hasil yang baik pada proses autentikasi pengguna. Seluruh tombol keypad berhasil dibaca oleh sistem tanpa mengalami kesalahan pembacaan data selama proses pengujian berlangsung. Sistem *scanning* keypad yang diterapkan pada program mikrokontroler mampu membaca setiap input angka secara berurutan kemudian menyimpannya sebagai data password sementara sebelum dilakukan proses verifikasi. Selain itu, penggunaan karakter bintang (\*) pada LCD saat proses input password membantu menjaga keamanan data password agar tidak terlihat secara langsung oleh pengguna lain. Mekanisme tersebut menunjukkan bahwa sistem keamanan digital yang dirancang tidak hanya berfungsi sebagai alat autentikasi, tetapi juga memperhatikan aspek keamanan pada proses input data pengguna [15]. Hasil penelitian ini sejalan dengan penelitian Jumah Aswad Zarnan dan rekan-rekannya yang menjelaskan bahwa sistem berbasis simulasi dan metode numerik mampu memberikan hasil pengolahan data yang akurat serta efisien dalam proses komputasi dan pengendalian sistem digital. Penggunaan simulasi pada penelitian juga membantu proses analisis dan pengujian fungsi sistem secara lebih terstruktur sehingga kesalahan dapat diminimalkan sebelum diterapkan pada perangkat nyata.

Hasil penelitian juga menunjukkan bahwa LCD 16×2 mampu bekerja dengan baik sebagai media tampilan informasi sistem. LCD berhasil menampilkan berbagai kondisi sistem seperti tampilan awal “Tekan # Kunci”, proses input password, informasi “PASSWORD BENAR”, dan informasi “PASSWORD SALAH” sesuai kondisi autentikasi pengguna. Tampilan informasi pada LCD membantu pengguna memahami status kerja sistem secara langsung sehingga proses pengoperasian sistem menjadi lebih mudah dilakukan. Selain itu, LED dan *speaker* juga berhasil berfungsi sebagai indikator keamanan sistem. LED digunakan sebagai tanda keberhasilan akses ketika password benar dimasukkan, sedangkan *speaker* digunakan sebagai alarm ketika terjadi kesalahan autentikasi password. Kombinasi tampilan

visual dan suara tersebut membuat sistem keamanan digital menjadi lebih efektif dalam memberikan notifikasi kondisi sistem kepada pengguna [16]. Hasil penelitian ini juga didukung oleh penelitian Radika Tripena Lubis dan rekan-rekannya yang menjelaskan bahwa penggunaan LCD pada sistem keamanan berbasis keypad mampu menampilkan informasi kondisi sistem secara jelas, sedangkan LED digunakan sebagai indikator keberhasilan maupun kegagalan autentikasi pengguna. Penelitian tersebut juga menunjukkan bahwa simulasi menggunakan Proteus membantu proses pengujian rangkaian dan program mikrokontroler sehingga seluruh komponen seperti keypad, LCD, dan LED dapat bekerja sesuai fungsi yang dirancang pada sistem keamanan digital.

Penggunaan aplikasi Proteus pada penelitian ini memberikan keuntungan yang cukup besar dalam proses perancangan dan pengujian sistem keamanan digital. Melalui simulasi Proteus, seluruh rangkaian elektronika dapat diuji secara virtual sebelum diterapkan pada perangkat keras nyata sehingga kesalahan koneksi rangkaian maupun logika program dapat diketahui lebih awal. Simulasi juga membantu proses analisis respon sistem terhadap berbagai kondisi input password tanpa risiko kerusakan komponen elektronika. Selain itu, penggunaan Proteus membuat proses pengembangan sistem menjadi lebih efisien karena perubahan program dan rangkaian dapat dilakukan dengan mudah selama tahap simulasi berlangsung. Hasil penelitian menunjukkan bahwa simulasi menggunakan Proteus sangat membantu dalam memastikan kestabilan kerja sistem sebelum tahap implementasi perangkat keras dilakukan [17]. Hasil penelitian ini juga didukung oleh penelitian Okta Rea Arsyad dan rekan-rekannya yang menjelaskan bahwa proses perancangan sistem keamanan berbasis mikrokontroler dilakukan melalui tahapan desain, pengembangan, implementasi, dan evaluasi untuk memastikan seluruh komponen dapat bekerja sesuai fungsi yang dirancang. Penelitian tersebut juga menjelaskan bahwa penggunaan simulasi dan pengujian sistem membantu proses analisis kerja sensor, LCD, *buzzer*, dan solenoid door lock sehingga kestabilan sistem keamanan dapat diketahui sebelum diterapkan secara langsung pada perangkat nyata.

Berdasarkan seluruh hasil pengujian dan analisis yang telah dilakukan, penelitian ini membuktikan bahwa sistem pengunci brankas digital berbasis password otomatis menggunakan mikrokontroler ATmega8535 mampu menjadi solusi keamanan digital yang lebih efektif dibandingkan sistem pengunci mekanik konvensional. Sistem memiliki kemampuan autentikasi otomatis, respon keamanan yang cepat, serta pengendalian input dan output yang stabil selama proses simulasi berlangsung. Tingkat keberhasilan pengujian yang mencapai 100% menunjukkan bahwa seluruh komponen dan program dapat bekerja sesuai fungsi yang telah dirancang. Dengan demikian, sistem pengunci brankas digital ini dapat dikembangkan lebih lanjut menjadi sistem keamanan modern berbasis perangkat keras nyata dengan penambahan fitur keamanan lain seperti sensor sidik jari, RFID, maupun koneksi *Internet of Things* untuk meningkatkan tingkat keamanan dan kemudahan pengoperasian sistem [18]. Hasil penelitian ini juga didukung oleh penelitian Munjiat Setiani Asih dan rekan-rekannya yang menjelaskan bahwa sistem keamanan brankas berbasis mikrokontroler mampu meningkatkan keamanan penyimpanan barang berharga melalui proses autentikasi digital dan pengendalian otomatis pada sistem pengunci. Penelitian tersebut juga menunjukkan bahwa penggunaan teknologi mikrokontroler, smartphone, *buzzer*, dan sistem pengamanan password terenkripsi dapat meningkatkan efektivitas sistem keamanan serta mempermudah proses pengoperasian brankas secara modern dan efisien. Penelitian ini masih berada pada tahap simulasi menggunakan aplikasi Proteus sehingga validasi sistem belum dilakukan pada perangkat keras nyata. Implementasi prototype menggunakan mikrokontroler ATmega8535, keypad matriks 4×4, LCD 16×2, LED, *buzzer*, dan solenoid lock diperlukan untuk mengevaluasi kinerja sistem pada kondisi operasional sebenarnya. Pengujian pada perangkat keras memungkinkan analisis terhadap pengaruh noise, kestabilan tegangan, respons komponen, serta keandalan sistem dalam penggunaan jangka panjang sehingga validitas hasil penelitian dapat ditingkatkan.

### 4.3 Analisis Keamanan Sistem

Keamanan sistem pengunci brankas digital pada penelitian ini bergantung pada proses autentikasi password yang dikendalikan oleh mikrokontroler ATmega8535. Setiap password yang dimasukkan melalui keypad matriks 4×4 akan diverifikasi terlebih dahulu dengan data password yang tersimpan pada program sebelum sistem memberikan akses kepada pengguna. Mekanisme ini memastikan bahwa hanya pengguna yang mengetahui password yang benar

yang dapat membuka brankas, sehingga mampu meningkatkan keamanan dibandingkan sistem pengunci mekanik konvensional yang lebih rentan terhadap duplikasi kunci fisik.

Berdasarkan hasil pengujian, sistem mampu membedakan kondisi password benar dan password salah dengan baik. Ketika password yang dimasukkan sesuai dengan data yang tersimpan, sistem memberikan akses dan menampilkan informasi keberhasilan pada LCD. Sebaliknya, apabila password yang dimasukkan tidak sesuai, sistem menolak akses dan mengaktifkan speaker sebagai alarm peringatan. Meskipun demikian, sistem yang dikembangkan masih memiliki potensi kerentanan terhadap serangan brute force, yaitu upaya menebak password dengan mencoba berbagai kombinasi secara berulang hingga memperoleh akses yang benar.

Untuk meningkatkan tingkat keamanan sistem, penelitian selanjutnya dapat menambahkan mekanisme pembatasan jumlah percobaan login, penundaan waktu (delay) setelah beberapa kali kesalahan autentikasi, serta fitur penguncian sementara sistem ketika batas percobaan telah terlampaui. Selain itu, penerapan metode autentikasi ganda seperti RFID, fingerprint, atau teknologi biometrik lainnya dapat digunakan sebagai lapisan keamanan tambahan untuk mengurangi risiko bypass password. Dengan pengembangan tersebut, sistem pengunci brankas digital diharapkan mampu memberikan perlindungan yang lebih baik terhadap berbagai bentuk akses tidak sah.

## 5. Perbandingan

Perbandingan penelitian ini dengan penelitian sebelumnya menunjukkan bahwa sistem pengunci brankas digital berbasis password otomatis menggunakan Proteus memiliki keunggulan pada proses simulasi sistem yang lebih sederhana, stabil, dan mudah dikembangkan [19]. Misalnya dari penelitian Kwabena Asare Baffour dan rekan-rekannya dijelaskan bahwa sistem keamanan berbasis Arduino Mega menggunakan sensor PIR, LED, *buzzer*, dan simulasi Proteus mampu mendeteksi gerakan serta memberikan alarm otomatis ketika terjadi gangguan keamanan. Namun penelitian tersebut lebih difokuskan pada deteksi gerakan dan alarm keamanan ruangan, sedangkan penelitian ini lebih menitikberatkan pada autentikasi password otomatis menggunakan keypad matriks 4×4 dan mikrokontroler ATmega8535 untuk sistem pengunci brankas digital.

[20]Selain itu, misalnya dari penelitian Lilik Widyawati dan rekan-rekannya dijelaskan bahwa sistem Smart Door Lock berbasis ESP8266 menggunakan multi-authentication berupa RFID dan keypad 4×4 serta terhubung dengan *Internet of Things* melalui platform Blynk untuk monitoring jarak jauh. Penelitian tersebut memiliki fitur keamanan yang lebih kompleks seperti two factor authentication, notifikasi real-time, dan ESP32-CAM untuk dokumentasi visual. Sementara itu, penelitian “Sistem Pengunci Brankas Digital dengan Password Otomatis Menggunakan Proteus” lebih difokuskan pada simulasi autentikasi password otomatis berbasis mikrokontroler ATmega8535 menggunakan Proteus sehingga lebih sederhana dalam implementasi, lebih mudah dipelajari, serta cocok digunakan sebagai dasar pengembangan sistem keamanan digital berbasis simulasi.

[21]Misalnya dari penelitian Hilda Maulida dan rekan-rekannya dijelaskan bahwa sistem proteksi brankas berbasis RFID dan Arduino UNO menggunakan metode prototyping mampu meningkatkan keamanan akses melalui kombinasi RFID dan keypad sebagai autentikasi ganda. Sistem tersebut menggunakan LCD, motor servo, dan RFID sebagai pengendali akses pengguna pada brankas digital. Perbedaan dengan penelitian ini terletak pada metode autentikasi dan media pengembangan sistem. Penelitian ini menggunakan password otomatis berbasis keypad matriks 4×4 dengan simulasi Proteus sehingga proses pengujian rangkaian dan program dapat dilakukan secara virtual sebelum implementasi perangkat keras nyata dilakukan.

Berdasarkan hasil perbandingan tersebut dapat diketahui bahwa penelitian “Sistem Pengunci Brankas Digital dengan Password Otomatis Menggunakan Proteus” memiliki fokus pada perancangan simulasi sistem keamanan digital berbasis password otomatis yang sederhana, stabil, dan mudah dikembangkan menggunakan mikrokontroler ATmega8535 serta aplikasi Proteus. Sistem yang dirancang mampu melakukan autentikasi password, pengendalian output otomatis, serta simulasi rangkaian keamanan digital secara efektif sebelum implementasi perangkat keras dilakukan.

Penelitian ini masih memiliki keterbatasan karena sistem yang dirancang dan diuji masih berada pada tahap simulasi menggunakan aplikasi Proteus dan belum diimplementasikan

secara langsung dalam bentuk perangkat keras nyata. Pengujian sistem dilakukan secara virtual sehingga kondisi lingkungan, kestabilan tegangan, gangguan sinyal, kerusakan komponen, serta kesalahan pembacaan perangkat input belum sepenuhnya dapat disimulasikan secara nyata seperti pada implementasi perangkat keras sebenarnya. Selain itu, performa sistem seperti respons keypad, kestabilan mikrokontroler, dan ketahanan komponen terhadap penggunaan jangka panjang kemungkinan dapat mengalami perbedaan ketika diterapkan pada perangkat fisik. Oleh karena itu, penelitian ini masih memerlukan tahap pengembangan lanjutan berupa implementasi perangkat keras secara langsung agar kinerja sistem keamanan brankas digital dapat diuji dan dianalisis secara lebih akurat pada kondisi penggunaan nyata.

## 6. Kesimpulan

Berdasarkan hasil perancangan, simulasi, dan pengujian yang telah dilakukan, penelitian “Sistem Pengunci Brankas Digital dengan Password Otomatis Menggunakan Proteus” berhasil membangun sistem keamanan digital berbasis mikrokontroler ATmega8535 yang mampu bekerja sesuai fungsi yang dirancang. Sistem dapat melakukan proses autentikasi password menggunakan keypad matriks 4×4 sebagai media input utama, kemudian memproses data password untuk menentukan akses pembukaan maupun penolakan akses pada brankas digital. Hasil pengujian menunjukkan bahwa seluruh komponen seperti keypad, LCD 16×2, LED, speaker, dan sistem pengendali bekerja secara stabil selama simulasi berlangsung. LCD mampu menampilkan informasi kondisi sistem dengan baik, sedangkan LED dan speaker berhasil memberikan indikator visual dan suara ketika terjadi autentikasi benar maupun salah. Selain itu, penggunaan karakter bintang (\*) saat proses input password membantu menjaga keamanan data password sehingga sistem menjadi lebih aman dibandingkan sistem pengunci mekanik konvensional.

Penggunaan aplikasi Proteus pada penelitian ini juga memberikan hasil yang efektif dalam proses simulasi dan pengujian rangkaian elektronika secara virtual sebelum diterapkan pada perangkat keras nyata. Sistem mampu membaca input password secara berurutan, melakukan autentikasi otomatis, serta memberikan respons keamanan dengan cepat dan stabil dengan tingkat keberhasilan pengujian mencapai 100%. Berdasarkan hasil penelitian dan perbandingan dengan penelitian sebelumnya, sistem pengunci brankas digital berbasis password otomatis menggunakan Proteus memiliki keunggulan pada kesederhanaan sistem, kemudahan simulasi, serta efektivitas autentikasi berbasis password digital. Sistem ini dapat menjadi dasar pengembangan sistem keamanan yang lebih kompleks dengan penambahan fitur seperti RFID, sensor sidik jari, face recognition, maupun teknologi Internet of Things untuk monitoring dan pengendalian jarak jauh. Hasil keberhasilan 100% menunjukkan algoritma autentikasi dan proses *scanning* keypad berjalan tanpa konflik logika selama simulasi. Namun, hasil tersebut belum tentu identik pada implementasi perangkat keras karena adanya faktor noise, bounce tombol, dan fluktuasi tegangan.

Penelitian ini masih memiliki keterbatasan karena sistem yang dirancang dan diuji hanya dilakukan dalam bentuk simulasi menggunakan aplikasi Proteus dan belum diimplementasikan secara langsung pada perangkat keras nyata. Kondisi simulasi belum sepenuhnya mampu menggambarkan kondisi penggunaan sebenarnya seperti gangguan tegangan, kerusakan komponen, kestabilan perangkat, serta kesalahan pembacaan input yang dapat terjadi pada implementasi fisik. Oleh karena itu, penelitian selanjutnya disarankan untuk mengembangkan sistem dalam bentuk perangkat keras nyata agar performa sistem dapat diuji secara langsung pada kondisi sebenarnya. Selain itu, peneliti selanjutnya juga dapat menambahkan fitur keamanan lain seperti RFID, sensor sidik jari, notifikasi berbasis *Internet of Things*, maupun kamera monitoring agar sistem keamanan brankas digital menjadi lebih modern, aman, dan efisien.

**Kontribusi Penulis:** Konseptualisasi: Muhammad Agil Wahyudy dan Dwi Titi Maesaroh; Metodologi: Muhammad Agil Wahyudy; Perangkat Lunak: Muhammad Agil Wahyudy; Validasi: Muhammad Agil Wahyudy, Dwi Titi Maesaroh, dan Rihartanto; Analisis formal: Muhammad Agil Wahyudy; Investigasi: Muhammad Agil Wahyudy; Sumber daya: Muhammad Agil Wahyudy; Kurasi data: Muhammad Agil Wahyudy; Penulisan—persiapan

draf asli: Muhammad Agil Wahyudy; Penulisan—peninjauan dan penyuntingan: Dwi Titi Maesaroh dan Rihartanto; Visualisasi: Muhammad Agil Wahyudy; Supervisi: Dwi Titi Maesaroh dan Rihartanto; Administrasi proyek: Muhammad Agil Wahyudy; Akuisisi pendanaan: Tidak ada.

**Pendanaan:** Penelitian ini tidak menerima pendanaan eksternal.

**Pernyataan Ketersediaan Data:** Data yang digunakan dan dihasilkan dalam penelitian ini tersedia dari penulis korespondensi berdasarkan permintaan yang wajar. Seluruh data penelitian berupa hasil simulasi Proteus, source code mikrokontroler, serta hasil pengujian sistem digunakan untuk mendukung hasil penelitian yang dilaporkan dalam artikel ini.

**Ucapan Terima Kasih:** Penulis mengucapkan terima kasih kepada Program Studi Teknologi Informasi Politeknik Negeri Samarinda yang telah memberikan dukungan akademik dan fasilitas selama proses penelitian berlangsung. Penulis juga mengucapkan terima kasih kepada dosen pembimbing yang telah memberikan arahan, saran, dan masukan dalam proses penyusunan penelitian “Sistem Pengunci Brankas Digital dengan Password Otomatis Menggunakan Proteus”. Selain itu, penulis menyampaikan terima kasih kepada seluruh pihak yang telah membantu proses pengujian dan pengembangan sistem keamanan digital ini hingga penelitian dapat diselesaikan dengan baik.

**Konflik Kepentingan:** Penulis menyatakan tidak ada konflik kepentingan. Pendana tidak memiliki peran dalam desain studi, pengumpulan data, analisis atau interpretasi data, penulisan naskah, maupun keputusan untuk menerbitkan hasil penelitian.

## Referensi

- [1] N. Z. Khairul Agus Rizal, "Sistem Pengaman Brankas Menggunakan Kode Password dan Sidik Jari Berbasis Mikrokontroler," *Jurnal Litek*, vol. 13, no. 1, pp. 37-43.
- [2] M. R. N. A. K. A. B. Sri Hartanto, "Rancang Bangun Keamanan Pintu Brankas Menggunakan RFID RC-522 dan Modul IoT WEMOS-D1-R1," *Jurnal Elektro & Informatika Swadharma (JEIS)*, vol. 6, no. 1, pp. 99-110, 2026.
- [3] Z. A. Pangaribuan, "Prototype Sistem Keamanan Brankas Manual Berbasis Arduino Uno Dan Telegram," Universitas Sriwijaya, Palembang, 2023.
- [4] D. M. S. A. M. S. A. Md. Maksudur Rahman, "Password Protected Electronic Lock System for Smart Home Security," *International Journal of Engineering Research & Technology (IJERT)*, vol. 7, no. 4, pp. 541-544, 2018.
- [5] A. P. O. Armenia, "Rancang Bangun Kunci Pintu Berbasis Pengenal Suara Dengan Metode Mel Frequency Cepstral Coefficient (MFCC)," Universitas Satya Negara Indonesia, Jakarta, 2024.
- [6] N. S. K, "RANCANG BANGUN SISTEM PENGAMAN BRANKAS BERBASIS MIKROKONTROLER ATmega8535," UNIVERSITAS DIPONEGORO, SEMARANG, 2012.
- [7] A. M. Y. Widya Anggraini, "Design and Implementation of Buck-Boost Converter Using Atmega 8535 Microcontroller," *Journal of Industrial Automation and Electrical Engineering*, vol. 1, no. 1, pp. 98-104, 2024.
- [8] D. A. W. K. H. K. Dimas Candra Syahputra, "Home Door Security System Using Voice Recognition And Keypad Matrix Module," *JTECS Jurnal Sistem Telekomunikasi Elektronika Sistem Kontrol Power Sistem & Komputer*, vol. 2, no. 1, pp. 29-36., 2022.
- [9] S. S. d. C. W. Hidayat, "Development of Digital Engineering Learning with Proteus Software Media and Emulators Department of Informatics Engineering Kanjuruhan University.," *Journal of Physics Conference Series*, vol. 1869, no. 1, pp. 1-4, 2021.
- [10] J. S. A. E. H. T. N. S. K. Dr Bhramaramba Ravi, "Diabetic Retinopathy Detection and Classification Using Deep Learning Algorithm," *International Research Journal of Engineering and Technology (IRJET)*, vol. 11, no. 2, pp. 653-658, 2024.

- [11] C. N. D. A. C. W. E. W. Eric A. Brewer, "PROTEUS: A High-Performance Parallel-Architecture Simulator," *Performance Evaluation Review*, vol. 20, no. 1, pp. 247-248, 1992.
- [12] R. A. Mahardika, "RISLOCK (RFID SMART DOOR LOCK).," Universitas Dinamika, Surabaya, 2024.
- [13] G. M. Kadena, ": Rancang Bangun Sistem Pengaman Pintu Brankas Menggunakan Fingerprint dan Keypad Berbasis Arduino," Politeknik Negeri Bali, Bali, 2023.
- [14] P. K. J. T. A. C. S. R. Tarak Bharambe, "A Detailed Review on Video Steganography," *International Research Journal of Engineering and Technology (IRJET)*, vol. 10, no. 5, pp. 652-656, 2023.
- [15] J. A. Zarnan, "A Novel Approach For The Solution Of Urysohn Integral Equations Using Hermite Polynomials," *International Journal of Applied Engineering Research*, vol. 12, no. 24, pp. 14391-14395, 2017.
- [16] R. T. L. d. Susilawati, "Sistem Kunci Pintu Berbasis PIN Menggunakan Arduino dan Keypad," *JATI (Jurnal Mahasiswa Teknik Informatika)*, vol. 8, no. 3, pp. 3830-3835, 2024.
- [17] K. d. P. K. Okta Rea Arsyad, "Rancang Bangun Alat Pengaman Brankas Menggunakan Sensor Sidik Jari Berbasis Arduino," *JATI (Jurnal Mahasiswa Teknik Informatika)*, vol. 5, no. 1, pp. 1-7, 2021.
- [18] M. S. A. d. A. Z. Hasibuan, "Pengamanan Kunci Pintu Brankas Menggunakan Kriptografi One Time Pad (OTP) Berbasis Android," *EXPLORER Journal of Computer Science and Information Technology*, vol. 3, no. 2, pp. 58-68, 2023.
- [19] I. A. A. d. I. P. K. A. Kwabena Asare Baffour, "Proteus Simulation and Implementation of an Arduino Mega-Based Motion Detection Alarm System," *International Journal of Research and Scientific Innovation (IJRSI)*, vol. 11, no. 6, pp. 199-205, 2024.
- [20] H. K. A. L. d. L. I. S. Lilik Widyawati, "Implementasi Multi-Authentication pada Smart Door Lock Berbasis ESP8266," *Jurnal Teknologi Informasi dan Multimedia*, vol. 8, no. 2, pp. 318-329, 2026.
- [21] I. R. V. O. N. d. F. R. Hilda Maulida, "Sistem Proteksi Brankas Berbasis RFID dan Arduino UNO Menggunakan Metode Prototyping," *J-HyTEL: Journal Hypermedia & Technology-Enhanced Learning*, vol. 1, no. 2, pp. 87-94, 2023.