

Desain Sistem Deteksi Password pada Keypad dan LCD dengan Arduino melalui Tinkercard untuk Pembelajaran Elektronika

Riskawati ^{1*}, Fira Kurnia ², Nursam³, Noviyanti ⁴, Nurul Annisa ⁵, Putri Mawa Sari Aco ⁶, Nur Muliana ⁷

^{1, 2, 3, 4, 5, 6, 7} Universitas Negeri Makassar, Indonesia

* riskawati@unm.ac.id

Abstrak

Keamanan sistem berbasis elektronik menjadi kebutuhan penting dalam berbagai aplikasi, baik di bidang pendidikan, industri, maupun rumah tangga. Salah satu solusi sederhana namun efektif dalam mendeteksi akses adalah penggunaan sistem password. Penelitian ini bertujuan untuk merancang dan mensimulasikan sistem deteksi password menggunakan *Arduino Uno* sebagai mikrokontroler utama, dengan memanfaatkan keypad 4x4 sebagai alat input, LCD 16x2 sebagai media tampilan informasi, serta *buzzer* dan LED sebagai indikator umpan balik. Platform simulasi *Tinkercad* digunakan untuk mempermudah proses perancangan, pengujian, dan validasi sistem secara virtual sebelum implementasi fisik dilakukan. Metode penelitian meliputi perancangan rangkaian elektronik, pemrograman *Arduino* dengan bahasa C/C++, serta simulasi fungsional pada *Tinkercad* untuk menguji performa sistem. Hasil simulasi menunjukkan bahwa sistem mampu membaca input password dari keypad, memprosesnya melalui *mikrokontroler*, dan memberikan keluaran berupa status yang ditampilkan pada LCD. Jika password yang dimasukkan sesuai, LED hijau akan menyala dan *buzzer* tidak berbunyi; jika salah, LED merah akan menyala disertai bunyi *buzzer* sebagai peringatan. Penggunaan *Tinkercad* sebagai alat bantu simulasi terbukti efektif dalam mengidentifikasi kesalahan desain sejak tahap awal, sehingga menghemat waktu dan sumber daya. Penelitian ini memberikan kontribusi dalam pengembangan sistem keamanan berbasis *Arduino* dengan pendekatan yang sederhana, edukatif, dan aplikatif. Hasil dari penelitian ini dapat dijadikan sebagai model pembelajaran elektronika interaktif serta sebagai dasar pengembangan sistem keamanan digital yang lebih kompleks di masa depan.

Keywords: *Arduino, Keypad, Pembelajaran elektronika, Simulasi, Tinkercad*

Pendahuluan

Pembelajaran elektronika berbasis simulasi telah menjadi metode yang semakin populer dalam pendidikan teknologi, terutama untuk memahami konsep dasar sistem elektronik tanpa memerlukan perangkat keras yang mahal (Said & Herman, 2024). *Tinkercad*, sebagai platform desain dan simulasi elektronik online, memberikan kemudahan bagi siswa untuk merancang, menguji, dan memvisualisasikan rangkaian elektronik secara virtual (Malik et al., 2024). Salah satu aplikasi menarik dari *Tinkercad* adalah dalam desain sistem deteksi password menggunakan komponen-komponen sederhana seperti *Arduino*, keypad, dan LCD (Rohman & Alfarizi, 2022). Sistem semacam

ini tidak hanya memberikan pemahaman tentang elektronika dasar, tetapi juga memungkinkan siswa untuk belajar mengenai pemrograman mikrokontroler serta aplikasi sistem keamanan berbasis teknologi (Riskawati, 2025). Penelitian-penelitian sebelumnya menunjukkan potensi besar dari penggunaan *Arduino* dalam desain sistem keamanan, seperti yang telah dibuktikan oleh dalam desain sistem keamanan pintu menggunakan *password*.

Sistem ini menggunakan *Arduino* sebagai kontrol utama yang terhubung dengan *keypad* untuk input *password* dan LCD untuk menampilkan status akses (Khairunnisa & Parlin, 2021). Selain itu, terdapat temuan yang menyoroti pentingnya pengembangan sistem berbasis *Arduino* dalam berbagai konteks, seperti sistem keamanan dan kontrol perangkat (Agustini & Sanusi, 2024). Namun, meskipun sistem ini sudah banyak diterapkan di bidang lain, pengintegrasian simulasi *Tinkercad* dalam pembelajaran elektronika khususnya untuk desain sistem deteksi *password* masih minim, yang membuat penelitian ini relevan dalam pengembangan kurikulum pendidikan elektronika. Masalah utama dalam penelitian ini adalah bagaimana menggunakan *Tinkercad* untuk mengajarkan konsep dasar elektronika melalui desain sistem deteksi *password* yang melibatkan komponen *Arduino*, *keypad*, dan LCD. Salah satu solusi untuk mengatasi masalah ini adalah dengan memanfaatkan *Tinkercad* sebagai alat simulasi untuk merancang sistem secara virtual, sehingga mempermudah siswa dalam memahami interaksi antar komponen tanpa harus bergantung pada perangkat keras fisik. Selain itu, integrasi penggunaan *Arduino* sebagai mikrokontroler dalam sistem ini memungkinkan siswa untuk belajar tidak hanya tentang elektronika, tetapi juga pemrograman dan pengendalian sistem secara praktis (Ernes & Wirawan, 2021).

Beberapa penelitian menunjukkan penggunaan komponen-komponen seperti *keypad* dan LCD dalam berbagai aplikasi. Temuan yang menyoroti penggunaan *keypad* dalam sistem kontrol akses, yang memungkinkan pengguna memasukkan *password* untuk mengakses sistem (Artono & Putra, 2019). Penelitian ini memberikan dasar penting tentang bagaimana mengintegrasikan input pengguna dan output tampilan, serta pentingnya keamanan dalam desain sistem. Selain itu, studi lain juga mengembangkan sistem keamanan berbasis *Arduino* yang memanfaatkan *keypad* dan LCD untuk menampilkan status akses (Nataliana et al., 2017). Sistem ini menunjukkan bagaimana teknologi sederhana dapat digunakan untuk menciptakan solusi keamanan yang efektif, yang dapat diterapkan pada berbagai jenis perangkat elektronik (Ramdani & Nursuwarnas, 2022). Penggabungan teknologi RFID dengan sistem *keypad* untuk memberikan lapisan keamanan tambahan. Meskipun penelitian ini berfokus pada sistem keamanan dengan RFID, hal ini menunjukkan bahwa kombinasi teknologi dapat meningkatkan keamanan. Dalam konteks sistem deteksi *password*, menggabungkan *keypad* dengan teknologi lain, seperti pengenalan sidik jari atau RFID, dapat memberikan solusi yang lebih robust. Penelitian-penelitian tersebut menunjukkan bahwa penerapan komponen yang sudah terbukti efektif, seperti *keypad* dan LCD dalam desain *Arduino*, memberikan dasar yang kuat untuk pengembangan lebih lanjut dalam sistem keamanan berbasis *password* (Sattar et al., 2021).

Berbagai penelitian telah mengembangkan dan mengimplementasikan sistem keamanan berbasis *Arduino*. Namun, sejumlah celah masih ditemukan, khususnya dalam konteks pembelajaran elektronika dan simulasi virtual. Penelitian yang ada umumnya berfokus pada aspek teknis sistem, tanpa mengaitkan secara spesifik penggunaan

Tinkercad sebagai media pembelajaran dalam proses perancangan. Tinkercad memberikan kesempatan kepada siswa untuk memahami dan menguji sistem secara virtual sebelum dirakit dalam bentuk fisik. Pendekatan ini mempercepat pemahaman terhadap konsep dasar elektronika serta meningkatkan keterampilan teknis dalam merancang sistem keamanan berbasis Arduino (Win, 2020).

Beberapa penelitian juga mengusulkan penggunaan berbagai teknologi untuk memperkuat keamanan sistem, seperti penggabungan RFID atau biometrik, namun penelitian tentang pengembangan sistem deteksi *password* dengan hanya menggunakan *Arduino*, *keypad*, dan LCD masih terbatas. Penelitian ini bertujuan untuk mengisi celah tersebut dengan mengintegrasikan *Tinkercad* sebagai alat pembelajaran yang memungkinkan siswa merancang, mensimulasikan, dan memprogram sistem deteksi *password* secara praktis. Dengan demikian, penelitian ini memberikan kontribusi untuk mengembangkan kurikulum pendidikan elektronika yang lebih aplikatif dan interaktif.

Tujuan dari penelitian ini adalah untuk mengembangkan metode pembelajaran elektronika melalui *Tinkercad* dengan fokus pada desain dan simulasi sistem deteksi *password* berbasis *Arduino*, *keypad*, dan LCD. Penelitian ini bertujuan untuk memperkenalkan konsep dasar elektronika, pemrograman, dan pengendalian sistem kepada siswa melalui pengalaman praktis yang dapat diakses secara virtual. Kebaruan penelitian ini terletak pada pengintegrasian *Tinkercad* dalam pembelajaran elektronika, memungkinkan siswa untuk merancang dan menguji sistem secara virtual sebelum implementasi fisik. Selain itu, penelitian ini juga memperkenalkan konsep sistem deteksi *password* sebagai bagian dari aplikasi sistem keamanan yang sederhana namun efektif.

Ruang lingkup penelitian ini meliputi perancangan dan simulasi sistem deteksi *password* menggunakan *Arduino*, *keypad*, dan LCD dalam platform *Tinkercad*. Penelitian ini juga akan mengeksplorasi potensi pengembangan sistem dengan menambahkan fitur keamanan tambahan seperti RFID atau sidik jari, meskipun fokus utamanya adalah pada penggunaan *password* sebagai metode utama autentikasi. Penelitian ini akan dilakukan dengan merancang skema rangkaian, pemrograman *Arduino*, dan simulasi penggunaan *Tinkercad* sebagai alat untuk memvisualisasikan interaksi antara komponen.

Metode

Desain sistem deteksi *password* menggunakan *Arduino* dimulai dengan pemilihan komponen yang sesuai. Komponen utama yang digunakan adalah *Arduino Uno* sebagai mikrokontroler, *keypad* 4x4 sebagai input pengguna, LCD 16x2 untuk tampilan informasi, dan *buzzer* serta LED untuk memberikan umpan balik. *Arduino Uno* dipilih karena kemudahan penggunaannya, komunitas pengembang yang besar, dan ketersediaan pustaka perangkat lunak yang mendukung berbagai aplikasi. *Keypad* 4x4 digunakan untuk memasukkan *password*, memungkinkan pengguna untuk memilih kode rahasia melalui tombol numerik. LCD 16x2 dipilih karena kemampuannya menampilkan dua baris informasi secara jelas, yang akan menunjukkan status akses (terima/tolak) dan pesan kesalahan jika *password* yang dimasukkan tidak sesuai.

Buzzer dan LED berfungsi sebagai indikator untuk memberikan umpan balik berupa suara dan cahaya, yang memperjelas status sistem secara visual dan auditori (Shah et al., 2019). Komponen-komponen ini kemudian dihubungkan dengan *Arduino* menggunakan pin digital untuk *keypad*, dan pin I2C untuk LCD. Untuk meningkatkan kualitas simulasi,

platform *Tinkercad* digunakan untuk merancang dan menguji rangkaian tanpa memerlukan perangkat keras fisik. Dengan menggunakan *Tinkercad*, siswa dapat melakukan simulasi skema rangkaian, menguji fungsionalitas logika, dan melihat bagaimana perangkat keras dan perangkat lunak berinteraksi sebelum rangkaian diterapkan secara nyata. Ini mengurangi risiko kesalahan atau kerusakan pada komponen saat tahap pengujian fisik dilakukan. Sistem ini diharapkan dapat memberikan pembelajaran tentang cara menghubungkan dan mengontrol berbagai komponen elektronika dalam desain yang lebih kompleks.

Setelah pemilihan komponen, tahap berikutnya adalah pengembangan rangkaian sistem menggunakan *Tinkercad*. *Tinkercad* memungkinkan siswa untuk merancang rangkaian secara virtual, termasuk menghubungkan pin-keypad dengan pin digital *Arduino*, serta menghubungkan LCD melalui modul I2C untuk mempermudah koneksi. Buzzer dan LED juga terhubung dengan pin digital untuk memberikan output berdasarkan status sistem. *Tinkercad* mempermudah verifikasi awal dengan memberikan visualisasi rangkaian serta memfasilitasi pengujian fungsionalitas sistem secara real-time. Dalam simulasi, siswa dapat menguji alur input, pengolahan data, dan output tanpa menggunakan komponen fisik yang rawan rusak. Melalui simulasi ini, siswa juga dapat melakukan troubleshooting dan memverifikasi apakah semua komponen terhubung dengan benar dan berfungsi sesuai yang diharapkan.

Setelah merancang rangkaian secara virtual, langkah selanjutnya adalah melakukan pengujian logika sistem dengan memasukkan *password* melalui keypad dan memeriksa apakah sistem memberikan umpan balik yang sesuai melalui LCD, buzzer, dan LED. Jika *password* yang dimasukkan sesuai dengan *password* yang telah diprogram, sistem memberikan sinyal positif, misalnya dengan menyalakan LED hijau dan memberikan bunyi dari buzzer. Sebaliknya, jika *password* yang dimasukkan salah, sistem akan menampilkan pesan kesalahan di LCD dan memberikan sinyal suara berbeda melalui buzzer. *Tinkercad* memungkinkan simulasi yang interaktif ini untuk meminimalkan kesalahan dan meningkatkan pemahaman siswa mengenai interaksi perangkat keras dan perangkat lunak dalam sistem elektronika berbasis mikrokontroler.

Setelah desain rangkaian diselesaikan dan diuji di *Tinkercad*, tahap berikutnya adalah pemrograman *Arduino* untuk mengontrol perangkat. Kode pemrograman ditulis menggunakan IDE *Arduino* dengan bahasa C++, di mana logika sistem dirancang untuk membaca input dari keypad, memverifikasi *password* yang dimasukkan, dan mengendalikan output ke LCD serta indikator lainnya (LED dan buzzer). Pustaka tambahan seperti *Keypad.h* digunakan untuk memudahkan pembacaan input dari keypad, sedangkan pustaka *LiquidCrystal_I2C.h* digunakan untuk menyederhanakan komunikasi dengan LCD melalui protokol I2C. Pemrograman dilakukan dengan menulis fungsi untuk membandingkan input *password* dengan *password* yang telah ditetapkan sebelumnya. Jika cocok, LED hijau akan menyala dan buzzer berbunyi sebagai tanda akses berhasil. Jika *password* salah, LED merah menyala dan buzzer mengeluarkan bunyi sebagai indikator kegagalan.

Langkah-langkah pengkodean ini diikuti dengan proses uji coba yang intensif menggunakan *Tinkercad* untuk memastikan bahwa program berjalan sesuai dengan yang diinginkan. Dengan demikian, simulasi ini tidak hanya memberikan siswa pemahaman tentang cara menulis kode untuk mikrokontroler, tetapi juga tentang pentingnya penanganan kesalahan dalam pengembangan sistem. Setiap kesalahan yang muncul, baik

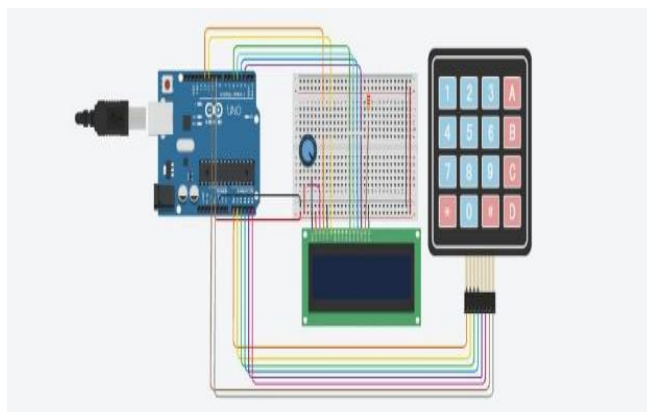
berupa kegagalan dalam pembacaan input, kesalahan logika dalam kode, atau koneksi yang salah antara komponen, dapat segera diperbaiki tanpa risiko kerusakan fisik pada perangkat keras. Setelah pengujian di *Tinkercad* berhasil, kode yang telah dibuat dapat diterapkan ke perangkat keras nyata untuk pengujian lebih lanjut.

Setelah rangkaian dan kode selesai, tahap selanjutnya adalah pengujian sistem di dunia nyata. Rangkaian fisik dirakit menggunakan komponen sebenarnya berdasarkan desain yang telah diuji di *Tinkercad*. Pengujian dilakukan dengan cara memasukkan *password* melalui *keypad* dan memeriksa respon sistem pada LCD, LED, dan *buzzer*. Evaluasi dilakukan untuk memastikan bahwa seluruh komponen bekerja sesuai dengan fungsinya, yaitu mendeteksi dan memverifikasi *password* yang dimasukkan, serta memberikan umpan balik yang tepat kepada pengguna. Selain itu, siswa diajak untuk melakukan troubleshooting pada tahap ini, baik terkait dengan kesalahan koneksi, kode yang belum optimal, maupun komponen yang tidak berfungsi sebagaimana mestinya.

Masalah yang umum ditemukan dalam pengujian fisik ini termasuk ketidaktepatan pembacaan input pada *keypad* atau kesalahan dalam pengaturan pin pada *Arduino*. Untuk mengatasi hal ini, siswa diminta untuk memeriksa koneksi, konfigurasi pin, serta memvalidasi kode pemrograman secara menyeluruh. Pengujian ini juga membantu siswa memahami keterbatasan dan tantangan yang dihadapi dalam implementasi sistem elektronik berbasis *Arduino*, serta memberikan mereka kesempatan untuk melakukan perbaikan dan pengembangan lebih lanjut, seperti menambahkan lapisan keamanan lain seperti RFID atau pengenalan sidik jari.

Hasil dan Pembahasan

Hasil Pengujian Sistem Monitoring Suhu Berbasis Arduino



Gambar 1. Desain Password Detection pada *Tinkercad*

Gambar tersebut menggambarkan diagram rangkaian untuk sistem deteksi *password* menggunakan *keypad* dan LCD berbasis *Arduino Uno*. Sistem ini dirancang untuk menerima input berupa angka atau karakter melalui *keypad*, memproses input tersebut menggunakan *Arduino*, dan menampilkan hasilnya pada layar LCD. Jika *password* yang dimasukkan sesuai dengan yang telah diprogram, sistem akan memberikan indikasi akses diterima, seperti menyalakan LED atau mengaktifkan relay. Sebaliknya, jika *password* salah, sistem menampilkan pesan akses ditolak. Kabel-kabel pada diagram menunjukkan hubungan antara *keypad*, LCD, *Arduino*, dan perangkat output. Sistem ini sering digunakan untuk mempelajari konsep autentikasi sederhana dan pemrograman mikrokontroler.

Desain sistem deteksi *password* menggunakan *Arduino*, *keypad*, dan LCD yang diilustrasikan dalam Gambar 1 mencerminkan penerapan prinsip fisika yang mendasari operasi berbagai komponen elektronik. Sistem ini memanfaatkan konsep arus listrik, hukum Ohm, dan interaksi optik serta mekanik untuk menjalankan fungsinya. *Arduino Uno* bertindak sebagai mikrokontroler utama yang mengontrol aliran arus listrik ke komponen lain, termasuk *keypad*, LCD, *buzzer*, dan LED. Dalam proses ini, hukum Ohm, yang menyatakan bahwa arus (I) berbanding lurus dengan tegangan (V) dan berbanding terbalik dengan resistansi (R), memainkan peran penting dalam menjaga kestabilan sistem (Herrera-Macías et al., 2021).

Ketika pengguna menekan tombol pada *keypad*, rangkaian resistansi berubah, menghasilkan sinyal arus yang kemudian diterjemahkan oleh *Arduino* menjadi data digital. Perubahan ini menunjukkan bagaimana prinsip dasar listrik digunakan untuk mendeteksi interaksi fisik pengguna. Selanjutnya, LCD menggunakan efek elektroluminesensi untuk menampilkan informasi. Ketika arus listrik mengalir melalui lapisan cairan kristal, molekul-molekul dalam cairan tersebut mengatur orientasinya sehingga memodulasi cahaya dan menampilkan pesan pada layar. Proses ini melibatkan interaksi antara arus listrik, materi, dan cahaya, yang merupakan aspek penting dalam fisika optik. *Buzzer* dalam sistem ini menggunakan prinsip *pizeoelektrik*. Ketika arus mengalir melalui elemen *pizeoelektrik*, elemen ini bergetar dan menghasilkan suara. Prinsip ini menunjukkan konversi energi listrik menjadi energi mekanik dan kemudian menjadi energi akustik, memperlihatkan transformasi energi sesuai hukum fisika. LED, di sisi lain, menggunakan sifat semikonduktor untuk mengubah arus listrik menjadi cahaya, yang menunjukkan bagaimana energi listrik dapat dirancang untuk memberikan umpan balik visual kepada pengguna.

Sistem ini dirancang dan diuji menggunakan platform simulasi *Tinkercad*, yang memungkinkan pengujian rangkaian virtual untuk memvalidasi fungsionalitas tanpa risiko kerusakan perangkat keras. Dengan memahami bagaimana hukum-hukum fisika diterapkan dalam desain ini, pengguna dapat mengoptimalkan interaksi antara komponen dan meningkatkan efisiensi sistem. Penelitian sebelumnya telah menunjukkan bahwa penguasaan prinsip fisika dapat memperbaiki kualitas desain elektronik, termasuk sistem berbasis *password* seperti ini. Desain ini adalah contoh nyata bagaimana teknologi modern dan konsep fisika saling berinteraksi untuk menciptakan sistem yang aman, efisien, dan aplikatif. Ini juga menunjukkan bagaimana perangkat elektronik sederhana dapat digunakan untuk mengatasi tantangan dunia nyata, seperti keamanan digital. Dengan memahami aspek fisika di balik komponen-komponen ini, siswa dan pengembang dapat merancang solusi yang lebih baik untuk tantangan teknologi masa depan.

Hasil simulasi dan implementasi desain sistem deteksi *password* menggunakan *Tinkercad* menunjukkan bahwa sistem ini berhasil berfungsi sesuai dengan tujuan awal. *Keypad* 4x4 digunakan untuk memasukkan input berupa *password*, yang kemudian diproses oleh *Arduino Uno* sebagai mikrokontroler utama. Output dari sistem ditampilkan pada LCD 16x2, yang menampilkan informasi status akses, seperti "Password Benar" atau "Password Salah." Selain itu, sistem juga memberikan umpan balik visual melalui LED dan umpan balik auditori melalui *buzzer*. Simulasi yang dilakukan di *Tinkercad* memverifikasi bahwa semua komponen dapat berfungsi secara terintegrasi tanpa adanya konflik antara perangkat keras dan perangkat lunak.

Sistem berhasil mengenali *password* yang benar dan memberikan akses dengan menyalakan LED hijau dan membunyikan *buzzer* dengan nada tertentu. Sebaliknya, untuk input *password* yang salah, LED merah menyala, dan *buzzer* berbunyi dengan nada berbeda, sesuai dengan logika yang telah diprogram. Kesuksesan simulasi menunjukkan bahwa *Tinkercad* dapat digunakan sebagai alat pembelajaran yang efektif untuk memahami desain rangkaian elektronik dan pemrograman *Arduino*. Hasil ini sejalan dengan temuan yang menunjukkan bahwa *Arduino*, *keypad*, dan LCD dapat diintegrasikan secara efisien untuk mendukung sistem keamanan berbasis *password* (Husni & Elfizon, 2022). Hasil dari penelitian ini mendukung dan memperluas temuan dari penelitian sebelumnya, seperti yang menyoroti keefektifan sistem berbasis *Arduino* dalam aplikasi keamanan, khususnya dalam implementasi *password* untuk mengontrol akses (Gaikwad, 2023). Namun, penelitian ini memberikan kontribusi tambahan dengan memanfaatkan *Tinkercad* sebagai alat simulasi untuk mendesain dan menguji sistem secara virtual sebelum dirakit secara fisik. Dengan menggunakan *Tinkercad*, proses pembelajaran menjadi lebih interaktif dan risiko kerusakan perangkat keras dapat diminimalkan.

Selain itu, dibandingkan dengan penelitian yang lebih berfokus pada kontrol sistem berbasis *Arduino* dalam aplikasi militer, penelitian ini menunjukkan bagaimana prinsip serupa dapat diterapkan pada sistem keamanan sehari-hari dengan desain yang lebih sederhana namun efektif (Adi et al., 2022). Integrasi komponen seperti *buzzer* untuk memberikan umpan balik auditori juga sesuai dengan temuan yang menunjukkan bahwa umpan balik suara dapat meningkatkan pengalaman pengguna dalam sistem keamanan rumah (Elsi et al., 2020). Temuan dari penelitian ini menunjukkan bahwa pembelajaran elektronika melalui *Tinkercad* dapat menjadi pendekatan yang efektif untuk mengajarkan konsep dasar elektronika, pemrograman, dan desain sistem kepada siswa. Dengan menggunakan simulasi, siswa dapat memahami bagaimana komponen elektronik seperti *keypad*, LCD, *buzzer*, dan LED bekerja bersama dalam satu sistem yang dikontrol oleh mikrokontroler *Arduino*. Proses ini tidak hanya memberikan pemahaman teoretis tetapi juga keterampilan praktis yang relevan dengan kebutuhan industri modern.

Selain itu, sistem ini memberikan gambaran tentang pentingnya keamanan dalam desain perangkat elektronik. Dengan menanamkan konsep keamanan melalui sistem deteksi *password*, siswa belajar bagaimana teknologi dapat digunakan untuk melindungi akses ke informasi atau aset penting. Penelitian ini juga menunjukkan bahwa sistem sederhana seperti ini dapat dikembangkan lebih lanjut, misalnya dengan menambahkan fitur RFID atau sidik jari (Costaner et al., 2022). Potensi pengembangan ini menunjukkan fleksibilitas dan skalabilitas desain berbasis *Arduino* dalam memenuhi kebutuhan yang lebih kompleks.

Implikasi dari penelitian ini mencakup dua aspek utama: pembelajaran dan penerapan teknologi. Dari sisi pembelajaran, penelitian ini menegaskan bahwa penggunaan *Tinkercad* sebagai platform simulasi sangat mendukung proses belajar siswa, terutama dalam memahami interaksi antara perangkat keras dan perangkat lunak. Dengan kemampuan untuk mendesain, memprogram, dan menguji sistem secara virtual, *Tinkercad* memungkinkan siswa untuk bereksperimen tanpa risiko kerusakan perangkat keras. Desain sistem deteksi *password* ini dapat digunakan sebagai prototipe untuk aplikasi keamanan sederhana, seperti pengamanan pintu atau perangkat. Sistem ini juga dapat diperluas dengan mengintegrasikan fitur IoT untuk memungkinkan pengendalian jarak jauh, seperti yang diusulkan dalam pengembangan sistem berbasis RFID dan IoT

(Hasanah et al., 2023). Potensi pengembangan ini mencakup integrasi dengan aplikasi mobile atau sistem cloud untuk meningkatkan fleksibilitas dan fungsi keamanan.

Penelitian ini menunjukkan bahwa kombinasi pembelajaran berbasis simulasi dengan penerapan teknologi sederhana dapat menjadi pendekatan yang efektif untuk mempersiapkan siswa menghadapi tantangan di bidang teknologi dan rekayasa. Dengan memahami dasar-dasar desain sistem seperti ini, siswa tidak hanya menguasai keterampilan teknis tetapi juga konsep-konsep penting dalam pengembangan teknologi yang lebih kompleks di masa depan.

Kesimpulan

Penelitian ini berhasil menunjukkan bahwa pembelajaran elektronika melalui *Tinkercad* dengan fokus pada desain sistem deteksi *password* menggunakan *Arduino*, *keypad*, dan LCD merupakan metode yang efektif untuk meningkatkan pemahaman siswa tentang konsep elektronika, pemrograman, dan desain sistem keamanan. Dengan memanfaatkan *Tinkercad*, siswa dapat merancang, mensimulasikan, dan menguji rangkaian elektronik secara virtual, sehingga mengurangi risiko kesalahan dan mempermudah proses pembelajaran. Hasil penelitian menunjukkan bahwa sistem deteksi *password* yang dirancang mampu bekerja sesuai dengan tujuan. Sistem ini dapat mengenali input *password* dari *keypad*, memprosesnya menggunakan *Arduino*, dan memberikan respon melalui tampilan pada LCD, serta indikator visual dan auditori menggunakan LED dan *buzzer*. Keberhasilan ini membuktikan bahwa desain sistem yang sederhana namun terstruktur dapat menghasilkan solusi keamanan yang efektif. Selain itu, penelitian ini menyoroti potensi pengembangan sistem yang lebih kompleks, seperti penambahan fitur keamanan tambahan menggunakan teknologi modern untuk meningkatkan tingkat keamanan. Pendekatan ini tidak hanya relevan dalam pembelajaran, tetapi juga dapat diterapkan dalam berbagai solusi keamanan di kehidupan nyata.

Meskipun demikian, penelitian ini memiliki keterbatasan dalam implementasi pada perangkat fisik yang lebih luas. Pengembangan lebih lanjut dapat dilakukan dengan mengeksplorasi teknologi tambahan dan memperluas aplikasi sistem ini untuk kebutuhan yang lebih kompleks. Secara keseluruhan, penelitian ini menunjukkan bahwa penggunaan *Tinkercad* sebagai alat pembelajaran memberikan nilai tambah yang signifikan dalam mengajarkan konsep dan keterampilan elektronika secara praktis dan aplikatif.

Acknowledgment

-

Daftar Pustaka

- Adi, I. M. T., Widiatmoko, D., & Suryadi, K. (2022). Elektronika Sistem Senjata Pengisi Munisi Pada Magazen Senjata Ss2-V4 Berbasis *Arduino* Mega 2560 Guna Mendukung Latihan Menembak: Teknologi. *Jurnal Elkasista*, 3(1), 29-34.
- Agustini, S., & Sanusi, D. K. (2024). Pengaruh *Tinkercad* sebagai Media Pembelajaran Elektronika Dasar melalui Proyek Digital measuring device. *Jurnal Pendidikan Fisika Undiksha*, 14(3), 532-540. <https://doi.org/10.23887/jjpf.v14i3.87280>

- Artono, B., & Putra, R. (2019). Penerapan internet of things (IoT) untuk kontrol akses keamanan berbasis password. *Jurnal Teknologi Informasi dan Terapan*, 5(1), 16-22. <https://doi.org/10.25047/jtit.v5i1.16>
- Costaner, L., Zamsuri, A., & Putra, P. P. (2022). Implementasi Simulasi Elektronika dan Arduino Virtual dengan Circuit Tinkercad. *J-COSCI: Journal of Computer Science Community Service*, 2(2), 109-116. <https://doi.org/10.31849/jcscis.v2i2.9139>
- Elsi, Z. R. S., Widyastuti, M. A., Primaini, S., & Apriansyah, A. (2020). Perancangan Sistem Keamanan Pintu Keluar Masuk Ruang Dengan Password. *Jurnal Digital Teknologi Informasi*, 3(2), 61-66. <https://doi.org/10.32502/digital.v3i2.2754>
- Ernes, R. N., & Wirawan, N. T. (2021). Pengimplementasian Artificial Intelligence pada Sistem Keamanan Locker Otomatis berbasis SMS Gateway dan Radio Frequency Identification. *Jurnal KomtekInfo*, 8(1), 57-65. <https://doi.org/10.35134/komtekinfo.v8i1.98>
- Gaikwad, P. (2023). Optimizing urban street lighting: a smart approach using iot. *International Journal for Research in Applied Science and Engineering Technology*, 11(9), 1494-1499. <https://doi.org/10.22214/ijraset.2023.55848>
- Hasanah, A., Ferdianty, C., Silvira, L., Farika, N., Faradillah, N., & Harijanto, A. (2023). Rancang Bangun Alat Peraga Water Heater Menggunakan Heater Portable Dan Sensor Ds18b20 Berbasis Arduino Uno R3 Pada Konsep Termodinamika. *Jurnal Ilmiah Wahana Pendidikan*, 9(12), 19-28. <https://doi.org/10.5281/zenodo.8067619>
- Herrera-Macías, J., Legón-Pérez, C., Suárez-Plasencia, L., Piñeiro-Díaz, L., Rojas, O., & Sosa-Gómez, G. (2021). Test for detection of weak graphic passwords in passpoint based on the mean distance between points. *Symmetry*, 13(5), 777. <https://doi.org/10.3390/sym13050777>
- Husni, M. F., & Elfizon, E. (2022). Rancang Bangun Pengaman Brankas Menggunakan RFID (Radio Frequency Identification), Pin Dan GPS Berbasis Arduino Mega dan Internet Of Things (Iot). *Ranah Research: Journal of Multidisciplinary Research and Development*, 4(2), 140-149.
- Khairunnisa, N., & Parlin, I. (2021). Implementasi sistem kontrol akses berbasis mikrokontroler dengan tampilan LCD. *Jurnal Penelitian Inovatif*, 14(2), 78-85. <https://doi.org/10.1080/1055.14.1055>
- Malik, M., Burhanuddin, A., & Mukhtar, A. (2024). Sistem Smart Home Berbasis Arduino Dengan Simulasi Tinkercad. *Jurnal Teknik Mesin Universits PGRI Semarang NISSIN*, 3(1), 31-41.
- Nataliana, D., ANWARI, S., & AKBAR, M. S. (2017). Implementasi Prototype Sistem Home Security dengan Pemanfaatan Kode Akses berbasis Arduino Mega. *ELKOMIKA: Jurnal Teknik Energi Elektrik, Teknik Telekomunikasi, & Teknik Elektronika*, 5(2), 119. <https://doi.org/10.26760/elkomika.v5i2.119>
- Ramdani, M. A., & Nursuwars, F. M. (2022). Komunikasi Data pada Penyewaan Sepeda Motor berbasis Internet of Things. *E-JOINT (Electronica and Electrical Journal Of Innovation Technology)*, 3(1), 42-47. <https://doi.org/10.35970/e-joint.v3i1.1626>

- Riskawati, R. (2025). Integrasi Simulasi Tinkercad dan Arduino untuk Pembelajaran Fisika: Inovasi Media Edukatif dalam Topik Pola Cahaya LED. *WANUA TO CARADDE: Journal of Educational Issues*, 1(1), 37-45.
- Rohman, A., & Alfarizi, H. (2022). Desain perangkat keamanan menggunakan keypad dan LCD untuk kontrol akses ruangan. *Jurnal Teknik Elektro Indonesia*, 9(3), 45-56. <https://doi.org/10.33050/jtei.v9i3.45>
- Said, S., & Herman, N. M. (2024). Efektivitas Simulasi Pola LED Menggunakan Tinkercad: Media Pembelajaran Inovatif pada Elektronika Dasar. *Jurnal Pendidikan Fisika Undiksha*, 14(3), 524-531. <https://doi.org/10.23887/jjpf.v14i3.87201>
- Sattar, M. K., Waseem, M., Fayyaz, S., Kalsoom, R., Hussain, H. A., & Saddique, M. S. (2021). IoT based fault detection and protection of power transformer in the smart grid. *Engineering Proceedings*, 12(1), 7. <https://doi.org/10.3390/engproc2021012007>
- Shah, H., Abdullah, M., Kamis, Z., & Sallehoddin, M. (2019). Desain sistem pengamanan berbasis keypad dan LCD untuk aplikasi rumah pintar. *Indonesian Journal of Electrical Engineering and Computer Science*, 15(1), 104-112. <https://doi.org/10.11591/ijeecs.v15.i1.pp104-112>
- Win, K., & Win, N. (2020). Sistem deteksi password menggunakan Arduino untuk aplikasi keamanan rumah. *International Journal of Advances in Scientific Research and Engineering*, 6(5), 82-87. <https://doi.org/10.31695/ijasre.2020.33807>