TRANSMISI: JURNAL ILMIAH TEKNIK ELEKTRO, 27, (1), JANUARI 2025
p-ISSN 1411-0814 e-ISSN 2407-6422

IMPLEMENTASI *FINGERPRINT* PADA RANCANGAN PROTOTIPE *SMART HOME* MENGGUNAKAN METODE KEAMANAN KRIPTOGRAFI *VIGENERE CIPHER* DAN *CAESAR CIPHER*

Dinah Salsabila, Suroso[*)] dan Jon Endri

Jurusan Teknik Elektro, Program Studi Sarjana Terapan Teknik Telekomunikasi, Politeknik Negeri Sriwijaya, Palembang, Indonesia

[*)] *Penulis korespondensi, E-mail: osorus11@gmail.com*

Abstrak

Meningkatnya angka kriminalitas dan pemborosan energi listrik menjadi perhatian utama dalam pengembangan teknologi rumah pintar (*Smart Home*). Penelitian ini bertujuan untuk mengembangkan prototipe *Smart Home* berbasis autentikasi sidik jari (*Fingerprint*) yang diperkuat dengan metode keamanan kriptografi *Vigenere Cipher* dan *Caesar Cipher*. Sistem ini dirancang untuk mengontrol akses pintu, lampu, dan alarm, sekaligus melindungi data yang ditransmisikan dalam lingkungan *Smart Home*. Penelitian ini meliputi perancangan perangkat keras dan lunak, pengujian integrasi, serta analisis performa sistem. Hasil pengujian menunjukkan bahwa sistem *Fingerprint* mampu memverifikasi dan menolak sidik jari dengan tingkat keberhasilan 100%, menunjukkan keandalan autentikasi. Metode kriptografi *Vigenere Cipher* dan *Caesar Cipher* efektif dalam mengenkripsi dan melindungi data selama transmisi, memastikan keamanan informasi dari serangan pihak ketiga. Prototipe menunjukkan integrasi yang baik antara perangkat keras dan perangkat lunak, dengan kontrol perangkat melalui sensor *Fingerprint* dan website yang berfungsi optimal. Sistem memiliki waktu respon yang cepat, yaitu 1 detik untuk autentikasi sidik jari, 0.5 detik untuk enkripsi *Vigenere Cipher*, 0.3 detik untuk *Caesar Cipher*, dan 0.2 detik untuk pengiriman data melalui website. Hasil ini membuktikan bahwa prototipe yang dikembangkan andal, efisien, dan aman untuk mendukung teknologi rumah pintar.

Kata kunci: Smart Home, Fingerprint, Kriptografi Vigenere Cipher dan Caesar Cipher, Keamanan, Autentikasi, Kontrol Akses

Abstract

The increasing crime rate and waste of electrical energy are the main concerns in the development of smart home technology. This research aims to develop a Smart Home prototype based on fingerprint authentication which is strengthened by the Vigenere Cipher and Caesar Cipher cryptographic security methods. The system is designed to control access to doors, lights, and alarms, while protecting data transmitted within the Smart Home environment. This research includes hardware and software design, integration testing, and system performance analysis. The test results show that the Fingerprint system is able to verify and reject Fingerprints with a 100% success rate, demonstrating the reliability of authentication. The cryptographic methods of Vigenere Cipher and Caesar Cipher are effective in encrypting and protecting data during transmission, ensuring information security from third-party attacks. The prototype shows good integration between hardware and software, with device control via the Fingerprint sensor and an optimally functioning website. The system has a fast response time, which is 1 second for Fingerprint authentication, 0.5 seconds for Vigenere Cipher encryption, 0.3 seconds for Caesar Cipher, and 0.2 seconds for sending data through the website. These results prove that the prototype developed is reliable, efficient, and safe to support Smart Home technology.

Keywords: Smart Home, Fingerprint, Vigenere Cipher and Caesar Cipher Cryptography, Security, Authentication, Access Control

1. Pendahuluan

Keamanan dan pemborosan energi listrik, menjadi salah satu aspek yang perlu diperhatikan. Menurut data kasus kejahatan terhadap hak milik/barang pencurian meningkat. Jumlah pencurian di Indonesia pada tahun 2016 sebanyak 26.636 kasus, dan pada tahun 2017 kejahatan pencurian meningkat menjadi 28.313 kasus [1]. Sementara itu, penggunaan listrik yang berlebihan sering terjadi di kalangan masyarakat, misalnya lampu yang tidak dimatikan ketika gedung (ruangan/rumah/kantor) ditinggalkan oleh pemiliknya, atau lupa mematikan alat elektronik seperti, lampu dan pendingin ruangan [2].

Kelengahan pemilik rumah menjadi faktor utama banyaknya tindak kriminal, seperti lupa mengunci pintu atau meninggalkannya dalam keadaan lampu mati [3]. Kebiasaan menyalakan lampu pada gedung (ruangan/rumah/kantor) yang ditinggalkan dalam waktu lama, menyebabkan pemborosan energi listrik, meskipun hal tersebut dilakukan dengan maksud keamanan, supaya penyusup dapat terlihat oleh orang lain. Kebiasaan seperti ini mungkin sedikit meningkatkan keamanan, tetapi memiliki dampak yang menyebabkan pemborosan energi listrik. Dengan tingginya angka kriminalitas khususnya pencurian yang terjadi saat ini, maka sistem keamanan menjadi kebutuhan yang mutlak untuk diterapkan [4]. *Smart Home* atau ruangan pintar adalah ruangan yang benda-benda di dalam ruangan tersebut dikendalikan secara mudah dan efisien oleh penggunanya, dalam hal ini benda-benda tersebut adalah benda-benda elektronika yang biasa terdapat pada sebuah ruangan seperti lampu, dan kunci pintu [5]. Namun, penerapan teknologi seperti Smart Home juga membutuhkan perhatian terhadap aspek keamanan data, terutama dalam konteks sistem berbasis Internet of Things (IoT) [6].

Aspek keamanan data menjadi hal yang krusial dalam berbagai aplikasi teknologi informasi. Beragam metode enkripsi telah dirancang untuk meningkatkan perlindungan data, di antaranya *Advanced Encryption Standard* (AES) [7]. AES dikenal memiliki tingkat keamanan yang sangat tinggi, tetapi sering kali memerlukan sumber daya komputasi yang signifikan, sehingga kurang optimal untuk aplikasi dengan keterbatasan perangkat keras seperti sistem IoT [8]. Meskipun sangat aman, AES memiliki kebutuhan komputasi yang tinggi, yang membuatnya kurang cocok untuk perangkat dengan sumber daya sehari-hari. Sebaliknya, Metode klasik yang digunakan dalam penelitian ini memberikan keuntungan dalam efisiensi pada perangkat berdaya rendah. *Vigenere Cipher* dan *Caesar Cipher* menawarkan kecepatan dan kemudahan dalam implementasi, yang sangat cocok dengan sistem IoT.[9].

Pada penelitian Dani Usman, Elis Wulandari dan Feri Siswoyo Hadisantoso dengan judul "Implementasi Fingerprint Dan IOT Untuk Pengaman Ruangan", penelitian ini dirancang alat ini Internet of Things digunakan untuk membuka dan menutup pintu dan memonitor keadaan pintu pada saat pintu terbuka dan pitu tertutup dengan menggunakan aplikasi blynk yang terhubung dengan Node MCU Esp8266. Pada alat ini menggunakan Arduino mega 2560 sebagai kontroller untuk kontrol utama pada alat. *Fingerprint* sebagai ID untuk menggunakan sistem pengaman pintu. Modul *Fingerprint* ini mengidentetifikasi sidik jari sehingga sangat sulit untuk dipalsukan karena sidik jari setiap orang berbeda. Pada sistem pengaman ruangan digunakan megnetik doorlock sebagai kunci pintu. Magnetic doorlock memiliki sifat kemagnetan yang sangat kuat. Sehingga pada alat ini hanya pengguna yang memiliki ID yang dapat melakukan akses terhadap ruangan. Data pengaman ruangan tersimpan pada database di log yang berbentuk file. Pada alat ini semua sistem dalam keadaan baik dan dapat bekerja sesuai fungsinya, serta keakuratan waktu pada saat penggunakan melakukan akses hanya memiliki perbedaan waktu beberapa detik saja, sehingga dapat dinyatakan bahwa waktu yang ada didatabase akurat [10].

Pada penelitian Muhammad Sutrisno dengan judul "Prototipe Sistem keamanan dan Otomatisasi Rumah Pintar Berbasis Internet Of Things (IOT)" penelitian ini dirancang dengan sistem *Smart Home* dengan mengimplementasikan dua fitur, yaitu sistem keamanan dan sistem otomatisasi. Sistem ini menerapkan konsep internet of things (IoT) menggunakan aplikasi mobile yang berjalan pada sistem operasi android sehingga dapat dipantau dan dikendalikan secara real time melalui smartphone dengan dilengkapi notifikasi pada android. Mikrokontroler yang digunakan yaitu Arduino Mega sebagai pusat pengendalian fitur sistem keamanan dan otomatisasi serta digunakan mikrokontroler nodeMCU sebagai jembatan bagi Arduino Mega untuk berkomunikasi dengan internet. Sensor yang digunakan adalah magnetic switch untuk mendeteksi kondisi daun pintu, fingerprint scanner sebagai media verifikasi sidik jari, sensor MQ-2 untuk mendeteksi kebocoran gas. Real Time Clock (RTC) sebagai referensi waktu atau acuan realtime dan untuk menyalakan atau mematikan lampu outdoor secara otomatis, dan sensor ultrasonik untuk menyalakan atau mematikan lampu outdoor secara otomatis, dan sensor ultrasonik untuk menyalakan atau mematikan lampu dan pendingin ketika mendeteksi adanya orang masuk ruangan [11].

Pada penelitian Rizki Tahara Shita dan Laauw Li Hin dengan judul "Implementasi Sensor *Fingerprint Smartphone* Android dan Mikrokontroler NODE MCU dalam Mengamankan Kendaran", penelitian ini dirancang dengan pemnanfaatan sensor *Fingerprint* dapat juga digunkaan untuk menambah tingkat keamanan dengan menerapkannya pada saat menyalakan maupun mematikan mesin kendaraan, sehingga tingkat keamanan tidak saja hanya menggunakan kunci kendaraan yang bisa digunakan pada umumnya [12].

Dari penelitian yang telah dilakukan sebelumnya, teknologi *Fingerprint* (Sidik Jari) dan Internet of Things (IoT) telah diterapkan pada sistem keamanan rumah dan kendaraan. Namun, masih ada beberapa keterbatasan yang berkaitan dengan kerentanan terhadap akses ilegal. Di samping itu, masih banyak penelitian yang belum mengintegrasikan metode keamanan kriptografi dalam meningkatkan perlindungan data dalam sistem *Smart Home*.

Oleh karena itu, penelitian ini bertujuan untuk mengembangkan prototipe Smart Home yang memanfaatkan teknologi *Fingerprint* dan diperkuat dengan

metode kriptografi *Vigenere Cipher* dan *Caesar Cipher*. Dengan demikian, penelitian ini tidak hanya hanya memperluas pengetahuan tentang solusi keamanan dalam *Smart Home*, tetapi juga memberikan kontribusi praktis dalam menciptakan sistem yang lebih aman, andal, dan efisien untuk rumah pintar masa depan.

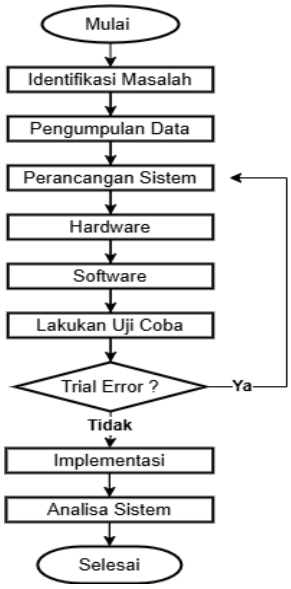
2. Metode

Dalam penelitian ini, menggunakan dua algoritma kriptografi klasik, Vigenere Cipher dan Caesar Cipher, untuk mengamankan data yang dikirim ke prototipe Smart Home. Algoritma-algoritma ini dipilih karena kecepatan dan kemudahan penggunaan mereka untuk perangkat berdaya rendah seperti NodeMCU dan Arduino [13].

1. Vigenere Cipher adalah teknik enkripsi berbasis substitusi polialfabetik yang menggunakan kunci yang diulangi untuk enkripsi setiap karakter dalam pesan. Dibandingkan dengan metode konvensional seperti Caesar Cipher, metode ini memiliki keunggulan dalam memberikan variasi pola enkripsi [14]. Namun, kelemahannya adalah keamanannya lebih rendah daripada algoritma modern karena rentan terhadap analisis frekuensi, terutama dalam kasus kunci yang tidak cukup panjang.
2. Caesar Cipher adalah mengubah karakter berdasarkan jumlah pergeseran tertentu [15]. Dalam penelitian ini, teknik ini digunakan sebagai tambahan enkripsi untuk melindungi data dari serangan dasar. Keunggulannya adalah proses enkripsi dan dekripsi yang sangat cepat, tetapi pola enkripsi yang terlalu sederhana.

2.1. Kerangka Penelitian

Adapun langkah-langkah penelitian yang akan dilakukan adalah sebagai berikut:



Gambar 1. Kerangka Penelitian

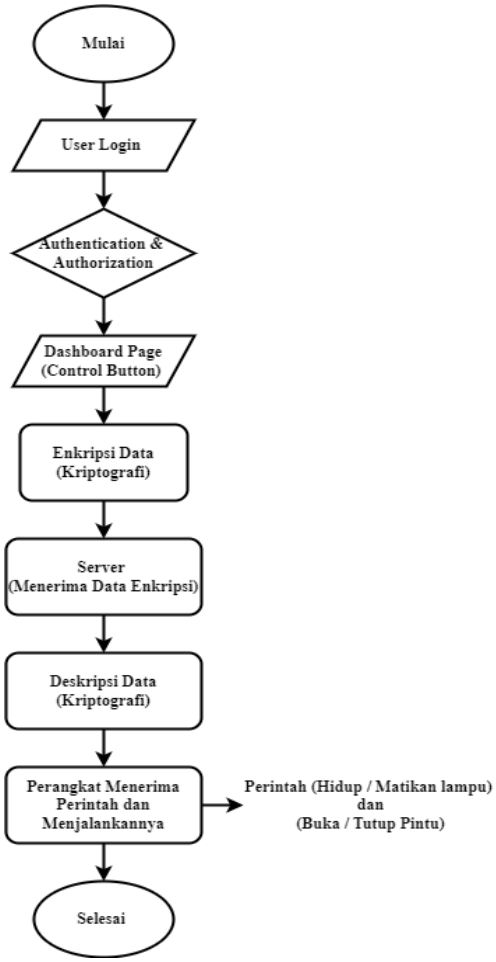
Berikut merupakan penjelasan dari diagram penelitian: 1) Mulai, 2) melakukan identifikasi masalah yang berkaitan dengan implementasi *Fingerprint* pada rancangan prototipe *Smart Home* menggunakan metode keamanan kriptografi berbasis internet of things. Langkah ini meliputi penentuan permasalahan yang mungkin muncul serta pencarian solusi yang sesuai untuk mengatasi permasalahan tersebut. 3) Melakukan pengumpulan data melalui studi literatur untuk mendapatkan informasi dari berbagai sumber seperti buku, jurnal, dan internet. Data yang terkumpul akan menjadi dasar referensi dalam penyusunan penelitian ini. 4) Setelah data terkumpul, dilakukan perancangan sistem yang mencakup aspek hardware dan software. Uji coba sistem dilakukan untuk memastikan keberhasilan implementasi, dan jika ditemukan kesalahan atau kegagalan, dilakukan analisis dan perbaikan sebelum melanjukan ke tahap selanjutnya. 5) Tahap implementasi melibatkan penerapan teknologi *Fingerprint* pada rancangan prototipe *Smart Home* menggunakan metode keamanan kriptografi berbasis internet of things. Implementasi dilakukan sesuai dengan desain yang telah dirancang sebelumnya. 6) Selanjutnya dilakukan analisis terhadap hasil implementasi serta pengambilan kesimpulan berdasarkan analisis tersebut. Tahapan inimerupakan tahap akhir dari penelitian, dimana hasil akhir dan kesimpulan penelitian dapat disusun. 7) Selesai.

2.2. Perancangan Perangkat

Dalam penelitian ini, pengembangan perangkat meliputi dua bagian utama yaitu pembuatan perangkat keras *(Hardware)* dan pembuatan perangkat lunak *(Software)*. Langkah pertama dalam pembuatan perangkat keras *(Hardware)* adalah membuat diagram blok untuk semua komponen yang digunakan secara keseluruhan.

2.2.1. Perancangan Perangkat Lunak *(Software)*

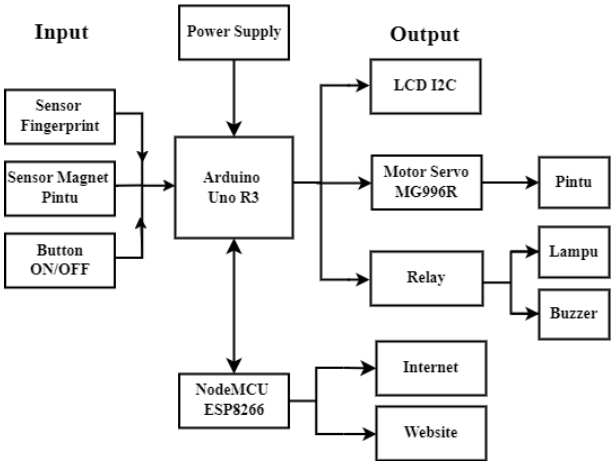
Berdasarkan flowchart yang ada pada gambar 2 tersebut dapat dipahami bahwa alur program dimulai dengan laman login yang menggunakan username dan password yang telah dibuat lalu setelahnya diarahkan ke halaman dashboard yang menampilkan kontrol button dari pintu, lampu, dan alarm lalu dari data tersebut di enkripsi menggunakan kriptografi *Vigenere Cipher* dan *Caesar Cipher* dan dihubungkan ke realtime database, selanjutnya perangkat alat menerima perintah dari server jika sebelumnya tidak ada perintah dari alat tersebut untuk menjalankannya.



Gambar 2. Flowchart Perangkat Lunak Web *(Software*)

2.2.2. Perancangan Perangkat Keras *(Hardware)*

Diagram blok merupakan suatu elemen penting dalam penelitian suatu perangkat. Hal ini dikarenakan diagram blok memungkinkan pemahaman tentang fungsi keseluruhan rangkaian.

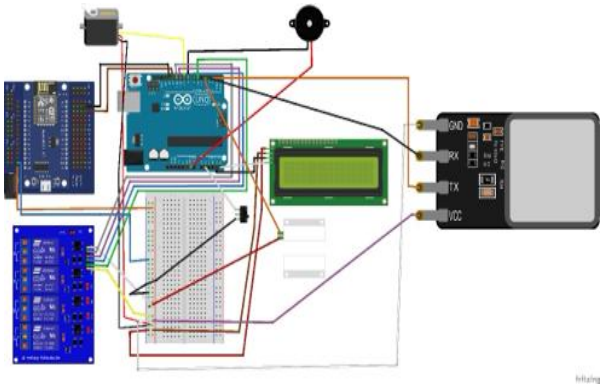


Gambar 3. Blok Diagram Perangkat Keras *(Hardware)*

Adapun penjelasan dari blok diagram tersebut yaitu: 1) NodeMCU digunakan untuk mengontrol dan mengirimkan data dari sensor dan perangkat lain ke server. 2) Arduino Uno digunakan untuk mengontrol relay yang mengendalikan perangkat listrik, serta berfungsi sebagai antarmuka untuk sensor dan LCD. 3) Sensor *Fingerprint* digunakan untuk mendeteksi sidik jari pengguna untuk otentikasi. 4) Relay untuk mengontrol daya ke perangkat seperti kunci pintu dan lampu. 5) Buzzer sebagai objek untuk menggantikan alarm pengingat pada pemilikrumah. 6) Sensor magnet pintu untuk mendeteksi status terbuka dan tertutupnya pintu. 7) LCD I2C digunakan untuk menampilkan informasi seperti pesan status atau intruksi kepada pengguna. 8) Power Supply digunakan untuk memberikan daya ke semua komponen dalam sistem. 9) Button digunakan untuk menghidupkan dan mematikan perangkat. 10) Website digunakan untuk mengatur antarmuka pengguna dan database yang mengakses dan mengontrol perangkat secara remote melalui internet.

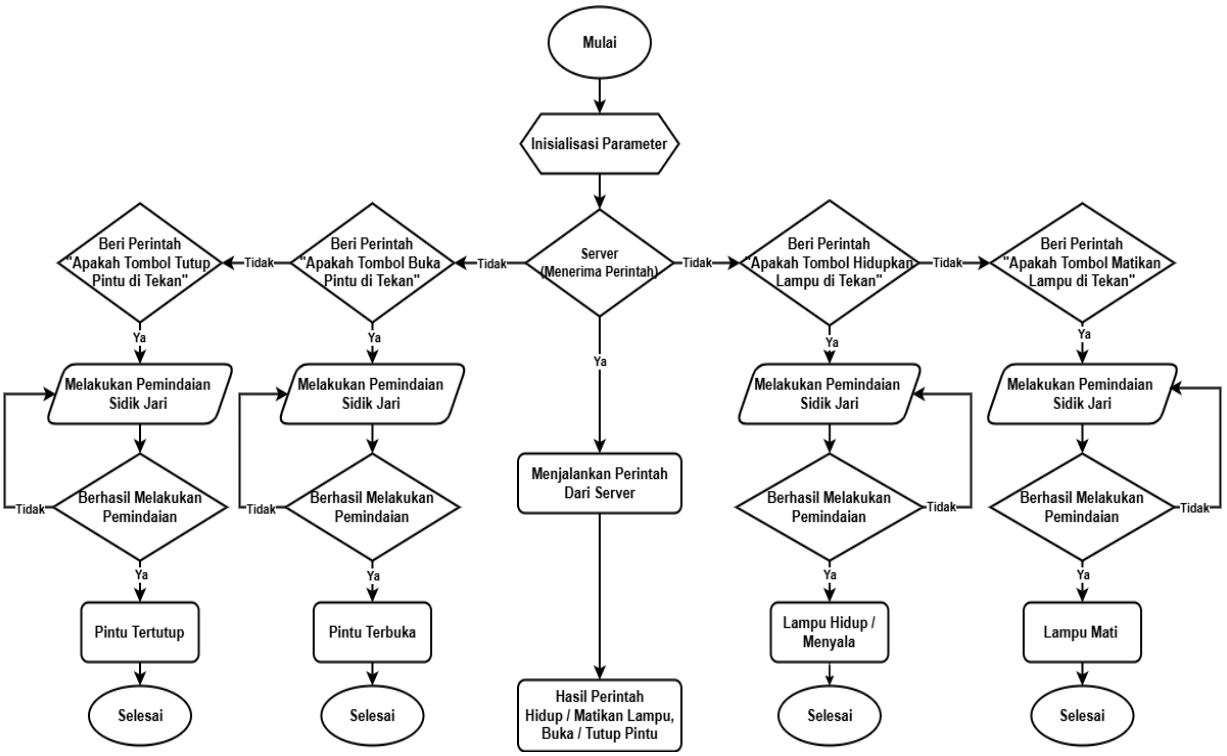
2.2.3. Skema Rangkaian

Skema Rangkaian adalah gambaran visual dari rangkaian elektronik yang menunjukan komponen perangkat keras *(Hardware)* dan cara mereka terhubung satu sama lain. Berikut adalah skema rangkaian perangkat keras *(Hardware)*:



Gambar 4. Skema Rangkaian

2.2.4. Prinsip Kerja Alat



Gambar 5. Flowchart Prinsip Kerja Alat

2.4.5. Test Kerja Sistem

Dalam melakukan pengujian kerja sistem prototipe smarthome ini menggabungkan teknologi IoT dengan metode kriptografi untuk meningkatkan keamanan, menggunakan komponen seperti Arduino, NodeMCU 8266, sensor *Fingerprint*, dan sensor magnet pintu. NodeMCU berkomunikasi dengan Firebase Realtime Database untuk mengelola data, yang dienkripsi menggunakan kombinasi algoritma *Vigenere Cipher* dan *Caesar Cipher* sebelum dikirim dan didekripsi setelah diterima. Sensor *Fingerprint* digunakan untuk autentikasi pengguna, sementara sensor magnet mendeteksi status pintu. Data dari sensor diolah dan dienkripsi di web server menggunakan Python dengan Flask, kemudian dikirim ke Firebase. NodeMCU membaca data dari Firebase, mendekripsi, dan mengendalikan relay serta motor servo. Pengujian sistem mencakup verifikasi autentikasi fingerprint, enkripsi- dekripsi data, kontrol perangkat, dan koneksi Firebase, memastikan semua komponen bekerja dengan baik dan data tetap aman.

3. Hasil dan Pembahasan

3.1. Hasil Implementasi

Pada tahapan ini berisi hasil dari implemtasi prototipe *Smart Home* yang menggunakan *Fingerprint*, metode kriptografi *Vigenere Cipher* dan *Caesar Cipher*, serta kontrol melalui website.

3.1.1. Implementasi *Fingerprint*

Sensor *Fingerprint* terpasang pada pintu dan dihubungkan dengan Arduino. Saat pengguna menempelkan jari pada sensor, Arduino akan membaca data sidik jari dan memverifikasinya dengan database. Jika sidik jari terverifikasi, Arduino akan mengirim sinyal ke relay untuk membuka pintu.

Gambar 6. Menunjukkan Sensor Fingerprint

3.1.2. Implementasi Website Sistem Kontrol

Website kontrol dikembangkan untuk mengontrol pintu, lampu, dan alarm. Data dari kontrol button dienkripsi menggunakan *Vigenere Cipher* dan *Caesar Cipher* sebelum dikirim ke server.

Gambar 7. Menunjukkan Tampilan Website Kontrol.

3.1.3. Implementasi Kriptografi

Data yang dikirim dari website kontrol ke server dienkripsi menggunakan metode *Vigenere Cipher* dan *Caesar Cipher* untuk meningkatkan keamanan. Proses enkripsi dan dekripsi dilakukan secara efisien untuk memastikan bahwa data tetap aman selama transmisi. Berikut adalah proses bagaimana metode enkripsi ini bekerja untuk mengamankan informasi selama pengiriman.

1. Menentukan data awal, di mana status On bernilai 1 dan status Off bernilai 0. Adapun 3 komponen yang dikontrol yaitu :
   Lampu Rumah : '1' (On / Hidup)
   Pintu Utama : '1' (On / Terbuka)
   Alarm Rumah : '0' (Off / Tidak Berbunyi)
2. Melakukan proses enkripsi *Vigenere Cipher* yang menggunakan kunci *Vigenere Cipher* yang telah ditentukan yaitu (*vigenere_key* = "LTWJRRSGGD").

```
key_length = 10
vigenere_key = "LTWJRRSGGD"
# print(vigenere_key)
vigenere_encrypted_lamp = vigenere_encrypt(lamp_status_str, vigenere_key)
vigenere_encrypted_door = vigenere_encrypt(door_status_str, vigenere_key)
vigenere_encrypted_alarm = vigenere_encrypt(alarm_status_str, vigenere_key)
```

Gambar 8. Code Enkripsi Menggunakan *Vigenere Cipher*.

Teknik ini memetakan setiap karakter '1' dan '0' ke karakter lain. Dalam hal ini, '0' dipetakan menjadi 'A' dan '1' dipetakan menjadi 'B'.

```
# Map "0" to "A" and "1" to "B"
lamp_status_str = 'A' if lamp_status == '0' else 'B'
door_status_str = 'A' if door_status == '0' else 'B'
alarm_status_str = 'A' if alarm_status == '0' else 'B'
```

Gambar 9. Code Pemetaan Untuk *Vigenere Cipher*.

Contohnya:
- '1' pertama dipetakan menjadi 'B'.
- '1' kedua dipetakan menjadi 'B'.
- '0' dipetakan menjadi 'A'.

Hasilnya adalah 'BBA' setelah proses pemetaan.

3. Melakukan proses enkripsi *Caesar Cipher*. Dari hasil 'BBA' data ini kemudian dienkripsi kembali menggunakan teknik *Caesar* yaitu dengan pergeseran tertentu (*caesar_shift* = 14).

```
caesar_shift = 14
caesar_encrypted_lamp = caesar_encrypt(vigenere_encrypted_lamp, caesar_shift)
caesar_encrypted_door = caesar_encrypt(vigenere_encrypted_door, caesar_shift)
caesar_encrypted_alarm = caesar_encrypt(vigenere_encrypted_alarm, caesar_shift)

combined_data = f"{caesar_encrypted_lamp}|{caesar_encrypted_door}|{caesar_encrypted_alarm}"
print(f"Combined encrypted data: {combined_data}")
```

Gambar 10. Code Enkripsi Menggunakan *Caesar Cipher*.

Contohnya:
- Huruf Pertama 'B':
  B berada pada posisi ke-2 dalam alfabet (A=1, B=2, ...).
  Geser 14 langkah ke depan dari posisi B : (2 + 14 = 16).
  Huruf pada posisi ke-16 adalah 'P'.
- Huruf Kedua 'B' :
  Sama seperti huruf pertama, B juga digeser 14 langkah ke depan : (2 + 14 = 16). Ini juga menjadi 'P'.
- Huruf Ketiga 'A' :
  A berada pada posisi pertama dalam alfabet.
  Lalu geser 14 langkah ke depan dari posisi A : (1 + 14 = 15).Huruf pada posisi ke-15 adalah 'O'.

  Hasilnya adalah 'PPO' setelah di enkripsi dengan *Caesar Cipher.*

```
TERMINAL
lamp : B
door: A
alarm : A
Combined encrypted data: P|O|O
127.0.0.1 - - [19/Aug/2024 19:37:49] "GET /static/img/turned-on.png HTTP/1.1" 304 -
127.0.0.1 - - [19/Aug/2024 19:37:50] "POST /control HTTP/1.1" 200 -
lamp : 1
door : 1
alarm : 0
<class 'str'>
<class 'int'>
<class 'str'>
lamp : B
door: B
alarm : A
Combined encrypted data: P|P|O
127.0.0.1 - - [19/Aug/2024 19:38:37] "POST /control HTTP/1.1" 200 -
```

Gambar 11. Tampilan Dari Terminal Visual Studio Code

4. Penggabungan Hasil Enkripsi :
   Hasil dari enkripsi kedua (*Caesar Cipher*) adalah 'PPO', dimana
   - 'P' pertama mewakili status terenkripsi dari Lampu Rumah.
   - 'P' kedua mewakili status terenkripsi dari Pintu Utama.
   - 'O' mewakili status terenkripsi dari alarm Alarm Pintu.

Jadi Ini merupakan Kombinasi hasil enkripsi dari ketiga Status Tersebut. Setelah data dienkripsi menjadi 'PPO', data ini dikirimkan dan disimpan ke Firebase Realtime Database.

3.2. Pengujian dan Evaluasi Sistem

Bagian ini menjelaskan hasil dari berbagai pengujian yang dilakukan untuk mengevaluasi kinerja, keamanan, dan keandalan sistem *Smart Home* yang telah dikembangkan. Pengujian mencakup aspek fungsional, keamanan, kinerja, dan integrasi sistem.

3.2.1. Pengujian Fungsional

Pengujian fungsional dilakukan untuk memastikan bahwa setiap komponen dan fungsi dari sistem smart home bekerja sesuai dengan yang diharapkan.

Tabel 1. Pengujian Perangkat

Pengujian Ke	*Fingerprint*	Keadaan Lampu	Keadaan Pintu	Keadaan Alarm	Delay (Satuan Detik)			
					Fingerprint	Lampu	Pintu	Alarm
1.	Terdeteksi	Hidup	Buka	Hidup	1.0 detik	2.0 detik	2.0 detik	2.0 detik
2.	Terdeteksi	Hidup	Buka	Hidup	1.0 detik	2.0 detik	2.0 detik	2.0 detik
3.	Terdeteksi	Mati	Tutup	Mati	1.1 detik	2.1 detik	2.1 detik	2.1 detik
4.	Terdeteksi	Mati	Tutup	Mati	1.1 detik	2.1 detik	2.1 detik	2.1 detik

Pada Tabel 1. merupakan hasil pengujian yang dilakukan secara berulang untuk memastikan bahwa respon pada perangkat sidik jari, Hidup/Matikan Lampu, Buka/Tutup Pintu dan juga Hidup/Matikan Alarm sepenuhnya berhasil susai dengan skema pengujian yang telah di lakukan. Berikut ini merupakan penjelasan lebih detail mengenai hasil pengujian.

a. Sidik Jari

Pengujian dilakukan dengan mendaftarkan beberapa sidik jari dan mencoba melakukan otentikasi menggunakan sidik jari yang terdaftar dan tidak terdaftar. Dari pengujian yang telah dilakukan mendapatkan hasil Sidik jari yang terdaftar berhasil diotentikasi dengan tingkat keberhasilan 100%. Dan juga Sidik jari yang tidak terdaftar ditolak oleh sistem.

b. Kontrol Pintu

Pengujian dilakukan dengan membuka dan menutup pintu melalui sensor *Fingerprint* dan website kontrol. Mendapatkan hasil Pintu berhasil dibuka dan ditutup dengan menggunakan sensor *Fingerprint*. Dan juga Kontrol pintu melalui website berfungsi dengan baik.

c. Kontrol Lampu

Pengujian dilakukan dengan menyalakan dan mematikan lampu melalui switch on-off manual dan website kontrol. Pada pengujian ini mendapatkan hasil lampu berhasil dinyalakan dan dimatikan dengan switch on-off manual. Dan juga Kontrol lampu melalui website berfungsi dengan baik.

d. Kontrol Alarm

Pengujian dilakukan dengan mengaktifkan dan menonaktifkan alarm melalui website kontrol. Pada pengujian ini mendapatkan hasil alarm berhasil diaktifkan dan dinonaktifkan melalui website kontrol.

3.2.2. Pengujian Keamanan

Pengujian keamanan dilakukan untuk memastikan bahwa metode kriptografi yang digunakan efektif dalam melindungi data dari serangan.

1. Pengujian *Vigenere Cipher*

Pengujian dilakukan dengan mencoba mendekripsi data yang terenkripsi menggunakan *Vigenere Cipher* tanpa mengetahui kuncinya. Pada pengujian ini mendapatkan hasil data terenkripsi tidak dapat didekripsi tanpa kunci yang benar, menunjukkan bahwa metode *Vigenere Cipher* efektif dalam melindungi data.

2. Pengujian *Caesar Cipher*

Pengujian dilakukan dengan mencoba mendekripsi data yang terenkripsi menggunakan *Caesar Cipher* tanpa mengetahui nilai pergeserannya. Pada pengujian ini mendapatkan hasil data terenkripsi tidak dapat didekripsi tanpa nilai pergeseran yang benar, menunjukkan bahwa metode *Caesar Cipher* efektif dalam melindungi data.

3. Pengujian Sniffing Data

Pengujian dilakukan dengan mencoba menangkap data yang dikirim dari website kontrol ke server dan mendekripsinya. Pada pengujian ini mendapatkan hasil data yang tertangkap tidak dapat dibaca tanpa kunci yang benar, menunjukkan bahwa transmisi data aman.

3.2.3. Pengujian Kinerja

Pengujian dilakukan untuk mengevaluasi kinerja keseluruhan prototipe *Smart Home* dalam skenario nyata.

1. Respon Sistem Terhadap Input dari Sensor

Pengujian dilakukan dengan mensimulasikan berbagai input dari sensor *Fingerprint* dan magnet pintu. Pada pengujian ini mendapatkan hasil kinerja bahwa sistem merespon input dari sensor dengan cepat dan akurat.

2. Efektivitas Kontrol Melalui *Fingerprint*

Pengujian dilakukan dengan mengotentikasi beberapa pengguna menggunakan sensor *Fingerprint*. Pada pengujian ini mendapatkan hasil kinerja bahwa sensor *Fingerprint* efektif dalam mengamankan akses ke rumah pintar.

3. Keandalan Sistem dalam Skenario Nyata

Pengujian dilakukan dengan mengoperasikan sistem dalam kondisi sehari-hari. Pada pengujian ini mendapatkan hasil kinerja bahwa sistem menunjukkan keandalan yang baik dan tidak mengalami gangguan signifikan.

3.2.4. Pengujian Prototipe *Smart Home*

Pengujian dilakukan untuk mengevaluasi kinerja keseluruhan prototipe *Smart Home* dalam skenario nyata.

1. Respon Sistem Terhadap Input dari Sensor

Pengujian dilakukan dengan mensimulasikan berbagai input dari sensor *Fingerprint* dan magnet pintu. Pada pengujian ini mendapatkan hasil kinerja bahwa sistem merespon input dari sensor dengan cepat dan akurat.

2. Efektivitas Kontrol Melalui *Fingerprint*:

Pengujian dilakukan dengan mengotentikasi beberapa pengguna menggunakan sensor *Fingerprint*. Pada bagian pengujian ini mendapatkan hasil kinerja sensor *Fingerprint* efektif dalam mengamankan akses ke rumah pintar.

3. Keandalan Sistem dalam Skenario Nyata

Pengujian dilakukan dengan mengoperasikan sistem dalam kondisi sehari-hari. Pada bagian pengujian ini mendapatkan hasil kinerja Sistem menunjukkan keandalan yang baik dan tidak mengalami gangguan signifikan.

3.2.5. Pengujian Website Sistem Kontrol

Pengujian website sistem kontrol dilakukan untuk memastikan tombol pintu, lampu, dan alarm berfungsi dengan baik dan data terenkripsi dapat dikirim dan diterima dengan benar. Dan setalah dilakukan pengujian pada semua alat dapat berfungsi dengan baik sesuai perintah dari website yang dibuat.

3.3. Hasil dan Analisis

Pada tahap ini membahas hasil dari pengujian dan evaluasi sistem yang telah dilakukan, mengevaluasi efektivitas, keandalan, dan kinerja dari prototipe *Smart Home* yang dikembangkan. Analisis ini akan memberikan gambaran mendalam mengenai seberapa baik sistem tersebut memenuhi tujuan dan kebutuhan yang telah ditetapkan.

3.3.1. Analisis Fungsional

Hasil pengujian fungsional menunjukkan bahwa setiap komponen dan fungsi utama dari sistem *Smart Home* bekerja sesuai dengan yang diharapkan.

1. Verifikasi Sidik Jari:

Sistem *Fingerprint* menunjukkan tingkat keberhasilan 100% dalam memverifikasi sidik jari yang terdaftar dan menolak sidik jari yang tidak terdaftar. Ini menunjukkan bahwa sensor fingerprint dan algoritma otentikasi bekerja dengan baik dan dapat diandalkan.

2. Kontrol Pintu, Lampu, dan Alarm:

Semua kontrol perangkat (pintu, lampu, dan alarm) melalui sensor *Fingerprint* dan website kontrol berfungsi dengan baik. Hal ini menunjukkan bahwa integrasi antara hardware (Arduino, relay, motor servo) dan *software* (website kontrol) berhasil dilakukan dengan baik.

3.3.2. Analisis Keamanan

Pengujian keamanan menunjukkan bahwa metode kriptografi yang digunakan (*Vigenere Cipher* dan *Caesar Cipher*) efektif dalam melindungi data.

1. *Vigenere Cipher* dan *Caesar Cipher*

Kedua metode kriptografi ini berhasil mengenkripsi dan melindungi data dengan baik. Pengujian menunjukkan bahwa tanpa kunci atau nilai pergeseran yang benar, data tidak dapat didekripsi, sehingga informasi tetap aman selama transmisi.

2. Pengujian Intersepsi Data

Hasil pengujian menunjukkan bahwa data yang dikirim dari website kontrol ke server tidak dapat dibaca tanpa kunci yang benar. Ini menunjukkan bahwa transmisi data antara sistem *Smart Home* dan server aman dan terlindungi dari serangan.

3.3.3. Analisis Kinerja

Pengujian kinerja menunjukkan bahwa sistem memiliki waktu respon yang cepat dan efisiensi penggunaan sumber daya yang baik.

1. Waktu Respon *Fingerprint*:

Waktu respon rata-rata 1 detik untuk verifikasi sidik jari menunjukkan bahwa sistem dapat memberikan respon yang cepat dan efisien, yang penting untuk kenyamanan pengguna.

2. Waktu Enkripsi dan Dekripsi:

Waktu enkripsi rata-rata 0.5 detik untuk *Vigenere Cipher* dan 0.3 detik untuk *Caesar Cipher* menunjukkan bahwa proses enkripsi dan dekripsi dilakukan dengan cepat tanpa menambahkan delay yang signifikan pada sistem.

3.3.4. Analisis Kinerja Prototipe *Smart Home*

Hasil pengujian prototipe menunjukkan bahwa sistem dapat merespon input dari sensor dengan cepat dan akurat.

1. Respon Sistem Terhadap Input dari Sensor

Prototipe dapat mendeteksi dan merespon input dari sensor *Fingerprint* dan magnet pintu dengan cepat dan tepat waktu. Hal ini menunjukkan bahwa sistem ini andal dalam mendeteksi perubahan status dan memberikan respon yang sesuai.

2. Efektivitas Kontrol Melalui *Fingerprint*

Kontrol akses melalui *Fingerprint* efektif dalam mengamankan akses ke rumah pintar. Pengguna yang tidak terdaftar tidak dapat mengakses rumah, meningkatkan keamanan secara signifikan.

3.3.5. Analisis Kinerja Website Sistem Kontrol

Hasil pengujian website kontrol menunjukkan bahwa tombol pintu, lampu, dan alarm berfungsi dengan baik, dan data terenkripsi dapat dikirim dan diterima dengan benar.

1. Respon Waktu Pengiriman Data:

Waktu respon rata-rata 0.2 detik untuk pengiriman data dari website kontrol ke server menunjukkan bahwa sistem ini memiliki latensi rendah, yang penting untuk kontrol real-time.

2. Keandalan Pengiriman Data:

Data selalu terkirim dengan andal dan terenkripsi dengan benar, menunjukkan bahwa sistem ini handal dan dapat diandalkan untuk penggunaan sehari-hari.

4. Kesimpulan

Dalam penelitian ini, implementasi *Fingerprint* pada rancangan prototipe *Smart Home* yang menggunakan metode keamanan kriptografi *Vigenere Cipher* dan *Caesar Cipher* telah berhasil dilakukan. Berdasarkan hasil pengujian dan evaluasi, dapat disimpulkan: Prototipe *Smart Home* yang dikembangkan menggunakan sensor *Fingerprint* untuk mengontrol akses ke perangkat seperti pintu, lampu, dan alarm. Sistem *Fingerprint* berhasil memverifikasi dan menolak sidik jari yang tidak terdaftar dengan tingkat keberhasilan 100%, menunjukkan keandalan sensor dan algoritma otentikasi. Metode kriptografi *Vigenere Cipher* dan *Caesar Cipher* efektif dalam mengenkripsi dan melindungi data selama transmisi, memastikan data aman dan tidak dapat dibaca tanpa kunci yang benar. Prototipe menunjukkan integrasi yang baik antara hardware dan software. Kontrol perangkat melalui sensor *Fingerprint* dan website kontrol berfungsi dengan baik, dengan waktu respon yang cepat. Rata-rata waktu respon untuk verifikasi sidik jari adalah 1 detik, dan waktu enkripsi masing-masing 0.5 detik (*Vigenere Cipher*) dan 0.3 detik (*Caesar Cipher*). Tombol kontrol pada website memiliki respon, dengan waktu respon rata-rata 0.2 detik untuk pengiriman data, membuktikan keandalan dan efisiensi sistem secara keseluruhan.

Referensi

[1]. BPS. (2023). Statistik Kriminal. *Badan Pusat Statistik*, *021*, 5–6.

[2]. A. M. Ibrahim dan A. Solikhin, “Sistem Kontrol dan Monitoring Berbasis IoT pada Lampu dan AC di Laboratorium Komputer Politeknik Mitra Karya Mandiri,” Jurnal Sistem Informasi, Teknologi Informasi dan komputer, vol. 13, no. 2, 2023.

[3]. I. Luthfianalela, “Sistem Kendali Otomatis Rumah Pintar Berbasis Android,” Skripsi, Politeknik Harapan Bersama, Kota Tegal, 2021.

[4]. A. Marzuky Ashshaff, “Implementasi Teknologi Internet of Things (IoT) Berbasis Android Sebagai Pengendali Smart Room,” Skripsi, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Lampung, Lampung, 2021.

[5]. M. Iqbal, B. Hermanto, A. M. Ashshaff, dan R. H. Dewantara, “Smart Room System Menggunakan Teknologi Internet of Things (IoT) dengan Sistem Kendali Berbasis Android,” Jurnal CoreIT, vol. 7, no. 1, 2021.

[6]. W. Najib, S. Sulistyo, dan Widyawan, “Tinjauan Ancaman dan Solusi Keamanan pada Teknologi Internet of Things,” Jurnal Nasional Teknik Elektro dan Teknologi Informasi, vol. 9, no. 4, 2020.

[7]. R. K. Endrayanto, A. Muttaqin, dan R.A Setyawan, “ Advanced Encryption Standard (AES) pada Modul Internet of Things (IoT), Jurnal TELKA, vol. 5, no 2, 2019.

[8]. A. Rachmayanti dan Wirawan, “Implementasi Algoritma Advanced Encryption Standard (AES) pada Jaringan Internet of Things (IoT) untuk Mendukung Smart Healthcare,” Jurnal Teknik ITS, vol. 11, no. 3, 2022.

[9]. E. W. Setyawan, A. Ashari, dan R. M. Hhujja, "Implementasi enkripsi AES-CCM dalam kunci rumah pintar dengan perangkat IoT berbasis Wi-Fi." Skripsi, Universitas Gadjah Mada, Yogyakarta, 2024.

[10]. D. Usman, E. Wulandari, dan F. S. Hadisantoso, "Implementasi Fingerprint dan IoT Untuk Pengaman Ruangan," Jurnal RAMATEKNO, vol.02 no.1. Hal 60-72, 2022.

[11]. M. Sutrisno, "Prototipe Sistem Keamanan Dan Otomatisasi Rumah Pintar Berbasis Internet of Things," Skripsi, Universitas Islam Sultan Agung, Semarang, 2021.

[12]. R. T. Shita, dan L. L. Hin, "Implementasi Sensor Fingerprint Smartphone Android dan Mikrokontroler NODEMCU dalam Mengamankan Kendaraan," Jurnal TICOM, vol.8 no.3, 2020.

[13]. V. M. Hidayah, D. I. Mulyana, dan Y. Bachtiar, "Algoritma Caesar Cipher atau Vigenere Cipher pada Pengenkripsian Pesan Teks," Journal On Education, vol. 5 no. 3, 2023.

[14]. T. T. P. Deby, "Penerapan Algoritma Vigenere Cipher untuk Meningkatkan Keamanan Pada Dashboard," Skripsi, Fakultas Teknik, Universitas Muhammadiyah Makasar, 2023.

[15]. Y. D. Putri, Rosihan, S. Lutfi, "Penerapan Kriptografi Caesar Cipher Pada Fitur Chatting Sistem Informasi Freelance," Jurnal Informatika dan Komputer, vol. 2, no.2, 2019.