IMPLEMENTASI SISTEM AUTENTIKASI SIDIK JARI DAN NFC UNTUK MEMBUKA AKSES *SSD NVME* ENKRIPSI DENGAN ARDUINO

Naskah Publikasi Jurnal

Diajukan oleh:

RUDI ARDIANTO
1513620040

PROGRAM STUDI PENDIDIKAN TEKNIK ELEKTRONIKA
FAKULTAS TEKNIK
UNIVERSITAS NEGERI JAKARTA
2025

NASKAH PUBLIKASI JURNAL

IMPLEMENTASI SISTEM AUTENTIKASI SIDIK JARI DAN NFC UNTUK MEMBUKA AKSES *SSD NVME* ENKRIPSI DENGAN ARDUINO

yang diajukan oleh :

RUDI ARDIANTO

1513620040

Telah disetujui oleh :

Pembimbing 1

Dr. Aodah Diamah, S.T, M.Eng
NIP. 197809192005012003

Tanggal 24 Juli 2025

Pembimbing 2

Dr. Arum Setyowati, M.T
NIP. 197309151999032002

Tanggal 29 Juli 2025

IMPLEMENTASI SISTEM AUTENTIKASI SIDIK JARI DAN NFC UNTUK MEMBUKA AKSES *SSD NVME* ENKRIPSI DENGAN ARDUINO

Rudi Ardianto[1], Dr. Aodah Diamah, S.T, M.Eng[2], Dr. Arum Setyowati, M.T[3]

[1] Mahasiswa Prodi PendidikanTeknik Elektronika, FT – UNJ
[2,3] Dosen Prodi Pendidikan Teknik Elektronika, FT – UNJ
[1]rudiardianto84@gmail.com, [2] adiamah@unj.ac.id, [3] asetyowati@unj.ac.id

Abstrak

Penelitian ini didasari oleh maraknya fenomena serangan *hacker* pada lembaga-lembaga negara di Indonesia yang menimbulkan kekhawatiran publik terkait keamanan data pribadi mereka. Salah satu upaya untuk meningkatkan keamanan data adalah dengan mengaktifkan sistem enkripsi. Penelitian ini bertujuan untuk menggantikan opsi masukkan password pada saat membuka enkripsi dengan autentikasi sidik jari dan NFC, baik melalui NFC *smartphone* maupun NFC kartu. Penelitian ini menggunakan metode penelitian borg and gall yang diambil terdiri 5 langkah yaitu: Penelitian dan Pengumpulan Informasi, Perencanaan, Pengembangan Produk Awal, Uji Coba Awal, dan Penyempurnaan Produk Akhir. Penelitian ini menggunakan mikrokontroler Arduino Atmega 256, sensor sidik jari AS608, modul NFC PN532. Adapun, hasil penelitian menunjukkan bahwa alat ini berfungsi dengan baik, pada pengujian untuk membuka enkripsi data 2,95 detik hingga 7,82 detik, pendaftaran sidik jari membutuhkan waktu 7,14 detik, pendaftaran nfc memerlukan 2,29 detik. Rata rata verifikasi antara sidik jari dan nfc yaitu 0,74 detik hingga 0,84 detik, respon penolakan yang tidak terdaftar sidik jari dan nfc yaitu 0,76 detik hingga 0,85 detik, dan dalam pengujian perangkat laptop dengan prosesor berbeda dapat berjalan dengan baik. Dalam hasil pengujian tersebut dapat disimpulkan bahwa alat ini efektif, efisien dan mampu menggantikan dari input manual password saat membuka enkripsi, dengan verifikasi sidik jari dan NFC.

Kata Kunci : *enkripsi data, sidik jari, nfc pn532, ssd nvme*

Abstract

This research is based on the phenomenon of the rise of hacker attacks on state institutions in Indonesia which raises public concerns about the security of their personal data. One effort to improve data security is to activate an encryption system. This research aims to replace the option of entering a password when opening encryption with fingerprint and NFC authentication, both via smartphone NFC and card NFC. This research uses the Borg and Gall research method which consists of 5 steps, namely: Research and Information Collection, Planning, Initial Product Development, Initial Trial, and Final Product Refinement. This research uses an Arduino Atmega 256 microcontroller, AS608 fingerprint sensor, PN532 NFC module. Meanwhile, the results of the study show that this tool functions well, in the test to open data encryption 2.95 seconds to 7.82 seconds, fingerprint registration takes 7.14 seconds, NFC registration takes 2.29 seconds. The average verification time between fingerprint and NFC was 0.74 seconds to 0.84 seconds, while the rejection time for unregistered fingerprint and NFC was 0.76 seconds to 0.85 seconds. Tests on laptops with different processors demonstrated good tool performance. The test results show that this tool is effective, efficient, and capable of replacing manual password input when unlocking encryption, with fingerprint and NFC verification.

Keywords *: data encryption, fingerprint, nfc pn532, nvme ssd*

1. Pendahuluan

Perkembangan teknologi digital mendorong peningkatan penggunaan perangkat penyimpanan data. seperti ssd sata 2,5 inc, ssd sata 2280, dan SSD NVME (Solid State Drive *Non-Volatile Memory Express*), namun yang popular digunakan ssd NVME yang menawarkan speed read/ write tinggi di bandingkan SSD sata 2,5 inch, dan SSD sata 2280. Namun seiring perkembangan ini terdapat ancaman terhadap keamanan juga meningkat pada perangkat penyimpanan data. Data yang bersifat rahasia dan sensitif, seperti data pribadi, data bisnis atau data negara, sangat rentan terhadap serangan hacker, seperti pencurian data, merusak data atau akses tidak sah. Pada kasus pembobolan data yang terjadi di Indonesia belakangan tahun berturut turut yaitu dimulai dari kebocoran data indihome, data registrasi kartu sim prabayar, data kpu, dokumen presiden RI. Pada kasus paling terparah yaitu pencurian data server PDN yang mengakibatkan beberapa sistem negara lumpuh, ini diakibatkan karena penggunaan sistem yang lemah yang menjadi penyebab kebobolan ini, pada jurnal (Tanzil Wahyu Ramadhan et al., 2024).

Oleh karena itu pentingnya melindungi data pribadi atau sensitif dengan membuat sistem proteksi/ menginstal software proteksi yang beredar dan mengaktifkan enkripsi SSD NVME, yaitu mengunci data dengan *Password* agar tidak dapat di akses tanpa izin. Penggunaan *password* enkripsi pada ssd diperlukan kata sandi yang rumit, terdiri dari 20-32 digit kata di kombin angka, huruf, symbol, misalnya “6ehj#9kL7&R&dY3!xWm7#bL2P” dan menghindari

penggunaan kata sandi berupa kalimat atau tanggal lahir karena dapat tembus di bobol brute force. Namun masalah muncul Ketika kata sandi atau kunci enkripsi digunakan. Sebagian besar pengguna termasuk peneliti susah mengingat kata sandi rumit dan kurang efektif. Untuk mengatasi masalah ini, memerlukan autentikasi biometric seperti sidik jari sebagai pengganti password untuk membuka kunci enkripsi pada ssd.

Bedasarkan latar belakang tersebut, penulis menulis dengan judul "Implementasi Sistem Autentikasi Sidik Jari dan NFC Untuk Membuka Akses SSD NVME (*Solid State Drive Non-Volatile Memory Express*) Enkripsi Dengan Arduino", menggunakan metode penelitian R&D berbasis *Borg and Gall*. Dan penelitian ini menggunakan mikrokontroler Arduino mega atmega 2560 sebagai pengontrol untuk membuka kunci enkripsi SSD NVME, dengan integrasi sensor sidik jari, NFC dan *Hardware*, sistem ini akan memberikan akses hanya yang terdaftar, serta mengirimkan password enkripsi ke komputer menggunakan windows 10/11. Serta system yang akan dibuat akan di buat responsif mungkin pada proses verifikasi sidik jari maupun NFC. Terdapat fitur tambahan yaitu pengolaan daya otomatis yang dapat mematikan Arduino setelah verifikasi juga di implementasikan menggunakan relay, sehingga dapat menghemat daya dan memalisir hacker masuk ke sistem arduino.

2. Dasar teori

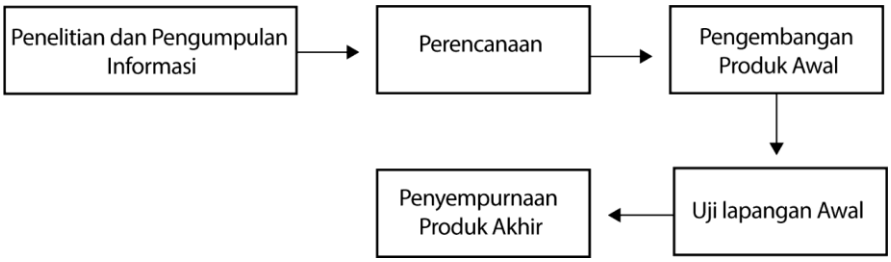
Penelitian ini menggunakan konsep pengembangan produk, di sebut juga dengan *Research and development* adalah proses yang terstruktur dan sistematis untuk menciptakan atau memperbaiki produk agar sesuai dengan permasalahan pengguna. Mahfud dan Fahrizki (2020), menjelaskan R&D adalah studi sistematis yang bertujuan untuk menghasilkan produk baru atau menyempurnakan produk yang telah ada beredar, dengan dasar analisis kebutuhan dan uji coba produk di lapangan. Lalu Jaedun (2010) di kutip dari (Waruwu, 2024), mendefinisikan penelitian dan pengembangan adalah suatu kegiatan yang bertujuan untuk mengembangkan, menguji kemanfaatan dan efektivitas produk yang dikembangkan, baik segi dari produk teknologi, material, organisasi, metode, dan alat-alat.

Konteks dalam penelitian ini, produk yang di kembangkan merupakan berhubungan keamanan meningkatkan opsi dalam autentikasi data, yang menambahkan autentikasi berbasis biometrik sidik jari dan NFC. Autentikasi merupakan tembok terdepan yang dapat memastikan hanya pengguna pemilik mengakses data terenkripsi. Ningsih, Elisa Setia (Ed) menjelaskan dikutip dari (Suling et al., 2017) autentikasi adalah sebuah langkah untuk dapat menentukan atau memastikan bahwa seseorang *user* (pengguna) yaitu autentik atau asli pemilik enkripsi data agar terhindar di akses oleh pihak tidak berwewenang. Melakukan autentikasi terhadap sebuah objek adalah melakukan konfirmasi terhadap suatu kepemilikan. Salah satu yang menurut penulis jenis autentikasi yang efektif yaitu menggunakan sidik jari dan nfc. Menurut Siswanto et al., (2018) dalam sistem biometric, terdapat 2 tahap terminologi, yaitu tahap verifikasi dan identifikasi. Tahap verifikasi yaitu mencocokkan pengguna biometric sidik jari untuk dapat memastikan satu identitas, sedangkan tahap identifikasi adalah membandingkan dengan pengguna biometric sidik jari untuk semua orang lain dalam database untuk dapat memastikan mereka tidak terdaftar sebelumnya. Menurut (Djamar, Sompie, & Putro,2017), NFC menggunakan prinsip kerja dengan memanfaatkan komunikasi dengan induksi medan magnet, dengan meletakkan 2 perangkat dalam area yang berdekatan, yang akan membentuk sebuah transformator dengan inti udara. NFC merupakan teknologi yang berkomunikasi data secara dua arah, yang dapat diartikan pada saat perangkat terhubung akan terjadi menulis dan membaca. Kecepatan transfer data dalam menggunakan NFC beragam, yaitu 106 Kbps, 212 Kbps dan 424 Kbps, dikutip dari jurnal (Nurhadi et al., 2022).

Setelah pengguna berhasil diverifikasi akan membuka perlindungan terhadap isi data dengan menggunakan penerapan enkripsi, pada data yang disimpan pada SSD NVME. Menurut Suhardi (2016), Enkripsi data adalah terapan dalam kriptografi yaitu proses mengubah plaintext menjadi ciphertext menggunakan algoritma tertentu. bertujuan untuk upaya pengamanan data dan mencegah akses terhadap data yang bersifat rahasia dan penting oleh pihak-pihak yang tidak mempunyai sandi untuk data tersebut. Dan (Farizy & Supriyatna, 2023) menjelaskan SSD NVMe adalah media penyimpanan atau Storage yang menggunakan chip NAND atau IC flash menjadi media penyimpanannya. Dalam mekanisme mencari data, SSD jauh lebih cepat ketimbang harddisk karena tidak memerlukan piringan atau komponen yang bergerak, sehingga waktu yang di butuhkan seek time atau pencarian data lebih cepat. hal ini disebabkan karena waktu seek time atau pencarian data yang lebih cepat diakses karena SSD menggunakan chip NAND atau flash, sehingga tidak menggunakan komponen yang bergerak pada SSD.

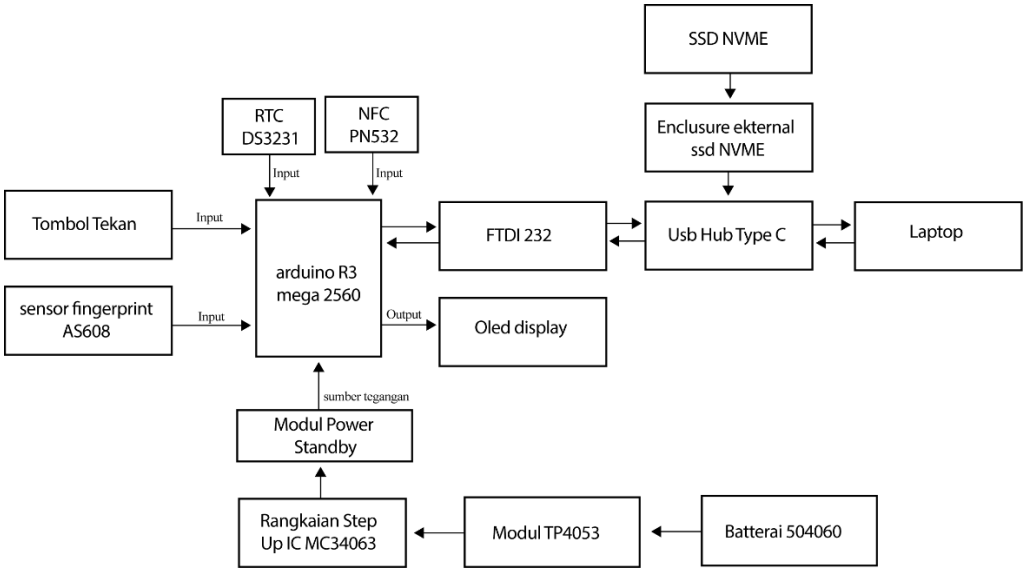
3. Metodologi

Metode penelitian yang digunakan dalam pengembangan produk ini adalah Research and Development (R&D) model borg and gall. Penelitian R&D model borg and gall (dalam sugiyono:2009:11) Dinyatakan bahwa metode penelitian dasar sering digunakan dalam studi untuk dapat menghasilkan produk hipotetik. Melalui eksperimen dan penelitian tindakan digunakan untuk menguji produk hipotetik. Setelah menguji produk, produk tersebut bisa dapat aplikasikan. Proses pengujian produk melalui eksperimen disebut penelitian terapan. Tujuan riset dan pengembangan adalah untuk menemukan, mengembangkan, dan memvalidasi produk(dikutip jurnal Sri Haryati, 2012). Pada penelitian nanti, peneliti tidak menggunakan 10 tahapan borg and gall dalam mengembangkan produknya. Peneliti akan menggunakan 5 langkah yaitu : Penelitian dan Pengumpulan Informasi, Perencanaan, Pengembangan Produk Awal, Uji Coba Awal, Penyempurnaan Produk Akhir, terlampir pada gambar 3.1.



Gambar 3. 1 Tahap Tahap pengembangan Penelitian

pada penelitian menggunakan arduino R3 mega 2560 sebagai otak dari sistem yang menanggani tiga input yaitu push button dan sensor fingerprint AS608, NFC PN532. RTC DS3231 berfungsi menyimpan waktu secara realtime. mikrokontroler ini mendapatkan sumber tegangan atau VCC dari baterai, dan di naikkan tegangan ke 5v menggunakan rangkaian step up dan modul tp 4053 digunakan untuk mengecas baterai. Modul power standby berfungsi sebagai stanby atau mematikan sementara semua modul lainnya seperti PN532, AS608, RTC, Oled pada saat sudah verifikasi maupun menghidupkannya. Output dari mikrokontroler ini yang pertama oled display sebagai menampilkan tulisan berupa status sistem, dan output kedua terhubung dengan FTDI 232 melalui komunikasi TXRX dari arduino. Pada SSD NVME akan di sambungkan enclosure/ case SSD NVME untuk menconvert dari PCIe Express menjadi usb type C. usb hub type c yang akan menghubungkan dari FTDI dan case Nvme sebelum terhubung dengan komputer melalui usb type C pada komputer. Lalu komputer akan membuka enkripsi data yang ada di SSD NVME. Terlampir pada gambar 3.2

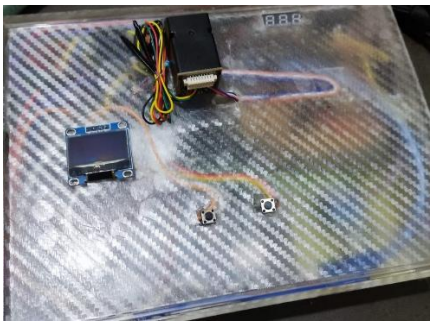


Gambar 3. 2 Gambar Blok Diagram sistem

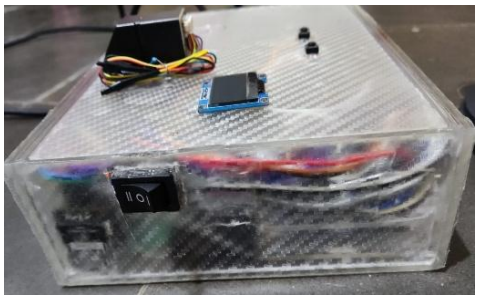
4. Hasil dan Analisis

4.1. Hasil Final produk

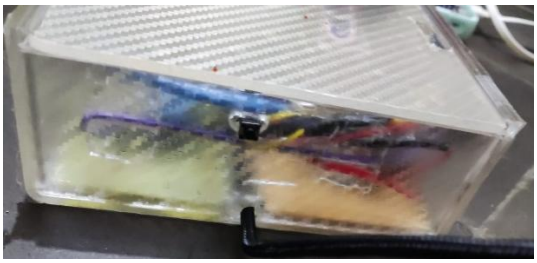
Berikut adalah design produk dalam bentuk nyata seperti gambar 4.1 hingga 4.3.



Gambar 4. 1 Nampak atas Produk



Gambar 4. 2 nampak Kiri Produk



Gambar 4. 3 Nampak kanan Produk

4.2 Hasil Pengujian pendaftaran sidik jari

Tabel 4. 1 Tabel Pengujian Pendaftaran Sidik Jari

percobaan	Jari yang digunakan	Status sistem	Waktu diperlukan	Gambar
1	Ibu Jari Kanan	Pendaftaran sukses!	6,26 Detik	
2	Jari Telunjuk Kanan	Pendaftaran sukses!	6,46 Detik	
3	Jari Tengah Kanan	Pendaftaran sukses!	6,81 Detik	
4	Jari Manis Kanan	Pendaftaran sukses!	6,11 Detik	

4.3 Hasil Pengujian Respon Sidik Jari Terdaftar

Tabel 4. 2 Pengujian Respon Sidik Jari Terdaftar

Percobaan	Status Sistem	Waktu Respon	Gambar Pengujian waktu
1	Verifikasi berhasil	0,72 detik	
2	Verifikasi berhasil	0,83 detik	
3	Verifikasi berhasil	0,68 detik	
4	Verifikasi berhasil	0,73 detik	

4.4 Hasil Pengujian Respon Sidik Jari Tidak Terdaftar

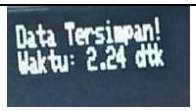
Tabel 4. 3 Pengujian respon sidik jari tidak terdaftar

Percobaan	Status Sistem	Waktu Respon	Gambar pengujian
1	Sidik jari Tidak Dikenal	0,86 Detik	
2	Sidik jari Tidak Dikenal	0,73 Detik	

3	Sidik jari Tidak Dikenal	0,73 Detik	
4	Sidik jari Tidak Dikenal	0,77 Detik	

4.5 Hasil Pengujian Pendaftaran NFC Handphone/ Kartu

Tabel 4. 4 Pengujian Pendaftaran handphone/Kartu

percobaan	Status sistem	Waktu yang diperlukan	Gambar
1	Data Tersimpan!	2,24 Detik	
2	Data Tersimpan!	2,24 Detik	
3	Data Tersimpan!	2,24 Detik	
4	Data Tersimpan!	2,24 Detik	

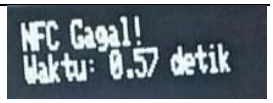
4.6 Hasil Pengujian Respon Terdaftar NFC Handphone/ Kartu

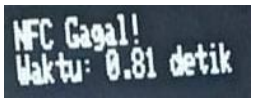
Tabel 4. 5 Pengujian Waktu Verifikasi Kartu

percobaan	Status sistem	Waktu yang diperlukan	Gambar Pengujian Waktu
1	NFC Berhasil	0,86 Detik	
2	NFC Berhasil	1,07 Detik	
3	NFC Berhasil	0,88 Detik	
4	NFC Berhasil	0,46 Detik	

4.7 Hasil Pengujian Respon Tidak Terdaftar NFC Handphone/ Kartu

Tabel 4. 6 Pengujian Waktu Respon Tidak Terdaftar Kartu

percobaan	Status sistem	Waktu yang diperlukan	Gambar
1	NFC Gagal	0,57 Detik	

2	NFC Gagal	0,79 Detik	
3	NFC Gagal	0,87 Detik	
4	NFC Gagal	0,81 Detik	

4.8 Hasil Pengujian Waktu Membuka SSD NVME Enkripsi Dan Ganti Password Berbagai Perangkat

Tabel 4. 7 Hasil Pengujian Berbagai Perangkat

Percobaan	Laptop Digunakan	Waktu Digunakan Mode Ganti Password	Jumlah data dienkripsi	Jumlah Error Data Password	Waktu Digunakan Mode Verifikasi
1	HP 14S – CF03076TU (Intel Core i3 1005G1) 2 Core	6 Menit 40 Detik	30	0	2,97 Detik
2	HP 14S – CF03076TU (Intel Core i3 1005G1) 2 Core	7 Menit 6 Detik	30	0	2,78 Detik
3	HP 14S – CF03076TU (Intel Core i3 1005G1) 2 Core	6 Menit 48 Detik	30	0	3,12 Detik
4	Legion 5 15ARH05 (AMD Ryzen 5 4600H) 6 Core	6 menit 40 detik	30	2	7,41 Detik
5	Legion 5 15ARH05 (AMD Ryzen 5 4600H) 6 Core	7 menit 24 detik	30	2	8,05 Detik
6	Legion 5 15ARH05 (AMD Ryzen 5 4600H) 6 Core	6 menit 26 detik	30	2	7,88 Detik
7	HP 14S- CS3010TU (Intel Core i5 1005G1) 4 Core	7 Menit 4 Detik	30	0	3,07 Detik
8	HP 14S- CS3010TU (Intel Core i5 1005G1) 4 Core	6 Menit 57 Detik	30	0	3,13 Detik
9	HP 14S- CS3010TU (Intel Core i5 1005G1) 4 Core	6 Menit 51 Detik	30	0	3,19 Detik

4.9 Analisis

Dari didapatkan hasil dari pengujian tabel 4.1 terlihat responsive dengan rata rata pendaftaran 5,44 Detik dengan kondisi 2 kali pendaftaran, yang pertama menempelkan jari yang akan didaftarkan, kedua menempelkan jari yang sama baru sistem berhasil didaftarkan. Pada tabel 4.2 terlihat waktu respon sidik jari terdaftar , pada pengujian ini hanya menguji seberapa cepat nya respon sidik jari untuk membaca Ketika sidik jari terdaftar, pada pengujian ini dengan rata rata respon sidik jari 0,99 detik. Lalu pada tabel 4.3 pengujian respon sidik jari tidak terdaftar, pada pengujian dilakukan dengan jari tidak terdaftar untuk menguji respon tersebut dan dalam uji coba peneliti mendapatkan rerata respon 0,68 detik. Selanjutnya pengujian sesi kedua yaitu pengujian NFC menggunakan Kartu elektronik dan NFC handphone pada tabel 4.4 hingga 4.6. terlihat pada tabel 4.4 pengujian pendaftaran NFC kartu Dan NFC handphone, proses nya masih sama yang pada sebelumya yaitu menguji seberapa cepat mendaftarkan data ke eeprom eksternal, pada pengujian ini rerata menyimpan data yaitu 2,24 detik. Selanjutnya pada tabel 4.5 merupakan pengujian verifikasi NFC pada kartu dan NFC handphone yang terdaftar, pada pengujian ini hasil yang didapatkan rata rata yaitu 0,84 Detik. Lalu yang terakhir pada tabel 4.6 merupakan pengujian respon menolak kartu dan Handphone yang tidak terdaftar, hasil yang didapatkan pengujian tersebut dengan rata rata 0,69 Detik.

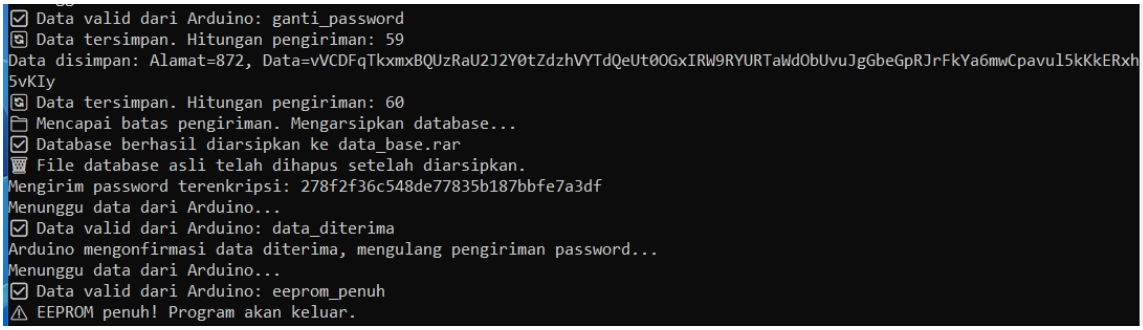
Langkah selanjutnya pengujian software, yang akan diuji terbagi dua bagian verifikasi dan Ganti password pada pengujian ini peneliti menggunakan laptop Legion 5 15ARH05 menggunakan CPU AMD Ryzen 5 4600H. Pada tabel 4.7 terlihat pengujian rerata waktu di butuhkan untuk membuka enkripsi ssd NVME yaitu 7,82 Detik. Berikut adalah gambar 4.4 merupakan isi data arduino untuk proses membuka enkripsi data ssd NVME.

Gambar 4. 4 Tampilan Data Dikirim Dari arduino

Pada gambar 4.4 dapat dijelaskan bagian bagian yang di tampilan CMD sebagai berikut:

1. Mode_Verifikasi : yaitu sebagai perintah dari arduino ke komputer untuk segera merubah mode di komputer.
2. 3 digit angka : yaitu sebagai perintah dari arduino ke komputer untuk mengload data base di komputer dengan Alamat tersebut.
3. 32 digit karakter : merupakan data enkripsi AES ECB dari arduino yang harus dipecahkan atau di dideksripsi oleh komputer.
4. Data terenkripsi lengkap: merupakan hasil dekripsi pada 15 digit depan dan sisanya merupakan data dari data base komputer yang akan digabung dan deksripsikan.
5. Password ditemukan : merupakan hasil pencarian password di dalam data gabungan di data terenkripsi, yang akan digunakan deksripsi data AES GCM pada bagian “data terenkripsi lengkap”.
6. Password terdeksripsikan : merupakan password asli dideksripsikan dari “data terenkripsi lengkap” yang akan digunakan untuk membuka kunci enkripsi SSD NVME melalui veracrypt.

Pada tabel 4.7 hasil yang di dapatkan dari pengujian waktu di butuhkan dalam Ganti password dengan hasil rata rata 7 menit 2 detik. Berikut merupakan tampilan pada mode Ganti password di CMD terlihat pada gambar 4.5 sebagai berikut.

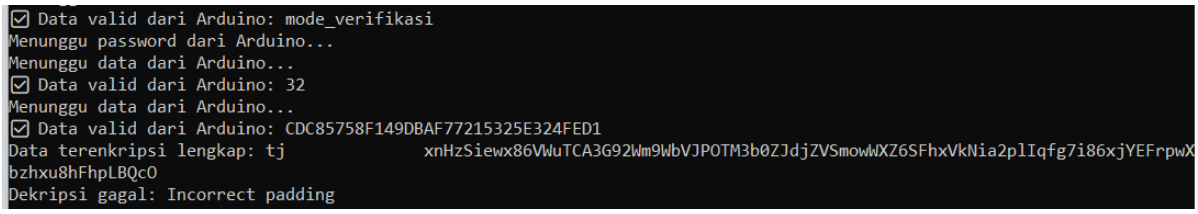


Gambar 4. 5 Tampilan Mode Ganti Password CMD

Pada gambar 4.5 dapat dijelaskan bagian bagian yang di tampilan CMD sebagai berikut:

1. “Data Tersimpan” terdiri dari Alamat dan data, merupakan data password asli terenkripsi beserta alamat yang akan disimpan di data base komputer.
2. Mengirim password terenskripsi, merupakan data 15 digit dari enkripsi keseluruhan yang akan di simpan ke data base, yang akan dikirim ke eeprom arduino menggunakan keamanan pengiriman AES ECB.
3. Hitungan Pengiriman, merupakan counter pada sistem di komputer yang tujuan untuk menghitung data yang keluar dan data ke data base, jika sudah mencapai hitungan 60 sistem akan secara otomatis mengunci data base agar terhindar dari serangan hecker.

Pada gambar 4.6 merupakan data error yang disebabkan CPU terdapat kesalahan karena dibawah spesifikasi sehingga proses enkripsi tidak berjalan dengan baik, sebagai berikut.



Gambar 4. 6 Tampilan ERROR Dalam Deksripsi Password

Dari gambar 4.6 terlihat jika data yang di enkripsi pada mode Ganti password ada terjadi kesalahan, pada saat ingin membuka enkripsi ssd terjadi data *corrupted* (error) seperti pada gambar 4.7. pada tabel 4.14 terlihat bahwa pengujian di berbagai laptop, pengujian di laptop intel core i3 1005G1 dengan 2 core tidak terdapat error pada pada mode Ganti password dan proses membuka enkripsi jauh lebih cepat di banding laptop peneliti gunakan yakni AMD Ryzen 5 4600 H dengan 6 core, jadi menurut peneliti program atau sistem di buat berjalan dengan normal di berbeda perangkat laptop.

5. Kesimpulan Dan Saran

Bedasarkan hasil penelitian akhir yang dilakukan dengan judul penelitian “Implementasi Sistem Autentikasi Sidik Jari dan NFC Untuk Membuka Akses SSD NVME Enkripsi Dengan Arduino” menghasilkan suatu produk sistem yang memiliki autentikasi sidik jari dan autentikasi hardware (NFC) secara berintegrasi berfungsi dengan baik, hasil akhir yang diharapkan setelah pengujian. Pertama, dari sisi dari perancangan dan implementasi sistem autentikasi sidik jari dan NFC terintegrasi dengan Arduino Mega ATmega 2560 untuk membuka akses pada SSD NVME terenkripsi, sistem ini dapat mampu menjalankan 4 inti utama secara responsif yang terdiri dari mode manajemen sidik jari, manajemen NFC, mode verifikasi, mode Ganti password. Sensor dan modul yang digunakan dalam pengembangan sistem ini menggunakan sensor fingerprint AS608 dan modul PN532. Hasil yang didapatkan dalam pengujian menunjukkan rata rata waktu yang diperlukan untuk proses pendaftaran sidik jari adalah 7,14 detik, sedangkan waktu rata-rata respon saat sidik jari yang terdaftar melakukan verifikasi adalah 0,74 detik, dan respon ketika sidik jari tidak terdaftar adalah 0,76 detik. Untuk pada bagian NFC, baik segi menggunakan smartphone atau kartu, rata-rata waktu dibutuhkan untuk pendaftaran yaitu 2,24–2,35 detik, rata-rata waktu dibutuhkan untuk verifikasi adalah 0,74–0,94 detik, dan waktu respon penolakan data yang tidak terdaftar adalah 0,85–0,86 detik. Hal ini dapat membuktikan bahwa autentikasi berfungsi secara responsif,akurat, dan efisien dalam mengelola autentikasi akses yang sah dan tidak sah.

Kedua, dari segi pada pengiriman password atau kunci enkripsi dari Arduino ke komputer setelah autentikasi berhasil, sistem yang dibuat mampu menjalankan pengiriman data secara aman melalui komunikasi usb. Berkat data password sebelum dikirim ke arduino di enkripsi dengan AES ECB, lalu di deksripsikan program yang berjalan di komputer untuk membuka enkripsi SSD NVME melalui software veracrypt. dari hasil pengujian rata rata waktu dibutuhkan untuk membuka enkripsi SSD NVME yaitu 2,95 detik hingga 7,82 detik. Ini hasil yang menunjukkan bahwa pada transmisi dan dekripsi data berjalan dengan lancar dan hambatan, serta menjawab tantangan dalam penelitian ini yaitu bagaimana menggantikan input password dengan autentikasi biometrik dan hardware (NFC) secara otomatis dan aman. Yang terakhir, hasil yang didapatkan dari pengujian di beberapa laptop dengan spesifikasi berbeda, baik prosesor Intel Core i3, i5 maupun AMD Ryzen 5, hasil yang menunjukkan bahwa sistem ini kompatibel dengan berbagai perangkat komputer berbasis Windows 10/11, dan dapat menjalankan dengan stabil tanpa mengalami gangguan, Rata-rata waktu yang dibutuhkan untuk ganti password mencapai 7 menit 2 detik, dengan jumlah error yang minim yang diakibatkan oleh cpu tidak mampu enkripsi secara optimal.

Dari hasil penelitian yang telah dilakukan, ada beberapa saran yang disampaikan untuk peneliti yang ingin mengembangkan produk ini secara lebih lanjut, sebagai berikut. Untuk saat ini peneliti menggunakan AES ECB untuk enkripsi pengiriman data, dengan pertimbangan keterbatasan kemampuan pada mikrokontroler arduino. AES- ECB dipilih karena ringan dalam proses enkripsi deksripsi, tapi mempunyai kelemahan pada pola data pada plaintext sama. Untuk saran kedepan nya menggunakan mikrokontroler esp 32 yang mempunyai pemrosesan yang tinggi disbanding dengan arduino, untuk dapat menerapkan dengan sistem AES GCM yang lebih aman dalam pengiriman data. Untuk

proses interface masih menggunakan CMD, peneliti menyadari bahwa beberapa pengguna umum tidak terbiasa dengan hal tersebut. Untuk saran kedepan mengembangkan (GUI) berbasis python atau software yang user – friendly agar dapat lebih nyaman dan aman. Sistem yang dikembangkan hanya untuk compatible pada windows 10/11, untuk kedapan nya dapat diperluas hingga sistem operasi mac os dan linux agar dapat bisa berjalan. Sistem yang dibangun saat ini mengandalkan autentikasi sidik jari dan NFC, meskipun keamanan ini sudah memberikan keamanan lebih baik, untuk pengembangan lebih lanjut di tambahkan seperti verifikasi titik Lokasi (Geo – Verifikasi) terdaftar, untuk menambah lapisan keamanan jika dicuri perangkat secara fisik.

Daftar Pustaka

Farizy, S., & Supriyatna, S. (2023). Analisis Terhadap Kinerja Sistem Komputer Yang Kurang Maksimal Atau Terjadinya Bottle Neck. *JITU: Jurnal Informatika Utama*, *1*(2). https://doi.org/10.55903/jitu.v1i2.158

Nurhadi, N., Suhaidi, M., & Latip, L. (2022). IMPLEMENTASI NEAR FIELD COMMUNICATION (NFC) UNTUK PEMBAYARAN RETRIBUSI TEMPAT KHUSUS PARKIR DI DINAS PERHUBUNGAN KOTA DUMAI BERBASIS E-MONEY. *Sebatik*, *26*(1), 139–146. https://doi.org/10.46984/sebatik.v26i1.1817

Siswanto, A., Efendi, A., & Yulianti, A. (2018). Alat Kontrol Akses Pintu Rumah Dengan Teknologi Sidik Jari Di Lingkungan Rumah Pintar Dengan Data Yang Di Enkripsi. *Jurnal Penelitian Pos Dan Informatika*, *8*(2), 97. https://doi.org/10.17933/jppi.2018.080201

Sri Haryati. (2012). *Research And Development (R&D) Sebagai Salah Satu Model Penelitian Dalam Bidang Pendidikan*.

Suhardi. (2016). Aplikasi Kriptografi Data Sederhana Dengan Metode Exlusive-Or (Xor). In *Jurnal Teknovasi* (Vol. 03, Issue 2).

Suling, C. E., Olivya, M., & Nur, R. (2017). *Seminar Nasional Teknik Elektro dan Informatika (SNTEI)*.

Tanzil Wahyu Ramadhan, Ike Desi Florina, & Didi Permadi. (2024). Analisis Framing Pemberitaan Peretasan Pusat Data Nasional (PDN) di Media Online Tempo.co. In *Journal of Education Research* (Vol. 5, Issue 3).

Waruwu, M. (2024). Metode Penelitian dan Pengembangan (R&D): Konsep, Jenis, Tahapan dan Kelebihan. *Jurnal Ilmiah Profesi Pendidikan*, *9*(2), 1220–1230. https://doi.org/10.29303/jipp.v9i2.2141