Sistem Keamanan Kartu NFC menggunakan Metode AES pada Sistem Pembayaran Elektronik

Susetyo Bagas Bhaskoro
Teknologi Rekayasa Informatika Industri
Politeknik Manufaktur Bandung
Bandung, Jawa Barat
bagas@ae.polman-bandung.ac.id

Pipit Anggraeni
Teknologi Rekayasa Otomasi
Politeknik Manufaktur Bandung
Bandung, Jawa Barat
pipit@ae.polman-bandung.ac.id

E. Nashrul Nijam
Teknologi Rekayasa Otomasi
Politeknik Manufaktur Bandung
Bandung, Jawa Barat
nashrul.nijam@mhs.polman-bandung.ac.id

Abstract— To maintain data security, a method is needed that can improve data security, one of which is by using cryptographic techniques. In an effort to meet the needs of data security, cryptography focuses on understanding and applying techniques to protect messages. There are several methods used in cryptography, one of which is the AES method which is recognized as the best encryption algorithm for several reasons, such as using a sufficiently secure key, high processing speed, and ensuring data integrity and confidentiality. In this study, the AES method is used to secure data in the form of nominal balances stored on NFC cards. Based on the test results, it can be seen that the NFC card can function as a balance storage with a maximum limit of IDR 1,000,000. Then based on the confusion matrix method, the security system on the NFC card has an accuracy value of 81,81%, 83.3% precision, and 93,75% recall.

Keywords— Data Security, Cryptography, Encryption, AES, NFC

I. PENDAHULUAN

Setiap individu, perusahaan, badan pemerintah, dan lembaga pendidikan menganggap bahwa data sebagai aset yang sangat berharga [1]. Oleh karena itu keamanan data harus mendapatkan perhatian yang serius. Dengan adanya sistem keamanan dapat memberikan kenyamanan dan ketenangan [2]. Dibutuhkan metode untuk meningkatkan keamanan data, salah satunya adalah melalui penggunaan teknik kriptografi [3]. Dalam memenuhi kebutuhan keamanan data, kriptografi berfokus pada pemahaman dan penerapan teknik untuk melindungi pesan selama proses pengiriman. Dalam hal ini, kriptografi memanfaatkan metode khusus untuk menyandikan pesan dengan maksud agar informasi di dalamnya tidak dimanfaatkan oleh pihak yang bukan penerima yang dituju [4]. Dalam kriptografi terdapat beberapa algoritma yang bisa digunakan untuk mengamankan sebuah data, salah satu contohnya adalah `AES (Advanced Encryption Standard)` yang merupakan sebuah algoritma kriptografi kunci simetris yang populer digunakan untuk melindungi keamanan data sensitif melalui proses enkripsi dan dekripsi, serta pengganti dari algoritma `DES (Data Encryption Standard)` [5]. `AES` dianggap sebagai algoritma enkripsi terbaik untuk beberapa alasan, seperti penggunaan kunci yang relatif aman, proses yang cepat, serta jaminan integritas dan kerahasiaan data [6]. Oleh karena itu cocok untuk perangkat dengan sumber daya terbatas seperti perangkat IoT dan sistem tertanam [7].

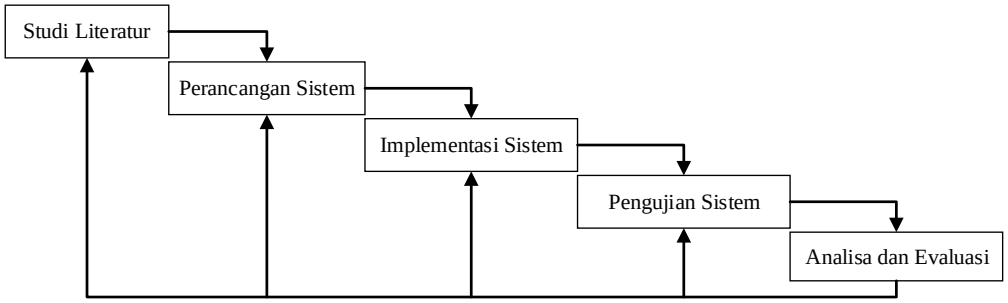
Menurut sebuah studi yang dilakukan oleh [8] menjelaskan bahwa sistem pembayaran elektronik dengan *smart card* bisa diamankan dengan menggunakan metode `caesar cipher`. Kemudian untuk sistem enkripsi menggunakan `AES` dapat diterapkan pada sistem pengamanan data pada `smart card` [9], pengamanan file [10], pengaman sistem presensi mahasiswa [11], dan pengamanan `QR-Code` [12]. Penelitian [13] merupakan penelitian

tentang penggunaan kartu NFC untuk pembayaran retribusi tempat khusus parkir berbasis E-Money, dalam penelitian tersebut teknologi NFC (Near Field Communication) digunakan sebagai sarana pembayaran digital yang tidak memerlukan uang tunai, kemudian seluruh proses transaksi dapat di pantau melalui halaman *web*. Penelitian [14] menjelaskan tentang sistem pengamanan pintu berbasis smart card menggunakan metode AES, penelitian tersebut berhasil mengimplementasikan metode AES. Tujuan dari penelitian ini untuk mengembangkan penelitian [8] sehingga kartu NFC yang digunakan memiliki sistem keamanan dengan metode AES.

Penelitian yang dilakukan oleh [8] memiliki celah kekurangan berupa metode yang digunakan untuk mengamankan kartu hanya menggunakan metode Caesar cipher sehingga tidak memiliki sistem keamanan yang kurang kuat. Sehingga dicoba diterapkan penelitian [13] dan penelitian [14]. Pembaharuan yang dilakukan yaitu terdapat pada metode yang digunakan untuk sistem keamanannya. Sehingga tercipta sistem keamanan kartu NFC menggunakan metode AES yang digunakan sebagai alat pembayaran non tunai. Jumlah saldo yang disimpan didalam kartu yang semula hanya di amankan menggunakan metode caesar cipher akan lebih kuat dan lebih aman bila menggunakan metode AES sehingga potensi terjadinya tindak kejahatan berupa pemalsuan data dapat diatasi. Kemudian seluruh proses transaksi akan terkirim ke dalam database dan dapat dipantau melalui halaman *web*.

II. METODE PENELITIAN

Dalam penelitian ini, metode waterfall digunakan untuk menyelesaikan permasalahan yang ada. Metode waterfall adalah suatu metode berurutan yang digunakan dalam pelaksanaan penelitian. Penjelasan mengenai pelaksanaan metode waterfall dapat dilihat pada Gambar 1.

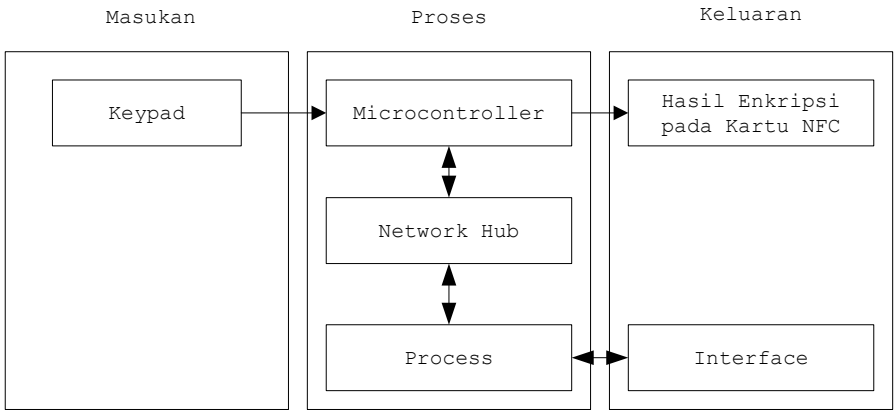


Gambar 1. Diagram Alir Metode Penelitian

Pada studi literatur dilakukan pemahaman terhadap teori-teori dasar yang berkaitan dengan penelitian ini. Mulai dari teori-teori mengenai kriptografi, enkripsi dan dekripsi menggunakan algoritma AES, serta sistem keamanan pada kartu NFC dengan menggunakan algoritma AES. Algoritma AES dipilih karena memiliki tingkat keamanan yang tinggi baik dari segi kunci maupun ukuran bila dibandingkan dengan kriptografi klasik. Selanjutnya, dalam tahap perancangan sistem ini, tujuannya adalah untuk merencanakan sistem yang akan dibuat., tahap ini dimulai dengan desain penentuan spesifikasi, perancangan wujud dan perancangan secara terperinci. Tahap implementasi merupakan proses untuk merealisasikan atau membuat sistem yang telah dibuat pada proses perancangan. Pengujian sistem dilakukan untuk menguji fungsi-fungsi yang telah direalisasikan. Tahap analisa dan evaluasi dilakukan untuk menganalisa sistem yang telah dibuat apakah telah sesuai teori-teori dan mengevaluasinya sesuai dengan spesifikasi.

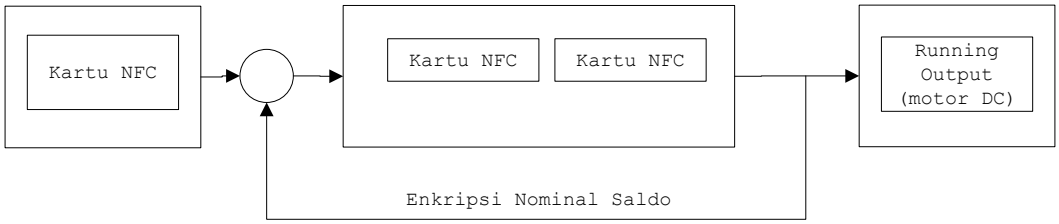
A. Perancangan Perangkat Keras

Sistem keamanan dengan algoritma AES pada pengendali 1 akan direalisasikan pada sistem pembayaran yang telah dirancang seperti pada Gambar 2.



Gambar 2. Skema Pengendali 1

Secara sederhana, skema dari pengendali 1 dapat dilihat pada Gambar 2. Pengendali 1 ini berfungsi untuk mendaftarkan kartu dan menambahkan saldo, komponen yang digunakan yaitu keypad yang berfungsi sebagai data masukkan. Data yang dimasukkan berupa jumlah nominal saldo. Selanjutnya data tersebut dikirim ke dalam Microcontroller kemudian terjadi proses enkripsi sehingga data tersebut sulit untuk dibaca. Data hasil enkripsi tersebut akan dikirimkan ke kartu NFC, sehingga kartu NFC tersebut memiliki nominal saldo yang sudah di enkripsi. Setiap proses transaksi penambahan nominal saldo akan tercatat dan masuk ke database. Kemudian data yang terdapat pada *database* akan diolah oleh halaman web sehingga admin bisa mengetahui setiap proses transaksi yang telah dilakukan. Sedangkan untuk rancangan pengendali 2 dapat dilihat pada Gambar 3.



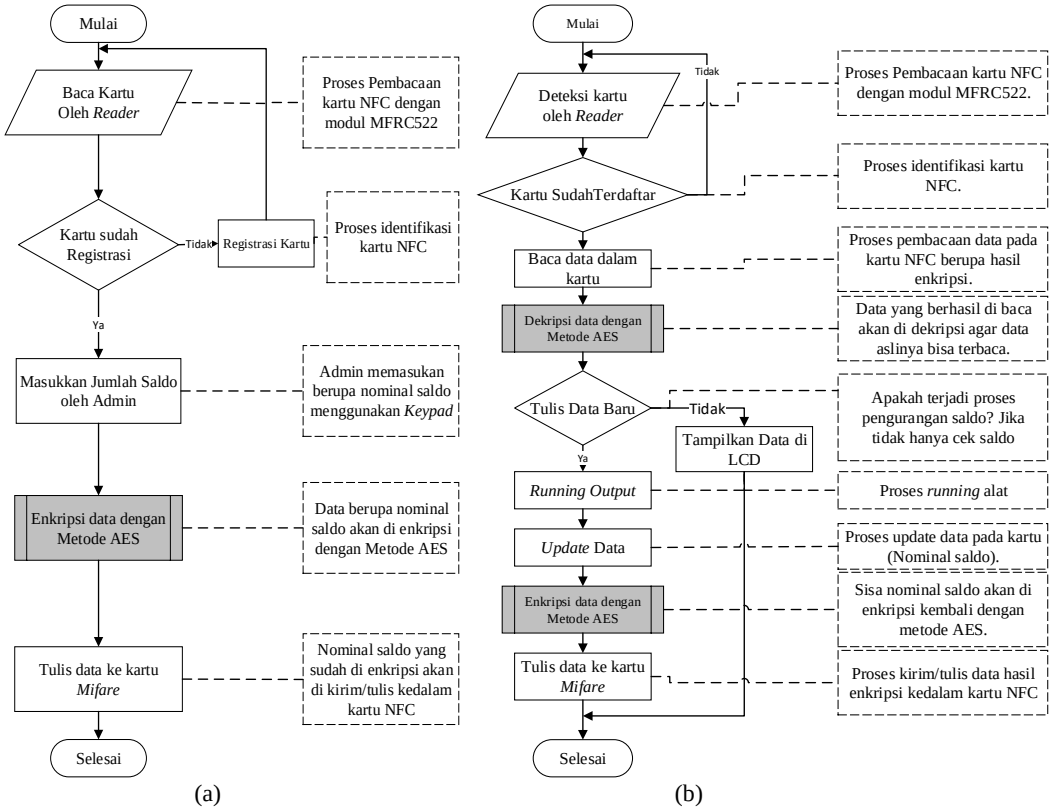
Gambar 3. Skema Pengendali 2

Untuk skema dari pengendali 2 dapat dilihat pada Gambar 3. Pengendali 2 ini berfungsi untuk mengurangi saldo yang terdapat pada kartu NFC, data hasil enkripsi yang terdapat pada kartu NFC selanjutnya akan di dekripsi terlebih dahulu oleh microcontroller sehingga jumlah nominal saldo yang sebelumnya tidak terbaca akan terbaca. Setelah proses dekripsi berhasil saldo akan berkurang kemudian *output* akan menyala. Saldo yang mengalami pengurangan akan di enkripsi kembali dan disimpan didalam kartu.

Pada sistem perangkat keras ini digunakan kartu NFC sebagai media penyimpanan data. Kartu NFC dipilih karena memiliki keunggulan bila dibandingkan dengan smart card lainnya. Dengan teknologi NFC, pengguna memiliki kemampuan untuk melakukan proses transaksi, mengakses konten digital, dan terhubung dengan perangkat elektronik tanpa harus melakukan kontak fisik secara langsung, cukup dengan sekali menyentuhnya. [15].

B. Perancangan Perangkat Lunak

Sistem dibagi menjadi 2 proses utama yaitu enkripsi dan dekripsi. Metode pada enkripsi dan dekripsi ini menggunakan Algoritma `AES`. Proses enkripsi berlangsung saat `admin` melakukan proses penambahan nominal saldo pada kartu `NFC`. Untuk proses dekripsi terjadi ketika pengguna akan melakukan proses `running output` berupa motor `12v`. Diagram alir proses enkripsi dan dekripsi dapat dilihat pada Gambar 4 dan Gambar 5.



Gambar 4. (a) Skema Pengendali 1 (b) Skema Pengendali 2

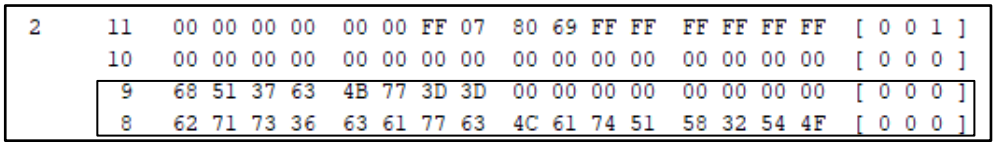
C. Realisasi Perangkat Lunak

Berdasarkan perancangan pada Gambar 4, secara umum proses dilakukan dengan menyimpan data hasil enkripsi ke dalam kartu `NFC`. Didalam kartu tersebut terdapat `16 sector` dan `64 blok` yang dapat diisi data apapun. Pada penelitian ini terdapat dua data yang disimpan didalam kartu. Data pertama yaitu pada saat proses pendaftaran kartu, kode daftar berupa hasil enkripsi disimpan pada `sector 3` dapat dilihat pada Gambar 5.

```
3     15   00 00 00 00   00 00 FF 07   80 69 FF FF   FF FF FF FF   [ 0 0 1 ]
      14   00 00 00 00   00 00 00 00   00 00 00 00   00 00 00 00   [ 0 0 0 ]
      13   69 69 4A 35   4C 51 3D 3D   00 00 00 00   00 00 00 00   [ 0 0 0 ]
      12   69 52 4B 39   74 64 67 75   5A 5A 42 6F   4C 77 4C 73   [ 0 0 0 ]
```

Gambar 5. Penyimpanan Kode Daftar Terenkripsi

Berdasarkan Gambar 5 bisa dilihat bahwa data hasil enkripsi dengan metode `AES` yang berjumlah `24 karakter` disimpan pada `sector 3`. Data kedua yang disimpan di dalam kartu adalah nominal uang yang di enkripsi, data tersebut disimpan di dalam kartu `NFC` pada `sector 2`. Untuk lebih jelasnya dapat dilihat pada Gambar 6.



Gambar 6. Penyimpanan Nominal Saldo Terenkripsi

III. HASIL DAN PEMBAHASAN

Dalam penelitian ini, terdapat beberapa langkah pengujian yang dilakukan untuk memastikan kesesuaian sistem dengan harapan yang diinginkan. Adapun proses pengujiannya meliputi pengujian sistem secara keseluruhan yang didalamnya terdapat pengujian pada kartu NFC, pengujian terhadap upaya pemalsuan data, dan pengujian metode AES. Data yang diperoleh selanjutnya diolah menggunakan metode Confusion Matrix.

A. Pengujian Pada Kartu NFC

Pada proses pengujian ini menggunakan 3 kartu NFC yang memiliki UID berbeda. Tujuan dari pengujian pada kartu ini yaitu untuk mengetahui apakah kartu NFC tersebut merupakan kartu yang disediakan oleh admin atau bukan dan apakah kartu NFC tersebut sudah diamankan dengan menggunakan metode AES atau belum. Penjelasan dari masing-masing kartu NFC bisa dilihat pada Tabel 1.

Tabel 1. Penjelasan Kartu yang Akan di Uji

No	UID Kartu	Deskripsi
1	1bfdcd51	Kartu Tidak Diketahui
2	f84a8c0d	Kartu dari admin tetapi tidak didaftarkan terlebih dahulu
3	b7f178e1	Kartu yang sudah di enkripsi

Pengujian ini dilakukan pada pengendali *2*. Pada saat kartu yang digunakan adalah kartu yang bukan disediakan oleh admin, maka sistem pada pengendali 2 akan menolak nya. Untuk hasil pengujiannya dapat dilihat pada Tabel 2.

Tabel 2. Hasil Pengujian Kartu Bukan dari *Admin*

No	UID	Hasil
1	1bfdcd51	Kartu Ditolak
2	1bfdcd51	Kartu Ditolak
3	1bfdcd51	Kartu Ditolak

Berdasarkan hasil pengujian pada Tabel 2, pengujian dilakukan sebanyak 3 kali pada kartu yang bukan disediakan oleh admin. Pengujian tersebut membuktikan bahwa kartu yang memiliki id 1bfdcd51 tidak terdaftar pada sistem sehingga tidak dapat digunakan untuk proses transaksi.

Pengujian selanjutnya yaitu pada kartu ke-2, pengujian yang dilakukan adalah pada saat kartu yang akan digunakan tidak didaftarkan terlebih dahulu, maka sistem pada pengendali 2 akan memberikan informasi bahwa kartu tersebut belum didaftarkan. Untuk hasil pengujiannya terdapat pada Tabel 3.

Tabel 3. Hasil Pengujian Kartu Tidak Terdaftar

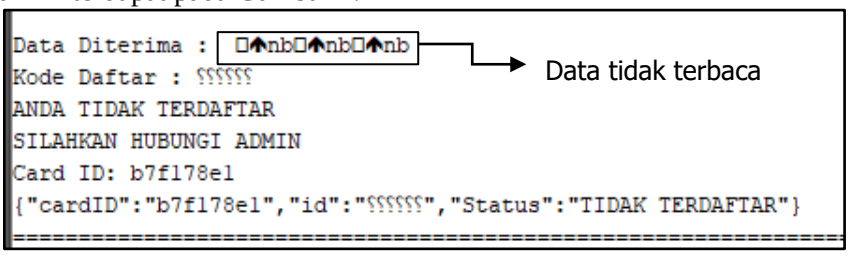
No	UID	Hasil
1	f84a8c0d	Kartu Tidak Terdaftar
2	f84a8c0d	Kartu Tidak Terdaftar
3	f84a8c0d	Kartu Tidak Terdaftar

Berdasarkan Tabel 3, pengujian dilakukan sebanyak 3 kali pada kartu yang belum didaftarkan. Hasilnya bisa diketahui bahwa sistem memberikan informasi jika kartu tidak terdaftar. Ini terjadi karena sistem akan membaca data yang terdapat pada `sector 3` terlebih dahulu, yang didalamnya terdapat kode daftar yang terenkripsi. Data tersebut akan di dekripsi terlebih dahulu kemudian membandingkan apakah data tersebut sudah sesuai dengan yang sudah ditentukan pada pengendali 2. Apabila data yang dibaca sudah sesuai maka selanjutnya sistem akan membaca data pada `sector 2` yang berisi nominal saldo yang terenkripsi kemudian data tersebut di dekripsi agar nominal saldo yang terdapat didalam kartu dapat terbaca. Untuk proses pengujiannya terdapat pada Tabel 4.

Tabel 4. Hasil Pengujian Pembacaan Jumlah Saldo

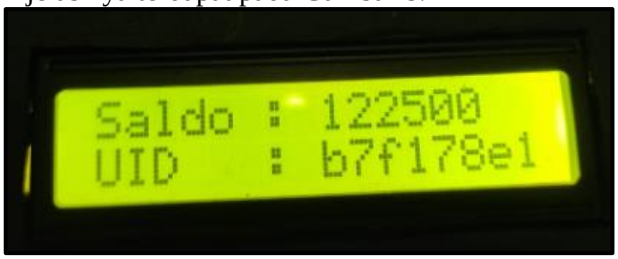
No	UID	Hasil
1	b7f178e1	Saldo Terbaca
2	b7f178e1	Saldo Terbaca
3	b7f178e1	Saldo Terbaca
4	b7f178e1	Saldo Tidak Terbaca
5	b7f178e1	Saldo Terbaca

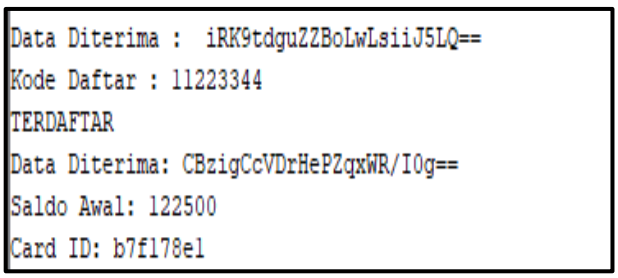
Berdasarkan Tabel 4, pengujian dilakukan sebanyak 5 kali dengan hasil keakuratan `80%`. Pada pengujian ke-4, saldo yang terdapat di dalam kartu tidak terbaca, ini terjadi karena gagalnya proses pembacaan data di dalam kartu. Untuk kegagalan proses pembacaan ini terdapat pada Gambar 7.



Gambar 7. Kegagalan Proses Pembacaan Data di Dalam Kartu

Berdasarkan Gambar 7, bisa dilihat bahwa data yang terdapat didalam kartu tidak dapat dibaca dengan sempurna sehingga data terenkripsi yang ada di dalam kartu berubah menjadi data yang tidak bisa di dekripsi menjadi data asli. Kemudian memberi informasi bahwa kartu tidak terdaftar. Sedangkan apabila data yang terdaftar di dalam kartu NFC terbaca dengan sempurna, maka nominal saldo yang terdapat pada `sector 2` akan terbaca. Untuk lebih jelas nya terdapat pada Gambar 8.





Gambar 8. Proses Pembacaan Saldo Pada Kartu

Selanjutnya pengujian terhadap penyimpanan nominal saldo di dalam kartu NFC. Pengujian ini dilakukan untuk menguji berapa jumlah saldo yang dapat disimpan di dalam kartu NFC. Pengujian dilakukan terhadap kartu yang memiliki saldo Rp 0, kemudian dilakukan penambahan sebanyak 5 kali. Untuk hasil pengujian dapat dilihat pada Tabel 5.

Tabel 5. Pengujian Penambahan Saldo

UID	Saldo Awal	Jumlah Penambahan	Saldo Akhir	Status
f84a8c0d	Rp. 0	Rp. 250.000	Rp. 250.000	Berhasil
f84a8c0d	Rp. 250.000	Rp. 250.000	Rp. 500.000	Berhasil
f84a8c0d	Rp. 500.000	Rp. 250.000	Rp. 750.000	Berhasil
f84a8c0d	Rp. 750.000	Rp. 250.000	Rp. 1.000.000	Berhasil
f84a8c0d	Rp. 1.000.000	Rp. 250.000	Rp. 1.000.000	Gagal

Berdasarkan pengujian yang dilakukan pada Tabel 5, dapat diketahui bahwa kartu NFC tidak dapat menyimpan saldo lebih dari Rp 1.000.000. Tujuan dari pembatasan ini yaitu untuk menghindari kerugian apabila kartu NFC yang digunakan hilang atau rusak, serta merupakan saran dari penelitian sebelumnya yang dilakukan oleh [8].

B. Pengujian Terhadap Upaya Pengubahan Data

Pengujian ini bertujuan untuk menguji apakah sistem keamanan yang dibuat sudah dapat mengatasi apabila terjadi upaya dalam pengubahan data. Pengujian dilakukan dengan mengubah hasil enkripsi yang tersimpan didalam *database*. Untuk hasil pengujian dapat dilihat pada Tabel 6.

Tabel 6. Pengujian Pengubahan Data pada *Database*

UID	Data Sebelum di Ubah	Data Sesudah di Ubah	Saldo yang Terbaca
b7f178e1	X0ZPGzkBjIJuSgrQSO3FSQ==	Q9TVHzkBjIJuSgrQSO3FSQ==	Rp. 120.000
07310ae0	bTUdlZmvz1R 2yINmVEriQ==	nGKilZmvz1R 2yINmVEriQ==	Rp. 250.440
6bb46b51	sUBcGLv4u5koYcih7MVRw==	pQBcGLv4u5koYcih7MVRw==	Rp. 457.750

Berdasarkan pengujian pada Tabel 6, pengujian dilakukan sebanyak 3 kali dengan mengubah beberapa karakter secara acak pada hasil enkripsi saldo yang tersimpan didalam database. Dari hasil pengujian tersebut dapat diketahui bahwa apabila terjadi proses pemalsuan data, nominal saldo yang terdapat didalam kartu tidak akan berubah. Ini terjadi karena media untuk menyimpan saldo terdapat didalam kartu NFC dan bukan didalam database. Kemudian pengujian selanjutnya dilakukan pada kartu NFC, pengujian dilakukan dengan mengubah data berupa nominal saldo terenkripsi yang terdapat di dalam kartu pada sector 2. Untuk hasil pengujiannya dapat dilihat pada Tabel 7.

Tabel 7. Pengujian Pengubahan data pada Kartu NFC

UID	Saldo Awal	Data Sebelum di Ubah	Data Sesudah di Ubah	Saldo yang Terbaca
b7f178e1	Rp. 120.000	X0ZPGzkBjIJuSgrQSO3FSQ==	300000	Rp. 0
07310ae0	Rp. 250.440	bTUdlZmvz1R 2yINmVEriQ==	500000	Rp. 0
6bb46b51	Rp. 457.750	sUBcGLv4u5koYcih7MVRw==	750000	Rp. 0

Berdasarkan pengujian pada Tabel 7, data didalam kartu NFC yang tersimpan pada `sector 2` saat diubah menjadi data yang tidak terenkripsi dengan mengindikasikan bahwa itu nominal saldo, maka sistem akan memberikan informasi bahwa saldo `Rp 0`. Dengan begitu kartu NFC dapat menyimpan saldo dengan karakter tidak dapat dimengerti dan dapat terhindar dari upaya penambahan saldo secara langsung tanpa proses enkripsi. Untuk contoh hasil percobaan pada Tabel 7 dapat dilihat pada Gambar 9.


```
Data Diterima :  iRK9tdguZZBoLwLsiiJ5LQ==
Kode Daftar : 11223344
TERDAFTAR
Data Diterima: 500000
Saldo Awal: 0
Card ID: 07310ae0
```

Gambar 9. Tampilan pada Sistem

C. Pengujian Metode AES

Pengujian ini dilakukan untuk mengetahui bahwa metode AES yang digunakan dapat menghasilkan karakter yang tidak dapat dibaca. Data berupa jumlah saldo dan kode daftar yang disimpan didalam kartu akan di enkripsi terlebih dengan metode AES. Pengujian dilakukan pada kartu dengan `UID f84a8c0d` dan memiliki saldo sebesar `Rp 1.000.000`. Gambar 10 merupakan data yang diperoleh dari kartu NFC pada `sector 2` yang berisi nominal saldo terenkripsi.

```
2     11   00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF  [ 0 0 1 ]
      10   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
       9   6D 4E 64 6C  4D 41 3D 3D  00 00 00 00  00 00 00 00  [ 0 0 0 ]
       8   76 52 58 78  48 79 54 4D  67 6A 50 65  70 6F 59 44  [ 0 0 0 ]
```

Gambar 10. Data di Dalam Kartu

Berdasarkan Gambar 10, data yang diperoleh adalah data hasil enkripsi yaitu `765258784879544D676A5065706F59443530794847513D3D`, kemudian data tersebut di dekripsi dengan `kunci (K) abcdefghijklmnop`. Untuk prosesnya adalah sebagai berikut.

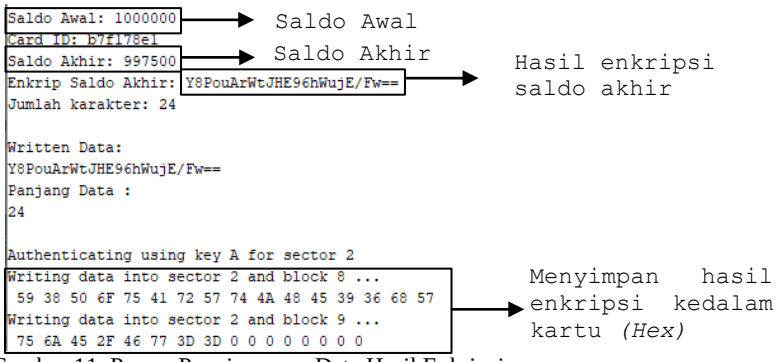
```
Hex             = 765258784879544D676A5065706F59443530794847513D3D
Text            = vRXxHyTMgjPepoYD50yHGQ==
Key             = abcdefghijklmnop
Base64          = MTAwMDAwMA==
Data Asli       = 1.000.000
```

Hasil enkripsi nominal saldo setelah mengalami proses pengurangan, selanjutnya akan disimpan di dalam kartu NFC pada *sector* 2 dalam bentuk *Hexadecimal*. Untuk proses pembuktiannya dapat dilihat pada Gambar 11.

```
Saldo Awal          = 1.000.000
Pengurangan         = 2.500
Saldo Akhir         = 997.500
```

```
Key                 = abcdefghijklmnop
Hasil Enkripsi      = Y8PouArWtJHE96hWujE/Fw==
Hex                 = 5938506F75417257744A484539366857756A452F46773D3D
```

Hasil enkripsi nominal saldo setelah mengalami proses pengurangan, selanjutnya akan disimpan didalam kartu NFC pada *sector* 2 dalam bentuk *Hexadecimal*. Untuk proses pembuktiannya dapat dilihat pada Gambar 11.



Gambar 11. Proses Penyimpanan Data Hasil Enkripsi

D. Pengujian Dengan Metode *Confusion Matrix*

Confusion matrix merupakan metode pengujian yang digunakan untuk menghitung tingkat akurasi dari sebuah sistem yang telah dibuat [16]. Pengujian dilakukan dengan mencari terlebih dahulu data dari sistem yang telah dibuat. Data tersebut berupa hasil pengujian dari beberapa elemen yang terdapat pada sistem. Data yang didapat dikelompokkan berdasarkan kategori jenis data tersebut, kemudiaan data diolah dengan persamaan pada metode confusion matrix. Pada penelitian ini, metode confusion matrix digunakan untuk menghitung nilai accuracy, precision, dan recall pada sistem. Untuk contoh tabel confusion matrix dapat dilihat pada Tabel 8.

Tabel 8. *Confusion Matrix*

n		Prediksi	
		True	***False***
Aktual	*True*	TP	FP
	False	FN	TN

```
TP (True Positive)      = Jumlah transaksi yang diprediksi aman dan sebenernya
                          aman.
                          (Data pada Tabel 2, 3, 4, dan 5)
TN (True Negative)      = Jumlah transaksi yang diprediksi tidak aman dan
                          sebenarnya
                          tidak aman. (Data pada Tabel 7)
FP (False Positive)     = Jumlah transaksi yang diprediksi tidak aman tetapi
                          sebenarnya aman. (Data pada Tabel 6)
FN (False Negative)     = Jumlah transaksi yang diprediksi aman tetapi sebenarnya
                          tidak aman. (Data pada Tabel 4 Pengujian No.4)
```

Accuracy digunakan untuk memprediksi seberapa aman transaksi yang dilakukan.

$$Accuracy = \frac{TP+TN}{TP+FP+FN+TN} . 100 \qquad (1)$$

Precision digunakan untuk memberikan informasi tentang kemampuan untuk mengklasifikasikan bahwa sistem aman dengan akurat.

$$Precision = \frac{TP}{TP+FP} . 100 \qquad (2)$$

Recall digunakan untuk mengetahui seberapa kuat sistem mampu mengenali transaksi yang sebenarnya tidak aman.

$$Recall = \frac{TP}{TP+FN} .100 \qquad (3)$$

Berdasarkan pengujian yang telah dilakukan, terdapat 22 data yang akan dikelompokan berdasarkan tabel confusion matrix. Untuk hasilnya dapat dilihat pada Tabel 9.

Tabel 9. Pemetaan Data pada tabel *Confusion Matrix*

22		**Prediksi**	
		True	***False***
Aktual	*True*	TP = 15	FP = 3
	False	FN = 1	TN = 3

Kemudian data tersebut diolah dengan menggunakan confusion matrix untuk menghitung nilai dari accuracy, precision, dan recall. Berikut masing-masing nilai hasil perhitungan.

$$Accuracy = \frac{15+3}{15+3+1+3} .100 = 81{,}81\,\%$$

$$Precision = \frac{15}{15+5} .100 = 83{,}3\,\%$$

$$Recall = \frac{15}{15+1} .100 = 93{,}75\,\%$$

Berdasarkan hasil perhitungan dengan metode confusion matrix, dapat diketahui bahwa sistem keamanan pada kartu NFC memilik nilai accuracy 81,81%, precision 83,3%, dan recall 93,75%.

IV. KESIMPULAN

Berdasarkan temuan dari penelitian yang telah dilaksanakan, dapat disimpulkan bahwa data berupa kode daftar dan nominal saldo yang disimpan didalam *sector 2* dan *sector 3* kartu NFC dapat diamankan dengan metode AES. Metode AES diakui sebagai algoritma enkripsi terbaik dengan beberapa alasan, seperti penggunaan kunci yang cukup aman, kecepatan proses yang tinggi, serta menjamin integritas dan kerahasiaan data. Jumlah saldo yang dapat disimpan didalam kartu adalah tidak lebih dari Rp 1.000.000. Berdasarkan pengujian dengan *confusion matrix* sistem keamanan pada kartu NFC memilik nilai accuracy 81,81%, precision 83,3%, dan recall 93,75%.

DAFTAR PUSTAKA

[1] D. Darwis, R. Prabowo, And N. Hotimah, "Kombinasi Gifshuffle, Enkripsi Aes Dan Kompresi Data Huffman Untuk Meningkatkan Keamanan Data," *Jurnal Teknologi Informasi Dan Ilmu Komputer*, Vol. 5, No. 4, P. 389, Oct. 2018, Doi: 10.25126/Jtiik.201854727.

[2] A. Salam And S. Bagas Bhaskoro, "Sistem Keamanan Cerdas Pada Kunci Pintu Otomatis Menggunakan Kode Qr," *Cybernetics*, Vol. 5, No. 01, Pp. 1–11, 2021.

[3] A. Rilo Pambudi, "Implementasi Kriptografi Pada Email Menggunakan Algoritma Rivest Code 4 (Rc4) Dan Data Encryption Standart (Des) Berbasis Java Desktop Pada Pt Vepro Nusa Persada," 2018.

[4] A. Aditya Permana, "Penerapan Kriptografi Pada Teks Pesan Dengan Menggunakan Metode Vigenere Cipher Berbasis Android," 2018.

[5] T. M. Kumar, K. S. Reddy, S. Rinaldi, B. D. Parameshachari, And K. Arunachalam, "A Low Area High Speed Fpga Implementation Of Aes Architecture For Cryptography Application," *Electronics (Switzerland)*, Vol. 10, No. 16, Aug. 2021, Doi: 10.3390/Electronics10162023.

[6] H. M. Mohammad And A. A. Abdullah, "Enhancement Process Of Aes: A Lightweight Cryptography Algorithm-Aes For Constrained Devices," *Telkomnika (Telecommunication Computing Electronics And Control)*, Vol. 20, No. 3, Pp. 551–560, 2022, Doi: 10.12928/Telkomnika.V20i3.23297.

[7] S. S. Dhanda, B. Singh, And P. Jindal, "Lightweight Cryptography: A Solution To Secure Iot," *Wirel Pers Commun*, Vol. 112, No. 3, Pp. 1947–1980, Jun. 2020, Doi: 10.1007/S11277-020-07134-3.

[8] D. Nataliana, F. Hadiatna, And A. Fauzi, "Rancang Bangun Sistem Keamanan Rfid Tag Menggunakan Metode Caesar Cipher Pada Sistem Pembayaran Elektronik," *Elkomika: Jurnal Teknik Energi Elektrik, Teknik Telekomunikasi, & Teknik Elektronika*, Vol. 7, No. 3, P. 427, Sep. 2019, Doi: 10.26760/Elkomika.V7i3.427.

[9] V. Nur Wijayaningrum, R. Ariyanto Jurusan Teknologi Informasi, And P. Negeri Malang Jalan Soekarno Hatta, "Pemanfaatan Aes Dengan Key Dinamis Sebagai Metode Pengamanan Data Pada Smart Card," 2021. [Online]. Available: Http://Sistemasi.Ftik.Unisi.Ac.Id

[10] K. Muttaqin And J. Rahmadoni, "Analysis And Design Of File Security System Aes (Advanced Encryption Standard) Cryptography Based," 2020.

[11] M. Alfan Rosid, "Sistem Presensi Mahasiswa Menggunakan Qr Code Dengan Fitur Geolocation Dan Enkripsi Aes," 2021.

[12] D. Qunita, P. Ambeq Paramarta, A. Kusyanti, And M. Data, "Implementasi Algoritme Advance Encryption Standard (Aes) Pada Enkripsi Dan Dekripsi Qr-Code," 2018. [Online]. Available: Http://J-Ptiik.Ub.Ac.Id

[13] N. Nurhadi, M. Suhaidi, And L. Latip, "Implementasi Near Field Communication (Nfc) Untuk Pembayaran Retribusi Tempat Khusus Parkir Di Dinas Perhubungan Kota Dumai Berbasis E-Money," *Sebatik*, Vol. 26, No. 1, Pp. 139–146, Jun. 2022, Doi: 10.46984/Sebatik.V26i1.1817.

[14] A. Pratiwi, A. Fauzi, And D. Sulistya Kusumaningrum, "Sistem Pengamanan Pintu Otomatis Berbasis Rfid Menggunakan Metode Aes," Vol. Iii, No. 2, P. 202, 2022.

[15] I. Frastika Fitri And Derisma, "Rancang Bangun Real Count E-Voting Menggunakan Mikrokontroler," *Chipset*, Vol. 1, No. 02, Pp. 69–78, Nov. 2020, Doi: 10.25077/Chipset.1.02.69-78.2020.

[16] E. W. Hary Candana, I. Gede, A. Gunadi, And D. G. H. Divayana, "Perbandingan Fuzzy Tsukamoto, Mamdani Dan Sugeno Dalam Penentuan Hari Baik Pernikahan Berdasarkan Wariga Menggunakan Confusion Matrix," *Jurnal Ilmu Komputer Indonesia (Jik)*, Vol. 6, No. 2, 2021.