Keamanan Data Transaksi Nasabah Pada Aplikasi Bank Sampah Berbasis Web Menggunakan Algoritma AES

Aditya Puji Nugroho[1], Arini[2], Hendra Bayu Suseno[3]

Program Studi Teknik Informatika, Fakultas Sains dan Teknologi
Universias Islam Negeri Syarif Hidaytullah Jakarta
[1]adityapuji40@gmail.com, [2]arini@uinjkt.ac.id, [3]hendra.bayu@uinjkt.ac.id

Abstract

The Malacca waste bank located in East Jakarta was established in 2008, the Malacca waste bank has a number of customers reaching more than 300 people and the waste absorbed every month reaches 2 - 2.5 tons. In carrying out its activities, the Malacca Sari waste bank still has several problems, including: the difficulty of recording the income of waste, the lack of integrity between the customer's savings book and the garbage bank's bookkeeping and the customer often does not carry a savings book, and even something is missing, to anticipate this and improve the services of the garbage bank, we need an application for processing data effectively and efficiently, which can have a secure data storage system and complement the application with good security techniques. In this case the researcher uses the cryptographic algorithm (Advanced Encryption System). With this application, it is expected that transaction data information stored in the application will be safe and not known to eavesdroppers or irresponsible parties. In this application, the encrypted information is only in the form of balance data at a garbage bank and only the management and customers can use this application. Based on program implementation and testing, researchers can conclude that this application is easy to use, the confidentiality of data and information able to maintain and protect

Keywords : *AES (Advanced Encryption System), MySQL, Cryptographic, Php, Waste Bank.*

1. PENDAHULUAN

Persampahan merupakan permasalahan yang dialami di kota-kota besar di Indonesia, perhari terdapat 625 juta liter atau 2,5 liter sampah. Pertambahan dan penurunan jumlah seiring dengan kondisi lingkungannya. Salah satu cara yang ditempuh oleh Kementerian Lingkungan yaitu pengembangan Bank Sampah. Hal ini dapat digunakan sebagai edukasi pada masyarakat dalam pengolahan sampah secara bijak dan menumbuhkan kesadaran pada masyarakat akan sampah, sehingga jumlah sampah yang dibawa ke tempat penampungan akhir sampah akan menurun/berkurang. Peraturan Pemerintah (PP) Nomor 81 Tahun 2012 mengenai sampah sejenis sampah RT (rumah tangga) dan cara pengolahannya mengatur untuk melakukan 3R yaitu diantaranya produk kemasan harus mudah diurai oleh alam, sampah yang dihasilkan sekecil mungkin, bahan produksi dapat didaur ulang atau digunakan kembali [1].

Jika diambil contoh bank sampah melalui program "Jakarta *Green* and *Clean" dari* pemprov DKI ialah Bank Sampah Malaka Sari RW 03 Jakarta Timur dengan jumlah nasabah mencapai lebih dari 300 orang dan sampah yang terserap setiap bulan mencapai 2 – 2.5 Ton, yang mulai dirintis tahun 2008 sampai sekarang.

Akan tetapi dalam proses pengimplementasiannya, dari hasil wawancara dan obeservasi masih terdapat beberapa masalah, antara lain : nasabah sering tidak membawa buku tabungan, bahkan ada yang hilang, sulitnya mendata pemasukan sampah, kurangnya integritas data antara buku tabungan nasabah dengan pembukuan bank sampah, maka diperlukan sebuah aplikasi untuk pengolahan data yang efektif dan efisien, yang di dalamnya dapat memilki sistem penyimpanan data yang aman dan tentunya melengkapi aplikasi dengan teknik pengamanan yang cukup baik untuk mengantisipasi adanya kemungkinan buruk yang akan terjadi seperti manipulasi data. Pada penelitian ini peneliti akan mengimplementasikan sistem pengamanan dengan menggunakan teknik kriptografi yaitu AES.

Copyright © 2020, the Authors. Published by QUERY: JURNAL SISTEM INFORMASI
This is an open access article under the CC BY license (https://creativecommons.org/licenses/by/4.0/).

Mengacu pada [2], dinyatakan AES memiliki kecepatan enkripsi dan deskripsi tertinggi, berikutnya Blowfish, DES dan IDEA. Menurut [3], menggunakan algoritma AES 256 untuk mengenkrip *Data Customer* pada *E-commerce* dan menghasilkan *text* yang tidak sama meskipun kuncinya sama (statis). Menurut [4], data berupa *plain image* dengan membandingkan kecepatan dan kualitas enkripsi dengan AES dan RSA. Pada [5], kode transaksi yang berupa *plain text* nantinya akan di enkripsi sebelum dikirim ke *server*, lalu proses dekripsinya dikirim oleh server, menggunakan algoritma Rijindael (AES). Menurut [6], menggunakan algoritma AES untuk data *excel*, *word* dan *pdf*. Menurut [7], *user* menginput *plain text* yang kemudian akan diproses menjadi Qr-Code, lalu Qr-code dan *plain text* di enkripsi menggunakan algoritma AES. Pada [8], yang menggabungkan AES dan Rivest Shamir yang secara simetris dan asimetris untuk aplikasi pesan. Dari beberapa literatur yang digunakan, penelitian ini akan menggunakan algoritma AES untuk mengamankan Data Transaksi Nasabah.

2. METODE PENELITIAN

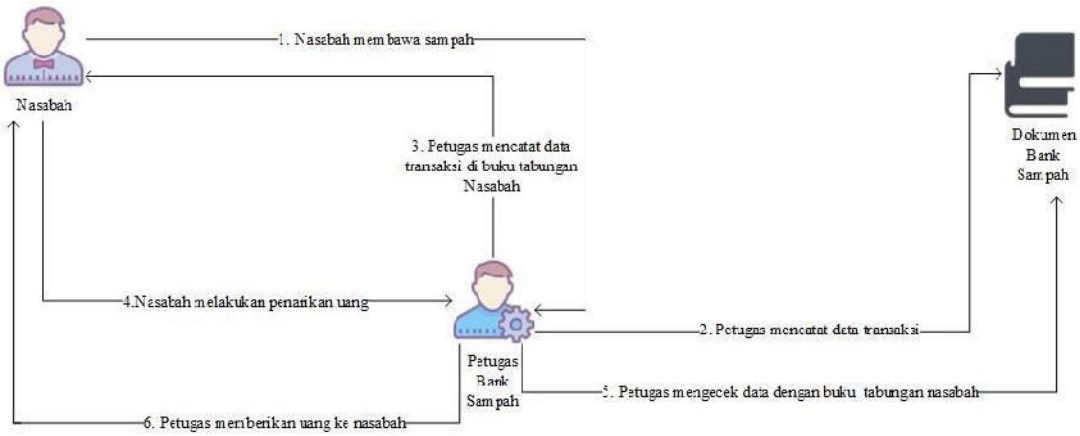
Metode untuk pengumpulan data menggunakan metode studi lapangan yaitu wawancara dan observasi, sedangkan untuk pengembangannya menggunakan *Rapid Application Development* (RAD) dengan tahapan yaitu :

a. *Requirements Planning* (Perencanaan Syarat-Syarat), terdiri dari tahap :
   1. Analisis masalah
   2. Identifikasi sistem yang sedang berjalan
   3. Membuat sistem usulan
b. *RAD Design Workshop* (*Workshop* Desain RAD), peneliti melakukan :
   1. Melakukan perancangan input,
   2. Merancang spesifikasi proses
   3. Merancang *Unifed Modeling Language* (UML), meliputi pembuatan diagram : *use case, activity, sequence* dan class
   4. Merancang basisdata
   5. Merancang antarmuka
   6. Melakukan pengkodean program.
c. *Implementation* (implementasi) menggunakan spesifikasi *hardware* dan *software* yang direncanakan dan terakhir implementasi antarmuka pengguna.

3. HASIL DAN PEMBAHASAN

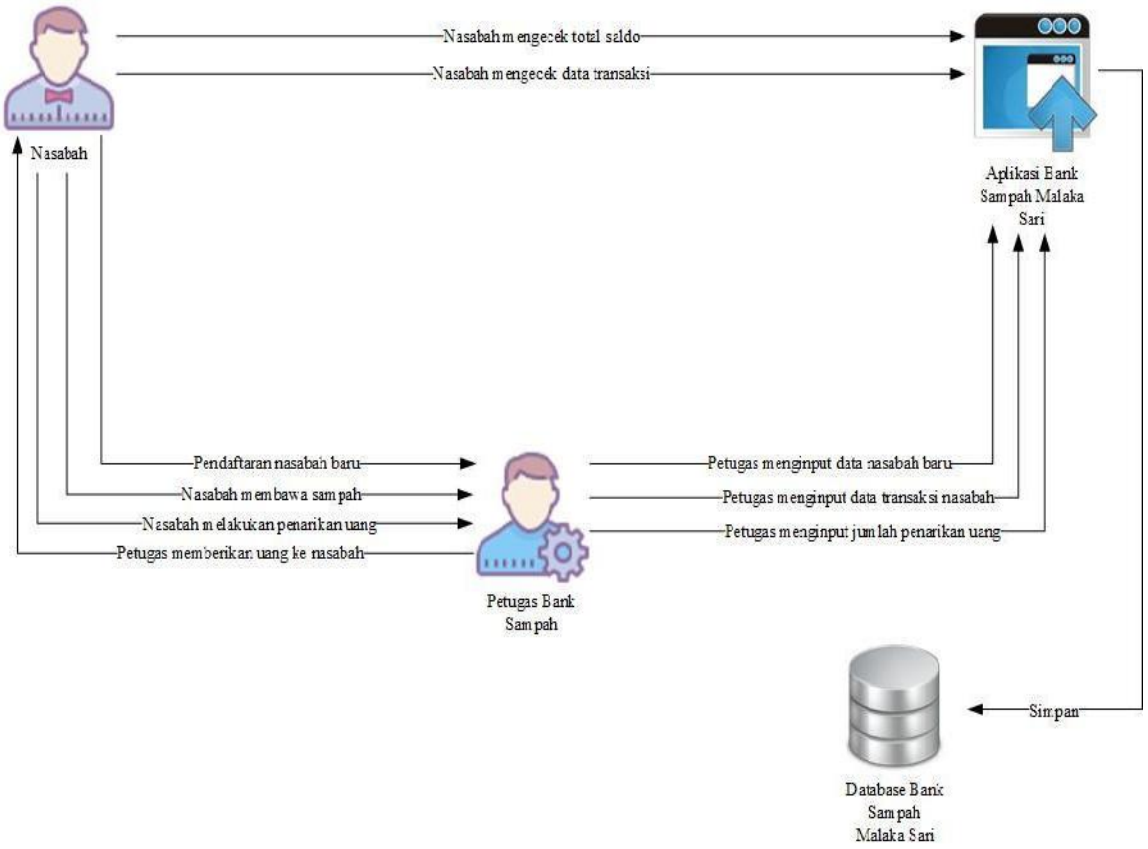
3.1 Perencanaan Syarat-Syarat

Berikut adalah sistem yang berjalan dan sistem yang diusulkan di Bank Sampah Malaka Sari.



Gambar 1. Sistem berjalan bank sampah malaka sari

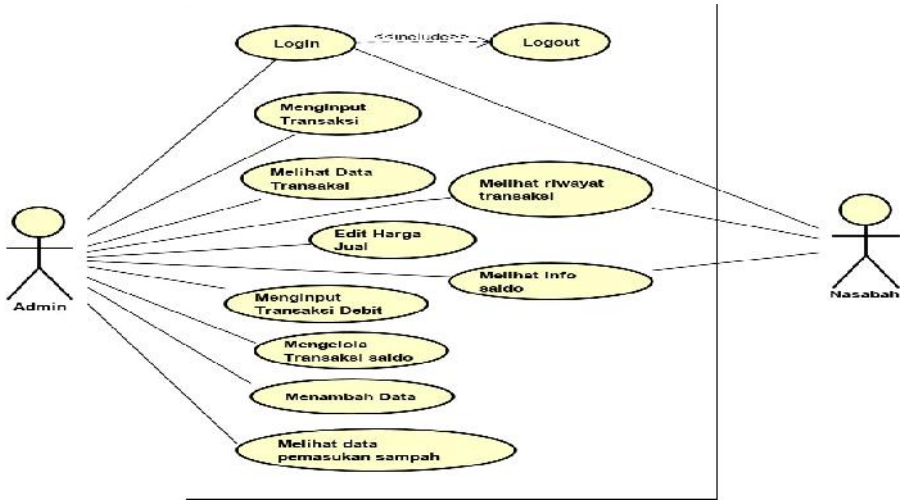
Copyright © 2020, the Authors. Published by QUERY: JURNAL SISTEM INFORMASI
This is an open access article under the CC BY license (https://creativecommons.org/licenses/by/4.0/).



Gambar 2. Sistem usulan

3.2. *Workshop* Desain RAD

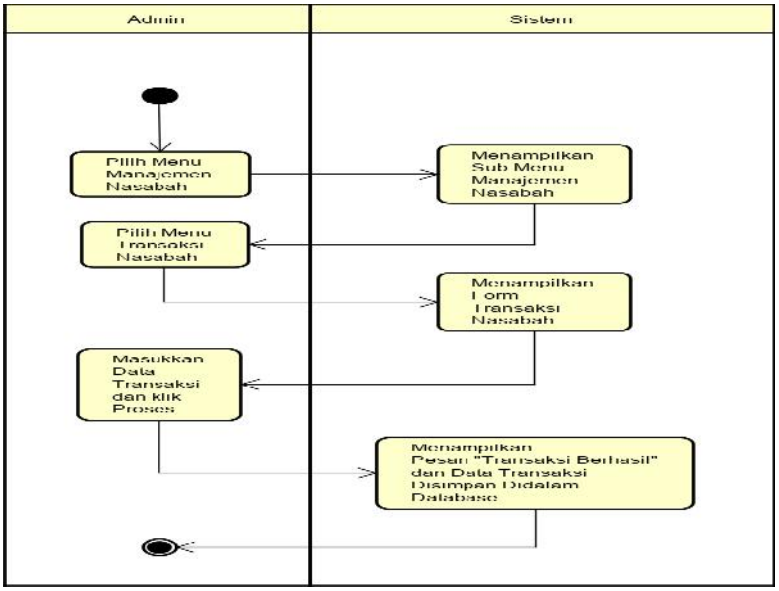
a. Untuk perancangan *input* awal pada proses *enkripsi* AES yang di implementasikan pada sistem
b. Perancangan UML
   Berikut adalah melakukan perancangan UML yang terdiri dari pembuatan :
   1. *Use case* diagram untuk menggambarkan aktor dan fungsi-fungsinya pada aplikasi bank sampah.



Gambar 3. *Use case diagram*

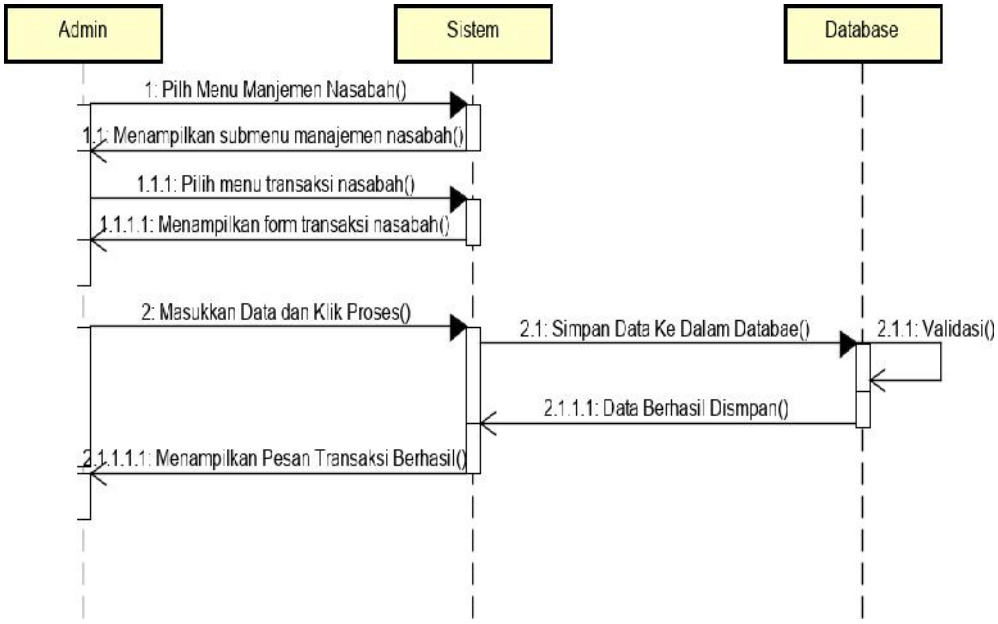
Copyright © 2020, the Authors. Published by QUERY: JURNAL SISTEM INFORMASI
This is an open access article under the CC BY license (https://creativecommons.org/licenses/by/4.0/).

2. *Activity* Diagram, setelah perancangan *use case* maka dilakukan perancangan *activity* diagram untuk menggambarkan kegiatan sistem



Gambar 4. *Activity* diagram *input* transaksi

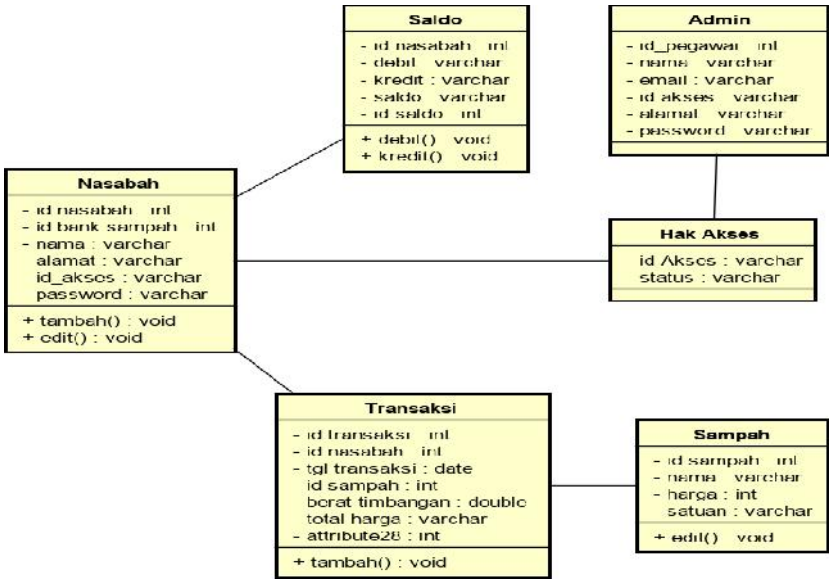
3. *Sequence* Diagram, digunakan untuk untuk menggambarkan interaksi diagram.



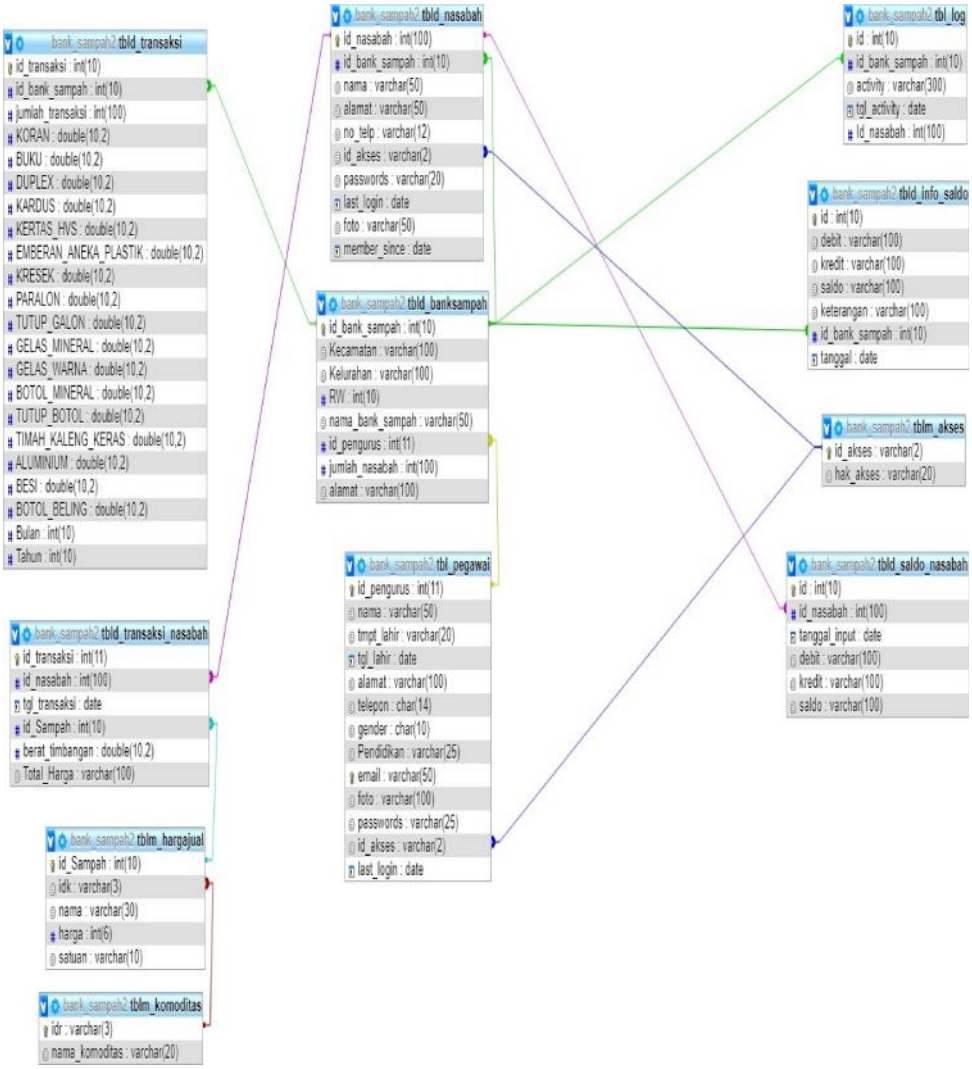
Gambar 5. *Sequence* diagram input transaksi

4. *Class* Diagram, digunakan untuk menggambarkan hubungan antar *table*, aturan, tanggung jawab entitas perilaku sistem.

Copyright © 2020, the Authors. Published by QUERY: JURNAL SISTEM INFORMASI
This is an open access article under the CC BY license (https://creativecommons.org/licenses/by/4.0/).



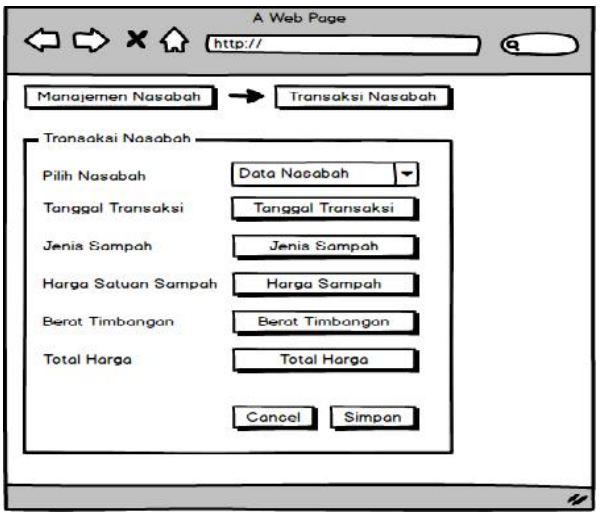
Gambar 6. *Class* diagram



Gambar 7. Skema *database*

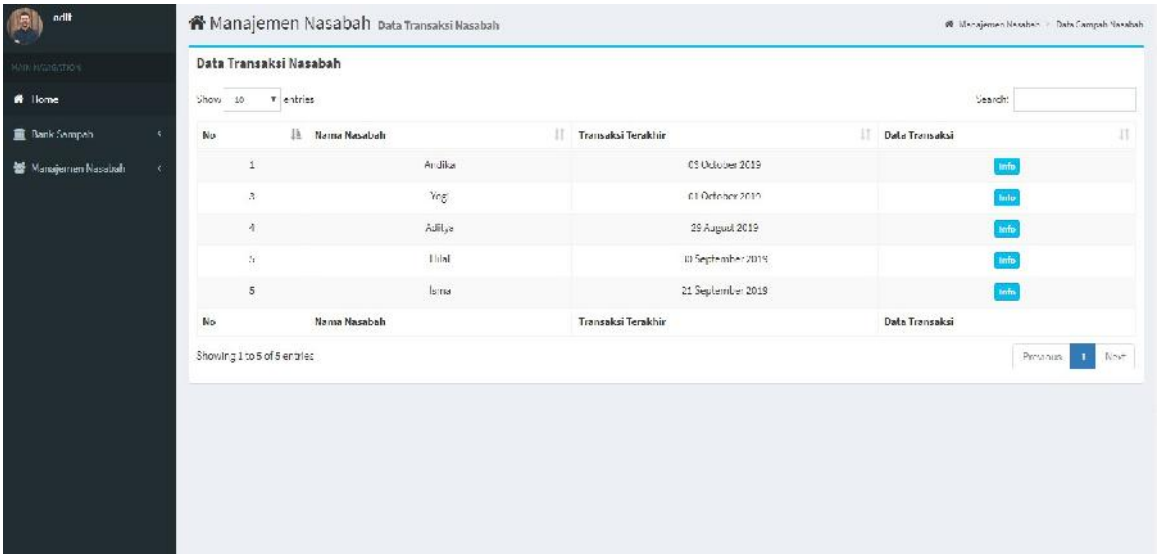
Copyright © 2020, the Authors. Published by QUERY: JURNAL SISTEM INFORMASI
This is an open access article under the CC BY license (https://creativecommons.org/licenses/by/4.0/).

c. Merancang *Database*, Gambar 7 adalah perancangan *database* sistem bank sampah.
d. Merancang *User Interface*, tampilan antarmuka pengguna dibuat untuk memudahkan dalam pembuatan yaitu dengan membuat rancangan bagi setiap pengguna sistem. Gambar 8, adalah salah satu *user interface* pada sistem, yaitu untuk transaksi nasabah.



Gambar 8. Halaman transaksi nasabah

e. Pengkodean
Untuk pemrograman dan implementasi sistem dengan menggunakan phpMyAdmin 7.1, database MySQL v.10.3.16 dan XAMPP v.3.2.4.
f. Pengujian sistem
Pengujian menggunakan *black-box testing* dengan melakukan *test-case* aplikasi, memasukkan data dan melihat *output* apakah sesuai. Berikut adalah salah satu pengujian transaksi nasabah.



Gambar 9. Hasil pengujian transaksi nasabah

Copyright © 2020, the Authors. Published by QUERY: JURNAL SISTEM INFORMASI
This is an open access article under the CC BY license (https://creativecommons.org/licenses/by/4.0/).

Options

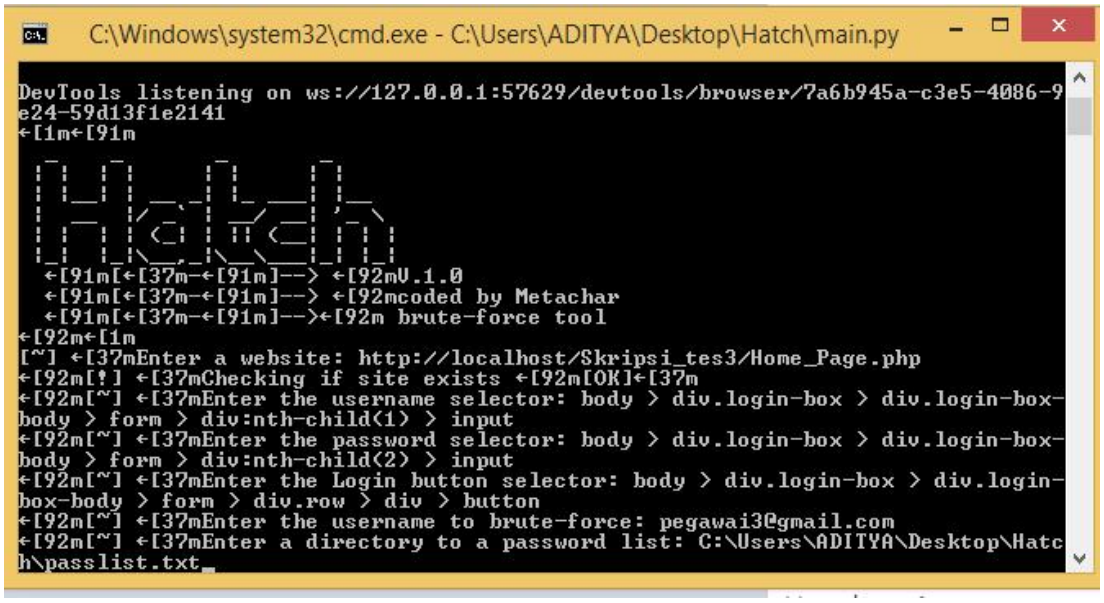
	id	id_nasabah	tanggal_input	debit	kredit	saldo
Edit Copy Delete	70	45	2019-12-07	cJkcVbSL7+2O8oOLfdCEsw==	cJkcVbSL7+2O8oOLfdCEsw==	cJkcvbSL7+2O8oOLfdCEsw==
Edit Copy Delete	71	45	2019-12-05	cJkcVbSL7+2O8oOLfdCEsw==	0tqKR+ssk8brAgYl2bkVqg==	0tcKR+ssk8brAgYl2bkVqg==
Edit Copy Delete	72	45	2019-12-07	0tqKR+ssk8brAgYl2bkVqg==	FDLOcWOGHr9zjjgPM1qPQ==	kyzIp24OeDK3Li4FyRy5pw==
Edit Copy Delete	74	45	2019-12-07	Z0Kjzod4OF7RGBXHbkp5jA==	cJkcVbSL7+2O8oOLfdCEsw==	8T5EDvCn1pcfLKjzx8YPTw==
Edit Copy Delete	75	46	2019-12-07	cJkcVbSL7+2O8oOLfdCEsw==	cJkcVbSL7+2O8oOLfdCEsw==	cJkcvbSL7+2O8oOLfdCEsw==
Edit Copy Delete	76	47	2019-12-07	cJkcVbSL7+2O8oOLfdCEsw==	cJkcVbSL7+2O8oOLfdCEsw==	cJkcvbSL7+2O8oOLfdCEsw==
Edit Copy Delete	77	48	2019-12-07	cJkcVbSL7+2O8oOLfdCEsw==	cJkcVbSL7+2O8oOLfdCEsw==	cJkcvbSL7+2O8oOLfdCEsw==
Edit Copy Delete	78	49	2019-12-07	cJkcVbSL7+2O8oOLfdCEsw==	cJkcVbSL7+2O8oOLfdCEsw==	cJkcvbSL7+2O8oOLfdCEsw==
Edit Copy Delete	79	50	2019-12-07	cJkcVbSL7+2O8oOLfdCEsw==	cJkcVbSL7+2O8oOLfdCEsw==	cJkcvbSL7+2O8oOLfdCEsw==
Edit Copy Delete	80	45	2019-12-05	cJkcVbSL7+2O8oOLfdCEsw==	0tqKR+ssk8brAgYl2bkVqg==	Z0Kjzod4OF7RGBXHbkp6jA==
Edit Copy Delete	81	46	2019-12-05	cJkcVbSL7+2O8oOLfdCEsw==	tArP3Ckt+OJb9GaXunGlNQ==	tArP3Ckt+OJb9GaXunGlWQ==

Check all With selected: Edit Copy Delete Export

Gambar 10. Hasil pengujian *database* yang sudah terenkripsi AES

g Pengujian Keamanan AES

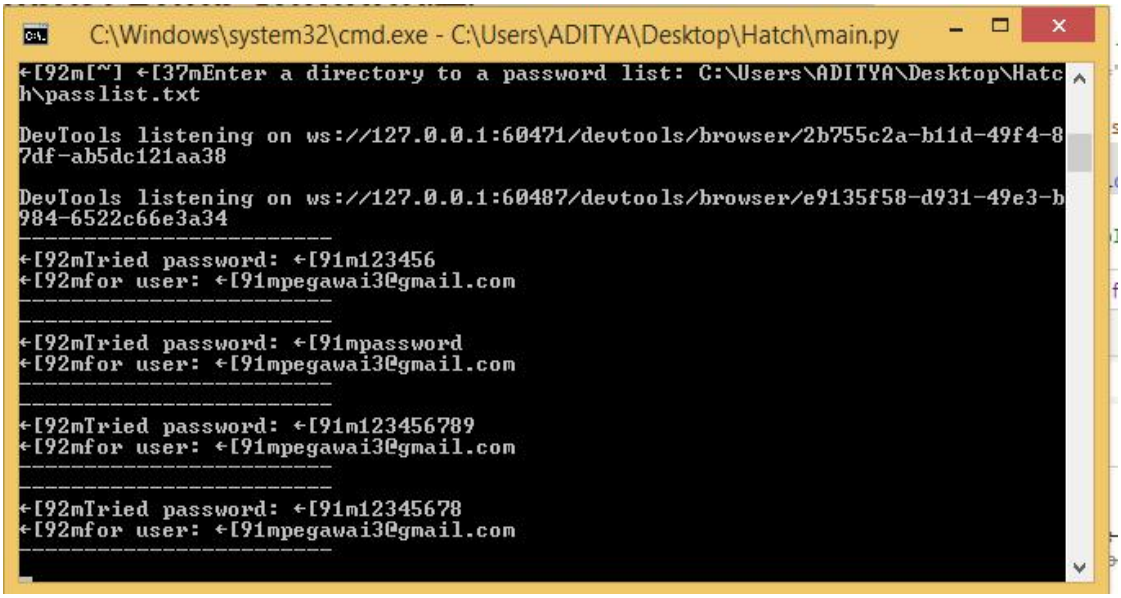
Pengujian kemanan bertujuan untuk mengetahui apakah algoritma AES berhasil di implementasikan ke dalam sistem. Pengujian keamanan dilakukan dengan teknik *brute force.*



Gambar 11. Pengujian keamanan dengan brute force

Setelah dilakukan pengujian seperti Gambar 12 adalah hasil pengujian yang menunjukkan bahwa serangan *brute force* butuh waktu yang sangat lama dan tidak dapat menembus keamanan yang sudah dienkripsi oleh AES.

Copyright © 2020, the Authors. Published by QUERY: JURNAL SISTEM INFORMASI
This is an open access article under the CC BY license (https://creativecommons.org/licenses/by/4.0/).



Gambar 12. Hasil pengujian keamanan AES dengan *brute force*

4. KESIMPULAN

Adapun kesimpulan yang didapat setelah melakukan penelitian adalah sebagai berikut :

1. Algoritma AES dinyatakan efektif dalam mengamankan data transaksi nasabah karena sulit untuk ditembus oleh serangan *brute force* dan memerlukan waktu yang sangat lama untuk menemukan kunci yang benar.
2. Proses enkripsi dan dekripsi pada algoritma AES dipengaruhi oleh panjang kunci. AES menetapkan panjang kunci adalah 128 bit, 192 bit dan 256 bit, jika semakin panjang kunci yang digunakan maka akan semakin banyak putaran yang dilalui dan semakin lama proses enkripsi dan dekripsi berlangsung
3. Aplikasi Bank Sampah Malaka Sari mampu memberikan alternatif untuk mengelola data bank sampah dengan baik karena adanya integritas data antara bank sampah dengan nasabah.

BAHAN REFERENSI

[1] Anih Sri Suryani, A. A, 2014. Peran Bank Sampah Dalam Efektivitas Pengelolaan Sampah, Aspirasi: *Jurnal Masalah-masalah Sosial*, Vol. 5, No.1, p.71-84, https://jurnal.dpr.go.id/index.php/aspirasi/article/view/447

[2] Meko, D. A. 2018, Perbandingan Algoritma DES, AES, IDEA, dan Blowfish dalam Enkripsi dan Dekripsi Data, *Jurnal Teknologi Terpadu*, Vol. 4, No. 1, Juli, p. 8-15 https://journal.nurulfikri.ac.id/index.php/jtt/article/view/110

[3] Santoso, K.I, Priyoatmoko, W, 2016, Pengamanan Data MySql Pada E-Commerce Dengan Algoritma AES 256, *Seminar Nasional Sistem Informasi Indonesia (SESINDO)*, Departemen Sistem Informasi, Institut Teknologi Sepuluh Nopember

[4] Putri, G.G, Styorini,W, Rahayani, R.D., 2018, Analisis Kriptografi Simetris AES dan Kriptografi Asimetris RSA pada Enkripsi Citra Digital, *Ethos: Jurnal Penelitian dan Pengabdian (Sains & Teknologi)*, Vol.6, No.2, https://doi.org/10.29313/ethos.v6i2.2909, https://ejournal.unisba.ac.id/index.php/ethos/article/view/2909

[5] Odiasa, I.W., 2015. Implementasi Algoritma Kriptografi Rijndael untuk Pengamanan Sistem Sms Banking dan Internet Banking, https://docplayer.info/38849995-Implementasi-algoritma-kriptografi-rijndael-untuk-pengamanan-sistem-sms-banking-dan-internet-banking-i-wayan-ordiyasa-abstraksi.html

Copyright © 2020, the Authors. Published by QUERY: JURNAL SISTEM INFORMASI
This is an open access article under the CC BY license (https://creativecommons.org/licenses/by/4.0/).

[6] Tullah, R, Dzulhaq, M.I., Setiawan, Y., 2016, Perancangan Aplikasi Kriptografi File Dengan Metode Algoritma Advanced Encryption Standard (AES), *Jurnal Sisfotek Global*, Vol.6, No.2, http://dx.doi.org/10.38101/sisfotek.v6i2.108

[7] Paramarta, D., Kusyanti, A., & Data, M. Implementasi Algoritme Advance Encryption Standard (AES) pada Enkripsi dan Dekripsi QR-Code. *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, vol. 2, no. 12, p. 6729-6736, agu. 2018. ISSN 2548-964X. Tersedia pada: <http://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/3732>

[8] Syamsinar, (2017). Implementasi Kombinasi Algoritma Asimetris Rivest Shamir Adleman Dan Algoritma Simetris Advanced Encryption Standard Pada Aplikasi Pesan Singkat, http://repositori.uin-alauddin.ac.id/3305/1/Syamsinar.pdf

[9] Nasution, Muhammad Irwan Padli, 2008, "Urgensi Keamanan Pada Sistem Informasi", Jurnal Iqra' Volume 02 Nomor 02.

[10] Fadhila Nisya Tanjung, Muhammad Irwan Padli Nasution, 2012, "Implementasi Pemrograman Java Untuk Alert Intrusion Detection System", pematang siantar, 31 agustus – 2 september 2012, ISBN 978-602-18749-0-5, https://www.researchgate.net/publication/307973619

Copyright © 2020, the Authors. Published by QUERY: JURNAL SISTEM INFORMASI
This is an open access article under the CC BY license (https://creativecommons.org/licenses/by/4.0/).