ISSN 2549-4805
Volume 7, Nomor 1, Mar - Jun 2022

IMPLMENTASI METODE KRIPTOGRAFI ADVANCED ENCRYPTION STANDARD DALAM MENGAMANKAN DATABASE PADA PT. WISATA MANDIRI TOUR

Irfan Setiawan[1], **Hidayatullah Al Islami**[2]
[1,2] Prodi Teknik Informatika, Universitas Pamulang
[1,2]Jl. Puspitek Buaran, Kec. Pamulang, Kota Tangerang Selatan, Banten, Indonesia, 15310
e-mail : [1]irfanse45@gmail.com , [2]dosen02408@unpam.ac.id

ABSTRACT

PT Wisata Mandiri Tour, which is engaged in tourism, must secure important files such as customer data and transaction data such as bookings and tickets, to make it more practical, important data. The process of sending data is not guaranteed security because it does not have any security. Data security applications are needed so that they cannot be accessed or stolen by parties who do not have access, so data protection using cryptographic techniques is needed. Cryptography is a method often used to protect a wide variety of data. One of the methods used is encryption where the information is made in such a way that it cannot be read or known by others who are unwanted. Data security is one of the very important issues in the development of technology these days. Therefore, a way is needed that can maintain confidentiality and security that refers to the protection of information from undue misuse of parties. One of the mechanisms to improve data security is to use cryptographic techniques. With cryptography, information that is considered confidential can be hidden by encoding techniques, so that it is not understood by anyone else, other than by the maker and recipient alone. There are various kinds of algorithms in cryptography including the Advance Encryption Standard (AES) Algorithm, then the author tried to propose by designing an information system using the AES-128 algorithm method using the PHP programming language and using a MySql database. The conclusion of this study 128 can make and improve data security from attacks by other parties and the system created is understandable to the user and can be run according to the specifications made..

Keyword: *Advanced Encryption Standard* (AES)-128, Database, Encryption, Decryption, Criptography, PT. Wisata Mandiri Tour.

ABSTRAK

PT. Wisata Mandiri Tour yang bergerak di bidang pariwisata, harus mengamankan berkas penting seperti data customer maupun data transaksi seperti pemesanan maupun tiket, agar lebih praktis, data penting. Proses pengiriman data tersebut tidak terjamin keamanannya karena tidak memiliki keamanan apapun. Diperlukan aplikasi pengamanan data agar tidak dapat diakses atau dicuri oleh pihak yang tidak memiliki akses, maka diperlukan perlindungan data dengan menggunakan teknik kriptografi. Kriptografi adalah suatu metode yang sering kali digunakan untuk melindungi berbagai macam data. Salah satu metode yang digunakan adalah enkripsi dimana informasi yang ada dibuat sedemikian rupa agar tidak dapat dibaca atau diketahui oleh orang lain yang tidak diinginkan. Keamanan data adalah salah satu masalah yang sangat penting pada perkembangan teknologi akhir-akhir ini. Oleh karena itu dibutuhkan cara yang dapat menjaga kerahasiaan dan keamanan yang merujuk pada perlindungan informasi dari

ISSN 2549-4805
Volume 7, Nomor 1, Mar - Jun 2022

penyalahgunaan pihak yang tidak semestinya. Salah satu mekanisme untuk meningkatkan keamanan data adalah dengan menggunakan teknik kriptografi. Dengan kriptografi, informasi yang dianggap rahasia dapat disembunyikan dengan teknik penyandian, sehingga tidak dimengerti oleh orang lain, selain oleh pembuat dan penerimanya saja. Ada berbagai macam algoritma dalam kriptografi diantaranya adalah Algoritma Advance Encryption Standard (AES), maka penulis mencoba mengusulkan dengan merancang sebuah sistem informasi menggunakan metode algoritme AES-128 menggunakan bahasa pemrograman PHP dan menggunakan database MySql. Kesimpulan dari penelitian ini 128 dapat membuat dan meningkatkan keamanan data dari serangan pihak lain dan sistem yang dibuat dapat dimengerti oleh pengguna serta dapat dijalankan sesuai dengan spesifikasi yang dibuat.

Kata Kunci: *Advanced Encryption Standard* (AES)-128, Database, Enkripsi, Dekripsi, Kriptografi, PT. Wisata Mandiri Tour.

1. Pendahuluan

Masalah keamanan dan kerahasiaan merupakan salah satu aspek penting dari data atau informasi. Kebenaran dan keaslian sangat penting pada saat suatu informasi atau data dikirim maupun diterima. Informasi atau data dapat disalahgunakan apabila pada saat pengiriman disadap atau dibajak oleh orang yang tidak berhak atau berkepentingan.

PT Wisata Mandiri Tour yang bergerak di bidang pariwisata, harus mengamankan berkas penting seperti data *customer* maupun data transaksi seperti pemesanan maupun tiket, agar lebih praktis, data penting. Proses pengiriman data tersebut tidak terjamin keamanannya karena tidak memiliki keamanan apapun. Diperlukan aplikasi pengamanan data agar tidak dapat diakses atau dicuri oleh pihak yang tidak memiliki akses, maka diperlukan perlindungan data dengan menggunakan teknik kriptografi. Kriptografi adalah suatu metode yang sering kali digunakan untuk melindungi berbagai macam data. Salah satu metode yang digunakan adalah enkripsi dimana informasi yang ada dibuat sedemikian rupa agar tidak dapat dibaca atau diketahui oleh orang lain yang tidak diinginkan. Keamanan data adalah salah satu masalah yang sangat penting pada perkembangan teknologi akhir-akhir ini.

Pengamanan informasi dapat dilakukan dengan menggunakan teknik enkripsi terhadap informasi atau data sehingga sulit untuk dibaca atau diterjemahkan yang biasa disebut sebagai kriptografi. Kriptografi memiliki tujuan agar pesan atau informasi yang dikirim diubah menjadi huruf yang tidak dapat dibaca atau diterjemahkan oleh pihak yang tidak memiliki hak akses. Untuk menjamin keamanan data yang dikirimkan adalah dengan penerapan teknik kriptografi dengan mengenkripsi isi dari file yang akan dikirimkan menggunakan algoritma yaitu kunci simetri AES (*Advanced Enrcyption Standard*)-128. Algoritma AES termasuk dalam jenis algoritma Kriptografi yang sifatnya simetri dan cipher block. Demikian algoritma ini mempergunakan kunci yang sama saat enkripsi dan dekripsi serta masukan dan keluarannya berupa blok dengan jumlah bit tertentu.

Oleh karena itu dibutuhkan cara yang dapat menjaga kerahasiaan dan keamanan yang merujuk pada perlindungan informasi dari penyalahgunaan pihak yang tidak semestinya. Dari uraian di atas maka penulis melakukan penelitian terhadap hal-hal tersebut yang akan dituangkan dalam tulisan berjudul "Implementasi Metode Kriptografi *Advanced Enrcyption Standard-128* Dalam Mengamankan Database Pada PT. Wisata Mandiri Tour"**.**

2. Metodologi Penelitian dan Landasan Teori

2.1 Metode Penelitian

Metode penelitian untuk memperoleh hasil yang lebih spesifik, menggunakan proses sebagai berikut :

1. Penelitian yang diambil dari jurnal

ISSN 2549-4805
Volume 7, Nomor 1, Mar - Jun 2022

Mencari beberapa sitasi untuk penelitian, mencari kumpulan jurnal mengenai kriptografi dan metode algoritma AES-128.

2. Menentukan metode kriptografi
   Enkripsi dan dekripsi masing-masing mempunyai dua metode algoritma yang sama.
3. Menentukan bahasa pemrograman
   Menggunakan bahasa PHP, program yang dibuat dapat diakses secara *localhost*.
4. Perancangan program
   Program yang digunakan berbasi *web,* keamanan data enkripsi dan dekripsi menggunakan metode algoritme AES-128, database menggunakan MySQL.
5. Kebutuhan program
   Program yang akan dijalankan menggunakan *web browser*.
6. Pengujian
   Pengujian program menggunakan sistem *black box* dan *white box*.

2.2 Landasan Teori

2.2.1 Sistem

Menurut Mulyani (2016:2) sistem adalah kumpulan dari dua atau lebih komponen yang saling bekerja dan berhubungan untuk mencapai tujuan tertentu. Dia juga berpendapat bahwa perusahaan adalah sebuah sistem yang terdiri dari beberapa departemen yang bertindak sebagai subsistem yang membentuk sistem perusahaan tersebut.

2.2.2 Perancangan Sistem

Menurut Satzinger, Jackson dan Burd (2012 : 5) perancangan sistem adalah sekumpulan aktivitas yang menggambarkan secara rinci bagaimana sistem akan berjalan. Hal itu bertujuan untuk menghasilkan produk perangkat lunak yang sesuai dengan kebutuhan *user*.

2.2.3 Kriptografi

Secara umum, kriptografi merupakan tekniik pengamanan informasi yang dilakukan dengan cara mengolah informasi awal (*plaintext*) dengan suatu kunci (*key*) tertentu menggunakan suatu metode enktiipsi tertentu sehingga menghasilkan suatu informasi baru (*ciphertext*) yang tidak dapat dibaca secara langsung (Sadikin, 2012).

Ada 4 (empat) tujuan mendasar dari ilmu kriptografi ini yang juga merupakan aspek-aspek keamanan di dalam kriptografi adalah (Ariyus, 2008):

a. *Convidentiality* (Kerahasiaan)
   Layanan yang ditujukan untuk menjaga agar pesan tidak dapat dibaca oleh pihak-pihak yang tidak berhak.
b. *Data Integrity* (Integritas)
   Layanan yang menjamin bahwa pesan masih asli / utuh atau belum pernah dimanipulasi selama pengiriman. Dengan kata lain, aspek keamanan ini dapat diungkapkan sebagai pertanyaan : “Apakah pesan yang diterima masih asli atau tidak mengalami perubahan (modifikasi)?”.
c. *Authentication* (Otentikasi)
   Layanan yang berhubungan dengan identifikasi, baik mengidentifikasi kebenaran pihak-pihak yang berkomunikasi (*user authentication* atau *entity authentication*) maupun mengidentifikasi kebenarasumber pesan (*origin authentication).*
d. *Non Repudiation* (Nirpenyangkalan)

ISSN 2549-4805
Volume 7, Nomor 1, Mar - Jun 2022

Layanan untuk mencegah entitas yang berkomunikasi melakukan penyangkalan, yaitu pengiriman pesan menyangkal melakukan pengiriman atau penerima pesan menyangkal telah menerima pesan.

2.2.4 Algoritma AES (*Advanced Encryption Standard*)

Algoritma AES termasuk dalam jenis algoritma Kriptografi yang sifatnya simetri dan cipher block. Demikian algoritma ini mempergunakan kunci yang sama saat enkripsi dan dekripsi serta masukan dan keluarannya berupa blok dengan jumlah bit tertentu. Algoritma AES mendukung berbagai variasi ukuran blok dan kunci yang akan digunakan. Namun AES mempunyai ukuran blok dan kunci yang tetap sebesar 128, 192, 256 bit. Panjang kunci dari AES terdiri dari panjang kunci 128 bit, 192 bit, dan 256 bit (Rahmawati & Rahardjo, 2016).

2.2.5 *Unified Modelling Language* (UML)

Unified Modeling Language (UML) spesifikasi bahasa standar, serta diperuntukan dalam mendokumentasikan, membangun, dan menspesifikasikan sebuah perangkat lunak. UML juga merupakan suatu metodologi dalam pengembangan sistem berorientasi objek serta merupakan suatu alat untuk mendukung pengembangan pada suatu sistem (Hendini, 2016).

2.2.6 MySQL

MySQL sebagai software database server dan bersifat *Open Source* yang menyatakan *software* ini dilengkapi dengan source code (kode yang dipakai untuk membuat MySQL, tentu saja bentuk *executable*-nya atau kode yang dapat dijalankan secara langsung dalam sistem operasi, dan bisa didapat dengan mengunduhnya gratis dari Internet. Perihal menarik lainnya yaitu MySQL juga bersifat multiplatform, artinya MySQL dapat dijalankan pada banyak sistem operasi yang ada (Amin, 2017).

3. Hasil Dan Pembahasan

3.1. Analisa Sistem Berjalan

Proses kegiatan yang berjalan saat proses transaksi di PT. Wisata Mandiri Tour sebagai berikut:

1) Proses Pemesanan

customer datang ke tempat dan memesan kebutuhan keberangkatan kepada bagian administrasi, lalu bagian administrasi melakukan ketersediaan jadwal keberangkatan. Jika tidak tersedia, bagian administrasi akan konfirmasi kepada *customer*. Bila tersedia, bagian administrasi akan informasikan biaya dan memberikan formulir yang diisi oleh *customer*, setelah itu *customer* melakukan pembayaran, kemudian bagian administrasi mencatatnya kedalam kwitansi yang akan diberikan kepada *customer*.

2) Proses Cetak Tiket

Pada proses ini bagian administrasi akan membuat tiket tentang informasi *customer* yang akan berangkat untuk diberikan kepada *customer* sebagai bukti dan membuat surat perjalanan kerja yang akan diserahkan kepada supir kendaraan.

3) Proses Pembuatan Laporan

Setiap bulannya bagian administrasi akan membuat laporan dari pemesanan. Setelah itu bagian administrasi akan menyerahkan laporan tersebut ke pemilik perusahaan.

3.2. Analisa Sistem Usulan

ISSN 2549-4805
Volume 7, Nomor 1, Mar - Jun 2022

Prosedur sistem usulan bertujuan untuk menjelaskan tahap-tahap yang akan dibuat ketika sistem sudah dibuatkan di PT. Wisata Mandiri Tour sebagai berikut:

1) Proses Pemesanan

customer datang ke tempat dan memesan kebutuhan keberangkatan kepada bagian administrasi, lalu bagian administrasi melakukan ketersediaan jadwal keberangkatan pada sistem. Jika tidak tersedia, bagian administrasi akan konfirmasi kepada *customer*. Bila tersedia, bagian administrasi akan mengentri data *customer*, pemesanan pada sistem dan informasikan biaya, setelah itu *customer* melakukan pembayaran, kemudian bagian administrasi mencetak kwitansi pada sistem yang akan diberikan kepada *customer*.

2) Proses Cetak Tiket

Pada proses ini bagian administrasi akan mencetak tiket pada sistem mengenai informasi *customer* yang akan berangkat untuk diberikan kepada *customer* sebagai bukti dan mencetak surat perjalanan kerja pada sistem yang akan diserahkan kepada supir kendaraan.

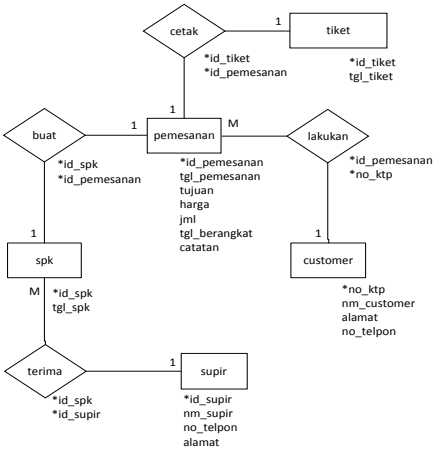
3) Proses Pembuatan Laporan

Setiap bulannya bagian administrasi akan mencetak laporan pada sistem dari total pemesanan. Setelah itu bagian administrasi akan menyerahkan laporan tersebut ke pemilik perusahaan.

3.3. Perancangan Desain

3.3.1. ERD

Model ini dirancang untuk keperluan pengembangan Sistem Penunjang Keputusan. Sebuah rancangan model data disajikan dalam bentuk *Entity Relationship Diagram* (ERD):

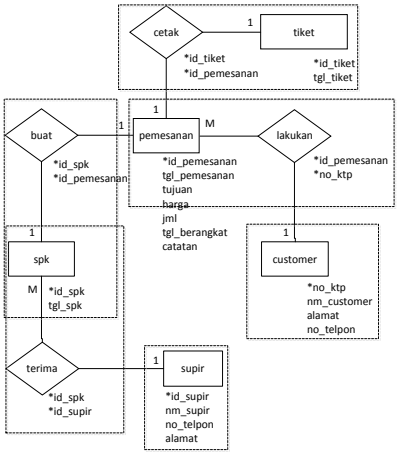


Gambar 1 : ERD

3.3.2. Transformasi ERD ke LRS

Transformasi diagram hubungan entitas ke dalam Logical Record Structure (LRS) merupakan kegiatan untuk membentuk data-data di ERD ke dalam LRS. Pada sebuah ERD nama field di tulis di luar kotak (di luar entity), sedangkan pada sebuah LRS setiap field ditulis di dalam kotak dan memiliki sebuah nama yang unik, pemodelannya seperti berikut:

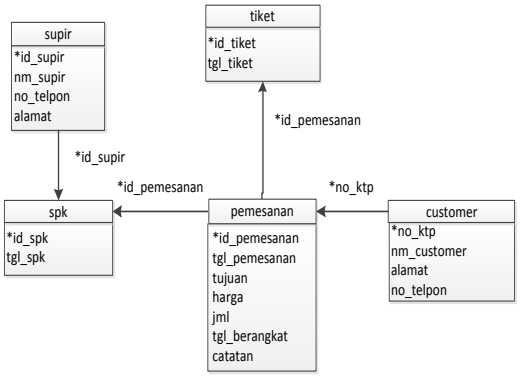
ISSN 2549-4805
Volume 7, Nomor 1, Mar - Jun 2022



Gambar 2 : Transformasi ERD ke LRS

3.3.3. LRS

Berikut ini adalah LRS yang terbentuk berdasarkan hasil transformasi ERD ke LRS:

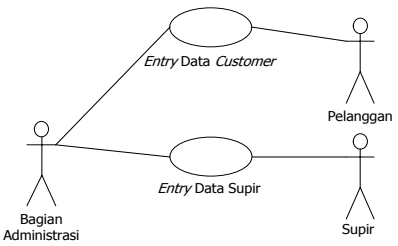


Gambar 3 : LRS

3.3.4. Use Case Diagram

Berikut ini desain diagram *use case* sistem informasi yang akan dirancang pada gambar 4 - 6. *Use case* menjelaskan bahwa aplikasi ini memiliki satu aktor aktif yaitu admin. Aktor admin dapat menggunakan seluruh fitur yang ada, seperti entri data *customer*, supir, pemesanan, cetak tiket, cetak spk dan pembuatan laporan seperti laporan pemesanan dan laporan spk.

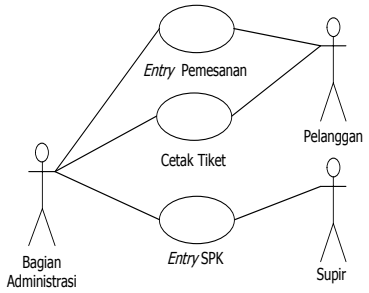
1) *Use Case Diagram* Master



Gambar 4 : Use Case Diagram Master

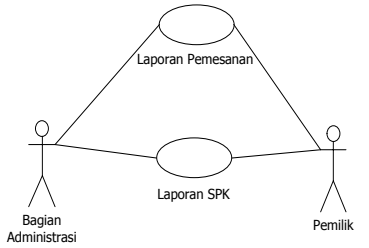
ISSN 2549-4805
Volume 7, Nomor 1, Mar - Jun 2022

2) *Use Case Diagram* Transaksi



Gambar 5 : *Use Case* Diagram Transaksi

3) *Use Case Diagram* Laporan



Gambar 6 : Use Case Diagram Laporan

3.4. Pengembangan Aplikasi

3.4.1. Lingkungan Perangkata Lunak

Dalam merancang suatu aplikasi, tentu dibutuhkan *tools* dan perangkat lunak guna membantu dalam pembuatan aplikasi. Berikut adalah *tools* dan *software* yang digunakan penulisan dalam perancangan aplikasi:

1) *Visual Studio Code*
   Penulis menggunakan aplikasi ini sebagai teks editor untuk membuat aplikasi.
2) PHP
   Penulis menggunakan PHP sebagai Bahasa pemrograman dalam merancang aplikasi.
3) MySQL
   Penulis menggunakan media penyimpanan data pada aplikasi yang akan dibuat. MySQL adalah sebuah DBMS (*Database Management System*) yang menggunakan perintah SQL (*Structured Query Language*).
4) Balsamic Mockup
   Penulis menggunakan tampilan rancangan layar aplikasi menggunakan Balsamic Mockup.

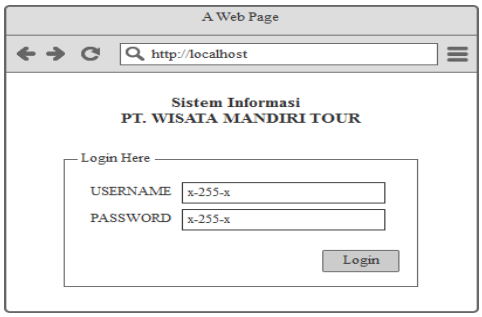
3.4.2. Implementasi *User Interface*

User interface merupakan tampilan aplikasi yang akan dibuat untuk memudahkan penggunakan berinteraksi dengan aplikasi.

1) *User Interface Login*

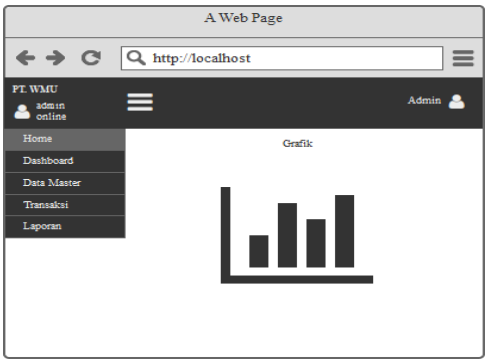
ISSN 2549-4805
Volume 7, Nomor 1, Mar - Jun 2022

Rancangan tersebut adalah ketika bagian administrasi ingin mengakses sistem dengan menginput username dan password kemudian menekan tombol login.



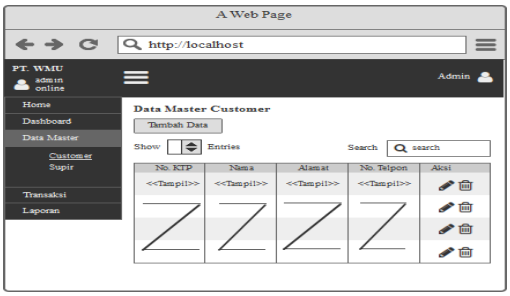
Gambar 7 : User Interface Login

2) *User Interface Dashboard*
Rancangan tersebut adalah informasi dashboard yang dapat user lihat, dashboard terdiri dari grafik pemesanan.



Gambar 8 : User Interface Dashboard

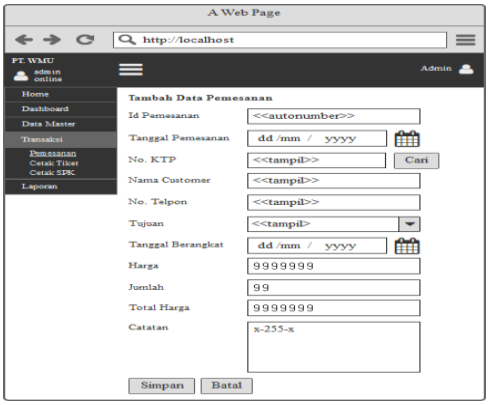
3) *User Interface* Data *Customer*
Rancangan tersebut adalah tampilan hasil data customer yang sudah disimpan. Terdapat informasi berupa no. ktp, nama, alamat, dan no.telpon.



Gambar 9 : User Interface Data *Customer*

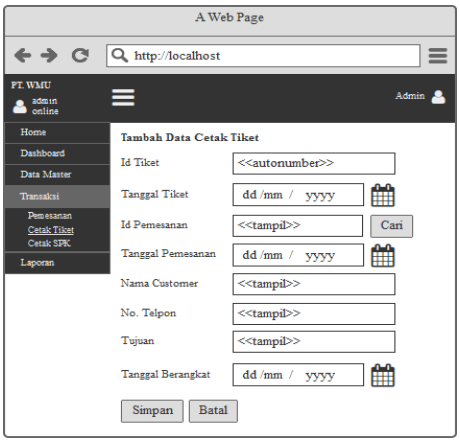
4) *User Interface* Entri Pemesanan
Rancangan emtri pemesanan adalah form input untuk menyimpan data pemesanan oleh user. *Autonumber* ditampilkan otomatis, lalu user mengklik cari data *customer*, lalu menginput data pemesanan. Kemudian mengklik tombol simpan untuk menyimpan data pemesanan.

ISSN 2549-4805
Volume 7, Nomor 1, Mar - Jun 2022



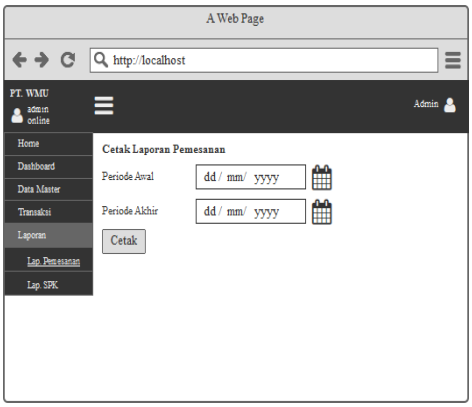
Gambar 10 : User Interface Entri Pemesanan

5) *User Interface* Cetak Tiket
Rancangan cetak tiket adalah form input untuk menyimpan data tiket oleh user. *Autonumber* ditampilkan otomatis, lalu user mengklik cari data pemesanan. Kemudian mengklik tombol simpan untuk menyimpan dan mencetak data tiket.



Gambar 11 : User Interface Cetak Tiket

6) *User Interface* Laporan Pemesanan
Rancangan tersebut adalah form cetak laporan pemesanan. User memilih periode awal dan periode akhir untuk menampilkan laporan pemesanan, kemudian klik tombol cetak untuk menampilkan laporan pemesanan berdasarkan periode yang sudah dipilih.



Gambar 12 : User Interface Laporan Pemesanan

ISSN 2549-4805
Volume 7, Nomor 1, Mar - Jun 2022

3.5. Pengujian Aplikasi

Metode pengujian dilakukan untuk memastikan apakah sistem yang akan digunakan sudah berjalan dengan lancer tanpa kendala sehingga sesuai dengan kebutuhan pengguna, Metode yang digunakan untuk pengujian ini adalah *black box testing*, yaitu pengujian yang berfokus pada fungsi dari perangkat lunak, percobaan ini dilakukan dengan menguji dari proses input dan melakukan pengetesan pada spesifikasi fungsional program yang dibuat.

1) Pengujian Halaman *Login*

Data *Input*	**Pengujian**	**Hasil Akhir**
Mengisi *Username* dan *Password*	Jika data hasil *input* lolos validasi oleh sistem, maka *user* akan masuk ke menu *Dashboard*	Diterima

2) Pengujian Halaman Supir

Data *Input*	**Pengujian**	**Hasil Akhir**
User memilih menu data master supir	*User* akan dialihkan ke halaman data master supir	Diterima
User menginput data yang terdapat pada *form* tambah supir	Jika data hasil *input* benar dan lolos validasi oleh sistem akan memproses data hasil *input* tersebut kemudian akan dienkripsikan dan disimpan	Diterima

ISSN 2549-4805
Volume 7, Nomor 1, Mar - Jun 2022

	dalam *database*.	

3) Pengujian Halaman *Customer*

Data *Input*	**Pengujian**	**Hasil Akhir**
User memilih menu data master *customer*	*User* akan dialihkan ke halaman data master *customer*	Diterima
User menginput data yang terdapat pada *form* tambah *customer*	Jika data hasil *input* benar dan lolos validasi oleh sistem akan memproses data hasil *input* tersebut kemudian akan dienkripsikan dan disimpan dalam *database*.	Diterima

4) Pengujian Halaman Pemesanan

Data *Input*	**Pengujian**	**Hasil Akhir**
User memilih menu data transaksi pemesanan	*User* akan dialihkan ke halaman data transaksi pemesanan	Diterima
User memilih data *customer* lalu	Jika data hasil *input* benar dan lolos validasi	Diterima

ISSN 2549-4805
Volume 7, Nomor 1, Mar - Jun 2022

menginput data yang terdapat pada *form* tambah pemesanan	oleh sistem akan memproses data hasil *input* tersebut kemudian akan dienkripsikan dan disimpan dalam *database*.	

5) Pengujian Halaman Cetak Tiket

Data *Input*	**Pengujian**	**Hasil Akhir**
User memilih menu data transaksi cetak tiket	*User* akan dialihkan ke halaman data transaksi cetak tiket	Diterima
User memilih data pemesanan lalu mencetak data yang terdapat pada *form* tambah cetak tiket	Jika data hasil *input* benar dan lolos validasi oleh sistem akan memproses data hasil *input* tersebut kemudian akan dienkripsikan dan disimpan dalam *database* serta akan mencetak otomatis	Diterima

ISSN 2549-4805
Volume 7, Nomor 1, Mar - Jun 2022

	berdasarkan sistem.	

4. Simpulan

Kesimpulan yang didapat dari proses analisis, perancangan dan analisa sistem adalah:

a. Dengan adanya sistem informasi enkripsi – dekripsi data menggunakan algoritme AES-128 dapat membuat dan meningkatkan keamanan data dari serangan pihak lain.
b. Sistem informasi yang telah di implementasikan dapat dimengerti oleh pengguna dan dapat dijalankan sesuai dengan spesifikasi yang telah dibuat.
c. Enkripsi Algoritma AES-128 dapat diimplementasikan pada sistem informasi pengamanan *database* dengan menggunakan bahasa PHP dan *database* MySQ.

References

Ade Hendini. (2016). Pemodelan UML Sistem Informasi Monitorig Penjualan dan Stok Barang (Studi Kasus: Dostro Zhezha Pontianak). Jurnal Khatulistiwa, Vol. 4 No. 2

Amin, R. (2017) 'Rancang Bangun Sistem Informasi Penerimaan Siswa Baru pada SMK Budhi Warman 1 Jakarta', Jurnal Ilmu Pengetahuan dan Teknologi Komputer, 2(2), pp. 113–121.

Ariyus, Donny 2008, *Pengantar Ilmu Kriptografi Teori, Analisis, dan Implementasi*, Yogyakarta: C.V Andi OFFSET.

Mulyani, Sri. 2016. Sistem Informasi Manajemen. Bandung: Abdi Sistematika.

Rahmawati R., Rahardjo D. (2016) "Aplikasi Pengamanan Data Menggunakan Algoritma Steganografi *Discrete Cosine Transform* dan Kriptografi AES 128 BIT pada SMK PGRI 15 Jakarta." Jurnal Teknik Informatika dan Sistem Informasi, 2(1), hal 67-73.

Sadikin, 2012, Kriptografi Untuk Keamanan Jaringan, Yogyakarta, Andi.