APLIKASI ENKRIPSI DATA PENILAIAN SISWA PADA DATABASE MENGGUNAKAN ALGORITMA KRIPTOGRAFI (AES-128) BERBASIS WEB

Faldi Rachmat Nopianto[1], **Ferdiansyah**[2]
[1]Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
[1,2]Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
E-mail : faldirachmat@gmail.com[1)], ferdiansyah@budiluhur.ac.id[2)]

Abstrak

Dalam meningkatkan suatu pendidikan yang bermutu membutuhkan upaya yang terus menerus untuk selalu meningkatkan kualitas pendidikan akademik. Permasalahan yang diperoleh saat ini para staff guru SMK Media Informatika, menulis suatu data akademik yaitu yang berisi data nilai dan lainya masih menggunakan buku. Dalam kegiatan guru saat ini memindahkan data nilai dan lainnya hasil yang diperoleh pada saat proses ajar siswa dan siswi masih ditulis manual pada sebuah buku khusus leger nilai atau buku besar umum, lalu untuk penyimpananya masih ditempat tertentu saja dan sangat terbatas. Hal ini tentunya banyak peluang bagi orang-orang yang tidak berkempentingan atau orang lain yang tidak dikenal dengan memanipulasi data akademik dan mengambil data informasi akademik dengan secara tidak ketahui oleh pemiliknya ataupun bahkan buku nilai dan lainya yang berisi data informasi akademik tersebut terselip lalu hilang. Dengan demikian hal ini sangat merugikan oleh pihak SMK Media Informatika. Karena begitu pentingnya sebuah data informasi akademik maka dibuatlah suatu aplikasi pengamanan database yang dimana sangat berguna selain itu dapat mengamankan data yang dimiliki. Dengan menerapkan algortima Kriptografi Advanced Encryption Standard (AES) 128. Tujuannya untuk mempermudah pada proses penyimpanan atau mengamankan data agar tidak bisa sadap ataupun diketahui oleh orang yang tidak berkempentingan. Dengan merancang suatu aplikasi pengamanan database dengan teknik tersebut yang berbasis Web, dimana data tersebut akan dienkripsi dengan menggunakan metode kriptografi. Data yang telah dienkripsi hanya bisa dibuka kembali oleh pemilik program ini seperti, guru (tata usaha) dari SMK Media Informatika.

Kata kunci: Kriptografi, AES 128, Keamanan Database

1. PENDAHULUAN

Dalam kemajuan teknologi yang sangat cepat dan akurat telah mengalami kemajuan setiap informasi akademik untuk terus berusaha mengikuti perkembangan dengan meningkatkan teknologi dan kemampuannya dalam mengelola suatu data-data dan informasi yang aman dan efisien karena sangat dibutuhkan oleh suatu informasi akademik. Penulisan sebuah informasi saat ini juga tidak lepas dari teknologi-teknologi kecanggihan saat ini. Hal ini masih banyak dari pihak intansi yang belum menggunakan atau mengelola teknologi secara maksimal, yang dimana teknologi ini sangat berguna untuk memudahkan sebuah informasi akademik, juga memudahkan kinerja operasional dari pihak guru SMK Media informatika.

Dalam hal ini permasalahan yang terjadi pada SMK Media Informatika yaitu, Pada proses ini siswa dan siswi mempunyai data yang dimana masing-masing data tersebut berbeda. Hal ini guru bertugas untuk mengelola atau mencatat dibuku khusus atau buku leger nilai, sesuai dengan data akademik. Data tersebut yang dimana berisi informasi akademik hasil proses kegiatan ajar, yang nati akan disimpan dikomputer ataupun bahkan disimpan pada tempat-tempat yang tertuntu saja agar isi dari buku tersebut tidak bisa ketehui atau dirubah oleh orang lain. Tentu saja hal ini kesempatan peluang bagi orang-orang yang tidak berhak misalnya dari pihak luar disadap untuk mengambil atau mengubah informasi pemilik data secara tidak diketahui ataupun disebabkan karena data-data yang berantakan akan terselip lalu hilang. Tentunya hal ini sangat merugikan bagi pihak SMK Media Informatika. Dampaknya pada pendataan boidata atau nilai siswa dan siswi saat kenaikan kelas untuk penyampaian informasi atau data tersebut menjadi kurang tepat dan kurang efektif.

Oleh karena itu masalah yang dihadapi untuk keamanan suatu data merupakan aspek yang sangat penting. pendataan baik biodata siswa dan siswi atau data nilai. Hal ini data-data tersebut seperti data biodata atau penilaian siswa-siswi yang sangat bersifat penting, karena data tersebut begitu rentan dan bersifat penting maka harus diberikan keamanan yang sangat baik, yang dimana agar tidak bisa di mengerti mengenai data tersebut oleh orang yang tidak bertanggung jawab.

Dari uraian permasalahan yang dihadapai oleh SMK Media Informatika. penulis membuat Aplikasi *Database* dengan menggunakan Algoritma Kriptografi *Advanced Encryption Standard* (AES-128) berbasis *Web* untuk mengamankan isi data berisikan informasi akademik didalam *database* yang penting. Dengan demikian aplikasi pengamanan database tersebut memiliki keamanan ganda pada *username, password* dan data yang terenkripsi. Salah

satu cara yang digunakan untuk menjamin keamanan data informasi akademik Enkripsi dilakukan pada saat penyimpanan didalam database. berbagai macam cara mengubah data-data asli yang akan menghasilkan data-data yang bersifat rahasia, sedangkan dekripsi dilakukan pada saat dengan mengubah data rahasia menjadi data asli. Data asli hanya bisa dilihat oleh *user* dengan menggunakan kunci rahasia.

2. ANALISA MASALAH DAN PERANCANGAN PROGRAM

2.1 Masalah

Pendataan informasi akademik berupa data nilai informasi akademik yang masih manual berupa tulisan yang dicatat dibuku besar atau leger nilai dan hanya disimpan pada tempat tertentu saja pada SMK Media Informatika hal ini masih kurang optimal. Pada proses ini dikarenakan kurangnya pengamanan dari sebuah data yang ada dibuku tersebut. Akibatnya bisa saja buku besar atau leger nilai tersebut akan hilang atau bisa diambil ataupun dirubah secara tidak sengaja diketahui oleh pemilik data tersebut. Dengan begitu pada saat data informasi akademik dibutuhkan, pada saat proses penyampaian atau pendataan informasi akademik menjadi kurang tepat atau kurang *flexsibel.*

Dengan adanya permasalahan ini maka penulis menarik kesimpulan yaitu membuat sebuah wadah untuk penyimpanan data informasi akademik tersebut, karena untuk antisipasi terjadinya pencurian data atau pengubahan data. Penyimpanan ini dapat bisa digunakan oleh guru SMK Media Informatika secara baik, yang nantinya saat data yang dibutuhkan tersimpan di dalam *database* yang nanti juga dapat diakses oleh *admin* yaitu guru (tata usaha) yang dikatagorikan juga sebagai admin atau pengelola data informasi akademik. Dengan demikian diharapkan data tersebut menjadi aman dengan data yang terenkripsi. Jika data tersebut ingin kembali seperti data semula maka hanya admin yaitu guru yang tahu dan dapat membukanya kembali data tersebut seperti semula.

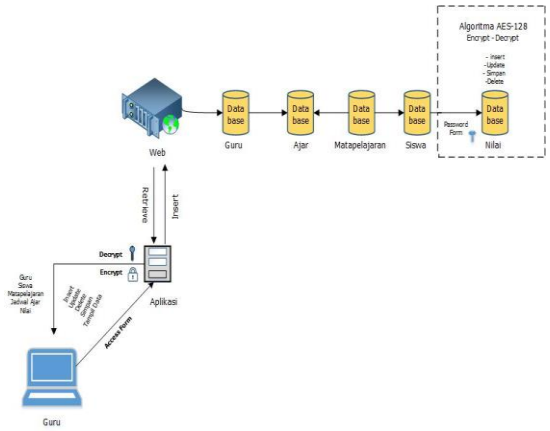
3.1. Penyelesaian Masalah

Dari penyelesaian permaslahan diatas, maka dibuatlah sebuah aplikasi *database* dengan pengamanan menggunakan algoritma *Advanced Encryption Standard AES-128 bit berbasis Web* yang dapat dijalan di *laptop* atau komputer yang sudah terinstal *software xampp* untuk menjalankan program tersebut dapat mengaktifkan *xampp* karena untuk menjalan suatu program yang berbasis Web, agar program dapat berjalan dengan optimal. Kemudian aplikasi ini mempunyai enkripsi dan dekripsi. masing-masing mempunyai kegunaanya bila melakukan enkripsi maka data tersebut tidak bisa dibaca berupa karakter data acak-acak dan jika ingin mengembalikan data tersebut maka proses dekripsi dan data tersebut akan menjadi data semula (asli)

2.2 Rancangan Aplikasi

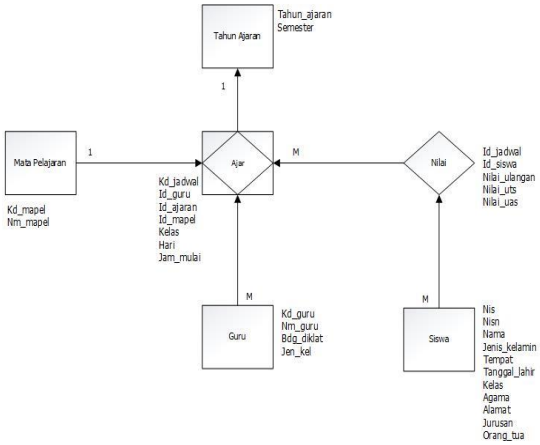
Padar rancangan ini adalah alur atau skema proses aplikasi untuk dapat memahami proses sistem yang dibangun, berikut adalah gambar 1 dibawah ini menjelaskan tentang alur aplikasi tersebut.

Gambar 1. Skema Arsitektur Sistem Akademik.



2.3 Rancangan ERD (*Entity Relationship Diagram*)

Pada rancangan *entity relationship diagram* adalah sebuah komponen-komponen himpunan entitas atau himpunan relasi, alur dari sebuah rancangan basis data yang diimplementasikan atau dirubah menjadi real yang nantinya agar mempermudah alur aplikasi. Masing-masing dilengkapi dengan atribut-atribut yang mewakili seluruh data yang ada. Seperti gambar berikut ini:

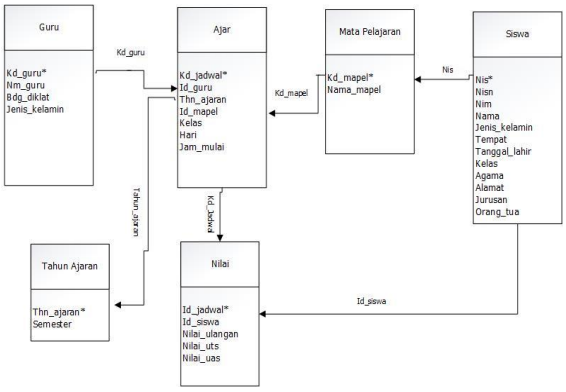


Gambar 2. Racangan *ERD* (*Entity Relationship Diagram*).

2.4 Rancangan LRS (*Logical Record Structure*).

Pada rancangan *logical record structure* adalah menjelaskan mengenai roses data yang akan saling terhubung satu sama lain, agar hasil data tersebut

dapat secara teratur. Hal ini terdapat suatu primary key berguna data tersebut saling terhubung pada tabel-tabel didalam suatu database. Seperti gambar berikut ini:



Gambar 3. Rancangan *LRS* **(*Logical Record Structure*).**

2.5 Spesisikasi Databse

Pada aplikasi database ini yang berbasis *web*, membutuhkan database yang terdiri dari *user*, guru, siswa, mapel, jadwal, nilai_semester, Tahun ajaran dan hasil pengujian. Menjelaskan mengenai database yang secara bersifat dinamis yang bisa diartikan bisa melakukan penambahan data, pengubahan data dan pengahapusan data tanpa mengubah program. Ataupun *file* database diberinama yang sesuai tertera pada tabel masing-masing.

Field	Type	Length	Keterangan
Id	Integer	11	User
username	Varchar	255	Username
password	Varchar	2555	Password
Active	Integer	1	Active

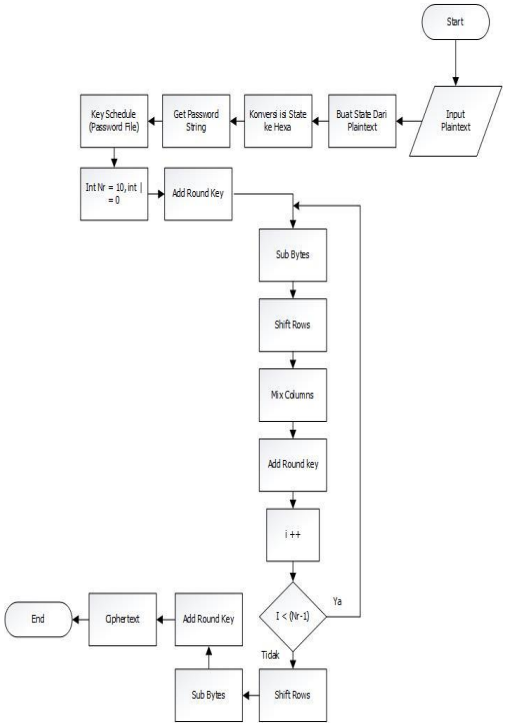
Tabel 1. Tabel Nilai_semester.

Field	Type	Length	Keterangan
Id	Integer	11	Id nilai semester
id_jadwal	Integer	11	Id jadwal
id_siswa	Integer	11	Id siswa
nilai_ulangan	Varchar	25	Nilai ulangan
nilai_uts	Varchar	25	Nilai uts
nilai_uas	Varchar	25	Nilai uas

Tabel 2. Tabel Nilai_semester.

2.6 Flowchart *Advanced Encryption Standard (AES-128)*.

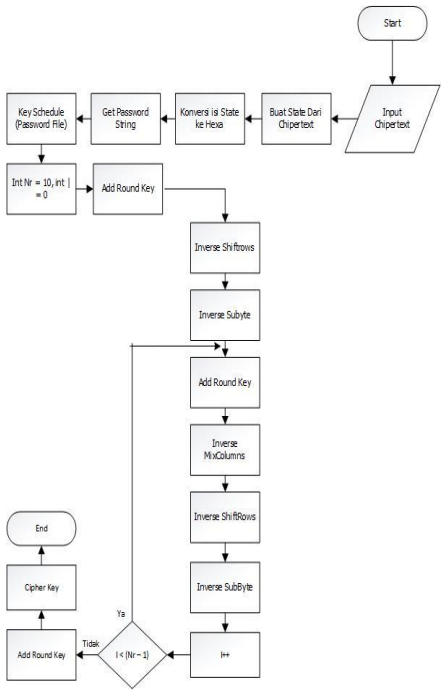
Proses ini saat menggambarkan alur enkripsi pada *flowchart* dibawah ini merupakan proses enkripsi algoritma *Advanced Encryption Standard* AES 128 *bit*. Bisa lihat pada gambar 4 berikut:



Gambar 4. Flowchart *Advenced Encryption Stadard* (AES-128).

2.7 Flowchart *Advanced Decryption Standard* (AES-128).

Proses ini saat menggambarkan alur dekripsi pada *flowchart* dibawah ini merupakan proses dekripsi algoritma *Advanced Encryption Standaes* AES 128 *bit*. Bisa lihat pada gambar 5 berikut:



Gambar 5. Flowchart *Advanced Decryption Standard* (AES-128).

3. HASIL DAN PEMBAHASAAN

4.1 Tampilan Layar Menu *Login.*

Pada tampilan layar menu *login* ini *user* dapat meng-*input* data diri yaitu *username* dan *password* yang sesuai, susudah itu maka proses tahap lainnya. Tampilan Layar *Login*. Berikut gambar 6 berikut ini

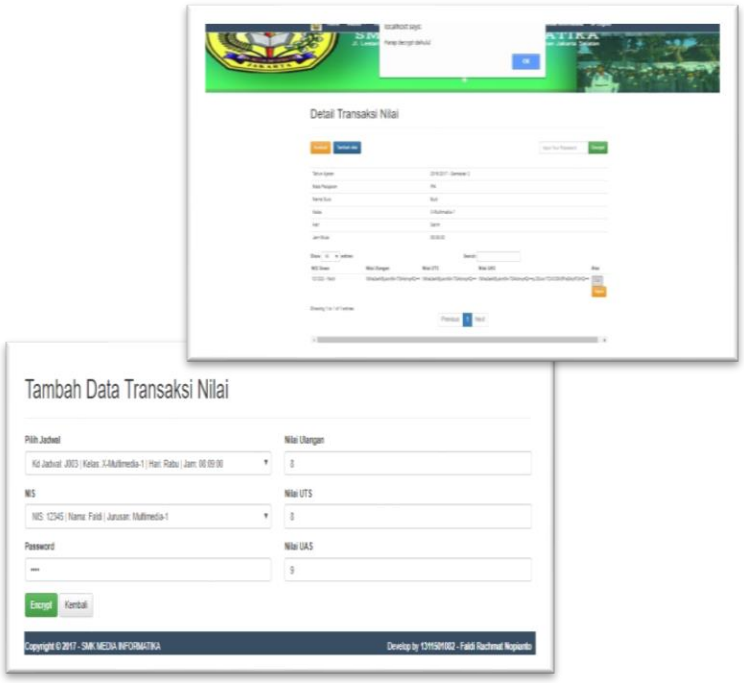
:Gambar 6. Tampilan Layar Menu *Login*.

4.2 Tampilan Layar Menu *Home*

Pada rancangan layar terdapat menu *home* ini *user* dapat memilih beberapa menu bar diantaranya adalah Master dengan isinya form Guru, form Siswa, form Mata Pelajaran dan form Tahun ajaran, Transaksi dengan isinya form Jadwal ajar dan Nilai dan Info dengan isinya form *Help* dan form *About.* Berikut Gambar 7. Tampilan Layar Menu *Home.*

Gambar 7. Tampilan Layar Menu *Home*.

4.3 Tampilan Layar Tambah Transaksi Nilai

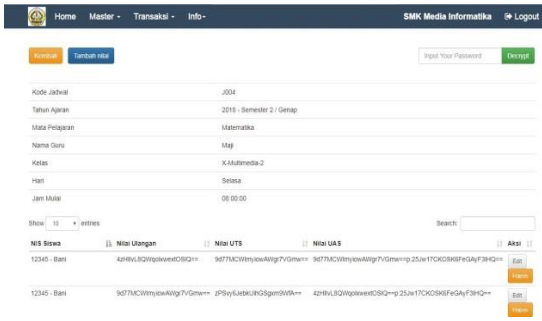


Pada tampilan layar ini adalah form transaksi Nilai, Disini *user* harus melakukn proses meng-*entry* kembali dengan memilih data yang sesuai pada saat proses awal di *input* dan memasukan *password* yang sesuai dengan benar lalu proses simpan dan *encrypt.* Berikut Gambar 8 Tampilan Layar.

Gambar 9. Tampilan Layar Tambah Transaksi Nilai.

4.4 Tampilan Layar *Detail* Transaksi Nilai

Pada tampilan layar *detail* transaksi nilai ini *user* dapat melihat hasil *encrypt* dari data nilai siswa dan jika *user* ingin merubah data menjadi data asli lakukan proses *input password* yang sesuai lalu proses pilih tombol *decrypt.* Data tersebut akan kembali seperti semula. Berikut Gambar 10 Tampilan Layar *Detail* Transaksi Nilai.



Gambar 10. Tampilan Layar *Detail* Transaksi Nilai.

4.5 Tampilan Layar *Edit Transaksi Nilai*

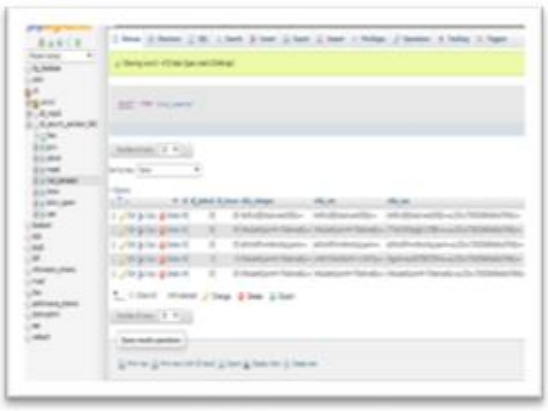
Tampilan layar *edit* transaksi nilai yaitu pada saat *user* melakukan pengisian data dan tersimpan pada database dan akan tetapi jika salah satu data terdapat kesalahan data maka melakukan proses *edit* dan selain itu terdapat tombol *encrypt* berguna untuk melakukan proses penyimpanan dan sekaligus mengamankan data tersebut agar memudahkan ataupun tidak bisa disadap oleh orang yang tidak bertanggung jawab Berikut Gambar 11 Tampilan Layar *Detail* Transaksi Nilai.

Gambar 11. Tampilan *Edit* Data Transaksi Nilai.

4. UJI COBA PROGRAM

4.1 Tampilan Layar Enkripsi Data Pada *Database* Nilai.

Tampilan layar enkripsi data pada *database* nilai dimana data tersebut merupakan proses sangat penting dan diakses oleh *user. dan database* yang terlihat beberapa menggambarkan hasil enkripsi dari beberapa tabel data yang ada. Berikut Gambar 12. Tampilan Layar Enkripsi Data Pada *Database*.



Gambar 12. Tampilan Layar Enkripsi Data Nilai Pada *Database.*

4.2 Tabel Hasil Pengujian Enkripsi Data Nilai

Berikut ini adalah pengujian Enkripsi data form pada *database*. Berikut Tabel 13 tampilan layar *chatting*.

a. Uji Coba Data Siswa XI
   a) Nis Siswa : 1617.239
   b) Nama Siswa : Adinda Az Zahra
   c) *Public key* : 12345678
   d) *Plaintext* (Nilai) : 80, 80, 80
   e) Waktu Proses : 0.17401003837585
   f) Size Filtering : 0.0009765625 KB
   g) *Ciphertext* :
   h) AES 128 :
   zPSvy6JebkUihGSgxm9WfA==
   MNqXTNkXQvhDr80KvsmDKw==
   ng4mzKqu7BbwvG0X3/8neA==p
   :25Jw17CKOSK6FeGAyF3lHQ==

Nis Siswa	Nama Siswa	Nilai Ulangan	Nilai Uts
1617.239	Adinda Az Zahra	zPSvy6JebkUihGSgxm9WfA==	MNqXTNkXQvhDr80KvsmDKw==

Nilai uas	Waktu Proses Enkripsi	Ukuran_filestring
ng4mzKqu7BbwvG0X3/8neA==p	0.17401003837585	0.0009765625 KB

Tabel 3. Hasil Pengujian Enkripsi Data Siswa ”Adinda Az Zahra”.

b. Uji Coba Data Siswa X
   a) Nis Siswa : 1327.458
   b) Nama Siswa : Doni
   c) *Public key* : 12345678
   d) *Plaintext* (Nilai) : 70, 90, 60
   e) Waktu Proses : 0.000262022
   f) Size Filtering : 0.0009765625 KB
   g) *Ciphertext* :
   h) AES 128 :
   g4i4cI9y04jeUPOXgqfmjA==
   46auOatWRPmOUvUhs5yWw==
   46auOatWRPmOUvUhs5yWw==p:25J
   w17CKOSK6FeGAyF3lHQ==

Nis Siswa	Nama Siswa	Nilai Ulangan	Nilai Uts
1327.458	Doni	WKe2eAt5jukmM+7GAdmq4Q==	WKe2eAt5jukmM+7GAdmq4Q==

Nilai uas	Waktu Proses Enkripsi	Ukuran_filestring
ng4mzKqu7BbwvG0X3/8neA==p	0.17401003837585	0.0009765625 KB

Tabel 4. Hasil Pengujian Enkripsi Data Siswa ”Doni”.

5. AKHIR PROGRAM

Adapun penulis menarik kesimpulam yang diperoleh setelah melewati tahap perancangan, pembuatan, dengan merangkai dan uji coba ataupun analisa program aplikasi *Database* ini, antara lain:

a. Kelebihan Program

1) Aplikasi ini mempunyai tampilan yang sangat *flexible*, agar memudahkan *user* dapat mengelola aplikasi tersebut dengan baik. Dengan tampilan yang sederhana agar *user* bisa menglola dan selain itu *user* dapat cepat mengetauhi aplikasi tersebut.
2) Terdapat keamanannya didalam suatu aplikasi tersebut. Dikarenakan dapat berguna untuk mengamankan data-data akademik secara langsung pada aplikasi tersebut. Selain itu *user* tidak usah kawatir dengan penyimpan data-data informasi akademik, Karena sudah terdapat pengamananya dan terdapat penampung subuah data-data didalam databaseData hasil dekripsi tidak mengalami perubahan (bentuk, ukuran, maupun nama) atau kerusakan dan dapat dibaca kembali oleh pengguna.
3) Terdapat pengamanan ganda yang dimaksud adalah terdapat *form login user* dapat memegang suatu *username*

dan *password.* Jika dari pihak luar atau pihak yang ingin bobol aplikasi tersebut maka tidak bisa karena cukup *user* (guru) saja yang bisa membuka atau menjalankan aplikasi tersebut.

4) Terdapat berupa pesan validasi *error* jika salah satu data atau pesan tidak terisi dengan sesuai..

b. Kekurangan Program

1) Aplikasi ini beesifat *offline* karena masih menggunakan server yang ada pada desktop.
2) aplikasi ini dapat menampung data hanya beberapa ratusan atau ribuan saja, jika data tersebut dimasukan semakin besar maka akan muncul valiadasi yaitu *error*.
3) Karena aplikasi offline dan masih menggunakan *server database* sebagai perantara ketiga maka untuk melakukan atau sewaktu-waktu *Sign in* pada aplikasi ini, perlu mengaktifkan *software MYSQL* dan *apache server* sebagai penghubung antara aplikasi dengan *database server*.

6. KESIMPULAN

6.1 Kesimpulan Aplikasi

Penulis dapat menarik kesimpulan berdasarkan hasil Uji coba dan berbagai analisa yang telah penulis lakukan terhadap permasalahan dan aplikasi yang akan dikembangkan, maka dapat menarik suatu kesimpulan-kesimpulan sebagai berikut:

a. Hal ini dengan adanya aplikasi keamanan *database* ini dapat mengambarkan bahwa data informasi akademik tersebut dapat diamankan secara *real* atau data tersebut tidak bisa disadap ataupun dimanipulasi oleh orang yang tidak bertanggung jawab. dengan mengimplementasikan sebuah keamanannya dengan menggunakan algoritma *Advanced Encryption Standard* (AES) 128. berguna untuk mengembangkan suatu informasi akademik yang lebih baik.
b. Dengan aplikasi ini, memudahkan pengguna untuk menyimpan data ke dalam *database* yang telah dienkripsi dengan menggunakan aplikasi ini.
c. Aplikasi ini juga dapat mengembalikan data yang sudah diamankan menggunakan algortima kriptografi *Advanced Encryption Standard* (AES) 128*bit* menjadi data yang orisinil tanpa mengalami perubahan sedikitpun.
d. Langkah selanjut mengenai tampilan *web,* Aplikasi ini memiliki fitur yang sangat menarik, dinamis atau juga tidak familliar ataupun untuk desainnya sangat efisien bisa dikembangkan kembali.
e. Selain itu terdapat keamanan ganda yang bermaksud untuk mencegah terjadi penyadapan atau dihack oleh orang yang tidak bertanggung jawab. sehingga dapat merahasiakan isi data akademik lebih baik. Aplikasi tersebut hanya dapat bisa dibuka atau digunakan oleh admin yang mempunyai *pas*sword tertentu.

7. SARAN

Dalam hal ini penulis dapat menyarankan dan menarik beberapa kesimpulan, dapat pula diajukan saran-saran yang mungkin bisa dijadikan pertimbangkan antara lain:

a. hanya dapat melakukan mengenkripsi data per-*record* pada database.
b. Aplikasi ini diharapkan dapat dikembangakan kembali saat melakukan mengenkripsi data per-tabel pada database.
c. Dapat diimplementasikan penggunaan metode kriptografi dengan menggunakan algoritma yang lain berguna untuk meningkatkan keamanan data yang begitu aman.
d. Aplikasi ini diharapkan dapat ditingkatkan kinerjanya sehingga data yang di enkripsi tidak hanya *plaintext* pada *database* saja, namun dapat bentuk gambar pada *database.*
e. Aplikasi ini diharapkan dapat dikembangkan beberapa fitur dan karakter masukkan kunci/*key* tidak hanya berupa angka tetapi dapat berupa karakter huruf.

8. DAFTAR PUSTAKA

[1] Halim, H. (2014). Penggunaan Algoritma AES-128 Bit Sebagai Teknik Pengamanan. *Halim, Richard*, 1–7.

[2] Jumrin, Sutardi, S., 2016. Aplikasi sistem keamanan basis data dengan teknik kriptografi rc4., 2 (1), pp 59–64.

[3] Marwanta, Y. Y. (2014). Aplikasi Pengamanan Basis Data dengan Teknik Kriptografi Stream Cipher. *Igarss 2014*, (1), 1–5. Available at: https://doi.org/10.1007/s13398-014-0173-7.2.

[4] Pabokory, F.N., Astuti, I.F. & Kridalaksana, A.H., 2015. Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard. *Jurnal Informatika Mulawarman*, 10(1), pp 20–31.

[5] Tullah (2016). Perancangan Aplikasi Kriptografi File Dengan Metode Algoritma Advanced Encryption Standard (AES). *Jurnal Sisfotek Global*, *6*(2), 24–30.

[6] Rahmawati, R., & Rahardjo, D., 2016. Aplikasi Pengamanan Data Menggunakan Algoritma Steganografi Discrete Cosine Transform dan Kriptografi grafi AES 128 BIT pada SMK PGRI 15 Jakarta. *Jurnal Teknik Informatika* Dan *Sistem Informasi*., *2*(April), 67–74.