JUKOMTEK
(Jurnal Komputer Dan Teknologi)
e-ISSN 2961-9009
p-ISSN 2963-1289

IMPLEMENTASI KRIPTOGRAFI *ADVANCED ENCRYPTION STANDARD* 128 BIT DALAM PENGAMANAN DATA KEUANGAN KAS (Studi Kasus: Masjid Al-Ikhlas Trini Sleman D.I.Yogyakarta)

Hilda Dwi Novianti[1], Ahmad Tri Hidayat[2]

Universitas Teknologi Yogyakarta, Sleman D.I.Yogyakarta 55285
** Email : hildadwi2611@gmail.com[1], ahmadth@staff.uty.ac.id[2]*

INFO ARTIKEL

Sejarah Artikel:
Diterima Tgl. 23/12/2022
Diperbaiki Tgl. 22/01/2023
Disetujui Tgl 25/01/2023
Tersedia daring Tgl 28/01/2023

e-ISSN 2961-9009
p-ISSN 2963-1289

DOI : 10.58290/jukomtek.v1i2.51

ABSTRAK

Masjid Al-Ikhlas merupakan masjid yang terletak di Dusun Trini, Kecamatan Gamping, Kabupaten Sleman, D.I. Yogyakarta. Masjid Al-Ikhlas memiliki sistem informasi keuangan untuk melakukan pendataan kas masjid dalam bentuk dokumen. Namun, pengamanan dokumen keuangan kas masjid masih dilakukan secara manual yaitu menyimpan dokumen ke dalam arsip digital di folder komputer tanpa diberi keamanan. Tindakan tersebut mengakibatkan rentan terjadinya pencurian data atau manipulasi data sehingga data yang keluar tidak akurat. Data keuangan kas sangat penting bagi masjid tersebut, dikarenakan jika ada kecurangan akan mengalami kerugian yang sangat fatal. Oleh karena itu, dilakukan penelitian yang bertujuan untuk membuat sebuah sistem untuk mengamankan data keuangan kas masjid dengan menggunakan metode *Advanced Encryption Standard* (AES) 128 Bit. AES berguna untuk memberikan tingkat keamanan yang tinggi berdasarkan kunci rahasia yang kompleks sehingga dapat merahasiakan data yang akan diamankan. Oleh karena itu, metode AES 128 BIT dibutuhkan untuk mengamankan isi dari data kas masjid agar terhindar dari pencurian data atau manipulasi data.

Kata Kunci:
Data Keuangan Kas, Kriptografi, Enkripsi, Dekripsi, AES-128 Bit.

PENDAHULUAN

Pesatnya perkembangan teknologi informasi dan telekomunikasi bermanfaat untuk aktivitas bertukar informasi baik dalam bentuk data atau dokumen yang bersifat rahasia. Di era kemajuan teknologi yang pesat, membuat banyak perubahan secara positif maupun negatif. Salah satunya, dampak negatif misalnya, pencurian data dan manipulasi data. Oleh karena itu, dibutuhkan sistem pengamanan untuk mengamankan data atau dokumen yang bersifat rahasia.

e-ISSN 2961-9009
p-ISSN 2963-1289

Masjid Al-Ikhlas merupakan masjid yang terletak di Dusun Trini, Kecamatan Gamping, Kabupaten Sleman, D.I. Yogyakarta. Masjid Al-Ikhlas dikelola oleh Dewan Kemakmuran Masjid (DKM). Masjid Al-Ikhlas memiliki sistem informasi keuangan yang dapat membantu pengurus untuk melakukan pendataan kas masjid dalam bentuk dokumen. Namun, pengamanan dokumen keuangan kas masjid masih dilakukan secara manual yaitu menyimpan dokumen ke dalam arsip digital didalam folder komputer tanpa diberi keamanan. Tindakan tersebut mengakibatkan rentan terjadinya pencurian data, manipulasi data sehingga data yang keluar tidak akurat. Data keuangan kas sangat penting bagi masjid tersebut, dikarenakan jika ada kecurangan akan mengalami kerugian yang sangat fatal.

(Cristy, N dan Riandari, F 2021) menjelaskan bahwa mengimplementasikan sistem untuk pengamanan data menggunakan metode AES yang digunakan untuk proses enkripsi dan dekripsi karena memberikan tingkat keamanan yang tinggi berdasarkan kunci rahasia yang kompleks sehingga dapat merahasiakan data yang akan diamankan. Pada penelitian ini telah dibuktikan bahwa hasil enkripsi dapat dilakukan pada dokumen dalam bentuk format excel dan menghasilkan suatu kemajuan teknologi yang dapat mengamankan data yang bersifat *sensitive*.

Berdasarkan penelitian sebelumnya, keamanan data menjadi sesuatu yang harus dijaga keamanannya. Pengamanan suatu data yang dienkripsi dan dekripsi dilakukan guna melindungi dari pencurian data, manipulasi data, dan penyalahgunaan data oleh pihak yang tidak berwenang. Oleh karena itu, penulis menggunakan algoritma Kriptografi AES (*Advanced Encryption Standard*) 128 bit untuk proses enkripsi dan deskripsi data. Penerapan algoritma ini akan dilakukan pada pengamanan data keuangan kas masjid. *Advanced Encryption Standard* (AES) memiliki putaran kunci untuk proses enkripsi dan deskripsi. AES berguna untuk memberikan tingkat keamanan yang tinggi berdasarkan kunci rahasia yang kompleks sehingga dapat merahasiakan data yang akan diamankan. Oleh karena itu, metode AES 128 BIT dibutuhkan untuk mengamankan isi dari data kas masjid agar terhindar dari pencurian data dan manipulasi data.

LANDASAN TEORI

a. Kriptografi

Menurut Menez yang dikutip oleh Munir dalam Kuliah Pengantar Kriptografi (2019), mendefinisikan bahwa kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi. Dalam ilmu kriptografi, terdapat dua buah proses yaitu

e-ISSN 2961-9009
p-ISSN 2963-1289

melakukan enkripsi dan deskripsi. Enkripsi berarti proses penyembunyian data pesan, mengubah *plaintext* menjadi *chipertext*. Sedangkan dekripsi merupakan kebalikan dari enkripsi, bertujuan untuk memahami pesan yang ada, dan kunci adalah teknik yang digunakan untuk enkripsi maupun dekripsi (Choiri, E.O., 2020).

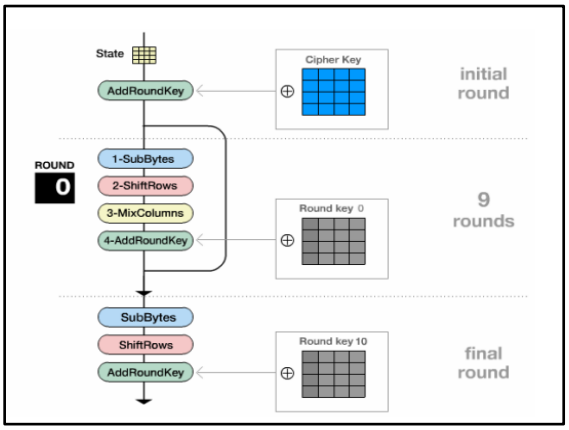
b. Enkripsi dan Dekripsi

Pada ilmu kriptografi terdapat istilah enkripsi dan dekripsi. Enkripsi adalah sebuah proses yang melakukan perubahan sebuah kode dari yang bisa dipahami menjadi sebuah kode yang tidak bisa dipahami. Dengan kata lain, enkripsi merupakan proses menyandikan *plainteks* (pesan asli) menjadi *cipherteks* (pesan tersandi). Dekripsi kebalikan dari proses enkripsi yaitu proses mengubah data yang telah dibuat tidak dapat dibaca melalui enkripsi kembali ke bentuk yang tidak dienkripsi. Data yang dienkripsi atau dikodekan akan dikembalikan ke bentuk aslinya.

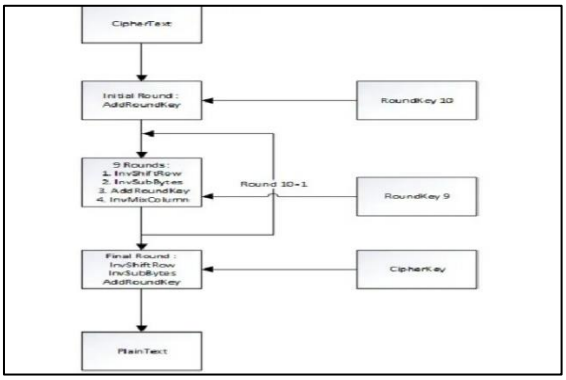
c. *Advanced Encryption Standart* (AES)

Advanced Encryption Standard merupakan algoritma kriptografi yang dapat digunakan untuk mengamankan data. Menurut (Leohani, R.A. dan Agus, I., 2016), *Advanced Encryption Standard* (AES) merupakan algoritma kriptografi yang bisa digunakan untuk melindungi data. Algoritma ini ditetapkan oleh *National Institute of Standards and Technology* (NIST), dimana menjadi pengganti DES dalam algoritma enkripsi simetri yang baru. Dikarenakan penggunaan DES *(Data Encryption Standart)* dianggap sudah tidak aman lagi karena dengan perangkat keras khusus kuncinya bisa ditemukan dalam beberapa hari.

AES menggunakan *chipper* blok simetri yang dapat memproses blok data 128 bit, dengan menggunakan kunci chipper yang panjangnya 128, 192, dan 256 bit. Berdasarkan hal tersebut, perbedaan panjang kunci mempengaruhi jumlah putaran yang akan diimplementasikan dalam algoritma AES. AES mempunyai panjang kunci paling sedikit 128 bit, maka AES tahan terhadap serangan exhaustive key search dengan teknologi saat ini. Dengan panjang kunci 128-bit, maka terdapat sebanyak 2128 = 3,4 x 1038 kemungkinan kunci.



Gambar 1. Diagram Alur Proses Enkripsi AES

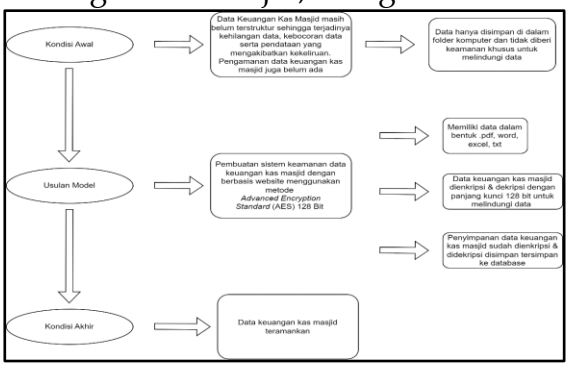

Gambar 2. Diagram Alur Proses Dekripsi AES

METODE PENELITIAN

(Notoatmodjo, 2018) menjelaskan bahwa kerangka penelitian merupakan suatu cara yang digunakan untuk menjelaskan

e-ISSN 2961-9009
p-ISSN 2963-1289

hubungan atau kaitan antara *variable* yang akan diteliti. Adapun kerangka penelitian yang akan dilakukan dalam pembuatan sistem keamanan data keuangan kas masjid, sebagai berikut.

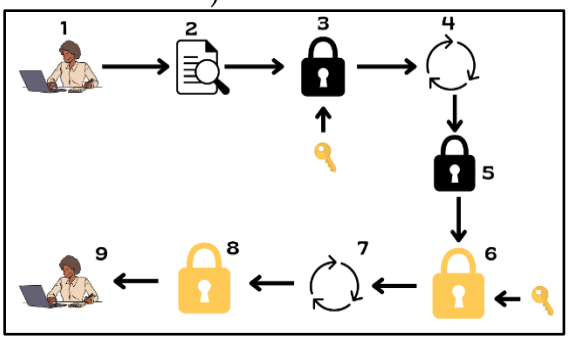


Gambar 3. Kerangka Penelitian

Sumber data diperoleh dari data primer dan data sekunder. Data primer mengacu pada informasi yang diperoleh langsung ketika melakukan wawancara dan melakukan observasi. Data sekunder diperoleh dari dokumentasi perusahaan, buku, jurnal ilmiah.

Dalam penelitian ini data diperoleh melalui observasi langsung ke tempatnya dan wawancara dengan Ketua dan Bendahara Masjid Al-Ikhlas Trini. Data yang diperoleh di Masjid Al-Ikhlas Trini sebagai acuan dalam implementasi enkripsi dan dekripsi data dokumen keuangan kas masjid.

Aplikasi sistem pengamanan pada data keuangan kas masjid di Masjid Al-Ikhlas Trini berbasis *Website* dapat diakses oleh orang tertentu yaitu admin dan pengurus masjid. Proses pengamanannya dengan cara, yaitu dimulai dengan *login* untuk bisa mengakses sistemnya (dimana orang tersebut sudah memiliki hak akses untuk login). Kemudian masuk ke halaman dashboard (*form* enkripsi, *form* dekripsi, dan *form* kas masjid). Setelah itu, masuk ke menu *form* enkripsi (dimana *file* data yang diinputkan akan terenkripsi). Setelah *file* data terenkripsi, masuk ke menu form dekripsi (*file* data yang terenkripsi akan di dekripsi, *file* tersebut kembali ke bentuk semula).

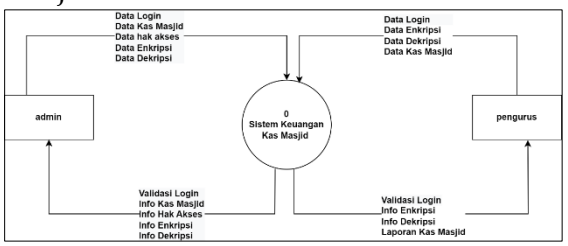


Gambar 4. Arsitektur Model

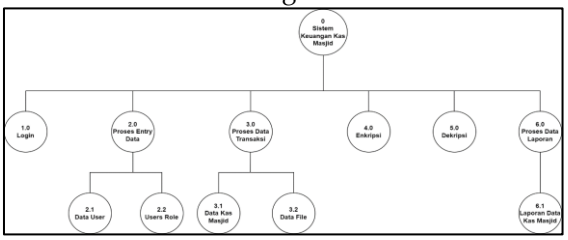
Perangkat keras yang digunakan dalam membangun aplikasi pengamanan data keuangan kas masjid sebagai berikut:
1. PC (*Personal Computer*) Acer Aspire 5
2. Processor Intel i5 11th Gen 2,42 GHz
3. Ram 8 Gb
4. SSD 512 Gb

Perangkat lunak yang digunakan mendukung dalam pembuatan dan pengoperasian program aplikasi sebagai berikut:
1. Sublime Text
2. XAMPP
3. *Draw.io*

Berikut merupakan perancangan sistem pengamanan data keuangan kas masjid Al-Ikhlas.

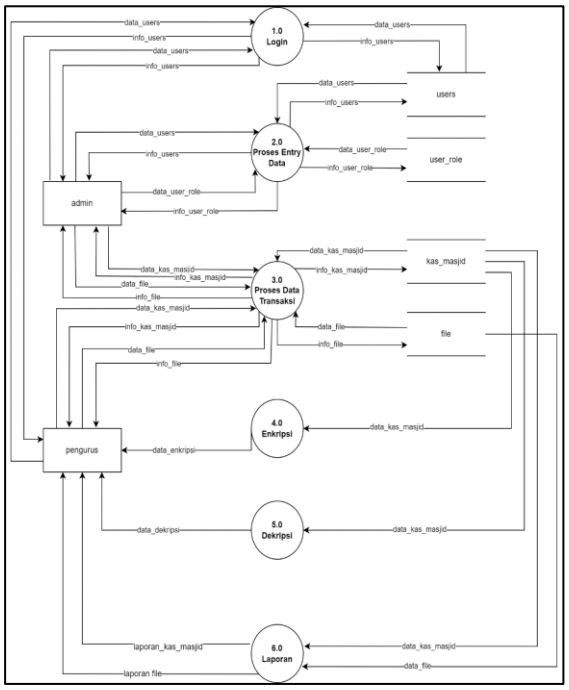


Gambar 5. Diagram Konteks

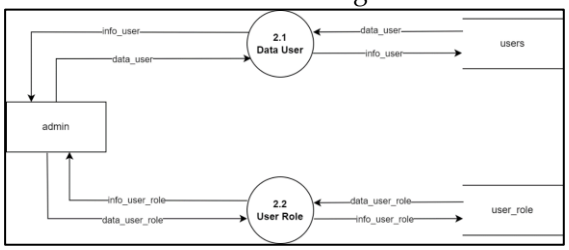


Gambar 6. Diagram Jenjang

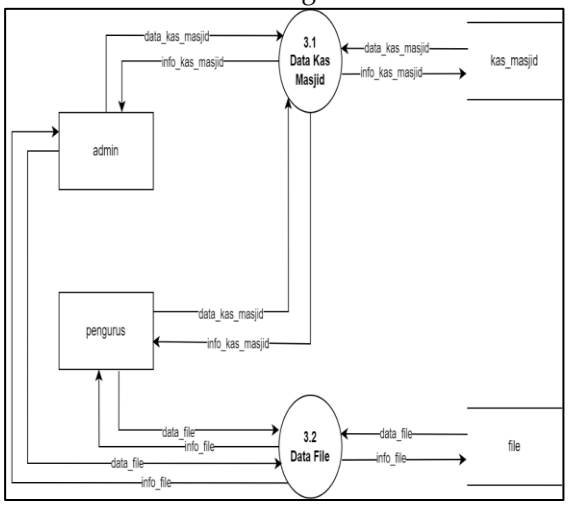
e-ISSN 2961-9009
p-ISSN 2963-1289



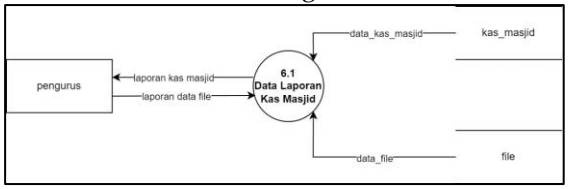
Gambar 7. Data Flow Diagram Level 1



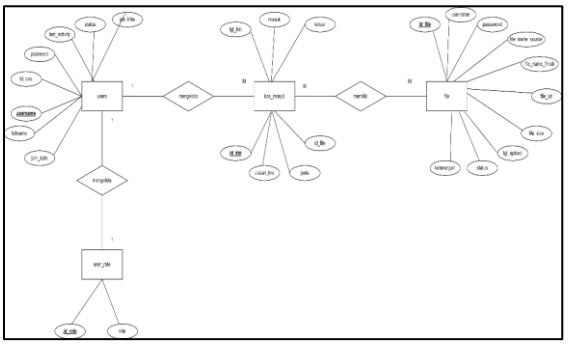
Gambar 8. Data Flow Diagram Level 2 Proses 2



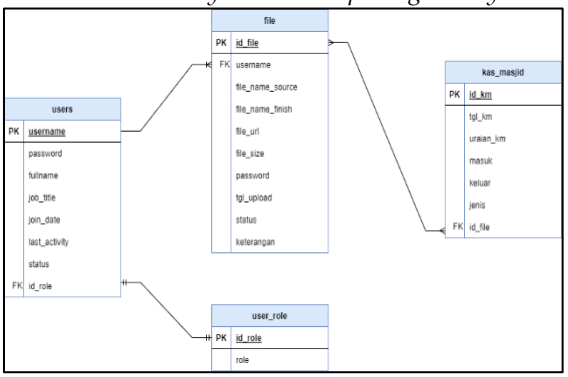
Gambar 9. Data Flow Diagram Level 2 Proses 3



Gambar 10. Data Flow Diagram Level 2 Proses 4



Gambar 11. *Entity Relationship Diagram System*



Gambar 12. Relasi Tabel

HASIL DAN PEMBAHASAN

Tampilan Menu Login

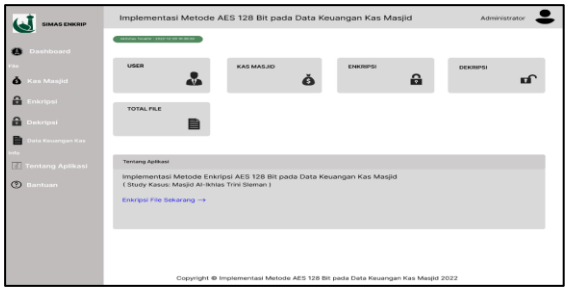
Sebelum *user* mengakses sistem, *user* diharuskan untuk login menggunakan *username* dan *password*.

Gambar 13. Halaman Login

Tampilan Menu *Dashboard*

Halaman ini adalah halaman yang pertama kali akan dilihat oleh Admin atau pengurus ketika setelah melakukan proses *login*.

e-ISSN 2961-9009
p-ISSN 2963-1289



Gambar 14. Halaman *Dashboard*

Tampilan Halaman Kas Masjid

Halaman data kas masjid ini adalah tampilan ketika admin menekan tombol kas masjid pada naviagasi. Pada halaman ini, admin atau pengurus dapat mengelola data pemasukan kas dan pengeluaran, mulai dari input, ubah, dan hapus.

Gambar 15. Halaman Kas Masjid

Tampilan Menu *Form* Enkripsi

Halaman data enkripsi ini adalah tampilan ketika admin menekan tombol enkripsi pada navigasi. Pada halaman ini, admin atau pengurus dapat mengelola atau menginputkan *file* yang akan dienkripsi. Di halaman ini, data/*file* yang diinputkan akan terenkripsi, kemudian klik tombol simpan, data/*file* akan terenkripsi.

Gambar 19. Halaman *Form* Enkripsi

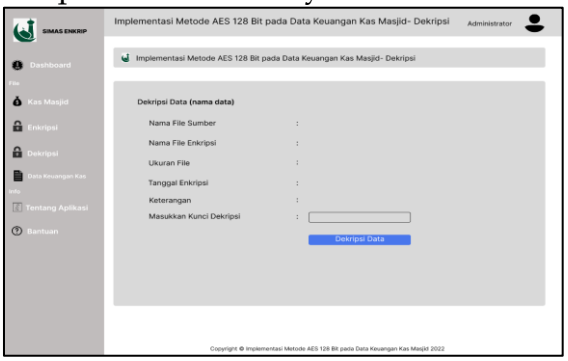
Tampilan Menu *Form* Dekripsi

Halaman data dekripsi ini adalah tampilan ketika admin menekan tombol enkripsi pada navigasi. Pada halaman ini, admin atau pengurus dapat mengelola data/*file* yang telah di enkripsi sebelumnya. Setelah itu, *file* akan tersimpan di halaman dekripsi dan klik pada aksi ada pilihan dekripsi atau enkripsi *file*. Di halaman ini, data yang telah dienkripsikan akan kembali ke data sebelumnya.

Gambar 20. Halaman *Form* Dekripsi

Tampilan Menu Proses Dekripsi File/Data

Halaman proses dekripsi adalah halaman untuk menampilkan proses dekripsi. Dimana, setelah *file* atau data di enkripsi kemudian klik dekripsi *file*, lalu akan menuju ke halaman proses dekripsi. Di halaman ini, menampilkan keterangan data atau file yang terenkripsi serta pengguna menginputkan *password* yang telah diinputkan sebelumnya

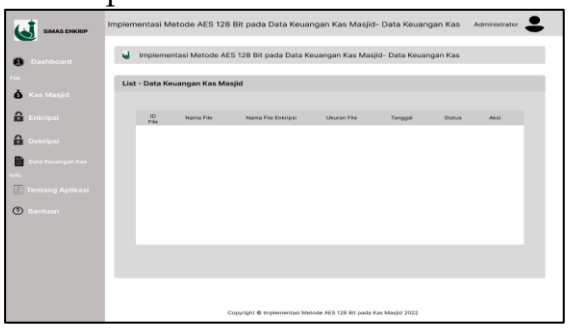


Gambar 21. Halaman Proses Dekripsi File/Data

e-ISSN 2961-9009
p-ISSN 2963-1289

Tampilan Menu Data Keuangan Kas

Halaman Data Keuangan Kas merupakan halaman untuk menampilkan data atau *file* baik dienkripsi maupun didekripsi akan tersimpan di database. Admin atau pengurus bisa melihat data atau *file* mana yang telah dienkripsi maupun didekripsi.



Gambar 22. Halaman Data Keuangan Kas

Tampilan Menu Tentang Aplikasi

Pada halaman tentang aplikasi merupakan halaman untuk memberikan informasi sistem tersebut.

Gambar 23. Halaman Tentang Aplikasi

Tampilan Menu Bantuan

Halaman bantuan ini adalah tampilan halaman jika pengurus ingin mengetahui tentang sistemnya, jika ada hal yang tidak diketahui bisa klik Halaman Bantuan untuk mengetahui jawaban yang belum diketahui.

Gambar 24. Halaman Bantuan

KESIMPULAN

Dari hasil penelitian yang telah dilakukan pada Masjid Al-Ikhlas Trini Sleman D.I.Yogyakarta, maka penulis menarik kesimpulan yaitu dengan adanya implementasi metode kriptografi AES 128 Bit pada data keuangan kas masjid Al-Ikhlas dapat membantu meminimalisir kebocoran dan penyalahgunaan data keuangan kas masjid serta menjaga keamanan data keuangan yang dianggap penting untuk dijaga kerahasiaan dari pihak yang tidak berwenang.

DAFTAR PUSTAKA

Choiri, E.O., 2020, *Pengertian Kriptografi, Sejarah & Jenis Algoritmanya,* akses 11 Oktober 2022.

Cristy, N. dan Riandari, F., 2021, *Implementasi Metode Advanced Encryption Standart (AES) 128 Bit Untuk Mengamankan Data Keuangan*, Jurnal Ilmu Komputer dan Sistem Informasi (JIKOMSI), Vol 04 No 02, 75-85.

Kristanto, A., 2018, *Perancangan Sistem Informasi dan Aplikasinya,* Yogyakarta: Gava Media.

Maniah dan Haminidin, D., 2017, *Analisis Dan Perancangan Sistem Informasi Pembahasan Secara Praktis Dengan Contoh Kasus*, Yogyakarta: Deepublish.

Mundzir 2018, *Kupas Tuntas Pengertian PHP dan Menurut Para Ahli*, diakses 17 Desember 2021.

Munir, R 2019, *Pengantar Kriptografi*, Bandung: Penerbit Informatika.

Notoatmodjo 2018, *Variable Terikat*, Variabel Terikat, 39.

Ramadan, A. dan Painem 2022, *Pengamanan Data Keuangan Menggunakan Algoritma Advanced Encryption Standart 128 Pada PT. Charise Deo Indonesia,* Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI), 49-57.

Sugiyono 2019, *Metode Penelitian Kuantitatif, Kualitatif, dan R&D*, Bandung, Alphabet.

Supono, Putratama., 2016, *Pemrograman Web Dengan Menggunakan PHP dan Framework Codeigniter*. Yogyakarta: Deepublish (Grup Penerbitan CV Budi Utama).

Wibowo, Y., dkk., 2022, *Penerapan Algoritma AES 128 Bit Untuk Keamanan Data Peminjaman Senjata Api Pada DENPOM I/5 Medan*, Jurnal CyberTech, Vol 2, No 12.

Widyawan, D. dan Imelda, I., 2021, *Pengamanan File Menggunakan Kriptografi Dengan Metode AES 128 Berbasis Web di Komite Nasional Keselamatan Transportasi,* Skanika, Vol 04 No 01, 15-22.