Analisa Alokasi Memori dan Kecepatan Kriptograpi Simetris Dalam Enkripsi dan Dekripsi

Resianta Perangin-angin[1,], Indra Kelana Jaya[2], Benget Rumahorbo[3], Berlian Juni R. Marpaung[4]

* Corresponding author : resianta88@gmail.com
[1,2,3] Universitas Methodist Indonesia, [4]SMK N 10 Medan
Jalan Hang Tuah No.8, Madras Hulu, Medan Polonia

Abstract--currently the focus of cryptography is on the security and speed of data transmission. Cryptography is the study of how to secure information. This security is done by encrypting the information with a special key. This information before being encrypted is called plaintext. After being encrypted with a key called ciphertext. At present, AES (Advanced Encryption Standard) is a cryptographic algorithm that is safe enough to protect confidential data or information. In 2001, AES was used as the latest cryptographic algorithm standard published by NIST (National Institute of Standard and Technology) in lieu of the DES (Data Encryption Standard) algorithm that has expired. The AES algorithm is a cryptographic algorithm that can encrypt and decrypt data with varying key lengths, namely 128 bits, 192 bits, and 256 bits. From the results of tests carried out for speed and classification memory, it can be concluded that the AES cryptographic algorithm is superior or faster if the size or size of the plaint text is not so large, because for the smaller AES algorithm the speed ratio in terms of encryption will become more fast, it becomes very different for the Blowfish algorithm itself where for large sizes plaint text can be encrypted faster than AES but for smaller sizes Blowfish is certainly slower in that case, for memory allocation in this case from the tests performed it can be concluded that AES requires more storage space or larger memory allocation compared to the blowfish algorithm

Keywords: symmetric cryptography, speed ratio, encryption, decryption

Abstrak-- *Yang menjadi fokus ilmu kriptografi di saat ini, berada pada keamanan dan kecepatan transmisi data. Kriptografi adalah ilmu yang mempelajari mengenai bagaimana cara mengamankan suatu informasi. Pengamanan ini dilakukan dengan mengenkrip informasi tersebut dengan suatu kunci khusus. Informasi ini sebelum dienkrip dinamakan plaintext. Setelah dienkrip dengan suatu kunci dinamakan ciphertext. Saat ini, AES (Advanced Encryption Standard) merupakan algoritma kriptografi yang cukup aman untuk melindungi data atau informasi yang bersifat rahasia. Pada tahun 2001, AES digunakan sebagai standar algoritma kriptografi terbaru yang dipublikasikan oleh NIST (National Institute of Standard and Technology) sebagai pengganti algoritma DES (Data Encryption Standard) yang sudah berakhir masa penggunaannya. Algoritma AES adalah algoritma kriptografi yang dapat mengenkripsi dan mendekripsi data dengan panjang kunci yang bervariasi, yaitu 128 bit, 192 bit, dan 256 bit. Dari hasil ujicoba yang dilakukan untuk rasio kecepatan dan alokassi memory maka dapat disimpulkan bahwa algoritma kriptografi AES lebih unggul atau lebih cepat apabila ukuran atau size plaint text tersebut tidak begitu besar, dikarenakan untuk algoritma AES ukuran semakin kecil maka rasio kecepatan dalam hal enkripsi akan menjadi lebih cepat, menjadi sangat berbeda untuk algoritma Blowfish sendiri dimana untuk plaint text yang memiliki ukuran yang besar dapat di enkripsi dengan lebih cepat dibandingkan dengan AES namun untuk ukuran lebih kecil tentu Blowfish lebih lambat dalam hal tersebut, untuk alokasi memori dalam hal ini dari ujicoba yang dilakukan dapat ditarik kesimpulan bahwa AES lebih membutuhkan ruang penyimpanan yang lebih besar atau alokasi memory yang lebih besar bila dibandingkan dengan algoritma blowfish.*

***Kata kunci** : kriptografi simetris, rasio kecepatan, enkripsi, dekripsi*

PENDAHULUAN

Keamanan merupakan komponen penting untuk memungkinkan adopsi teknologi dan aplikasi secara luas [1], dan yang menjadi focus ilmu kriptografi di saat ini, berada pada keamanan dan kecepatan transmisi data.[2], Kriptografi adalah ilmu yang mempelajari mengenai bagaimana cara mengamankan suatu informasi. Pengamanan ini dilakukan dengan mengenkrip informasi tersebut dengan suatu kunci khusus. Informasi ini sebelum dienkrip dinamakan plaintext. Setelah dienkrip dengan suatu kunci dinamakan ciphertext.[3]

Kriptografi (cryptography) merupakan ilmu dan seni untuk menjaga pesan agar aman. (Cryptography is the art and science of keeping messages secure) .Crypto. berarti .secret. (rahasia) dan .graphy. berarti .writing. (tulisan). [4], masalah keamanan tidak mungkin bisa dihilangkan dikarerenakan sistem digitalisasi merupakan sesuatu yang sangat riskan terhadap masalah keamanan. Selama beberapa tahun terakhir, algoritma kriptografi menjadi semakin penting. Algoritma Advanced Encryption Standard (AES) diperkenalkan pada awal tahun 2000.[5]

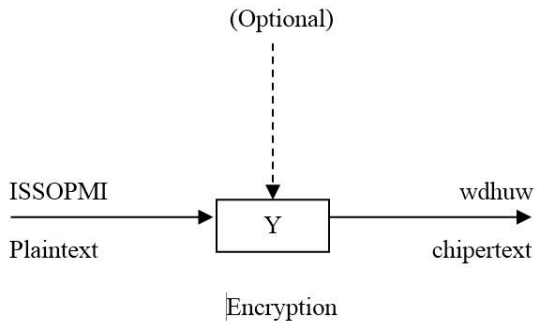
Saat ini, AES (*Advanced Encryption Standard*) merupakan algoritma kriptografi yang cukup aman untuk melindungi data atau informasi yang bersifat rahasia. Pada tahun 2001, AES digunakan sebagai standar algoritma kriptografi terbaru yang dipublikasikan oleh NIST (*National Institute of Standard and Technology*) sebagai pengganti algoritma DES (*Data Encryption Standard*) yang sudah berakhir masa penggunaannya. Algoritma AES adalah algoritma kriptografi yang dapat mengenkripsi dan mendekripsi data dengan panjang kunci yang bervariasi, yaitu 128 bit, 192 bit, dan 256 bit.[6]

Salah satu algoritma simteri selain dari pada AES yaitu adalah algoritma Blowfish alogitma ini sendiri diciptakan oleh Bruce Schneier, seorang Cryptanalyst Presiden perusahaan Counterpane Internet Security, Inc pada tahun 1993. Dan dipublikasikan tahun 1994.[7]. Blowfish merupakan salah satu algoritma yang kuat karena memiliki ruang kunci yang besar dan panjangnya bisa beragam, sehingga tidak mudah diserang pada bagian kuncinya. Suatu sistem kriptografi yang baik terletak pada kerahasiaan kunci dan bukan pada kerahasiaan algoritma yang digunakan. Blowfish pada strategi implementasi yang tepat akan lebih optimal, dapat berjalan pada memori kurang dari 5 KB dan kesederhanaan pada algoritmanya.[8]. Algoritma blowfish juga pernah di buat sebagai landasan dalam mengamankan data seluler di cloud menggunakan kriptografi, di mana algoritma Elliptic Curve Cryptography dan Blowfish terintegrasi untuk memberikan otentikasi dan kerahasiaan.[9], oleh karena itu kedua algoritma ini layak untuk dicompare dalam hal rasio kecepatan dan alokasi memori, dimana memang hal ini sangat menjadi focus dalam dunia kriptografi. Dalam penelitian kali ini difocuskan untuk analisa perbandingan rasio kecepatan dan alokasi memori dari setiap algoritma tersebut.

Sekema Algoritma Kriptografi Simeteris

Symmetric algorithm atau disebut *juga secret key algorithm* adalah algoritma yang kunci enkripsinya dapat dihitung dari kunci dekripsi dan begitu pula sebaliknya, kunci dekripsi dapat dihitung dari kunci enkripsi. Pada sebagian besar *symmetric algorithm* kunci enkripsi dan kunci dekripsi adalah sama. *Symmetric algorithm* memerlukan kesepakatan antara pengirim dan penerima pesan pada suatu kunci sebelum dapat berkomunikasi secara aman. Keamanan *symmetric algorithm* tergantung pada rahasia kunci. Pemecahan kunci berarti memungkinkan setiap orang dapat mengenkripsi dan mendekripsi pesan dengan mudah.[10]

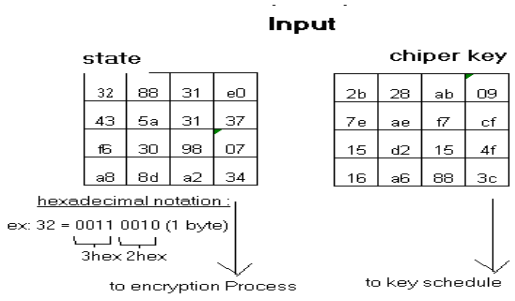
Symmetric algorithm dapat dikelompokkan menjadi dua jenis, yaitu *stream cipher* dan *block cipher*, dan akan dijelaskan sebagai berikut :



Gambar 1. *Sistem Stream Cipher*

Sekema Algoritma AES

Sebelum membuat perancangan aplikasi AES, terdapat analisa bagaimana proses enkripsi sampai pendekripsian kembali. Berikut ini adalah contoh penerapan proses enkripsi AES lihat. Pada rounds pertama *plaintext* dan *key* yang bernotasi *hexadecimal* di XOR.

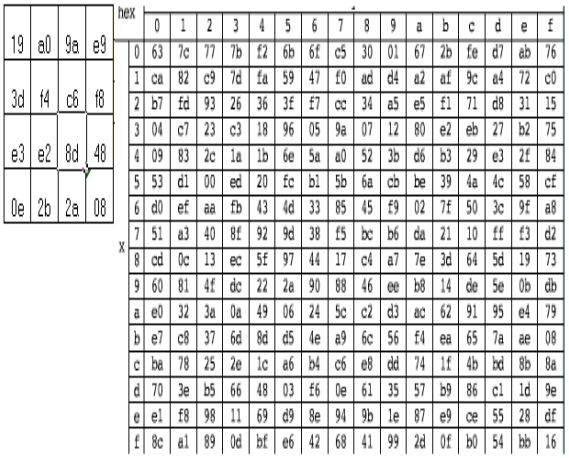


Gambar 2. *Elemen state dan kunci dalam notasi HEX*

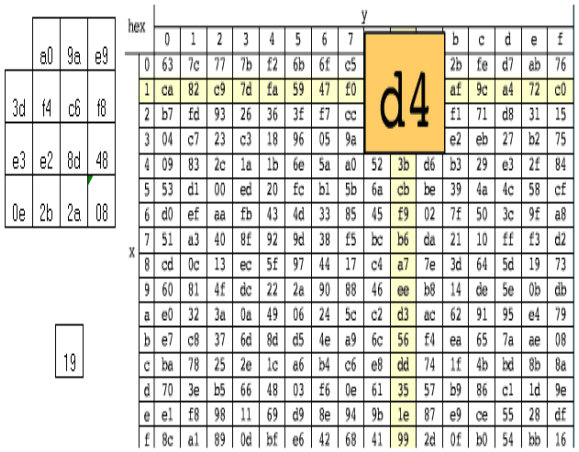
Input dan output dari algoritma AES terdiri dari urutan data sebesar 128 bit. Urutan data yang sudah terbentuk dalam satu kelompok 128 bit tersebut disebut juga sebagai blok data atau plaintext yang nantinya akan dienkripsi menjadi ciphertext. AES mempunyai kunci 128, 192 dan 256 bit sehingga berbeda dengan panjang dari putaran Rijandael. AES 128 bit menggunakan panjang kunci 4 kata yang setiap katanya terdiri dari 32 bit sehinnga total kunci 128 bit, ukuran blok teks asli 128 bit dan putaran 10 kali.

Seluruh byte dalam algoritma AES diinterpretasikan sebagai elemen finite field. Elemen finite field ini dapat dikalikan dan dijumlahkan, tetapi hasil dari penjumlahan dan perkalian elemen finite field sangat berbeda dengan hasil dari penjumlahan dan perkalian bilangan biasa.

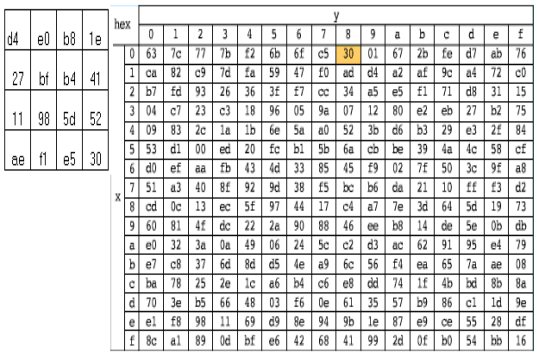
SubBytes() memetakan setiap byte dari *array state* dengan menggunakan *S-box.* Untuk lebih jelasnya dapat dilihat gambar 3.4 Input & S-box dan proses pemetaan input dengan S-box.



Gambar 4. *Input & S-box*



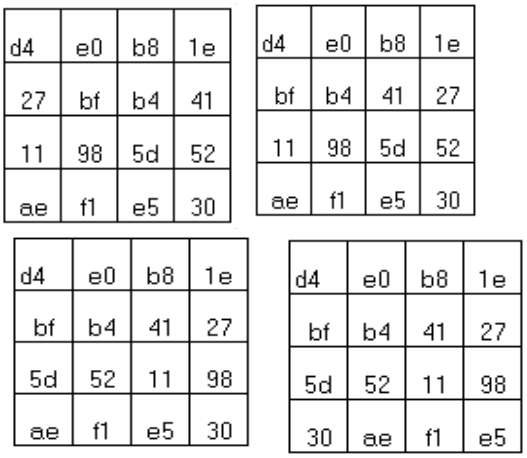
Gambar 5. *Proses pemetaan input dengan S-box*



Gambar 6 . *Input yang telah dipetakan S-box*

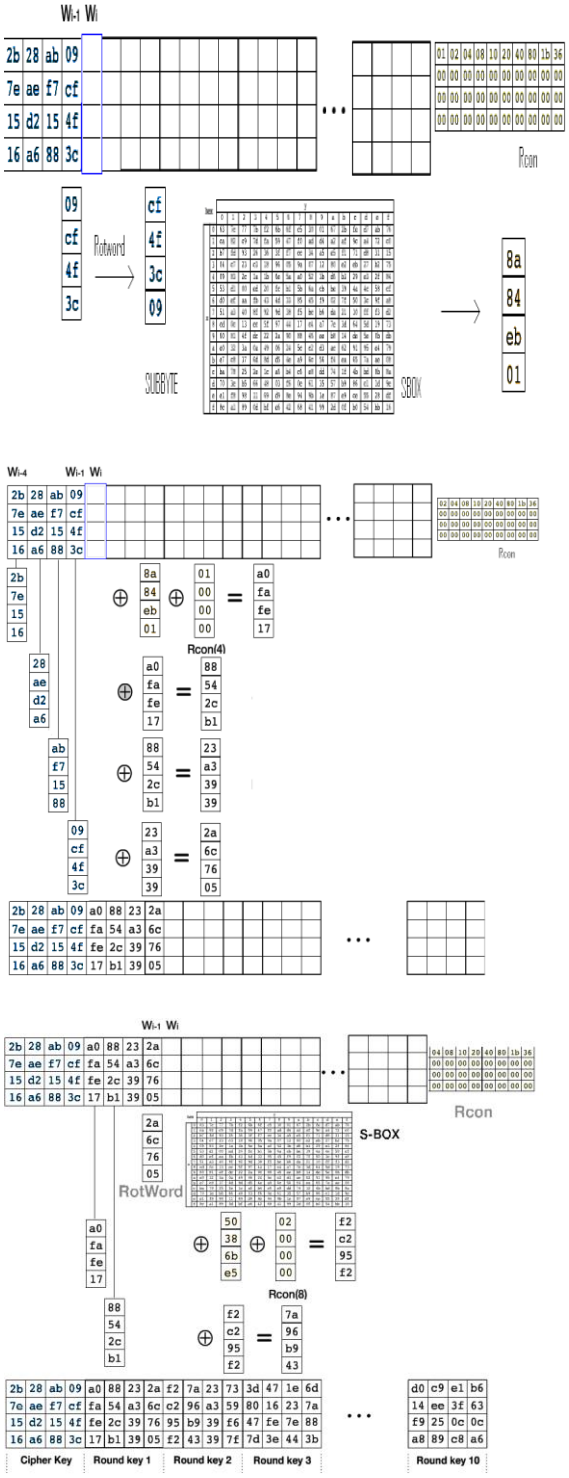
Transformasi ShiftRows

1. Transformasi *ShiftRows()* melakukan pergeseran secara *wrapping* (siklik) pada 3 baris terakhir dari *array state*.
2. Jumlah pergeseran bergantung pada nilai baris (*r*). Baris *r* = 1 digeser sejauh 1 *byte*, baris *r* = 2 digeser sejauh 2 *byte*, dan baris *r* = 3 digeser sejauh 3 *byte*. Baris *r* = 0 tidak digeser.



Gambar 7. *State awal ,rotate 1, rotate2 dan rotate 3*

Pada AES memiliki sistem penjadwalan kunci sehingga pada setiap perputaran atau rounds kunci selalu berubah- ubah seperti pada gambar 8 Penjadwalan kunci.



Gambar 8. *Penjadwalan kunci*

Hasil Penelitian

A. ParamaterAnalisis

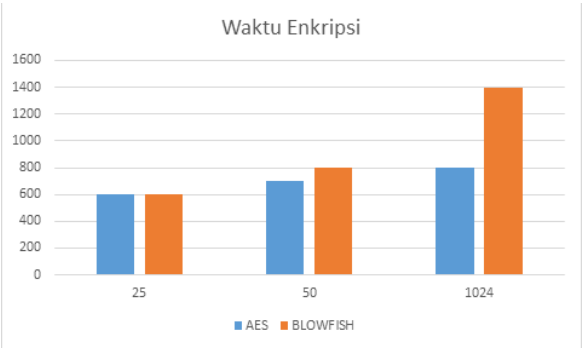
Masing-masing teknik enkripsi memiliki masing-masing kelebihan dan kelemahannya. Untuk menerapkan algoritma kriptografi pada aplikasi, kita harus memiliki pengetahuan mengenai kinerja, kekuatan dan kelemahan dari algoritma. Oleh karena itu, algoritma ini harus dianalisis berdasarkan beberapa fitur. Dalam tulisan ini, analisis dilakukan dengan metrik berikut di mana cryptosystems dapat dibandingkan dijelaskan di bawah ini:

1. Waktu Enkripsi
   Waktu yang dibutuhkan untuk mengubah plaintext menjadi ciphertext. Waktu enkripsi tergantung pada ukuran kunci, ukuran dan blok plainteks. Dalam percobaan, kami telah mengukur waktu enkripsi dalam milidetik. Waktu enkripsi berdampak pada kinerja enkripsi. Waktu enkripsi yang lebih sedikit adalah bukti algoritma yang efektif dan efisien.

2. Waktu Dekripsi
   Waktu untuk mengembalikan plaintext dari ciphertext disebut waktu dekripsi. Waktu dekripsi diharapkan mirip dengan waktu enkripsi untuk membuat algoritma responsif dan cepat. Waktu dekripsi berdampak pada kinerja sistem. Dalam percobaan, waktu yang digunakan untuk mengukur adalah milidetik

3. Alokasi Penggunaan Memory
   Teknik enkripsi yang berbeda membutuhkan ukuran memori yang berbeda untuk setiap algoritma. Kebutuhan memori ini tergantung pada jumlah operasi yang harus dilakukan oleh algoritma, ukuran kunci yang digunakan, iterasi yang digunakan dan jenis operasi. Penggunaan memory yang lebih sedikit membukikan alokasi yang dibutuhkan algoritma tersebut lebih kecil dan lebih efisien

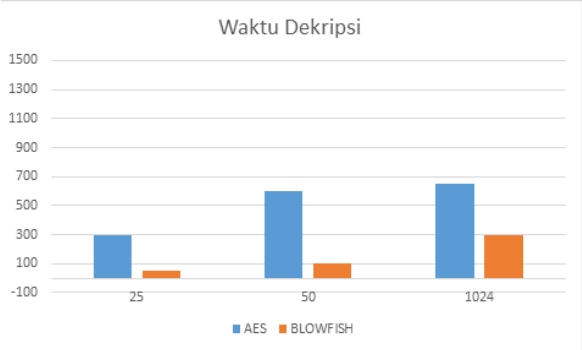
B. Hasil Rasio Kecepatan Algoritma AES dan Blowfish



Gambar 9. *Waktu Enkripsi Kedua Algoritma Kriptografi Simetri*

Pada gambar 9 ditunjukan pada ukuran 25 kb waktu yang dibutuhkan sama. Dengan

bertambahnya ukuran bytenya algoritma blowfish menunjukan peningkatan waktu yang lebih banyak dibandingkan algoritma AES.



Gambar 10. *Waktu Dekripsi Kedua Algoritma Kriptografi Simetri*

Pada grafik diatas, proses dekripsi pada ukuran 25 kb dibutuhkan waktu 300 milisecond untuk algoritma AES sedangkan untuk algoritma Blowfish dibutuhkan waktu yang lebih sedikit. Sehingga dapat dibuktikan bahwa pada proses dekripsi algoritma yang lebih efisien adalah algoritma Blowfish.

C. Hasil Pengujiian Alokasi Memory Algoritma AES dan Blowfish

Tabel 1. *Alokasi Memory Setiap Algoritma*

Algoritma	Penggunaan Memory (kb)
AES	14.7
Blowfish	9.38

Pada table penggunaan memory untuk setiap algoritma ditunjukkan bahwa algoritma AES lebih tinggi yakni 14.7 dibandingkan Blowfish yang hanya menggunakan 9.38

D. Hasil Analisa

Dalam hal kecepatan dengan mengesampingkan faktor yang menjadikan hal tersebut maka algoritma AES lebih cepat untuk melakukan enkripsi plaint text bila dibandingkan dengan Algoritma Blowfish, dikarenakan dalam algoritma AES panjang chiper text mencapai 128 bite dimana 128 bite dibagi menjadi 4 block, yang masing-masing blok memiliki panjang 32 bite, sedangkan Blowfish memiliki panjang chiper text mulai dari 32 sampai 448 bite, dimana panjang tersebut minimal 64 bite, inilah yang menyebankan algoritma AES dalam hal kecepatan enkripsi menjadi lebih unggul.

Namun berbeda dengan hasil kecepatan dalam dekripsi yakni algoritma Blowfish lebih cepat dibandingkan dengan algoritma AES dikarenakan hasil dari enkripsi algoritma AES lebih panjang dibandingkan dengan algoritma Blowfish, berangkat dari masalah tersebut sudah bisa disimpulkan bahwa algoritma blowfish akan lebih cepat dalam hal dekripsi dikarenakan hasil chiper text lebih pendek.

Sedangkan hasil ujicoba dari kedua algoritma dalam hal alokasi memory ternyata dari hasil percobaan yang dilakukan untuk algoritma AES lebih banyak memakan ruang penyimpanan dikarenakan jumlah putaran yang dihasilkan yakni matriks 4x4 sebanyak 10 kali iterasi, dan selanjutnya dilakukan permutasi dan subtitusi sehingga ini membutuhkan banyak ruang dalam pengimplementasiannya, berbeda dengan algoritma blowfish dimana untuk hal alokasi memori tidak begitu membutuhkan banyak ruang dikarenakan setiap panjang dari chiper text yang dihasilkan dibagi 64bite tentu hal ini akan memberikan sedikit blok atau sedikit ruang penyimpanan yang di butuhkan.

Kesimpulan

Dari hasil ujicoba yang dilakukan untuk rasio kecepatan dan alokassi memory maka dapat disimpulkan bahwa algoritma kriptografi AES lebih unggul atau lebih cepat apabila ukuran atau size plaint text tersebut tidak begitu besar, dikarenakan untuk algoritma AES ukuran semakin kecil maka rasio kecepatan dalam hal enkripsi akan menjadi lebih cepat, menjadi sangat berbeda untuk algoritma Blowfish sendiri dimana untuk plaint text yang memiliki ukuran yang besar dapat di enkripsi dengan lebih cepat dibandingkan dengan AES namun untuk ukuran lebih kecil tentu Blowfish lebih lambat dalam hal tersebut, untuk alokasi memori dalam hal ini dari ujicoba yang dilakukan dapat ditarik kesimpulan bahwa AES lebih membutuhkan ruang penyimpanan yang lebih besar atau alokasi memory yang lebih besar bila dibandingkan dengan algoritma blowfish.

DAFTAR PUSTAKA

[1]M. Suresh and M. Neema, “Hardware Implementation of Blowfish Algorithm for the Secure Data Transmission in Internet of Things,” *Procedia Technology*, vol. 25, pp. 248–255, Jan. 2016.

[2]D. Smekal, J. Frolka, and J. Hajny, “Acceleration of AES Encryption Algorithm Using Field Programmable Gate Arrays,” *IFAC-PapersOnLine*, vol. 49, no. 25, pp. 384–389, Jan. 2016.

[3]D. Surian, “ALGORITMA KRIPTOGRAFI AES RIJNDAEL,” *TESLA Jurnal Teknik Elektro UNTAR*, vol. 8, no. 2, pp. 97–101, Oct. 2009.

[4]J. Sasongko, "Pengamanan Data Informasi menggunakan Kriptografi Klasik," *Dinamik - Jurnal Teknologi Informasi*, vol. 10, no. 3, 2005.

[5]U. Farooq and M. F. Aslam, "Comparative analysis of different AES implementation techniques for efficient resource usage and better performance of an FPGA," *Journal of King Saud University - Computer and Information Sciences*, vol. 29, no. 3, pp. 295–302, Jul. 2017.

[6]S. H. Putra, E. Santoso, S. Si, M. Kom, L. Muflikhah, and S. Kom, "IMPLEMENTASI ALGORITMA KRIPTOGRAFI ADVANCED ENDRYPTION STANDARD (AES) PADA KOMPRESI DATA TEKS," *Jurnal Ilmu Komputer Universitas Brawijaya*, 2013.

[7]Y. P. Astuti, E. H. Rachmawanto, and C. A. Sari, "OPTIMASI ENKRIPSI PASSWORD MENGGUNAKAN ALGORITMA BLOWFISH," *Techno.Com*, vol. 15, no. 1, pp. 15–21, 2016.

[8]S. Sitinjak, Y. Fauziah, and J. Juwairiah, "APLIKASI KRIPTOGRAFI FILE MENGGUNAKAN ALGORITMA BLOWFISH," *Seminar Nasional Informatika (SEMNASIF)*, vol. 1, no. 3, Jul. 2015.

[9]P. Patel, R. Patel, and N. Patel, "Integrated ECC and Blowfish for Smartphone Security," *Procedia Computer Science*, vol. 78, pp. 210–216, Jan. 2016.

[10]A. Rosyadi, "IMPLEMENTASI ALGORITMA KRIPTOGRAFI AES UNTUK ENKRIPSI DAN DEKRIPSI EMAIL," *TRANSIENT*, vol. 1, no. 3, pp. 63–67, Sep. 2012.