

**IMPLEMENTASI KRIPTOGRAFI AES-256 UNTUK *FILE CITRA BITMAP*
PADA *PRIVATE CLOUD SERVICE* DENGAN VERIFIKASI DAN
PENGAMANAN DATA**

SKRIPSI

diajukan untuk memenuhi bagian dari
syarat memperoleh gelar Sarjana Komputer
pada Departemen Pendidikan Ilmu Komputer
Program Studi Ilmu Komputer.



Oleh

Farah Wihda Imarah

1306312

**PROGRAM STUDI ILMU KOMPUTER
DEPARTEMEN PENDIDIKAN ILMU KOMPUTER
FAKULTAS PENDIDIKAN MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS PENDIDIKAN INDONESIA
BANDUNG
2020**

Farah Wihda Imarah, 2020
*IMPLEMENTASI KRIPTOGRAFI AES-256 UNTUK FILE CITRA BITMAP PADA PRIVATE CLOUD SERVICE
DENGAN VERIFIKASI DAN PENGAMANAN DATA*

Universitas Pendidikan Indonesia | repository.upi.edu | perpustakaan.upi.edu

**IMPLEMENTASI KRIPTOGRAFI AES-256 UNTUK *FILE CITRA BITMAP*
PADA *PRIVATE CLOUD SERVICE* DENGAN VERIFIKASI DAN
PENGAMANAN DATA**

Oleh
Farah Wihda Imarah

Sebuah skripsi yang diajukan untuk memenuhi salah satu syarat memperoleh gelar Sarjana
Komputer di Fakultas Pendidikan Matematika dan Ilmu Pengetahuan Alam

© Farah Wihda Imarah 2020
Universitas Pendidikan Indonesia
Februari 2020

Hak Cipta Dilindungi Oleh Undang-Undang
Skripsi ini tidak boleh diperbanyak seluruhnya atau sebagian,
dengan dicetak ulang, difotokopi, atau cara lainnya tanpa izin dari peneliti.

Farah Wihda Imarah, 2020
**IMPLEMENTASI KRIPTOGRAFI AES-256 UNTUK *FILE CITRA BITMAP* PADA *PRIVATE CLOUD SERVICE*
DENGAN VERIFIKASI DAN PENGAMANAN DATA**

Universitas Pendidikan Indonesia | repository.upi.edu | perpustakaan.upi.edu

LEMBAR PENGESAHAN
IMPLEMENTASI KRIPTOGRAFI AES-256 UNTUK *FILE CITRA BITMAP*
PADA *PRIVATE CLOUD SERVICE* DENGAN VERIFIKASI DAN
PENGAMANAN DATA

Oleh:

Farah Wihda Imarah
1306312

DISETUJUI DAN DISAHKAN OLEH:

Pembimbing 1

Drs. Eka Fitrajaya Rahman, M.T

NIP. 196402141990031003

Pembimbing 2

Eddy Prasetyo Nugroho, M.T

NIP. 197505152008011014

Mengetahui,

Kepala Departemen Pendidikan Ilmu Komputer

Dr. Rani Megasari, M.T

Farah Wihda Imarah, 2020
IMPLEMENTASI KRIPTOGRAFI AES-256 UNTUK *FILE CITRA BITMAP* PADA *PRIVATE CLOUD SERVICE*
DENGAN VERIFIKASI DAN PENGAMANAN DATA

Universitas Pendidikan Indonesia | repository.upi.edu | perpustakaan.upi.edu

NIP. 198705242014042002

**IMPLEMENTASI KRIPTOGRAFI AES-256 UNTUK FILE CITRA BITMAP
PADA PRIVATE CLOUD SERVICE DENGAN VERIFIKASI DAN
PENGAMANAN DATA**

Oleh
Farah Wihda Imarah – farah.wihda.imarah@student.upi.edu
1306312

ABSTRAK

Perkembangan teknologi yang bergantung pada suatu Cloud terutama pada Private Cloud diperlukan pengelolaan identitas dan otentikasi data atau informasi. Salah satu informasi yang rawan diamankan adalah File Citra Bitmap. File Citra Bitmap adalah representasi gambar dari sebuah objek yang lebih bagus dari format JPEG dan mudah dipetakan dalam bit. Dalam menjaga keamanan data informasi terdapat cabang ilmu dalam pengembangannya seperti kriptografi. Advanced Encryption Standard (AES) merupakan algoritma Kriptografi yang dapat digunakan untuk mengamankan data dimana algoritmanya adalah blok chipertext simetrik yang dapat mengenkripsi (encipher) dan dekripsi (decipher) informasi. Pada penelitian ini, dibangun sebuah sistem enkripsi dan dekripsi File Citra Bitmap untuk menganalisis performa algoritma tersebut. Hasil analisa perbandingan penelitian Implementasi File Citra Bitmap pada Private Cloud dari dimensi piksel (px) gambar dengan lama waktu eksekusi enkripsi-dekripsi yang didapatkan pada sistem ini adalah algoritma AES menghasilkan keamanan cipher image yang lebih baik namun membutuhkan waktu proses yang lebih lama enkripsi 0.0040sc dan dekripsi 0.003sc dan menguji keamanan hasil enkripsi dan dekripsi pada web tool encrypt-decrypt yang tidak bisa didecrypt.

Kata kunci: File Citra Bitmap, Private Cloud, AES-256, Kriptografi, Private Cloud

Farah Wihda Imarah, 2020
IMPLEMENTASI KRIPTOGRAFI AES-256 UNTUK FILE CITRA BITMAP PADA PRIVATE CLOUD SERVICE
DENGAN VERIFIKASI DAN PENGAMANAN DATA

Universitas Pendidikan Indonesia | repository.upi.edu | perpustakaan.upi.edu

IMPLEMENTASI KRIPTOGRAFI AES-256 UNTUK FILE CITRA BITMAP PADA PRIVATE CLOUD SERVICE DENGAN VERIFIKASI DAN PENGAMANAN DATA

By

Farah Wihda Imarah – farah.wihda.imarah@student.upi.edu

1306312

ABSTRACT

The development of technologies that depend on a Cloud, especially on Private Cloud, requires the management of identity and authentication of data or information. One of the information that is vulnerable to safekeeping is the Bitmap Image File. A Bitmap Image File is an image representation of an object that is better than the JPEG format and is easy to map in bits. In maintaining the security of information data there are branches of science in its development such as cryptography. Advanced Encryption Standard (AES) is a Cryptographic algorithm that can be used to generate data where the algorithm is a symmetric ciphertext block that can encrypt (encipher) and decrypt (decipher) information. In this research, an encryption and decryption file for Bitmap Image was built to analyze the performance of the algorithm. Results of comparative analysis of research Implementation of a Bitmap Image File on a Private Cloud from the pixel dimensions (px) of an image with the encryption-decryption execution time obtained on this system is that the AES algorithm produces better cipher image security but requires a longer processing time of encryption 0.0040sc and decryption 0.003sc and test the security of the encryption and decryption results on the encrypt-decrypt web tool that cannot be decrypted.

Keywords: Bitmap Image Files, Private Cloud, AES-256, Cryptography, Private Cloud.

Farah Wihda Imarah, 2020

IMPLEMENTASI KRIPTOGRAFI AES-256 UNTUK FILE CITRA BITMAP PADA PRIVATE CLOUD SERVICE DENGAN VERIFIKASI DAN PENGAMANAN DATA

Universitas Pendidikan Indonesia | repository.upi.edu | perpustakaan.upi.edu

DAFTAR PUSTAKA

ABSTRAK.....	iv
ABSTRACT	5
KATA PENGANTAR.....	Error! Bookmark not defined.
UCAPAN TERIMA KASIH	Error! Bookmark not defined.
DAFTAR PUSTAKA	6
DAFTAR GAMBAR	Error! Bookmark not defined.
DAFTAR TABEL.....	Error! Bookmark not defined.
DAFTAR LAMPIRAN	Error! Bookmark not defined.
BAB I PENDAHULUAN	Error! Bookmark not defined.
1.1 Latar Belakang Penelitian	Error! Bookmark not defined.
1.2 Rumusan Masalah Penelitian.....	Error! Bookmark not defined.
1.3 Tujuan Penelitian	Error! Bookmark not defined.
1.4 Batasan Masalah	Error! Bookmark not defined.
1.5 Sistematika Penulisan.....	Error! Bookmark not defined.
BAB II KAJIAN PUSTAKA	Error! Bookmark not defined.
2.1 Rangkuman Penelitian Terdahulu.....	Error! Bookmark not defined.
2.2 Cloud Computing	Error! Bookmark not defined.
2.3 Layanan Cloud Computing.....	Error! Bookmark not defined.
2.4 Cloud Service	Error! Bookmark not defined.
2.5 Deployment Model Cloud Computing	Error! Bookmark not defined.
2.6 Private Cloud Service.....	Error! Bookmark not defined.
2.7 Kriptografi	Error! Bookmark not defined.
2.8 Sejarah Kriptografi.....	Error! Bookmark not defined.
2.9 Tujuan Kriptografi	Error! Bookmark not defined.
2.10 Advanced Encryption Standard (AES).....	Error! Bookmark not defined.
2.11 Perbedaan AES 128, 192, 256	Error! Bookmark not defined.

Farah Wihda Imarah, 2020

IMPLEMENTASI KRIPTOGRAFI AES-256 UNTUK FILE CITRA BITMAP PADA PRIVATE CLOUD SERVICE DENGAN VERIFIKASI DAN PENGAMANAN DATA

2.11.1	Proses Enkripsi AES	Error! Bookmark not defined.
2.11.2	Proses Dekripsi AES.....	Error! Bookmark not defined.
2.12	File Citra Bitmap	Error! Bookmark not defined.
2.13	Format Bitmap	Error! Bookmark not defined.
2.14	PHP.....	Error! Bookmark not defined.
2.15	Bitwise SSH.....	Error! Bookmark not defined.
BAB III METODE PENELITIAN		Error! Bookmark not defined.
3.1	Desain Penelitian	Error! Bookmark not defined.
3.1.1	Tahap Awal Penelitian	Error! Bookmark not defined.
3.1.2	Studi Literatur.....	Error! Bookmark not defined.
3.1.3	Tahapan Implementasi dan Pengujian ..	Error! Bookmark not defined.
3.1.4	Tahapan Dokumentasi.....	Error! Bookmark not defined.
3.2	Metode Penelitian	Error! Bookmark not defined.
3.2.1	Metode Pengumpulan Data	Error! Bookmark not defined.
3.2.2	Metode Pengembangan Perangkat Lunak	Error! Bookmark not defined.
3.3	Alat dan Bahan Penelitian	Error! Bookmark not defined.
3.3.1	Alat Penelitian	Error! Bookmark not defined.
3.3.2	Bahan Penelitian	Error! Bookmark not defined.
BAB IV HASIL PENELITIAN DAN PEMBAHASAN		Error! Bookmark not defined.
4.1	Studi Literatur.....	Error! Bookmark not defined.
4.2	Pembahasan Penelitian.....	Error! Bookmark not defined.
4.2.1	Rancangan Perangkat Lunak	Error! Bookmark not defined.
4.2.2	Alur Enkripsi dan Dekripsi <i>File Citra Bitmap</i>	Error! Bookmark not defined.
4.2.3	Batasan Perangkat Lunak	Error! Bookmark not defined.
4.2.4	Proses Operasional Perangkat Lunak....	Error! Bookmark not defined.
4.3	Implementasi	Error! Bookmark not defined.
4.3.1	Implementasi Modul Program.....	Error! Bookmark not defined.
4.3.2	Implementasi Antarmuka	Error! Bookmark not defined.
4.3.3	Implementasi AES-256.....	Error! Bookmark not defined.
4.4	Pengujian	Error! Bookmark not defined.

Farah Wihda Imarah, 2020

IMPLEMENTASI KRIPTOGRAFI AES-256 UNTUK FILE CITRA BITMAP PADA PRIVATE CLOUD SERVICE DENGAN VERIFIKASI DAN PENGAMANAN DATA

4.5	Pembahasan Implementasi Kriptografi AES-256 Untuk File Citra Bitmap Pada Private Cloud Service	Error! Bookmark not defined.
4.5.1	Hasil Enkripsi	Error! Bookmark not defined.
4.5.2	Pengujian	Error! Bookmark not defined.
4.6	Analisa Hasil Uji	Error! Bookmark not defined.
4.6.1	Pengaruh Dimensi File Citra Bitmap	Error! Bookmark not defined.
4.6.2	Empat Bentuk Keamanan Kriptografi...	Error! Bookmark not defined.
BAB V KESIMPULAN DAN SARAN		Error! Bookmark not defined.
5.1	Kesimpulan	Error! Bookmark not defined.
5.2	Saran	Error! Bookmark not defined.
DAFTAR PUSTAKA		9
LAMPIRAN		Error! Bookmark not defined.

DAFTAR PUSTAKA

- Alessio, C. (2018). *Animal pictures of 10 different categories taken from google images*.
<https://www.kaggle.com/Alessiocorrado99/Animals10>.
<https://www.kaggle.com/alessiocorrado99/animals10>
- Arora, M. (2012). *How secure is AES against brute force attacks*.
- Attar, N., & Shahin, M. (2018). A Proposed Architecture for Data Security in Cloud Storage Space. *Journal of Biostatistics and Biometric Applications*, 3(2), 1–7.
- Bitvise. (2020). *About SSH / Bitvise*. <https://www.bitvise.com/ssh2>
- Bonzo, B. P., & Lin, K. (2019). *DEBUGGING IN A PRIVATE CLOUD ENVIRONMENT*. 2.
- Budiyanto, A. (2012). *Pengantar Cloud Computing*. 10. <http://www.cloudindonesia.or.id/wp-content/uploads/2012/05/E-Book-Pengantar-Cloud-Computing-R1.pdf>
- Daemen, J., & Vincent, R. (2001). Reijndael: The Advanced Encryption Standard. *Dr. Dobb's Journal: Software Tools for the Professional Programmer*, 26(3), 137–139.
- Delfin, Prof, S., B. Sai, R., J.V, M., Lakshmi, K., & Sharma, S. (2018). CLOUD DATA SECURITY USING AES ALGORITHM. *International Research Journal of Engineering and Technology (IRJET) e-ISSN: 05(10)*, 1189–1192.
- Fachry, M., Kusyanti, A., & Amron, K. (2018). Pengamanan Data pada Media Penyimpanan Cloud Menggunakan Teknik Enkripsi dan Secret Sharing. *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer (J-PTIHK) Universitas Brawijaya*, 2(11), 4863–4869.
- Gao, H., Hu, J., Huang, T., Wang, J., & Chen, Y. (2013). Security Issues in Online Social Networks. *Communications in Computer and Information Science*, 361 CCIS, 740–746. <https://doi.org/10.1007/978-3-642-36321-4-69>
- Gayathri, K. S., Thomas, T., & Jayasudha, J. (2012). Security Issues Of Media Sharing In Social Cloud. *Procedia Engineering*, 38, 3806–3815. <https://doi.org/10.1016/j.proeng.2012.06.436>
- Group, T. P. (2020). *What is PHP?* <https://www.php.net/manual/en/intro-whatish.php>
- Insiders, C. (2019). Cloud Security Report (ISC)2. *Cloud Security Report*.
- Jana, B., Poray, J., Mandal, T., & Kule, M. (2018). A multilevel encryption technique in cloud security. *Proceedings - 7th International Conference on Communication Systems and Network Technologies, CSNT 2017*, 220–224. <https://doi.org/10.1109/CSNT.2017.8418541>
- Kacha, L., & Zitouni, A. (2018). *An Overview on Data Security in Cloud Computing*. 661(September), 67618. <https://doi.org/10.1007/978-3-319-67618-0>
- Kumar, K. V. K. M. (2014). Software as a Service for Efficient Cloud Computing. *International*

Farah Wihda Imarah, 2020

IMPLEMENTASI KRIPTOGRAFI AES-256 UNTUK FILE CITRA BITMAP PADA PRIVATE CLOUD SERVICE DENGAN VERIFIKASI DAN PENGAMANAN DATA

Universitas Pendidikan Indonesia | repository.upi.edu | perpustakaan.upi.edu

Journal of Research in Engineering and Technology, 7, 10.

- Mell, P. (NIST), & Grance, T. (2011). The NIST Definition of Cloud Computing. *Special Publication 800-145*, 269–274.
- Metz, R. (2010). *Cloud Computing Explained*.
- Munir, R. (2006). *Pengantar Kriptografi*. ITB.
- Munir, R. (2011). Algoritma Enkripsi Citra dengan Pseudo One-Time Pad yang Menggunakan Sistem Chaos. *Konferensi Nasional Informatika*, 12–16.
- Murni, A., & Setiawan, S. (1992). *Pengantar Pengolahan Citra*. PT Elex Media Komputindo.
- Pabokory, F. N., Astuti, I. F., & Kridalaksana, A. H. (2016). IMPLEMENTASI KRIPTOGRAFI PENGAMANAN DATA PADA PESAN TEKS, ISI FILE DOKUMEN, DAN FILE DOKUMEN MENGGUNAKAN ALGORITMA ADVANCED ENCRYPTION STANDARD. *Informatika Mulawarman : Jurnal Ilmiah Ilmu Komputer*, 10(1), 20. <https://doi.org/10.30872/jim.v10i1.23>
- Potdar, V., & Chang, E. (2015). Disguising Text Cryptography using Image Cryptography. *Audio*, November.
- Priyanto, B. (1992). *Dasar-dasar Pengolahan Citra*. Elexmedia Komputindo.
- Raj, G., Kesireddi, R. C., & Gupta, S. (2015). Enhancement of Security Mechanism for Confidential Data using AES-128, 192 and 256 bit Encryption in Cloud. *Proceedings on 2015 1st International Conference on Next Generation Computing Technologies, NGCT 2015, September*, 374–378. <https://doi.org/10.1109/NGCT.2015.7375144>
- Ramgovind, S., Mariki M, E., & Smith, E. (2017). The Management of Security in Cloud Computing. *Education for Information*, 33(2), 75–88. <https://doi.org/10.3233/EFI-170990>
- Sommerville, I. (2011). *Software Engineering 9TH Edition*.
- Symantec. (2019). Adapting to the New Reality of Evolving Cloud Threats. *Cloud Security Threat Report (CSTR)*, 1(June 2019).