

**TUGAS AKHIR – IF184802**

**Implementasi Perangkat Lunak Audit Keamanan Cloud dengan Data Terenkripsi**

MUHAMMAD FAJRI SALAM

NRP 05111540000099

Dosen Pembimbing I

Ir. MUCHAMMAD HUSNI, M.Kom.

Dosen Pembimbing II

HENNING TITI CIPTANINGTYAS, S.Kom., M.Kom.

DEPARTEMEN INFORMATIKA

Fakultas Teknologi Informasi dan Komunikasi

Institut Teknologi Sepuluh Nopember

Surabaya 2019



**TUGAS AKHIR – IF184802**

**Implementasi Perangkat Lunak Audit Keamanan Cloud dengan Data Terenkripsi**

**MUHAMMAD FAJRI SALAM**

**NRP 05111540000099**

**Dosen Pembimbing I**

**Ir. MUCHAMMAD HUSNI, M.Kom.**

**Dosen Pembimbing II**

**HENNING TITI CIPTANINGTYAS, S.Kom., M.Kom.**

**DEPARTEMEN INFORMATIKA**

**Fakultas Teknologi Informasi dan Komunikasi**

**Institut Teknologi Sepuluh Nopember**

**Surabaya 2019**

***(Halaman ini sengaja dikosongkan)***

******

**UNDERGRADUATE THESIS – IF184802**

**Secure Cloud Auditing Over Encrypted Data Software Implementation**

**MUHAMMAD FAJRI SALAM**

**NRP 05111540000099**

First Advisor

Ir. MUCHAMMAD HUSNI, M.Kom.

**Second Advisor**

**HENNING TITI CIPTANINGTYAS, S.Kom., M.Kom.**

**INFORMATICS DEPARTMENT**

**Faculty of Information Communication and Technology**

**Institut Teknologi Sepuluh Nopember**

**Surabaya 2019**

***(Halaman ini sengaja dikosongkan)***

**LEMBAR PENGESAHAN**

**Implementasi Perangkat Lunak Audit Keamanan Cloud dengan Data Terenkripsi**

**TUGAS AKHIR**

Diajukan untuk Memenuhi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer

pada

Bidang Studi Arsitektur Jaringan Komputer

Program Studi S-1 Departemen Informatika

Fakultas Teknologi Informasi dan Komunikasi

Institut Teknologi Sepuluh Nopember

Oleh:

**MUHAMMAD FAJRI SALAM**

**NRP: 05111540000099**

Disetujui oleh Pembimbing tugas akhir:

1. Ir. MUCHAMMAD HUSNI, M.Kom. ..........................

(NIP. 19600221 198403 1 001) (Pembimbing 1)

1. HENNING TITI CIPTANINGTYAS,

S.Kom., M.Kom. ..........................

(NIP. 19840708 201012 2 004) (Pembimbing 2)

**SURABAYA**

**JUNI, 2019**

***(Halaman ini sengaja dikosongkan)***

**Implementasi Perangkat Lunak Audit Keamanan Cloud dengan Data Terenkripsi**

|  |  |  |
| --- | --- | --- |
| **Nama Mahasiswa** | **:** | **MUHAMMAD FAJRI SALAM** |
| **NRP** | **:** | **05111540000099** |
| **Departemen** | **:** | **Informatika FTIK ITS** |
| **Dosen Pembimbing 1** | **:** | **Ir. MUCHAMMAD HUSNI, M.Kom.** |
| **Dosen Pembimbing 2** | **:** | **HENNING TITI CIPTANINGTYAS, S.Kom., M.Kom.** |

# Abstrak

Komputasi awan adalah teknologi populer yang memungkinkan untuk mengakses data melalui Internet yang bahkan dapat menyimpan data sebagai pengganti penyimpanan lokal. Cloud memungkinkan pengguna untuk menyimpan data mereka di cloud tanpa perlu khawatir akan keakuratan dan keandalannya. Namun menyimpan data di cloud menimbulkan tantangan keamanan tertentu. Mengalihdayakan data di cloud menyebabkan pemilik data kehilangan kontrol fisik atas data mereka. Penyedia Layanan Cloud tertentu dapat beroperasi secara tidak jujur ​​dengan data pengguna cloud, mereka dapat mengakses data dari cloud dan menjualnya kepada pihak ketiga untuk mendapatkan keuntungan. Jadi, meskipun *outsourcing* data di cloud tidak mahal dan mengurangi kompleksitas penyimpanan dan pemeliharaan berdurasi lama, setidaknya ada jaminan integritas data, privasi, keamanan, dan ketersediaan di server cloud.

Tugas Akhir ini akan berfokus pada strategi verifikasi integritas untuk data *outsourcing*. Skema yang diusulkan adalah menggabungkan mekanisme enkripsi dengan verifikasi integritas. Skema enkripsi yang digunakan di sini adalah algoritma kriptografi AES-256 dan fungsi *hash* SHA-256 yang digunakan untuk memastikan kebenaran penyimpanan data pada server yang tidak terpercaya

***Kata kunci : Cloud Computing, AES-256, SHA-256, TPA.***

**Implementation of Secure Cloud Auditing Over Encrypted Data Software**

**Student’s Name : MUHAMMAD FAJRI SALAM**

**Student’s ID : 05111540000099**

**Department : Informatika FTIK-ITS**

**First Advisor : Ir. MUCHAMMAD HUSNI, M.Kom**

|  |  |  |
| --- | --- | --- |
| **Second Advisor** | **:** | **HENNING TITI CIPTANINGTYAS, S.Kom., M.Kom.** |

# Abstract

*Cloud computing is a popular technology which permits storing and accessing data over Internet instead of storing it on local machine’s hard drive. Cloud enables users to store their data on cloud without fearing about its accuracy and reliability. However storing data on cloud imposes certain security challenges. Outsourcing data in cloud result in data owners losing physical control over their data. Certain Cloud Service Providers may operate dishonestly with the cloud users’ data, they may sneak the data from cloud and sell it to third parties in order to earn profit. Thus even though outsourcing data on cloud is inexpensive and reduces long duration storage and maintenance complexity, there is least assurance of data integrity, privacy, security and availability on cloud servers. A number of solutions have been recommended to solve the security issues in cloud.*

*This undergraduate thesis focuses on the integrity verification strategy for outsourced data. The proposed scheme combines the encrypting mechanism along with integrity verification strategy. The encrypting scheme used here is cryptographic algorithm like AES-256 and SHA-256 hash function is employed for ensuring data storage correctness on untrusted server*

***Kata kunci : Cloud Computing, AES-256, SHA-256, TPA.***

# KATA PENGANTAR



Puji syukur kepada Allah Yang Maha Esa atas segala karunia dan rahmat-Nya sehingga penulis dapat menyelesaikan tugas akhir yang berjudul

***“*IMPLEMENTASI PERANGKAT LUNAK AUDIT KEAMANAN CLOUD DENGAN DATA TERENKRIPSI”.**

Harapan dari penulis, semoga apa yang tertulis di dalam buku tugas akhir ini dapat bermanfaat bagi pengembangan ilmu pengetahuan saat ini dan ke depannya, serta dapat memberikan kontribusi yang nyata.

Dalam pelaksanaan dan pembuatan tugas akhir ini tentunya sangat banyak bantuan yang penulis terima dari berbagai pihak, tanpa mengurangi rasa hormat penulis ingin mengucapkan terima kasih sebesar-besarnya kepada:

1. Allah SWT. dan Nabi Muhammad SAW. yang telah membimbing penulis selama hidup.
2. Keluarga penulis (Ayah, Ibu, Mas Dicky, Dina, Aldan, dan keluarga penulis yang lain) yang selalu memberikan dukungan baik berupa doa, moral, dan material yang tak terhingga kepada penulis, sehingga penulis dapat menyelesaikan tugas akhir ini.
3. Bapak Ir. Muchammad Husni, M.Kom. selaku Dosen Pembimbing penulis yang telah membimbing, memberikan nasihat, dan memotivasi penulis sehingga penulis dapat menyelesaikan tugas akhir ini.
4. Bapak Dr.Eng. Darlis Herumurti, S.Kom., M.Kom. selaku kepala Departemen Informatika ITS.
5. Bapak dan Ibu Dosen yang telah memberikan ilmunya selama penulis berkuliah di Informatika ITS.
6. Teman-teman penulis Developer Arya-Fajar Production (Achmadaniar A.R, Hikmawan Cahya Putra dan Fuad Dary Rosyadi) yang selalu memberikan semangat secara tidak langsung kepada penulis, selalu memberikan hiburan, selalu menemani hari-hari penulis saat senang maupun susah, dan juga menjadi keluarga baru penulis saat berkuliah di Departemen Informatika ITS.
7. Teman-teman KP PLN Hero, Purina, Huda, dan Eritha yang telah menemani kerja praktik penulis dan mau mem-*back up* penulis dikala sakit.
8. Teman-teman penulis Ronald, Rezky, Ufa dan lain-lain yang telah mewarnai kehidupan penulis.
9. Teman-teman dari keluarga besar Laboratorium NCC (Hero, Sisil, Yoga, Dely, Zulfa, Ubut, Zayn, Ical, Azki, Nuza, Akmal, Siraj, Adin, Wasil) yang telah menemani, memberi semangat, doa, serta hiburan dikala penulis sedang jenuh saat pengerjaan tugas akhir ini.
10. Teman-teman dari Kabinet Semangat Berpadu BEM FTIK periode 2017/2018 yang telah mewarnai hari-hari penulis dan mengajarkan makna ikhlas dan sabar, yang sudah berjuang bersama penulis selama kurang lebih satu setengah tahun, yang terkadang membuat penulis kesal namun tidak apa-apa.
11. Teman-teman EA Bahagia BEM FTIf Presisi Bermanfaat yang telah menjadi teman organisasi penulis, menambah rumah baru bagi penulis.
12. Teman-teman Hublu Inspirasi HMTC Inspirasi yang telah menjadi teman berhimpun penulis.
13. Teman-teman Pemandu Phoenix yang telah menjadi rekan mandu penulis selama berkiprah di kepemanduan fakultas.
14. Teman-teman Saman TC yang telah memberikan hiburan, mengajarkan penulis menari saman, dan menjadikan penulis lebih bijak dalam menghadapi adik tingkat.
15. Teman-teman SSL yang telah menjadikan Minggu pagi penulis lebih bermanfaat.
16. Teman-teman pejuang SW 119 yang selalu memberikan informasi penting dan semangat kepada penulis untuk menyelesaikan tugas akhir.
17. Teman-teman angkatan 2015 (Masamalas) yang sudah menjadi saksi hidup perjalanan karir penulis selama berkuliah di Informatika ITS.
18. Untuk orang-orang yang tidak dapat disebutkan satu persatu oleh penulis dan pembaca buku tugas akhir ini.

Penulis telah berusaha sebaik-baiknya dalam menyusun tugas akhir ini. Namun, penulis memohon maaf apabila terdapat kekurangan, kesalahan maupun kelalaian yang telah penulis lakukan. Kritik dan saran yang membangun dapat disampaikan sebagai bahan perbaikan selanjutnya. Tetap semangat dalam menjalani kehidupan, jangan menyerah, karena Allah masih ingin melihat kita berjuang. Semoga kita semua selalu diberi kebahagiaan lahir dan batin dan kesuksesan dunia akhirat. Aamiin.

Surabaya, 7 Juni 2019

Muhammad Fajri Salam

***(Halaman ini sengaja dikosongkan)***

Contents

[LEMBAR PENGESAHAN v](#_Toc11116933)

[Abstrak vii](#_Toc11116934)

[Abstract ix](#_Toc11116935)

[KATA PENGANTAR x](#_Toc11116936)

[DAFTAR GAMBAR xv](#_Toc11116937)

[DAFTAR TABEL xvii](#_Toc11116938)

[KODE SUMBER xix](#_Toc11116939)

[BAB I PENDAHULUAN 1](#_Toc11116940)

[1.1 Latar Belakang 1](#_Toc11116941)

[1.2 Rumusan Masalah 1](#_Toc11116942)

[1.3 Batasan Permasalahan 1](#_Toc11116943)

[1.4 Tujuan 2](#_Toc11116944)

[1.5 Manfaat 2](#_Toc11116945)

[1.6 Metodologi 2](#_Toc11116946)

[1.6.1 Penyusunan Proposal Tugas Akhir 2](#_Toc11116947)

[1.6.2 Studi Literatur 3](#_Toc11116948)

[1.6.3 Perancangan Sistem 3](#_Toc11116949)

[1.6.4 Implementasi Sistem 3](#_Toc11116950)

[1.6.5 Pengujian. 3](#_Toc11116951)

[1.6.6 Penyusunan Buku 3](#_Toc11116952)

[1.7 Sistematika Penulisan Laporan 3](#_Toc11116953)

[BAB II TINJAUAN PUSTAKA 6](#_Toc11116954)

[2.1 Laravel 6](#_Toc11116956)

[2.1.1 PHP 6](#_Toc11116957)

[2.1.2 MySQL 7](#_Toc11116958)

[2.1.3 Kelebihan Laravel 8](#_Toc11116959)

[2.2 Python 9](#_Toc11116960)

[2.3 Advanced Encryption Standard (AES) 256 9](#_Toc11116961)

[2.3.1 Proses Enkripsi Advanced Enryption Standard 11](#_Toc11116962)

[2.3.2 Proses Deskripsi Advanced Enryption Standard 14](#_Toc11116963)

[2.3.3 Proses Ekspansi Kunci 17](#_Toc11116964)

[2.4 Secure Hash Algorithm (SHA) 256 18](#_Toc11116965)

[BAB III PERANCANGAN 19](#_Toc11116966)

[3.1 Analisis Kebutuhan Sistem 19](#_Toc11116968)

[3.1.1 Peran Pengguna 19](#_Toc11116969)

[3.1.2 Proses Bisnis 19](#_Toc11116970)

[3.2 Rangcangan Sistem 20](#_Toc11116971)

[3.2.1 Arsitektur Sistem 20](#_Toc11116972)

[3.2.2 Arsitektur Basis Data 20](#_Toc11116973)

[BAB IV IMPLEMENTASI 22](#_Toc11116974)

[4.1 Lingkungan Pembangunan Sistem 22](#_Toc11116976)

[4.2 Membuat Proyek Laravel Baru 22](#_Toc11116977)

[4.3 Implementasi Model 22](#_Toc11116978)

[4.3.1 Model User 22](#_Toc11116979)

[4.3.2 Model File 23](#_Toc11116980)

[4.3.3 Model Log 24](#_Toc11116981)

[4.3.4 Model Sharing 24](#_Toc11116982)

[4.4 Implementasi Controller 25](#_Toc11116983)

[4.4.1 Controller Home 25](#_Toc11116984)

[4.4.2 Controller File 25](#_Toc11116985)

[4.4.3 Controller Log 25](#_Toc11116986)

[4.4.4 Controller Sharing 25](#_Toc11116987)

[4.5 Implementasi View 25](#_Toc11116988)

[BAB V UJI COBA DAN EVALUASI 27](#_Toc11116989)

[4.6 Lingkungan Uji Coba 27](#_Toc11116990)

[BAB VI KESIMPULAN DAN SARAN 28](#_Toc11116991)

[4.7 Kesimpulan 28](#_Toc11116992)

[4.8 Saran 28](#_Toc11116993)

[DAFTAR PUSTAKA 29](#_Toc11116994)

[LAMPIRAN 33](#_Toc11116995)

[BIODATA PENULIS 34](#_Toc11116996)

***(Halaman ini sengaja dikosongkan)***

# DAFTAR GAMBAR

[**Gambar 2.1** Contoh Zona *Routing* Node S dengan Radius 2[4] 9](file:///D:\Kuliah\IF\TA-Buku\BUKU\Buku%20TA_ver%204.docx#_Toc535423290)

[**Gambar 2.2** Arsitektur ZRP[4] 10](#_Toc535423291)

[**Gambar 3.1** Diagram Rancangan Simulasi ZRP Modifikasi 18](#_Toc535423292)

[**Gambar 3.2** *Pseudocode* Penghitungan Kepadatan *Node* Tetangga 21](#_Toc535423293)

[**Gambar 3.3** *Pseudocode* Penghitungan Radius 21](#_Toc535423294)

[**Gambar 5.1** Grafik Rata-rata *Packet Delivery Ratio* pada Simulasi NS-2 50](#_Toc535423295)

[**Gambar 5.2** Grafik Rata-rata *Routing Overhead* pada Simulasi NS-2 52](#_Toc535423296)

[**Gambar 5.3** Grafik Rata-rata *Delivery Delay* pada Simulasi NS2 53](#_Toc535423297)

***(Halaman ini sengaja dikosongkan)***

# DAFTAR TABEL

[**Tabel 2.1** Detail Penjelasan *Trace File* ZRP 14](#_Toc535423275)

[**Tabel 3.1** Daftar Istilah 19](#_Toc535423276)

[**Tabel 3.2** Parameter Lingkungan Simulasi 22](#_Toc535423277)

[**Tabel 4.1** Tabel Lingkungan Pembangunan Sistem 25](#_Toc535423278)

[**Tabel 5.1** Spesifikasi Perangkat yang Digunakan 47](#_Toc535423279)

[**Tabel 5.2** Hasil Pra-Uji Coba Penentuan *Threshold* 49](#_Toc535423280)

***(Halaman ini sengaja dikosongkan)***

# KODE SUMBER

[**Kode Sumber 4.1** Modifikasi Fungsi print\_tables dalam Kelas NDPAgent 27](#_Toc535423252)

[**Kode Sumber 4.2** Menghitung *Node* di dalam IARP 28](#_Toc535423253)

***(Halaman ini sengaja dikosongkan)***

# BAB I PENDAHULUAN

## Latar Belakang

Seiring dengan perkembangan jaman, teknologi saat ini mengalami perkembangan kearah pencapaian kemudahan dan kenyamanan yang luar biasa, sehingga kegiatan sehari-hari yang di anggap tidak mungkin di kerjakan dalam waktu yang singkat menjadi mungkin untuk dilakukan secara singkat. Pengembangan teknologi komputasi berbasis internet saat ini lebih di arahkan pada proses aplikasi sistem yang mudah dan tidak memerlukan banyak waktu dan tenaga.

Perkembangan teknologi komputasi berbasis internet ini biasa dikenal sebagai *Cloud Computing*. Ada banyak jenis implementasi dari *Cloud Computing*, salah satunya adalah penyimpanan data secara *online*. Keunggulan menyimpan data secara *online* adalah pengguna dapat mengakses datanya dimanapun dan kapanpun dengan internet.

Perkembangan *Cloud Computing* ini tidak selalu berujung ke hal-hal yang positif. Ada juga penyedia layanan *Cloud Computing* yang melakukan penyalahgunaan data pengguna. Bentuk penyalahgunaan data ini berupa pencurian data, penjualan data dan perubahan data.

Tujuan dari pengerjaan tugas akhir ini adalah untuk memecahkan masalah tentang keamanan penyimpanan data pada layanan *Cloud*.

## Rumusan Masalah

Rumusan masalah yang diangkat dalam tugas akhir ini dapat dipaparkan sebagai berikut:

1. Bagaimana cara mengaplikasikan algoritma enkripsi AES-256 pada *framework* Laravel?
2. Bagaimana cara mengetahui bahwa data yang tersimpan pada sistem tidak dimodifikasi oleh pihak yang berbuat kecurangan?

## Batasan Permasalahan

Berdasarkan masalah yang diuraikan oleh penulis, maka batasan masalah pada tugas akhir ini adalah:

* 1. Bahasa pemrograman yang digunakan adalah PHP dan Python sedangkan basis data yang digunakan adalah MySQL.
  2. Lingkungan pengembangan yang digunakan menggunakan *framework* Laravel *5.8.*

## Tujuan

Tujuan dari pembuatan tugas akhir ini antara lain :

1. Merancang *website* dengan *framework* Laravel yang mengaplikasikan algoritma enkripsi AES-256.
2. Menghasilkan *Secret hash key* yang dihasilkan oleh aplikasi *checksum* yang menggunakan algoritma SHA-256.
3. Sistem ini diharapkan bisa membantu untuk audit forensik pada sebuah kasus tertentu yang melibatkan file digital.
4. Membandingkan kinerja algoritma AES-256 dan El-Gamal.

## Manfaat

Manfaat dari tugas akhir ini adalah terciptanya sistem penyimpanan data berbasis *website* yang memastikan akan keamanan data tanpa campur tangan penyedia layanan *Cloud*. Hasil tugas akhir ini diharapkan kedepannya dapat diterapkan sebagai aplikasi di lingkungan masyarakat umum

## Metodologi

Pembuatan tugas akhir ini dilakukan dengan menggunakan metodologi sebagai berikut:

### Penyusunan Proposal Tugas Akhir

Proposal tugas akhir ini berisi gambaran tentang tugas akhir yang akan dibuat. Pendahuluan proposal tugas akhir meliputi hal yang menjadi latar belakang diajukannya usulan tugas akhir, rumusan masalah yang diangkat, batasan masalah yang menjadi konstrain dari tugas akhir, tujuan pembuatan tugas akhir, dan manfaat dari hasil tugas akhir. Di dalam proposal tugas akhir juga dijabarkan mengenai tinjauan pustaka yang menjadi referensi pendukung dalam pembuatan tugas akhir ini.

### Studi Literatur

Pada studi literatur, akan dilakukan pengumpulan informasi dan referensi yang digunakan dalam pengerjaan tugas akhir yaitu mengenai Laravel, PHP, Python, MySQL, Algoritma AES-256 dan SHA-256

### Perancangan Sistem

Pada tahap perancangan sistem, akan dilakukan perancangan bisnis proses dari sistem. Bisnis proses ini meliputi proses pendaftaran, mengunggah data, mengunduh data dan membagikan data kepada pengguna yang lain.

### Implementasi Sistem

Pada tahap implementasi sistem akan dilakukan implementasi pembuatan sistem sesuai pada tahap perancangan sistem. Keluaran yang diharapkan dari tahap ini adalah Sistem PenyimpananData yang aman dan siap untuk dipakai.

### Pengujian.

Pengujian dilakukan untuk mengetahui tingkat keberhasilan pada sistem yang dibangun serta untuk memeriksa apakah sistem sudah berjalan dengan baik dan dipastikan agar tidak ada kesalahan yang terjadi.

### Penyusunan Buku

Pada tahap ini dilakukan penyusunan buku sebagai dokumentasi dari pelaksanaan tugas akhir yang mencakup seluruh konsep, teori, implementasi, serta hasil yang telah dikerjakan.

## Sistematika Penulisan Laporan

Sistematika penulisan laporan tugas akhir adalah sebagai berikut:

* + 1. Bab I. Pendahuluan

Bab ini berisi penjelasan mengenai latar belakang, rumusan masalah, batasan permasalahan, tujuan, manfaat, metodologi, dan sistematika penulisan dari pembuatan tugas akhir.

* + 1. Bab II. Tinjauan Pustaka

Bab ini berisi kajian teori atau penjelasan dari metode, algoritma, *library*,dan *tools* yang digunakan dalam penyusunan tugas akhir ini. Kajian teori yang dimaksud berisi tentang penjelasan singkat mengenaiLaravel, PHP, Python, MySQL, Algoritma AES-256 dan Algoritma SHA-256.

* + 1. Bab III. Perancangan

Bab ini berisi pembahasan mengenai perancangan proses bisnis yang akan diimplementasikan dalam tugas akhir. Perancangan proses bisnis berupa perancangan proses pendaftaran, mengunggah data, mengunduh data dan membagikan data.

* + 1. Bab IV. Implementasi

Bab ini menjelaskan implementasi yang berbentuk kode sumber dari proses bisnis yang terjadi pada aplikasi mulai pendaftaran, mengunggah data, mengunduh data dan membagikan data.

* + 1. Bab V. Pengujian dan Evaluasi

Bab ini berisi hasil pengujian dan evaluasi pada aplikasi Sistem Penyimpanan Data.

* + 1. Bab VI. Kesimpulan dan Saran

Bab ini merupakan bab yang menyampaikan kesimpulan dari hasil uji coba yang dilakukan, masalah-masalah yang dialami pada proses pengerjaan tugas akhir, dan saran untuk pengembangan tugas akhir ke depannya.

* + 1. Daftar Pustaka

Bab ini berisi daftar pustaka yang dijadikan literatur dalam tugas akhir.

* + 1. Lampiran

Dalam lampiran terdapat kode sumber program secara keseluruhan.

***(Halaman ini sengaja dikosongkan)***

# BAB II TINJAUAN PUSTAKA

Bab ini berisi pembahasan mengenai teori-teori dasar atau penjelasan dari metode dan alat yang digunakan dalam tugas akhir. Penjelasan ini bertujuan untuk memberikan gambaran secara umum terhadap program yang dibuat dan berguna sebagai penunjang dalam pengembangan riset yang berkaitan.



## Audit

Perkembangan terbaru dalam Teknologi Informasi (TI) telah memberi dampak besar atas bidang audit. TI telah menginspirasi rekayasa ulang berbagai proses bisnis tradisional untuk mendukung operasi yang lebih efisien dan untuk meningkatkan komunikasi dalam entitas serta antara entitas dengan para pelanggan dan pemasoknya. Akan tetapi, berbagai kemajuan ini membawa berbagai risiko baru yang membutuhkan pengendalian internal khusus. Kemajuan ini telah melahirkan kebutuhan akan berbagai teknik baru untuk mengevaluasi pengendalian dan untuk memastikan keamanan serta akurasi data perusahaan dan sistem informasi yang menghasilkannya.

Audit adalah proses sistematis mengenai mendapatkan dan mengevaluasi secara objektif bukti yang berkaitan dengan penilaian mengenai berbagai kegiatan dan peristiwa ekonomi untuk memastikan tingkat kesesuaian antara penilaian-penilaian tersebut membentuk kriteria serta menyampaikan hasilnya ke para pengguna yang berkepentingan.

Lembaga auditor internal (*Institite of Internal Auditory* - *IIA*) mendefinisikan audit internal sebagai fungsi penlaian independen yang dibentuk dalam perusahaan untuk mempelajari dan mengevaluasi berbagai aktivitasnya sebagai layanan bagi perusahaan. Para auditor internal melakukan berbagai jenis aktivitas atas nama perusahaan, termasuk melakukan audit keuangan, mempelajari ketaatan suatu operasi terhadap kebijakan perusahaan, mengkaji ketaatan perusahaan terhadap kewajiban hukumnya, mengevaluasi efisiensi operasional, mendeteksi dan mengejar pelaku penipuan dalam perusahaan, serta melakukan audit TI.

## Audit pada Komputasi Awan

Secara umum, audit adalah ketika pihak ketiga, kelompok independen dilibatkan untuk memperoleh bukti melalui penyelidikan, pemeriksaan fisik, pengamatan, konfirmasi, prosedur analitik, dan / atau kinerja ulang.

Dalam audit komputasi awan, variasi langkah-langkah ini diselesaikan untuk membentuk pendapat atas desain dan efektivitas operasional kontrol yang diidentifikasi dalam bidang berikut:

* Komunikasi
* Insiden keamanan
* Keamanan jaringan
* Pengembangan sistem atau manajemen perubahan
* Manajemen risiko
* Manajemen data
* Kerentanan dan manajemen remediasi

### Tujuan Audit Komputasi Awan

Selama tahap perencanaan dan pelaksanaan audit, penting untuk memiliki pemahaman yang jelas tentang apa yang termasuk dalam tujuan audit. Perusahaan harus berusaha untuk menyelaraskan tujuan bisnis mereka dengan tujuan audit. Ini akan memastikan bahwa waktu dan sumber daya yang dihabiskan akan membantu mencapai lingkungan kontrol internal yang kuat dan menurunkan risiko pendapat yang berkualitas.

Auditor menggunakan tujuan sebagai cara untuk menyimpulkan bukti yang mereka peroleh. Di bawah ini adalah daftar contoh tujuan komputasi awan yang dapat digunakan oleh auditor dan bisnis.

* **Tetapkan Rencana TI Strategis**

Penggunaan sumber daya TI harus selaras dengan strategi bisnis perusahaan. Ketika mendefinisikan tujuan ini, beberapa pertimbangan utama harus mencakup apakah investasi TI didukung oleh kasus bisnis yang kuat dan pendidikan apa yang akan diperlukan selama peluncuran investasi TI baru.

* **Definisikan Arsitektur Informasi**

Arsitektur informasi mencakup persyaratan jaringan, sistem, dan keamanan yang diperlukan untuk menjaga integritas dan keamanan informasi. Apakah informasi itu diam, dalam perjalanan atau sedang diproses.

* **Definisikan Proses, Organisasi, dan Hubungan TI**

Menciptakan proses yang didokumentasikan, terstandarisasi, dan diulang menciptakan untuk lingkungan TI yang lebih stabil. Bisnis harus fokus pada pembuatan kebijakan dan prosedur yang mencakup struktur organisasi, peran dan tanggung jawab, kepemilikan sistem, manajemen risiko, keamanan informasi, pemisahan tugas, manajemen perubahan, manajemen insiden, dan pemulihan bencana.

* **Berkomunikasi Tujuan dan Arah Manajemen**

Manajemen harus memastikan kebijakan, misi, dan tujuannya dikomunikasikan di seluruh organisasi.

* **Menilai dan Mengelola Risiko TI**

Manajemen harus mendokumentasikan risiko-risiko yang dapat mempengaruhi tujuan perusahaan. Ini dapat mencakup kerentanan keamanan, undang-undang dan peraturan, akses ke pelanggan atau informasi sensitif lainnya, dll.

## Laravel

Laravel adalah sebuah framework berbahasa pemrogaman PHP terbaik yang dikembangkan oleh *Taylor Otwell.* Proyek pembuatan framework ini dimulai pada April 2011, yang didasari atas keresahan *Taylor Otwell* karena tidak adanya framework PHP yang *up to date*  dengan versi PHP [6].

### PHP

*Taylor Otwell* memilih bahasa pemrograman PHP untuk frameworknya dikarenakan bahasa ini merupakan bahasa pemrograman yang sangat popular dalam membangun sebuah CMS (Content Management System). Popularitas PHP dikarenakan beberapa kelebihan yang ditawarkan oleh bahasa ini :

* **Kesederhanaan**, bahasa PHP merupakan bahasa yang sederhana. User atau pengguna yang hanya sedikit tahu atau bahkan sama sekali tidak mengerti tentang pemrograman bisa dengan cepat belajar PHP. Selain itu PHP juga menyediakan fungsi *built-in* untuk menangani kebutuhan standar pembuatan web.
* **Banyaknya referensi,** bahasa PHP dipilih karena bahasa ini telah ada sejak lama yaitu tahun 1995 dan sudah memiliki komunitas yang sangat besar. Dengan komunitas yang besar ini tentu saja referensi tentang bahasa pemrograman PHP sudah sangat banyak.
* ***Open source***, bahasa PHP merupakan bahasa *open source*  yang dapat digunakan di berbagai sistem operasi seperti: Linux, Unix, Macintosh, dan Windows.
* **Banyaknya web server**, web server yang mendukung bahasa PHP dapat ditemukan dimana-mana mulai dari Apache, IIS, Lighttpd, hingga Xitami yang pengkonfigurasiannya relative mudah [7].

### MySQL

Selain kelebihan yang ditawarkan oleh bahasa PHP itu sendiri, bahasa PHP juga popular digunakan karena mendukung banyak jenis database. Salah satu database yang sering digunakan bersama dengan bahasa pemrograman PHP adalah database MySQL.

MySQL (My Structure Query Language) adalah sebuah perangkat lunak sistem manajemen basis data SQL (Database Management System) atau sering disingkat DBMS. MySQL merupakan DBMS yang multithread, multi-user, yang bersifat gratis dan dibawah lisensi GNU General Public License. MySQL ini dipilih oleh banyak orang karena beberapa kelebihan yang ditawarkan:

* MySQL dapat berjalan dengan stabil pada berbagai sistem operasi , seperti Windows, Linux, FreeBSD, Mac OS X Server, Solaris dan masih banyak lagi
* Bersifat Open Source, MySQL didistribusikan secara open source (gratis)
* Bersifat Multi User, MySQL dapat digunakan oleh beberapa user dalam waktu yang bersamaan tanpa mengalami masalah.
* MySQL memiliki kecepatan yang baik dalam menagani query (perintah SQL). Dengan kata lain MySQL dapat memroses lebih banyak SQL per satuan waktu.
* Dari segi security atau keamanan data, MySQL memiliki beberapa lapisan sekuriti, seperti level subnet mask, nama host, dan izin akses user dengan sistem perizinan yang mendetail serta password yang terenkripsi.
* MySQL memiliki interface (antarmuka) terhadap aplikasi dan bahasa pemrograman.
* Dukungan banyak komunitas, biasanya tergabung dalam sebuah forum untuk saling berdiskusi membagi informasi tentang MySQL [7].

### Kelebihan Laravel

Dengan dukungan serta popularitas PHP serta MySQL pada Laravel, framework ini tentu saja juga mendapatkan popularitas yang serupa pula. Selain itu ada beberapa alasan lain mengapa banyak orang memilih dan menggunakan framework Laravel daripada framework lain diantaranya:

* **Mudah dan Dokumentasinya Lengkap**

Platform Laravel menarik dan mudah digunakan. Seorang pengguna yang tidak ahli dalam bidang web developmentpun bisa menggunakannya. Dokumentasi resmi yang dimiliki Laravel pun tergolong ke dalam dokumentasi yang sangat baik, rapi, mudah dan jelas. Dokumentasi ini tersedia pada <https://laravel.com/docs>

* **Open source**

Laravel merupakan framework open source yang dapat digunakan secara bebas, gratis, dan memungkinkan pengguna untuk membuat web aplikasi yang besar dan kompleks dengan mudah.

* **Arsitektur MVC**

Dengan menggunakan pola MVC, kita dapat membuat arsitektur kode yang lebih rapi dimana pola tersebut memisahkan antara logika dan view. Arsitektut MVC dapat meningkatkan *performance* serta memiliki beberapa fungsi built-in.

* **Blade Template**

Laravel memiliki fitur blade template yang mempermudah pengguna untuk memetakan template yang dia miliki dengan membaginya menjadi beberapa bagian sehingga lebih mudah diatur.

* **Memiliki Fitur Migration**

Migration adalah salah satu fitur utama yang dimiliki Laravel. Dengan migration, memungkinkan pengguna untuk mempertahankan struktur database yang dia miliki tanpa membuatnya kembali. Dengan migration memungkinkan untuk mengatur database dengan menuliskan kode PHP.

* **Keamanan**

Keamanan aplikasi merupakan prioritas nomor satu dalam mengembangkan website. Terlebih lagi jika website tersebut menyimpan banyak data yang sangat penting dan sensitive. Laravel memberikan kita beberapa pilihan penting yang dapat digunakan untuk membuat aplikasi kita agar tetap aman. ORM Laravel menggunakan PDO yang dapat mencegah SQL Injection, memiliki csrf token, dan banyak hal lainnya

* **Komunitas yang besar**

Laravel merupakan framework yang popular dan memiliki komunitas yang besar. Dengan adanya komunitas ini pengguna dapat lebih mudah beljar dan mencari solusi yang tepat atas setiap permasalahannya.

* **Hemat waktu**

Dengan berbagai abstraksi yang tersedia di Laravel. Pengguna jadi lebih fokus untuk memikirkan logika bisnis dari aplikasi yang dia buat. Jika ada developer baru yang masuk ke project, dia cukup mempelajari dokumentasi resmi Laravel sehingga lebih menghemat waktu [6].

## Python

Python adalah bahasa pemrograman interpretatif yang dianggap mudah dipelajari serta berfokus pada keterbacaan kode. Dengan kata lain, Python diklaim sebagai bahasa pemrograman yang memiliki kode-kode pemrograman yang sangat jelas, lengkap, dan mudah untuk dipahami [3].

Python dianggap memiliki kehebatan untuk menangani pembuatan aplikasi-aplikasi kekinian yang mengandung kata kunci *big data*, *data mining*, *deep learning*, *data science*, hingga *machine learning*. Dengan kata lain, Python adalah bahasa pemrograman yang sederhana untuk membuat aplikasi berbasis kecerdasan buatan (*Artificial Intelligence*) [3].

Python secara umum berbentuk pemrograman berorientasi objek, pemrograman imperatif, dan pemrograman fungsional. Istilah lainnya adalah bahasa pemrograman multi-paradigma.

Python dapat digunakan untuk berbagai keperluan pengembangan perangkat lunak dan dapat berjalan di berbagai platform sistem operasi [3].

### Platform Pemrograman Python

Python dapat dijalankan di berbagai platform sistem operasi. Oleh karena itu, distribusi aplikasi yang dibuat menggunakan Python sangatlah luas dan *multi-platform*.

Beberapa platform yang mendukung Python di antaranya Linux / Unix, Windows, Mac OS, Java Virtual Machine, OS/2, Amiga, Palm dan Symbian [3].

### Lisensi Python

Pada prinsipnya, Python dapat diperoleh dan digunakan secara bebas oleh siapapun, bahkan bagi *developer* yang menggunakan bahasa pemrograman ini untuk kepentingan komersial. Namun pengguna *package* atau modul dari pihak ketiga mungkin saja membutuhkan lisensi yang berbeda, misalnya lisensi berbayar [3].

### Sejarah Python

Python dikembangkan oleh Guido van Rossum, ahli pemrograman kelahiran Belanda pada tahun 1991 di CWI, Amsterdam sebagai kelanjutan dati bahasa pemrograman ABC.

Nama Python dipilih oleh Guido sebagai nama bahasa ciptaanya karena kecintaan Guido pada acara televisi Monty Python’s Flying Circus [3].

Saat ini pengembangan Python terus dilakukan oleh sekelompok programmer yang dikoordinir oleh Guido dan Python Software Foundation. Saat ini distribusi Python sudah mencapai versi 3.7. perkembangan bahasa pemrograman ini bisa dilihat di situs resmi di ***www.python.org.***

### Fitur Bahasa Pemrograman Python

Beberapa fitur dan kelebihan yang dimiliki Python adalah:

* Memiliki koleksi kepustakaan yang banyak. Artinya telah tersedia modul-modul ‘siap pakai’ untuk berbagai keperluan seperti pembuatan permainan hingga kecerdasan buatan.
* Memiliki struktur bahasa yang jelas, sederhana dan mudah dipelajari
* Berorientasi prosedural dan objek sekaligus (multi-paradigma)
* Memiliki sistem pengelolaan memori otomatis (*garbage collection*)
* Bersifat modular sehingga mudah dikembangkan dengan menciptakan modul-modul baru, baik dibangun dengan bahasa Python maupun C/C++

## Advanced Encryption Standard (AES) 256

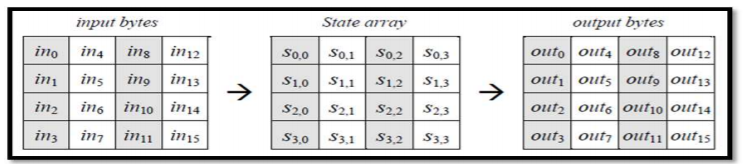
Advanced Encryption Standard (AES) merupakan algoritma cryptographic yang dapat digunkan untuk mengamakan data. Algoritma AES adalah blok chipertext simetrik yang dapat mengenkripsi (encipher) dan dekripsi (decipher) informasi. AES dipilih karena kuat terhadap serangan differential, serangan truncated differential, serangan linear, serangan interpolation, dan serangan square [8].

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. Cipher key dari AES terdiri dari key dengan panjang 128 bit, 192 bit, atau 256 bit. Perbedaan panjang kunci akan mempengaruhi jumlah round yang akan diimplementasikan pada algoritma AES ini. Berikut ini adalah Tabel 2.4.1 yang memperlihatkan jumlah round / putaran ( Nr ) yang harus diimplementasikan pada masingmasing panjang kunci

|  |  |  |  |
| --- | --- | --- | --- |
|  | Jumlah Key  (Nk) | Ukuran Block  (Nb) | Jumlah Putaran  (Nr) |
| AES-128 | 4 | 4 | 10 |
| AES-192 | 6 | 4 | 12 |
| AES-256 | 8 | 4 | 14 |

Tabel 2.4.1 Perbandingan Jumlah Round dan Key [9]

Pada dasarnya, operasi AES dilakukan terhadap array of byte dua dimensi yang disebut dengan state. State mempunyai ukuran NROWS X NCOLS. Pada awal enkripsi, data masukan yang berupa in0, in2, in3, in4, in5, in6, in7, in8, in9, in10, in11, in12, in13, in14, in15 disalin ke dalam array state. State inilah yang nantinya dilakukan operasi enkripsi / dekripsi. Kemudian keluarannya akan ditampung ke dalam array out. Gambar 2.4.1 mengilustrasikan proses penyalinan dari input bytes, state array, dan output bytes.



Gambar 2.4.1 Proses Input Bytes, State Array, dan Output Bytes [9]

Pada saat permulaan, input bit pertama kali akan disusun menjadi suatu array byte dimana panjang dari array byte yang digunakan pada AES adalah sepanjang 8 bit data. Array byte inilah yang nantinya akan dimasukkan atau dicopy ke dalam state dengan urutan dimana r ( row / baris ) dan c (column/kolom) :

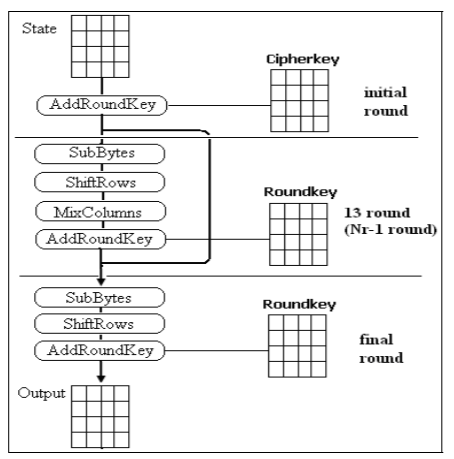
**s[r,c] = in[r+4c] untuk 0 ≤ r < 4 dan 0 ≤ c < Nb**

sedangkan dari state akan dicopy ke output dengan urutan :

**out[r+4c] = s[r,c] untuk 0 ≤ r < Nb**

### Proses Enkripsi Advanced Enryption Standard

Proses enkripsi algoritma AES terdiri dari 4 jenis transformasi bytes, yaitu SubBytes, ShiftRows, Mixcolumns, dan AddRoundKey. Pada awal proses enkripsi, input yang telah dicopykan ke dalam state akan mengalami transformasi byte AddRoundKey. Setelah itu, state akan mengalami transformasi SubBytes, ShiftRows, MixColumns, dan AddRoundKey secara berulang-ulang sebanyak Nr. Proses ini dalam algoritma AES disebut sebagai round function. Round yang terakhir agak berbeda dengan round-round sebelumnya dimana pada round terakhir, state tidak mengalami transformasi MixColumns. Ilustrasi proses enkripsi AES dapat digambarkan seperti pada Gambar 2 di bawah ini :



Gambar 2.4.2 Ilustrasi Proses Enkripsi AES [9]

#### *AddRoundKey*

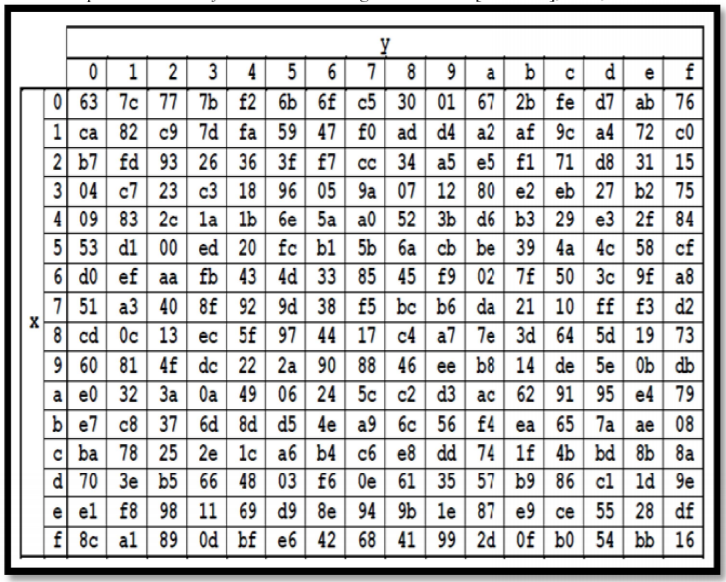
Pada proses enkripsi dan dekripsi AES proses AddRoundKey sama, sebuah round key ditambahkan pada state dengan operasi XOR. Setiap round key terdiri dari Nb word dimana tiap word tersebut akan dijumlahkan dengan word atau kolom yang bersesuaian dari state sehingga :



[ wi ] adalah word dari key yang bersesuaian dimana i = round\*Nb+c. Transformasi AddRoundKey pada proses enkripsi pertama kali pada round = 0 untuk round selanjutnya round = round + 1, pada proses dekripsi pertama kali pada round = 14 untuk round selanjutnya round = round - 1.

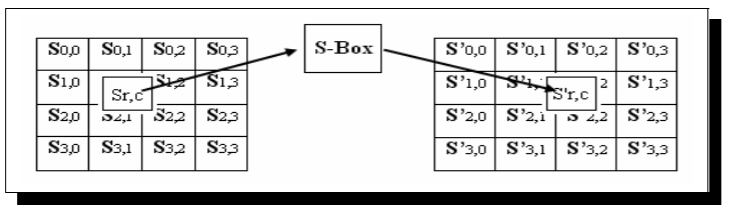
#### *SubBytes*

SubBytes merupakan transformasi byte dimana setiap elemen pada state akan dipetakan dengan menggunakan sebuah tabel substitusi ( S-Box ). Tabel substitusi S-Box akan dipaparkan dalam Tabel 2.4.2



Tabel 2.4.2 Tabel S-Box SubBytes

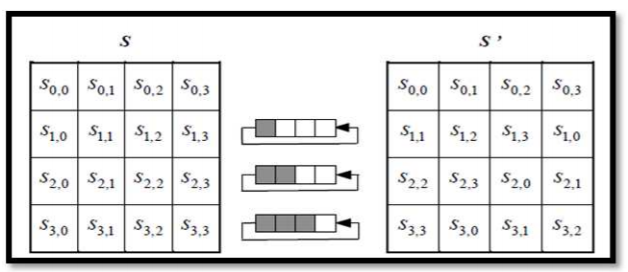
Untuk setiap byte pada array state, misalkan S[r, c] = xy, yang dalam hal ini xy adalah digit heksadesimal dari nilai S[r, c], maka nilai substitusinya, dinyatakan dengan S’[r, c], adalah elemen di dalam tabel subtitusi yang merupakan perpotongan baris x dengan kolom y. Gambar 2.4.3 mengilustrasikan pengaruh pemetaan byte pada setiap byte dalam state



Gambar 2.4.3 Pengaruh Pemetaan pada Setiap Byte dalam State [9]

#### *Shiftrows*

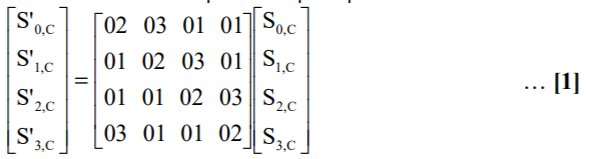
Transformasi Shiftrows pada dasarnya adalah proses pergeseran bit dimana bit paling kiri akan dipindahkan menjadi bit paling kanan ( rotasi bit ). Proses pergeseran Shiftrow ditunjukkan dalam Gambar 2.4.4 berikut:



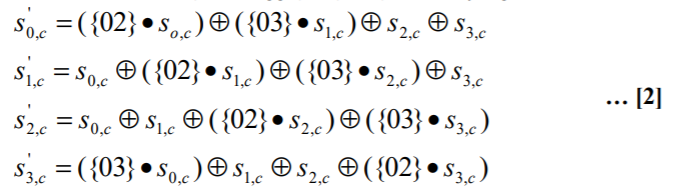
Gambar 2.4.4 Transformasi ShiftRows [9]

#### *MixColumns*

MixColumns mengoperasikan setiap elemen yang berada dalam satu kolom pada state. Secara lebih jelas, transformasi mixcolumns dapat dilihat pada perkalian matriks berikut ini:

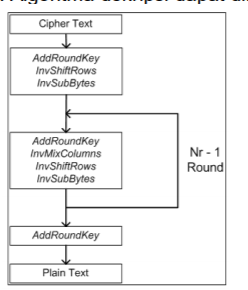


Hasil dari perkalian matriks diatas dapat dianggap seperti perkalian yang ada di bawah ini :



### Proses Deskripsi Advanced Enryption Standard

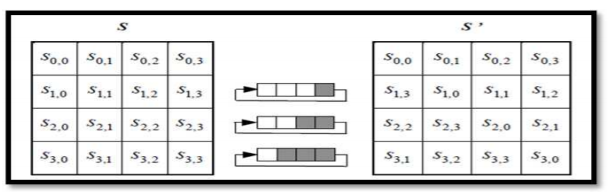
Transformasi cipher dapat dibalikkan dan diimplementasikan dalam arah yang berlawanan untuk menghasilkan inverse cipher yang mudah dipahami untuk algoritma AES. Transformasi byte yang digunakan pada invers cipher adalah InvShiftRows, InvSubBytes, InvMixColumns, dan AddRoundKey. Algoritma dekripsi dapat dilihat pada skema berikut ini:



Gambar 2.4.5 Ilustrasi Proses Deskripsi AES [9]

#### *InvShiftRows*

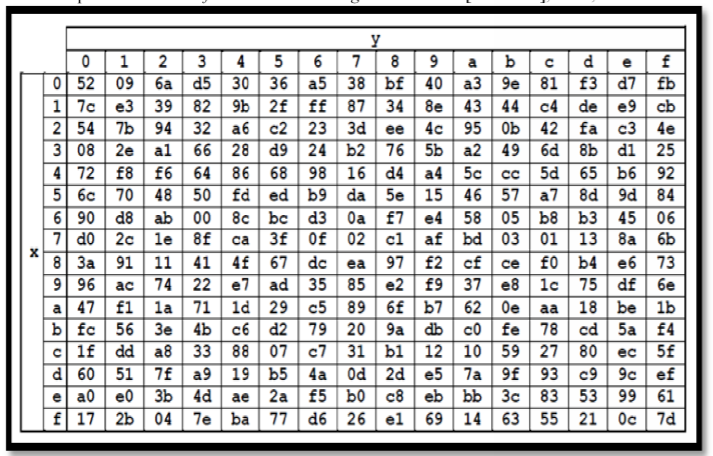
InvShiftRows adalah transformasi byte yang berkebalikan dengan transformasi ShiftRows. Pada transformasi InvShiftRows, dilakukan pergeseran bit ke kanan sedangkan pada ShiftRows dilakukan pergeseran bit ke kiri. Ilustrasi transformasi InvShiftRows terdapat pada Gambar 2.4.6:



Gambar 2.4.6 Transformasi InvShiftRows [9]

#### *InvSubBytes*

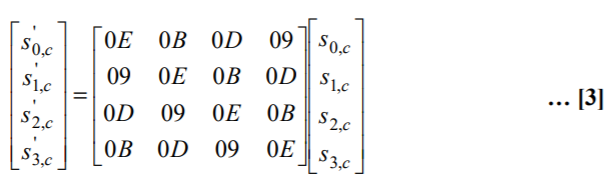
InvSubBytes juga merupakan transformasi bytes yang berkebalikan dengan transformasi SubBytes. Pada InvSubBytes, tiap elemen pada state dipetakan dengan menggunakan tabel Inverse S-Box. Tabel Inverse S-Box akan ditunjukkan dalam Tabel 2.4.3 berikut:



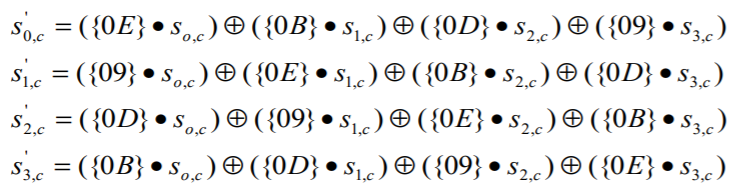
Tabel 2.4.3 Tabel Inverse S-Box [9]

#### *InvMixColumns*

Setiap kolom dalam state dikalikan dengan matrik perkalian dalam AES. Perkalian dalam matrik dapat dituliskan :

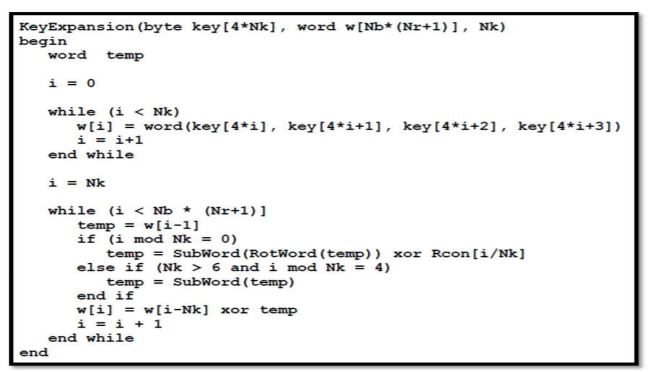


Hasil dari perkalian dalam matrik adalah :



### Proses Ekspansi Kunci

Algoritma AES mengambil kunci cipher dan melakukan rutin ekspansi kunci ( key expansion ) untuk membentuk key schedule. Ekspansi kunci menghasilkan total Nb(Nr+1) word. Algoritma ini membutuhkan set awal key yang terdiri dari Nb word, dan setiap round Nr membutuhkan data kunci sebanyak Nb word. Hasil key schedule terdiri dari array 4 byte word linear yang dinotasikan dengan [ wi ]. SubWord adalah fungsi yang mengambil 4 byte word input dan mengaplikasikan S-Box ke tiap-tiap data 4 byte untuk menghasilkan word output. Fungsi RotWord mengambil word [a0, a1, a2, a3] sebagai input, melakukan permutasi siklik, dan mengembalikan word [a1, a2, a3, a0]. Rcon[i] terdiri dari nilai-nilai yang diberikan oleh [xi-1, {00}, {00}, {00}], dengan xi-1 sebagai pangkat dari x (x dinotasikan sebagai {02}). Pseudocode dari proses ekspansi kunci dapat dilihat dalam gambar berikut ini:



Gambar 2.4.7 Pseudocode Ekspansi Kunci [9]

Dari Gambar 2.4.7 dapat dilihat bahwa word ke Nk pertama pada ekspansi kunci berisi kunci cipher. Setiap word berikutnya, w[i], sama dengan XOR dari word sebelumnya, w[i-1] dan word Nk yang ada pada posisi sebelumnya, w[i-Nk]. Untuk word pada posisi yang merupakan kelipatan Nk, sebuah transformasi diaplikasikan pada w[i-1] sebelum XOR, lalu dilanjutkan oleh XOR dengan konstanta round, Rcon[i]. Transformasi ini terdiri dari pergeseran siklik dari byte data dalam suatu word RotWord, lalu diikuti aplikasi dari lookup tabel untuk semua 4 byte data dari word SubWord [9]

## Secure Hash Algorithm 256 (SHA-256)

Pada bulan Agustus 1991, NIST (The National Institute of Standard and Technology) mengumumkan bakuan (standard) untuk tanda-tangan digital yang dinamakan *Digital Signature Standard (DSS)*,. DSS terdiri dari dua komponen, yang pertama adalah algoritma tanda-tangan digital yang disebut *Digital Signature Algorithm (DSA)*, dan yang kedua adalah fungsi hash standard yang disebut Secure Hash Algorithm [6].

SHA adalah fungsi hash satu arah yang dibuat oleh NIST dan digunakan bersama DSS. SHA dinyatakan sebagai standard fungsi hash satu arah oleh United States National Security Agency (NSA). SHA didasarkan pada MD4 yang dibuat oleh Ronald L. Rivest dari MIT [6].

### Awal Perkembangan SHA-256

Awal terbentuknya SHA-256 dimulai dari sejarah algoritma SHA, dimana hingga saat ini ada lima algoritma SHA yaitu SHA-0, SHA-1, SHA-224, SHA-256, SHA-384, dan SHA-512. Varian SHA-0 dikenal dengan SHA-0 pada tahun 1991, varian SHA-1 dikenal dengan SHA-1 pada tahun 1993, varian SHA-224, SHA-256, SHA-384, dan SHA-512 dikenal dengan SHA-2 pada tahun 2000 [7] [8]. Dari seitulah SHA-256 muncul yang merupakan pecahan dari SHA- 2 yang mempunyai varian di dalamnya antara lain : varian SHA-224, SHA-256, SHA-384, dan SHA-512.

### Dasar Prinsip

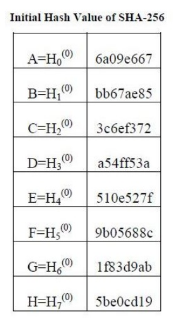
Algoritma SHA-256 dapat digunakan untuk menghitung nilai message digest dari sebuah pesan, dimana pesan tersebut memiliki panjang maksimum 264 bit. Algoritma ini menggunakan sebuah message schedule yang terdiri dari 64 element 32-bit word, delapan buah variabel 32-bit, dan variabel penyimpan nilai hash 8 buah word 32-bit. Hasil akhir dari algoritma SHA-256 adalah sebuah message digest sepanjang 256-bit [9].

### Cara Kerja

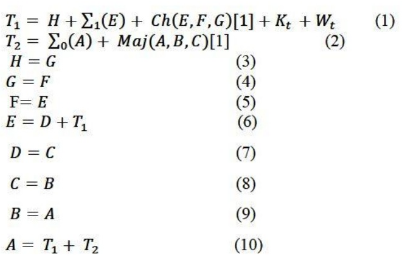
Cara Kerja SHA-256 mengubah pesan masukan ke dalam message digest 256 bit. Berdasarkan Secure Hash Signature Standard, pesan masukan yang panjangnya lebih pendek dari 264 bit, harus dioperasikan oleh 512 bit dalam kelompok dan menjadi sebuah message diggest 256-bit [10].

Tahapan-tahapan cara kerja SHA-256 adalah sebagai berikut [10]:

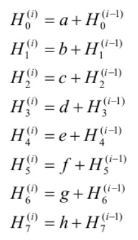
1. Message Padding : Pada tahap pertama, pesan yang berupa binary disisipkan dengan angka 1 dan ditambahkan bit-bit pengganjal yakni angka 0 hingga panjang pesan tersebut kongruen dengan 448 modulo 512. Panjang pesan yang asli kemudian ditambahkan sebagai angka biner 64 bit. Setelah itu maka panjang pesan sekarang menjadi kelipatan 512 bit.
2. Parsing : Pesan yang sudah dipadding tadi kemudian dibagi menjadi N buah blok 512 bit : M(1) , M(2) , ..., M(N).
3. Message Expansion : Masing-masing blok 512-bit tadi lalu dipecah menjadi 16 buat word 32-bit : M0(i) , M1(i) , ..., M15(i) yang mana nantinya diperluas menjadi 64 word yang diberi label W0, W1, ..., W63 dengan aturan tertentu yang sudah ditentukan sebelumnya oleh standar SHA-2.
4. Message Compression : Masing-masing dari 64 word yang diberi label W0, W1, ..., W63 tadi kemudian diproses dengan algoritma fungsi hash SHA-256. Dalam proses tersebut, inti utama dari algoritma SHA-256 adalah membuat 8 variabel yang diberikan nilai untuk nilai awal dari H0(0) - H7(0) di awal masing-masing fungsi hash. Nilai-nilai awal tersebut adalah sebagai berikut :



1. Algoritma ini melakukan perhitungan sebanyak 64 kali putaran untuk setiap perhitungan blok. Delapan variabel yang diberi label A, B, C, ..., H tadi nilainya terus berganti selama perputaran sebanyak 64 kali putaran sebagai berikut :



1. Setelah perputaran sebanyak 64 kali tadi, nilai hash H(i) kemudian dihitung sebagai berikut :



1. Selanjutnya hasil akhir SHA-256 didapat dari penggabungan delapan variabel yang tadi sudah dikomputasi.



# BAB III PERANCANGAN

Bab ini membahas mengenai perancangan implementasi sistem yang dibangun pada tugas akhir. Bagian yang akan dijelaskan pada bab ini adalah analisis kebutuhan sistem dan perancangan sistem berdasarkan analisis yang dibuat.



## Analisis Kebutuhan Sistem

Pada tugas akhir ini akan dibangun sistem Penyimpanan Data Terenkripsi Menggunakan AES-256. Sistem ini akan dibangun menggunakan kerangka kerja Laravel dan basis data MySQL.

Dengan adanya sistem ini diharapkan nantinya pengguna bisa menyimpan datanya di *Cloud* dengan aman tanpa adanya kecurangan dari pihak ketiga.

### Peran Pengguna

Pada sebuah sistem tentina ada beberapa pengguna ang terlibat di dalamnya. Para pengguna ini tentu saja memiliki peran (*role*) yang berbeda-beda. Dalam sistem ini akan ada 2 peran pengguna (*role user*):

* User, sebagai pengguna sistem user dapat menyimpan datanya di sistem dan dapat membagikan datanya kepada user lain.
* Admin, sebagai pengelola sistem memiliki tugas untuk mengawasi aktivitas para pengguna, selain itu admin juga dapat menyimpan datanya di sistem dan membagikan datanya kepada pengguna lain.

### Proses Bisnis

Dalam sebuah sistem pastinya ada proses bisnis yang berjalan di dalamnya. Proses bisnis inilah yang menentukan arah dan tujuan sebuah sistem dibuat. Dalam sistem ini terdapat 3 proses bisnis utama:

#### Unggah Data

Dalam proses ini para pengguna dapat mengunggah data mereka ke sistem dan sistem akan menyimpan data tersebut sebelum sistem menyimpan data tersebut sistem melakukan enkripsi terhadap data tersebut, hal ini dilakukan demi privasi data pengguna. Setelah data terenkripsi, sistem akan menghasilkan *secret hash key* dari data terenkripsi tersebut.

#### Unduh Data

Dalam proses ini para pengguna dapat mengunduh data yang telah mereka unggah di sistem. Selain data yang diunggah, para pengguna juga dapat mengunduh data-data yang dibagikan oleh pengguna yang lain. Sebelum mengunduh sistem melakukan proses verifikasi terhadap file yang ingin diunduh dengan cara membandingkan *secret hash key* yang tersimpan di basis data dengan *secret hash key* pada file yang akan diunduh. Apabila *secret hash key* tersebut sama maka file akan didekripsi, karena data yang tersimpan pada sistem ini adalah data yang terenkripsi. Apabila *secret hash key* tidak sama maka sistem akan menampilkan pesan *error*.

#### Bagikan Data

Dalam proses ini para pengguna dapat membagikan hak akses data yang telah mereka unggah kepada pengguna yang lain. Sehingga pengguna lain dapat mengunduh data yang telah dibagikan.

#### Meminta Checksum

Dalam proses ini para pengguna dapat meminta checksum dari file yang dimiliki dengan cara mengisi form yang tersedia pada sistem. Untuk mendapatkan checksum tersebut harus menunggu persetujuan dari admin. Apabila admin menyetujui permintaan tersebut, maka pengguna akan mendapatkan pesan yang berisi dari checksum tersebut. Jika admin menolak permintaan tersebut, maka pengguna akan mendapatkan pesan yang berisi pesan bahwa permintaannya ditolak.

#### Persetujuan Checksum

Proses persetujuan checksum ini hanya bisa dilakukan oleh admin. Admin dapat menyetujui ataupun menolak permintaan dari pengguna, tergantung dari isi form yang ditulis oleh pengguna.

### Spesifikasi Kebutuhan Sistem

Dari peran pengguna (role user) dan proses bisnis yang ada dapat digambarkan ke dalam use case diagram berikut.



#### Masuk ke Sistem

Kebutuhan masuk ke sistem digunakan oleh setiap peran yang ada pada sistem.

|  |  |
| --- | --- |
| Komponen | Deskripsi |
| Nama | Masuk ke Sistem |
| Nomor | UC-001 |
| Deskripsi | Aktor masuk (login) ke dalam sistem |
| Tipe | Fungsional |
| Aktor | Pemilik Ide Usaha, Pemilik Dana, Verifikator, Admin |
| Kondisi Awal | Aktor belom terotentifikasi atau masuk (login) ke dalam sistem |
| Kondisi Akhir | Aktor berhasil terotentifikasi dan sistem menampilkan halama dashboard |
| Alur Normal | 1. Aktor membuka halaman login sistem 2. Sistem menampilkan halaman login 3. Aktor memasukkan dan memilih pilihan login. 4. Sistem memeriksa kebenaran kredensial pengguna 5. Aktor berhasil terotentifikasi pada sistem. |
| Alur Alternatif | - |
| Eksepsi | 4.a. Data kredensial tidak benar  4.a.1 Sistem menampilkan pesan error. |



#### Registrasi

Kebutuhan registrasi dibutuhkan oleh User. Registrasi adalah fungsi pendaftaran yang dilakukan setiap pengguna agar terdaftar dalam sistem.

|  |  |
| --- | --- |
| Komponen | Deskripsi |
| Nama | Registrasi |
| Nomor | UC-002 |
| Deskripsi | User mendaftar pada sistem |
| Tipe | Fungsional |
| Aktor | User |
| Kondisi Awal | User belum terdaftar pada sistem |
| Kondisi Akhir | User berhasil terdaftar pada sistem |
| Alur Normal | 1. User membuka halaman registrasi 2. Sistem menampilkan halaman registrasi. 3. User memasukkan data kredensial dan memilih pilihan daftar 4. Sistem memeriksa kebenaran data dari pengguna 5. Sistem memverifikasi akun pengguna 6. Sistem menampilkan akun berhasil dibuat dan diverifikasi. |
| Alur Alternatif | - |
| Eksepsi | 4.a. Data Email sudah pernah digunakan  4.a.1 Sistem menampilkan pesan error. |



#### Mengunggah File

#### Mengunduh File

#### Meminta checksum

#### Persetujuan permintaan checksum

#### Monitoring Aktivitas

#### Melihat notifikasi

## Rangcangan Sistem

Rancangan sistem yang akan dibuat meliputi arsitektur sistem, rancangan basis data yang akan dibuat dalam bentuk *Conceptual Data Model (CDM)* dan *Physical Data Model (PDM)*, rancangan enkripsi dan dekripsi data, rancangan berbagi data dan rancangan antarmuka sistem.

### Arsitektur Sistem

Arsitektur sistem yang akan digunakan pada tugas akhir ini adlaah menggunakan arsitektur MVC yaitu kerangka kerja Laravel. Arsitektur dari Laravel bisa dilihat pada gambar di bawah



View (antarmuka) dan Routing adalah lapisan yang terhubung langsung dengan pengguna. Controller adalah penghubung antara model dan basis data dengan antarmuka pengguna.

### Rancangan Basis Data

Dalam pembuatan suatu sistem diperlukan adanya suatu basis data tempat menyimpan informasi informasi dalam sistem. Dalam tugas akhir ini basis data yang digunakan adalah MySQL karena merupakan salah satu jenis basis data yang *reliable.*

Rancangan basis data yang akan digunakan adalah dalam bentuk *Conceptual Data Model (CDM) dan Physical Data Model (PDM)* ditunjukkna pada gambar di bawah ini.

#### Tabel User

Tabel user mencatat pengguna-pengguna yang terdaftar pada sistem. Tabel ini memiliki hubungan dengan tabel role, file, log, dan sharing.

#### Tabel File

Tabel file mencatat data file yang telah diunggah oleh pengguna. Tabel ini memiliki hubgungan dengan tabel user, sharing dan log

#### Tabel Log

Tabel log mencatat aktivitas yang dilakukan oleh pengguna. Aktivitas yang dicatat pada tabel ini adalah mengunggah, mengunduh dan menghapus data, selain itu juga menyimpan data aktivitas permintaan dan persetujuan checksum. Tabel ini memiliki hubungan dengan tabel user dan file.

#### Tabel Sharing

Tabel ini mencatat aktivitas berbagi data yang dilakukan oleh pengguna. Tabel ini memiliki hubungan dengan tabel user dan tabel file.

### Rancangan Proses Mengunggah File

Sebelum file yang diunggah oleh pengguna disimpan di server, terdapat beberapa tahap yang dilakukan oleh sistem untuk memperkuat keamanan data. Berikut adalah tahap-tahap dalam proses pengunggahan data:

1. Pengguna mengunggah File.

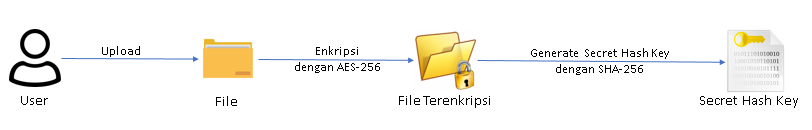
Pengguna mengunggah file dari form yang tersedia di aplikasi.

1. Enkripsi file.

Saat file sudah terupload, sistem akan mengenkripsi file tersebut dengan menggunakan algoritma AES-256 dengan key dari pengguna tersebut dan file tersebut akan disimpan di sistem.

1. Generate secret hash key.

Setelah file dienkripsi, sistem akan generate secret hash key untuk disimpan di basis data. Secret hash key ini nantinya akan digunakan untuk proses audit file tersebut.



### Rancangan Proses Mengunduh File

Untuk mengunduh file terdapat beberapa tahap yang dilakukan oleh sistem.

1. Verifikasi file

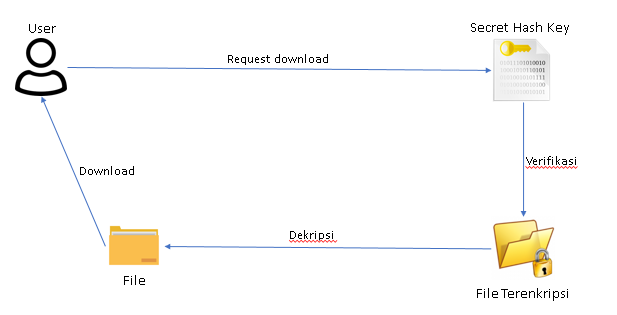
Untuk mengetahui bahwa file yang akan diunduh tidak mengalami modifikasi, secret hash key pada file tersebut akan dibandingkan dengan secret hash key yang sudah tersimpan di basis data. Jika secret hash key file dan basis data sama, maka file tersebut tidak mengalami modifikasi, begitu juga sebaliknya.

1. Dekripsi file.

Setelah file terverifikasi, sistem akan mendekripsi file tersebut dengan menggunakan key yang sudah tersimpan.

1. Download file

Setelah file didekripsi barulah file tersebut dikirimkan ke pengguna.



### Rancangan Audit File

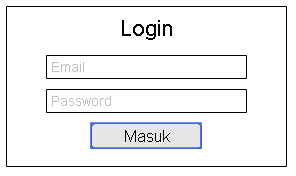
Proses audit file ini menggunakan program yang berjalan di background process. Cara kerjanya adalah dengan membandingkan secret hash key pada file dengan secret hash key yang tersimpan di basis data. Apabila secret hash key tersebut tidak sama, maka program ini akan mengubah data file di basis data yang menandakan bahwa file tersebut telah termodifikasi.

### Rancangan Antarmuka

Perancangan antarmuka pengguna merupakan hal yang penting dalam melakukan perancangan sistem. Antarmuka pengguna berhubungan langsung dengan aktor yang harus mudah dipahami oleh pengguna. Selain mudah dipahami, antarmuka juga harus menarik bagi para pengguna. Sistem ini memiliki beberapa antarmuka pengguna yang mana akan dijelaskan di bawah ini.

#### Antarmuka Masuk ke Sistem

Halaman ini ajan digunakan untuk kebutuhan masuk ke sistem (UC-001). Pada halaman ini terdapat dua isian yang harus diisi pengguna untuk masuk ke dalam sistem yaitu email dan password. Setelah itu pengguna diharuskan menekan tombol login untuk masuk ke sistem. Rancangan halaman antarmuka login bisa dilihat pada gambar di bawah ini.



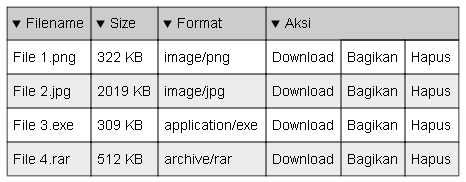
#### Antarmuka Registrasi

Halaman ini digunakan untuk kebutuhan registrasi pengguna (UC-002). Pada halam ini terdapat empat isian yang harus diisi oleh pengguna untuk registrasi, yaitu email, nama, password dan konfirmasi password. Setelah itu pengguna diharuskan untuk menekan tombol register untuk mendaftar. Rancangan halaman antarmuka registrasi bisa dilihat pada gambar di bawah ini.



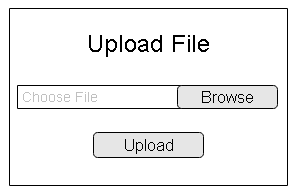
#### Antarmuka File Saya

Halaman ini digunakan untuk kebutuhan melihat file.pada halaman ini terdapat tabel yang memiliki empat kolom yaitu Filename, Size, Format dan Aksi. Pada kolom Aksi terdapat tombol tiga tombol yaitu Download, Bagikan dan Hapus. Rancangan antarmuka dari melihat File dapat dilihat pada gambar dibawah ini.



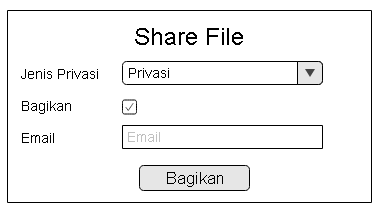
#### Antarmuka Unggah File

Halam ini digunakan untuk kebutuhan mengunggah file. Terdapatsatu isian yang digunakan untuk memilih file yang akan diunggah. Setelah pengguna memilih file pengguna diharuskan untuk menekan tombol Upload untuk mengngaah file yang telah dipilih tersebut. Rancangan antarmuka dari mengunggah file bisa dilihat dibawah ini.



#### Antarmuka Berbagi File

Halaman ini digunakan untuk kebutuhan Berbagi File. Pada awalnya halaman ini memiliki dua isian yang pertama adalah pilihan Jenis Privasi yang berisikan Privasi dan Publik.

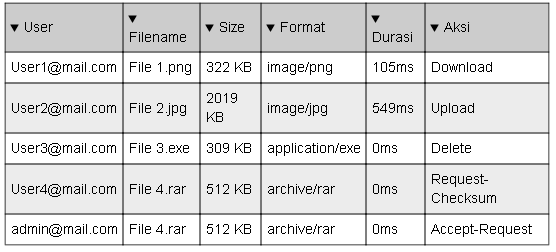


#### Antarmuka Meminta Checksum

Halaman ini digunakan untuk kebutuhan meminta checksum. Halaman ini menampilkan form yang berisikan tentang biodata pengguna dan alasan mengapa pengguna meminta checksum tersebut

#### Antarmuka Log Aktivitas

Halaman ini digunakan untuk kebutuhan monitoring aktivitas. Halaman ini menampilkan tabel yang memiliki 6 kolom yaitu User, Filename, Size, Format, Durasi dan Aksi. Rancangan antarmuka dari monitoringaktivitas bisa dilihat pada gambar di bawah ini.



# BAB IV IMPLEMENTASI

Pada bab ini akan dibahas mengenai implementasi sistem sesuai dengan analisis dan perancangan proses bisnis secara umum pada sistem Penyimpanan Data yang telah dijabarkan pada bab sebelumnya.

Implementasi yang akan dijelaskan meliputi lingkungan pembangunan sistem atau perangkat lunak, kode sumber utama yang berisi *pseudocode*, implementasi antarmuka perangkat lunak dan implementasi *client*. Arsitektur sistemyang digunakan adalah MVC dengan kerangka kerja Laravel.



## Lingkungan Pembangunan Sistem

Lingkungan sistem yang digunakan untuk membangun perangkat lunak ini:

1. Windows 10 Enterprise sebagai sistem operasi
2. Sublime Text Editor 3128 sebagai *Integrated Development Environment (IDE)*
3. Laravel 5.8 sebagai kerangka kerja (*framework*)
4. PHP 7.2.12 sebagai bahasa pemrograman yang digunakan.
5. Python 3.7.3 sebagai bahasa pemrograman untuk program pihak ketiga.
6. MariaDB Server 10.1.37 (MySQL) dan HeidiSQL sebagai sistem manajemen basis data
7. Apache 2.4.37 sebagai *web server*

## Membuat Proyek Laravel Baru

## Implementasi Model

### Model User

### Model File

### Model Log

### Model Sharing

## Implementasi Controller

### Controller Home

#### Fungsi Index

### Controller File

Fungsi Index

Fungsi formUpload

Fungsi upload

Fungsi download

### Controller Log

Fungsi index

### Controller Sharing

Fungsi index

Fungsi form

Fungsi update\_share

## Implementasi View

***(Halaman ini sengaja dikosongkan)***

# BAB V UJI COBA DAN EVALUASI

Bab ini membahas mengenai uji coba yang dilakukan dan evaluasi sesuai dengan rancangan dan implementasi. Dari hasil yang didapatkan setelah melakukan uji coba, akan dilakukan evaluasi sehingga dapat diambil kesimpulan untuk bab selanjutnya.

## Lingkungan Uji Coba

Uji coba dilakukan pada perangkat dengan spesifikasi seperti yang tertera pada Tabel 5.1.

*Tabel 3.12.1 Spesifikasi Perangkat yang Digunakan*

|  |  |
| --- | --- |
| **Komponen** | **Spesifikasi** |
| **CPU** | Intel(R) Core(TM) i5-7400 CPU @ 3.00GHz 3.00 GHz |
| **Sistem Operasi** | Ubuntu Bionic 18.04 LTS 64 bit |
| **Linux Kernel** | Linux kernel 4.4 |
| **Memori** | RAM 8 GB |
| **Penyimpanan** | 928 GB |

Pengujian dilakukan dengan menjalankan skenario yang disimulasikan menggunakan NS-2. Dari simulasi tersebut dihasilkan sebuah *trace file* dengan ekstensi .tr yang akan dianalisis menggunakan skrip AWK untuk mendapatkan *Packet Delivery Ratio*, *Routing Overhead*, dan *Delivery Delay* dengan kode masing-masing pada lampiran 7. Kode Skrip AWK *Packet Delivery Ratio*, lampiran 8. Kode Skrip AWK *Routing* *Overhead*, dan lampiran 9. Kode Skrip AWK *Delivery Delay*.

.

# BAB VI KESIMPULAN DAN SARAN

Bab ini membahas mengenai kesimpulan yang diperoleh dari tugas akhir yang telah dikerjakan dan saran terkait pengembangan dari tugas akhir ini yang dapat dilakukan pada masa yang akan datang.

## Kesimpulan

## Saran

***(Halaman ini sengaja dikosongkan)***

# DAFTAR PUSTAKA

|  |  |
| --- | --- |
| [1] | Hermansyah, Hukum Perbankan Nasional: Edisi Kedua, Jakarta: : Prenadamedia Group, 2014. |
| [2] | S. M. Happy Susanto, Panduan Lengkap Menyusun Proposal, Jakarta: Visimedia, 2010. |
| [3] | M. Dr. Andri Soemitra, Bank dan Lembaga Keuangan Syariah, Depok: Kencana, 2009. |
| [4] | M. Dr. Rozalinda, Fikih Ekonomi Syariah: Prinsip dan Implementasinya Pada Sektor Keuangan Syariah, Jakarta: Rajawali Pers, 2016. |
| [5] | B. K. Adhikary, Crowdfunding: Lessons from Japan's Approach, Singapura: Springer, 2018. |
| [6] | Y. Yudhanto, Panduan Mudah Belajar Framework Laravel, Jakarta: Gramedia, 2018. |
| [7] | S. Anhar, PHP & MySql Secara Otodidak, Jakarta: Mediakita, 2010. |
| [8] | W. Stallings, The Advanced Encryption Standard., San Jose: The Internet Protocol Journal, 2001. |
| [9] | V. Yuniati, Enkripsi Dan Dekripsi Dengan Algoritma Aes 256 Untuk Semua Jenis File, Jurnal Informatika Universitas Kristen Duta Wacana, 2009. |
| [10] | T. Tambunan, Usaha Mikro Kecil dan Menengah di Indonesia (Isu-Isu Penting), Jakarta: LP3ES, 2012. |
| [11] | C. P. E, Trik Sukses Menuju Sukses, Yogyakarta: 2000, Grafika Indah. |

***(Halaman ini sengaja dikosongkan)***

# LAMPIRAN

# BIODATA PENULIS

 Muhammad Fajri Salam lahir di Bojonegoro pada tanggal 28 September 1996. Penulis menempuh pendidikan formal di TK Bustanul Athfal Sumberrejo (2001-2003), MI Muhammadiyah Sumberrejo Bojonegoro (2003-2009), SMP Plus Ar-Rahmat Bojonegoro (2009-2012), SMAN Model Terpadu Bojonegoro (2012-2015), dan Informatika ITS Surabaya (2015-2019). Bidang studi yang diambil oleh penulis saat berkuliah di Departemen Informatika ITS adalah Arsitektur Jaringan Komputer (AJK). Penulis aktif dalam organisasi Himpunan Mahasiswa Teknik Computer-Informatika 2017-2018 di Departemen Kesejahteraan Mahasiswa dan Keluarga Muslim Informatika 2017-2018 di Departemen Keilmuan. Penulis juga aktif dalam kegiatan kepanitiaan seperti SCHEMATICS 2016-2017 divisi Kamzin, Kegiatan Mentoring dari Keluarga Muslim Informatika 2016-2017 dan Kegiatan Mentoring dari Jamaah Masjid Manarul Ilmi 2017-2018. Penulis juga pernah menjadi admin dan *developer* di admindt.net dan menjadi *developer* ppdbriau.net. Penulis dapat dihubungi melalui nomor handphone 08970427472 atau melalui email fajrisalam289@gmail.com

***(Halaman ini sengaja dikosongkan)***