**IMPLEMENTASI ONTOLOGI SEMANTIK PADA RANCANG BANGUN SISTEM MANAJEMEN PENGETAHUAN GAMELAN BALI BERBASIS WEB**

**SKRIPSI**



**OLEH:**

**I MADE WARDANA**

**NIM. 1608561029**

**PROGRAM STUDI INFORMATIKA**

**FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM**

**UNIVERSITAS UDAYANA**

**BUKIT JIMBARAN**

**2020**

# LEMBAR PERNYATAAN

Saya yang bertandatangan dibawah ini:

|  |  |  |
| --- | --- | --- |
| Nama | : | I Made Wardana |
| NIM | : | 1608561029 |
| Program Studi | : | Teknik Informatika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Udayana |
| Judul | : | Implementasi Ontologi Semantik dalam Rancang Bangun Sistem Manajemen Pengetahuan Gamelan Bali Berbasis Web |

Menyatakan dengan sesungguhnya bahwa karya tulis tugas akhir ini benar-benar saya kerjakan sendiri.

Karya tulis tugas akhir ini bukan merupakan plagiarisme, pencurian hasil karya milik orang lain, hasil kerja orang lain untuk kepentingan saya karena hubungan material maupun non material, ataupun segala kemungkinan lain yang pada hakekatnya bukan merupakan karya tulis tugas akhir saya secara orisinil dan otentik.

Pernyataan ini saya buat dengan kesadaran sendiri dan tidak atas tekanan ataupun paksaan dari pihak manapun demi meningkatkan integritas akademik di institusi ini.

Bukit Jimbaran, 16 April 2020

I Made Wardana

# LEMBAR PENGESAHAN TUGAS AKHIR

Judul : Implementasi Algoritma RSA pada Sistem Layanan

Musik Streaming Khusus Musik Tradisional Berbasis

Web

Kompetensi : Keamanan Digital

Nama : I Gusti Ngurah Guna Wicaksana

NIM : 1608561050

Tanggal Seminar : 06 Maret 2020

Disetujui oleh:

Pembimbing I

Ida Bagus Made Mahendra , S.Kom., M.Kom.

NIP. 198006212008121002

-

Penguji I

I Putu Gede Hendra Suputra, S.Kom., M.Kom.

NIP. 198812282014041001

-

Pembimbing II

Gusti Ayu Vida Mastrika Giri, S.Kom., M.Cs.

NIP. 1990060620181123001

-

Penguji II

I Komang Ari Mogi, S.Kom., M.Kom.

NIP. 198409242008011007

-

Penguji III

Dr. Ir. I Ketut Gede Suhartana, S.Kom., M.Kom.

NIP. 197201102008121001

-

Mengetahui,

Program Studi FMIPA Universitas Udayana

Ketua

Dr. Ir. I Ketut Gede Suhartana, S.Kom., M.Kom.

NIP. 197201102008121001

-

Judul : Implementasi Algoritma RSA pada Sistem Layanan Musik

*Streaming* Khusus Musik Tradisional Berbasis Web

Nama : I Gusti Ngurah Guna Wicaksana

Pembimbing : 1. Ida Bagus Made Mahendra , S.Kom., M.Kom.

2. Gusti Ayu Vida Mastrika Giri, S.Kom., M.Cs.

# ABSTRAK

Musik di Indonesian tumbuh dan berkembang dengan pesat, mulai dari yang tradisional hingga yang tergolong musik modern. Namun kini di era digital, pesatnya perkembangan musik modern yang dengan sangat mudah diakses melalui berbagai layanan internet yang berimbas pada semakin tergerusnya musik tradisional daerah, selain itu masih kurangnya *platform* digital untuk mempermudah akses masyarakat menikmati musik tradisional. Maka melalui tugas akhir ini dikembangkannya sistem layanan musik tradisional berbasis web.

Dalam membangun sebuah sistem, keamanan data adalah salah satu hal yang paling perlu diprioritaskan, data dapat diamankan dengan penerapan kriptografi, dan algoritma kriptografi yang digunakan pada penelitian ini adalah RSA (Rivest Shamir Adleman). Mekanisme kerja algoritma RSA cukup sederhana dan mudah dimengerti, tetapi tetap kokoh.

Berdasarkan hasil pengujian terhadap data audio MP3 menunjukan bahwa algoritma RSA dapat diterapkan pada file audio MP3 pada sistem layanan musik berbasis web dan nilai pengujian *avalanche effect* terhadap algoritma RSA pada sistem diperoleh rata-rata nilai sebesar 54,2%, sehingga dapat disimpulkan algoritma RSA yang diimplementasikan pada sistem ini sangat baik.

Kata Kunci : MP3, Musik Tradisional, Algoritma RSA, Sistem Layanan Musik, *Avalanche Effect*

Judul : Implementation of the RSA Algorithm in the Music Service

System Streaming Special Traditional Music Web Based

Name : I Gusti Ngurah Guna Wicaksana

Supervisor : 1. Ida Bagus Made Mahendra , S.Kom., M.Kom.

2. Gusti Ayu Vida Mastrika Giri, S.Kom., M.Cs.

# ABSTRACT

Music in Indonesia grows and develops rapidly, ranging from traditional to modern music. But now in the digital era, the rapid development of modern music which is very easily accessed through various internet services has an impact on the erosion of traditional regional music, while still improving the digital platform to facilitate public access to enjoy traditional music. So through this thesis the development of a traditional web-based music service system.

In building a system, data security is one of the things that needs to be prioritized the most, data can be secured using cryptography, and the cryptographic algorithm used in this study is RSA (Rivest Shamir Adleman). RSA is quite easy and easy to use, but still sturdy.

Based on the results of testing of MP3 audio data shows that RSA can be applied to MP3 audio files on a web-based music service system and the test value of the avalanche effect on the RSA algorithm on the system obtained an average value of 54.2%, can be concluded on the RSA algorithm that implemented on this system is very good.

Keywords : MP3, Traditional Music, RSA Algorithm, Music Service System, Avalanche Effect

# KATA PENGANTAR

Penelitian dengan judul “IMPLEMENTASI ONTOLOGI SEMANTIK PADA RANCANG BANGUN SISTEM MANAJEMEN PENGETAHUAN GAMELAN BALI BERBASIS WEB” ini disusun dalam rangkaian kegiatan pelaksanaan Tugas Akhir di Program Studi Teknik Informatika FMIPA UNUD. Laporan tugas akhir ini disusun dengan harapan dapat menjadi pedoman dan referensi bagi pembaca dan peneliti lainnya.

Sehubungan dengan telah terselesaikannya penelitian ini, maka diucapkan terima kasih dan penghargaan kepada berbagai pihak yang telah membantu penyusun, antara lain:

1. Bapak Dr. Ir. I Ketut Gede Suhartana, S.Kom., M.Kom. selaku Koordinator Prodi Teknik Informatika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Udayana;
2. Bapak Cokorda Rai Adi Pramartha, ST.MM.Ph.D dan Bapak Ida Bagus Gede Dwidasmara, S.Kom., M.Cs selaku dosen pembimbing yang telah banyak membimbing dan menyempurnakan penelitian ini;
3. Kawan-kawan mahasiswa di Program Studi Teknik Informatika yang telah memberikan dukungan, motivasi dan semangat dalam melakukan penelitian dan penulisan tugas akhir ini;
4. Keluarga, kerabat serta semua pihak yang turut serta dalam memberikan dukungan semangat dan motivasi sehingga tugas akhir ini dapat terselesaikan.

Disadari pula bahwa sudah tentu hasil-hasil dari penelitian ini masih mengandung kelemahan dan kekurangan. Memperhatikan hal ini, maka masukan dan saran-saran penyempurnaan sangat diharapkan.

Bukit Jimbaran, April 2020

Penulis

# DAFTAR ISI

[LEMBAR PERNYATAAN ii](#_Toc35471710)

[LEMBAR PENGESAHAN TUGAS AKHIR iii](#_Toc35471711)

[ABSTRAK iv](#_Toc35471712)

[ABSTRACT v](#_Toc35471713)

[KATA PENGANTAR vi](#_Toc35471714)

[DAFTAR ISI viii](#_Toc35471715)

[DAFTAR TABEL xi](#_Toc35471716)

[DAFTAR GAMBAR xii](#_Toc35471717)

[DAFTAR LAMPIRAN xiv](#_Toc35471718)

[BAB I 1](#_Toc35471719)

[PENDAHULUAN 1](#_Toc35471720)

[1.1 Latar Belakang 1](#_Toc35471721)

[1.2 Rumusan Masalah 3](#_Toc35471722)

[1.3 Batasan Masalah 3](#_Toc35471723)

[1.4 Tujuan penelitian 3](#_Toc35471724)

[1.5 Manfaat Penelitian 4](#_Toc35471725)

[1.6 Metodologi Penelitian 4](#_Toc35471726)

[1.6.1 Desain Penelitian 5](#_Toc35471727)

[1.6.2 Pengumpulan data 6](#_Toc35471728)

[1.6.3 Metode Pengembangan Sistem 6](#_Toc35471729)

[BAB II 9](#_Toc35471730)

[TINJAUAN PUSTAKA 9](#_Toc35471731)

[2.1 Tinjauan Studi 9](#_Toc35471732)

[2.2 Website 12](#_Toc35471733)

[2.3 File MP3 15](#_Toc35471734)

[2.4 Musik Tradisional Bali 15](#_Toc35471735)

[2.5 Audio Streaming 17](#_Toc35471736)

[2.5.1 HTTP Streaming 18](#_Toc35471737)

[2.6 Kriptografi 19](#_Toc35471738)

[2.6.1 Sejarah Kriptografi 20](#_Toc35471739)

[2.6.2 Tujuan Kriptografi 23](#_Toc35471740)

[2.7 Algoritma RSA 24](#_Toc35471741)

[*2.8* *System Development Life Cycle (SDLC)* 26](#_Toc35471742)

[2.9 Pengujian Avalanche Effect 29](#_Toc35471743)

[BAB III 30](#_Toc35471744)

[ANALISIS DAN PERANCANGAN SISTEM 30](#_Toc35471745)

[3.1 Analisis Kebutuhan 30](#_Toc35471746)

[3.1.1 Kebutuhan Fungsional 30](#_Toc35471747)

[3.1.2 Kebutuhan Non Fungsional 31](#_Toc35471748)

[3.2 Rancangan Data 32](#_Toc35471749)

[3.3 Rancangan Umum Sistem dengan Penerapan Algoritma RSA 32](#_Toc35471750)

[3.4 Rancangan Use-Case 34](#_Toc35471751)

[3.4.1 Dekripsi Use Case 35](#_Toc35471752)

[3.5 Rancangan Antarmuka Sistem 36](#_Toc35471753)

[3.6 Rancangan Database 44](#_Toc35471754)

[3.6.1 ERD (Entity Relationship Diagram) 44](#_Toc35471755)

[3.6.2 Conceptual Data Model 45](#_Toc35471756)

[3.6.3 Physical Data Model 46](#_Toc35471757)

[3.7 Pengolahan Data 46](#_Toc35471758)

[3.8 Pengujian dan Evaluasi 47](#_Toc35471759)

[3.8.1 Pengujian Fungsionalitas 47](#_Toc35471760)

[3.8.2 Pengujian Data Audio MP3 49](#_Toc35471761)

[3.8.3 Pengujian Keamanan Algoritma RSA 50](#_Toc35471762)

[BAB IV 51](#_Toc35471763)

[HASIL DAN PEMBAHASAN 51](#_Toc35471764)

[4.1 Pengumpulan Data Set 51](#_Toc35471765)

[4.2 Diagram Alir Pembentukan Kunci pada Sistem 51](#_Toc35471766)

[4.3 Diagram Alir Pembentukan Kunci Public dan Private 52](#_Toc35471767)

[4.4 Diagram Alir Proses Enkripsi terhadap Path Data Musik 54](#_Toc35471768)

[4.5 Diagram Alir Dekripsi Path Data Musik 55](#_Toc35471769)

[4.6 Diagram Alir Enkripsi Karakter pada Data MP3 56](#_Toc35471770)

[4.7 Diagram Alir Enkripsi Karakter pada Chiperteks File MP3 58](#_Toc35471771)

[4.8 Implementasi Sistem 59](#_Toc35471772)

[4.8.1 Lingkungan Implementasi 59](#_Toc35471773)

[4.8.2 Pembuatan Basis Data 60](#_Toc35471774)

[4.8.3 Membuat Kode Program 63](#_Toc35471775)

[4.9 Tampilan Antarmuka Sistem 63](#_Toc35471776)

[4.10 Pengujian Sistem 67](#_Toc35471777)

[4.10.1 Pengujian Fungsionalitas Sistem 67](#_Toc35471778)

[4.10.2 Pengujian Keamanan Algoritma RSA 72](#_Toc35471779)

[4.10.3 Pengujian Data Audio MP3 84](#_Toc35471780)

[BAB V 89](#_Toc35471781)

[KESIMPULAN DAN SARAN 89](#_Toc35471782)

[5.1 Kesimpulan 89](#_Toc35471783)

[5.2 Saran 89](#_Toc35471784)

[DAFTAR PUSTAKA 90](#_Toc35471785)

# DAFTAR TABEL

[Tabel 2. 1 Contoh Hasil Pengujian Avalanche Effect (Wibowo, M., & Saputra, 2015) 29](#_Toc35779081)

[Tabel 3. 1 Kebutuhan Fungsional………………………………………………..30](#_Toc35779100)

[Tabel 3. 2 Pengujian Blackbox 48](#_Toc35779101)

[Tabel 3. 3 Hasil Pengujian Blackbox 48](#_Toc35779102)

[Tabel 3. 4 Tabel Pengujian Gelombang Suara Data MP3 49](#_Toc35779103)

[Tabel 3. 5 Perbandingan Ukuran Data MP3 50](#_Toc35779104)

[Tabel 3. 6 Pengujian Avalanche Effect 50](#_Toc35779105)

[Tabel 4. 1 Daftar Spesifikasi Perangkat Keras…………………………….……..59](#_Toc35779120)

[Tabel 4. 2 Daftar Spesifikasi Perangkat Lunak 59](#_Toc35779121)

[Tabel 4. 3 Hasil Pengujian Fungsionalitas 68](#_Toc35779122)

[Tabel 4. 4 Hasil Pengujian Avalanche Effect Data Pertama 72](#_Toc35779123)

[Tabel 4. 5 Hasil Pengujian Avalanche Effect Data Kedua 73](#_Toc35779124)

[Tabel 4. 6 Hasil Pengujian Avalanche Effect Data Ketiga 74](#_Toc35779125)

[Tabel 4. 7 Hasil Pengujian Avalanche Effect Data Keempat 75](#_Toc35779126)

[Tabel 4. 8 Hasil Pengujian Avalanche Effect Data Kelima 77](#_Toc35779127)

[Tabel 4. 9 Hasil Pengujian Avalanche Effect Data Keenam 78](#_Toc35779128)

[Tabel 4. 10 Hasil Pengujian Avalanche Effect Data Keenam 79](#_Toc35779129)

[Tabel 4. 11 Hasil Pengujian Avalanche Effect Data Kedelapan 80](#_Toc35779130)

[Tabel 4. 12 Hasil Pengujian Avalanche Effect Data Kesembilan 81](#_Toc35779131)

[Tabel 4. 13 Hasil Pengujian Avalanche Effect Data Kesepuluh 82](#_Toc35779132)

[Tabel 4. 14 Tabel Pengujian Gelombang Suara Data MP3 84](#_Toc35779133)

[Tabel 4. 15 Tabel Perbandingan Ukuran Data MP3 87](#_Toc35779134)

# DAFTAR GAMBAR

[Gambar 2. 1 Arsitektur Dasar Streaming 18](#_Toc35778699)

[Gambar 2. 2 Mesin Enigma yang Digunakan Tentara Jerman pada Perang Dunia ke II (Munir, 2006) 23](#_Toc35778700)

[Gambar 2. 3 Waterfall Pressman (Pressman, 2015) 26](#_Toc35778701)

[Gambar 3. 1 Flowchart Sistem Secara Umum……………………...……..………...33](#_Toc35778713)

[Gambar 3. 2 Rancangan Use Case Sistem Layanan Musik 34](#_Toc35778714)

[Gambar 3. 3 Rancangan Halaman Utama 37](#_Toc35778715)

[Gambar 3. 4 Rancangan Halaman Pencarian 38](#_Toc35778716)

[Gambar 3. 5 Rancangan Halaman Penelusuran 39](#_Toc35778717)

[Gambar 3. 6 Rancangan Halaman Musik Saya 40](#_Toc35778718)

[Gambar 3. 7 Rancangan Halaman Akun 41](#_Toc35778719)

[Gambar 3. 8 Rancangan Halaman User Detail 42](#_Toc35778720)

[Gambar 3. 9 Rancangan Halaman Unggah Musik 43](#_Toc35778721)

[Gambar 3. 10 Rancangan ERD Sistem 44](#_Toc35778722)

[Gambar 3. 11 Rancangan Conceptual Data Model 45](#_Toc35778723)

[Gambar 3. 12 Rancangan Physical Data Model 46](#_Toc35778724)

[Gambar 4. 1 Diagram Alir Proses Pembentukan Kunci Pengguna………………52](#_Toc35778745)

[Gambar 4. 2 Diagram Alir Pembentukan Kunci Public dan Private 53](#_Toc35778746)

[Gambar 4. 3 Diagram Alir Proses Enkripsi terhadap Path Data Musik 54](#_Toc35778747)

[Gambar 4. 4 Diagram Alir Dekripsi Path Data Musik 55](#_Toc35778748)

[Gambar 4. 5 Diagram Alir Enkripsi Pada Karakter MP3 57](#_Toc35778749)

[Gambar 4. 6 Diagram Alir Dekripsi Pada Chiperteks File MP3 58](#_Toc35778750)

[Gambar 4. 7 Tabel artist pada Database 60](#_Toc35778751)

[Gambar 4. 8 Tabel froms pada Database 61](#_Toc35778752)

[Gambar 4. 9 Tabel genres pada Database 61](#_Toc35778753)

[Gambar 4. 10 Tabel playlists pada Database 61](#_Toc35778754)

[Gambar 4. 11 Tabel playlistsongs pada Database 62](#_Toc35778755)

[Gambar 4. 12 Tabel songs pada Database 62](#_Toc35778756)

[Gambar 4. 13 Tabel users pada Database 63](#_Toc35778757)

[Gambar 4. 14 Tampilan Halaman Registrasi 63](#_Toc35778758)

[Gambar 4. 15 Tampilan Halaman Utama 64](#_Toc35778759)

[Gambar 4. 16 Tampilan Halaman Pencarian 64](#_Toc35778760)

[Gambar 4. 17 Tampilan Halaman Musik Saya 65](#_Toc35778761)

[Gambar 4. 18 Tampilan Halaman Akun 66](#_Toc35778762)

[Gambar 4. 19 Tampilan Halaman User Detail 66](#_Toc35778763)

[Gambar 4. 20 Tampilan Halaman Unggah 67](#_Toc35778764)

[Gambar 4. 21 Gelombang Suara Data Audio Asli 86](#_Toc35778765)

[Gambar 4. 22 Gelombang Suara Data Audio Terenkripsi 86](#_Toc35778766)

[Gambar 4. 23 File MP3 Terenkripsi Tidak Dapat Diakses 88](#_Toc35778767)

# DAFTAR LAMPIRAN

LAMPIRAN A DESKRIPSI USE-CASE………………………………………..93

LAMPIRAN B SOURCECODE PROGRAM………………………………….100

# BAB I

# PENDAHULUAN

## Latar Belakang

Indonesia memiliki banyak jenis warisan budaya dan seni. Salah satu warisan budaya dan seni tersebut adalah gamelan Bali. Jumlah gamelan yang tersebar di suatu daerah di Indonesia, khususnya di Provinsi Bali dan instrumennya sangat beragam. Keberagaman informasi mengenai gamelan Bali ini harus dideskripsikan dengan baik (Spiller, 2004).

Namun, pengetahuan tentang gamelan Bali masih cenderung kurang terkumpul secara eksplisit. Hal tersebut menghasilkan pengetahuan warisan budaya, khususnya gamelan Bali yang menantang untuk dipelajari oleh generasi muda dan masa depan Bali. Oleh karena itu, keragaman pengetahuan tentang gamelan Bali harus didokumentasikan dan dijelaskan dengan baik, terutama dalam bentuk digital.

Oleh karena kompleksnya ruang lingkup karakteristik dari instrumen musik tradisional, dibutuhkan representasi dari pengetahuan berbasis web semantik (Kolozali, 2011). Secara teknis, sebuah pengetahuan direpresentasikan dalam bentuk kelas-kelas, deskripsi data, penempatan, dan obyek ke dalam sebuah skema ontologi. Pengetahuan direpresentasikan dengan menggunakan perangkat lunak Protégé dengan harapan pembaruan yang fleksibel dan dapat diimplementasikan ke dalam bentuk pengetahuan lainnya.

Penggunaan ontologi sebagai teknik representasi informasi menjadi pilihan solusi dalam permasalahan ini. Ontologi pada semantic web adalah sebuah katalog dimana skemanya menggunakan ontologi. Ontologi diperlukan untuk meningkatkan pengembangan aplikasi semantik terutama di web semantik perusahaan, yang terdiri dari penerapan teknologi semantik di lingkungan perusahaan (Zhou, 2010). Ontologi untuk warisan budaya Bali, khususnya gamelan Bali, dapat digunakan untuk menangkap, mendokumentasikan, dan merepresentasikan pengetahuan yang melingkupi domain gamelan Bali.

Teknologi semantik memungkinkan menggambarkan objek dan repository dalam bentuk ontologi. Ontologi merepresentasikan pengetahuan pada level semantik karena ontologi berisikan entitas semantik (concept, relation dan instance) sebagai pengganti kata. Selain itu ontologi memungkinkan untuk menspesifikasikan hubungan semantik antar entitas dan juga untuk menyimpan fakta dan aksioma tentang domain pengetahuan (Salton, 1993).

Ontologi yang ada saat ini yang merangkum instrumen gamelan belum dapat merepresentasikan kekayaan instrumen musik tradisional di Indonesia. Terlebih di Bali, yang merupakan daerah yang kaya akan warisan instrumen musik tradisional yang disebut gamelan (Tenzer, 2000). Hal tersebut tidak lepas dari kenyataan bahwa pengetahuan mengenai gamelan Bali masih berupa pengetahuan tacit. Artinya pengetahuan gamelan Bali merupakan warisan turun temurun, sehingga hanya warga tradisional saja yang memahaminya.

Ontologi merupakan cara untuk merepresentasikan pengetahuan dari sekumpulan konsep dalam sebuah domain informasi dan hubungan-hubungan (relationships) antara konsep-konsep tersebut, sehingga ontologi dapat digunakan untuk penyajian informasi secara semantik serta melakukan pengorganisasian dan pemetaan kumpulan sumber daya informasi secara sistematis dan terstruktur. Hal ini sangat berguna dalam hal interoperabilitas data karena dapat dilakukan dengan cara yang lebih efektif dan efisien (Davies et al., 2006). Sehingga, ketika pengetahuan instrumen tradisional yang telah diakuisisi secara eksplisit dikumpulkan dalam bentuk skema ontologi dan diimplementasikan ke dalam sebuah sistem manajemen pengetahuan gamelan Bali, kemudahan pengorganisasian dan manajemen data akan lebih terjamin berkat adanya ontologi semantik instrumen musik tradisional Bali.

Salah satu metode pengembangan ontologi yang banyak digunakan adalah metode Methontology. Metode Methontology merupakan salah satu metodologi pembangunan model ontologi yang terstruktur dengan baik yang digunakan untuk membangun ontologi dari awal. Metode ini memiliki keunggulan terkait dengan deskripsi setiap aktivitas yang harus dilakukan secara mendetail. Dengan menggunakan metode Methontology, ontologi yang dibangun dapat digunakan kembali untuk pengembangan sistem lebih lanjut (Fernández-López et al., 1997).

Dalam sebuah sistem berbasis web, semantik ontologi dapat digunakan sebagai basis pengetahuan atau metadata yang menerapkan konsep semantik. Sistem manajemen pengetahuan gamelan Bali berbasis web semantik yang dikembangkan akan menyediakan fungsi penjelajahan dan pencarian pengetahuan mengenai gamelan Bali berdasarkan informasi yang ada pada gamelan seperti nama instrumen gamelan, jenis instrumen gamelan, cara memainkan instrumen gamelan, dan informasi lain yang berhubungan dengan gamelan Bali.

Berdasarkan hal tersebut, penulis mencoba untuk meneliti lebih jauh mengenai bagaimana merancang sebuah sistem manajemen pengetahuan gamelan Bali berbasis teknologi web semantik. Tujuan utama dari penelitian ini adalah untuk mendokumentasikan dan berbagi informasi secara digital mengenai satu aspek dari warisan budaya Bali, yaitu alat musik tradisional atau gamelan. Sistem gamelan adalah bagian dari sistem instrumen musik tradisional Bali yang bervariasi dari satu kegiatan ke kegiatan lainnya dan tetap digunakan dalam komunitas Bali. Penulis mengubah pengetahuan budaya dan praktik terkait ke dalam bentuk eksplisit dan digital, agar publik dapat mengakses dan berbagi pengetahuan ini.

Pada penelitian ini, penulis mengembangkan ontologi yang telah dibangun untuk meningkatkan kualitas ontologi dan kemudian diterapkan ke dalam sistem pengetahuan gamelan Bali berbasis web semantik. Pembangunan ontologi menggunakan metode Methontology, sedangkan pembangunan sistem menggunakan metode Prototyping. Penulis kemudian membahas metode yang penulis gunakan untuk merancang, mengembangkan, mengimplementasikan dan mengevaluasi sistem manajemen pengetahuan yang diperkaya secara semantik untuk mendokumentasikan dan berbagi aspek penting dari gamelan sebagai salah satu warisan budaya Bali.

## Rumusan Masalah

Penelitian ini mengangkat 3 (tiga) buah rumusan yang menjadi pokok permasalahan dalam pendekatan dengan metode Methontology untuk pembangunan model ontologi gamelan Bali, pendekatan dengan metode Prototyping untuk rancang bangun sistem manajemen pengetahuan gamelan Bali, dan evaluasi sistem. Rumusan masalah tersebut adalah sebagai berikut.

### Bagaimana metode Methontology digunakan untuk mengembangkan ontologi gamelan Bali?

### Bagaimana metode Prototyping digunakan untuk merancang bangun sistem manajemen pengetahuan gamelan Bali berbasis web dengan mengimplementasikan ontologi gamelan Bali?

### Bagaimana pengujian dan evaluasi dilakukan terhadap sistem untuk mengetahui seberapa bermanfaat dan mudah digunakan sistem manajemen pengetahuan gamelan Bali berbasis web yang dikembangkan?

## Batasan Masalah

Berdasarkan latar belakang yang telah dipaparkan, batasan masalah dalam penelitian ini adalah sebagai berikut.

1. Mengimplementasikan metode Methontology sebagai metode pengembangan ontologi dan metode *Prototyping* sebagai metode pengembangan sistem.
2. Mengimplementasikan ontologi gamelan Bali pada program aplikasi berbasis website.
3. Lingkup pengetahuan yang digunakan adalah pengetahuan mengenai benda (*artefact*) dan praktik dari gamelan tradisional di Provinsi Bali.
4. Bahasa pemrogramanan yang digunakan untuk implementasi sistem adalah

PHP, JavaScript, dan SPARQL.

## Tujuan penelitian

Adapun tujuan dari penelitian ini adalah sebagai berikut.

1. Membangun model ontologi untuk memudahkan pengklasifikasian pengetahuan mengenai gamelan Bali yang kemudian diimplementasikan ke dalam sistem manajemen pengetahuan semantik berbasis web.
2. Membangun sistem manajemen pengetahuan gamelan Bali berbasis web, dimana sistem ini bertujuan untuk melakukan manajemen pengetahuan terkait gamelan Bali secara semantik.
3. Menguji seberapa mudahkah sistem yang dibangun digunakan dan seberapa berguna sistem yang dibangun terhadap aktivitas pengguna.

## Manfaat Penelitian

Penelitian ini memiliki manfaat untuk beberapa komponen, antara lain sebagai berikut.

1. Masyarakat: penelitian ini dapat memudahkan masyarakat dalam menjelajahi maupun melakukan pencarian mengenai pengetahuan gamelan Bali. Selain itu, dapat digunakan sebagai salah satu upaya pelestarian warisan budaya khususnya gamelan Bali dengan pemanfaatan teknologi informasi.
2. Keilmuan: penelitian ini dapat menjadi referensi pada penelitian lain yang memiliki karakteristik *ontology semantic web,* sistem manajemen pengetahuan,danwarisan budaya digital.

## Metodologi Penelitian

Metodologi merupakan suatu formula dalam penerapan penelitian yang terdapat langkah-langkah dan juga hasil penelitian di dalamnya (Maddison, R.N). Menurut Hasibuan Metodologi penelitian dalam Ilmu Komputer merupakan tahapan dalam perencanaan dengan menggunakan bantuan metode, teknik, *tools* dan pengarsipan bertujuan agar bisa meminimalkan resiko pada kegagalan dan memfokuskan pada proses penelitian di bidang ilmu komputer.

Pada metodologi penelitian ini akan dijelaskan langkah-langkah dalam penelitian ini, yaitu sebagai berikut.

### Desain Penelitian

Pada bagian ini akan menjelaskan mengenai langkah-langkah yang akan dilakukan dalam perancangan dan implementasi sistem manajemen pengetahuan gamelan Bali berbasis web dengan menggunakan metode Methontology untuk membangun ontologi dan metode Prototyping untuk membangun sistem.

Tahapan pertama yang dilakukan dalam penelitian ini adalah mengidentifikasi permasalahan yang diangkat. Tahap ini merupakan salah satu tahap yang sangat penting dalam proses penelitian karena jalannya proses penelitian terlaksana berdasarkan permasalahan yang terjadi. Kemudian tahapan yang diperlukan selanjutnya adalah menentukan rumusan masalah dan tujuan yang ingin dicapai dalam penelitian ini. Pada penelitian ini identifikasi permasalahan dilakukan dengan pengamatan melalui studi pustaka. Dengan teknik ini maka akan dapat diketahui mengenai permasalahan yang diangkat.

Tahapan kedua yang dilakukan dalam penelitian ini yakni studi literatur. Studi literatur dilaksanakan dengan menggunakan literatur-literatur pendukung dari jurnal-jurnal ilmiah, baik jurnal nasional maupun jurnal internasional dan juga dari beberapa buku. Dalam studi literatur ini, penulis mencari sumber sumber terakit permasalahan-permasalahan yang perlu menjadi perbaikan dalam penelitian sebelumnya.

Tahap ketiga adalah pengumpulan data yang mendukung dalam permasalahan yang ingin diselesaikan. Metode pengumpulan data digunakan untuk mendapatkan data yang membantu proses dalam melakukan penelitian mengenai masalah yang dibahas.

Tahap keempat adalah membangun ontologi semantik gamelan Bali yang nantinya akan diimplementasikan ke dalam sistem. Ontologi dibangun dengan menggunakan metode Methontology.

Tahap kelima adalah membuat perancangan arsitektur dari sistem manajemen pengetahuan gamelan Bali berbasis web dengan menggunakan metode Prototyping. Perancangan dibuat dalam bentuk *flowchart* dan desain *use-case.*

Tahap keenam adalah mengimplemetasikan hasil perancangan ke dalam kode program sekaligus mengimplementasikan ontologi semantik gamelan Bali yang telah dibangun sebelumnya. Pada penelitian ini aplikasi yang dikembangkan adalah sistem aplikasi berbasis *website* menggunakan bahasa pemrograman PHP, JavaScript dan SPARQL.

Tahap terakhir adalah pengujian dan evaluasi sistem yang telah dibuat. Dalam penelitian ini akan dilakukan pengujian terhadap sistem yang telah dibangun dengan menggunakan pengujian *black box testing* dan pengujian akurasi sistem. Selain itu, juga dilakukan evaluasi terhadap sistem untuk mengetahui seberapa berguna dan seberapa mudah digunakankah sistem yang dibangun.

### Pengumpulan Data

Setelah tahapan identifikasi masalah, rumusan, dan tujuan masalah telah dilaksanakan, maka tahapan selanjutnya adalah tahap pengumpulan data. Pengumpulan data dilakukan dengan tujuan untuk mengetahui data apa saja yang dibutuhkan untuk menyelesaikan masalah.

Data dalam penelitian ini dibedakan menjadi 2 (dua), yaitu data untuk membangun model ontologi dan data hasil pengujian sistem. Dalam sistem manajemen pengetahuan gamelan Bali ini, sistem membutuhkan data untuk membangun model ontologi yang kemudian diimplementasikan ke dalam sistem untuk ditampilkan ke pengguna dalam bentuk informasi. Data yang dibutuhkan tersebut berupa kumpulan pengetahuan maupun informasi mengenai gamelan Bali. Sedangkan data hasil pengujian sistem merupakan data hasil pengujian dan evaluasi sistem berupa skor dari peserta yang melakukan serangkaian pengujian dan skala dari peserta yang melakukan evaluasi sistem.

Metode pengumpulan data dibedakan menjadi 2 (dua) yaitu metode pengumpulan data untuk membangun model ontologi dan metode pengumpulan data untuk pengujian dan evaluasi sistem. Metode pengumpulan data untuk membangun model ontologi dimaksudkan untuk mengumpulkan data-data pendukung yang dibutuhkan dalam proses pembuatan sistem manajemen pengetahuan gamelan Bali ini. Metode yang digunakan adalah melalui studi literatur, yaitu dengan mengumpulkan dan mempelajari sejumlah referensi dari berbagai sumber yang berkaitan dengan gamelan Bali. Selain itu, metode yang digunakan adalah melalui observasi, dimana penulis melakukan pengambilan data secara langsung ke objek penelitian, dalam hal ini gamelan yang terdapat di balai banjar, sekolah, maupun sanggar. Sedangkan metode pengumpulan data untuk pengujian dan evaluasi sistem adalah melalui kuesioner yang dibagikan kepada peserta pengujian dan evaluasi sistem.

### Metode Pembangunan Model

Metode yang digunakan dalam membangun model ontologi pada penelitian ini adalah metode Methontology. Metode Methontology merupakan salah satu metodologi pembangunan model ontologi yang memiliki keunggulan terkait dengan deskripsi setiap aktivitas yang harus dilakukan secara mendetail. Selain itu, metode Methontology juga memiliki kemampuan yaitu ontologi yang dibangun dapat digunakan kembali untuk pengembangan sistem lebih lanjut (Fernández-López et al., 1997). Berikut ini tahapan dari metode pembangunan model dengan metode Methontology.

* + 1. Tahap Spesifikasi

Dalam tahap ini, dihasilkan deskripsi dari ontologi gamelan Bali sebagai berikut.

1. Domain: Gamelan Bali
2. Tujuan: Untuk membangun model ontologi untuk memudahkan pengklasifikasian gamelan Bali
3. Tingkat formalitas: Semi formal
4. Ruang lingkup: Gamelan Bali
5. Sumber pengetahuan: Buku, jurnal, internet
   * 1. Tahap Akuisisi Pengetahuan

Dalam tahap ini, teknik-teknik yang penulis gunakan untuk mengakuisisi pengetahuan ontologi Gamelan Bali adalah sebagai berikut.

1. Berdiskusi dengan pembimbing maupun narasumber terkait untuk membangun draf awal dokumen spesifikasi persyaratan.
2. Analisis teks informal, untuk mempelajari konsep-konsep utama yang diberikan dalam buku dan studi pegangan.
3. Analisis teks formal. Hal yang dilakukan adalah mengidentifikasi struktur yang akan dideteksi (definisi, penegasan, dan lain-lain) dan jenis pengetahuan yang dikontribusikan oleh masing-masing (konsep, atribut, nilai, dan hubungan).

Data yang digunakan untuk membangun model ontologi dalam penelitian ini adalah data mengenai gamelan di Provinsi Bali. Data ini diperoleh baik dari buku, jurnal, maupun sumber internet yang dapat dipercaya.

* + 1. Tahap Konseptualisasi

Dalam tahap ini, dihasilkan model konseptual dari ontologi gamelan Bali.

* + 1. Tahap Integrasi

Dalam tahap ini, penulis mengintegrasikan model ontologi yang dibuat dengan kerangka kerja Tri Hita Karana (THK) dan Desa Kala Patra (DKP) yang diusulkan oleh Pramartha (2016).

* + 1. Tahap Implementasi

Dalam tahap ini, dilakukan proses pendefinisian kembali dan proses implementasi dari rancangan ontologi gamelan Bali menggunakan perangkat lunak Protégé.

* + 1. Tahap Evaluasi

Dalam tahap ini, dilakukan proses evaluasi ontologi gamelan Bali menggunakan perangkat lunak Protégé.

* + 1. Tahap Dokumentasi

Pada tahap terakhir ini, dilakukan proses dokumentasi ontologi ontologi gamelan Bali baik dalam kode ontologi, teks bahasa alami yang dilampirkan pada definisi formal, maupun makalah yang diterbitkan dalam proses konferensi dan jurnal yang mengatur pertanyaan-pertanyaan penting dari ontologi yang sudah dibangun.

### Metode Pengembangan Sistem

Metode pengembangan sistem yang digunakan untuk membuat Sistem Manajemen Pengetahuan Gamelan Bali Berbasis Web adalah metode *Prototyping.* Metode *Prototyping* meliputi beberapa tahapan antara lain pengumpulan kebutuhan, membangun *prototyping,* evaluasi *prototyping,* pembangunan sistem, pengujian sistem, dan evaluasi sistem.

Berikut ini penjelasan dari masing-masing langkah tersebut.

1. **Pengumpulan Kebutuhan**

Tahapan ini bertujuan untuk mengidentifikasikan format seluruh perangkat lunak, mengidentifikasikan semua kebutuhan, dan garis besar sistem yang akan dibuat. Pada tahapan ini dilakukan beberapa kegiatan antara lain sebagai berikut.

1. Pengumpulan informasi dan data

Diperlukan data dan informasi yang terkait dengan topik yang diangkat, yaitu gamelan Bali. Untuk mendapatkan data dan informasi tersebut, dilakukan dengan cara membaca berbagai jenis referensi buku, artikel di internet maupun sumber terpercaya lainnya.

1. Kebutuhan perangkat lunak dan perangkat keras

Perangkat lunak yang dibutuhkan adalah Protégé, Visual Studio Code, Apache Jena Fuseki, EasyRDF, dan XAMPP. Sedangkan perangkat keras yang dibutuhkan adalah komputer atau laptop.

1. **Membangun *Prototyping***

Membangun *prototyping* dengan membuat perancangan sementara yang berfokus pada penyajian, misalnya dengan membuat input dan format output. Bentuk perancangan sistem yang dibuat antara lain dengan membuat diagram alir sistem, *activity diagram*, *work breakdown structure*, perancangan antarmuka pengguna dan perancangan ontologi.

1. **Evaluasi *Prototyping***

Evaluasi ini dilakukan untuk mengetahui apakah *prototyping* yang sudah dibangun sudah sesuai dengan keinginan. Selain evaluasi, terdapat kegiatan revisi atau perbaikan perancangan hingga sistem dinyatakan benar dan layak untuk dibuat.

1. **Pembangunan Sistem**

Pada tahapan ini yaitu memulai membangun sistem yang sesuai dengan perancangan atau *prototyping* sebelumnya. Pembangunan sistem dilakukan dengan beberapa tahapan antara lain sebagai berikut.

1. Pemodelan ontologi. Pemodelan ontologi adalah pemodelan dengan menggunakan perangkat lunak Protégé 4.3, sehingga menghasilkan file OWL (*web ontology language*).
2. Penentuan domain. Domain yang ditentukan pada sistem ini adalah pengetahuan gamelan Bali.
3. Penentuan *class*. Dalam menentukan *class*, dilakukan dengan melakukan konseptualisasi berdasarkan data yang didapat.
4. Mendefinisikan *slot* atau *properties*, yaitu mendefinisikan *properties* yang digunakan sebagai penghubung antar *class* atau antar individu.
5. Membuat *instances*, yaitu membuat *instances* atau individu untuk tiap-tiap *class*.
6. Pengkodean. Pada tahap pengkodean, dilakukan proses mengintegrasikan file OWL dengan bahasa pemrograman PHP dan bahasa *query* SPARQL. Selain itu, juga menggunakan *library* EasyRDF sebagai *parser* dari file OWL.
7. **Pengujian Sistem**

Setelah sistem selesai dibangun, dilakukan pengujian terhadap sistem.  Pengujian yang dilakukan untuk menguji sistem dilakukan dengan 2 (dua) langkah pengujian, yaitu validasi dan pengujian akurasi sistem. Pengujian bertujuan untuk memastikan bahwa sistem yang dibangun telah berjalan sesuai dengan metode yang digunakan. Berikut ini langkah pengujian tersebut.

* + 1. Validasi

Uji coba validasi dikatakan berhasil apabila fungsi yang ada pada sistem sesuai dengan yang diharapkan pengguna. Validasi sistem merupakan kumpulan seri uji coba *Black Box* yang menunjukkan sistem dapat menjalankan sesuai dengan yang diperlukan.

* + 1. Pengujian Akurasi Sistem

Pengujian ini dilakukan untuk mengetahui keakuratan sistem manajemen pengetahuan gamelan Bali dalam menampilkan data hasil penjelajahan dan pencarian pengetahuan gamelan Bali oleh pengguna. Pengujian yang digunakan adalah pengujian *semantic browsing* dan *semantic searching*. Dalam pengujian ini penulis merekrut sejumlah peserta yang bersedia untuk melakukan pengujian sistem.

Peserta dimasukkan melalui sesi pelatihan singkat menggunakan video tutorial yang penulis sediakan di sistem manajemen pengetahuan. Video tutorial menguraikan langkah-langkah yang diperlukan untuk penelitian ini. Setelah menonton video tutorial, semua peserta diminta untuk melakukan berbagai tugas penjelajahan (*browsing*) dan pencarian (*searching*) menggunakan fitur dan fasilitas yang tersedia di sistem manajemen pengetahuan.

Tugas-tugas yang dilakukan oleh peserta dijabarkan sebagai berikut. Pertama, peserta diminta untuk melakukan tugas penjelajahan (eksplorasi sistem dengan mengikuti satu tautan menarik ke yang lain) pada modul penjelajahan. Di setiap tugas penjelajahan, peserta diminta untuk menjawab pertanyaan dengan membuat beberapa elemen kueri menggunakan modul penjelajahan sistem manajemen pengetahuan. Berikut ini contoh pertanyaan penjelajahan.

1. Sebutkan dua (2) nama gamelan yang digunakan untuk kegiatan manusa yadnya!

Kedua, peserta diminta untuk melakukan tugas pencarian (meminta sepotong informasi dari *database*) menggunakan modul pencarian sistem manajemen pengetahuan. Agar dapat menjawab pertanyaan menggunakan fasilitas pencarian, para peserta diminta untuk membangun beberapa elemen dari query sebagai filter input dan membentuk satu *query* kategori dari hirarki ontologi sebagai filter output, lalu diikuti dengan mengklik tombol pencarian. Berikut ini contoh dari pertanyaan pencarian:

1. Sebutkan dua (2) nama instrumen gamelan yang termasuk ke dalam gamelan Gong Kebyar, di mana instrumen terdapat dua (2) di setiap gamelan, pemasangannya berdampingan, dan memiliki 10 bilah nada!
2. **Evaluasi Sistem**

Tahap terakhir setelah dilakukan pengujian sistem yaitu melakukan evaluasi sistem. Sistem dievaluasi dari segi kebermanfaatan dan kemudahan penggunaan untuk mengetahui apakah pengguna menemukan sistem manajemen pengetahuan bermanfaat dan mudah digunakan dari perspektif belajar tentang gamelan Bali dan praktik terkait.

Evaluasi ini dirancang untuk menilai persepsi pengguna tentang kegunaan dan kemudahan penggunaan sistem manajemen pengetahuan. Kegunaan yang dirasakan didefinisikan sebagai "sejauh mana seseorang percaya bahwa menggunakan sistem tertentu akan meningkatkan kinerja pekerjaannya" (Davis, 1989). Sedangkan persepsi kemudahan penggunaan mengacu pada "sejauh mana seseorang percaya bahwa menggunakan sistem tertentu akan bebas dari upaya" (Davis, 1989).

Proses evaluasi dan analisis dijabarkan sebagai berikut. Setelah melakukan tugas penelusuran dan pencarian, peserta menjawab serangkaian pertanyaan mengenai kemudahan penggunaan dan kegunaan sistem manajemen pengetahuan. Penulis mengadopsi kuesioner yang dibangun oleh Davis (1989), di mana penulis fokus pada dua dimensi: persepsi kegunaan (*perceived usefullness,* PU) dan persepsi kemudahan penggunaan (*perceived ease of use,* PE). Kegunaan yang dirasakan (PU) terdiri dari lima item, yaitu sebagai berikut.

1. Menggunakan sistem manajemen pengetahuan akan memungkinkan saya menyelesaikan tugas lebih cepat.
2. Menggunakan sistem manajemen pengetahuan akan meningkatkan kinerja tugas saya.
3. Menggunakan sistem manajemen pengetahuan akan meningkatkan efektivitas saya dalam melakukan tugas-tugas saya.
4. Menggunakan sistem manajemen pengetahuan akan membuat lebih mudah untuk melakukan tugas saya.
5. Saya akan menemukan sistem manajemen pengetahuan berguna untuk menyelesaikan tugas saya.

Sedangkan persepsi kemudahan penggunaan (PE) terdiri dari tiga item, yaitu sebagai berikut.

1. Saya akan menemukan mudah untuk mendapati sistem manajemen pengetahuan melakukan apa yang saya inginkan.
2. Saya akan menemukan sistem manajemen pengetahuan fleksibel untuk berinteraksi.
3. Akan mudah bagi saya untuk menjadi terampil dalam menggunakan sistem manajemen pengetahuan.

Item diukur menggunakan skala Likert 7 poin (sangat setuju = 7, setuju = 6, agak setuju = 5, tidak setuju maupun tidak-setuju (netral) = 4, agak tidak setuju = 3, tidak setuju = 2, dan sangat tidak setuju = 1).

### Metode Pengolahan Data

Setelah melakukan pengujian dan evaluasi sistem, data yang diperoleh dari pengujian dan evaluasi sistem manajemen pengetahuan gamelan Bali ini selanjutnya akan diolah melalui beberapa proses. Terdapat 4 (empat) macam pengolahan data, yaitu sebagai berikut.

1. Pengolahan Data Pengujian Tugas Penjelajahan (*Browsing*)

Setelah peserta selesai melakukan tugas penelusuran, penulis menandai masing-masing kiriman. Penulis mengklasifikasikan skim penandaan menjadi tiga kategori, yaitu sebagai berikut.

1. Salah. Skor ini diberikan ketika peserta tidak memberikan jawaban yang benar untuk tugas yang diberikan.
2. Sebagian benar. Skor ini diberikan ketika jawaban cocok dengan kriteria yang diperlukan.
3. Sepenuhnya benar. Skor ini diberikan jika peserta memiliki jawaban yang sepenuhnya benar untuk pertanyaan itu.
4. Pengolahan Data Pengujian Tugas Pencarian (*Searching*)

Mirip dengan tugas penjelajahan, penulis menandai setiap jawaban yang dicoba oleh peserta. Penulis menggunakan skala yang sama (salah, sebagian benar, dan sepenuhnya benar) seperti yang digunakan untuk tugas penjelajahan untuk mengevaluasi jawaban.

1. Pengolahan Data Pengujian Manfaat yang Dipersepsi dan Kemudahan Penggunaan yang Dipersepsi

Setelah semua peserta menyelesaikan tugas penelusuran dan pencarian, peserta diundang untuk menjawab serangkaian pertanyaan kecil terkait dengan manfaat yang dirasakan dan kemudahan penggunaan sistem manajemen pengetahuan. Untuk menganalisis hasil kuesioner, analisis statistik berikut dilakukan dengan menggunakan perangkat lunak SPSS.

1. Analisis Ukuran Kecukupan Sampel Kaiser-Meyer-Olkin (KMO) dilakukan untuk memastikan bahwa ada variabilitas yang memadai dan tinggi dalam data yang dikumpulkan untuk analisis faktor.
2. *Bartlett Test of Sphericity* dilakukan untuk memastikan bahwa item-item instrumen berkorelasi cukup.
3. Uji reliabilitas (*Cronbach's Alpha*) dilakukan untuk menemukan konsistensi internal di antara item.
4. Uji-t Satu-Sampel (*One-Sample t-Test*) dilakukan untuk menentukan apakah sistem dianggap mudah digunakan dan bermanfaat.
5. Analisis komponen utama dengan rotasi *varimax* dilakukan pada data yang dikumpulkan. Metode ini digunakan untuk menentukan jumlah faktor atau komponen utama yang harus dipertahankan.

*Kaiser-Meyer-Olkin Measure of Sampling* (KMO) dan *Bartlett's Test of Sphericity* adalah ukuran kecukupan sampel yang direkomendasikan untuk memeriksa rasio kasus-terhadap-variabel untuk analisis yang dilakukan. Sedangkan keandalan item dinilai dengan *alpha Cronbach*.

Untuk memudahkan interpretasi dan untuk menilai persepsi pengguna terhadap sistem, penulis membuat skor rata-rata peserta pada masing-masing dari dua item komponen di atas (PU dan PE). Juga, karena sifat eksplorasi dari elemen penelitian ini, penulis memperlakukan skor di atas dengan bobot yang sama (Hair et al., 1998).

# BAB II

# TINJAUAN PUSTAKA



## Tinjauan Studi

Terdapat beberapa penelitian serupa baik pendekatan, metode, maupun lingkup penelitian yang mirip seperti penelitian ini. Berikut ini beberapa penelitian tersebut.

1. Penelitian oleh (S. Kolozali, M. Barthet, G. Fazekas, dan M.B. Sandler, 2011) yang berjudul “KNOWLEDGE REPRESENTATION ISSUES IN MUSICAL INSTRUMENT ONTOLOGY DESIGN”. Dalam penelitian ini, penulis mengusulkan sebuah desain dalam desain ontologi instrumen musik berdasarkan klasifikasi skema Hornbostel dan Sach yang mengklasifikasi peran utama dari setiap instrumen. Desain ini menjadi inspirasi untuk melakukan pengembangan ontologi instrumen musik tradisional di Bali. Ontologi instrumen tradisional menggunakan kriteria asal dari instrumen, sumber bunyi, bahan dasar, dan cara bermain sebagai informasi detail dari masing-masing instrumen.
2. Penelitian oleh (S. A. M. Nasir dan N. L. M. Noor, 2010) yang berjudul “INTEGRATING ONTOLOGY-BASED APPROACH IN KNOWLEDGE MANAGEMENT SYSTEM (KMS): CONSTRUCTION OF BATIK HERITAGE ONTOLOGY”. Penelitian ini menetapkan pendekatan untuk mengintegrasikan ontologi dalam Sistem Manajemen Pengetahuan (knowledge management system, KMS) untuk memungkinkan potensi penuh aplikasi e-Museum di web untuk direalisasikan. Penelitian ini berkaitan dengan desain e-Museum berbasis komunitas yang dimaksudkan untuk mendukung pelestarian warisan budaya digital. Untuk menggambarkan pendekatan, penelitian ini mempertimbangkan manajemen pengetahuan dan metodologi ontologi untuk menjelaskan proses konstruksi ontologi (Nasir et al., 2010).
3. Penelitian oleh (H. R. Sanabila dan R. Manurung, 2014) yang berjudul “TOWARDS AUTOMATIC WAYANG ONTOLOGY CONSTRUCTION USING RELATION EXTRACTION FROM FREE TEXT”. Penelitian ini menjadi acuan pelaporan pekerjaan peneliti untuk secara otomatis membangun dan mengisi ontologi mitologi wayang (wayang kulit Indonesia) dari teks bebas menggunakan ekstraksi relasi dan pengelompokan relasi. Referensi ontologi digunakan untuk mengevaluasi ontologi yang dihasilkan. Referensi ontologi berisi konsep dan properti dalam domain karakter wayang. Peneliti memeriksa pengaruh variasi data corpus, variasi nilai ambang batas dalam proses pengelompokan relasi, dan penggunaan pasangan entitas atau tipe pasangan entitas selama tahap ekstraksi fitur (Sanabila et al., 2014).
4. Penelitian oleh (M. Fernández-López, A. Gómez-Pérez dan N. Juristo, 1997) yang berjudul “METHONTOLOGY: FROM ONTOLOGICAL ART TOWARDS ONTOLOGICAL ENGINEERING”. Tujuan dari penelitian ini adalah untuk mengklarifikasi kepada pembaca yang tertarik untuk membangun ontologi dari awal, kegiatan yang harus mereka lakukan dan dalam urutan apa, serta serangkaian teknik yang akan digunakan dalam setiap fase metodologi. Penelitian ini menyajikan satu set kegiatan yang sesuai dengan proses pengembangan ontologi, siklus hidup untuk membangun ontologi berdasarkan prototipe yang berkembang, dan Methontology, metodologi terstruktur dengan baik yang digunakan untuk membangun ontologi dari awal. Penelitian ini mengumpulkan pengalaman penulis tentang membangun ontologi dalam domain bahan kimia (Fernández-López et al., 1997).
5. Penelitian oleh (C. R. A. Pramartha dan Joseph G. Davis, 2016) yang berjudul “DIGITAL PRESERVATION OF CULTURAL HERITAGE: BALINESE KULKUL ARTEFACT AND PRACTICES”. Dalam penelitian ini, penulis memperkenalkan kerangka kerja baru berdasarkan prinsip-prinsip budaya Bali (Tri Hita Karana dan Desa Kala Patra) untuk menangkap, mengklasifikasikan, dan mengatur artefak budaya dan mempraktikkan pengetahuan, dan merancang dan mengembangkan prototipe portal digital online untuk memungkinkan berbagi dan pertumbuhan pengetahuan terkait ke kulkul Bali. Tujuan dari penelitian ini adalah untuk mendokumentasikan, melestarikan, dan mendidik masyarakat Bali dan generasi muda khususnya pada aspek penting dari budaya Bali. Komunitas ini akan didorong tidak hanya untuk belajar tentang kulkul dan praktik terkait, tetapi juga berkontribusi pengetahuan mereka sendiri untuk memungkinkan portal digital online untuk berkembang menjadi tempat penyimpanan pengetahuan budaya Bali. Pengetahuan dan pemahaman kulkul dasar diperoleh melalui wawancara mendalam dengan beberapa pakar budaya Bali terpilih dan anggota masyarakat berpengetahuan (profesor dari universitas di Bali, pemimpin spiritual, pemimpin komunitas senior, dan pengrajin). Sebagai bagian dari portal digital, penelitian penulis juga mencakup pengembangan ontologi dasar konsep dan istilah terkait kulkul, dan hubungan antar mereka untuk mendukung pencarian semantik dan penelusuran sumber daya online (Pramartha et al., 2016).
6. Penelitian oleh (C. R. A. Pramartha, 2018) yang berjudul “ASSEMBLY THE SEMANTIC CULTURAL HERITAGE KNOWLEDGE”. Penelitian ini bertujuan untuk mengumpulkan pengetahuan warisan budaya semantik yang berhubungan dengan satu aspek dari warisan Bali, sistem kulkul. Penulis membahas metode dan prosedur penulis untuk mewujudkan tujuan proyek. Kontribusi yang signifikan dari ahli warisan budaya menghasilkan spesifikasi dan fitur kulkul. Juga, keterlibatan komunitas berpengetahuan membantu penulis untuk memperluas dan mengesahkan ontologi kulkul. Akhirnya, pengetahuan warisan budaya dibuat tersedia dalam bentuk ontologi untuk mewakili pengetahuan yang dapat diproses dan dimanipulasi oleh program komputer (Pramartha, 2018).
7. Penelitian oleh (C. R. A. Pramartha, J. G. Davis, dan K. K. Y. Kuan, 2018) yang berjudul “A SEMANTICALLY-ENRICHED DIGITAL PORTAL FOR THE DIGITAL PRESERVATION OF CULTURAL HERITAGE WITH COMMUNITY PARTICIPATION”. Dalam penelitian ini, penulis menyajikan rincian penelitian yang berhubungan dengan satu aspek budaya Bali, sistem komunikasi tradisional Bali (kulkul), yang dilakukan di pulau Bali, Indonesia. Penelitian ini bertujuan untuk mendokumentasikan, mengorganisasi, dan melestarikan pengetahuan kulkul yang relevan untuk manfaat masyarakat Bali, dan generasi muda khususnya dengan merancang dan mengembangkan portal digital sebagai repositori dinamis. mengumpulkan pengetahuan warisan budaya semantik yang berhubungan dengan satu aspek dari warisan Bali, sistem kulkul. Portal digital prototipe diimplementasikan oleh penulis di cloud untuk memfasilitasi pertumbuhan elastis dan akses pengguna yang mudah ke sumber daya untuk membaca dan menambahkan konten. Hasil evaluasi penelitian menunjukkan bahwa sebagian besar pengguna menganggap portal digital relatif berguna dan mudah digunakan. (Pramartha, 2018).

## Website

Secara etimologi, website adalah kumpulan dari halaman-halaman situs yang terangkum dalam sebuah domain atau sub domain yang tempatnya berada dalam *World Wide Web (WWW)* di dalam internet. Sebuah halaman web biasanya berupa dokumen yang ditulis dalam format HTML *(Hyper Texs Markup Language)* yang selalu bisa diakses melalui HTTP, yaitu sebuah protokol yang menyampaikan informasi dari server website untuk ditampilkan kepada para pemakai melalui web broser. Semua publikasi dari website tersebut dapat membentuk sebuah jaringan informasi yang sangat besar. Adapun pengertian website atau WWW menurut para ahli adalah:

*World Wide Web* merupakan jaringan dokumentasi yang sangat besar yang saling berhubungan satu dengan yang lain. Satu set protocol yang mendefinisikan bagaimana system bekerja dan mentransfer data, dan sebuah software yang membuatnya bekerja dengan mulus. Web menggunakan teknik hypertext dan multimedia yang membuat internet mudah digunakan dijelajahi dan dikontribusikan. Web merupakan sistem *hypermedia* yang berarea luas yang ditujukan untuk akses secara universal. Salah satu kuncinya adalah kemudahan tempat seseorang atau perusahaan dapat menjadi bagian dari web berkontribusi pada web (Hanson, 2000). Sedangkan menurut (Hardjono, 2006) “web merupakan fasilitas *hyperteks* untukmenampilkan data berupa teks, gambar, suara, animasi, dan data multimedia lainnya.” Halaman-halaman dari website dapat diakses melalui URL *(uniform Resoursce Locator)* yang biasanya disebut dengan *HOMEPAGE*. *URL* ini mengatur halaman situs untuk manjadi sebuah hirarki mekipus hyperlink yang ada di dalam halaman tersebut mengatur para pembaca dan memberi tahu mereka susunn keseluruhan dan bagaimana arus informasi ini berjalan. Beberapa website membutuhkan subskripsi (data masukan) agar para user bisa mengakses sebagian atau keseluruhan isi website tersebut. Contohnya, ada beberapa situs-situs bisnis, situs email gratis, yang membutuhkan sub skripsi agar dapat mengakses situs tersebut. Penemu website adalah Sir Timthy John Barnes Lee, sedangkan website yang tersambung dalam jaringan pertama kali muncul pada tahun 1991. Awalnya Sir Timthy membuat website adalah untuk mempermudah tukar menukar dan mempengaruhi informasi kepada sesama peneliti di tempat Sir Timthy bekerja. Pada tanggal 30 April 1993, CERN (Tempat dimana Sir Timthy bekerja) menginformasikan bahwa WWW dapat digunakan secara gratis oleh semua orang. Sebuah website bisa berupa hasil bekerja dari perorangan atau individu, atau menunjukan kepemilikan dari sebuah organisasi, perusahaan, dan biasanya website menunjukan beberapa topik khusus, atau kepentingan tertentu.

*Website* ditulis atau secara dinamik dikonversi menjadi *HTML* dan diakses melalui sebuah program software yang biasa disebut dengan web broser, yang dikenal juga dengan *HTTP* client. Halaman *website* dapat dilihat atau diakses melalui jaringan komputer dan internet, perangkat dapat berupa komputer pribadi, laptop, PDA ataupun telepon seluler. Sebuah website dibuat di dalam sebuah sistem komputer yang dikenal dengan web server, atau yang disebut yang disebut juga *HTTP* *server*, artinya software yang dipakai akan menjalankan sutau sistem, yang kemudian menerima intruksi dari penggunjung website, lalu mengirim halaman-halaman yang dipelukan untuk memenuhi permintaan pengunjung. Apache dan *Microsoft Internet Server (IIS).* adalah perangkat lunak yang biasa digunakan untuk web server.

Beberapa tahun lalu, masih sangat mudah untuk mengelompokan jenis-jenis Website berdasarkan fungsi dan tujuannya, namun dengan berkembanganya teknologi baik internet, browser, script dan program untuk membangun website serta teknologi alat untuk mengakses internet, maka jenis websitepun semakin beragam dan semakin kompleks.

Untuk membuat *website* diperlukan beberapa komponen yang harus ada (terinstal) di dalam komputer, yaitu :

* 1. *Web browser* merupakan komponen yang wajib yang harus ada di komputer. Untuk menjalankan aplikasi web harus menggunakan web browser, beberapa contoh web browser yaitu : *Internet Exsploler, Mozila Firefox, Opera, Chrome, Safari*, dan lain-lain.
  2. *Web Server* merupakan perangkat lunak wajib jika membuat halaman web dinamis. Dalam web server semua *script web* diletakkan, biasanya diletakkan di *“document root”* dalam web server tersebut. Dengan menggunakan *web server* maka pembuat web dapat melakukan ujicoba terhadap halaman-halaman web yang dibuat, tanpa adanya koneksi langsung ke internet (localhost). Contoh *web server* adalah *IIS, Apache, Xitami.*
  3. *Script* digunakan untuk membuat web statis menggunakan *client side scripting* *(HTML, CSS, Java Script).* Untuk membuat web dinamis menggunakan server side scripting *(ASP, PHP, JSP).*
  4. Database server merupakan tempat penyimpanan data dalam sebuah web. Contohnya *MySQL, Microsoft SQL Server, Oracle, DB2 (IBM), PostgreSQL*.
  5. *Web editor* merupakan perangkat lunak yang digunakan untuk mengetikan perintah-perintah script yang diguankan baik itu client side scrpting maupun *server side scripting*. Beberapa *web editor* dapat digunakan untuk mengatur layout (tampilan) web secara instan. Berikut contoh *web editor* : *Sublime Text, Notepad, Macromedia Dreamweaver, Ultra Edit, Adobe Go Live, Netbean.*
  6. *Image Editor* merupakan perangkat lunak yang digunakan untuk mengelola gambar-gambar dan animasi yang akan digunakan di dalam halaman web. Berikut contoh *Image Editor*: *Adobe Photoshop, Corell Draw, Macromedia Flash*.

## Semantic Web

*Semantic web* merupakan perluasan dari web saat ini, dimana informasi memiliki arti yang terdefinisi secara lebih baik dengan mengupayakan persamaan persepsi antara konsep-konsep yang ada, sehingga memungkinkan manusia dan komputer untuk bekerjasama secara lebih optimal (Berners-Lee., 2001).

*W3C (World Wide Web Consortium*) memberikan suatu visi dari semantic web yaitu gagasan untuk memiliki data di web yang didefinisikan serta dihubungkan sedemikian rupa sehingga bisa digunakan oleh mesin, bukan hanya untuk ditampilkan tetapi juga untuk tujuan automasi, integrasi dan penggunaan kembali data antar berbagai aplikasi (*W3C*, 2001).

*Semantic web* mengindikasikan bahwa makna data pada web dapat dipahami, baik oleh manusia maupun oleh komputer (Passin, 2004). Agar dapat diproses oleh mesin, dokumen web dinotasikan dengan metadata.

Menurut *World Wide Web Consortium (W3C)*, arsitektur dari *semantic web* terdiri dari beberapa *layer* yang ditunjukkan oleh Gambar 2.1.



**Gambar 2.1** Arsitektur *semantic web*

Berikut ini deskripsi dari masing-masing *layer*.

1. *Layer Unicode* dan *URI. Uniform Resource Identifiers (URI)* memastikan penggunaan sekumpulan karakter yang telah disepakati secara internasional dan menyediakan alat untuk mengidentifikasi objek di semantik web. Jenis *URL* yang terkenal adalah *URL (Uniform Resource Locator)* yang akan memberitahu komputer dimana letak suatu *resource*.
2. *Layer XML, Namespace, XML Schema.* Layer ini mengintegrasikan definisi *Semantic web* dengan dokumen *XML (Extensible Markup Language)* lain yang sesuai standar. *XML* merupakan format standar untuk dokumen terstruktur dan sebagai cara paling fleksibel untuk menciptakan standar bagi format informasi dan kemudian menyediakan format tersebut beserta datanya di web. *XML Schema* menggambarkan struktur dan batasan dari isi dokumen *XML, namespace* merupakan standar yang digunakan untuk menentukan label unik kepada sekumpulan nama elemen yang didefinisikan oleh *XML Schema*.
3. *RDF* dan *RDF Schema. RDF (Resource Description Framework)* dan *RDF Schema* memungkinkan pengguna untuk membuat pernyataan tentang objek dan *URI* serta mendefinisikan kosakata yang bisa diacu dengan *URI* tersebut. Layer inilah yang menentukan tipe dari *resource* dan *link*. *RDF Schema* mendeklarasikan keberadaan kelas dan properti, termasuk subkelas, sub properti, domain dan range.
4. *Ontology vocabulary. Ontology* mendukung perkembangan kosakata karena *pada Layer RDF* dapat ditentukan relasi antar konsep yang berbeda.
5. *Logic. Layer logic* menyediakan *framework* untuk menulis aksioma dari aturan dasar sistem. Layer ini digunakan untuk meningkatkan bahasa ontologi dan memungkinkan penulisan aplikasi pengetahuan deklaratif khusus.
6. *Proof. Layer proof* mengeksekusi aturan dari *Layer logic*. *Layer proof* melibatkan proses deduktif serta representasi proof dalam bahasa web dan validasi proof.
7. *Trust. Layer trust* mengevaluasi apakah hasil dari Layer proof bisa dipercaya. Layer ini akan muncul melalui penggunaan *digital signature* berdasarkan rekomendasi yang diberikan oleh agen yang terpercaya.
8. *Digital Signature. Digital signature* mendefinisikan blok dari data yang terenkripsi yang akan dimanfaatkan oleh komputer dan agen untuk memastikan apakah suatu informasi yang disediakan oleh sumber yang terpercaya serta mendeteksi adanya perubahan pada dokumen.

## Ontologi dan Peranannya dalam Pelestarian Budaya

*Semantic web* memanfaatan ontologi untuk merepresentasikan basis pengetahuan dan sumber daya *web*. Ontologi menghubungkan simbol-simbol yang dipahami manusia dengan bentuknya yang dapat diproses oleh mesin, dengan demikian ontologi menjadi jembatan antara manusia dan mesin (Davies dkk., 2006).

Ontologi bermanfaat untuk meningkatkan akurasi dalam proses pencarian informasi di web. Mesin pencari dapat mencari halaman yang merujuk pada konsep yang tepat dalam sebuah ontologi. Mesin pencari dapat menemukan dokumen yang relevan, juga dapat menyarankan pengguna untuk memberikan *query* yang lebih umum (Nurkhamid, 2009). Jika terlalu banyak dokumen yang ditemukan, mesin pencari dapat menyarankan *quer*y yang lebih spesifik (Antoniou & van Harmelen, 2008).

Antoniou dan Van Harmelen (2008), mengemukakan bahwa sebuah ontologi didefinisikan sebagai sebuah spesifikasi formal dan eksplisit dari sebuah konseptual. Makna konseptual merujuk pada model abstrak dari sesuatu hal. Eksplisit mengindikasikan bahwa elemen-elemen konseptual harus didefinisikan dengan jelas, dan formal berarti bahwa spesifikasi tersebut harus dapat diproses oleh mesin. Dalam pandangan Gruber ontologi merupakan representasi pengetahuan dari sebuah domain, dengan sekumpulan objek dan relasi dideskripsikan oleh sebuah *vocabulary*.

*W3C* menyebutkan bahwa ontologi adalah sebuah istilah yang diambil dari ilmu filsafat yang merujuk pada bidang ilmu yang mendeskripsikan berbagai entitas dalam dunia dan bagaimana entitas-entitas tersebut saling berelasi (McGuinness & van Harmelen, 2004). Ontologi menyediakan deskripsi untuk elemen kelas-kelas (*classes*) dalam berbagai domain, relasi (*relations*) antar kelas-kelas, dan properti (*property*) yang dimiliki oleh kelas-kelas tersebut.

Ontologi digunakan untuk bidang kecerdasan buatan, representasi pengetahuan, pemrosesan bahasa alami, web semantik, rekayasa perangkat lunak, dan banyak bidang lainya. Dalam sistem informasi, ontologi adalah spesifikasi yang jelas tentang serangkaian konsep yang menjelaskan sebuah wilayah pengetahuan tertentu yang dipakai bersama oleh para pengguna sistem yang bersangkutan.

Beberapa manfaat menggunakan ontologi (Antoniou dan Van Harmelen, 2008), yaitu: 1) Ontologi dapat membagi pemahaman atau definisi tentang konsep-konsep dalam sebuah *domain* (*sharing* informasi); 2) Ontologi menyediakan cara untuk menggunakan kembali domain pengetahuan (*knowledge domain reusable*); 3) Ontologi  membuat asumsi eksplisit sebuah *domain*; 4) Ontologi bersama dengan bahasa deskripsi (seperti *RDF Schema*), menyediakan cara untuk mengkodekan pengetahuan dan semantik seperti *machine-understand*; 5) Ontologi memungkinkan pemrosesan mesin otomatis dalam skala besar.

Ontologi digunakan secara luas di bidang warisan budaya, terutama dalam melestarikan aspek material dan fisik dari peninggalan masa lalu. Ontologi dipilih sebagai solusi untuk menyelesaikan interoperabilitas struktur data dan terlibat dalam implementasi nyata (Cameron et al., 2007). Beberapa penelitian yang fokus dalam penggunaan ontologi dalam usaha melestarikan warisan budaya adalah pada penelitian oleh Noor et al. (2010), Sanabila et al. (2014), dan Pramartha et al. (2016, 2018).

## OWL (Ontology Web Language)

*OWL (Ontology Web Language)* merupakan suatu bahasa ontologi yang digunakan untuk mendeskripsikan kelas-kelas, properti-properti dan relasi antar objek-objek dalam suatu cara yang dapat diinterpretasi oleh mesin (Breitman dkk., 2007).

*OWL* merupakan sebuah *vocabulary,* namun dengan tingkatan semantik yang lebih tinggi dibandingkan dengan *RDF* dan *RDF Schema*. *OWL* menyediakan tiga sub bahasa yang berbeda tingkatan bahasanya yang dirancang untuk berbagai kebutuhan tertentu dari pengguna, antara lain (Breitman dkk., 2007):

1. *OWL Lite: OWL Lite* menyediakan pendefinisian hirarki kelas dan properti dengan batasan-batasan (*constraints*) yang sederhana. Jenis ini digunakan jika pengguna hanya membutuhkan hirarkis kelas yang sederhana dengan batasan yang sederhana pula.
2. *OWL DL (Description Logic): OWL DL* mendukung pengguna yang menginginkan ekspresi maksimum tanpa kehilangan perhitungan yang lengkap dan ketepatan, *OWL DL* meliputi semua bahasa konstruksi dalam *OWL* dengan batasan tertentu. *OWL DL* dapat menghasilkan hirarkis klasifikasi secara otomatis dan mampu mengecek konsisten dalam suatu ontologi karena *OWL DL* mendukung reasoning.
3. *OWL Full; OWL Full* berguna untuk pengguna yang menginginkan ekspresi maksimum dan kebebasan sintaksis dari *RDF* tanpa ada jaminan perhitungan. *OWL Full* memperbolehkan ontologi untuk meningkatkan arti dari kosakata yang belum digambarkan (*RDF* atau *OWL*). *OWL Full* diperuntukkan bagi pengguna yang menginginkan subbahasa yang sangat ekspresif dan secara sintaks lepas dari RDF tanpa jaminan komputasional.

## RDF (*Resource Description Framework*)

*Resource Description Framework (RDF)* merupakan sebuah model data yang sederhana dan fleksibel untuk mendeskripsikan hubungan antara sumberdaya-sumberdaya web dalam bentuk *RDF statement* (Breitman dkk., 2007). *RDF* mendukung interoperabilitas antar aplikasi yang melakukan pertukaran informasi dan bersifat *machine-understandable* di web. *RDF* menggunakan graf untuk merepresentasikan kumpulan pernyataan. Simpul dalam graf mewakili suatu entitas, dan tanda panah mewakili relasi antar entitas. RDF didasarkan pada gagasan dimana hal-hal yang sedang diuraikan memiliki properti yang didalamnya mempunyai nilai-nilai dan *resource* yang dapat diuraikan dengan pembuatan *statement* (Manola dan Miller, 2004).

*RDF* menggunakan istilah tertentu untuk menguraikan suatu *statement*. Bagian yang mengidentifikasi dalam *statement* dapat disebut subject, karakteristik (*property*) dari *subject* disebut sebagai predicate, sedangkan nilai dari *property* disebut sebagai *object*.

Lassila dan Swick (1999) menyatakan model data *RDF* terdiri atas tiga objek tipe: 1) *Resource*, segala sesuatu yang digambarkan dengan *RDF* disebut resource. *Resource* bisa berupa keseluruhan atau bagian dari sebuah halaman web. *Resource* ini biasanya diberi nama menggunakan *URI (Uniform Resource Identifier)*. *URI* bersifat bisa diperluas maka *URI* bisa digunakan sebagai pengenal bagi berbagai macam entitas; 2) Properti (*property*), merupakan aspek atau karakteristik, atribut, serta relasi khusus yang digunakan untuk menggambarkan sebuah *resource*.  Setiap properti memiliki arti khusus, mendefinisikan nilai yang mungkin, tipe *resource* yang digambarkan dan relasinya dengan properti lain. Pernyataan (*statement*), suatu *resource* bersama dengan properti dan nilai dari suatu properti untuk *resource* membentuk suatu pernyataan *RDF*. Ketiga bagian ini disebut subjek, predikat dan objek, yang membentuk *RDF triple*. Objek dapat berupa *resource* lain, atau berupa literal (*string* sederhana atau tipe data primitif lain yang didefinisikan oleh *XML*).

## SPARQL

SPARQL adalah bahasa *query* untuk RDF. Graph RDF merupakan terdiri dari triple yang terbentuk dari subjek, predikat dan objek. RDF dapat didefinisikan pada konsep RDF dan konsep abstrak sintaks. Triple ini dapat datang dari berbagai macam sumber. Instance dapat diperoleh secara langsung dari dokumen RDF dan dapat disimpulkan dari triple RDF. Ekspresi RDF dapat disimpan dalam format lain seperti XML dan *Database Relational*.

## Apache Jena Fuseki

Apache Jena Fuseki bertindak sebagai server untuk mengeksekusi SPARQL dalam mengolah data RDF. Pada dasarnya SPARQL sama seperti SQL, yakni bahasa *query* data. Perbedaannya adalah SQL merupakan *command* untuk PHP, sedangkan SPARQL untuk RDF. Fuseki juga memungkinkan web mengakses file ontologi untuk proses *upload*, *update*, dan *query* di dalam browser, juga melihat hasil untuk proses yang terjadi tanpa mengubah file asal. Berbeda dengan Protégé, Fuseki merupakan *tools* untuk membina ontologi serta tidak menjalankan *query* di browser, melainkan di *local*. Oleh karena itu, Fuseki perlu diinstal untuk menjalankan proses secara protokol HTTP.

## Protégé

Perangkat lunak Protégé dikembangkan oleh Stanford Center for Biomedical Informatics Research di Stanford University School of Medicine. Perangkat lunak Protégé bersifat *open source* dibawah lisensi bernama Mozilla Public License (MPL). Perangkat lunak Protégé merupakan alat bantu untuk membantu pengembang ontologi untuk memngembangkan sistem yang didasarkan pada sistem basis pengetahuan (*knowledge base system*). Protégé dapat membuat, mengedit dan menyimpan ontologi dalam format CLIPS, RDF, XML, UML dan Relational Database. Secara umum, Protégé memudahkan pengguna untuk membuat pemodelan dasar secara lebih sederhana yang dilengkapi dengan visualisasi hubungan *subclass* dalam *tree*.

## Technology Acceptance Model (TAM)

Model penerimaan teknologi (*Technology Acceptance Model,* TAM) adalah teori sistem informasi yang memodelkan bagaimana pengguna menerima dan menggunakan teknologi. TAM bertujuan untuk menjelaskan dan memprediksi penerimaan pengguna terhadap sistem informasi. Model penerimaan teknologi Davis (1989) telah diuji secara luas dan diterima secara luas di antara para peneliti di bidang TI sebagai model berbasis teori dengan validitas prediktif yang baik. TAM menjelaskan hubungan sebab akibat antara keyakinan (kegunaan sistem informasi dan kemudahan penggunaan sistem informasi) dan sikap, niat, dan penggunaan aktual dari pengguna. TAM secara luas dianggap sebagai model teoritis yang relatif kuat untuk menjelaskan penggunaan TI. Dari perspektif praktisi, TAM berguna untuk memprediksi apakah pengguna akan mengadopsi teknologi informasi baru. TAM berupaya menguji dan memprediksi mengapa orang menerima atau menolak teknologi informasi (Davis, 1989). Gambar 2.2 menunjukkan diagram alur dari TAM.



**Gambar 6.2** Diagram alur dari TAM, diadopsi dari Davis (1989)

Berikut ini penjelasan dari diagram alur TAM di atas.

## Warisan Budaya Digital

Warisan budaya digital adalah penggunaan media digital dalam layanan melestarikan warisan budaya atau alam. Piagam tentang Pelestarian Warisan Digital UNESCO mendefinisikan warisan budaya digital sebagai “merangkul sumber daya budaya, pendidikan, ilmiah, dan administratif, serta informasi teknis, hukum, medis, dan jenis lain yang dibuat secara digital, atau diubah menjadi bentuk digital dari sumber daya analog yang ada” (Cameron, 2007).

## Gamelan Tradisional Bali

Gamelan Bali memiliki alat musik tabuh, gesek, tiup, petik dan sebagainya. Gamelan dapat digolongkan berdasarkan zaman munculnya Gamelan. Gamelan Bali dibagi menjadi tiga garis besar, yaitu Gamelan Wayah, Gamelan Madya, dan Gamelan Anyar (Sunarto, 2014).

1. Gamelan Wayah

Jenis gamelan yang dapat digolongkan menjadi Gamelan Wayah adalah Gamelan yang ada sebelum abad XV yang pada umumnya didominasi oleh alat berbentuk bilahan dan belum terlalu banyak menggunakan kendang. Gamelan yang meliputi gamelan Wayah yaitu, Gamelan Angklung, Gamelan Baleganjur, Gamelan Caruk, Gamelan Gambang, Gamelan Gender Wayang, Gamelan Gong Bheri, Gamelan Gong Luwang, dan Gamelan Selonding.

1. Gamelan Madya

Jenis Gamelan yang dapat digolongkan menjadi Gamelan Madya adalah Gamelan yang berasal dari abad XVI-XIX dimana barungan Gamelan mulai memakai kendang dan instrumen berpencon (bermoncol). Gamelan yang termasuk golongan Gamelan madya yaitu, Gamelan Joged Pingitan, Gamelan Penggambuhan, Gamelan Gong Gede, Gamelan Pelegongan, dan Gamelan Semar Pegulingan.

1. Gamelan Anyar

Jenis Gamelan yang dapat digolongkan menjadi Gamelan Anyar adalah Gamelan yang muncul pada abad XX dimana Gamelan pada zaman ini mulai menonjolkan permainan kendang. Gamelan yang termasuk golongan Gamelan anyar adalah Gamelan Geguntangan, Gamelan Gong Kebyar, Gamelan Janger, Gamelan Joged Bumbung, dan Gamelan Semarandana.

Gamelan juga dapat digolongkan berdasarkan kegunaannya dalam Upacara Yadnya, khususnya atas jenis dan prosesi Yadnya yang dilakukan. Sesuai dengan konsep Panca Yadnya, maka penggunaan gamelan dalam Upacara Yadnya dapat dipaparkan seperti berikut ini (Arsana dkk., 2014).

1. Dewa Yadnya

Dewa Yadnya adalah persembahan yang tulus ikhlas yang ditujukan kepada Ida Sang Hyang Widhi Wasa dan para Dewa sebagai wujud syukur atas rahmat dan karunia yang telah diberikan-Nya kepada umat manusia. Dalam upacara Dewa Yadnya biasanya digunakan gamelan Gong Gede, Gong Kebyar, Angklung, dan Baleganjur.

1. Rsi Yadnya

Rsi Yadnya adalah sebuah upacara yang ditujukan kepada para Rsi atau orang suci, seperti melakukan upacara penobatan sulinggih (*mediksa*), mengamalkan ajaran beliau, serta mengaturkan punia kepada beliau. Dalam upacara Rsi Yadnya biasanya digunakan gamelan Gong Gede dan Gender Wayang.

1. Manusa Yadnya

Manusa Yadnya merupakan upacara korban suci yang ditujukan untuk membersihkan diri manusia secara lahir dan batin. Dalam upacara Manusa Yadnya biasanya digunakan gamelan Semar Pegulingan dan Gender Wayang.

1. Pitra Yadnya

Pitra Yadnya adalah persembahan kepada leluhur sebagai pernyataan rasa terima kasih atas jasa-jasanya untuk keselamatan bersama. Dalam upacara Pitra Yadnya biasanya digunakan gamelan Gambang, Baleganjur, Gender Wayang, dan Angklung.

1. Bhuta Yadnya

Bhuta Yadnya adalah korban suci kepada Bhuta dan Kala (kekuatan negatif) yang bertujuan untuk membersihkan alam beserta isinya. Dalam upacara Bhuta Yadnya biasanya digunakan gamelan Baleganjur.

## Kerangka Kerja Tri Hita Karana (THK) dan Desa Kala Patra (DKP)

Kerangka Kerja Tri Hita Karana (THK) dan Desa Kala Patra (DKP) adalah kerangka kerja yang diusulkan oleh Pramartha (2016) yang mengambil filosofi budaya Bali yaitu Tri Hita Karana dan Desa Kala Patra. Tri Hita Karana memiliki arti tiga penyebab kebahagiaan dengan menekankan kepada keseimbangan hubungan manusia di dalam dunia ini, yaitu sebagai berikut.

* 1. Parahyangan yaitu hubungan manusia dengan Tuhan (*Universal/God*).
  2. Palemahan yaitu hubungan manusia dengan alam sekitarnya (*environment*).
  3. Pawongan yaitu hubungan dengan sesama manusia (*social*).

Sedangkan konsep desa kala patra (*time, space, circumstances*) merupakan konsep dimana orang Bali menerima perbedaan yang terjadi di masyarakat yang disebabkan oleh pebedaan tempat (desa), waktu (kala), dan keadaan (patra). Juga, konsep ini memberikan pemahaman bahwa budaya Bali merupakan budaya yang sangat dinamis, terus berkembang dan beradaptasi seiring dengan perubahan jaman maupun masuknya budaya lain tanpa menghilangkan identitas inti dari budaya Bali itu sendiri. Gambar 2.3 menunjukkan diagram dari kerangka kerja THK dan DKP.



**Gambar 2.3** Diagram kerangka kerja Tri Hita Karana (THK) dan Desa Kala Patra (DKP)

## Metode Methontology

Metode Methontology merupakan salah satu metodologi pembangunan model ontologi yang memiliki keunggulan terkait dengan deskripsi setiap aktivitas yang harus dilakukan secara mendetail. Selain itu, metode Methontology juga memiliki kemampuan yaitu ontologi yang dibangun dapat digunakan kembali untuk pengembangan sistem lebih lanjut (Fernández-López et al., 1997). Gambar 2.4 menunjukkan alur dari metode Methontology.

****

**Gambar 2.4** Diagram alur dari metode Methontology, diadopsi dari Fernández-López et al. (1997)

Berikut ini deskripsi dari masing-masing tahapan pada metode Methontology.

1. Tahap Spesifikasi

Tujuan dari fase spesifikasi adalah untuk menghasilkan dokumen spesifikasi ontologi informal, semi formal atau formal yang ditulis dalam bahasa alami, masing-masing menggunakan seperangkat representasi menengah atau menggunakan pertanyaan kompetensi.

1. Tahap Akuisisi Pengetahuan

Akuisisi pengetahuan adalah kegiatan independen dalam proses pengembangan ontologi. Sebagian besar akuisisi dilakukan bersamaan dengan fase spesifikasi persyaratan, dan berkurang seiring proses pengembangan ontologi berkembang maju.

1. Tahap Konseptualisasi

Pada bagian ini akan disusun pengetahuan domain dalam model konseptual yang menggambarkan masalah dan solusinya dalam hal kosa kata domain yang diidentifikasi dalam aktivitas spesifikasi ontologi. Hal yang dilakukan adalah membangun daftar istilah lengkap. Istilah mencakup konsep, *instance*, kata kerja, dan properti. Jadi, daftar istilah mengidentifikasi dan mengumpulkan semua pengetahuan domain yang berguna dan berpotensi dapat digunakan beserta artinya.

Dalam menyusun pengetahuan domain dalam model konseptual yang menggambarkan masalah dan solusinya dalam hal kosakata domain yang diidentifikasi dalam aktivitas spesifikasi ontologi, dibangun daftar istilah lengkap yang mencakup konsep, *instance*, kata kerja, dan properti. Daftar istilah mengidentifikasi dan mengumpulkan semua pengetahuan domain yang berguna dan berpotensi dapat digunakan serta artinya.

1. Tahap Integrasi

Dalam tahap ini, mempertimbangkan penggunaan kembali definisi yang sudah dibangun ke dalam ontologi. Dalam mempertimbangkan penggunaan kembali definisi yang sudah dibangun ke dalam ontologi, penulis memeriksa meta-ontologi untuk memilih yang lebih sesuai dengan konsep. Tujuannya adalah untuk menjamin bahwa set definisi baru dan yang digunakan kembali didasarkan pada set istilah dasar yang sama. Kemudian, penulis mencari tahu perpustakaan ontologi mana yang memberikan definisi istilah-istilah yang semantik dan implementasinya koheren dengan istilah-istilah yang diidentifikasi dalam konseptualisasi.

1. Tahap Implementasi

Tahap ini merupakan proses implementasi dari perancangan ontologi. Setiap bagian ontologi didefinisikan sesuai dengan hasil dari tiap tahapan tugas pada Methontology, dimana *concept* didefinisikan sebagai *class*, *ad-hoc* *binary relation* didefinisikan sebagai *object properties*, *class attribute* dan *instance attribute* didefinisikan sebagai *datatype properties*, dan *instances* didefinisikan sebagai individual. Perancangan konseptual ontologi yang telah dilakukan menggunakan metode Methontology kemudian diformalisasikan menggunakan perangkat lunak Protégé.

1. Tahap Evaluasi

Evaluasi berarti melaksanakan penilaian teknis ontologi, lingkungan perangkat lunak, dan dokumentasinya sehubungan dengan kerangka acuan (dalam kasus kami dokumen spesifikasi kebutuhan) selama setiap fase dan antara fase dari siklus hidup mereka. Evaluasi merangkum istilah verifikasi dan validasi. Verifikasi mengacu pada proses teknis yang menjamin kebenaran ontologi, lingkungan perangkat lunak terkait, dan dokumentasi sehubungan dengan kerangka acuan selama setiap fase dan antara fase dari siklus hidup mereka.

1. Tahap Dokumentasi

Tidak ada pedoman yang disepakati tentang cara mendokumentasikan ontologi. Dalam banyak kasus, satu-satunya dokumentasi yang tersedia adalah dalam kode ontologi, teks bahasa alami yang dilampirkan pada definisi formal, dan makalah yang diterbitkan dalam proses konferensi dan jurnal yang mengatur pertanyaan-pertanyaan penting dari ontologi yang sudah dibangun.

* 1. Metode Prototyping

Metode *Prototyping* merupakan salah satu metode pengembangan perangkat lunak yang banyak digunakan. Dengan metode *Prototyping* ini, pengembang dan pengguna dapat saling berinteraksi selama proses pembuatan sistem. Gambar 2.5 menunjukkan diagram alur pengembangan sistem yang menggunakan metode *Prototyping*.



**Gambar 7.2** Diagram alur pengembangan sistem dengan metode *Prototyping*

## Pengujian Ukuran Kecukupan Sampel Kaiser-Meyer-Olkin (KMO)

Pengujian Ukuran Kecukupan Sampel Kaiser-Meyer-Olkin (KMO) merupakan pengujian yang digunakan untuk memastikan bahwa ada variabilitas yang memadai dan tinggi dalam data yang dikumpulkan untuk analisis faktor.

## Pengujian *Bartlett Test of Sphericity*

Pengujian *Bartlett Test of Sphericity* merupakan pengujian yang digunakan untuk memastikan bahwa item-item instrumen berkorelasi cukup.

## Pengujian Reliabilitas (*Cronbach's Alpha*)

Pengujian reliabilitas (*Cronbach's Alpha*) merupakan pengujian yang digunakan untuk menemukan konsistensi internal di antara item.

## Pengujian Uji-t Satu-Sampel (*One-Sample t-Test*)

Pengujian Uji-t Satu-Sampel (*One-Sample t-Test*) merupakan pengujian yang digunakan untuk menentukan apakah sistem dianggap mudah digunakan dan bermanfaat.

# BAB III

# ANALISIS DAN PERANCANGAN SISTEM

## Analisis Kebutuhan

Kebutuhan sistem harus didefinisikan secara lengkap, agar nantinya dapat dirancang desain dan implementasinya. Pada subbab berikut ini analisis dari kebutuhan sistem akan dibagi menjadi dua bagian, yaitu analisis kebutuhan fungsional dan analisis kebutuhan nonfungsional.

### Kebutuhan Fungsional

Kebutuhan fungsional merupakan kebutuhan yang berisi proses-proses apa saja dan fitur-fitur apa saja yang nantinya harus disediakan oleh sistem, mencakup bagaimana sistem harus bereaksi pada input tertentu agar sesuai dengan kebutuhan user. Berikut merupakan kebutuhan fungsional yang didekripsikan pada Tabel 3.1.

Tabel 3. 1 Kebutuhan Fungsional

|  |  |  |
| --- | --- | --- |
| **No.** | **Dekripsi Kebutuhan** | **Target**  **Aktor** |
|  | Sistem menyediakan beberapa fitur menu untuk memenuhi kebutuhan *user* di dalam aplikasi. Berikut merupakan rinciannya:   * 1. *User* dapat mengakses menu “Home”. Pada halaman ini menampilkan halaman utama aplikasi *website.*   2. *User* dapat mengakses daftar pengetahuan dengan memilih menu “Browsing”, kemudian memilih pengetahuan yang diinginkan.   3. *User* dapat memilih menu “Searching” yang berfungsi untuk menemukan ansambel maupun instrumen gamelan dengan kriteria tertentu. | User |

|  |  |  |
| --- | --- | --- |
| **No.** | **Dekripsi Kebutuhan** | **Target**  **Aktor** |
| KFI | * 1. *User* dapat memilih menu “Telusuri” dimana fitur ini menampilkan musik tradisional daerah yang ada pada sistem sehingga mempermudah *user* untuk menemukan musik-musik daerah yang tersedia.   2. *User* dapat memilih menu “Musik Saya” dimana didalam menu ini akan menampilkan daftar putar yang dimiliki oleh akun *user* tersebut.   3. *User* dapat membuat daftar putar baru sesuai dengan keinginan mereka dengan mengakses tombol “DAFTAR PUTAR BARU”.   4. *User* dapat mengunggah data musik, serta menentukan akses terhadap musik tersebut, dengan mengakses menu Unggah   5. *User* dapat melihat menu “USER DETAIL” dan menu “KELUAR” dengan mengakses menu akun pada navigasi bar.   6. *User* dapat memilih menu “USER DETAIL” dimana pada menu ini *user* dapat mengganti informasi email dan *password* akun.   7. *User* dapat memilih menu “KELUAR” untuk mengeluarkan akses akun tersebut. | User |

### Kebutuhan Non Fungsional

Kebutuhan non fungsional merupakan kebutuhan yang menitikberatkan pada properti perilaku yang dimiliki oleh sistem. Adapun beberapa kebutuhan non fungsional pada sistem ini antara lain sebagai berikut.

1. Sistem dapat dijalankan oleh beberapa *software web browser* diantaranya Google Chrome, Microsoft Edge, Internet Explorer, dan Mozilla Firefox.
2. Sistem memiliki tampilan antarmuka yang mudah dipahami *user.*

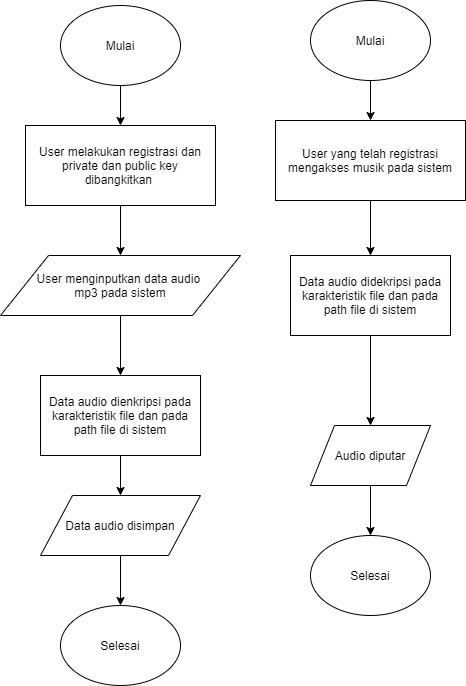
## Rancangan Data

Data yang digunakan pada penelitian ini menggunakan data primer yang diperoleh dengan metode observasi, dengan bekerja sama dengan pihak seniman *sekaa gong* untuk memperoleh data pengetahuan serta informasi detail gamelan tradisional tersebut. Adapun rincian data yang digunakan sebagai berikut.

1. Data berupa pengetahuan gamelan Bali dalam bentuk teks dan gambar.
2. Data yang digunakan merupakan data pengetahuan yang diperoleh langsung dari narasumber seniman *sekaa gong* yang tersebar di beberapa daerah di Provinsi Bali, adapun data-data yang diminta adalah data audio dari musik daerah tersebut, judul musik, nama kelompok seniman, dan jenis musik daerah tersebut. Periode untuk mengumpulkan data-data tersebut adalahh 17 Oktober sampai dengan 6 Desember 2019.

## Rancangan Umum Sistem dengan Penerapan Algoritma RSA

Rancangan proses secara umum yang diimplementasikan pada sistem layanan musik streaming ini menggunakan algoritma RSA ini digambarkan melalui flowchart seperti terlihat pada Gambar 3.1

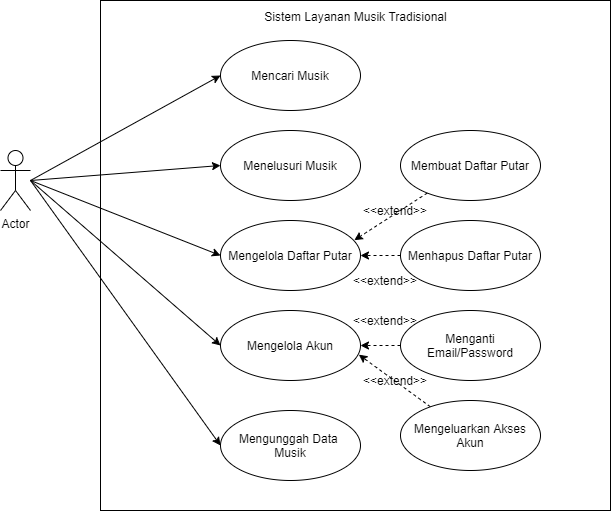


Gambar 3. 1 Flowchart Sistem Secara Umum

Secara umum, pada tahap awal user yang akan mengakses pada sistem harus melakukan proses registrasi dimana setelah itu kunci public dan private akan dibangkitkan pada sistem, kemudian user dapat menggunggah data musik dan setelah proses tersebut data audio akan terenkripsi pada path dan karakteristik file, kemudian data yang telah dienkripsi akan disimpan pada sistem. Kemudian jika user akan mengakses musik tersebut data audio akan didekripsi terlebih dahulu menggunakan kunci private pada path dan karakteristik filenya, kemudian audio yang telah didekripsi akan diputar.

## Rancangan Use-Case

Pada tahap ini dilakukan pembuatan diagram *use case* yang digunakan untuk memodelkan layanan yang disediakan pada aplikasi *website*, dan juga membuat dekripsi *use case* untuk menjelaskan mengenai masing-masing fungsionalitas aplikasi. Gambar 3.1 merupakan *use case model* untuk sistem layanan musik *streaming* berbasis web. *Use case diagram* dapat dilihat pada Gambar 3.2. *Software* yang digunakan untuk membuat gambar adalah aplikasi *website* “Lucid Chart”.



Gambar 3. 2 Rancangan Use Case Sistem Layanan Musik

### Dekripsi Use Case

Pada tahap ini, merupakan tahap pembuatan dekripsi *use case,* yakni terdiri dari UC-01 melakukan pencarian musik, UC-02 melakukan penelusuran musik, UC-03 mengelola daftar putar musik, UC-04 mengelola akun.

1. **UC-01 : Mencari Musik**

UC-01 Merupakan kebutuhan fungsi untuk pengguna melakukan pencarian terhadap musik yang ingin dicari, Use case dimulai ketika user berada pada halaman utama, setelah melalui proses login. Dengan mengakses menu “Cari” user tinggal memasukan kata kunci yang ingin ditemukan.. Tabel dekripsi UC-01: Melakukan Pencarian Musik dapat dilihat pada LAMPIRAN A DEKRIPSI USE CASE.

1. **UC-02 : Menelusuri Musik**

UC-02 merupakan kebutuhan fungsi pengguna untuk melakukan penelusuran musik yang disediakan oleh sistem, Use case dimulai ketika user berada pada halaman utama, setelah melalui proses login. Dengan mengakses menu “Telusuri”. Kemudian sistem akan menampilan musik-musik yang tersedia pada sistem, pengguna tinggal memilih dan memutar musik sesuai dengan yang diinginkan. Tabel dekripsi UC-02: Melakukan Penelusuran Musik dapat dilihat pada LAMPIRAN A DEKRIPSI USE CASE.

1. **UC-03 : Mengelola Daftar Putar**

UC-02 merupakan kebutuhan fungsi pengguna untuk melakukan pengelolaan pada daftar putar musik yang tersedia. Use case dimulai ketika user berada pada halaman utama, setelah melalui proses login. Dengan mengakses menu “Musik Saya”, kemudian sistem akan menampilkan daftar putar yang dimiliki, selain itu user juga memiliki akses untuk membuat daftar putar baru, serta menghapus daftar putar yang ada. Tabel dekripsi UC-03: Mengelola Daftar Putar dapat dilihat pada LAMPIRAN A DEKRIPSI USE CASE.

1. **UC-04 : Mengelola akun**

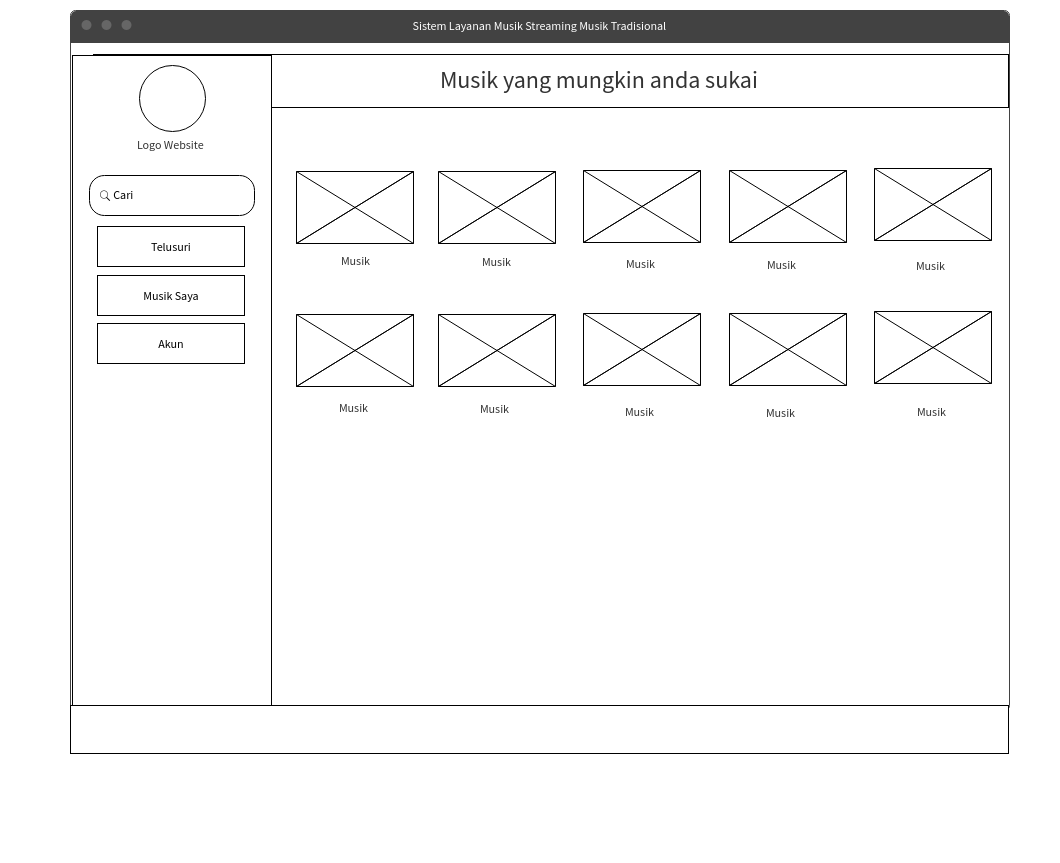
UC-04 merupakan kebutuhan fungsi pengguna untuk melakukan pengelolaan terhadap akun *user.* Use case dimulai ketika user berada pada halaman utama, setelah melalui proses login. Dengan mengakses menu akun (nama akun), kemudian sistem akan menampilkan menu “User Detail” dan “Keluar”, dimana menu “User Detail” digunakan untuk mengganti *email* atau *password* user, dan menu “Keluar” digunakan untuk mengeluarkan akses akun tersebut. . Tabel dekripsi UC-04: Mengelola Akun dapat dilihat pada LAMPIRAN A DEKRIPSI USE CASE.

1. **UC-05 : Mengunggah Data Musik**

UC-05 merupakan kebutuhan fungsi pengguna untuk mengunggah atau menginputkan data musik, dimana pengguna menginputkan berkas audio, judul musik, pada tahap ini juga *user* dapat menentukan apakah data musik, dapat diakses oleh publik, atau diprivasi dengan dibatas aksesnya menggunakan proses enkripsi Tabel dekripsi UC-05: Mengunggah Data Musik dapat dilihat pada LAMPIRAN A DEKRIPSI USE CASE.

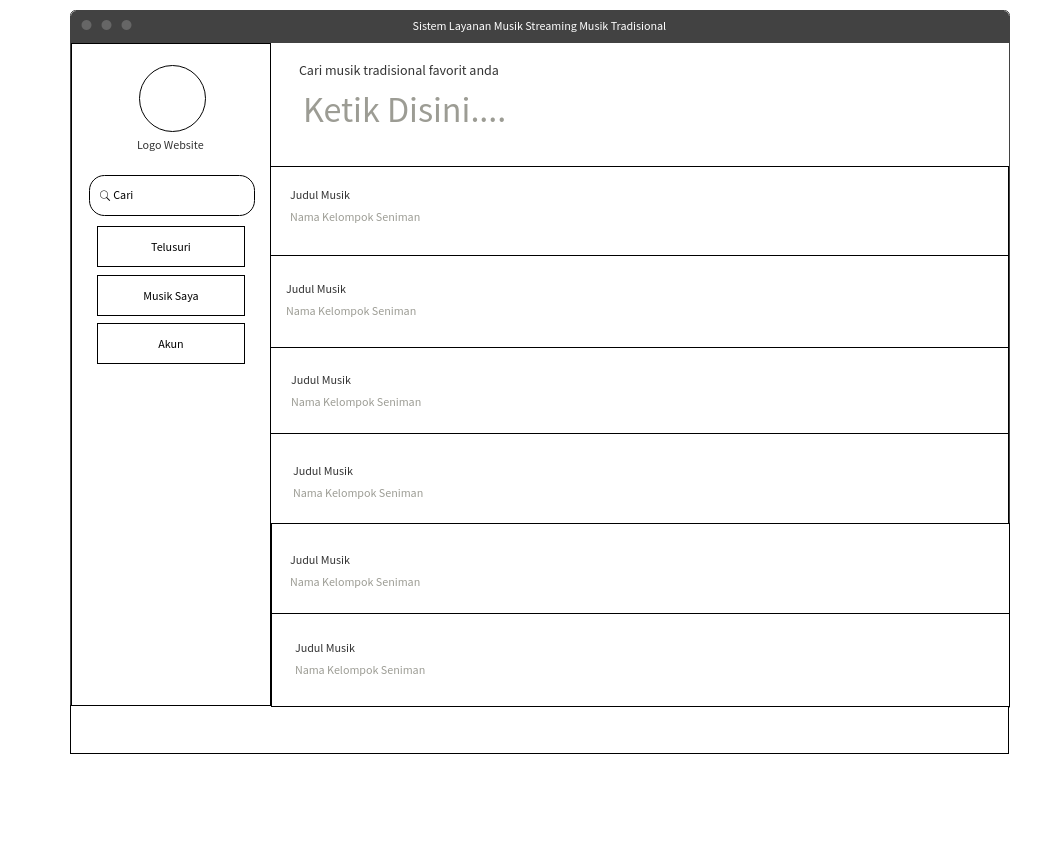
## Rancangan Antarmuka Sistem

Pada tahap ini membuat rancangan desain tampilan halaman aplikasi *website* yang akan dibangun. Desain antamuka sistem aplikasi *website* dirancang sesuai dengan hasil analisis kebutuhan aplikasi yang telah didefinisikan sebelumnya yang mengacu pada dekripsi *Use Case* yang telah dibuat. Desain antarmuka dapat dilihat pada Gambar 3.2, Gambar 3.3, Gambar 3.4, Gambar 3.5, Gambar 3.6, Gambar 3.7, dan Gambar 3.8.



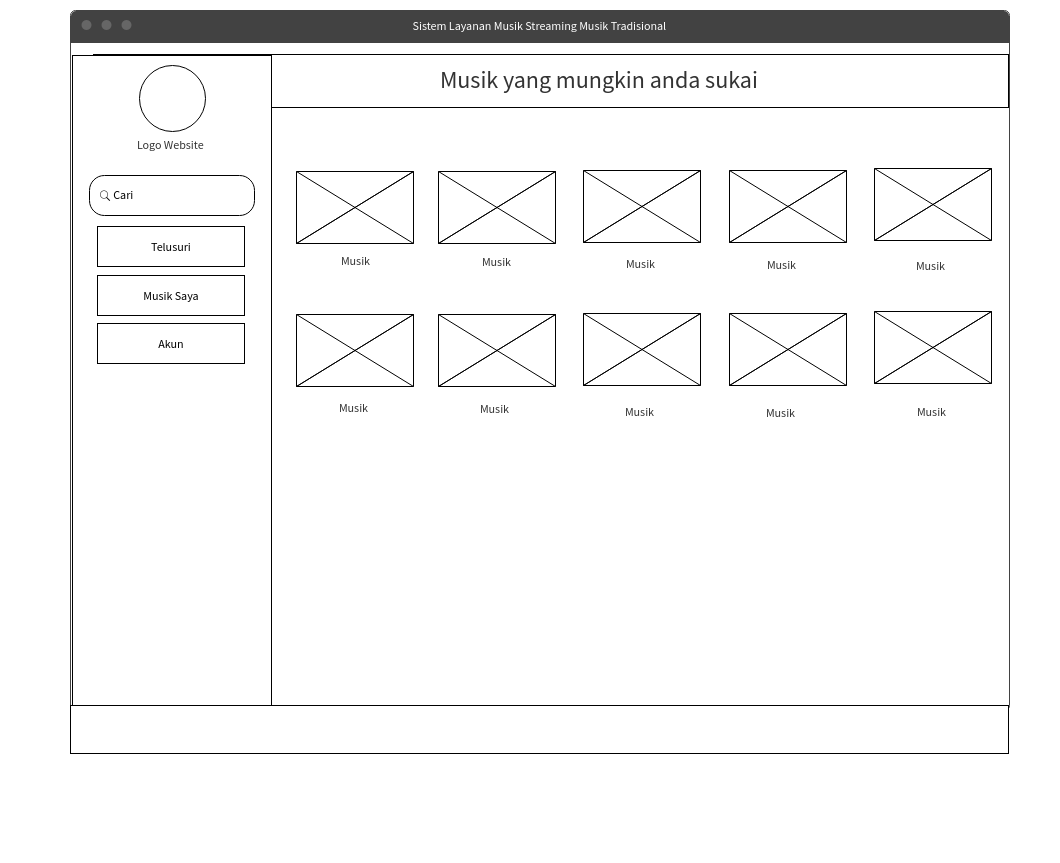
Gambar 3. 3 Rancangan Halaman Utama

Pada Gambar 3.3 diatas menunjukan tampilan rancangan halaman utama atau halaman beranda dari sistem layanan musik streaming. Pada halaman ini sistem menampilkan menu atau fitur yang tersedia pada sistem aplikasi.



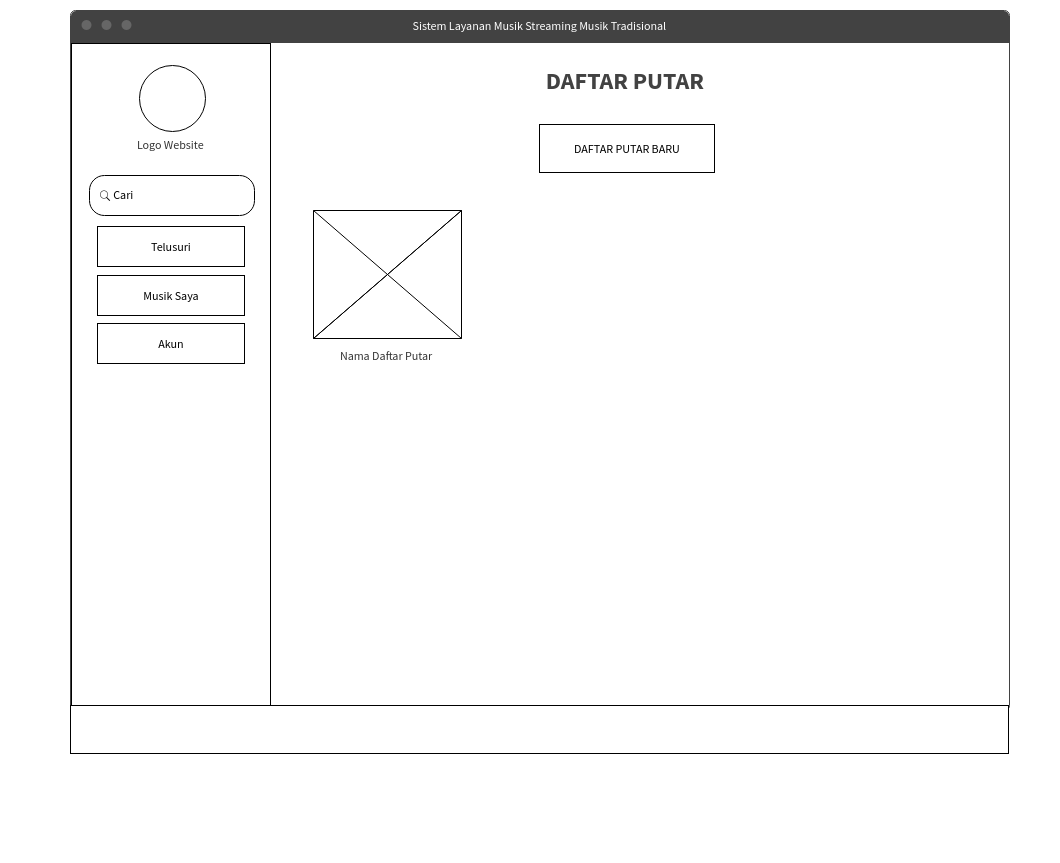
Gambar 3. 4 Rancangan Halaman Pencarian

Pada Gambar 3.4 diatas menunjukan tampilan halaman pencarian pada sistem, *user* hanya perlu memasukan kata kunci yang ingin dicari, baik itu berupa judul musik, nama kelompok seniman, atau asal daerah musik tersebut, sistem akan menampilkan daftar hasil pencarian pada bagian bawah bar pencarian.



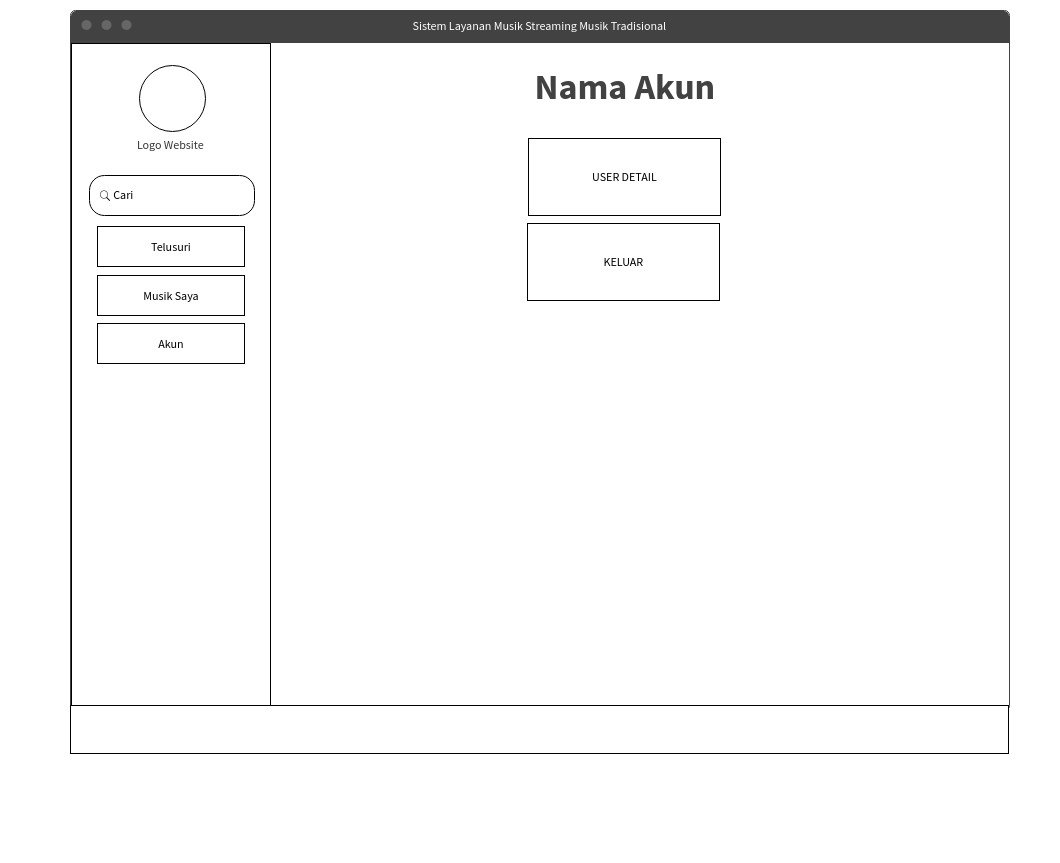
Gambar 3. 5 Rancangan Halaman Penelusuran

Pada Gambar 3.5 diatas menunjukan tampilan halaman penelusuran pada sistem, *user* hanya perlu mengakses menu tersebut dengan mengklik menu “Telusuri”, kemudian sistem akan menampilkan musik-musik yang tersedia pada sistem. *User* hanya perlu memilih musik yang disukai.



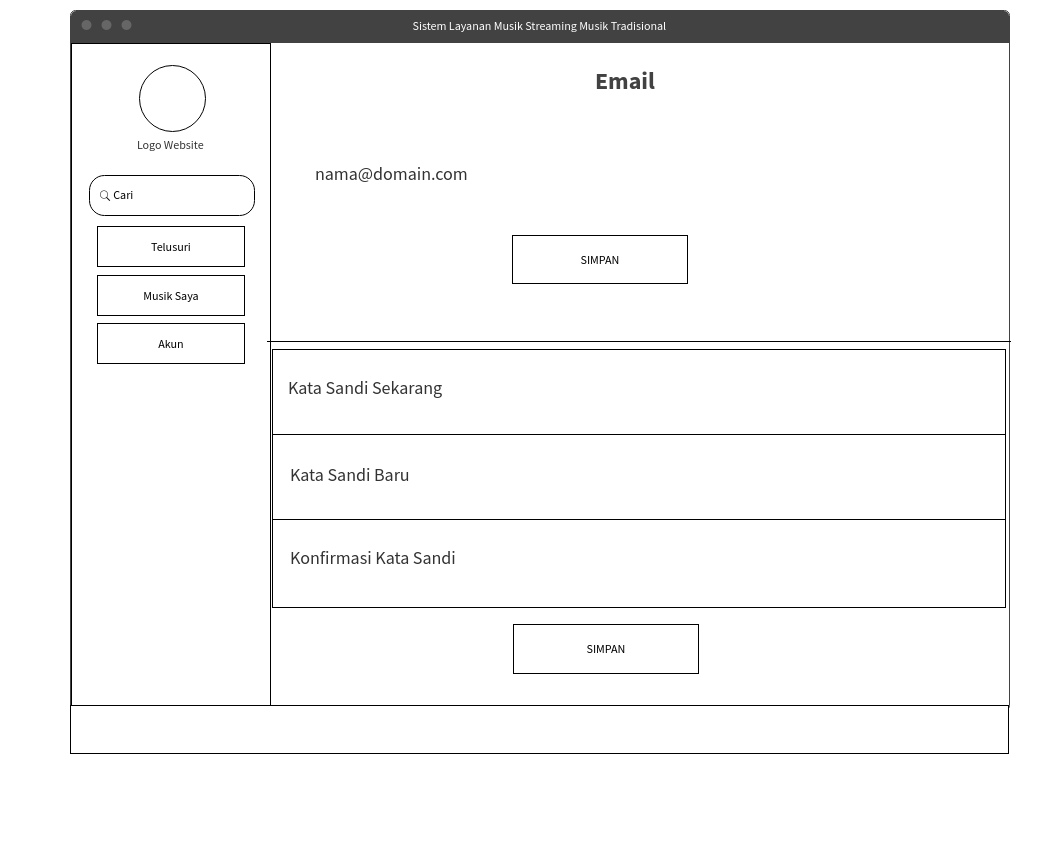
Gambar 3. 6 Rancangan Halaman Musik Saya

Pada Gambar 3.6 diatas menunjukan tampilan Halaman Musik Saya dimana menuini berfungsi untuk menampilkan daftar putar musik yang dimiliki oleh *user* tersebut, selain itu pada menu ini *user* dapat menambahkan daftar putar baru dengan mengklik tombol “DAFTAR PUTAR BARU”, selain itu *user* dapat menghapus daftar putar.



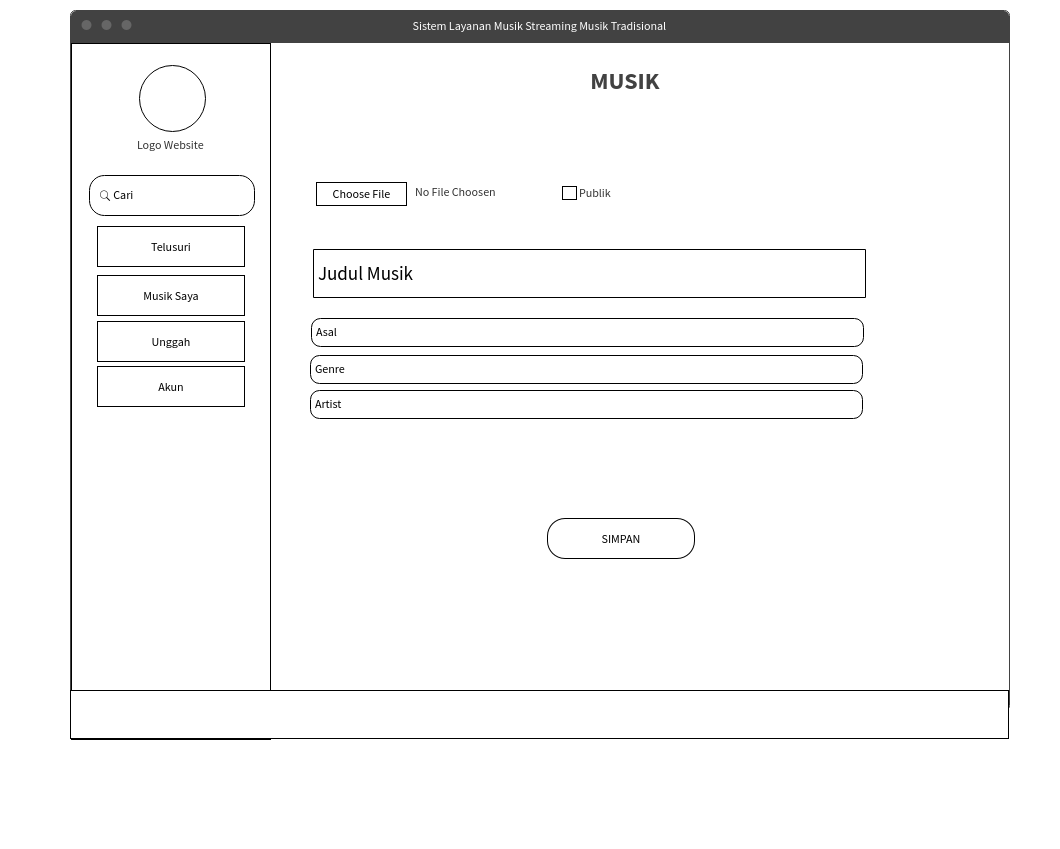
Gambar 3. 7 Rancangan Halaman Akun

Pada Gambar 3.7 diatas menunjukan tampilan Halaman Akun dimana *user* disediakan menu untuk mengubah *email* atau *password* dengan mengakses “User Detail”, dan jika *user* ingin mengeluarkan akses terhadap akun tersebut dengan hanya mengakses tombol keluar.



Gambar 3. 8 Rancangan Halaman User Detail

Pada Gambar 3.8 diatas menunjukan tampilan Halaman “User Detail” pada menu disediakan disediakan fitur untuk mengubah *email* atau *password*, dengan menginputkan data yang baru dan mengklik tombol “SIMPAN”.

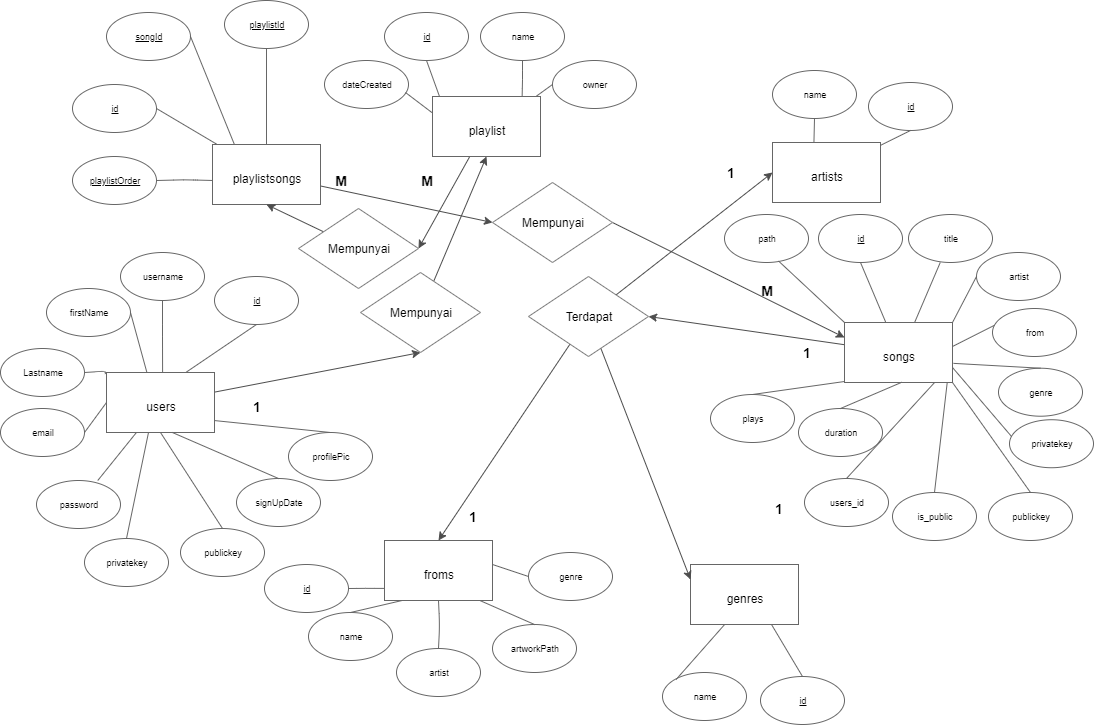


Gambar 3. 9 Rancangan Halaman Unggah Musik

Pada Gambar 3.9 diatas menunjukan tampilan Halaman Unggah Musik, dimana pada menu ini *user* dapat mengunggah atau menginputkan data musik tradisional yang dimiliki, data yang diinputkan berupa berkas file audio, judul, asal, genre atau jenis, serta nama kelompok seni *(artist)* yang memiliki karya musik tersebut, selain itu pada menu ini *user* dapat menentukan apakah data musik tersebut dapat diakses oleh publik, atau dibatasi aksesnya *(private)* agar tidak dapat digunakan oleh pihak yang tidak berhak sehingga data pada sistem terlindungi.

## Rancangan Database

### ERD (Entity Relationship Diagram)

****

Gambar 3. 10 Rancangan ERD Sistem

Pada Gambar 3.10 Rancangan ERD Sistem diatas terdapat tujuh entitas, yaitu entitas users, entitas songs, entitas artists, entitas genres, entitas genres, entitas froms, entitas playlist, dan entitas playlistsongs. Entitas songs, entitas artists, entitas genres, entitas genres, dan entitas froms dihubungkan dalam satu relasi yaitu Terdapat. Pada entitas users dan entitas playlist dihubungkan dalam satu relasi yaitu Mempunyai, sedangkan pada entitas playlistsongs dan entitas songs dihubungkan dalam satu relasi yaitu Mempunyai, pada entitas songs terdapat duabelas atribut antara lain: id, title, artist, from, genre, duration, plays, path, privatekey, publikey, is\_public dan users\_id pada entitas froms terdapat id, name, artist, artworkPath, dan genre, pada entitas genres terdapat id dan name, pada entitas artist id dan name, pada entitas playlist terdapat id, name, owner, dan dateCreated, pada entitas playlistsongs terdapat id, songId, playlistId dan playlistOrder.

Relasi yang digunakan pada ERD diatas untuk entitas songs, froms, artists, dan genres adalah *one to one*, dimana setiap entitas songs berhubungan terhadap satu entitas froms, artists dan genres, pada entitas users dan entitas playlist relasi yang digunakan adalah *one to many,* dimana entitas pada users dapat berhubungan dengan banyak playlist, pada entitas playlists dan playlistsongs relasi yang digunakan adalah *many to many,* yang berarti banyak entitas playlist dapat berhubungan dengan banyak entitas playlistsongs, kemudian untuk entitas playlistsongs dan entitas songs relasi yang digunakan adalah *many to many,* yang berarti banyak entitas playlistsongs dapat berhubungan dengan banyak entitas songs.

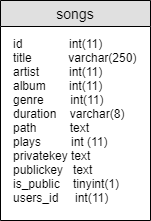
### Conceptual Data Model

****

Gambar 3. 11 Rancangan Conceptual Data Model

Gambar 3.11 diatas merupakan rancangan database yang akan digunakan pada sistem layanan musik *streaming* dengan mengimplementasikan algoritma RSA, berikut merupakan tabel yang dibutuhkan pada sistem ini, yaitu tabel songs,tabel songs digunakan untuk menyimpan menyimpan informasi detail dari setiap musik yang disimpan, kolom path pada basis data pada sistem ini nantinya akan diamankan melalui proses enkripsi dan dekripsi menggunakan algoritma RSA menggunakan kunci privatekey dan publickey yang disimpan pada tabel.

### Physical Data Model

****

Gambar 3. 12 Rancangan Physical Data Model

Pada Gambar 3.12 diatas merupakan Physical Data Model untuk tabel songs. Pada tabel songs terdapat atribut id, artist, from, genre, plays, dan users\_id masing-masing menggunakan tipe data interger dengan Panjang sebelas, title menggunakan tipe data varchar dengan panjang dua ratus lima puluh, dan duration menggunakan tipe data varchar dengan panjang delapan, path, privatekey, dan publickey menggunakantipe data text, dan pada atribut is\_public menggunakan tipe data tinyin

## Pengolahan Data

Proses pengolahan data ini terdiri dari beberapa proses untuk dapat diimplementasikan algoritma RSA untuk menjaga keamanan data pada sistem. Ada empat tahap dalam proses pengolahan data:

1. **Input Data**

Pada tahap ini merupakan tahap pengambilan data melalui observasi yang diambil langsung ke lapangan untuk memperoleh data lengkap terhadap data musik yang akan digunakan pada sistem.

1. **Pre-processing**

Pada proses ini, data yang didapatkan akan diolah dulu untuk menyesesuaikan dengan penerapan algoritma RSA untuk menjaga keamanan data.

1. **Proses Implementasi Algoritma RSA**

Setelah data diperoleh, proses selanjutnya adalah bagaimana mengolah data tersebut dengan menerapkan algoritma kriptografi RSA, untuk menjaga keamanan data. Dengan menerapkan algoritma ini, pengguna dapat menentukan apakah data musik dapat diakses oleh publik atau hanya pengguna tersebut saja dan menambahkan enkripsi dan dekripsi pada karakter file audio.

1. **Post-Processing**

Setelah data diproses, selanjutnya sistem akan menghasilkan output terhadap keamanan data dimana pada basis data tabel songs pada kolom *path* data akan terenkripsi sehingga pihak yang tidak berhak untuk mengkases data tersebut, tidak dapat mengakses dan membaca data tersebut.

## Pengujian dan Evaluasi

Pada tahap ini akan dilakukan pengujian terhadap aplikasi *website* yang telah dibuat pada bagian sebelumnya. Di dalam proses pembuatan suatu sistem, pasti tentu terdapat proses pengujian atau *testing.* Setelah sistem selesai dibangun, maka selanjutnya sistem digunakan dan diuji untuk membuktikan keakuratan sistem yang dibuat. Pengujian sistem akan dilaksanakan dalam dua tahap, yaitu pengujian fungsionalitas sistem dan pengujian keamanan data pada sistem.

### Pengujian Fungsionalitas

Pengujian fungsionalitas sistem menggunakan metode pengujian *Black Box,* Tahap pengujian fungsionalitas merupakan tahap yang digunakan untuk memastikan apakah sistem yang sudah dibuat telah memenuhi tujuan yang diinginkan . Pengujian pada penelitian ini mengacu pada sistem secara keseluruhan, apakah sudah memenuhi rancangan atau belum.

*Black box texting* adalah metode pengujian perangkat lunak yang menguji fungsionalitas aplikasi yang bertentangan dengan struktur internal atau kerja. Pengetahuan khusus dari kode aplikasi / struktur internal dan pengetahuan pemrograman pada umumnya tidak diperlukan. Uji kasus dibangun di sekitar spesifikasi dan persyaratan, yakni, aplikasi apa yang seharusnya dilakukan. Menggunakan deskripsi eksternal perangkat lunak, termasuk spesifikasi, persyaratan, dan desain untuk menurunkan uji kasus. Tes ini dapat menjadi fungsional atau non-fungsional, meskipun biasanya fungsional. Perancang uji memilih input yang valid dan tidak valid dan menentukan output yang benar.

Tabel 3. 2 Pengujian Blackbox

|  |  |
| --- | --- |
| *Tingkah Laku Sistem* |  |
| *Deskripsi* |  |
| *Kondisi awal* |  |
| *Tanggal Pengujian* |  |
| *Penguji* |  |
| *Skenario* | |
| 1. |  |
| 2. |  |
| Dst… |  |

Tabel 3. 3 Hasil Pengujian Blackbox

|  |  |  |
| --- | --- | --- |
| **Hasil yang Diharapkan** | **Hasil yang Didapatkan** | **Kesimpulan** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

### Pengujian Data Audio MP3

Proses pengujian data audio MP3 bertujuan untuk memastikan bahwa proses enkripsi dan dekripsi telah dapat diimplementasikan pada *file* MP3 dan bekerja dengan baik, dengan melakukan perbandingan gelombang suara sebelum dan sesudah enkripsi dilakukan. Dari hasil pengujian ini akan terlihat bahwa ada perbedaan gelombang suara sebelum dan setelah dilakukan proses enkripsi. Hal ini menunjukan bahwa data asli telah mengalami perubahan setelah proses enkripsi. Selain itu dilakukan juga pembandingan terhadap ukuran file yang telah terenkripsi dengan file yang telah terdekripsi yang akan menunjukan bahwa data telah mengalami proses dekripsi dan enkripsi (Diarse & Bendi, 2016), yang terakhir akan dilakukan skenario pengujian terhadap akses data file MP3 dengan mengaksesnya pada direktori *folder* dimana data MP3 yang telah dienkripsi akan disimpan.

Tabel 3. 4 Tabel Pengujian Gelombang Suara Data MP3

|  |  |  |  |
| --- | --- | --- | --- |
| **Perbandingan Gelombang Suara File MP3** | | | |
| **No.** | **Nama File** | **Sebelum Terenkripsi *(Plaintext File)*** | **Setelah Terenkripsi *(Chipertext File)*** |
| 1. |  |  |  |
| 2. |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Tabel 3. 5 Perbandingan Ukuran Data MP3

|  |  |  |  |
| --- | --- | --- | --- |
| **Perbandingan Ukuran Data File MP3** | | | |
| **No.** | **Nama Data** | **File Terenkripsi** | **File Terdekripsi** |
| 1. |  |  |  |
| 2. |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

### Pengujian Keamanan Algoritma RSA

Pengujian keamanan algoritma enkripsi RSA pada tugas akhir ini yaitu dengan menghitung persentase dari *avalanche effect* menggunakan rumus persamaan [2.1]*.* Semakin besar perubahan yang terjadi, semakin baik performansi dari algoritma kriptografi tersebut. Diharapkan persentase *avalanche effect* yang dihasilkan berkisar 45 –60 % dari keseluruhan bit ciphertext (sekitar separuhnya dimana 50 % adalah hasil yang sangat baik bagi sebuah algoritma).

Tabel 3. 6 Pengujian Avalanche Effect

|  |  |  |
| --- | --- | --- |
| ***Plaint Text*** | ***Chiper Text*** | ***Avalanche Effect*** |
|  |  |  |
|  |  |  |

# BAB IV

# HASIL DAN PEMBAHASAN

Pada bab ini akan membahas mengenai bagaimana sistem diimplementasikan serta hasil yang didapatkan beserta penjelasan dari tiap proses dalam melindungi data pada sistem dengam mengimplementasikan algoritma RSA.

## Pengumpulan Data Set

Data yang digunakan pada penelitian ini menggunakan data primer yang diperoleh dengan metode observasi langsung ke lapangan. Adapun rincian data yang digunakan adalah sebagai berikut.

1. Data berformat MP3, yang merupakan data audio yang direkam pada saat observasi, data inilah yang nantinya menjadi data utama yang akan digunakan oleh user untuk diputar dan didengarkan, dan pada berkas data audio berformat MP3 ini, file akan diberikan nama yang nantinya akan dipergunakan sebagai path yang dienkripsi pada *database* dengan menggunakan algoritma RSA dan juga proses enkripsi pada karakter file.
2. Data yang dibutuhkan adalah informasi detail mengenai setiap berkas audio, diantara lain judul musik, asal daerah, nama kelompok seni, jenis atau genre, durasi, data-data tersebut merupakan data yang akan ditampilkan langsung pada antarmuka sistem.

## Diagram Alir Pembentukan Kunci pada Sistem

Pada tahap ini akan menggambarkan dan menjabarkan tentang bagaimana implementasi algoritma RSA untuk pengamanan data pada sistem dengan menggunakan diagram alir *(flowchart)* untuk mengambarkan proses enkripsi data pada sistem.



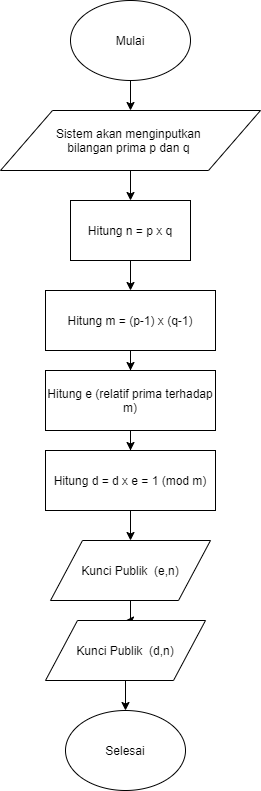
Gambar 4. 1 Diagram Alir Proses Pembentukan Kunci Pengguna

Pada tahap ini dapat dilihat pada Gambar 4.1 menjelaskan pada proses apa kunci akan dibangkitkan pada sistem, yaitu kunci akan dibangkitkan setelah pengguna *(user)* selesai melakukan proses registrasi, ketika data pengguna dikirim dari *web server* ke *database server* pada saat itu juga *public key* dan *private key* dipasangkan dan disimpan pada tabel *users.*

* 1. **Diagram Alir Pembentukan Kunci Public dan Private**

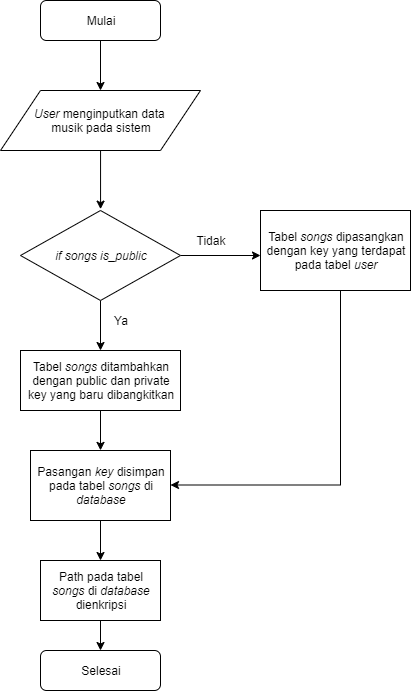
Proses pembentukan kunci public dan kunci private yang digunakan pada sistem untuk proses enkripsi dan dekripsi dapat dilihat pada Gambar 4.2 berikut.

* 1. Sistem akan membangkitkan dua buah bilangan prima misalkan p dan q.
  2. Diperoleh n = p x q dan m = (p - 1) x (q - 1).
  3. Sistem akan menghitung nilai e, , dengan gcd(e,m) = 1.
  4. Sistem akan menghitung d, yaitu de = 1 (mod m).
  5. Diperoleh pasangan kunci publik (e,n) dan kunci privat (d,n).

****

Gambar 4. 2 Diagram Alir Pembentukan Kunci Public dan Private

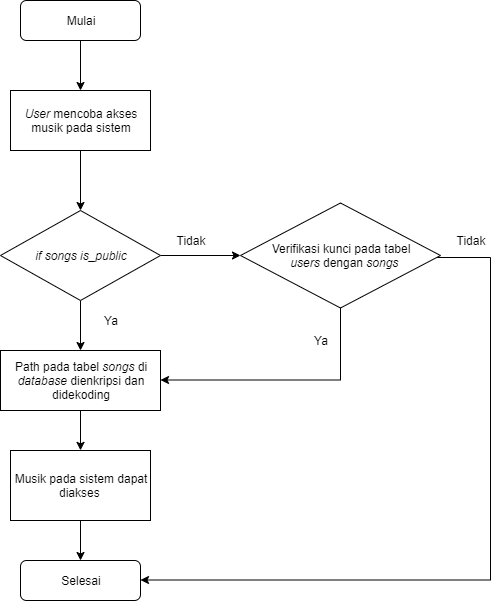
* 1. **Diagram Alir Proses Enkripsi terhadap Path Data Musik**



Gambar 4. 3 Diagram Alir Proses Enkripsi terhadap Path Data Musik

Pada Gambar 4.3 dapat dilihat mengenai bagaimana proses dari awal data diinputkan pada sistem sampai data tersebut terlindungi dengan enkripsi, diawali dengan *user* menginputkan atau mengunggah data berkas audio MP3 yang sudah diberi nama, judul musik, genre, dan nama kelompok seni dan asal daerah, pada tahap ini user juga menentukan apakah musik dapat diakses secara publik atau privasi, dan jika data musik bersifat publik, maka sistem akan membangkitkan pasangan kunci baru untuk data musik tersebut, dan menyimpannya pada tabel songs tetapi jika musik bersifat privasi maka pasangan kunci yang digunakan adalah pasangan kunci yang dibangkitkan oleh *user* pada saat *user* tersebut registrasi*,* kemudian *path* pada tabel songs akan dienkripsi sehingga data musik, tidak dapat dibaca dan diakses oleh pihak yang tidak berhak.

* 1. **Diagram Alir Dekripsi Path Data Musik**

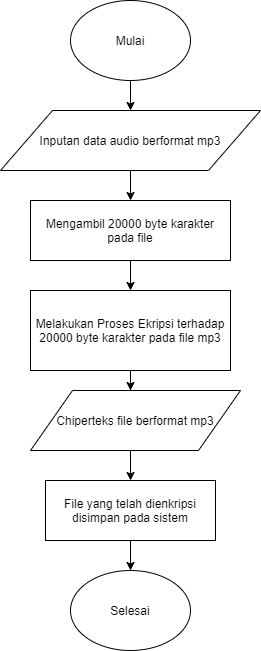


Gambar 4. 4 Diagram Alir Dekripsi Path Data Musik

Pada Gambar 4.4 dapat dilihat mengenai bagaimana proses oleh *user* untuk mengakses data yang sudah terlindungi dengan enkripsi pada sistem, pada saat user akan mencoba mengakses musik, akan dicek apakah musik berisifat publik atau privasi, *path* pada tabel songs yang sebelumnya sudah dienkripsi pada sistem akan otomatis didekripsi dan didekoding lalu dapat diakses, tetapi jika musik bersifat privasi maka pasangan kunci yang terdapat pada tabel usersyang akan mengakses kunci tersebut akan dicocokan dengan pasangan kunci yang terdapat pada tabel songs, jika tidak cocok maka proses akan terhenti sampai disitu karena artinya bukan *user* tersebut yang menginputkan data musik ke sistem tersebut, namun jika cocok maka *path* pada tabel songs yang sebelumnya sudah dienkripsi pada sistem akan otomatis didekripsi dan didekoding lalu dapat diakses, karena artinya *user* tersebutlah yang menginputkan atau mengunggah data ke sistem.

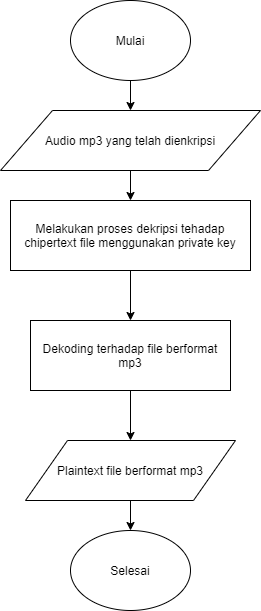
* 1. **Diagram Alir Enkripsi Karakter pada Data MP3**

Pada gambar 4.5 menunjukan bagaimana file audio berformat MP3, mengalami proses enkripsi pada sistem, dimana data audio yang telah diunggah akan diambil dan dibaca karakteristik pada file, kemudian karaktar akan dienkripsi sebanyak 2000 *bytes* karakter menggunakan public key sepanjang 2048 *bit* untuk mencegah file digunakan oleh pihak yg tidak berhak, lalu file yang telah dienkripsi akan disimpan dan menghasilkan *chipertext file* berformat MP3 yang tidak akan bisa diakses tanpa proses dekripsi.

**

Gambar 4. 5 Diagram Alir Enkripsi Pada Karakter MP3

* 1. **Diagram Alir Enkripsi Karakter pada Chiperteks File MP3**



Gambar 4. 6 Diagram Alir Dekripsi Pada Chiperteks File MP3

Pada Gambar 4.6 menunjukan proses terhadap data yang telah terenkripsi atau *chipertext file MP3,* dimana data sebanyak 20000 *byte* karakter yang telah terenkripsi sebelumnya akan dibaca dan karakter yang telah terenkripsi akan didekripsi menggunakan *private key* agar file yang terenkripsi tersebut dapat diakses kembali oleh User.

## Implementasi Sistem

Pada tahap ini dijelaskan mengenai pembuatan aplikasi sistem layanan musik *streaming* berbasis web dengan mengimplementasikan algoritma RSA sebagai perlindungan data.

### Lingkungan Implementasi

Sistem dibangun dan dirancang pada lingkungan berbasis sistem operasi Windows 10 Pro 64-bit. Sistem dirancang dan dibangun menggunakan notebook yang mempunyai sesifikasi hardware dengan CPU AMD FX-7500 Radeon R7, 10 Compute Cores 4C+6G (4 CPUs) ~2.1GHz. Dengan RAM 8192MB.

Sistem dibangun menggunakan Bahasa pemrograman PHP dan *JavaScript* dengan *database* menggunakan phpMyAdmin. Berikut merupakan spesifikasi lengkap, ditunjukan pada tabel 4.1 dan tabel 4.2

Tabel 4. 1 Daftar Spesifikasi Perangkat Keras

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Perangkat Keras** | **Spesifikasi** | | | |
| **Processor** | **Monitor** | **RAM** | **Hardisk** |
| **PC** | AMD FX-7500 Radeon R7, 10 Compute Cores 4C+6G (4 CPUs) ~2.1GHz. | 15.6 Inch | 8192MB | 500GB |

Tabel 4. 2 Daftar Spesifikasi Perangkat Lunak

|  |  |  |
| --- | --- | --- |
| **No.** | **Perangkat Lunak** | **Fungsi** |
| 1. | Windows 10 Pro 64-bit | Sistem Operasi Notebook |
| 2. | Sublime Text 3 | *Text Editor* untuk *coding* |
| 3. | phpMyAdmin | *Platform* mengelola *database* |
| 4. | XAMPP for Windows | Sebagai server pada localhost |
| 5. | Microsoft Word 2016 | Untuk membuat laporan |
| 6. | Draw.io | Untuk mendesain diagram perancangan |
| 7. | Google Chrome | Sebagai *browser* untuk uji coba sistem |
| 8. | Audacity | Untuk visualisi gelombang suara pada proses pengujian data |

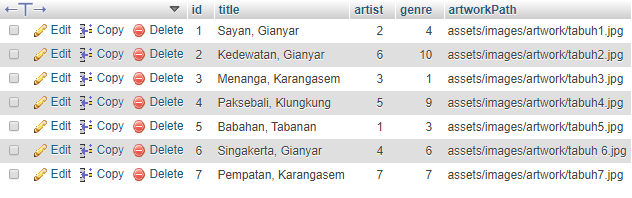
### Pembuatan Basis Data

Pada tugas akhir ini, pembuatan basis data untuk sistem itu sendiri dilakukan dengan phpMyAdmin dengan database yang diberi nama “musita”. Pada sistem secara keseluruhan menggunakan tujuh tabel, yaitu tabel “artists” “froms” “genres” “playlists” “playlistsongs” “songs” dan “users”.



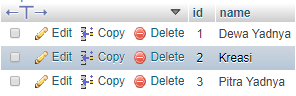
Gambar 4. 7 Tabel artist pada Database

Gambar 4.7 diatas adalah tampilan dari tabel “artists” yang digunakan untuk menyimpan infomasi mengenai nama grup seniman (sekaa gong) yang terdapat pada sistem.



Gambar 4. 8 Tabel froms pada Database

Gambar 4.8 diatas adalah tampilan dari tabel “froms” yang digunakan untuk menyimpan informasi asal daerah dari seniman (sekaa gong), serta menyimpan informasi seniman, jenis musik, serta gambar kelompok seniman yang akan ditampilkan pada sistem.



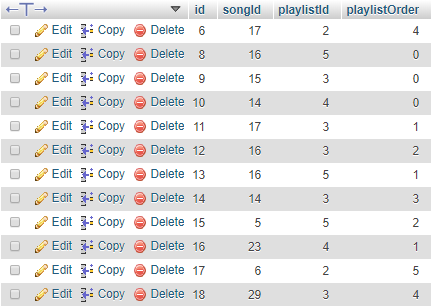
Gambar 4. 9 Tabel genres pada Database

Gambar 4.9 diatas adalah tampilan dari tabel “genres” yang digunakan untuk menyimpan informasi mengenai nama jenis musik yang terdapat pada sistem.



Gambar 4. 10 Tabel playlists pada Database

Gambar 4.10 diatas adalah tampilan dari tabel “playlist” yang digunakan untuk menyimpan informasi dari playlist *user,* adapun data yang disimpan pada tabel ini adalah nama dari playlist, user pemilik playlist, dan tanggal pembuatan playlist tersebut.



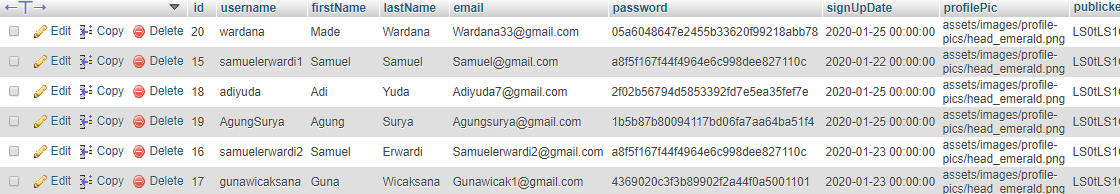
Gambar 4. 11 Tabel playlistsongs pada Database

Gambar 4.11 diatas adalah tampilan dari tabel “playlistsongs” yang digunakan untuk menyimpan informasi mengenai data musik yang disimpan pada playlist.



Gambar 4. 12 Tabel songs pada Database

Gambar 4.12 diatas adalah tampilan dari tabel “songs” yang digunakan untuk menyimpan informasi mengenai informasi detail musik, adapun data yang disimpan id musik, nama atau judul, seniman, asal, jenis musik, durasi, dan path yang menghubungkan berkas audio terhadap sistem tersebut.



Gambar 4. 13 Tabel users pada Database

Gambar 4.13 diatas adalah tampilan dari tabel “users” yang digunakan untuk menyimpan informasi mengenai informasi user atau pengguna yang sudah melakukan registrasi pada sistem, adapun data yang disimpan adalah *username,* nama depan, nama belakang, alamat email, kata sandi, dan tanggal melakukan registrasi pada sistem.

### Membuat Kode Program

Ada beberapa potongan file dan skrip kode program yang digunakan untuk membangun sistem layanan musik streaming dengan mengimplementasikan algoritma enkripsi RSA ini, Untuk *source code* lengkap akan dilampirkan pada halaman lampiran B. Source Code Program.

## Tampilan Antarmuka Sistem



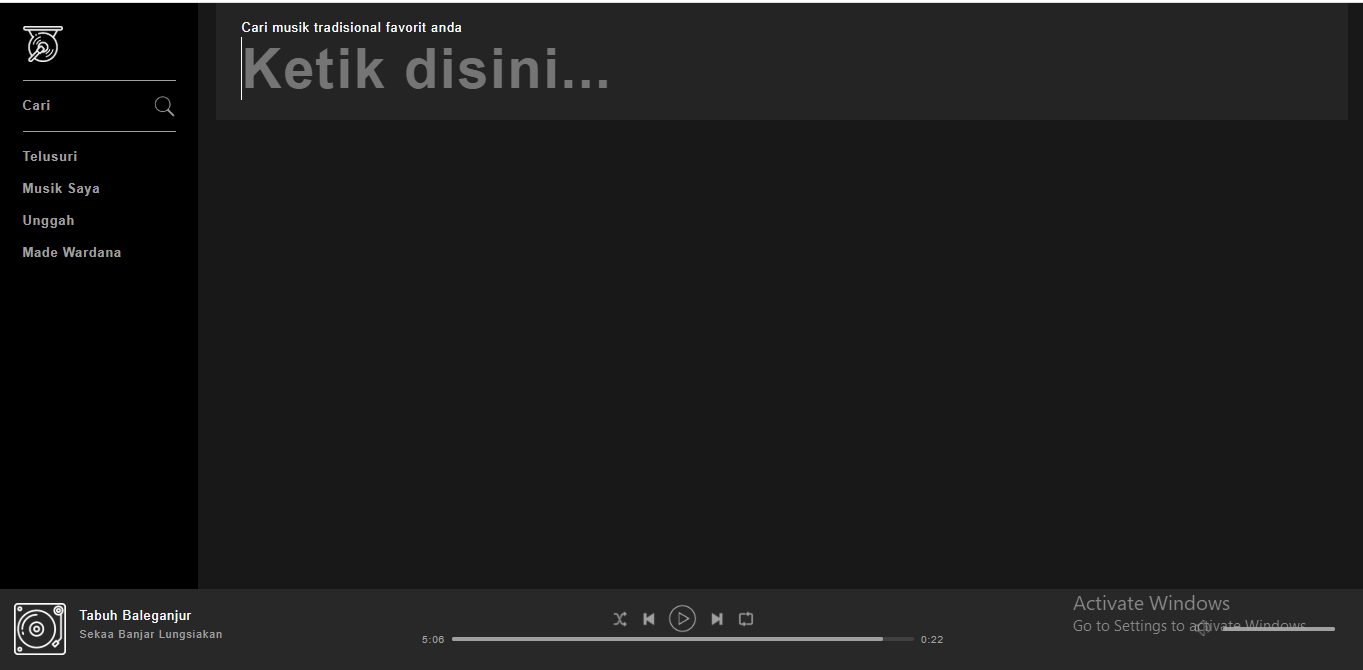
Gambar 4. 14 Tampilan Halaman Registrasi

Gambar 4.14 diatas merupakan tampilan halaman registrasi sistem, sebelum user ingin mengakses layanan pada sistem, user diwajibkan untuk memiliki akun dengan cara melakukan proses registrasi dengan mengisi form-form data pribadi pengguna. Setelah itu user baru memiliki akses untuk menggunakan layanan yang terdapat pada sistem.



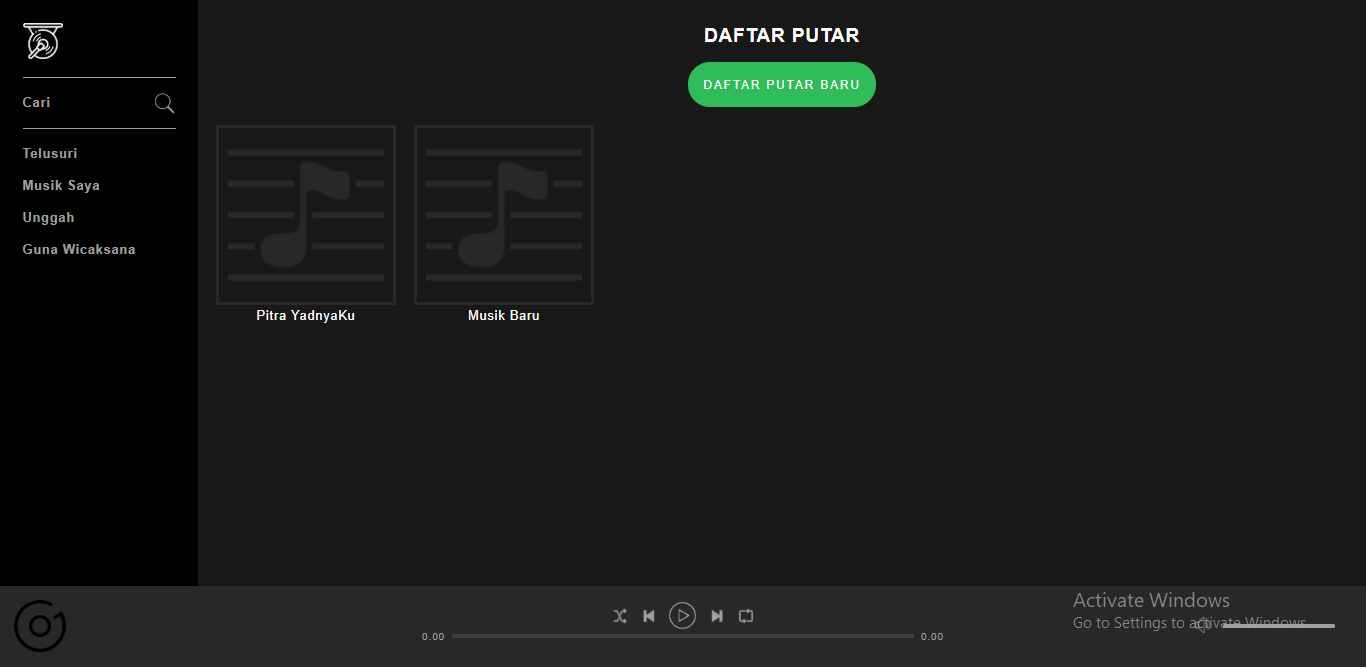
Gambar 4. 15 Tampilan Halaman Utama

Gambar 4.15 diatas menunjukan tampilan rancangan halaman utama atau halaman beranda dari sistem layanan musik *streaming*. Pada halaman ini sistem menampilkan menu atau fitur yang tersedia pada sistem aplikasi.



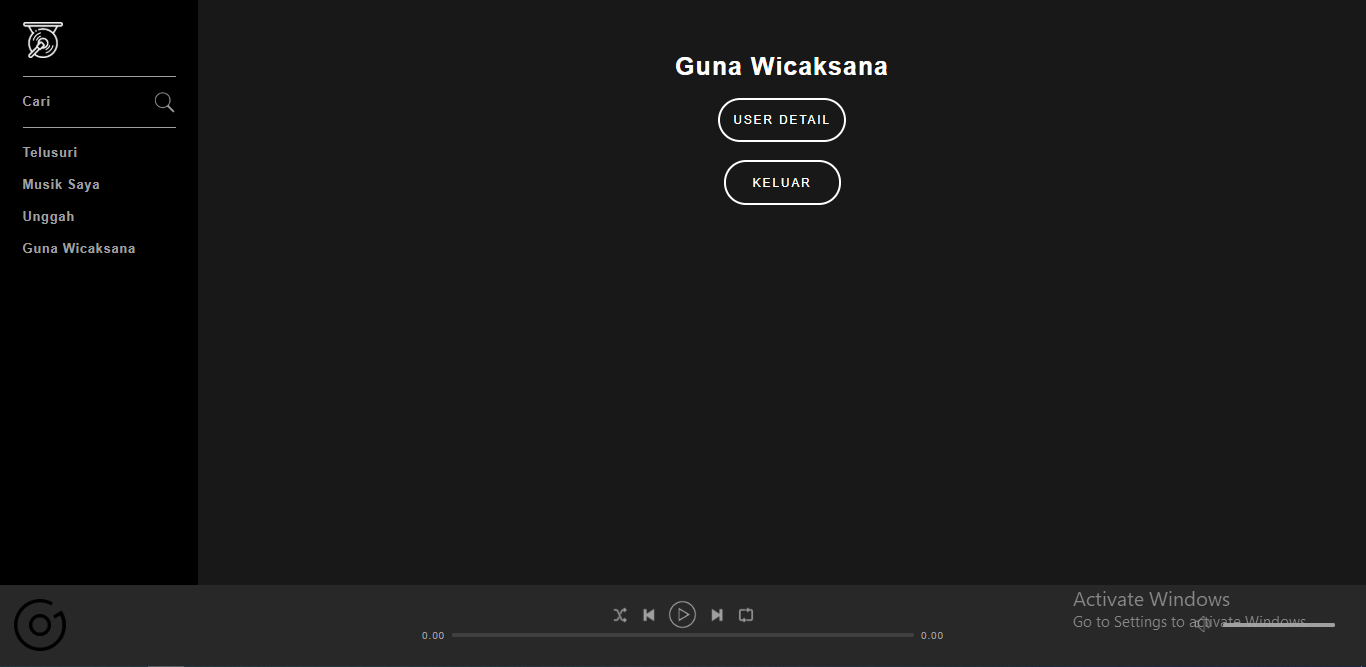
Gambar 4. 16 Tampilan Halaman Pencarian

Pada Gambar 4.16 diatas menunjukan tampilan halaman pencarian pada sistem, user hanya perlu memasukan kata kunci yang ingin dicari, dapat berupa judul musik, nama kelompok seniman, atau asal daerah musik tersebut, sistem akan menampilkan daftar hasil pencarian pada bagian bawah bar pencarian



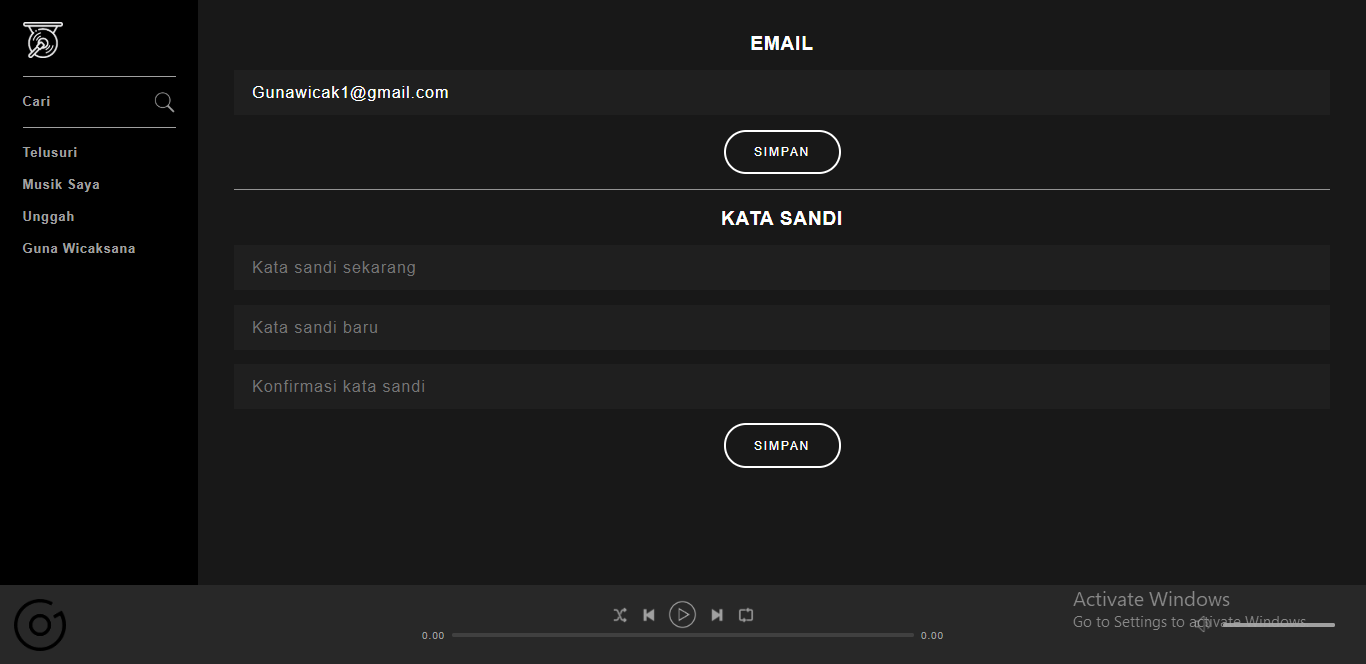
Gambar 4. 17 Tampilan Halaman Musik Saya

Gambar 4.17 diatas menunjukan tampilan Halaman Musik Saya dimana menuini berfungsi untuk menampilkan daftar putar *(playlist)* musik yang dimiliki oleh *user* tersebut, selain itu pada menu ini *user* dapat menambahkan daftar putar baru dengan mengklik tombol “DAFTAR PUTAR BARU”, selain itu *user* dapat menghapus daftar putar.



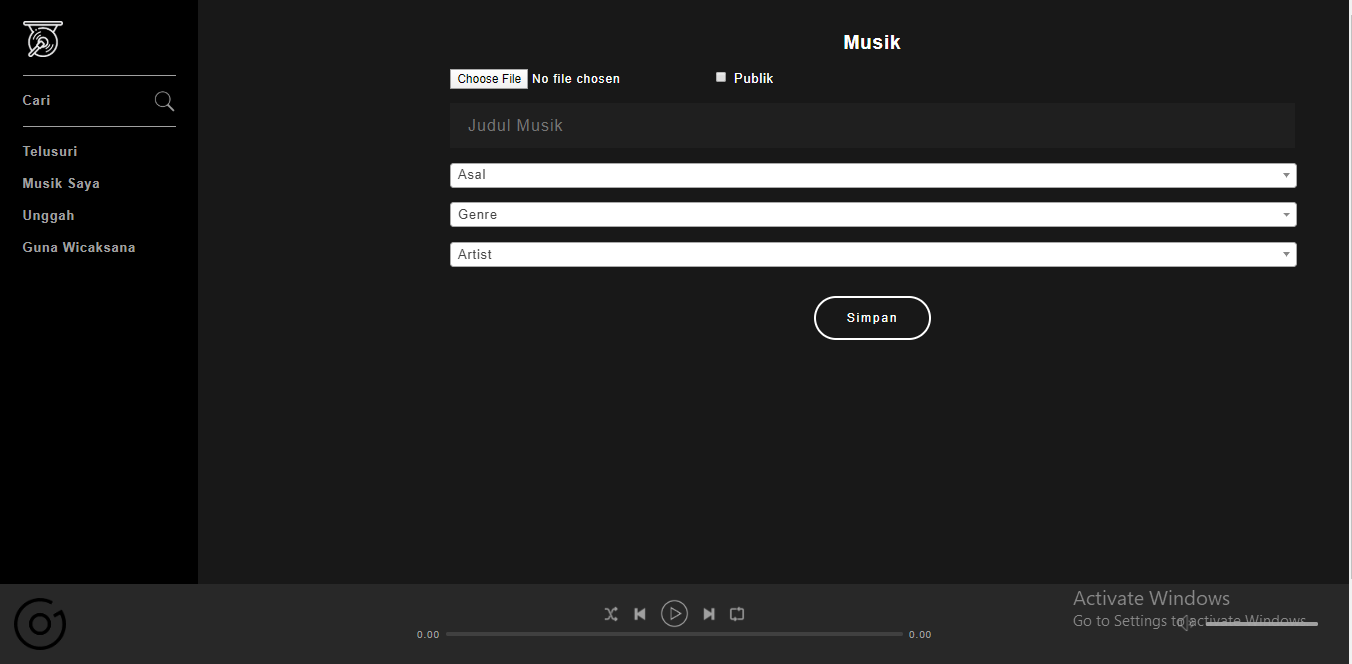
Gambar 4. 18 Tampilan Halaman Akun

Pada Gambar 4.18 diatas menunjukan tampilan Halaman Akun dimana *user* disediakan menu untuk mengubah *email* atau *password* dengan mengakses “User Detail”, dan jika *user* ingin mengeluarkan akses terhadap akun tersebut hanya perlu mengakses tombol keluar.



Gambar 4. 19 Tampilan Halaman User Detail

Gambar 4.19 diatas menunjukan tampilan Halaman “User Detail” pada menu disediakan disediakan fitur untuk menampilkan dan mengubah email atau password, dengan menginputkan data yang baru dan mengklik tombol “SIMPAN”.



Gambar 4. 20 Tampilan Halaman Unggah

Gambar 4.20 merupakan tampilan dari Halaman Unggah User dapat mengunggah data musik, menginputkan berkas audio, judul musik, asal daerah musik tersebut, genre atau jenis, serta nama kelompok seniman dari musik tersebut, serta menentukan akses terhadap musik tersebut, dengan mengakses menu Unggah

## Pengujian Sistem

Pada sub bab ini akan dilakukan proses pengujian sistem dari segi fungsionalitas sistem dan pengujian keamanan algoritma RSA

### Pengujian Fungsionalitas Sistem

Pengujian dilakukan dengan menggunakan metode pengujian *black-box.* Uji coba sistem dilakukan untuk mengetahui ketepatan fungsional pada fitur-fitur yang tersedia pada sistem berdasarkan fungsional yang telah dibahas dan dijabarkan pada bagian desain dan implementasi sistem. Uji coba aplikasi sistem dilakukan sesuai dengan skenario pada detail *use case* yang telah dijelaskan pada bagian desain *use case* pada bab analisis dan perancangan. Adapun beberapa langkah yang dilaksanakan dalam uji coba sistem aplikasi adalah:

1. Mempersiapkan file aplikasi yang dibangun.
2. Membuat daftar fungsionalitas dari aplikasi dan aktivitas apa yang harus sistem dapat kerjakan pada sistem layanan musik streaming. Tabel 4.3 menunjukan skenario-skenario untuk melakukan uji coba aplikasi sistem musik *streaming*. Semakin banyak fungsi pada aplikasi yang berhasil berjalan, semakin bagus dan tepat juga aplikasi yang dibuat.

Tabel 4. 3 Hasil Pengujian Fungsionalitas

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| No. | Nama Fungsi | Skenario Pengujian | Hasil Pengujian | Kesimpulan |
| 1. | Menu Home | Sistem akan mengarahkan user pada halaman utama setelah *user* melakukan registrasi atau login ke sistem. | User dapat mengakses menu “Home”. Pada halaman ini menampilkan halaman utama aplikasi *website*. | Valid |
| 2*.* | Akses Musik | 1. Sistem akan memproses perintah untuk memutar musik yang terdapat pada sistem, setelah user mengklik tombol putar.  2. Sistem tidak akan memutar musik yang sifatnya privasi. | 1.User dapat mengakses lagu untuk didengarkan dengan memilih salah satu lagu, kemudian mengklik tombol putar.  2. User tidak akan bisa mengakses musik yang berisfat privasi. | Valid |
| 3. | Pencarian | 1.Sistem akan menampilkan hasil pencarian, setelah user menginputkan kata kunci yang ingin dicari.  2. Sistem tidak akan menampilkan hasil pencarin dengan kata kunci yang tidak sesuai | 1.User dapat memilih menu “Cari” yang berfungsi untuk menemukan judul musik,, asal daerah, dan seniman.  2.User tidak dapat menggunakan fitur pencarian dengan kata kunci yang tidak sesuai dan sistem tidak menampilkan hasil pencarian. | Valid |
| 4. | Telusuri | Sistem akan menampilkan hasil penelusuran terhadap musik-musik yang terdapat pada sistem, setelah user mengklik tombol telusuri. | User dapat memilih menu “Telusuri” dimana fitur ini menampilkan musik yang tersedia pada sistem sehingga mempermudah user untuk menemukan musik-musik daerah yang tersedia. | Valid |
| 5. | Musik Saya | 1.Sistem akan menampilkan list-list daftar putar yang dimiliki oleh user dengan mengakses bar “Musik Saya”  2. Sistem tidak akan dapat menampilkan list daftar putar jika user tersebut belum pernah membuat sebelumnya. | 1.User dapat memilih menu “Musik Saya” dimana didalam menu ini akan menampilkan daftar putar yang dimiliki oleh akun user tersebut.  2. User akan ditampilkan halaman musik saya tanpa adanya list daftar putar karena belum membuat sebelumnya. | Valid |
| 6. | Membuat Daftar Putar | 1.Sistem memberi akses untuk membuat daftar putar *(playlist)* dan menyimpannya pada *database* sistem.  2. Sistem tidak akan berhasil jika user tidak menginputkan nama daftar putar. | 1.User dapat membuat daftar putar baru sesuai dengan keinginan mereka dengan mengakses tombol “DAFTAR PUTAR BARU”.  2. User tidak berhasil membuat daftar putar karena tidak menginputkan nama daftar putar. | Valid |
| 7. | Menu Akun | Sistem menampilkan fitur yang terdapat pada menu akun, dengan mengakses tombol akun. | Sesuai.  Pada menu ini user dapat melihat menu “USER DETAIL” dan menu “KELUAR” dengan mengakses menu akun pada navigasi bar | Valid |
| 8. | User Detail | Sistem akan menampilkan form-form bagi user yang ingin merubah data email dan *password* dengan menginputkan data terbaru, lalu sistem akan menyimpan perubahan pada *database.* | Sesuai.  User dapat memilih menu “USER DETAIL” dimana pada menu ini user dapat mengganti informasi email dan password akun. | Valid |
| 9. | Keluar | Sistem akan mengeluarkan akses terhadap akun yang sedang login pada sistem tersebut, dengan mengklik tombol keluar. | Sesuai.  User dapat memilih menu “KELUAR” untuk mengeluarkan akses akun tersebut. | Valid |
| 10 | Unggah | 1.Sistem akan menampilkan form yang digunakan untuk menginput data musik pada sistem, *user* berhak menentukan akses terhadap musik tersebut.  2. Sistem tidak akan berhasil mengunggah data musik ke dalam sistem, jika user tidak menginputkan data dengan benar sesuai dengan format data. | 1. User dapat mengunggah data musik ke dalam sistem, serta menentukan akses terhadap musik yang diunggah.  2. User tidak berhasil mengunggah data musik ke dalam sistem dan sistem menampilkan peringatan bahwa user belum memasukan data dengan benar. | Valid |

### Pengujian Keamanan Algoritma RSA

Pada pengujian keamanan algoritma enkripsi RSA tugas akhir ini yaitu dengan menghitung persentase dari *avalanche effect* yang memiliki persamaan : yang diambil dari *chipertext* data yang dilakukan sebanyak dua kali dan menghasilkan hasil yang sama*.* Tujuan dari pengujian ini untuk menguji kompleksitas dari algoritma kriptografi yang digunakan, diharapkan persentase *avalanche effect* yang dihasilkan berkisar 45 –60 % dari keseluruhan bit *ciphertext* (sekitar separuhnya dimana 50 % adalah hasil yang sangat baik bagi sebuah algoritma).

Tabel 4. 4 Hasil Pengujian Avalanche Effect Data Pertama

|  |  |  |
| --- | --- | --- |
| ***Plaint Text*** | ***Chiper Text*** | ***Avalanche Effect*** |
| assets/music/Tabuh eled semar pagulingan.MP3 | HJ1+FtnxrZjpsrw6p4ZXewLlOj2IxQKjznvWhZMHS/iXqxbF/6MVNmqac3VrmT5I68+Anayd+FO0zF/44aYC7EY7AJedA7VQLuLGKV6mH/718UQNk4hPYstOwrxo/d/ZTWr4AZ2vsTeS+zFV8VuwxqoocLDl9bdX4V0h7Q+3hi+JNAT+Pqhuew9rZYxcytJwCSjj6/fno1OachgriUCa4XA95FpFbT0H74AY/eIoN3AemKhDfHsjkuv8OtPQ0duSp9SYFxC8o0Ayo+lTUX1iwHrF8GB5F4tXDnMaSf2A9iyRb5/Fg8I+6b9fGqV9KQQZoho3XBF56G7FH66u3X4l1w== | 176 Perubahan bit /  344 bit Chipertext x 100 % = 50,8 % |
| ***Modifikasi Plain Text*** | ***Hasil Modifikasi Chiper Text*** |
| assets/music/Tabuh eled semar pagulingam.MP3 | HJ1+FtnxrZjpsrw6p4ZXewLlOj2IxQKjznvWhZMHS/iXqxbF/6MVNmqac3VrmT5I68+Anayd+FO0zF/44aYC7EY7AJedA7VQLuLGKV6mH/718UQNk4hPYstOwrxo/d/ZTWr4AZ2vsTeS+zFV8VuwxqoocLDl9bdX4V0h7Q  iuKSffl30U7kYH+lfFrweiF4I4axoNrv8BHS5t6yCXh=VXTdqnKDgPG57Ye8ZFpqt=9hGnu5wjA9o6b5js++oR3O9QSXOZr9QFb/C8a/yo+/48G09i3hAQAaTcwthBeuoAmy+19ICpwu04ixXcAg6hjYF6PbHFHJD2FUJAFS1TfNo6M31X |

Tabel 4. 5 Hasil Pengujian Avalanche Effect Data Kedua

|  |  |  |
| --- | --- | --- |
| ***Plaint Text*** | ***Chiper Text*** | ***Avalanche Effect*** |
| assets/music/Tabuh hujan.MP3 | VSB+Vndjp7zqOKFrIPJHIQA6l71yygBBYRkXCkIuuShdg4F5MgBg/Y7PAzfpJCePh3eHFehTC4HhDwHCXnwfl/L45XBSh6yNLblX35rdj/7ED/s6YUsSnlkACnBX35gfHFYtef5nL8kXFa/zOikdo6bWXeIeWKCT4LcONrbBQDW1bmPp00kclPOpbqiZZH0I0qEUTfYgG0GM3EN1pNX4c0Gi7dbJ6+nWkjj0QyPuT2gSbCvOh8o+EaNmjyCx7enE/ws+aefHPUMJ/S2Llh3ToAk5MP1/EbTyPrWzByuVUVakYPhJyEsyMU45tHWpODX7TWZcgMZRp5yaV+PV3QR79w== | 190 Perubahan bit /  344 bit Chipertext x 100 % = 55,2 % |
| ***Modifikasi Plain Text*** | ***Hasil Modifikasi Chiper Text*** |
| assets/music/Tabuh hujab.MP3 | VSB+Vndjp7zqOKFrIPJHIQA6l71yygBBYRkXCkIuuShdg4F5MgBg/Y7PAzfpJCePh3eHFehTC4HhDwHCXnwfl/L45XBSh6yNLblX35rdj/7ED/s6YUsSnlkACnBX35gfHFYtef5nL8kXFa/zOik sUN7ySTz0NHk4LUxpoPQJC13ZNageWDVYqZcvXbmnkH/M0PqNPobbdPppRMPQ0WewEcA7Ta9YJj=MOpir+1yjM7Gb8EOBc35PaWwIWib+4VpOdReXXUlBZhbWUErg=1yEuEmklbThVTyQPVZLJD+5fGg2t36W+HO/WIjKyTf7CcayEs4/k060TuSCyMP2o050Gneh |

Tabel 4. 6 Hasil Pengujian Avalanche Effect Data Ketiga

|  |  |  |
| --- | --- | --- |
| ***Plaint Text*** | ***Chiper Text*** | ***Avalanche Effect*** |
| assets/music/tabuh gora merdawa.MP3 | bI796Yu1+tewcMj/FdpoQVkwOUKJyqV//1Qm2+jU6BXHG0BllLjl2sQSkUwkgJYnMc5DrIj5uFeyRvIZGifDJtzhIAa/TY3Us2+Lc7LQfqBXqMVlYI51vh04rpKUPRCE8MmdkB1gksep56pIwHNtE+38RTq39AIV21Tpc74lvMLplQnL9PgKCn5rLCEG26B7hFBDalXAIZK89pnMgNCzxPzQgtthZOpgaElmpHhxXmGYXgGbFbhnrExZOUnJ4636zV+YlubBqF7U2MLPb8eEIVGdchUxW1JcZhu/kJ3PiqSXqdBBVFok+FcJ8rHCQJX2sU9GbEfqfMa+nLsADrvLUQ== | 195 Perubahan bit /  344 bit Chipertext x 100 % = 56,6 % |
| ***Modifikasi Plain Text*** | ***Hasil Modifikasi Chiper Text*** |
| assets/music/tabuh gora merdawe.MP3 | bI796Yu1+tewcMj/FdpoQVkwOUKJyqV//1Qm2+jU6BXHG0BllLjl2sQSkUwkgJYnMc5DrIj5uFeyRvIZGifDJtzhIAa/TY3Us2+Lc7LQfqBXqMVlYI51vh04rp eE38rcxEHKhMV38sQaXBtUOlPg+gb9xFfHX1rNC8CkPJAYEdPVh6QnlXJbILig=pLbAJ1qBqrulfXR7U1UId9EwZpESdGmHZlEv6G4n6xnYrzFVugv3L8pnR6CgOM45nZ8GGhoL/sp+Mt5tmZce2CkJI=hbz3sMATWDM9LBpNTBpF+KhFUJcCc+B2PKQn2ab7FmDEzqXkpxGBQhU7aU9LIqlk2PqVg |

Tabel 4. 7 Hasil Pengujian Avalanche Effect Data Keempat

|  |  |  |
| --- | --- | --- |
| ***Plaint Text*** | ***Chiper Text*** | ***Avalanche Effect*** |
| assets/music/Tabuh tari margapati.MP3 | SbJEz9Vw1Wdbh5nTEBWHVirLGWFvGomoOd35x40CwT9AcSKOuxzPe0kVQ3y3kIZzG2aULEJTboMtCKZzLzx5QLpi6ei6TKXUzaKfRLzdHU2Ddjv2TWpqonYoadFs2tda7+JcJE+9vpA6A6YCXP0Vd1IvlKmiyG+AI/Ia6bttrFLyqvTEKOSdfp2t3ibho8aQyDCRwjN1Y9dD4e0iSjgOP0AhqcE70J3NUMu7sV/s42tBc/l9Y5wXPJqmHvaq07yk1B5mNLPjz4G7Y2tRNHrUQEEz/m5gGgUZYh+OUQfgQspzS2KF6CFsj+tPQ1xHugo+Z4OXTMlUXjRUiz5uchJWaQ== | 187 Perubahan bit /  344 bit Chipertext x 100 % = 54,3 % |
| ***Modifikasi Plain Text*** | ***Hasil Modifikasi Chiper Text*** |
| assets/music/Tabuh tari margapato.MP3 | SbJEz9Vw1Wdbh5nTEBWHVirLGWFvGomoOd35x40CwT9AcSKOuxzPe0kVQ3y3kIZzG2aULEJTboMtCKZzLzx5QLpi6ei6TKXUzaKfRLzdHU2Ddjv2TWpqonYoadFs2tda7+JcJE+9vpA6A6YCXP0Vd1IvlKmiyG+AI/Ia6btt OzQ5UxNHycKTQOzrFaE1UDXstBge/oNij2u8Bu3qwsAoTQEtt7zZH+Fs92y4PJ3N9cmRhwp+4ZggfhG10CSYEpJQVYM5GOUKXszjR/7EPaHvPMqq4Wh15O/C0SmiFujyRf6aUjQSD7dUg0YUqd==72vNl4kXtc+Yirj2LP0hmlJb5LQg |

Tabel 4. 8 Hasil Pengujian Avalanche Effect Data Kelima

|  |  |  |
| --- | --- | --- |
| ***Plaint Text*** | ***Chiper Text*** | ***Avalanche Effect*** |
| assets/music/Tabuh beblatukan.MP3 | H9arb6P6Td56FinDkBqyER3tZPFxWCCmopKzNimXrMGH5Zvx7i7ZEDRs7LZ71RtSy30DEO56vzFcLkGE7uxiiEy7LP6/Wtft7zX0DIQ/uvlJ9kdR1/X2kPB5kcqhol5TipAi3I6brumypxByn5W3syRlRIx9RC43HuPX6DVSZhanYUwDqeSnx/X22WgoMDSxmQtTnisfV3Ge8n8jkfcaQZqZCuHpdhnEBo3Xsu3uL6Z7zxWGpIgVBXgTb3HX5dpxiyaN4Hu56x7BoSau4PzhmPCcBYNN1LXAe5rrXkmL8fDEyQc6vpiQDAxr7Fak91C3CbGtnZ+9YA69454eC01Bqg== | 191 Perubahan bit /  344 bit Chipertext x 100 % = 55,5 % |
| ***Modifikasi Plain Text*** | ***Hasil Modifikasi Chiper Text*** |
| assets/music/Tabuh beblatukam.MP3 | H9arb6P6Td56FinDkBqyER3tZPFxWCCmopKzNimXrMGH5Zvx7i7ZEDRs7LZ71RtSy30DEO56vzFcLkGE7uxiiEy7LP6/Wtft7zX0DIQ/uvlJ9kdR1/X2kPB5kcqhol5TipAi3I6brumypxByn5W3syRlRIx9RC43HuPX6D 3V3SEpYnomPmQLfxzeZPC0EX1g8yarB7Zpi=GDknVtIn8pxAa5x6qaGqnhC5ehSFgHy4GfDN333X4u8Z4agSsNrqxXxkvdA5BU61kiTY6uuSfoozXCCu9MBHjH2LnLwCnNZD7D9Q5WpcZuBcXdcb/Tx=gV+eiQW9m6YQsb2ea7th1AB4Xr |

Tabel 4. 9 Hasil Pengujian Avalanche Effect Data Keenam

|  |  |  |
| --- | --- | --- |
| ***Plaint Text*** | ***Chiper Text*** | ***Avalanche Effect*** |
| assets/music/tabuh baleganjur.MP3 | idoPFQfbJgqC0afEShZZVx3yEhgYGmzjSiN1vuxvweizLTwVAXe2n+fvs9TtBzCpgsTKMBHPA484RIvzvaXbi0il3AnjY/WBYVUlu6DFE+/Z7tU4en/G0r1CTAZNGyb3rsqWhLejRP0h1GdnqBJ3pGxkfuZNCx+iaa4Vop/it6kgYqtKFwsmt1EM74XA6kynf71dCaCJldvwkzh0X3cMO/2FJ8TgcIiuaqJmrhWkoidlvLNTE5QYW4+FimNu4gwTr5bBbScvCS2pbH3q7/lCB/JttmDh7jKmzzndbfa2grL+GxvXkr4/kToSJ28nTlZmvC2MWoHgYTgA7tBomLS03A== | 188 Perubahan bit /  344 bit Chipertext x 100 % = 54,6 % |
| ***Modifikasi Plain Text*** | ***Hasil Modifikasi Chiper Text*** |
| assets/music/tabuh baleganjut.MP3 | idoPFQfbJgqC0afEShZZVx3yEhgYGmzjSiN1vuxvweizLTwVAXe2n+fvs9TtBzCpgsTKMBHPA484RIvzvaXbi0il3AnjY/ JMlt3C2opN4vgzXSQfkACp=d+CwfguaBm+5xrNvt3TkCW4VJ8EchFJz/ihtnaJ=3wkS12OioqZt7/dTxcko8i/4i2o4qBhTaGJzmb7W16kXrGEbY/XCtMTTmmgvaLnymLZ32WADoxjSK7/0dmkF+g05uBmIvMfc24wK6rHalTNnuCHFpglbrbtAdYki7YSqlL7svg== |

Tabel 4. 10 Hasil Pengujian Avalanche Effect Data Keenam

|  |  |  |
| --- | --- | --- |
| ***Plaint Text*** | ***Chiper Text*** | ***Avalanche Effect*** |
| assets/music/baleganjur singakerta.MP3 | If6zKXxnUAHSj8kF1tsWmiN7Y2RITKMl5vXGO4iKCzThjN6Twq7xaV5SQHqpnrpJj7PtpuyI9gkWfjTzc8QubZ7tQ52KHlmDVn5rv0BgM83sQQ4CjzYsl3MwWj1mN9sNZ9G1CS3RZ450bXNsyWsubD88zaoBWckCB66HOCkM8SG8CtOlUWLpOP/BFLo2G6qHog0ZSBp2a2SNfFdeuVxP010jG8dkTy4qAJTN5tvnkfWEW1VFvPIK3Xstx6boR/rnbByiKY3LN80kfMFUSY/iCKmq70ul5ufEXefP7rJvh4833FtobuYEPxk1X0BinFFx2xz4NiE7hW3DCgpM08+7FQ== | 192 Perubahan bit /  344 bit Chipertext x 100 % = 55,8 % |
| ***Modifikasi Plain Text*** | ***Hasil Modifikasi Chiper Text*** |
| assets/music/tabuh baleganjut.MP3 | If6zKXxnUAHSj8kF1tsWmiN7Y2RITKMl5vXGO4iKCzThjN6Twq7xaV5SQHqpnrpJj7PtpuyI9gkWfjTzc8QubZ7tQ52KHlmDVn5rv0BgM83sQQ4CjzYsl3MwWj1mN9sNZ9G1CS3RZ450bXNO0uPSS0Ak20EtpS3K=RF286pyuGpFBW4x6XgW2HkEKolT+4aNBlsb0N3330CfXBJnHS788PCLC0=vyYuuhNh1j0bBFtxC1t8YoivKr8MUUQiNFIokLq3mW5o4D6XP1ni/ioqetxWyWdZ5VOF8zeWd7f/bsvFFL2kgOzBcME767uVMnrfGaPCD8FPqkGkf/bsxExBTY8Jf |

Tabel 4. 11 Hasil Pengujian Avalanche Effect Data Kedelapan

|  |  |  |
| --- | --- | --- |
| ***Plaint Text*** | ***Chiper Text*** | ***Avalanche Effect*** |
| assets/music/Gilak Penutup.MP3 | WS+crT1xfG1DKBcNOXUHaZ3DjaMF73ppWUMirwdmftXK4MYbsSuyizvvb8kEgIREYeRHlTRENvoayswtrfet7JceC2sWNaPkmXflaxCxdaYsWGKn7l49Rv4KMJV3HPg+P9eR/Emq8dJjlaHvsL21orrWxRsJn/cyLd/m0ahhkpLYAJ3CIQFcftrqERH9Wf4ZxuxDHilAA3xkXLL56UzMA7AwU2czBqW24bdy5hzg1H68VmRTFceSHguspY8Dd/Tri/qoOo5pFgev9OJmeC4Ww/bSEht+P3stqussnalwLfaje1v9ikE15cSMCohnMtbWgMgu/qyYvbxQ3wv6/aWYIQ== | 188 Perubahan bit /  344 bit Chipertext x 100 % = 54,6 % |
| ***Modifikasi Plain Text*** | ***Hasil Modifikasi Chiper Text*** |
| assets/music/Gilak Penutuv.MP3 | WS+crT1xfG1DKBcNOXUHaZ3DjaMF73ppWUMirwdmftXK4MYbsSuyizvvb8kEgIREYeRHlTRENvoayswtrfet7JceC2sWNaPkmXflaxCxdaYsWGKn7l49Rv4KMJV3HPg+P9eR/Emq8dJjlaHvsL21orrWxRsJn/cyLd/m0ahh TqMyaRLgvpWJEw/Hw4Y/gMWLWYuey5tgnUjiQ9StAno6fqv193HPu=5eO13mkWMFmYwkiq9sfQ7RdpCAErks2duVsJzvOzSx=ltCh3cebc4t4UWHA2Q1hcrFaAoiM5sfXDxwY5C8x6g6abzLq8EI3bpeox//blL/THIu+cADFvBhZqgS |

Tabel 4. 12 Hasil Pengujian Avalanche Effect Data Kesembilan

|  |  |  |
| --- | --- | --- |
| ***Plaint Text*** | ***Chiper Text*** | ***Avalanche Effect*** |
| assets/music/Lelambatan.MP3 | gBk2dS+b1LDlGYQaDAh2r2gWzixkFIHgFvA09Pln75TlnBxuNkWWc0F8wDlxG7cGM/IPg4s561nMhz4PvE75LXHStP+BKQ/2jnWwJrz6Hop1a46+MYn+f79RbTEzN7ft4hwTAmeXTcDkHfnYaD+TKzNZtiVkcLpr3VF7e+5bCGeCUr8fXK8C7sDT+ZZPQmXlHWdPia20s7hlVUTH9skim75jfykVfXs6H/bKPR98mkmE2RhAX4wToDqm5YhApP/+7GIpP54SKaDB1EkPD3Xjg81fYLTlkeL0mhCP+OFBHl/2hg0z01Ad6CI2RdTzL/uHwz8EGNlaxIN3WkZbbgjGZQ== | 179 Perubahan bit /  344 bit Chipertext x 100 % = 52 % |
| ***Modifikasi Plain Text*** | ***Hasil Modifikasi Chiper Text*** |
| assets/music/tabuh Lelambatab.MP3 | gBk2dS+b1LDlGYQaDAh2r2gWzixkFIHgFvA09Pln75TlnBxuNkWWc0F8wDlxG7cGM/IPg4s561nMhz4PvE75LXHStP+BKQ/2jnWwJrz6Hop1a46+MYn+f79RbTEzN7ft4hwTAmeXTcDkHfnYaD+TKzNZt80m9ZPXHpz903dfFfPi=srj8QRm5HBLzPgl6V3/lfm1kLkhRH/wmVyThbbKSXDZP/PKlpzmcGN+lXhg+7T+FfC71h2L4hQeEsDGWDbC8ljaws5I2KUkAx8WoEkb3eO/dkGTLHd5rZBD71U=Ve2iXYTCgViXjAT72IGC4aCY0ERIaPkZk7HAqmsu5+6P8pN0 |

Tabel 4. 13 Hasil Pengujian Avalanche Effect Data Kesepuluh

|  |  |  |
| --- | --- | --- |
| ***Plaint Text*** | ***Chiper Text*** | ***Avalanche Effect*** |
| assets/music/Gong suling bali.MP3 | u0HGrn4TCYOGxJ4iZMLeDI8qbJhGCnLfoz4RMEea7kr1fcsBYNegjd8nzmjomXaEcixvN3QN5sYT5HWCJkkE4w4ez4NfE0R+Ammk6DW+2wSJxM4x/ds+vxNhPBjE43VGgQSoKNkQ7WJRXiZ8HyVA+3L89Jh2akPfnXf/AZhcZRxE4/3YarLcP/8F1O/qKMd9x+MRR8BUWrWwGfIYlLB+5S3zuL5KzfZJTIzIsWeahTFNwW2WC79Tax+KVLLehiXCRS7sclllv7VtOYh/HLLplBh95xXNqfiJU+pIHS4js0KETaDax9o12Esjy3+vwff0DgNFV2nGx1jgOmbs107Oiw== | 185 Perubahan bit /  344 bit Chipertext x 100 % = 53,7 % |
| ***Modifikasi Plain Text*** | ***Hasil Modifikasi Chiper Text*** |
| assets/music/Gong suling balo.MP3 | u0HGrn4TCYOGxJ4iZMLeDI8qbJhGCnLfoz4RMEea7kr1fcsBYNegjd8nzmjomXaEcixvN3QN5sYT5HWCJkkE4w4ez4NfE0R+Ammk6DW+2wSJxM4x/ds+vxNhPBjE43VGgQSoKNkQ7WJRXiZ8HyVA+3L89Jh2akPfnXf/AZhcZRxE4/3YarLcP/IxHqaajB0KumdhRsTDUThN2x1Cfxl1xW9MwYfTsFMWzW=tXOIL89L7V/qhceTY/RLarLS2fHp5lCBIO4VKwpliO2SJb3igzczWBDPGWs+5KR5+7nv+efE1G1jOh0w7NL=s7a8EXfji+/9J0+sLFIoVygxSlZ3LFlNK9wUv |

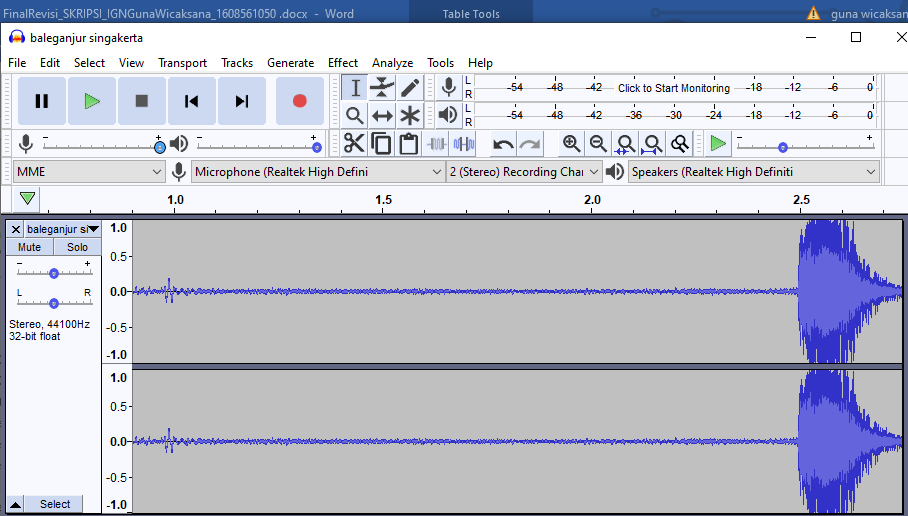
Berdasarkan hasil pengujian *avalanche effect* yang ditunjukan pada skenario pengujian kesepuluh data *chipertext* terhadap hasil modifikasi *chipertext* data pada sistem diperoleh rata-rata nilai dari *avalanche effect* nya adalah sebesar 54,2 %, sehingga dapat disimpulkan berdasarkan nilai *avalanche effect* yang diperoleh*,* algoritma RSA yang diimplementasikan pada sistem ini sangat baik.

### Pengujian Data Audio MP3

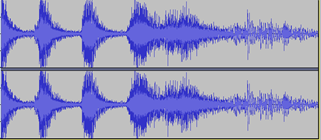
Pada pengujian data audio MP3 bertujuan untuk memastikan bahwa proses enkripsi dan dekripsi telah dapat diimplementasikan pada *file* MP3 dan bekerja dengan baik, dengan melakukan perbandingan gelombang suara sebelum dan sesudah enkripsi dilakukan. Dari hasil pengujian ini telah terlihat bahwa ada perbedaan gelombang suara sebelum dan setelah dilakukan proses enkripsi. Hal ini menunjukan bahwa data asli telah mengalami perubahan setelah proses enkripsi dan tidak bisa diakses. Selain itu dilakukan juga pembandingan terhadap ukuran *file* yang telah terenkripsi dengan file yang telah terdekripsi yang telah menunjukan bahwa data telah mengalami proses enkripsi dan dekripsi.

Tabel 4. 14 Tabel Pengujian Gelombang Suara Data MP3

|  |  |  |  |
| --- | --- | --- | --- |
| **Perbandingan Gelombang Suara File MP3** | | | |
| **No.** | **Nama File** | **Sebelum Terenkripsi *(Plaintext File)*** | **Setelah Terenkripsi *(Chipertext File)*** |
| 1. | Tabuh eled semar pagulingan.MP3 |  |  |
| 2. | Tabuh hujan.MP3 |  |  |
| 3. | Tabuh gora merdawa.MP3 |  |  |
| 4. | Tabuh tari margapati.MP3 |  |  |
| 5. | Tabuh beblatukan.MP3 |  |  |
| 6. | tabuh baleganjur.MP3 |  |  |
| 7. | baleganjur singakerta.MP3 |  |  |
| 8. | Gilak Penutup.MP3 |  |  |
| 9. | Lelambatan.MP3 |  |  |
| 10. | Gong suling bali.MP3 |  |  |



Gambar 4. 21 Gelombang Suara Data Audio Asli

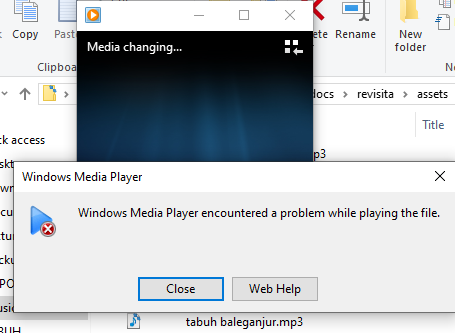
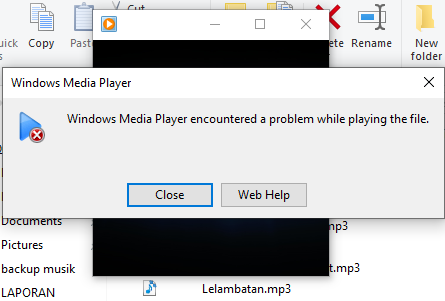


Gambar 4. 22 Gelombang Suara Data Audio Terenkripsi

Berdasarkan pada Gambar 4.16 yang menunjukan gelombang suara pada data MP3 yang belum terenkripsi dan Gambar 4.17 yang menunjukan gelombang suara pada data audio yang telah terenkripsi. Terlihat bahwa adanya perbedaan gelombang suara pada kedua data diatas.

Tabel 4. 15 Tabel Perbandingan Ukuran Data MP3

|  |  |  |  |
| --- | --- | --- | --- |
| **Perbandingan Ukuran Data File MP3** | | | |
| **No.** | **Nama Data** | **Ukuran File Terenkripsi** | **Ukuran File Terdekripsi** |
| 1. | Tabuh Eled Semar Pagulingan | 6,709,711 bytes | 6,678,455 bytes |
| 2. | Tabuh Hujan | 7,193,081 bytes | 7,161,825 bytes |
| 3. | Tabuh Gora Merdawa | 6,766,135 bytes | 6,734,879 bytes |
| 4. | Tabuh Tari Margapati | 10,615,540 bytes | 10,584,284 bytes |
| 5. | Tabuh Beblatukan | 5,612,568 bytes | 5,581,312 bytes |
| 6. | Tabuh Baleganjur | 7,860,771 bytes | 7,829,515 bytes |
| 7. | Baleganjur Singakerta | 11,153,453 bytes | 11,122,197 bytes |
| 8. | Gilak Penutup | 8,151,119 bytes | 8,119,863 bytes |
| 9. | Lelambatan | 6,159,259 bytes | 6,128,003 bytes |
| 10. | Gong Suling bali | 2,294,181 bytes | 2,262,925 bytes |



Gambar 4. 23 File MP3 Terenkripsi Tidak Dapat Diakses

Berdasarkan hasil pengujian ini telah terlihat pada Tabel 4.14 dan Tabel 4.15 diatas bahwa ukuran *file* yang telah mengalami proses enkripsi lebih besar dibandingkan dengan *file* setelah melalui proses dekripsi serta terdapat perbedaan frekuensi gelombang suara sebelum dan setelah dilakukan proses enkripsi. Hal ini menunjukan bahwa data asli telah mengalami perubahan setelah proses enkripsi. Pada Gambar 4.18 diatas menujukan file MP3 yang telah diunggah kedalam sistem, dicoba diakses melalui direktori folder, dimana file yang telah dienkripsi disimpan dan menunjukan ternyata file tersebut tidak dapat diakses karena karakter pada file MP3 tersebut telah dienkripsi.

# BAB V

# KESIMPULAN DAN SARAN

Pada bab ini dibahas mengenai kesimpulan dari semua proses yang telah dilakukan dan saran yang dapat diberikan untuk pengembangan penelitian terkait agar lebih baik di masa mendatang.

## Kesimpulan

Berdasarkan semua proses yang telah dilaksanakan, ditarik kesimpulan bahwa algoritma RSA telah berhasil diterapkan pada sistem untuk keamanan data musik pada sistem untuk mencegah data diakses dan digunakan oleh pihak yang tidak berhak melalui proses enkripsi dan dekripsi data pada sistem layanan musik yang telah berhasil dibangun dan sudah berfungsi dengan baik sesuai dengan pengujian fungsionalitas menggunakan pengujian *blackbox*, serta berdasarkan hasil pengujian data audio MP3 menunjukan bahwa algoritma RSA dapat diterapkan pada file MP3 pada sistem layanan musik berbasis *web* serta berdasarkan hasil pengujian *avalanche effect* yang pada sistem diperoleh rata-rata nilai dari avalanche effect nya adalah sebesar 54,2%, sehingga dapat disimpulkan algoritma RSA yang diimplementasikan pada sistem ini sangat baik.

## Saran

1. Untuk algoritma kriptografi yang digunakan pada sistem ini yakni algoritma RSA dapat dikombinasikan dengan algoritma kriptografi lainnya untuk meningkatkan tingkat keamanan data pada sistem.
2. Pada proses pengujian sebaiknya skema pengujian dan sampel data diperbanyak untuk meningkatkan akurasi pengujian *avalanche effect* terhadap algoritma kriptografi RSA pada sistem.

# DAFTAR PUSTAKA

Ariyus, D. (2008). *Pengantar Ilmu Kriptografi : teori, analisis dan implementasi.* Yogyakarta: ANDI.

Awang K, H., Yusika R, A., & Ansharie, A. (2017). ENKRIPSI DATA AUDIO MENGGUNAKAN METODE KRIPTOGRAFI RSA.

*Code Politan*. (2019). Retrieved from Mengenal RESTful Web Services: https://www.codepolitan.com/mengenal-restful-web-services

Damanik, I. S., & Hartama, D. (n.d.). PENERAPAN ALGORITMA RSA PADA APLIKASI LAPORAN NILAI AKHIR DOSEN.

Diarse, N. N., & Bendi, J. K. (2016, Desember). PENERAPAN ALGORITMA RSA PADA SISTEM KRIPTOGRAFI FILE AUDIO MP3. *Jurnal HOAQ-Teknologi Informasi, 7*.

Firdaus, J., Marwati, R., & Gozali, S. M. (2018). Penyandian Pesan Menggunakan Algoritma RSA yang Ditingkatkan Dan Algoritma Elgamal. *EuraMatika*.

Goshwe, N. Y. (2013, July 7). Data Encryption and Decryption Using RSA Algorithm in a Network Environment. *IJCSNS International Journal of Computer Science and Network Security, , Volume 13*.

Gunawan, I. (2018). 124 KOMBINASI ALGORITMA CAESAR CIPHER DAN ALGORITMA RSA UNTUK PENGAMANAN FILE DOKUMEN DAN PESAN TEKS.

Hanson, W. (2000). *Pemasaran Internet.* Jakarta: Penerbit Salemba Empat.

Hardjono, D. (2006). *Seri Panduan Lengkap Menguasai Pemrograman Web dengan PHP 5.* Yogyakarta.

Listiyono, H. (2009). Implementasi Algoritma Kunci Piblic Pada Algoritma RSA. *Din. Inform., vol. Vol.1, no. No.2*.

McLeod, R., & Schell, G. P. (2004). *Management Information System.* Prentice Hall.

*Mengulik Data Suku di Indonesia*. (2015, 11 18). Retrieved from bps.go.id: https://www.bps.go.id/news/2015/11/18/127/mengulik-data-suku-di-indonesia.html

Mollin, R. (2007). *An Introduction to Cryptography.* Florida: Chapman & Hall/CRC.

Munir, R. (2006). *Kriptografi.* Bandung: Informatika.

Pressman, R. S. (2015). *Software engineering : a practitioner's approach.*

Ridwan, M., Arifin, Z., & Yulianto. (2016, September 2). RANCANG BANGUN E-VOTING DENGAN MENGGUNAKAN KEAMANAN ALGORITMA RIVEST SHAMIR ADLEMAN (RSA) BERBASIS WEB (STUDI KASUS : PEMILIHAN KETUA BEM FMIPA). *Jurnal Informatika Mulawarman, 11*.

Rohmah, M. (2017). IMPLEMENTASI TEKNOLOGI WEB SERVICE PADA SISTEM INFORMASI ADMINISTRASI KEPENDUDUKAN DENGAN WEB SERVICE.

Rosnawan, D. (2011). APLIKASI ALGORITMA RSA UNTUK KEAMANAN DATA PADA SISTEM INFORMASI BERBASISWEB.

Schneier, B. (1996). *Applied Cryptography,.* Unites Stated of America: John Wiley & Sons, Inc.

Sugiartha, I. G. (2015, March). Bentuk dan Konsep Estetik Musik Tradisional Bali. *Panggung , 25*.

Trihatmaja, A., Wibisono, W., & Pratomo, B. A. (2013). Penerapan Steganografi Adaptive Partial Matching Menggunakan Triple M-Sequences pada Streaming Audio. *JURNAL TEKNIK POMITS Vol. 2, No. 1*, 1-2.

Tri Susilo, A. (2018). Penerapan Algoritma Asimetris RSA Untuk Keamanan Data Pada Aplikasi Penjualan CV. Sinergi Computer Lubuklinggau Berbasis Web. *Jurnal SIMETRIS, Vol. 9 No. 2 November 2018*.

Tropiana Ipan, I., Abdillah, G., & Ilyan , R. (2019). PENGAMANAN DATA USER PADA DATABASE MENGGUNAKAN KRIPTOGRAFI RIVEST SHAMIR ADLEMAN DAN CIPHER BLOCK CHAINING. *eminar Nasional Teknologi Informasi dan Komunikasi 2019 (SENTIKA 2019)*.

*What is HTTP Streaming*. (2019). Retrieved 10 14, 2019, from pubnub.com: https://www.pubnub.com/learn/glossary/what-is-http-streaming/

Wibowo, G. T., M., R. R., & Saputra, R. E. (2015, Agustus). ANALISIS DAN IMPLEMENTASI ENKRIPSI DAN DEKRIPSI GANDA KOMBINASI ALGORITMA BLOWFISH DAN ALGORITMA TRIPLE DES UNTUK SMS PADA SMARTPHONE ANDROID. *e-Proceeding of Engineering, 2*.

Wicaksono, P. A. (2008). Enkripsi Menggunakan Algoritma RSA. *Jurnal Program Studi Teknik Informatika, Sekolah Teknik Elektro dan Informatika*.

**LAMPIRAN A**

**DESKRIPSI USE-CASE**

Tabel A. 1 UC-01 Mencari Musik

|  |  |  |
| --- | --- | --- |
| UC-01 Mencari Musik | | |
| Use Case Name | Mencari Musik | |
| Purpose | Untuk melakukan pencarian terhadap musik yang terdapat pada sistem. | |
| Overview | Use case dimulai dari pengguna memilih menu Cari pada halaman beranda sistem, kemudian pengguna diarahkan memasukan kata kunci. | |
| Actors | Pengguna Aplikasi | |
| Pre-Condition | * Komputer pengguna harus tersambung ke internet untuk mengakses sistem layanan musik. * Komputer pengguna harus memiliki web browser untuk mengakses sistem layanan musik. * Komputer pengguna harus beroperasi dengan baik. * Pengguna mengklik menu “Cari” | |
| Post-Condition | * Sistem layanan musik dapat diakses * Pengguna telah berhasil masuk dan melakukan pencarian musik | |
| Typical Course of Event | Actor Actions | System Actions |
| 1. Pengguna masuk ke halaman utama dan mengakses menu cari | 1. Sistem akan menampilkan hasil pencarian yang diinputkan *user.* |

|  |  |
| --- | --- |
| Alternative Flow of Events | * Koneksi internet gagal, makan halaman utama website tidak bisa diakses, dan tidak dapat melakukan pencarian musik |
| Exceptional Flow of Events | * Pengguna secara tiba-tiba keluar atau aplikasi tidak bisa diakses karena listrik mati |

Tabel A. 2 UC-02 Menelusuri Musik

|  |  |  |
| --- | --- | --- |
| UC-02 Menelusuri Musik | | |
| Use Case Name | Menelusuri Musik | |
| Purpose | Untuk melakukan penelusuran terhadap musik yang terdapat pada sistem. | |
| Overview | Use case dimulai dari pengguna memilih menu Telusuri pada halaman beranda sistem, kemudian sistem akan menampilkan musik yang ada pada sistem. | |
| Actors | Pengguna Aplikasi | |
| Pre-Condition | * Komputer pengguna harus tersambung ke internet untuk mengakses sistem layanan musik. * Komputer pengguna harus memiliki web browser untuk mengakses sistem layanan musik. * Komputer pengguna harus beroperasi dengan baik. * Pengguna mengklik menu “Telusuri” | |
| Post-Condition | * Sistem layanan musik dapat diakses * Pengguna telah berhasil masuk dan melakukan penelusuran musik | |
| Typical Course of Event | Actor Actions | System Actions |
| 1. Pengguna masuk ke halaman utama dan mengakses menu telusuri | 1. Sistem akan menampilkan hasil musik yang terdapat atau disediakan pada sistem. |
| Alternative Flow of Events | * Koneksi internet gagal, makan halaman utama website tidak bisa diakses, dan tidak dapat melakukan penelusuran musik | |
| Exceptional Flow of Events | * Pengguna secara tiba-tiba keluar atau aplikasi tidak bisa diakses karena listrik mati | |

Tabel A. 3 UC-03 Mengelola Daftar Putar

|  |  |  |
| --- | --- | --- |
| UC-03 Mengelola Daftar Putar | | |
| Use Case Name | Mengelola Daftar Putar | |
| Purpose | Untuk membuat dan menghapus daftar putar user. | |
| Overview | Use case dimulai dari pengguna memilih menu Musik Saya pada halaman beranda sistem, kemudian sistem akan menampilkan menu membuat daftar putar baru atau menghapus daftar putar yang sudah ada. | |
| Actors | Pengguna Aplikasi | |
| Pre-Condition | * Komputer pengguna harus tersambung ke internet untuk mengakses sistem layanan musik. * Komputer pengguna harus memiliki web browser untuk mengakses sistem layanan musik. * Komputer pengguna harus beroperasi dengan baik. | |
| Post-Condition | * Sistem layanan musik dapat diakses * Pengguna telah berhasil masuk dan dapat membuat atau, menghapus daftar putar yang ada. * Pengguna mengklik menu “Musik Saya” | |
| Typical Course of Event | Actor Actions | System Actions |
| 1. Pengguna masuk ke halaman utama dan mengakses menu Musik Saya, lalu memilih untuk membuat atau menghapus daftar putar | 1. Sistem akan mengarahkan untuk membuat daftar putar baru atau menghapus daftar putar yang sudah ada. |
| Alternative Flow of Events | * Koneksi internet gagal, makan halaman utama website tidak bisa diakses, dan tidak dapat melakukan membuat atau menghapus daftar putar. | |
| Exceptional Flow of Events | * Pengguna secara tiba-tiba keluar atau aplikasi tidak bisa diakses karena listrik mati * Pengguna menutup *web browser* sebelum langkah-langkah selesai dilakukan. | |

Tabel A. 4 UC-04 Mengelola Akun

|  |  |  |
| --- | --- | --- |
| UC-04 Mengelola Akun | | |
| Use Case Name | Mengelola Akun | |
| Purpose | Untuk mengganti email/password atau mengeluarkan akses akun. | |
| Overview | Use case dimulai dari pengguna memilih menu *user* (menampilkan nama user) pada halaman beranda sistem, kemudian sistem akan menampilkan menu mengganti email/password atau keluar dari akun tersebut. | |
| Actors | Pengguna Aplikasi | |
| Pre-Condition | * Komputer pengguna harus tersambung ke internet untuk mengakses sistem layanan musik. * Komputer pengguna harus memiliki web browser untuk mengakses sistem layanan musik. * Komputer pengguna harus beroperasi dengan baik. * Pengguna mengklik menu “Akun” | |
| Post-Condition | * Sistem layanan musik dapat diakses * Pengguna telah berhasil masuk dan dapat mengganti email/password atau mengeluarkan akses akun. | |
| Typical Course of Event | Actor Actions | System Actions |
| 1. Pengguna masuk ke halaman utama dan mengakses menu user (menampilakan nama user) dan memilih mengganti email/password atau mengeluarkan akses akun. | 1. Sistem akan mengarahkan untuk mengganti email/password atau mengeluarkan akses akun. |
| Alternative Flow of Events | * Koneksi internet gagal, makan halaman utama website tidak bisa diakses, dan tidak dapat melakukan membuat atau menghapus daftar putar. | |
| Exceptional Flow of Events | * Pengguna secara tiba-tiba keluar atau aplikasi tidak bisa diakses karena listrik mati. * Pengguna menutup *web browser* sebelum langkah-langkah selesai dilakukan. | |

Tabel A. 5 UC-05 Mengunggah Data Musik

|  |  |  |
| --- | --- | --- |
| UC-05 Mengunggah Data Musik | | |
| Use Case Name | Mengunggah Data Musik | |
| Purpose | Untuk mengunggah data musik ke dalam sistem. | |
| Overview | Use case dimulai dari pengguna memilih menu Unggah pada halaman beranda sistem, kemudian menampilkan form-form yang perlu dimasukan sebagai data musik serta memilih akses publik atau *private* pada musik tersebut.. | |
| Actors | Pengguna Aplikasi | |
| Pre-Condition | * Komputer pengguna harus tersambung ke internet untuk mengakses sistem layanan musik. * Komputer pengguna harus memiliki web browser untuk mengakses sistem layanan musik. * Komputer pengguna harus beroperasi dengan baik. * Pengguna sudah memiliki file audio berfomat MP3. * Pengguna mengklik menu “Unggah” | |
| Post-Condition | * Sistem layanan musik dapat diakses * Pengguna telah mengunggah data musik ke dalam sistem dan sistem menampilkan musik. | |
| Typical Course of Event | Actor Actions | System Actions |
| 1. Pengguna masuk ke halaman utama dan mengakses menu Unggah kemudian memasukan data-data pada form yang disediakan dan menentukan akses publik atau *private* pada musik tersebut. | 1. Sistem akan mengarahkan untuk memasukan data pada form dan menggungah file audio. |
| Alternative Flow of Events | * Koneksi internet gagal, makan halaman utama website tidak bisa diakses, dan tidak dapat melakukan membuat atau menghapus daftar putar. * File yang diunggah bukan merupakan file audio berformat MP3 maka musik tidak dapat diakses. | |
| Exceptional Flow of Events | * Pengguna secara tiba-tiba keluar atau aplikasi tidak bisa diakses karena listrik mati. * Pengguna menutup *web browser* sebelum langkah-langkah selesai dilakukan. | |

**LAMPIRAN B**

**SOURCE CODE PROGRAM**

<?php

function bikin\_key(){

$pasanganKey = openssl\_pkey\_new(array(

'private\_key\_bits' => 2048, // Ukuran Key.

'private\_key\_type' => OPENSSL\_KEYTYPE\_RSA,

));

openssl\_pkey\_export($pasanganKey,$privateKey);//Membuat Private Key

//echo $privateKey . "<br /><br />";

$arrayHasilRSA = openssl\_pkey\_get\_details($pasanganKey);//Membuat Public Key

$publicKey = $arrayHasilRSA['key'];//Mengambil public key

$kunci['privat']=base64\_encode($privateKey);

$kunci['publik']=base64\_encode($publicKey);

//Menghapus dari memory

openssl\_free\_key($pasanganKey);

return $kunci;

}

//$kunci=bikin\_key();

|  |
| --- |
| function encrypt($data, $kunciPublik)  {      if(openssl\_public\_encrypt($data, $enkripsi, $kunciPublik)){ //$enkripsi adalah variabel yang menyimpan hasil  return $enkripsi;  }else  return "Data terlalu besar";  }        function decrypt($data, $kunciPrivat)  {      openssl\_private\_decrypt($data, $dekripsi,$kunciPrivat);//$dekripsi adalah variabel yang menyimpan hasil  return $dekripsi;    }    function ssl\_encrypt($source,$key){  //Assumes 2048 bit key and encrypts in chunks.  $maxlength=200;  $pangjangSumber = strlen($source);  $output='';  //$input= substr($source,0,$maxlength);  //$ok= openssl\_public\_encrypt($input,$encrypted,$key);  $i=0;  //while($i<10){  while($source){  $input= substr($source,0,$maxlength);  $source=substr($source,$maxlength);    $ok= openssl\_public\_encrypt($input,$encrypted,$key);      $output.=$encrypted;  if($i==100)  break;  $i++;  }    //}  $sisa = substr($source,20000, $pangjangSumber-20000);  $output.=$sisa;  return $output;  }    function ssl\_decrypt($source,$key){  // The raw PHP decryption functions appear to work  // on 256 Byte chunks. So this decrypts long text  // encrypted with ssl\_encrypt().  $maxlength=256;  $pangjangSumber = strlen($source);  $output='';  $i=0;  while($source){  $input= substr($source,0,$maxlength);  $source=substr($source,$maxlength);  $ok= openssl\_private\_decrypt($input,$out,$key);      $output.=$out;  if($i==100)  break;  $i++;  }  $sisa = substr($source,25600, $pangjangSumber-25600);  $output.=$sisa;  return $output;  }    ?> |

|  |
| --- |
| <?php  set\_time\_limit(3600);  include "includes/enkripsiRSA.php";  include "Model.php";  $albums = mysqli\_query($con, "SELECT \* FROM albums WHERE 1");  $genres = mysqli\_query($con, "SELECT \* FROM genres WHERE 1");  $artists = mysqli\_query($con, "SELECT \* FROM artists WHERE 1");  if (!empty($\_POST) && $\_POST["action"] == "save") {  // var\_dump($\_POST);  // var\_dump($\_SESSION['userLoggedIn']);  $userLoggedIn = new User($con, $\_SESSION['userLoggedIn']);  $user = $userLoggedIn->getObject();  // var\_dump($\_POST);  // var\_dump($\_FILES);  $is\_public = !empty($\_POST["is\_public"]) ? $\_POST["is\_public"] == "on" ? : 1 : 0;  $title = $\_POST["title"];  $artist = $\_POST["artist"];  $album = $\_POST["album"];  $genre = $\_POST["genre"];  // die;  $file = $\_FILES["file"];  $path = "assets/music/" .$file["name"];  //$path = "assets/music/" . 'MR\_Man\_Ana';  // $upload = move\_uploaded\_file($file["tmp\_name"], $path);    if ($is\_public) {  $kunci = bikin\_key();  $privatekey = base64\_decode($kunci["privat"]);  $publickey = base64\_decode($kunci["publik"]);  }else{  $privatekey = base64\_decode($user->privatekey);  $publickey = base64\_decode($user->publickey);  }  //Get file content  $file = file\_get\_contents($file["tmp\_name"]);  //Encrypt file  $Encrypt = ssl\_encrypt($file, $publickey);  //Create new file  $fileE = fopen($path, 'w') or die("can't open file");  //Put crypted content  fwrite($fileE, $Encrypt);  //Close file  fclose($fileE);      // $ciphertext = base64\_encode($rsa->encrypt($path));  $ciphertext = base64\_encode(encrypt($path, $publickey));  // if ($upload) {  $model = new Model($con);  // insert songs  $model->insert($title, $album, $artist, $genre, $ciphertext, base64\_encode($privatekey), base64\_encode($publickey), $is\_public, $user->id);  // }  // else{  // }  die;  }  ?> |

|  |
| --- |
| <?php  set\_time\_limit(3600);  include("../../config.php");  include(\_\_DIR\_\_."/../../classes/User.php");  include(\_\_DIR\_\_."/../../enkripsiRSA.php");  if(isset($\_REQUEST['songId'])) {  $songId = $\_REQUEST['songId'];  $dataUser = new User($con, $\_SESSION['userLoggedIn']);  $user = $dataUser->getObject();  // var\_dump($user);die;  $query = mysqli\_query($con, "SELECT \* FROM songs WHERE id='$songId'");  $result = mysqli\_fetch\_object($query);  if ($result->is\_public) {  $privatekey = $result->privatekey;  $publickey = $result->publickey;  }  else{  $privatekey = $user->privatekey;  $publickey = $user->publickey;  }  // var\_dump($privatekey);  // die;  // $rsa\_decrypt = new \phpseclib\Crypt\RSA();  // $rsa\_decrypt->loadKey(base64\_decode($privatekey));  $ciphertext = base64\_decode($result->path);    $path = ssl\_decrypt($ciphertext, base64\_decode($privatekey) );      $posTitik = strrpos($path, '.');  $pathAwal = substr($path,0,$posTitik);  $pathDecrypt = '../../../'.$pathAwal."\_decrypt.MP3";  //$result->path = $pathDecrypt;  $result->path = '../../../revisita/'.$pathAwal."\_decrypt.MP3";  if(!file\_exists($pathDecrypt)){  $file = file\_get\_contents('../../../'.$path);  //Encrypt file  $decrypt = ssl\_decrypt($file, base64\_decode($privatekey));  //Create new file    $fileTujuan = $pathDecrypt;  $fileE = fopen($fileTujuan , 'w') or die("can't open file");  //Put crypted content  fwrite($fileE, $decrypt);  //Close file  fclose($fileE);  }  // die;  echo json\_encode($result);  }  ?> |

|  |
| --- |
| <?php  // include("includes/includedFiles.php");  include("includes/header.php");  // include("includes/classes/Artist.php");  // include("includes/classes/Album.php");  include("src/uploadController.php");  ?>  <div class="userDetails">  <form method="POST" enctype="multipart/form-data">  <div class="container">  <h2>Unggah Musik</h2>  <input type="file" name="file" placeholder="" required="true">  <input type="checkbox" name="is\_public" id="is\_public" placeholder="Publik">  <label for="is\_public">  Publik  </label>  <input type="text" name="title" placeholder="Judul Musik">  <select class="js-example-basic-single" name="album" required>  <option disabled selected value="">Asal</option>  <?php  if (!empty($albums)) {  while($data = mysqli\_fetch\_array($albums)) { ?>  <option value="<?= $data["id"]?>"><?= $data["title"]?></option>  <?php }  }  ?>  </select>  <select class="js-example-basic-single" name="genre" required>  <option disabled selected value="">Genre</option>  <?php  if (!empty($genres)) {  while($data = mysqli\_fetch\_array($genres)) { ?>  <option value="<?= $data["id"]?>"><?= $data["name"]?></option>  <?php }  }  ?>  </select>  <select class="js-example-basic-single" name="artist" required>  <option disabled selected value="">Artist</option>  <?php  if (!empty($artists)) {  while($data = mysqli\_fetch\_array($artists)) { ?>  <option value="<?= $data["id"]?>"><?= $data["name"]?></option>  <?php }  }  ?>  </select>  <span class="message"></span>  <button type="submit" class="button" name="action" value="save">Simpan</button>  </div>  </form>  </div>  <script type="text/javascript">  $(document).ready(function() {  $('.js-example-basic-single').select2();  });  </script>  <?php  include("includes/footer.php");  ?> |

|  |
| --- |
| <?php  include "Model.php";  $albums = mysqli\_query($con, "SELECT \* FROM albums WHERE 1");  $genres = mysqli\_query($con, "SELECT \* FROM genres WHERE 1");  $artists = mysqli\_query($con, "SELECT \* FROM artists WHERE 1");  if (!empty($\_POST) && $\_POST["action"] == "save") {  // var\_dump($\_POST);  // var\_dump($\_SESSION['userLoggedIn']);  $userLoggedIn = new User($con, $\_SESSION['userLoggedIn']);  $user = $userLoggedIn->getObject();  // var\_dump($\_POST);  // var\_dump($\_FILES);  $is\_public = !empty($\_POST["is\_public"]) ? $\_POST["is\_public"] == "on" ? : 1 : 0;  $title = $\_POST["title"];  $artist = $\_POST["artist"];  $album = $\_POST["album"];  $genre = $\_POST["genre"];  // die;  $file = $\_FILES["file"];  $path = "assets/music/" .$file["name"];  $upload = move\_uploaded\_file($file["tmp\_name"], $path);  $rsa = new \phpseclib\Crypt\RSA();  if ($is\_public) {  $keys = $rsa->createKey();  $privatekey = $keys["privatekey"];  $publickey = $keys["publickey"];  }  else{  $privatekey = base64\_decode($user->privatekey);  $publickey = base64\_decode($user->publickey);  }  // echo base64\_encode($privatekey)."<br><br>";  // echo base64\_encode($publickey);  $rsa->loadKey($privatekey);  $rsa->loadKey($publickey);  $ciphertext = base64\_encode($rsa->encrypt($path));  if ($upload) {  $model = new Model($con);  // insert songs  $model->insert($title, $album, $artist, $genre, $ciphertext, base64\_encode($privatekey), base64\_encode($publickey), $is\_public, $user->id);  }  else{  }  die;  }  ?> |