# DESAIN FREAMWORK OWASP UNTUK MENGIDENTIFIKASI CELAH KEAMANAN PADA AUDIO MENGGUNAKAN ALGORITMA RSA

**AMELIA[1)], SYAKILA AINI[2)], NIKI FAHDILA JAYA[3)], NAZWA KHAIRUNNISA[4)], ACHMAD FAUZI[5)]**

[1,2,3,4,5)]STMIK Kaputama
*Jalan Veteran No. 4A-9A, Binjai Selatan, Kota Binjai, Sumatera Utara*
*Email : nikifahdila0@gmail.com*

***ABSTRACT***

*The development of multimedia technology, particularly digital audio, has increased the need for data security systems capable of protecting information from cyber threats. Audio is often used as a medium for communication, storing sensitive information, and voice authentication, making it vulnerable to attacks such as eavesdropping, manipulation, and data theft. This study aims to design a security framework based on OWASP (Open Web Application Security Project) to identify security vulnerabilities in audio processing systems by implementing the RSA cryptography algorithm. The proposed framework integrates OWASP principles in the risk analysis process, vulnerability identification, as well as the application of audio encryption and decryption using RSA. The research results show that implementing the RSA algorithm can enhance the confidentiality and integrity of audio data, while the OWASP framework helps identify and systematically mitigate potential security gaps. Thus, this framework design can serve as a reference in the development of a more reliable and structured audio security system.*

***Keywords: Information Security, OWASP, Digital Audio, Cryptography, RSA***

## 1. PENDAHULUAN

Keamanan informasi merupakan aspek krusial dalam sistem informasi modern. Tidak hanya data teks dan gambar, data audio juga menjadi target serangan siber karena sering mengandung informasi sensitif, seperti percakapan rahasia, data biometrik suara, dan rekaman komunikasi penting. Tanpa mekanisme keamanan yang memadai, data audio dapat dengan mudah disadap, dimodifikasi, atau disalahgunakan oleh pihak yang tidak berwenang.

OWASP (Open Web Application Security Project) menyediakan panduan dan framework untuk mengidentifikasi serta mengatasi celah keamanan pada sistem aplikasi. Meskipun OWASP umumnya diterapkan pada aplikasi web, prinsip-prinsipnya dapat diadaptasi untuk sistem pengolahan audio. Selain itu, algoritma RSA sebagai salah satu algoritma kriptografi kunci publik memiliki keunggulan dalam menjaga kerahasiaan dan keamanan data.

Perkembangan pesat di bidang teknologi informasi dan komunikasi telah memberikan dampak besar pada cara manusia melakukan penyimpanan, pengelolaan, dan distribusi data digital. Salah satu jenis data digital yang semakin banyak diterapkan adalah audio digital, baik itu berupa rekaman suara, interaksi daring, media hiburan, maupun sistem autentikasi berbasis suara. Dengan bertambahnya penggunaan audio digital, risiko keamanan data juga meningkat, terutama dalam hal kerahasiaan, integritas, serta perlindungan terhadap akses yang tidak sah.

Ancaman terhadap keamanan, seperti pendengapan, perubahan data, dan pencurian informasi, menjadi masalah serius yang memerlukan penanganan yang sistematis. Oleh karena itu, diperlukan pendekatan keamanan yang terstruktur dan standar untuk mendeteksi dan mengurangi celah keamanan dalam sistem pengolahan audio. Framework OWASP (Open Web Application Security Project) dan algoritma kriptografi RSA adalah dua pendekatan yang dapat digabungkan untuk meningkatkan keamanan data audio. Dengan merancang framework keamanan yang tepat, diharapkan bahwa sistem audio digital dapat terlindungi dengan baik dari berbagai ancaman siber.

## 2. METODOLOGI PENELITIAN

### 2.1 Keamanan Informasi

Keamanan informasi bertujuan melindungi data dari berbagai ancaman dengan memastikan tiga aspek pokok, yaitu kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan (availability).

### 2.2 Audio Digital dan Ancaman Keamanan

Audio digital Adalah representasi sinyal suara dalam format data digital. Ancaman keamanan terhadap audio mencakup:

1. Penyadapan (eavesdropping)
2. Manipulasi data audio
3. Pencurian dam pemalsuan audio

### 2.3 OWASP (Open Web Application Security Project)

OWASP merupakan organisasi nirlaba yang menyediakan standar dan panduan keamanan aplikasi. OWASP Top 10 sering dijadikan acuan untuk mengidentifikasi celah keamanan umum, seperti:

1. Broken Authentication
2. Sensitive Data Exposure
3. Security Misconfiguration

### 2.4 Algoritma RSA

RSA Adalah algoritma kriptografi kunci public yang menggunakan pasangan kunci public dan kunci privat. Algoritma ini banyak digunakan untuk mengamankan data karena Tingkat keamanannya yang tinggi, yang di dasarkan pada kesulitan memfaktorkan bilangan prima besar.

### 2.5 Metode Penelitian

Pendekatan yang di terapkan dalam penelitian ini Adalah deskriptif dan eksperimental, meliputi Langkah-langkah analisis, desain, pelaksanaan, dan penilaian.

### 2.6 Desain Framework OWASP

Framework yang di kembangkan mencakup beberapa Langkah:

1. Pengenalan aset audio
2. Penilaian ancaman sesuai dengan OWASP Top 10
3. Pelaksanaan Langkah keamanan
4. Penialaian dan pengurangan risiko

### 2.7 Impementasi Algoritma RSA pada Audio

Prosedur pengamanan audio menggunakan algoritma RSA terdiri dari:

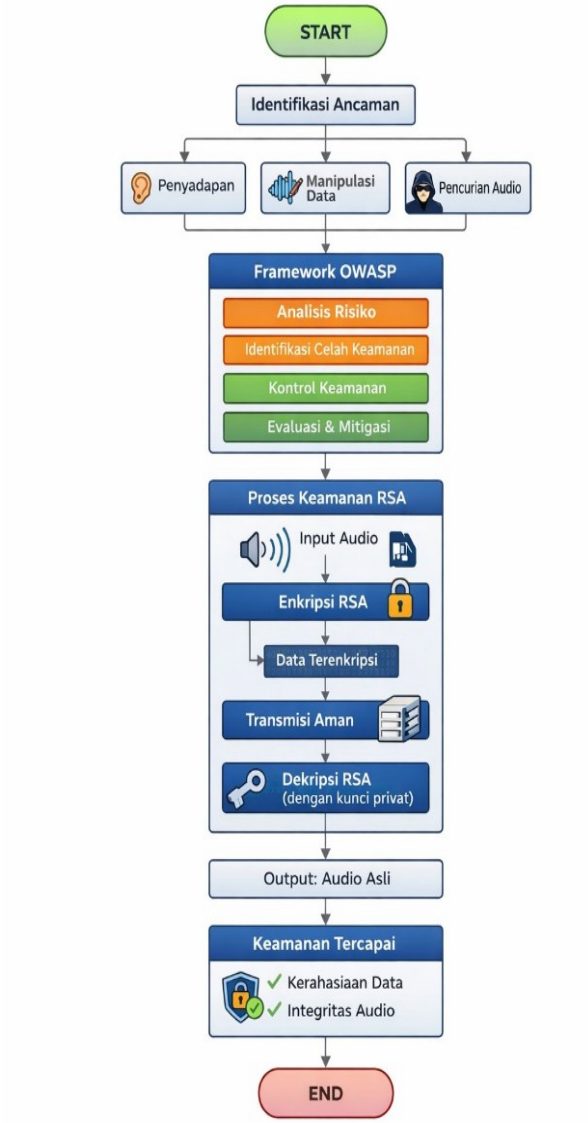
1. Mengubah audio menjadi format data biner
2. Melakukan enkripsi terhadap data audio dengan menggunakan kunci public RSA
3. Menyimpan atau mengirim audio yang telah dienkripsi
4. Melakukan deskripsi audio menggunakan kunci privat RSA

## 3 HASIL DAN PEMBAHASAN

### 3.1 Rancangan Kerangka Kerja OWASP dalam Keamanan Audio.

Berdasarkan studi yang telah dilakukan, kerangka kerja OWASP dibangun untuk mengenali dan mengurangi kelemahan keamanan dalam system audio digital. Kerangka ini menerapkan prinsip-prinsip dari OWASP Top 10, terutama terkait dengan risiko Eksposur Data Sensitif,

Kontrol Akses yang Rusak, dan Konfigurasi Keamanan yang Tidak Tepat, yang sering muncul dalam system multimedia.




Gambar 1. Alur Pengerjaan RSA

Gambar 1 menggambarkan Langkah-langkah analisis risiko, pengenalan kelemahan keamanan implementasi algoritma RSA, dan penelitian serta pengurangan risiko keamanan.

Dalam gambar tersebut terlihat bahwa proses dimulai dari input audio yang mungkin menyimpan data sensitif. Tanpa adanya system keamanan, audio dapat dengan mudah disadap, dimanipulasi, dan dicuri.

### 3.2 Identifikasi Ancaman Keamanan Audio

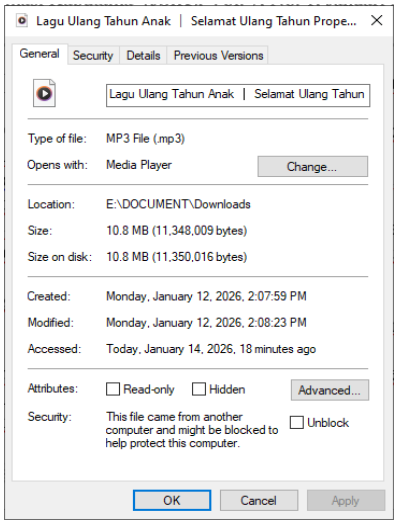
Penggunaan framework OWASP membantu dalam mengidentifikasi ancaman keamanan terhadap data audio digital. Berdasarkan framework OWASP, beberapa ancaman utama pada audio Adalah sebagai berikut:

1. Penyadapan (Eaverdropping) : Penyerangan dapat menangkap data audio selama proses transmisi jika tidak dilindungi dengan enkripsi.
2. Manipulasi Data Audio : Data audio dapat diubah atau dimodifikasi tanpa izin, sehingga menyebabkan kerusakan integritas informasi.
3. Pencurian Audio : Audio dapat dicuri dan digunakan tanpa izin pemiliknya, yang merupakan ancaman serius terhadap privasi.

Ancaman-ancaman tersebut menunjukkan bahwa data audio digital memerlukan perlindungan kriptografi yang kuat untuk menjaga kerahasiaan dan integritasnya.

### 3.3 Penerapan Algoritma RSA pada Sistem Audio

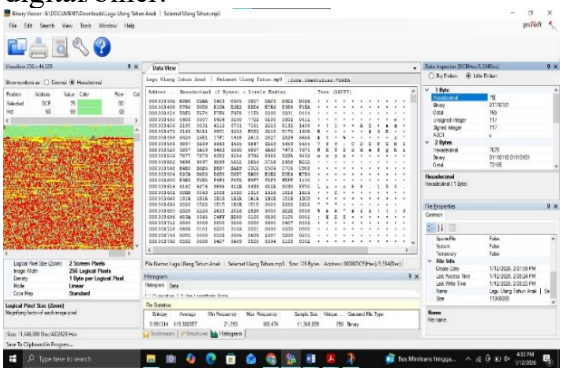
Berikut adalah file audio selamat ulang tahun yang kami ambil sebagai bahan penelitian




Gambar 2. File Audio Lagu Selamat Ulang Tahun dengan Format Mp3 dan Size 10.8 MB (11,348,009 bytes)

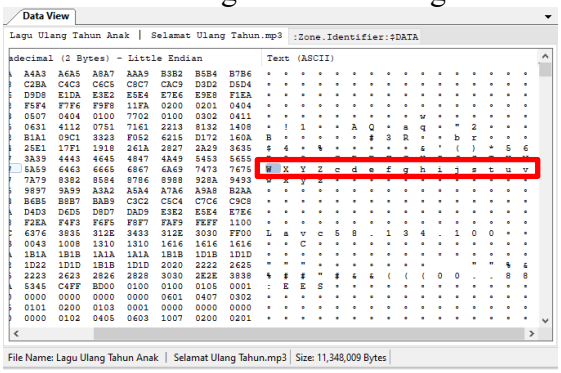
Seperti ditunjukkan pada Gambar 1, algoritma RSA diterapkan pada tahap enkripsi dan dekripsi data audio melalui beberapa tahapan:

1. Data audio dikonversi ke bentuk digital/biner.



Gambar 3. Aplikasi Binary Viewer dengan Audio Lagu Selamat Ulang Tahun

Berikut adalah sample data yang kami ambil dari file Lagu Selamat Ulang Tahun:



Gambar 4. Data Pada Aplikasi Binary Viewer

2. Data audio dienkripsi menggunakan kunci publik RSA.

Berikut Adalah perhitungan hasil konversi audio ke bentuk biner menggunakan algoritma RSA:

p = 17
q = 11

n = p x q = 17 x 11 = 187

e = 7
cari nilai d
d.e mod Φn = 1
d.7 mod 160 = 1
23.7 mod 160 = 1
161 mod 160 = 1
1 = 1
maka, d = 23

- **Proses Enkripsi** :

Plainfile = W X Y Z c d e f g h i j s t u v
Langkah pertama plainfile = W X Y Z c d e f g h i j s t u v akan diubah ke tabel ASCII
W = 87
X = 88
Y = 89
Z = 90
c = 99
d = 100
e = 101
f = 102
g = 103
h = 104
i = 105
j =106
s = 115
t = 116
u =117
v =118

c[0] = m^e mod n = 87^7 mod 187 = 43
c[1] = m^e mod n = 88^7 mod 187 = 11
c[2] = m^e mod n = 89^7 mod 187 = 166
c[3] = m^e mod n = 90^7 mod 187 = 95
c[4] = m^e mod n = 99^7 mod 187 = 176
c[5] = m^e mod n = 100^7 mod 187 = 144
c[6] = m^e mod n = 1017 mod 187 = 84
c[7] = m^e mod n = 102^7 mod 187 = 119
c[8] = m^e mod n = 103^7 mod 187 = 137
c[9] = m^e mod n = 104^7 mod 187 = 179
c[10] = m^e mod n = 105^7 mod 187 = 96
c[11]= m^e mod n = 106^7 mod 187 = 149
c[12] = m^e mod n = 115^7 mod 187 = 157
c[13] = m^e mod n = 116^7 mod 187 = 74
c[14] = m^e mod n = 117^7 mod 187 = 127
c[15] = m^e mod n = 118^7 mod 187 = 101

Ubah dalam bentuk karakter ASCII
c[0] = 43 = +
c[1] = 11 = VT
c[2] = 166 = ª
c[3] = 95 = _

c[4] = 176 = ▒
c[5] = 144 = É
c[6] = 84 = T
c[7] = 119 = w
c[8] = 137 = ë
c[9] = 179 = │
c[10] = 96 = `
c[11] = 149 = ò
c[12] = 157 = Ý
c[13] = 74 = J
c[14] = 127 = ⌂
c[15] = 101 = e

Ciphertext = + VT ª _ ▒ É T w ë │ ` ò Ý J ⌂ e

- **Proses Dekripsi :**

Ciphertext = + VT ª _ ▒ É T w ë │ ` ò Ý J ⌂ e

+ = 43
VT = 11
ª = 166
 = 95
▒ = 176
É = 144
T = 84
W = 119
ë = 137
│ = 179
` = 96
ò = 149
Ý = 157
J = 74
⌂ = 127
e = 101

p[0] = c^d mod n = 43^23 mod 187 = 87
p[1] = c^d mod n = 11^23 mod 187 = 88
p[2] = c^d mod n = 166^23 mod 187 = 89
p[3] = c^d mod n = 95^23 mod 187 = 90
p[4] = c^d mod n = 176^23 mod 187 = 99
p[5] = c^d mod n = 144^23 mod 187 = 100
p[6] = c^d mod n = 84^23 mod 187 = 101
p[7] = c^d mod n = 119^23 mod 187 = 102
p[8] = c^d mod n = 137^23 mod 187 = 103
p[9] = c^d mod n = 179^23 mod 187 = 104
p[10] = c^d mod n = 96^23 mod 187 = 105
p[11] = c^d mod n = 149^23 mod 187 = 106
p[12] = c^d mod n = 157^23 mod 187 = 115
p[13] = c^d mod n = 74^23 mod 187 = 116
p[14] = c^d mod n = 127^23 mod 187 = 117
p[15] = c^d mod n = 101^23 mod 187 = 118

Ubah dalam bentuk karakter ascii
p[0] = 87 = W
p[1] = 88 = X
p[2] = 89 = Y
p[3] = 90 = Z
p[4] = 99 = c
p[5] = 100 = d
p[6] = 101 = e
p[7] = 102 = f
p[8] = 103 = g
p[9] = 104 = h
p[10] = 105 = i
p[11] = 106 = j
p[12] = 115 = s
p[13] = 116 = t
p[14] = 117 = u
p[15] = 118 = v

Plaintext = W X Y Z c d e f g h i j s t u v
Hasil dekripsi dari ciphertext ke plaintext membuktikan bahwa data kembali ke bentuk awal.

Audio yang telah dienkripsi dapat disimpan atau ditransmisikan melalui jaringan.
Penerima melakukan dekripsi menggunakan kunci privat RSA untuk mendapatkan audio asli.
Penerapan RSA ini bertujuan menjaga kerahasiaan dan integritas data audio, yang terlihat pada symbol keamanan berbentuk gembok.

### 3.4 Analisis Keamanan Sistem Berdasarkan Framework OWASP

Penerapan framework OWASP dan algoritma RSA menghasilkan system keamanan audio yang lebih terstruktur.

Berdasarkan hasil analisis:

1. Framework OWASP berperan dalam mengidentifikasi ancaman dan risiko keamanan pada system.
2. Algoritma RSA berperan dalam melindungi data audio dari akses yang tidak sah.
3. System ini mampu meminimalkan risiko data leakage dan manipulasi data audio.
4. Visualisasi pada Gambar 1 menunjukkan bahwa setiap tahapan keamanan saling terintegrasi, mulai dari analisis risiko hingga mitigasi, sehingga membentuk system keamanan audio yang komprehensif.

### 1.5 Pembahasan Hasil

Hasil penelitian menunjukkan bahwa penggunaan framework OWASP memberikan panduan yang sistematis dalam mengidentifikasi celah keamanan pada data audio digital. Sementara itu, algoritma RSA terbukti efektif dalam menjaga kerahasiaan dan integritas data audio selama proses penyimpanan dan transmisi. Oleh karena itu, desain framework ini dapat meningkatkan Tingkat keamanan audio secara signifikan dan menjadi acuan dalam pengembangan system keamanan multimedia.

## 4. KESIMPULAN

Berdasarkan hasil penelitian, dapat disimpulkan bahwa:

1. Framework OWASP efektif dalam mengidentifikasi kerentanan keamanan pada system audio.
2. Algoritma RSA mampu meningkatkan keamanan audio melalui mekanisme enkripsi dan dekripsi.
3. Integrasi OWASP dan RSA menghasilkan system keamanan audio yang lebih terstruktur dan andal.

## 5. SARAN

Penelitian selanjutnya disarankan untuk:

1. Menggunakan framework lain sebagai perbandingan.
2. Menguji performa system pada skala data audio yang lebih besar.
3. Mengintegrasikan algoritma keamanan dengan system real-time.

## DAFTAR PUSAKA

[1]. Andress, J. (2021). The baSsics of information security: Understanding the fundamentals of InfoSec in theory and practice. Syngress.
[2]. Kahn Academy. (2023). RSA encryption. Diakses dari https://www.khanacademy.org
[3]. Kurniawan, D., & Setiawan, A. (2020). Implementasi algoritma RSA untuk pengamanan data digital. Jurnal Teknologi Informasi, 8(2), 45–52.
[4]. Munir, R. (2019). Kriptografi. Bandung: Informatika.
[5]. OWASP Foundation. (2023). OWASP Top 10 Web Application Security Risks. Diakses dari https://owasp.org
[6]. Paar, C., & Pelzl, J. (2010). Understanding cryptography: A textbook for students and practitioners. Springer.
[7]. Prasetyo, E. (2018). Keamanan sistem informasi. Yogyakarta: Andi Offset.