DESIGN AND IMPLEMENTATION OF AN OWASP BASED FRAMEWORK FOR IDENTIFYING SECURITY VULNERABILITIES IN RSA ENCRYPTED AUDIO SYSTEMS

SUCI RAMADANI[1], RIZKA PUTRI RAHAYU[2], ACHMAD FAUZI*[3]

[1,3] STMIK Kaputama, Jl. Venteran No.4A-9A Binjai, 20714, Sumatera Utara, Indonesia
E-mail: fauzyrivai88@gmail.com*

ABSTRACT

The rapid advancement of multimedia technology, particularly in digital audio systems, has significantly increased the demand for robust information security mechanisms. Digital audio is widely used for communication, storage of sensitive information, and voice-based authentication, making it vulnerable to cyber threats such as eavesdropping, tampering, and unauthorized access. Despite these risks, many existing audio processing systems lack a structured and standardized security assessment framework to systematically identify and mitigate potential vulnerabilities. This study aims to design and implement an OWASP based security framework to identify, analyze, and mitigate security vulnerabilities in audio processing systems integrated with the RSA cryptographic algorithm. The proposed solution combines OWASP security principles for risk analysis, vulnerability assessment, and mitigation planning with RSA encryption and decryption mechanisms to ensure data confidentiality and integrity during audio transmission and storage. The results indicate that the implementation of RSA enhances the protection of audio data against unauthorized access, while the OWASP based framework provides a systematic and structured methodology for detecting and addressing security gaps. This research offers a practical and comprehensive reference model for developing more secure, resilient, and standardized digital audio security systems in modern multimedia environments

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

1. INTRODUCTION

Information security is a crucial aspect of modern information systems. Not only text and image data, but audio data has also become a target of cyberattacks, as it often contains sensitive information such as confidential conversations, voice biometric data, and recordings of critical communications[1]. The rapid advancement of information and communication technology has significantly increased the use of digital audio across various sectors, including online communication, entertainment media, monitoring systems, and voice-based authentication[2]. However, the increasing utilization of digital audio has not always been accompanied by the implementation of adequate security mechanisms. Without a structured protection system, audio data remains vulnerable to threats such as eavesdropping, data manipulation, forgery, and information theft[3]. Although numerous studies have examined the application of cryptographic algorithms to secure digital data, most have primarily focused on text and image data, while integrated and systematic security approaches for audio processing systems remain relatively limited. Furthermore, cryptographic implementations are often not accompanied by standardized risk analysis frameworks to comprehensively identify and evaluate potential security vulnerabilities[4]. This gap underscores the necessity of developing a more comprehensive security approach.

This study aims to design and implement an OWASP-based security framework integrated with the RSA cryptographic algorithm to identify, analyze, and mitigate security vulnerabilities in digital audio processing systems[5],[6],[7]. OWASP is employed as a systematic approach for risk analysis and vulnerability identification, while RSA is implemented to ensure the confidentiality and integrity of audio data through public-key encryption and decryption mechanisms[8]. The solution proposed in this study is a structured security framework model that integrates risk identification, vulnerability

assessment, and audio encryption processes into a unified approach. The contribution of this research lies in providing both conceptual and technical references for system developers in designing digital audio systems that are more secure, reliable, and aligned with modern information security principles, thereby reducing the risks of data leakage and misuse of audio data in digital environments[9], [10], [11].

2. METHODOLOGY

Information security aims to protect data from various threats by ensuring three fundamental principles: confidentiality, integrity, and availability [9], [12].

2.1 Digital Audio and Security Threats

Digital audio is a representation of sound signals in digital data format. Security threats to audio include:

1. Eeavesdropping
2. Audio data manipulation
3. Audio theft and forgery

2.2 OWASP (Open Web Application Security Project)

OWASP is a non-profit organization that provides standards and guidelines for application security. The OWASP Top 10 is widely used as a reference for identifying common security vulnerabilities, such as:

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

2.3 RSA Algorithm

RSA is a public-key cryptographic algorithm that utilizes a pair of keys: a public key and a private key. This algorithm is widely used to secure data due to its high level of security, which is based on the computational difficulty of factoring large prime numbers. The following are the fundamental equations of the RSA algorithm [13],[14],[15], [16].

- **p** and **q** are prime numbers (secret)
- n = p . q (public)
- ϕ (n) = (p – 1)(q – 1) (secret)
- e (encryption key) (public)
- d (decryption key) (secret)
- m (plaintext) (secret)
- c (ciphertext) (public)

2.4 Research Methodology

The approach applied in this study is descriptive and experimental, encompassing the stages of analysis, design, implementation, and evaluation.

2.6 OWASP Framework Design

The developed framework consists of several stage:

1. Identification of audio assets
2. Threat assessment in accordance with the OWASP Top 10
3. Implementation of security measures
4. Risk evaluation and mitigation

2.7 Implementation of the RSA Algorithm for Audio

The audio security procedure using the RSA algorithm consists of the following steps:

1. Converting the audio into binary data format.
2. Encrypting the audio data using the RSA public key.
3. Storing or transmitting the encrypted audio.
4. Decrypting the audio using the RSA private key.

3. RESULTS AND DISCUSSION

Based on the conducted study, the OWASP framework was adopted to identify and mitigate security vulnerabilities in digital audio systems. This framework applies the principles of the OWASP Top 10, particularly those related to Sensitive Data Exposure, Broken Access Control, and Security Misconfiguration, which commonly arise in multimedia systems

3.1 RESULTS

To facilitate a clearer understanding of the design and implementation stages of the audio security system, a workflow diagram is presented to systematically illustrate the research process. The diagram demonstrates the integration between OWASP-based risk analysis and the implementation of the RSA algorithm in identifying and mitigating potential security vulnerabilities.

Figure 1. RSA Processing Workflow

Figure 1 illustrates the stages of risk analysis, identification of security vulnerabilities, implementation of the RSA algorithm, and the assessment and mitigation of security risks. The figure shows that the

process begins with an audio input that may contain sensitive data. Without an adequate security system, the audio can be easily intercepted, manipulated, or stolen.

3.1.1 Identification of Audio Security Threats

The use of the OWASP framework assists in identifying security threats to digital audio data. Based on the OWASP framework, several primary threats to audio systems are as follows:

1. Eavesdropping: Attackers may intercept audio data during transmission if it is not protected by encryption
2. Audio Data Manipulation: Audio data may be altered or modified without authorization, thereby compromising the integrity of the information.
3. Audio Theft: Audio files may be stolen and used without the owner's consent, posing a serious threat to privacy.

These threats indicate that digital audio data requires strong cryptographic protection to ensure its confidentiality and integrity.

3.1.2 Implementation of the RSA Algorithm in the Audio System

The following is the "Happy Birthday" audio file selected as the research sample for this study

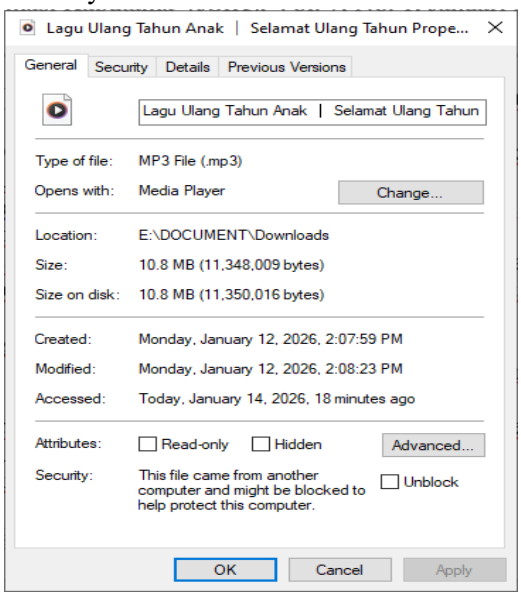

Figure 2. "Happy Birthday Song" Audio File in MP3 Format with a Size of 10.8 MB (11,348,009 bytes)

As illustrated in Figure 1, the RSA algorithm is applied at the audio data encryption and decryption stages through several sequential steps.

a. The audio data is converted into digital/binary form

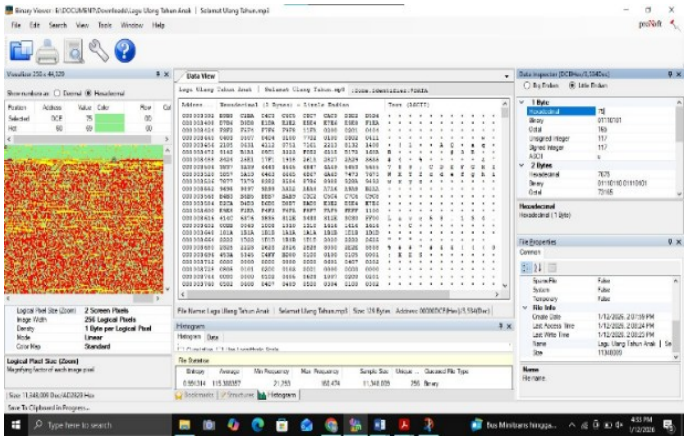

Figure 3. Binary Viewer Application Displaying the "Happy Birthday Song" Audio File

The following is a sample of data extracted from the file *"Happy Birthday Song"*:

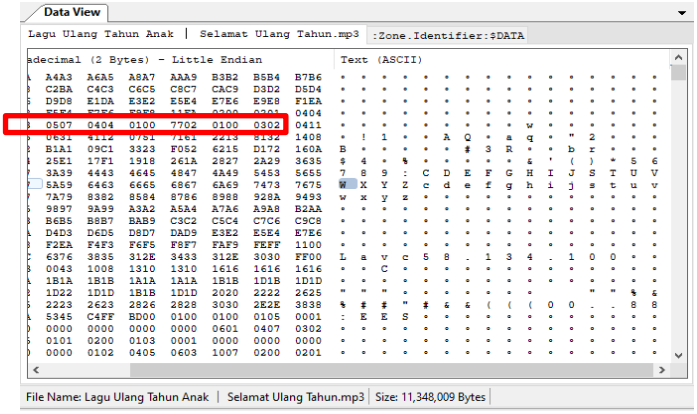

Figure 4. Data in the Binary Viewer Application

b. The audio data is encrypted using the RSA public key

Here is the calculation result of converting audio into binary form using the RSA algorithm

p = 17

q = 11

n = p x q = 17 x 11 = 187

e = 7

Find the value of **d**.

d.e mod Φn = 1

d.7 mod 160 = 1

23.7 mod 160 = 1

161 mod 160 = 1

1 = 1

Therefore, d = 23

c. Encryption process

plaintext file = **W X Y Z c d e f g h i j s t u v**

The first step is the plaintext file = **W X Y Z c d e f g h i j s t u v**

Will be converted into an ASCII table

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

Convert into ASCII characters.
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
Cipherfile = + VT ª _ ▒ É T w ë │ ` ò Ý J ⌂ e

d. Decryption process
Cipherfile = + 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

Convert into ASCII characters.
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
Plainfile = **W X Y Z c d e f g h i j s t u v**
The decryption results from ciphertext to plaintext demonstrate that the data is successfully restored to its original form

3.2 DISCUSSION

Audio encrypted using the RSA algorithm can be stored or transmitted over a network with a higher level of security, as the data is transformed into an unintelligible ciphertext form that cannot be interpreted without the corresponding key. On the recipient's side, the decryption process is performed using the RSA private key to restore the audio to its original form in its entirety. This mechanism ensures that only authorized parties are able to access the information, thereby maintaining data confidentiality during both storage and transmission processes.

Moreover, data integrity is preserved, as any alteration or manipulation of the encrypted data will result in an invalid or corrupted decryption output. Therefore, the implementation of RSA functions not only as an encryption method but also as a cryptographic protection layer that strengthens the security of the audio system against threats such as interception, unauthorized modification, and information theft

3.2.1 System Security Analysis Based on the OWASP Framework

The implementation of the OWASP framework in conjunction with the RSA algorithm results in a more structured and systematic audio security system.
Based on the analysis results:

1. The OWASP framework plays a critical role in identifying potential threats and assessing security risks within the system.
2. The RSA algorithm functions as a cryptographic mechanism to protect audio data from unauthorized access
3. The proposed system is capable of minimizing the risks of data leakage and unauthorized manipulation of audio data
4. The visualization presented in Figure 1 illustrates that each security phase is interconnected—from risk analysis to mitigation—thereby forming a comprehensive and integrated audio security framework

3.2.2 Discussion of Results

The findings of this study indicate that the implementation of the OWASP framework provides a systematic and structured approach to identifying security vulnerabilities in digital audio processing systems. Through stages of risk analysis, vulnerability identification, and threat evaluation, the framework effectively maps potential weak points within the system, encompassing data storage, transmission, and audio data management processes. This standards-based approach enables a more focused and methodical testing procedure compared to vulnerability identification conducted without a clearly defined framework.

Furthermore, the implementation of the RSA algorithm demonstrates that public key–based encryption and decryption mechanisms are effective in ensuring the confidentiality and integrity of audio data. Encrypted audio data cannot be accessed or modified without the corresponding private key, thereby minimizing the risks of interception and unauthorized manipulation. In addition, the application of RSA provides an additional layer of security during data transmission, particularly in network environments that are susceptible to cyber threats

The integration of the OWASP framework and the RSA algorithm results in a security approach that is not only preventive in nature but also analytical and evaluative. While the OWASP framework functions to detect and mitigate potential security vulnerabilities, RSA serves as a technical protection mechanism for safeguarding data. The combination of these two approaches significantly enhances the overall security level of the audio system and offers a more comprehensive security model that can be applied in the development of secure and reliable multimedia systems.

4. CONCLUSION

Based on the findings of this study, it can be concluded that:

1. The OWASP framework has proven to be effective as a systematic approach for identifying, analyzing, and evaluating security vulnerabilities in audio processing systems, thereby enabling a more structured and targeted risk detection process
2. The RSA algorithm enhances the security level of audio data by ensuring confidentiality and integrity through public-key–based encryption and decryption mechanisms, thereby protecting the data from unauthorized access and manipulation
3. The integration of the OWASP framework and the RSA algorithm results in a more comprehensive, standardized, and reliable audio security system model, which can serve as a reference for the development of secure digital audio systems in accordance with modern information security principles.

5. SUGGESTIONS

Future research is recommended to:

1. Conduct a comparative analysis between the OWASP framework and other established security frameworks to evaluate their relative effectiveness and advantages in securing digital audio systems
2. Perform experimental evaluations using large-scale audio datasets to comprehensively assess the performance, efficiency, and scalability of the RSA algorithm in practical implementations
3. Integrate the proposed security system into real-time audio-based applications in order to examine its stability, robustness, and overall effectiveness under actual operational conditions

REFERENCES

[1] A. Fauzi, "Integration Of Data Filtering With Hybrid Rsa Deep Learning Algorithm For IOT Data," vol. 103, no. 22, pp. 9646–9659, 2025.

[2] A. H. Kridalaksana, A. Y. Rangan, and A. Ansharie, "Audio Data Encryption Using RSA Cryptography Method," *Sebatik*, vol. 17, no. 1, pp. 6–10, 2021, doi: 10.46984/sebatik.v17i1.79.

[3] M. Al Kahfi, M. Auva, D. P. Putra, C. D. P. B. Ginting, and A. Fauzi, "Super Text Data Encryption: Combination of Affine Cipher, Elgamal, and RSA Algorithms for Optimal Protection," *J. Sist. Inf. Kaputama*, vol. 9, no. 1, pp. 20–34, Jan. 2025, doi: 10.59697/JSIK.V9I1.949.

[4] A. Fauzi, "Asymmetric Cryptography: A Technical Analysis Of The RSA And Elgamal Algorithms," 2025th ed., no. 27, Medan: PT. Pustaka Pratama, 2025, p. 86. [Online]. Available: https://store.pustakapratama.com/product/asymmetric-cryptography-a-technical-analysis-of-the-rsa-and-elgamal-algorithms/

[5] T. B. Surbakti, A. Fauzi, and H. Khair, "Hybrid Sistem Algoritma Rivest Shamir Adleman (RSA) dan Algoritma Blum Blum Shub (BBS) dalam Mengamankan File Database E-Absensi," *Indones. J. Educ. Comput. Sci.*, vol. 1, no. 3, pp. 89–97, Aug. 2023, doi: 10.60076/INDOTECH.V1I2.59.

[6] Muhammad Al Kahfi, Mita Auva, Denny Prayuda Putra, Chintya Dwi Putri Br. Ginting, and Achmad Fauzi, "Super Text Data Encryption: Combination of Affine Cipher, Elgamal, and RSA Algorithms for Optimal Protection," *J. Sist. Inf. Kaputama*, vol. 9, no. 1, pp. 20–34, Jan. 2025, doi: 10.59697/JSIK.V9I1.949.

[7] M. Rahmani, A. Nitaj, A. Tadmori, and M. Ziane, "An Improved Attack on the RSA Variant Based on Cubic Pell Equation," *Cryptography*, vol. 9, no. 2, pp. 1–16, 2025, doi: 10.3390/cryptography9020040.

[8] A. Fauzi and Y. Maulita, "Rivest Shamir Adleman (RSA) Super Encryption Algorithm with Vigenere Cipher Algorithm Modification for Image Security," vol. 4, no. 1, 2024.

[9] A. Nitaj and T. Rachidi, "Applications of Neural Network-Based AI in Cryptography," *Cryptography*, vol. 7, no. 3, pp. 1–26, 2023, doi: 10.3390/cryptography7030039.

[10] H. Small *et al.*, "Small Private Exponent Attacks on RSA Using Continued Fractions and Multicore Systems," *Symmetry 2022, Vol. 14, Page 1897*, vol. 14, no. 9, p. 1897, Sep. 2022, doi: 10.3390/sym14091897.

[11] S. Fatima, T. Rehman, M. Fatima, S. Khan, and M. A. Ali, "Comparative Analysis of Aes and Rsa Algorithms for Data Security in Cloud Computing," *Eng. Proc. 2022, Vol. 20, Page 14*, vol. 20, no. 1, p. 14, Jul. 2022, doi: 10.3390/engproc2022020014.

[12] M. Almutairi and F. T. Sheldon, "Resilience of Post-Quantum Cryptography in Lightweight IoT Protocols: A Systematic Review," *Eng*, vol. 6, no. 12, pp. 1–16, 2025, doi: 10.3390/eng6120346.

[13] M. Cesati, "A New Idea for RSA Backdoors," *Cryptography*, vol. 7, no. 3, 2023, doi: 10.3390/cryptography7030045.

[14] V. O. Nyangaresi *et al.*, "A Symmetric Key and Elliptic Curve Cryptography-Based Protocol for Message Encryption in Unmanned Aerial Vehicles," *Electron.*, vol. 12, no. 17, 2023, doi: 10.3390/electronics12173688.

[15] K. Liu *et al.*, "A Rivest-Shamir-Adleman-Based Robust and Effective Three-Factor User Authentication Protocol for Healthcare Use in Wireless Body Area Networks," *Sensors (Basel).*, vol. 23, no. 21, pp. 1–19, 2023, doi: 10.3390/s23218992.

[16] M. Kumar *et al.*, "BBNSF: Blockchain-Based Novel Secure Framework Using RP2-RSA and ASR-ANN Technique for IoT Enabled Healthcare Systems," *Sensors 2022, Vol. 22, Page 9448*, vol. 22, no. 23, p. 9448, Dec. 2022, doi: 10.3390/s22239448.