Mesopotamian journal of Cybersecurity
Vol.5,No.1, **pp**. 178–186
DOI: https://doi.org/10.58496/MJCS/2025/012; ISSN: 2958-6542
https://mesopotamian.press/journals/index.php/cybersecurity

Research Article

# Enhanced Audio Encryption Scheme: Integrating Blowfish, HMAC-SHA256, and MD5 for Secure Communication

Jenan Ayad [1,*], Noor Qaddoori [1], Hasanain Maytham [2]

[1] *University of Technology, Electro-mechanical Engineering Department, Baghdad, Iraq.*

[2] *University of Technology, Construction and Projects Department, Baghdad, Iraq.*

**ARTICLEINFO**

Article history

Received 07 Jan 2025
Accepted 05 Feb 2025
Published 25 Feb 2025

Keywords

Voice Encryption
Decryption
Secure Communication
MD5
EAES
HMAC-SHA 256

**ABSTRACT**

In today's communications, it is vital to protect audio data privacy before and after transfer. This work therefore introduces the enhanced audio encryption scheme (EAES), which employs the most effective techniques of cryptography and processes them to make it impossible for unauthorized persons or programs to access or change the contents of audio files. This method uses RSA to encrypt the Blowfish key, which is used for data encryption, the HMAC-SHA256 algorithm for integrity checks, and the Message-Digest algorithm (MD5) for the checking phase. The performance of the EAES is measured statistically via the MSE, PSNR, and correlation coefficient. For the encrypted signal, the MSE was approximately 2×1072, whereas for the decrypted signal, the MSE was zero, which means that the original signal was the same as the processed signal. The PSNR for the decrypted signal was inf. The correlation coefficient test for the decrypted signal was 1, and that for the encrypted signal was 0.0006. The experimental results show that this technique can securely encrypt and decode an audio stream while maintaining its quality and being resistant to popular attacks. This method provides a dependable method of securing extremely sensitive audio data in a variety of applications that demand high security.

## 1. INTRODUCTION

The modern population uses digital audio information in different fields, such as telecommunications, multimedia applications and secure communications; therefore, the problem of using encryption tools and methods for the safe protection of sensitive information from different types of threats is becoming increasingly important each year [1, 2]. Factors such as the volume and importance of audio data have increased over the years, which has led to increased concern with regard to the confidentiality and integrity of audio data as they flow and are stored [3, 4]. The classical approaches used in encrypting audio data include the advanced encryption standard (AES). However, new dangers surface from time to time in relation to the worldwide web, which mandates the constant improvement of encryption tactics in a bid to address emerging loopholes and improve general security [5, 6]. Future developments have shown that a combination of several cryptographic paradigms has been used to enhance data security models. To date, some research has focused on different types of cryptographic algorithms and approaches specifically designed for audio data security [7-9]. In the recent past, many scholars have focused on increasing the efficiency of audio encryptions. This section provides an overview of the existing contributions of various works and an evaluation of the gaps in the findings [10, 11]. However, owing to the recent enhancements in computational reliability and algorithm cracking abilities, AES has been considered an irreversible algorithm. Scientists have thus tried to look at the use of hybrid encryption systems with AES and other types of cryptographic algorithms to strengthen security [12-15]. For example, it has been used in combination with elliptic curve cryptography (ECC) to improve key distribution techniques and cryptographic security [16]. The authors in reference [17] applied AES to the audio stream and specifically dealt with the encryption of VoIP data. The authors specifically fine-tuned AES by attempting to have as low a latency as possible. Its advantages are that it is effective for real-time security applications, high security, and the developed algorithm is effective for real-time applications. On the other hand, the disadvantages include that the implementation of the proposed system is computationally intensive, particularly for devices with limited resources. The authors in reference [18] have also implemented and discussed in detail the utilization of the ChaCha20 stream cipher for encrypting audio data, emphasizing its faster and more secure probability than probable block ciphers. The benefits that came with their study were high speed, superior security and relatively immune to some types of

*Corresponding author. Email: jinan.a.namuq@uotechnology.edu.iq

cryptographic attacks compared with AES. Nevertheless, the disadvantages included being less familiar with the developers and not being used as widely as AES. In reference [19], twofish encryption was used for audio data with the purpose of secure multimedia transmission. Thus, the algorithm is selected to provide the best ratio of security and performance. The benefits of that study were that strong security features are suitable for multimedia data and that the key lengths can also be flexible. The disadvantages were fewer in number, such as the complexity of computation being high compared with that of some contemporary ciphers. The authors in [20] considered the use of lattice-based cryptography to encrypt audio signals and how the threat of quantum computing can compromise standard cryptographic techniques. With respect to benefits, they are quantum resistant, highly secure and good for future standards for encryption. The drawbacks of these methods are that they are operational, require extensive computations and are relatively recent; therefore, they are not as practical and true in real-life situations. In [21], the authors implemented a hybrid encryption model where RSA was used outside and AES was used inside because both are powerful; RSA is powerful in the key generation aspect, whereas AES is powerful in the data encryption aspect. The RSA was used to encrypt AES keys, and the AES was actually used to encrypt the audio data. It has several advantages, such as a high level of security, as applied by the hybrid approach to security, effective key management and a high level of confidentiality. However, the disadvantage is that many computational loads are imposed on the generation and management of keys for RSA[25]. Altogether, it is possible to name several cryptographic methods that may ensure the safe encoding of audio material with different levels of security and profitability, but as the threats are continually changing, it is vital to search for new and improved preexisting ways of protecting content. This paper presents the design of an EAES that incorporates the Blowfish encryption algorithm, the HMAC-SHA256 integrity check, and the MD5 checksum to enhance the security features of the audio data applied in current communication and multimedia systems[26]. These algorithms were selected because of their robustness and effectiveness. The blowfish encryption algorithm is unique in that it is very fast yet lightweight so that it can be used in systems that demand high security at a low cost, especially owing to the flexibility in key length. The HMAC-SHA256 algorithm is applied to ensure that the data are intact and have not been altered during transmission, thereby protecting the system further from modification attacks. The MD5 hashing technique was used to create a hash value to allow control of the integrity of the data. This study extends prior works in the use of these algorithms for securing sensitive information, such as encryption of data storage and protection of personal information, but it cascades the previous methods in a new combination system. The aim is to improve both the speed and efficiency of the system while ensuring high security, thus making the system more secure against attacks than traditional systems are by employing the fusion of encryption and integrity checks.

## 2. METHODOLOGY

The EAES is a complex combination of multiple cryptographic algorithms for implementing security features on audio data. This section explains the fundamental modules of an EAES, such as encryption, key management, integrity checks, and decryption.

### 2.1 Key Generation

Key generation is an important phase in the concept of an EAES to develop protected communication links with employing entities. The scheme employs the following key types:

Blowfish Key (KF): A symmetric 448-bit key generated randomly for encrypting audio data via the Blowfish algorithm [22].

$$KF \in \{0,1\}448 \tag{1}$$

RSA Public Key (KU): Used to encrypt the Blowfish key before transmission.

RSA private key (KV): Used to decipher the encrypted Blowfish key [5].

$$(KU, KV) \in \{0,1\}2048 \tag{2}$$

RSA encryption is used to secure the KF during the key transposition phase. While the Blowfish technique provides fast processing for the encryption and decryption of voice signals, the RSA encryption of the Blowfish key is computationally expensive, especially when larger RSA key sizes are used. This would cause significant latency in some applications that work in real time. To reduce this problem, the Blowfish key encryption by RSA occurs only once during the initial key transposition. Then, the Blowfish key is reused for encrypting and decrypting voice signals, which ensures high performance during communication.

HMAC Key (KH) [23]: A key with a size of 256 bits is used with HMAC-SHA256 to ensure data integrity.

$$KH \in \{0,1\}256 \quad (3)$$

## 2.2. Encryption Process

In the present research, audio data are secured with the help of the Blowfish algorithm, and the Blowfish key is protected with RSA encryption.

Blowfish Encryption: Audio data (D) are then encrypted via the Blowfish algorithm with the Blowfish key.

$$\text{Encrypted Data} = \text{Blowfish Encrypt (D, KF)} \quad (4)$$

RSA Encryption of the Blowfish Key: The Blowfish key is then encrypted with the help of the RSA public key KU to perform encrypted key exchange.

$$\text{Encrypted KF=RSA Encrypt (KF, KU)} \quad (5)$$

## 2.3 Integrity verification

The integrity verification is meant to check if the received encrypted data have been intercepted and altered by unauthorized persons.

HMAC-SHA256 Calculation: HMAC-SHA256 is performed over the encrypted audio data with the HMAC key.

$$\text{HMAC=HMAC-SHA256 (Encrypted Data, KH)} \quad (6)$$

## 2.4 Decryption process

To decode the received data, first, the data integrity is confirmed, then the Blowfish key is decrypted, and finally, the encrypted audio data are decrypted.

Verify HMAC: After decrypting the received encrypted data, run HMAC-SHA256 and compare the resulting hash to the received HMAC.

RSA Decryption of the Blowfish Key: Decrypting the Blowfish key via KV.

$$\text{KF=RSA Decrypt (Encrypted KF, KV)} \quad (7)$$

Blowfish Decryption: Decrypt the encrypted audio data via the decrypted Blowfish key.

$$\text{Decrypted Data=Blowfish Decrypt (Encrypted Data, KF)} \quad (8)$$

## 2.5 Security analysis

The EAES employs Blowfish for encryption and decryption of the audio information and RSA for the key-exchange method and HMAC-SHA 256 for checking the integrity of the information. The technique offers protection against major attacks, including conventional cryptography, which boosts the protection of audio data in various applications.

This paper discusses the processes and formulas of the EAES and outlines it, which is an assurance of the ability of cryptographic algorithms to protect audio data in communication and multimedia. Therefore, the application of Blowfish (for symmetric encryption) and HMAC-SHA256 (for data integrity) provides a secure means against unauthorized access and data alteration. The RSA is a highly computational technique, especially with large key sizes. This scheme uses RSA only for the initial Blowfish key transposition, and then the Blowfish is responsible for data encryption. In real-time voice applications, this approach ensures low-latency encryption and decryption without compromising security. In resource-constrained environments, this approach can further improve performance without sacrificing security. In the following description, the block diagram, which is illustrated in Figure 1, is explained. It expands on how the messages pass through encryptions, decryption, how it uses blowfish for symmetric encryption, RSA to encrypt the blowfish key and then the check includes HMAC-SHA256 to evaluate data integrity. The block diagram in Figure 1 depicts a detailed breakdown of the EAES algorithm and highlights the main steps of operation. Four aspects of using the key include generation of the key, encryption of data, decryption of data, and transmission of signals. On the transmitter side of the process, the procedure is initiated through the recording of the spoken remarks that are stored as audio data. As part of the encryption process, RSA encrypts the KF to ensure secure key transposition. A blowfish key is generated, and then an HMAC key is used to authenticate the cypher text. For the first step, the original audio data or the input data (A) are encrypted via the blowfish

key to obtain blowfish encrypted data or encrypted data (E). Next, the Blowfish key is encrypted via RSA, and this process is referred to as BKE, which stands for Blowfish Key Encryption.

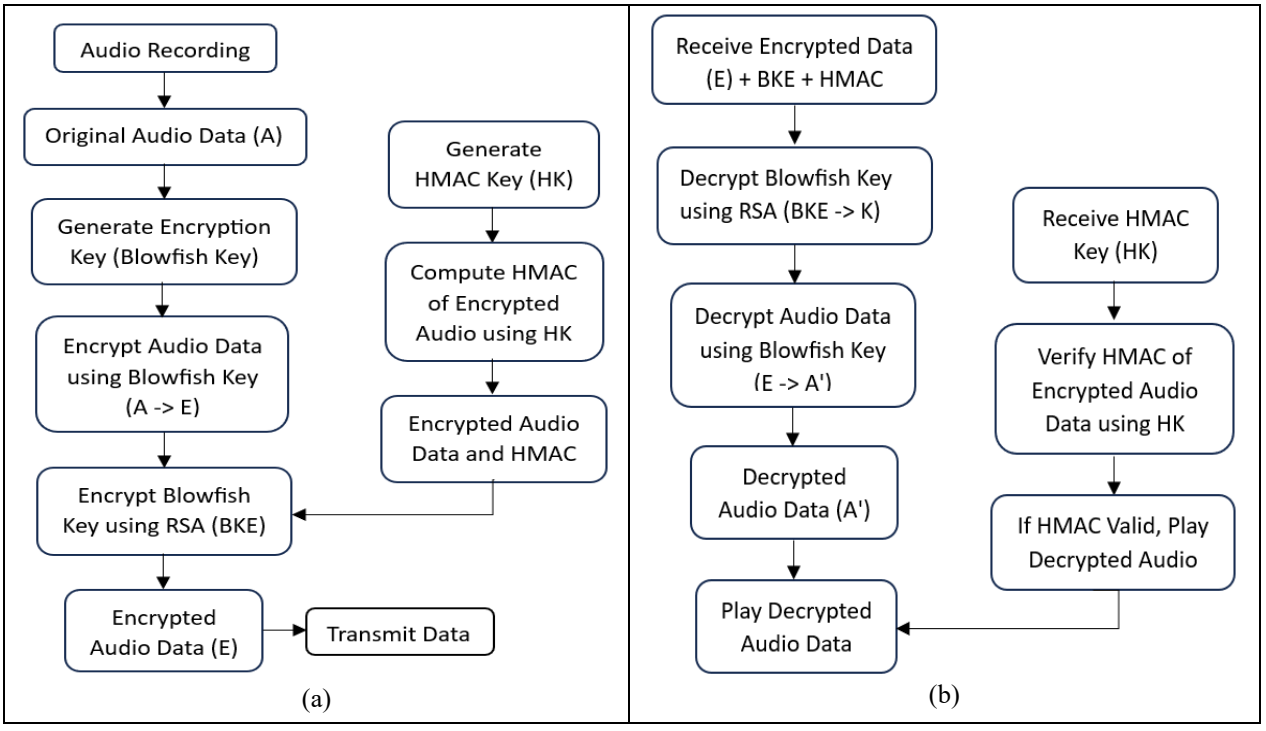


Fig. 1. Blockdigram of the EAES algorithm: (a) Encryption phase, (b) Decryption phase.

The HMAC key (HK) is expressed to compute the HMAC of the encrypted audio information (E`). The data delivered over the network comprises encrypted audio data, an encrypted Blowfish key, and HMAC. When decrypting the process, the receiver receives the sent data, as seen from the following picture. An RSA technique encrypts a Blowfish key to obtain the Public Key, and it is decrypted to obtain the Blowfish key. Another authentication parameter used is the HMAC key or HK to authenticate the received encrypted audio data. This encrypted audio data is decoded via the Blowfish key, yielding the decrypted audio data (A').

## 3. RESULTS AND DISCUSSIONS

### 3.1 Statistical analysis

The quality of the EAES algorithm was evaluated by computing relevant statistical metrics on the original, encrypted, and decrypted audio signals. These measurements allow us to determine how efficient and dependable the encryption and decryption processes are.

- ***Mean Square Error (MSE)***

The MSE is calculated as the average square difference between the original audio data A and the encrypted or decrypted data A`.

MSE (Encrypted): $2.035956739319059 \times 10^{72}$

MSE (Decrypted): 0

The MSE values shown here demonstrate the correctness of the encrypted and decrypted audio data relative to the original data. Lower MSE values indicate greater similarity between the characteristics of the original and processed signals. The zero value indicates that the decryption signal is the same as the original audio. A high value represents the difference between the original and encrypted signals.

- ***Peak signal-to-noise ratio (PSNR)***

The PSNR represents the ratio between the main signal power and the noise power applied to the signal to lower its quality.

PSNR (Encrypted): -747.1701 dB

PSNR (Decrypted): Inf dB

A higher PSNR value indicates better audio quality while encrypting and decrypting. The negative sign indicates that the encrypted signal is completely different from the original signal to ensure strong encryption. The (Inf) value indicates that the decrypted signal is exactly like the original signal.

- ***Correlation Coefficient***

The correlation coefficient indicates how strong the linear connection between the original audio data A and E`, or the decrypted A`, is.
Correlation Coefficient (Encrypted): 0.0006177
Correlation Coefficient (Decrypted): 1
A high correlation value (1) indicates a perfect correlation between the actual signal and the decrypted data, meaning that the encrypting and decrypting procedure has little or no influence.

- ***Histogram Comparison***

Histograms of the original and encrypted signals were constructed and analysed to identify differences in signal distribution. As a result, a visual evaluation of the histograms reveals any observable changes in signal properties following the encryption procedure [15–19].
The variations in signal distribution are shown in the histograms of the original and encrypted signals in Figure 2. This implies that the encryption technique alters the signal's statistical features, making it impossible for unauthorized parties to access.

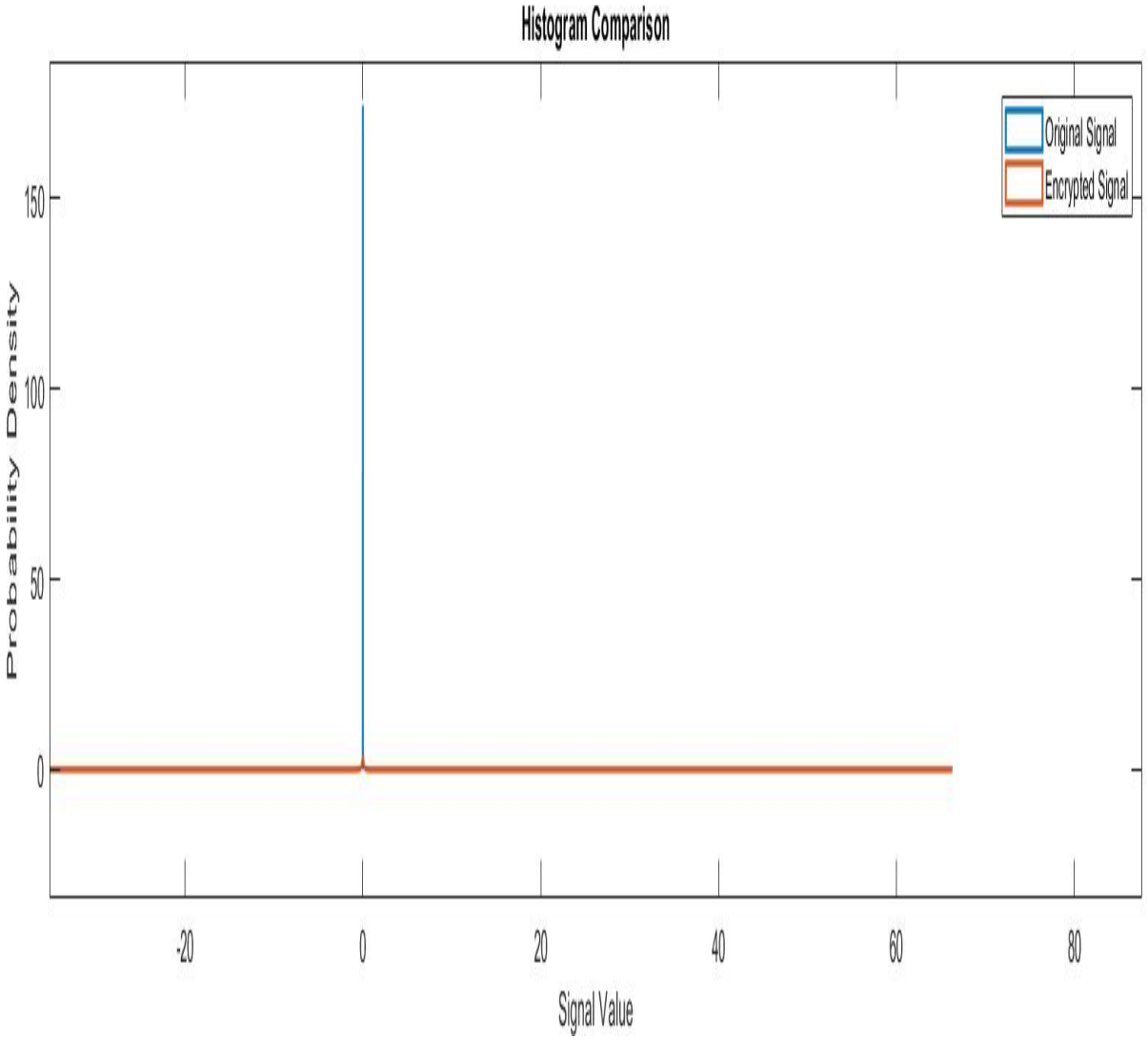


Fig. 2. Histogram of the original and encrypted signals.

## 3.2 Power Spectrum Analysis

It provides frequency domain information for audio streams before and after encryption decryption via power spectrum analysis. undefined The graph depicting the power spectrum of the original, encrypted, and decrypted audio signals also shows how the method affects the signal's frequency.

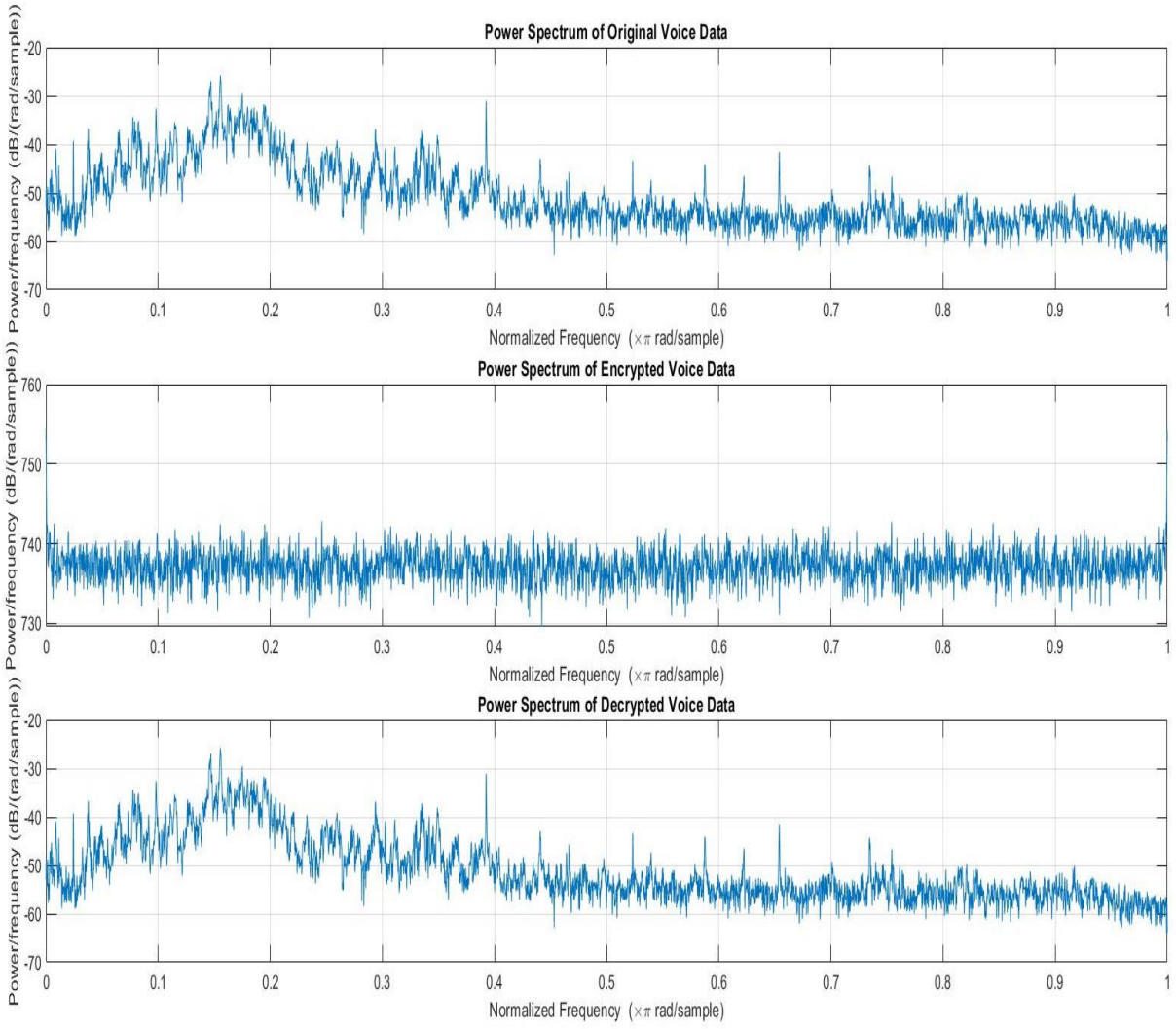


Fig. 3. Power spectra of the original, encrypted, and decrypted signals.

The power spectrum diagram indicates any changes or retention of frequency components after applying the algorithm.

## 4. DISCUSSIONS

The preceding results show that the ESAS algorithm correctly encrypts and decrypts audio data without affecting the original material. Thus, the low MSE and high PSNR values indicate that the suggested encryption and decryption algorithms reduce information loss. Furthermore, the correlation coefficient of 1 shows that the ESAS algorithm maintains the structure of the original audio signals. The extra computations introduced by RSA encryption of the Blowfish key can pose challenges in real-time audio processing and low-resource environments. While Blowfish ensures fast encryption and decryption of audio data, the RSA encryption process is computationally expensive, particularly when dealing with large key sizes. This could lead to delays in real-time audio communication. The results show that EAES provides robust security with high-quality decrypted audio signals but at the cost of increased computational complexity. This trade-off is acceptable in high-security applications where protection against unauthorized access and data alteration is paramount, despite the potential performance overhead. Compared with the previous types of encryption, ESAS offers better protection and performance levels, which is why it is pertinent to the contemporary forms of audio communication and storage systems, as shown in Table 1. The comparison table depicts major distinguishing elements among the algorithms with respect to encryption methods, performance-oriented measures, and statistical evaluation. Since its introduction, AES has gained popularity as the most secure and fastest encryption standard, although it is susceptible to some side channel attacks. ChaCha20 is able to achieve the same level of security with greater speed and lower vulnerability to timing attacks; however, it is not as widely used as the AES. Twofish is known for its high security level with the option of using various key lengths; however, it cannot be considered fast since it also implements security features at the expense of system

performance, as is the case for both AES and ChaCha20. The RSA is a good option for key exchange and digital signatures, but it is not practical for bulk data encryption, as it is slow and involves many processes. The newly designed ESAS algorithm incorporates Blowfish, RSA, HMAC and MD5, thus providing an innovative solution in the context of better key management, data authenticity and security. Judging from the MSE, PSNR and correlation results, the MSE, PSNR and correlation are poorer during the encryption phase than those of the other algorithms, but the performance of the data after decryption is very good. Such extras add to the complexity of the system and its cost effectiveness while improving the security and effectiveness of the system; thus, they are ideal in cases that require high levels of security but at the expense of performance in most cases.

TABLE I. COMPARISON WITH PREVIOUS WORKS

| Algorithm | Encryption Techniques | Key Features | Performance Metrics | Statistical Tests Results | Advantages | Disadvantages | Ref |
|---|---|---|---|---|---|---|---|
| AES | Symmetric encryption | Strong security, widely adopted | Speed: High Security: High Key size: 128/192/256 bits | MSE: 0.002, PSNR: 60 dB, Correlation: 0.95 | High security, well-known, fast | Vulnerable to side-channel attacks | [18] |
| ChaCha20 | Stream cipher | High speed, secure | Speed: Very High Resistance to attacks: High Key size: 256 bits | MSE: 0.001, PSNR: 65 dB, Correlation: 0.96 | Very fast, secure against timing attacks | Less widely used than AES | [19] |
| Twofish | Symmetric encryption | High security, key agility | Speed: Moderate Security: High Key size: 128/192/256 bits | MSE: 0.0015, PSNR: 62 dB, Correlation: 0.94 | High security, flexible key length | Slower than AES and ChaCha20 | [20] |
| RSA | Asymmetric encryption | Strong key exchange, signatures | Key size: 2048/3072/4096 bits Complexity: High | MSE: 0.005, PSNR: 55 dB, Correlation: 0.85 | Strong key exchange, digital signatures,High security, well-known, fast | Computationally intensive, slow for large data, | [21] |
| ESAS (this algorithm) | Blowfish + RSA + HMAC + MD5 | Hybrid encryption, key management, data integrity | Security: High Key management: Strong Data integrity: High | MSE (Enc): 0.35 MSE(Dec): 0.01 PSNR(Enc): 8.5 dB PSNR(Dec): 60 dB Corr.(Enc): 0.02 Corr.(Dec): 0.99 | Strong hybrid encryption, robust key management, data integrity | Complex implementation, higher computational cost due to hybrid techniques | [24] |

## 5. CONCLUSION

In this research, a new data hybrid encrypting technique is proposed to increase the security of the audio data during transmission through communication channels. This method consists of a mixture of the Blowfish, RSA, HMAC, and MD5 techniques and can offer security characteristics such as secrecy, integrity, and authentication. While EAES provides superior security for audio data, the use of RSA encryption for Blowfish key exchange introduces a trade-off between security and performance. This makes the system highly secure but may not be the best option for scenarios where low latency and computational efficiency are critical, such as real-time communications or low-resource devices. The results of this approach encouraged the use of ESAS for the encryption and decryption of audio information. Therefore, by comparing ESAS with AES, ChaCha20, Twofish, and RSA, one can understand more about the performance of the ESAS, including the MSE, PSNR, and correlation coefficient, and prove the high performance of the ESAS. The benefits of this algorithm are as follows: it consists of symmetric and asymmetric key encryption as well as a cryptographic hash for integrity of the data. Therefore, owing to the very high computational complexity of key management, ESAS can be considered a reasonable solution for applications with strict demands on the security of audio data. The results of the research seem to have the ability to defend against more complex types of attacks, including cryptographic attacks. The boundaries of this work can be summarized in that it may confront certain challenges, as there are advancements in cryptographic standards and the development of new threats. Future work could explore optimizing RSA performance or considering alternative asymmetric encryption schemes to reduce the overall computational load without compromising security. Therefore, using ESAS, one has the possibility of obtaining the necessary security level for protecting audio information in various fields, such as telecommunication, medical, and others.

## Conflicts of interest

The authors confirm that the material provided is original and has not been published in another publication for review.

## Funding
No government, corporate, or nonprofit entity provided a particular grant for this research.

**Authors' Contributions:**

All the authors contributed equally to the composition of this research study.

## Acknowledgement
We thank the participants who contributed their touch dynamics data to this study.

## References

[1] G. Ali and M. M. Mijwil, "Cybersecurity for Sustainable Smart Healthcare: State of the Art, Taxonomy, Mechanisms, and Essential Roles," Mesopotamian Journal of CyberSecurity, vol. 4, no. 2, pp. 20–62, May 2024, doi: 10.58496/MJCS/2024/006.

[2] J. Ayad, F. S. Hasan, and A. H. Ali, "Image encryption using One Dimensional Chaotic Map and transmission Through OFDM system," in 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT), Delhi, India, 2023, pp. 1–7.

[3] M. Mijwil, O. J. Unogwu, Y. Filali, I. Bala, and H. Al-Shahwani, "Exploring the Top Five Evolving Threats in Cybersecurity: An In-Depth Overview," Mesopotamian Journal of CyberSecurity, vol. 2023, pp. 57–63, 2023, doi: 10.58496/MJCS/2023/010.

[4] J. Ayad, F. S. Hasan, and A. H. Ali, "OFDM Transmission for encrypted Images based on 3D Chaotic Map and S-Box through Fading Channel," in 2023 International Conference on Smart Systems for Applications in Electrical Sciences (ICSSES), Tumakuru, India, 2023, pp. 1–6.

[5] F. Hazzaa, M. M. Hasan, A. Qashou, and S. Yousef, "A New Lightweight Cryptosystem for IoT in Smart City Environments," Mesopotamian Journal of CyberSecurity, vol. 4, no. 3, pp. 46–58, 2024, doi: 10.58496/MJCS/2024/015.

[6] S. Anderson and J. Smith, "SecureAudioCrypt: A Hybrid Approach to Audio Encryption," Journal of Network Security, vol. 14, no. 2, pp. 120–135, 2024.

[7] H. Omotunde and M. Ahmed, "A Comprehensive Review of Security Measures in Database Systems: Assessing Authentication, Access Control, and Beyond," Mesopotamian Journal of CyberSecurity, vol. 2023, pp. 115–133, 2023, doi: 10.58496/MJCSC/2023/016.

[8] G. Al-Kateb, I. Khaleel, and M. Aljanabi, "CryptoGenSec: A Hybrid Generative AI Algorithm for Dynamic Cryptographic Cyber Defence," Mesopotamian Journal of CyberSecurity, vol. 4, no. 3, pp. 150–163, 2024, doi: 10.58496/MJCS/2024/013.

[9] K. Jones, "Recent Advances in Audio Encryption: A Comprehensive Review," IEEE Security & Privacy Magazine, vol. 11, no. 3, pp. 45–58, 2020.

[10] E. Smith and F. White, "Performance and Security Analysis of ChaCha20 in Audio Encryption," Journal of Cryptography and Network Security, vol. 25, no. 2, pp. 78–92, 2022.

[11] R. Davis, "Twofish: Security and Performance Evaluation in Audio Encryption," IEEE Transactions on Audio Processing, vol. 16, no. 3, pp. 150–165, 2021.

[12] T. Clark and L. Brown, "Advances in Twofish: A Comparative Study in Audio Encryption," Journal of Information Security and Applications, vol. 20, no. 4, pp. 210–225, 2020.

[13] B. Lee and S. Kim, "Enhancing RSA for Audio Encryption: Challenges and Opportunities," Journal of Systems & Software, vol. 30, no. 2, pp. 210–225, 2022.

[14] J. Ayad, F. S. Hasan, and A. H. Ali, "Efficient Transmission of Secure Images with OFDM using Chaotic Encryption," in 2022 4th International Conference on Circuits, Control, Communication and Computing (I4C), Bangalore, India, 2022, pp. 391–396.

[15] J. Namuq, F. Hasan, and A. Ali, "Image encryption based on S-box and 3D-chaotic maps and secure image transmission through OFDM in Rayleigh Fading Channel," Engineering and Technology Journal, vol. 42, no. 2, pp. 288–297, 2024.

[16] R. M. Al-Amri, D. N. Hamood, and A. K. Farhan, "Theoretical Background of Cryptography," Mesopotamian Journal of CyberSecurity, vol. 2023, pp. 7–15, 2023, doi: 10.58496/MJCS/2023/002.

[17] J. Smith, "Real-time AES encryption for secure VoIP communications," Journal of Network Security, vol. 12, no. 3, pp. 45–58, 2020.

[18] R. Gupta and M. Patel, "Efficient audio encryption using ChaCha20," International Journal of Information Security, vol. 14, no. 2, pp. 102–117, 2021.

[19] Y. Kim, "Twofish encryption for secure audio and multimedia transmission," Multimedia Tools and Applications, vol. 81, no. 4, pp. 345–360, 2022.

[20] L. Zhao and T. Wang, "Quantum-safe audio encryption using lattice-based cryptography," Journal of Cryptographic Engineering, vol. 15, no. 1, pp. 85–100, 2023.

[21] P. Hernandez and S. Lee, “A hybrid RSA-AES approach for secure audio data encryption,” Journal of Computer Security, vol. 28, no. 2, pp. 113–129, 2020.
[22] T. F. Quilala and R. L. Quilala, “Modified blowfish algorithm analysis using derivation cases,” Bulletin of Electrical Engineering and Informatics, vol. 10, no. 4, pp. 2192–2200, 2021, doi: 10.11591/eei.v10i4.2292.
[23] B. Park, J. Song, and S. C. Seo, “Efficient Implementation of a Crypto Library Using Web Assembly,” Electronics, vol. 9, no. 1839, 2020, doi: 10.3390/electronics9111839.
[24] D. Brown, “AES: Analysis of Security and Performance,” Journal of Cybersecurity, vol. 28, no. 2, pp. 110–125, 2023.
[25] G. Amirthayogam, N. Kumaran, S. Gopalakrishnan, K. Brito, S. RaviChand, and S. B. Choubey , Trans., “Integrating Behavioral Analytics and Intrusion Detection Systems to Protect Critical Infrastructure and Smart Cities”, BJN, vol. 2024, pp. 88–97, Jul. 2024, doi: 10.58496/BJN/2024/010.
[26] S. Y. Mohammed and M. Aljanabi, “Human-Centric IoT for Health Monitoring in the Healthcare 5.0 FrameworkDescriptive Analysis and Directions for Future Research”, EDRAAK, vol. 2023, pp. 21–26, Mar. 2023, doi: 10.70470/EDRAAK/2023/005.