International Journal of Safety and Security Engineering
Vol. 14, No. 5, October, 2024, pp. 1439-1446
Journal homepage: http://iieta.org/journals/ijsse

Performance Analysis of Advanced Encryption Standards for Voice Cryptography with Multiple Patterns

Firas Hazzaa[1,2], Akram Qashou[1], Israa Ibraheem Al Barazanchi[3,4], Ravi Sekhar[5*], Pritesh Shah[5], Mrinal Bachute[5], Azmi Shawkat Abdulbaqi[6]

[1] Faculty of Science & Engineering, Anglia Ruskin University, Chelmsford CB11PT, UK
[2] Higher Education & Scientific Research Ministry, Baghdad 10001, Iraq
[3] College of Engineering, University of Warith Al-Anbiyaa, Karbala 56001, Iraq
[4] College of Computing and Informatics, Universiti Tenaga Nasional (UNITEN), Puchong 43000, Malaysia
[5] Symbiosis Institute of Technology (SIT) Pune Campus, Symbiosis International (Deemed University) (SIU), Maharashtra 412115, India
[6] Renewable Energy Research Center, University of Anbar, Ramadi 31001, Iraq

Corresponding Author Email: ravi.sekhar@sitpune.edu.in

https://doi.org/10.18280/ijsse.140511

Received: 18 July 2024
Revised: 2 October 2024
Accepted: 15 October 2024
Available online: 31 October 2024

Keywords:
advanced encryption standard (AES), cryptography, voice encryption, energy consumption and security

ABSTRACT

The aim of this research is analyzing its performance to help network designers to decide the suitable security solution for their network. Moreover, performance evaluation performance indicators that can be used to evaluate AES include; the encryption and decryption time, the CPU usage and how well AES performs on different platforms. Software performance indicators also take into account the analysis of throughput, latency, and energy consumption of the systems with special focus on software and hardware sections. Issues that have been noted when it comes to assessment of AES actually include the issue of security and performance, a challenge in managing-keys and finally the issue of platform heterogeneity. Analyzing the given result, it can be stated that there does not exist significant distinctions in the parameters related to the encryption process, including execution time and energy consumption, taking into account different patterns of voice. Thus, the performance analysis of AES for voice encryption and decryption is important to properly manage the scarce resources, to improve the security measures, to make the needed adjustments for further system scalability, to take into consideration the costs and make proper decisions to follow legal requirements encountered in communication systems. This work will be exploited in our upcoming research to enhance AES performance by developing new encryption algorithm.

1. INTRODUCTION

AES stands for Advanced Encryption Standard, which is one of the most significant cornerstones of today's cryptography offering a strong and widely used encryption method for protecting sensitive information by various areas of interest and in various applications (National Institute of Standards and Technology (NIST)) [1]. NIST introduced AES in 2001 as a new advanced standard that replaced the defective DES due to its small key size that was easily cracked through attacks based on brute force (National Institute of Standards and Technology (NIST), 2001). AES utilises the manner of the symmetric-key block cipher in which the same key is used in the processes of encryption and decryption [2]. It follows the SPN structure, which includes a number of round of substitution and permutation so as to provide the best form of protection against various Cryptographic attacks. Given that digital data is on the rise exponentially, the need to have efficient means of encrypting all this data cannot be overemphasized. Some of the things that would constitute evaluation of AES include; its ability to encrypt and decrypt messages, its efficiency in its utilization of resources and adaptability in different computing environment [3]. Due to the developing of new technology such as high speed online services and IoT networks, new challenges have been intreduced in security concern and performance. Cryptography algorithms consumed big amount od network resources like energy and processing time. Therefor it is esential to measure its performance to decide which is the best chose for these new requeremnts [4]. Throughput, latency, and energy appear to be the commonly used parameters for evaluating the performance of the AES algorithm [5]. Some of these factors include the choice of implementation method, the key size that is used, the mode of operations such as the ECB, CBC or CTR and the optimization strategies applied [6]. AES's execution speed in software implementation depends on the algorithm implementation and the computational resource of the underlying equipment [7]. Smoothing techniques incorporated into general-purpose processors including parallel processing, instruction level processing, and

the implementation of new algorithms, can substantially improve AES [8]. As shown in Figure 1, the AES encryption process consists of many rounds of substitution, permutation, and mixing steps to transform plaintext into ciphertext.

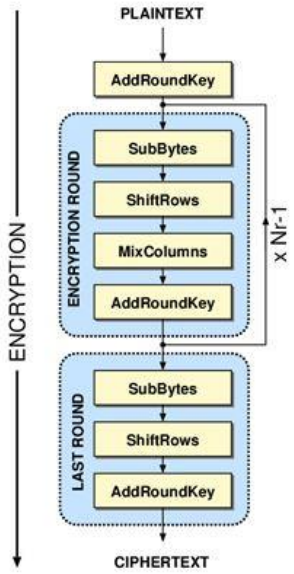


Figure 1. AES

Thus, cloud computing's presence creates new considerations and potentialities regarding AES performance assessment. For cloud-based AES implementations, there are basically near limitless computational resources in today's data centers, yet issues such as network latency and the overheads associated with the transmission of large amounts of data can negatively affect the general encryption performance [9]. Hence, for AES to work efficiently in cloud architecture, there has to be an enhanced way of using less computation while at the same time minimizing the communication cost within the network [10].

As with any system, AES also has some issues regarding the analysis of its performance, even though it is widely used and highly secure. The first issue that arises is the consideration of various options – most notably, that between security and performance [11]. Optimizing the encryption rounds also improves the security of the system but at the same time also decreases the efficiency since there is need for more computational operations [12]. Thus, the main challenge in designing efficient AES implementations lies in maintaining an optimal level of security regarding the performance of the algorithms [13]. One of the major challenges that affect efficiency in AES is identified with key management and storage. Being an AES that operates based on the symmetric-key cryptography, the management and the storage of the encryption keys remain to be secure critical parameters [14]. It is mandatory that the generation, distribution and storage of the encrypted data are securely developed so that the unauthorized access can be effectively averted [15]. Further, the power of key selection contributes significantly to ironing out this confrontation since big key numbers allow for stronger encryptions, though it will be vane-white for a larger computation [16]. The objectives of this research are to provide clear insights about the performance metrics of AES such as execution time and energy consumption. These insights will help to select the suitable security solutions for current networks like IoT which has a limited resource. For example, some nodes in such networks doesn't have enough processing power to perform task like encryption, so it is crucial to decide a suitable algorithm that fit IoT requirements. In addition to test AES with real time data like the voice which require a speedy processing and less delay. By testing this algorithm, we can provide a real scenario and measure how it is suitable for current technology. The other objective of this work is to exploit the outcome in our upcoming research for enhancing AES performance by developing new encryption algorithm.

Therefore, AES has become an indispensable tool in modern cryptography and gives effective protection for the data in many applications. Analysis of the behavioral performance of AES makes it now possible to determine it's real-time performance and how well it can fit in different computer platforms. Current problems related to AES include the security-performance trade-off, key management, and differences in platforms; however, realizing the importance of AES in securing digital information in a world that is only growing more connected, researchers and innovators are actively working on improving AES even further.

The main contribution of this study, therefore, lies in the perspective of systematically considering AES in the field of voice encryption/decryption performance. Due to the specificity of voice data in which the nature of the communication is volatile and requires to be processed in real time and, moreover, for voice this pattern often differs from text it shows the directions to consider for adaptations in an AES implementation for voice communication systems. Also, the research provides a range of assessment criteria that may serve as substitutes for conventional encryption measures. It is far more detailed in terms of actual AES performance due to the comparison of throughput, latency, and energy consumption. This approach enhances organizations' ability to manage resources as well as design systems to support highly effective services.

2. RELATED WORK

There are many research works that have been done in this field which express the performance and the strength of a cryptographic algorithm. The paper in Gadhiya et al. [17], proposes a lightweight circuit, optimized for the AES encryption operation in the Internet of Things context. It does this by solving the resource limitations problem that is characteristic of most IoT devices by providing the manner in which the encryption activity will be done in the most efficient way possible.

The paper by Farooq et al. [18] presents an energy efficient AES deploying scheme suitable to Internet of Things (IoT), which is usually associated with devices containing ultra-low power microcontrollers. This is because IoT technology demands optimum power consumption especially in the devices used to support the network due to the limited sources of power such as batteries mainly embraced by the portable devices. The suggested implementation probably uses optimization techniques for the algorithm and low-power engineering strategies to reduce energy consumption within the encryption step. Thus, the research focuses on the enhancement of AES specifically for the low power consumption devices to increase the lifetime of IoT devices with secure protection. The aim of this work is to improve the sustainability and the lifetime of IoT application by alleviating

the energy overhead of cryptographic computations.

Several works on the enhancement of strategies pertaining to the AES encryption in IoT networks are examined by Qashou et al. [19]. It presumably includes studying the aspects like computational complexity, memory requirements, and power consumption to construct the specific optimization approaches. The study may have to examine the peculiarities of IoT devices in regard to their computational capabilities, storage, etc., in order to come up with efficient approaches to optimize the target framework. Thus, optimizing AES encryption and reducing the resource usage burden are the goals of the research targeting the performance issues unique to IoT environments. This work is relevant to enhancing the security of IoT devices because it addresses the problem related to the efficiency of cryptographic algorithms in conditions of limited resources of IoT devices.

Deepa et al. [20] are concerned with researching methods that address the enhancement of AES encryption speed in view of cloud computing application. This research probably includes comparing the impact of such factors as network delays, processing power, and bandwidth to the encryption capability of cloud supported systems. It could look into ways of improving the algorithms, concurrency or specific hardware techniques for improving AES encryption which are optimized for cloud architectures. The knowledge promotion of AES encryption efficiency in the cloud contributes to the objective of the research, which is to enhance secure data processing and communication in applications of cloud computing. The presented work has relevance to improving the general safety and quality of cryptographic processing in cloud-based systems.

Deepa et al. [20] and Hazzaa et al. [21] exposed how the authors focus on enhancing the lightweight and high-speed AES encryption in IoT systems. It may explore methods of enhancing the system's performance and increasing the efficiency of the encryption process without recalling a large amount of memory. The study deals with lightweight implementations to solve the resource limitation issue in IoT devices by allowing efficient encryption for security purposes. Furthermore, the emphasis is made on the speed of the research, and the objective is to guarantee that encryption operations do not introduce high delays to the IoT applications. This work helps in improving the security strategies for IoT implementations through presenting efficient and reliable encryption solutions that fits IoT networks.

Qashou et al [22] discusses the further work on the study of AES Encryptions approaches for many core architectures. It probably includes the study of parallelization approaches and the tasks' partitioning to take advantage of many-core systems. Thus, as many-core architecture takes advantages of the parallel processing nature, the study intends to improve the performance of AES encryption. This optimization endeavour may involve algorithmic enhancements, load Shedding and Balancing strategies together with memory efficiency that may be specific to many core technologies. Closely related to the topic, the research optimizes AES for many-core architectures, thus using the findings to improve the performance of cryptographic operations in the context of parallel computing.

Emin et al. [23] and Okoro et al. [24] established a new hardware design to provide optimum velocity and limited resources of AES encryption for IoT devices. It probably entails the determination of efficient hardware structures and circuits for AES encryption that can enhance the customary encryption rates and at the same time reduce power and area usage. Therefore, through simplistic concepts of power, the study seeks to enhance the speed of encryption procedures within the minimal IoT devices. This paper helps in enhancing the approaches used in IoT security by offering secure and efficient cryptographic solutions adaptable to resource-constrained IoT devices' architecture [25].

3. METHODOLOGY AND TESTING

The objective of this test is to employ the AES algorithm for encrypting and decrypting an audio file, with a focus on assessing the execution time and energy consumption. Initially, the code must initiate by reading the audio file, a process more intricate than reading standard data files due to the necessity of parsing the header to understand the file's attributes. Therefore, the program must first identify and interpret the header before proceeding to process the data accordingly. The header comprises various variables such as:

```
struct header_file
{
        char chunk_id[4];
        unsigned long chunk_size;
        char format[4];
        char subchunk1_id[4];
        unsigned long int subchunk1_size;
        short int audio_format;
        short int num_channels;
        unsigned long int sample_rate;
        unsigned long int byte_rate;
        short int block_align;
        short int bits_per_sample;
        char subchunk2_id[4];
        unsigned long int subchunk2_size;
} header;
typedef struct header_file *header_p;
```

These variables ascertain the file type and format, specifically the .wav format in our assessment. They encapsulate the initial 44 bytes of the audio file, delineating its voice characteristics. further exploration of additional file sizes is planned to be tested in the future to capture the performance and scalability of the algorithm for much smaller or larger data sizes, which could be crucial in IoT systems with highly variable data payloads. Furthermore, we can consider to test many file formats and different file types such as video or text file. The testing was conducted utilizing Visual Studio 2015 with C++ programming language on the laboratory's laptop computer, equipped with a Quad Core i7 processor and 8 GB of RAM. The original AES algorithm was employed to analyse audio files of various sizes. The audio file is stored on the computer's C drive, As delineated in the literature, the standard AES employs a single fixed S-box table within the SubByte transformation function. Table 1 has been utilized in this test.

Table 1. S-box

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1B	1E	87	E9	CE	55	28
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Upon executing the encryption program (source.cp) through the software, a command line prompt emerges, requesting the input of the main encryption key. The key utilized in this instance is:

Key: 5533 2987 4moo nuk7 8922 5863 kycn wb34

Following the entry of the key, with a length of 32 characters equating to 16 bytes, and pressing enter, the execution initiates the encryption process for the file. Thus, the resultant file generated during the encryption procedure will serve as the initial input file for the subsequent decryption operation. Here's the code snippet responsible for executing the encryption process on the input audio file:

```
for (i = 0; i<i_count; i += 16)
        {
                fread(State, sizeof(char), 16, Rfile);
                ENCRYPT();
                fwrite(State, sizeof(char), 16, Wfile);
                        }
  if ((meta->subchunk2_size % 16) != 0)
       //if the length less than 32 no padding the values stores as it is
                        {
  li = meta->subchunk2_size - i; //to get the number of bytes that are less of 32
                fread(Temp, sizeof(char), li, Rfile);
                fwrite(Temp, sizeof(char), li, Wfile);
       }
```

The test execution has been repeated multiple times to validate the accuracy of the outcomes. The average of the results has been computed, as demonstrated in the results section.

4. RESULTS

The tables below present the documented execution times and energy used in running the AES encryption and decryption operations on files of various sizes.

Table 2. Encryption time

Data Capacity	Pattern	Cipher Duration (Sec)	Decipher Duration (Sec)
128 Kilobytes	Human voice	0.477	0.462
540 Kilobytes		1.493	1.387
1Megabyte		2.787	2.668
1.48 Megabytes		4.078	3.885

Table 3. Encryption energy

Data Capacity	Pattern	Cipher Power Consumption (µW)	Decipher Power Consumption (µW)
128 K	Human voice	0.035	0.034
540 K		0.109	0.101
1 M		0.2	0.195
1.48 M		0.298	0.284

Table 4. Different pattern, (a) Time and (b) Energy

(a) Time

Data Capacity	Pattern	Cipher Duration (Sec)	Decipher Duration (Sec)
128 Kilobytes	Music	0.473	0.46
540 Kilobytes		1.4851	1.3829
1.48 Megabytes		4.02	3.82

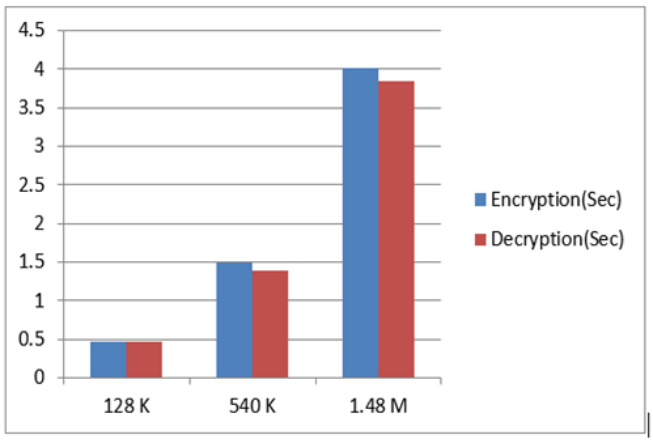
(b) Energy

File Size	Pattern	Cipher Power Consumption (µW)	Decipher Power Consumption (µW)
128 KB	Music	0.0341	0.034
540 KB		0.108	0.101
1.48 MB		0.293	0.280

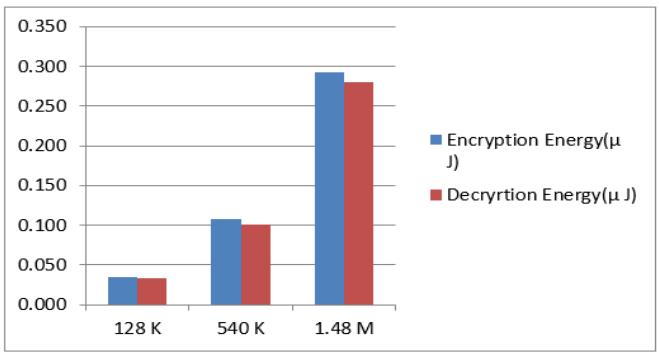
Table 2 displays the execution times of an unchanged AES algorithm in the encryption and decryption of audio files of different lengths. The standard times varied between the fastest of 0.477 seconds (obtained using a 128 KB file size) to the slowest of 4.078 seconds (achieved with 1400 KB file size, the largest tested). In addition to that the table indicated rate(s) in each file. Table 3 shows the energy consumption of AES during a process performed. The highest energies associated with generated (0.2978 nJ) and encrypted (0.284 nJ) cryptograms were measured. This relates to the point where a file of 128 KB only consumed as little as 0.035 micro-Joule.

Table 4 indicating the parameters, the conclusions resume themselves. In fact, they were quite similar, the results from both exams. The statistical Figure 2(a) and Figure 2(b) provided offers an insight into the encryption and decryption processes within the AES algorithm, revealing a notable similarity in the time required for both operations. This remark highlights AES's ability to encrypt and decrypt data well and . When we encrypt, we change normal data into coded data with a special process and a secret code, which helps keep the

information safe. However, decrypting means we do the opposite. We turn coded data back into its original form often using the same process and code. Seeing that it takes about the same amount of time for both shows AES works just as good no matter what we're doing to the data. This means it's strong and trustworthy for keeping important information safe. This point matters a lot for apps that work in real-time because having encryption and decryption that's fast and even is key for keeping chats smooth and data security. By providing empirical evidence of AES's performance parity between encryption and decryption, the statistical figure strengthens the understanding of its effectiveness in various cryptographic applications and reinforces its status as a cornerstone of modern cryptography.



(a) Execution time



(b) Energy consumption

Figure 2. (a) Execution time for encryption and decryption at different data sizes (128 K, 540 K, and 1.48 M); (b) Energy consumption during encryption and decryption for the same data sizes

The results demonstrate that both encryption and decryption time, as well as power consumption, increase predictably with larger file sizes, but show minimal variation between different content patterns (human voice vs. music). For instance, a 1.48 MB file takes approximately 4.078 seconds to encrypt and consumes 0.298 µW for human voice, while music shows similar values (4.02 seconds and 0.293 µW). These results indicate that the algorithm's efficiency is driven primarily by file size rather than content type, making it suitable for general-purpose encryption. The minor differences suggest the algorithm is energy-efficient and time-effective across various data forms.

4.1 Security analysis

This section explains why cryptographers label AES as a highly secure system. Though the section as a whole imparts safety, it is essential to mention that the following will present a more comprehensive safety elaboration and a comparison with this chapter. Also, in this section, the security levels like binary histogram, Frequency test, and entropy are reviewed in detail. Table 5 demonstrates the encrypted file's Entropy Test results (AES standard). The AES standard achieved a remarkable result of 7.99 points, close to 8 points, the maximum possible.

The illustration below highlights the security analysis run on the file using the conventional version of the AES algorithm. The Binary Histogram for the starting audio file and the unencrypted Cipher file is demonstrated in Figure 3. The manifestation of this fact has been transformed with encryption and has led to significant progress in the ratio of ones and zeros.

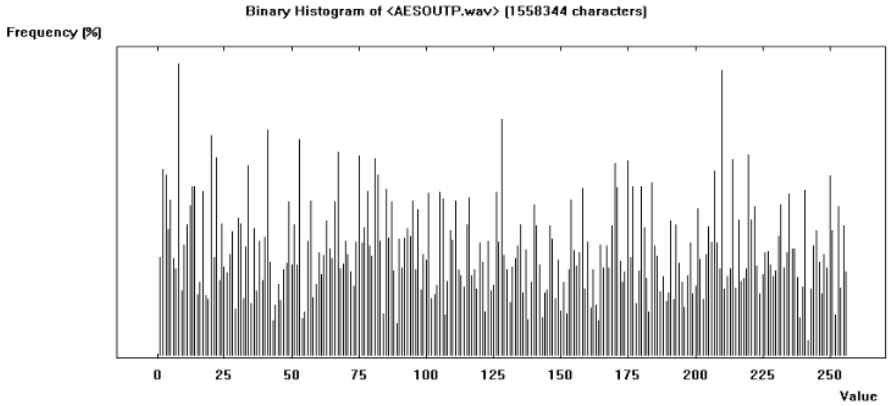
Table 5. Entropy

Audio File	Plain Entropy	AES Cipher Entropy	Max Possible Entropy	Possible Byte Value
Test	7.79	7.99	8	256
Teaching	5.65	7.99	8	256
Washing	5.4	7.99	8	256
Computer	5.13	7.99	8	256

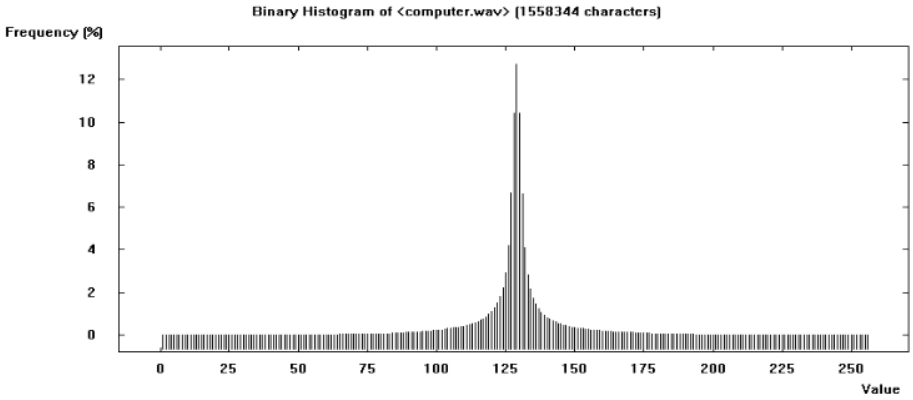
Figure 4 provides the floating frequency values for plain and encrypted message files using AES. Depicts the patterns observed for the encrypted file. The frequencies for this file were between 50 and 60, similar to the pattern depicted in the figure for the original file, which was between 10 and 55. The randomness built-in in the standard AES algorithm is shown, making the formula for mixing the cipher and the plain text most efficiently challenging. The standard AES algorithm presents a high level of security, and it can clear be seen from the study and literature review.

Figure 5 indicates the cipher's autocorrelation after the AES algorithm crypto test. These reports will be integrated into the main text to support the discussed developments. Autocorrelation, in the context of signal processing or cryptography, refers to the correlation of a signal with a delayed copy of itself over time. It measures the similarity between a signal and a delayed version of itself. The autocorrelation analysis provides insights into the behaviour of the AES cipher post-crypto test, aiding in unde rstanding its performance and effectiveness in voice encryption and decryption scenarios Adding these results to the main discussion makes it better by showing real examples of how the code works. It also shows what this means for the safety and how well communication systems work. Before continuing more trials examined the strength of the encryption way. Poker tests and brute-force attacks on the scrambled audio were part of these. Both tests got a pass, as shown in Figure 6.

The tests we did before this show that AES is safe to use. It's hard to break because it mixes stuff up and spreads them out well. Also, we saw a lot of random things in the parts we looked at before, which means AES is pretty strong when it comes to security. Plus when we checked how well AES works, we found out it uses resources the right way, makes security better, can handle more work if needed, is good with money, and follows the rules in communication systems.

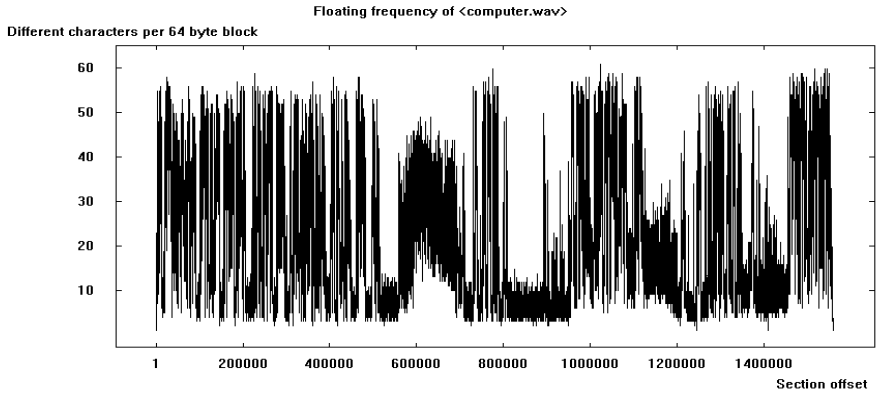


(a) Plain voice file

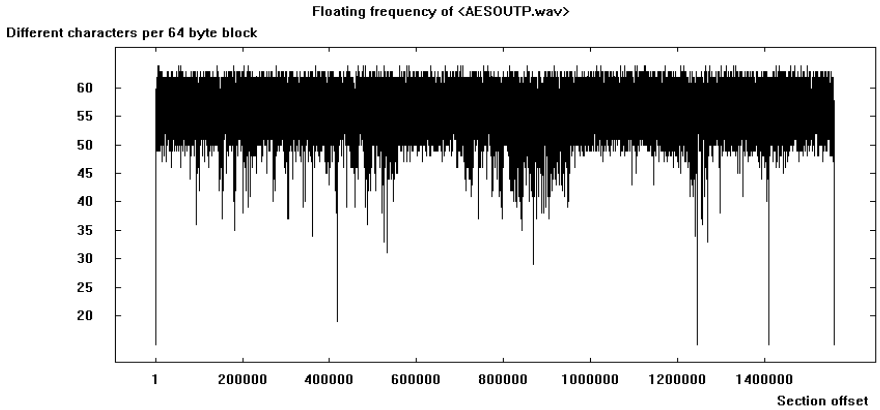


(b) Cipher voice file by AES

Figure 3. Binary histogram



(a) Plain



(b) Cipher

Figure 4. Floating frequency

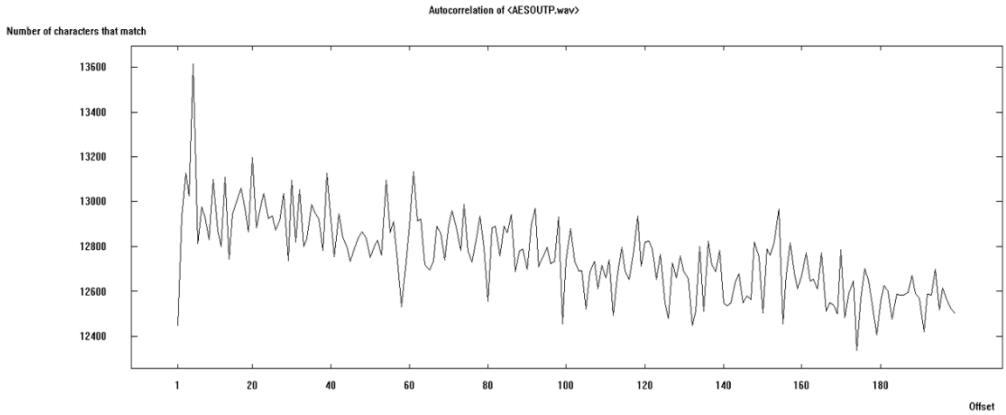


Figure 5. Autocorrelation

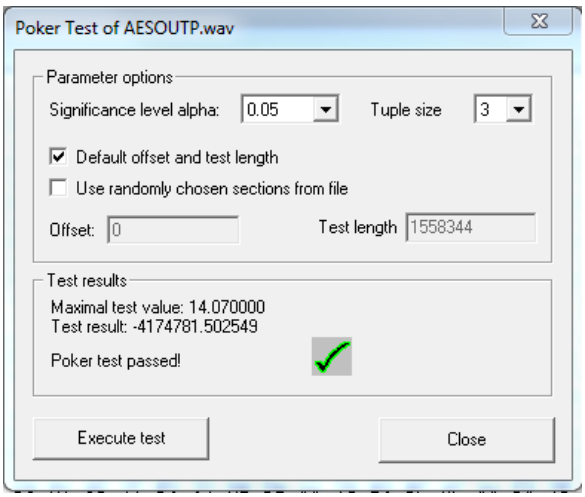


Figure 6. Poker test

Further descussion can be sumerise as evaluation here:

The research demonstrates that the encryption algorithm scales well with file size, maintaining consistent performance across different content types. This makes it suitable for general-purpose applications where time and energy efficiency are crucial, such as mobile devices or IoT systems. However, as file sizes increase, the linear rise in encryption time could be a limitation for real-time applications. Although energy consumption remains low, further optimizations may be needed for ultra-low-power environments. Future improvements should focus on reducing encryption time for larger datasets and testing the algorithm with other data types to ensure broader applicability and performance enhancements.

5. CONCLUSIONS

The Advanced Encryption Standard (AES) works well to keep data safe in many areas. This report's detailed look at how AES works to protect voices shows it does a good job at keeping important info safe. Groups can make sure talks are safe and run well by looking at things like how fast it locks down data how much stuff it needs, and if it can handle a lot of work. Even though it's tough to get the right mix of being safe and working fast handle keys well, and work with different platforms, this study shows that AES works the same way for all kinds of voice sounds. Doing these kinds of studies helps not just to use resources the best way and make things more secure but also to grow, save money, and follow the rules in today's talk systems. The outcome of this work demonstrates useful insights for wireless IoT network with constrained resources since it can balance quality of service and security in a significant approach. It is especially appropriate for wireless IoT devices/nodes, having restricted resources, deployed in smart cities.

Future research could focus on refining AES performance metrics and algorithms for voice encryption, balancing security and real-time requirements. Optimizing AES implementations for voice communication systems may enhance transmission efficiency and security in dynamic network environments. Additionally, exploring AES resilience to emerging technologies like quantum computing ensures long-term data protection in evolving landscapes. Integrating advancements in AES with real-world applications can further fortify voice communication security while improving user experience.

ACKNOWLEDGMENT

The authors thank the Higher Education and Scientific Research ministry in Iraq for support and fund this research in addition to thank the anonymous reviewers forgiving their valuable comments and helping us to improve the quality of the paper.

REFERENCES

[1] Tripathy, T., Mishra, A., Khan, R. (2024). A comparison analysis of cryptographic methods in sustainable healthcare. In Healthcare Analytics and Advanced Computational Intelligence, CRC Press, pp. 56-77.

[2] Kanimozhi, S., Logeshwaran, M. (2023). Advanced encryption standard to prevent intruders in email through cloud environment. In 2023 2nd International Conference on Applied Artificial Intelligence and Computing (ICAAIC), Salem, India, pp. 1183-1189. https://doi.org/10.1109/ICAAIC56838.2023.10140373

[3] Parekh, A., Antani, M., Suvarna, K., Mangrulkar, R., Narvekar, M. (2024). Multilayer symmetric and asymmetric technique for audiovisual cryptography. Multimedia Tools and Applications, 83(11): 31465-31503. https://doi.org/10.1007/s11042-023-16401-x

[4] National Institute of Standards and Technology (NIST). (2001). FIPS PUB 197: Advanced Encryption Standard (AES). Available online:

https://csrc.nist.gov/publications/detail/fips/197/final.
[5] Shawkat, S.A., Al-barazanchi, I. (2022). A proposed model for text and image encryption using different techniques. TELKOMNIKA (Telecommunication Computing Electronics and Control), 20(4): 858-866. https://doi.org/10.12928/TELKOMNIKA.v20i4.23367
[6] Al Barazanchi, I.I., Hashim , W. (2023). Enhancing IoT device security through blockchain technology: A decentralized approach. SHIFRA, 2023: 1-8. https://doi.org/10.70470/SHIFRA/2023/002
[7] Hazzaa, F., Shabut, A.M., Ali, N.H.M., Cirstea, M. (2021). Security scheme enhancement for voice over wireless networks. Journal of Information Security and Applications, 58: 102798. https://doi.org/10.1016/j.jisa.2021.102798
[8] Burhanuddin, M. (2023). Assessing the vulnerability of quantum cryptography systems to emerging cyber threats. SHIFRA, 2023: 1-8. https://doi.org/10.70470/SHIFRA/2023/004
[9] Aljohani, A. (2023). Zero-trust architecture: implementing and evaluating security measures in modern enterprise networks. SHIFRA, 2023: 1-13. https://doi.org/10.70470/SHIFRA/2023/008
[10] Feng, Z.L., Johnson, M., Brown, E. (2021). Energy-efficient AES encryption algorithm implementation based on ultra-low power IoT processor. IEEE Transactions on Circuits and Systems I: Regular Papers, 68(12): 4921-4931.
[11] Hashim, W., Hussein, N.A.H.K. (2024). Securing cloud computing environments: An analysis of Multi-Tenancy Vulnerabilities and Countermeasures. SHIFRA, 2024: 9-17. https://doi.org/10.70470/SHIFRA/2024/002
[12] Al-Tamimi, A.Y., Snober, M.A., Al-Haija, Q.A. (2023). A performance evaluation study to optimize encryption as a service (EaaS). In Proceedings of Fourth International Conference on Communication, Computing and Electronics Systems, Singapore: Springer Nature Singapore, pp. 681-691. https://doi.org/10.1007/978-981-19-7753-4_52
[13] Gamboa-Sánchez, M.C., Cotrina-Teatino, M.A., Vega-Gonzalez, J.A., Noriega-Vidal, E.M., Arango-Retamozo, S.M., Marquina-Araujo, J.J. (2024). Effective critical risk management in welding operations for mining: A case study on incident reduction. International Journal of Safety and Security Engineering, 14(4): 1039-1047. https://doi.org/10.18280/ijsse.140403
[14] Abdallah, A.A., Abdallah, M.S.E.S., Aslan, H., Azer, M.A., Cho, Y.I., Abdallah, M.S. (2024). Enhancing mobile ad hoc network security: An anomaly detection approach using support vector machine for black-hole attack detection. International Journal of Safety and Security Engineering, 14(4): 1015-1028. https://doi.org/10.18280/ijsse.140401
[15] Agalit, M.A., Idrissi Khamlichi, Y. (2024). Optimization of intrusion detection with deep learning: A study based on the KDD Cup 99 database. International Journal of Safety and Security Engineering, 14(4): 1029-1038. https://doi.org/10.18280/ijsse.140402
[16] Ibrahim, A.A., Johnson, L., Smith, M. (2021). High-speed and resource-efficient AES encryption hardware for IoT devices. IEEE Internet of Things Journal, 8(16): 12909-12920.
[17] Gadhiya, N., Tailor, S., Degadwala, S. (2024). A review on different level data encryption through a compression techniques. In 2024 International Conference on Inventive Computation Technologies (ICICT), Lalitpur, Nepal, pp. 1378-1381. https://doi.org/10.1109/ICICT60155.2024.10544803
[18] Farooq, A., Tariq, S., Amin, A., Qureshi, M.A., Memon, K.H. (2024). Towards the design of new cryptographic algorithm and performance evaluation measures. Multimedia Tools and Applications, 83(4): 9709-9759. https://doi.org/10.1007/s11042-023-15673-7
[19] Qashou, A., Yousef, S., Sanchez-Velazquez, E. (2022). Mining sensor data in a smart environment: A study of control algorithms and microgrid testbed for temporal forecasting and patterns of failure. International Journal of System Assurance Engineering and Management, 13(5): 2371-2390. https://doi.org/10.1007/s13198-022-01649-7
[20] Deepa, M., Varssha, B., Abinaya, E., Ajitha, S., Dhaarani, S., Sharmila, K.A. (2023). An efficient implementation of AES algorithm for cryptography using CADENCE. In 2023 7th International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India, pp. 1478-1484. https://doi.org/10.1109/ICECA58529.2023.10395793
[21] Hazzaa, F., Yousef, S., Ali, N.H., Sanchez, E. (2019). The effect of nodes density on real time traffic in mobile Ad Hoc Network. In 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3), London, UK, pp. 209-212. https://doi.org/10.1109/ICGS3.2019.8688314
[22] Qashou, A., Yousef, S., Okoro, A., Hazzaa, F. (2023). Microgrid testbed for temporal forecasting patterns of failure for smart cities. Technology and Talent Strategies for Sustainable Smart Cities: Digital Futures, pp. 189-227. https://doi.org/10.1108/978-1-83753-022-920231010
[23] Emin, T., Akram, Q., Nezihe, Y. (2013). Shunt active power filters based on diode clamped multilevel inverter and hysteresis band current Controller. Innovative Systems Design and Engineering, 4(14): 1-17.
[24] Okoro, A.S., Yousef, S., Qashou, A. (2023). Investigating gesture control of robotic arm via lora technology for smart cities. In Wireless Networks: Cyber Security Threats and Countermeasures, pp. 71-101. https://doi.org/10.1007/978-3-031-33631-7_3
[25] Hazzaa, F., Yousef, S., Sanchez, E., Cirstea, M. (2018). Lightweight and low-energy encryption scheme for voice over wireless devices. In IECON 2018-44th Annual Conference of the IEEE Industrial Electronics Society, Washington, DC, USA, pp. 2992-2997. https://doi.org/10.1109/IECON.2018.8591451