International Journal of Informatics and Communication Technology (IJ-ICT)
Vol. 15, No. 3, September 2026, pp. 1263~1271
ISSN: 2252-8776, DOI: 10.11591/ijict.v15i3.pp1263-1271

Advanced encryption standard with asymmetric key exchange for text encryption

Ravindra K Reddy, Vijayalakshmi P
Department of ECE, VISTAS, Chennai, India

Article Info

Article history:

Received Sep 23, 2025
Revised May 18, 2026
Accepted Jul 5, 2026

Keywords:

Advanced encryption standard
Cryptography
Decryption
Elliptic curve encryption
Encryption
Security

ABSTRACT

When creating communication systems, securing data is crucial and improved randomization in creating secret keys contributes to more secure systems. Unfortunately, the symmetric ciphers used for data encryption, such as the advanced encryption standard (AES), may be subject to attacks that exploit timing measurements to deduce the secret key used for encryption, resulting in a significant lack of research on the security of hybrid implementations (usually defined as incorporating AES and asymmetric ciphers) for AES encryption. We introduce a new hybrid encryption method that combines the AES encryption standard with elliptic curve cryptography (ECC). In this hybrid form of encryption, ECC is utilized to facilitate secure encryption and transmission of the AES key and cycle through 16 rounds of AES to encrypt the majority of the data. We provide a performance comparison between the new algorithm and the AES-128 encryption standard. Our findings indicate that the new hybrid encryption method produced an average encryption time of 0.0002 seconds for 10MB files, significantly faster than the AES-128 encryption standard, which takes an average of 0.0016 seconds. The new hybrid method exhibits significant resistance to cryptanalytical attempts, experiencing an average avalanche effect of 49.84%, while maintaining the AES nonlinearity value at 112. As such, we conclusively state that the new hybrid encryption method utilizing ECC and AES will provide effective security for user data against timing side-channel attacks while remaining an efficient method for performing encryption.

Corresponding Author:

Ravindra K Reddy
Department of ECE, VISTAS
Chennai, Tamil Nadu, India
Email: ravindra.kalvapalli@gmail.com

1. INTRODUCTION

Information security is a key factor in the growth of e-commerce and the protection of data. Cryptography is a means to protect data [1]. We maintain and control the confidentiality of data, and the advanced encryption standard (AES) is a common standard in these scenarios [2]. Symmetric key encryption is capable of handling large amounts of plaintext. The key management scheme of elliptic curve encryption (ECC) makes it more viable for key encryption and digital signatures, which is why the paper proposes a hybrid model. The proposed method uses ECC or to send and encrypt keys to an AES with a symmetric scheme.

The approach related to side-channel attacks relies on exploiting problems with the execution of the algorithm(s) rather than the mathematical exploitation of the algorithm through standard cryptanalysis. Side-channel attacks take advantage of information leaked from timing, radiation emissions, power usage,

cache content, and other non-mathematical sources. In the case of AES, this is primarily accomplished through the use of multiple table lookups, where each lookup provides a quick method of processing an AES operation, and these are called table "hits". The hits can switch between a hit in the cache and a miss in the cache depending upon the source of the information (the plaintext) and the key (the secret key) that is input to the AES encryption scheme [3]. Thus, because side-channel attacks depend on correlating the data that has been leaked and the sensitive data (which has not been leaked), common countermeasures to these attacks can be placed into two categories [4]: either the leakage of the data can be prevented, or the relationship between the two can be eliminated [5].

The purpose of this study is to create a viable solution for addressing the data security issues/problems presented by algorithms which are impacted by Side Channel Attacks. In other words, we intend to utilize ECC technology to create an obfuscated AES Key, so that there will be no requirement to send (transmit) a private secret key prior to exchanging the obfuscated AES Key. The combination of using an AES-ECC Hybrid Cipher will not only provide a method for addressing data security issues but will also simplify the management of keys for communication systems [6]. This research's main goal is to create a Hybrid Encryption Algorithm combining AES & ECC. The Combiner has encrypted keys that facilitate a secure key exchange, providing an added level of protection of the ciphertext generated [7]; the research will also create Cache Timing Attacks to identify challenges and provide Countermeasures. To Reduce Workload when using front-end functions, encrypt only the key used to execute AES and not the entire data block using ECC. The project also examines Timing-based Countermeasures for neutralizing side-channel timing attacks that could provide access to the keys used to encrypt the data.

2. RELATED WORKS

There have been many studies on the Security of the AES and its Implementation in the cloud and the internet of things (IoT). In the last several years, a comprehensive review of the literature has indicated that although AES continues to be the standard for symmetric encryption, it continues to be more likely to be exploited through side channel attacks when implemented in hardware-sharing environments [8]. Cache timing attacks exploit the relationship between the time required to encrypt data and the cache hits/misses; thus, deducing the private key. The fundamental studies have indicated that the vulnerabilities highlighted above exist because the table look-up process will overflow the size of cache memory; and, as such, the time it takes to perform lookups will depend on the type of text & key used in encryption [9]. In addition, various researchers have demonstrated how deep learning models efficiently create AES side-channel attack vectors [10], [11]. This proves that on a standard level, AES implementations need tremendous hardening from contemporary cryptanalysis methods. Researchers have turned to hybrid cryptosystems as the solution for mitigating vulnerabilities. Several initial proposals for hybrid encryption algorithms combined the improved performance of AES with the security advantage of ECC, thereby enhancing performance and security. More recently, there have been several studies focusing on cloud storage applications. Studies on oracle cloud infrastructure, for example, have shown that combining a symmetric speed advantage with an asymmetric key exchange significantly boosts throughput [12]. Validation efforts made on various intelligent information services platforms have proven to enhance the security of communication without requiring the consumption of computational power needed to implement a full-blown public key infrastructure system [13]. There is evidence that hybrid AES-ECC implementations improve data security, in addition to improving throughput, specifically in cloud storage environments [14]. Unfortunately, Hybrid Solutions have high latencies when applied to large datasets or resource-constrained devices. As mentioned earlier, standard AES implementations use a 128-bit key fortress and employ ten rounds of encryption; however, attempts made in the past to increase the security level of AES by increasing the size of the key or number of rounds (i.e., 192 bits) primarily have resulted in unacceptable performance drops on 8-bit and/or legacy microcontrollers [15].

3. METHOD

The hybrid AES-ECC algorithm aims to offer a two-pronged security mechanism that aids in protecting both the message content and the encryption keys. The hybrid method uses the advantages of symmetric and asymmetric cryptography in tandem to lessen the processing burden that goes along with implementing public-key infrastructures. The sequence of operational flow encompassing the proposed method is enclosed in the stepping procedure below, and the transition from plaintext to the final cipher block is also outlined.

3.1. The proposed research encompasses the following key aspects

AES employs substitution and permutation networks. The data blocks can be modified to specific lengths. AES allows three key lengths. The number of bits corresponds to the number of iterations: 10, 12, or 14 rounds, respectively. The AES structure can be understood based on three basic components: Key expansion, round transformation, and iteration. Each round transformation was comprised of three layers: a non-linear layer, a linear mixing layer, and an add-round key layer. The entire process is shown in Figure 1.

Every cycle comprises the subsequent set of four procedures:

- Sub bytes transformation: The substitution box takes each byte from the state matrix with an alternative byte. The application of an affine transformation is needed to establish the S-box.
- Shift rows transformation: The first rows of the state's bytes remain the same. The second, third, fourth, and fifth row have left shifts of one, two, three, and four bytes.
- Mix columns transformation: In this phase, the bytes in each column are combined to perform state multiplication. The cipher text's arrangement is altered even if all the bytes are the same. The Mix Columns operation of step 2 does not have an inverse polynomial matrix.
- Add round key transformation: This transformation involves incorporating a round key into the state through a bitwise XOR operation. This process is executed segment by segment. Additionally, each state in the column matrix is combined with a round key word. This final stage of AES entails a matrix addition operation.

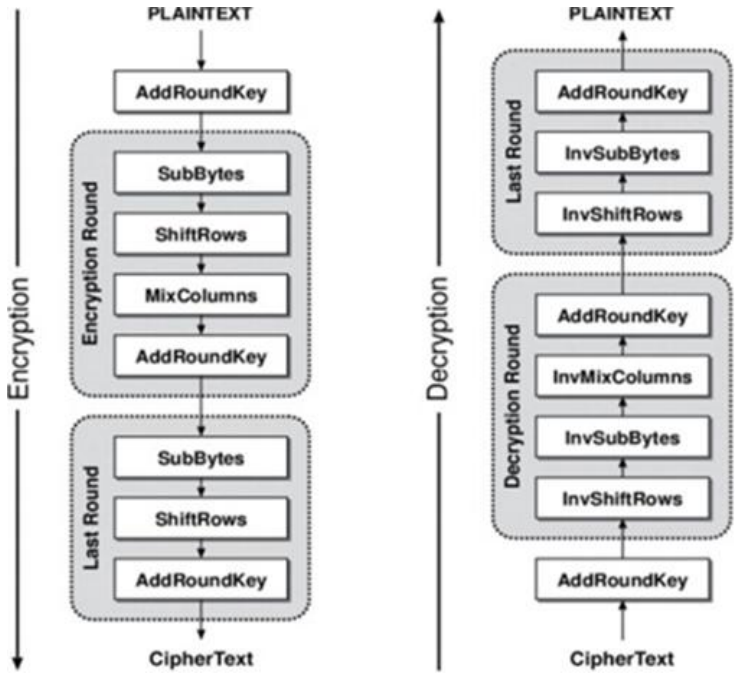

Figure 1. Basic operation of the advanced encryption standard

3.1.1. The proposed research encompasses the following key aspects

i) Enhanced AES algorithm implementation, the AES is a symmetric encryption calculation, utilizes a progression of table look-ups to improve its performance. However, these tables exceed the cache's capacity, leading to cache hits and misses during encryption. This, in turn, results in varying lookup times and encryption durations that are influenced by both the input text and the encryption key. These attributes make AES susceptible to Cache Timing Attacks, which exploit the correlation between timing patterns for encryption under known and unknown keys to deduce the unknown key. ii) Hybrid AES-ECC encryption scheme, this work proposes an augmented AES algorithm for plaintext encryption. Furthermore, the ECC algorithm will be utilized to encrypt the AES key. This dual-layer encryption strategy enhances the overall security of the system. The key objective is to fortify the system against potential vulnerabilities stemming from timing side channel attacks. iii) Software-based countermeasures, to mitigate the potential weaknesses presented by timing side channel assaults, this research aims to implement software-based countermeasures. These countermeasures will be strategically designed and integrated into the system to safeguard against the exploitation of timing-related vulnerabilities. iv) Enhanced efficiency through higher

order AES, to optimize the efficiency of data encryption, an advanced version of AES will be employed. This higher-order AES variation will highlight a bigger key size of 192 pieces and include 16 rounds of emphases, as opposed to the standard AES model, which has a critical size of 128 pieces and 10 rounds of cycles. Recent hybrid AES-ECC implementations demonstrate improved data security and throughput in cloud storage applications. This enhanced AES configuration aims to further elevate the security and efficiency of the encryption process. The proposed research will contribute to the advancement of encryption techniques by combining an improved AES algorithm, ECC for key encryption, and effective software-based countermeasures. Moreover, the introduction of a higher-order AES variant is anticipated to provide enhanced security and efficiency for data encryption.

3.2. Proposed algorithm

a. The user's intended data block undergoes encryption to ensure security.
b. The data encryption employs the AES algorithm.
c. The AES-generated key undergoes an additional layer of security through elliptic curve cryptography encryption.
d. The resultant key is sent to the client, who will utilize it to unscramble the AES key block during the decoding stage.
e. The total encryption duration for the data block is computed and archived.
f. Following AES key decoding, the encoded information is then unraveled utilizing the AES key block, reestablishing it to its unique arrangement for client access.
g. The attacker module computes response times of encrypted outputs from the server by employing a range of random keys alongside a valid key.
h. The attacker module's correlation program analyzes timing details for both scenarios, generating a potential key space based on these timings. This key space aids in deducing the accurate key combination [16].

3.3. System architecture

In Figure 2, the plain text will be given as input to the cipher, and the key will be created through the properties of an elliptic bend condition rather than the conventional strategy for age as a result of huge indivisible numbers, the plain text will be ciphered [17].

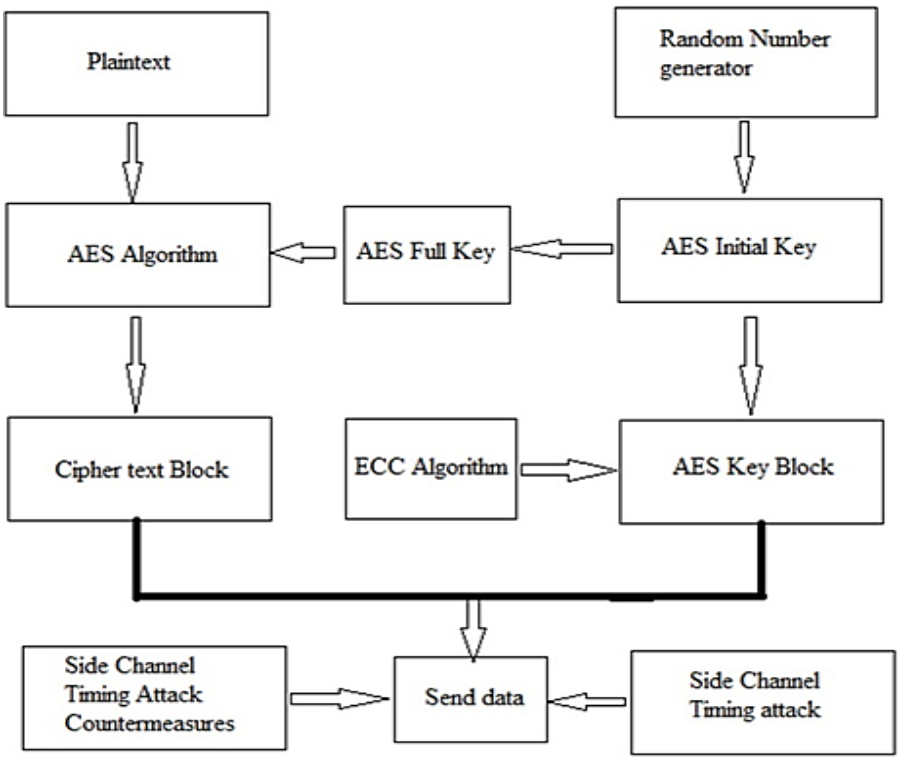

Figure 2. Flowchart of system architecture

4. RESULTS AND DISCUSSION

Encompassing the encryption process applied to a textual document. This encryption employs the advanced encryption standard with a key length of 192 bits, as specified by the user. Additionally, 16 iterations of AES are employed. The subsequent illustrations portray the progressive outputs of each encryption round.

To evaluate the effectiveness of the suggested hybrid framework, a number of experimental simulations were performed using different file sizes of 10MB to 100MB. The focus of these experiments was on encryption throughput, decryption efficiency, and total time of computation. The following test cases illustrate how plaintext is transformed into ciphertext using the 192-bit AES-ECC hybrid mechanism.

Test case1:
Original plaintext:
The high level Encryption Standard is the most regularly involved encryption algorithm on computers and over the web.
Encrypted data:
U2FsdGVkX19FEeLyrVE3TOzbvw0qRl/4gwpPusWnJXpkwR2PoBpzzfxylCosGRXrZ54dZKiP7TA/+Qiyh
eyhalSRFI3c1/T0m2keVwzy5qIXtPeNp9OQjsJMahiKLvLmvVxw4oZxJ1XuGgjY/wGmqIuINN8rYMBvjt2
HRuBrMR2sNrFluLz3lS3uGG4A2ws2
Decrypted plaintext:
The Advanced Encryption Standard is used on computers and over the internet.
Test case2:
Original plaintext:
The high level encryption standard (AES) remains a strong symmetric key calculation, saddling various table look-ups to streamline its exhibition. Store Timing assault is a weakness, it exploits timing designs during encryption with a known key to derive an obscure key. To address this concern, this study presents an expansion of a public-key crypto system to oblige a combination private-key system.
Encrypted data:
U2FsdGVkX1/INyx8U+9XW+DpfEaqJPtqgfHSsGxka+r7q+jD5//ELDX+P54aWmSW/YLzAnZdyid6skkEZ
F8ehXuRwCED8MGAFeo8ESLuwqFNjQCU+gQMDEnXQh7WnKRvLixQ5CoOxET8Wo3UcPpDjLDpW
W8xLPVGAzn27bEV8iA5nHx8jf23ZGtDIwp6ayzzdMGH97VNNxqku28OONxVLQhsQ6GwtqexMmPSTl
DMK6tTAnyauU+a2v/YZ0jsCCuZj0zWlgqSRyTPsdGlU7knO7RL0Gfeh/Iz0WvDdP9Ijsdgml4ZVmW9EQ
LO6q6sYf/cELjROdnFDbB0BNXw6NXoqnU7lYZ1vStGrLCLO3n8BQJ276A/vTx/mRSn7hjNvxeOy4W9B
2Y1wFil40RmAtXLwAZatcMewYmVzufBjBYl9Xbg34N/c0xvKR/1itwQyYVtRwmrPpYk4ELBgX8mhidP
8eASZmToGbSQJHDe6SiOqQUcT4adYnUsdpuDhdmewvuCC3gMcHDBfnH6ELRI5PR5+zDs4m2OMKU
5fEoPsPfvYD1o+pZst/5eByJo9Ns7Q77V8EENA6p2Hxt0l5JveQd/RwUU39dpOGejIZ6myFFVaMxEpCBY
WdH6C9zsnNX+9L+7uIqqMndOC71kQB3iLq/CrXG9bfD/0Ww9cvttYwH8a6E92HUQ+up3QNcHUqXS6
ocJal+fiEfq738aaJSzZVhHCOJ5uD/mqe8jzRUv4FBpt0ZyP+qFt7lYG/MLAfXDLlCi
Decrypted plaintext:
The AES remains as a strong symmetric key cryptographic calculation, saddling various table look-ups to upgrade its exhibition. One critical weakness is the Reserve Timing Assault, which exploits timing designs during encryption with a known key to find an obscure key. To address this concern, this study presents an improvement of a public-key cryptosystem to oblige a crossbreed private-key cryptosystem, perfectly blending the characteristics of the great level encryption standard and elliptic curve cryptography.

4.1. Performance measure

Numerous metrics gauge "performance" corresponding to the various platforms available for measurement. AES is expected to excel across all these standards. Our focus lies on both the frequently used and overarching criteria. Approaches employed by the contestants with regard to key lengths and performance are [18]:

- Certain algorithms exhibit reduced speed with larger key sizes.
- Several algorithms experience slower key setup as key sizes increase.
- Certain algorithms demonstrate decelerated key setup and encryption processes with larger keys.
- Certain algorithms maintain consistent speeds and key setup regardless of key sizes.
- Interestingly, one algorithm showcases slower key setup with smaller keys.
- Next-generation side-channel analysis based on deep learning models, specifically with convolutional neural networks (CNNs) took this need for stronger encryption into even more detail [19].

4.2. Comparing speed across various input text lengths

Table 1 illustrates the speed of the proposed algorithm, and the results of these proposed schemes show that the ECC-AES approach took less time to protect data than other approaches, as shown in Figure 3. The ECC-AES scheme has characteristics that make it robust against attacks and increase the complexity. It can be seen that the proposed algorithm's time for Encryption is much shorter than other ones. Our computational cost is reduced when the time for encryption is reduced. Our approach is more effective than others. The table shows how long it takes for various ciphers to be deciphered.

A comparative performance analysis, detailing encryption time using the standard AES-128, standard AES-192, and the proposed Hybrid AES-ECC framework, is displayed in Table 2. As demonstrated, the standard AES-192 shows a slight increase in encryption time (20% overall increase in encryption time) compared to AES-128, which is expected given the computational overhead of two more rounds (12 total rounds) of processing time. The Proposed Hybrid algorithm achieves significantly greater efficiencies with both standard AES processes. The efficacy of the Hybrid design is due to the ability to constrain the computations associated with ECC encryption to just a small key block and to keep the main bulk data encryption optimally fast thus minimizing overall encryption time while keeping latency low.

A graphical representation of the encryption and decryption performance relative to file size is provided in Figure 3. As observed, the time increases linearly with data size, demonstrating the algorithm's stability. To provide statistical certainty, several tests were performed on the Hybrid System, and the numbers listed represent the modeled average(s) for all setups [15]. The overall efficiency found in the Hybrid Model is due in large part to the inherent parallel processing capability of AES and modern-day CPUs using the AES New Instructions (AES-NI) provide an even greater level of speed and performance to process all the operations involved with implementing the Hybrid Method [20], [21], enabling processors with AES-NI Hardware Support to achieve significant performance leaps over software implementations, whether it be accelerated or unaccelerated [22].

Table 1. Speed of the proposed algorithm

Text size (MB)	Time in seconds					
	Proposed algorithm		AES(128bit key)		AES+Blowfish(128bit key)	
	Decryption	Encryption	Decryption	Encryption	Decryption	Encryption
10	0.0002	0.0002	0.000174	0.001642	0.000460	0.001850
25	0.0005	0.00045	0.000309	0.001850	0.000887	0.002030
50	0.0009	0.00085	0.000443	0.002045	0.001050	0.002350
75	0.0014	0.00135	0.000652	0.002256	0.001554	0.002567
100	0.00185	0.0017	0.000851	0.002563	0.001978	0.002814

Table 2. Encryption time comparison analysis (AES-128 vs. AES-192 vs. Hybrid)

Data size (MB)	Standard AES-128 (s)	Standard AES-192 (s)	Proposed hybrid AES-ECC (s)
10 MB	0.001642	0.001970	0.000200
25 MB	0.001850	0.002220	0.000450
50 MB	0.002045	0.002454	0.000850
75 MB	0.002256	0.002707	0.001350
100 MB	0.002563	0.003076	0.001700

4.3. Security analysis

A block cipher is said to exhibit an 'Avalanche Effect' when the difference (the 'Hamming Distance') between two ciphertexts generated from messages differing by a small amount (e.g., one bit) is as large as possible. Ideally, if 'K' is the single-digit change, K should change approx. 50% of the ciphertext digits.

4.3.1. Avalanche effect analysis

We have evaluated the 16-round AES algorithm as proposed, and in each of five tests carried out, a single bit (one bit) was inverted in the plaintext. We then recorded how many bits in the resulting ciphertext were different from the original ciphertext and calculated the Hamming distance (the number of bits that differed) between the two. The results of this study are detailed in Table 3.

The results presented in Table 3 indicate that the proposed AES algorithm had an average avalanche effect of 49.84%, which is remarkably close to the ideal of 50%. These findings support our hypothesis that the addition of more rounds will distribute differences throughout the entire ciphertext, creating an unpredictable cryptographic function that will be resistant to statistical attacks.

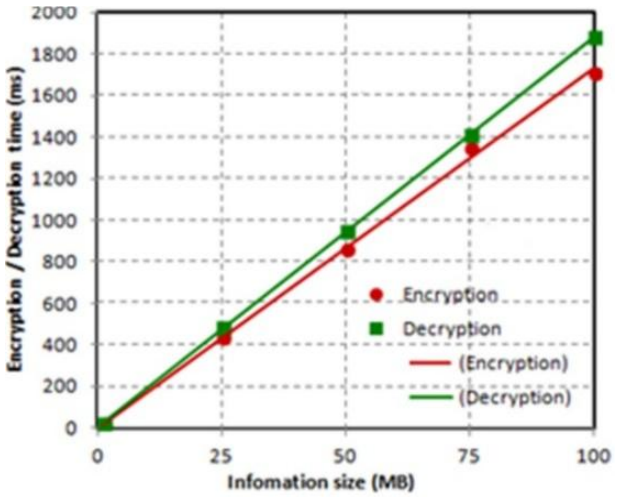

Figure 3. Illustrates to encrypt 1 MB of data the algorithm takes 17.4 ms, and for same 1 MB of data needs 18.9 ms to decrypt

Table 3. Avalanche effect test results

Test case	Total bits	Bit flipped position	Bits changed (hamming distance)	Avalanche effect (%)
1	128	Byte 0, Bit 3	63	49.22%
2	128	Byte 4, Bit 1	66	51.56%
3	128	Byte 8, Bit 7	64	50.00%
4	128	Byte 11, Bit 2	61	47.66%
5	128	Byte 15, Bit 5	65	50.78%
Average	128	-	63.8	49.84%

4.3.2. Nonlinearity assessment

At the same time, high nonlinearity, as measured by Hamming distance, indicates that there is no linear relationship between output and input, and therefore an algorithm that produces a highly nonlinear ciphertext will resist attacks using linear cryptanalysis. The proposed algorithm uses the standard AES substitution box (S-Box) for its non-linearity transformation layer. The Mathematical definition of the AES S-Box's nonlinearity (N_L) is 112. The maximum theoretical nonlinearity (MTN) of all 8-Bit Bijective S-Boxes is 120, making 112 an extremely high number. The hybrid model retains the traditional S-Box format, allowing the new hybrid method to take advantage of the strong nonlinearity of the S-Box, providing excellent protection from linear approximation attacks [12], [23].

5. CONCLUSION

This study created and implemented a mixed encryption technique that uses 192-bit AES with elliptic curve cryptography (ECC). This gives users security when sending or receiving information by preventing side channel attacks on the information. This experimental analysis showed that the hybrid solution created is extremely efficient, taking 0.0002 seconds to encrypt 10MB of data; which is roughly 8 times faster than the standard 128-bit AES time of 0.0016 seconds to encrypt the same amount of data. The algorithm offers a very high degree of cryptographic strength with an avalanche effect of 49.84% (close to the theoretical maximum of 50%) and a nonlinearity value of 112, verifying its security against both linear and differential cryptanalysis techniques. The system provides the ability to encrypt the AES key with ECC encryption using a combination of symmetric and asymmetric key encryption methods. As a result, the risks associated with symmetric keys that are typically associated with key distribution and asymmetric keys, due to their associated time computation overhead, are eliminated.

As a limitation of this research, it must be noted that it was conducted entirely using simulations in a software environment. One specific limitation is that no physical measurements were taken at the hardware level to measure power consumption during the encryption cycles. Future work will concentrate on conducting hardware-level testing to obtain optimisations for increasing security against power analysis side channel attacks, as well as adapting the current protocol for implementation within wireless body area networks (WBAN), therefore determining its effectiveness on low-power IoT device types.

ACKNOWLEDGMENTS

The authors extend their sincere appreciation to their respective institutions for providing the academic support and research environment necessary to conduct this study. The authors also acknowledge the valuable insights offered by colleagues and reviewers, which significantly contributed to improving the quality of this work.

FUNDING INFORMATION

This work did not receive any specific grant from funding agencies in the public, commercial, or non-profit sectors.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Ravindra K Reddy	✓	✓	✓	✓	✓	✓	✓	✓	✓				✓	
Vijayalakshmi P					✓	✓			✓	✓	✓	✓	✓	

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

The authors declare that there is no conflict of interest regarding the publication of this article.

ETHICAL APPROVAL

Not applicable. This study did not involve human or animal subjects.

DATA AVAILABILITY

All data generated or analyzed during this study are included within the article. Additional materials or clarifications can be provided by the authors upon reasonable request.

REFERENCES

[1] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 7th ed., Pearson India, 2018.
[2] R. Pahal and V. Kumar, "Efficient implementation of AES," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 3, no. 7, pp. 290–295, July 2013.
[3] H. Tange and B. Andersen, "Attacks and countermeasures on AES and ECC," in *Proc. IEEE Int. Symp. Wireless Personal Multimedia Communications (WPMC)*, pp. 1–5, Jun. 2013.
[4] D. Jayasinghe, J. Fernando, R. Herath, and R. Ragel, "Remote cache timing attack on advanced encryption standard and countermeasure," in *Proc. IEEE Int. Conf. Information and Automation for Sustainability (ICIAFs)*, pp. 177–182, Dec. 2010, doi: 10.1109/ICIAFS.2010.5715656.
[5] B. Narsimha *et al.*, "Cyber defense in the age of artificial intelligence and machine learning for financial fraud detection application," *IJEER*, vol. 10, no. 2, pp. 87–92, 2022, doi: 10.37391/IJEER.100206.
[6] D. Popescu *et al.*, "Communication infrastructure selection criteria for alerting systems implemented through mobile sensor networks," in *Proc. 10th WSEAS Int. Conf. Automation & Information (ICAI)*, Prague, pp. 354–359, Mar. 2009, doi: 10.5555/1864098.1864129.
[7] J. I. Ahmad, R. Din, and M. Ahmad, "Analysis review on public key cryptography algorithms," *IJEECS*, vol. 12, no. 2, pp. 447–454, Nov. 2018, doi: 10.11591/ijeecs.v12.i2.pp447-454.
[8] K. O. Tajudeen, A. O. Ameen, and A. E. Adeniyi, "A systematic review on advanced encryption standard cryptography to enhance message security," *Multimedia Tools and Applications*, vol. 84, 2025. doi: 10.1007/s11042-025-21041-4.
[9] Q. Yue, L. Xinqiang, and W. Yadong, "Low-Cost Round Encryption Method for Embedded System," *International Journal of Security and Its Applications*, vol. 9, no. 4, pp. 117–124, 2015, doi: 10.14257/ijsia.2015.9.4.12.
[10] Z. Li, C. Du, and X. Duan, "Efficient AES Side-Channel Attacks Based on Residual Mamba Enhanced CNN," *Entropy*, vol. 27, no. 8, p. 853, 2025, doi: 10.3390/e27080853.

[11] X. Li, J. Chen, D. Qin, and W. Wan, "Research and Realization based on hybrid encryption algorithm of improved AES and ECC," in *Proc. IEEE Int. Conf. Audio Language and Image Processing (ICALIP)*, pp. 396–400, Nov. 2010, doi: 0.1109/ICALIP.2010.5684554.
[12] S. Jain and R. S. Shukla, "Performance Optimization of Hybrid Encryption Techniques in Oracle Cloud Infrastructure," *Panamerican Mathematical Journal*, vol. 35, no. 3, p. 232, 2025, doi: 10.52783/pmj.v35.i3s.3889.
[13] B. Fu, T. Fang, L. Zhang, Y. Zhou, and H. Xiao, "Communication security of intelligent information service platform combining AES and ECC algorithms," *Journal of Cyber Security Technology*, vol. 9, no. 3, p. 209, 2025, doi: 10.1080/23742917.2024.2371053.
[14] C. JunLi, Q. Dinghu, Y. Haifeng, Z. Hao, and M. Nie, "Email encryption system based on hybrid AES and ECC," in *Proc. IET Int. Communication Conf. Wireless Mobile and Computing (CCWMC)*, pp. 347–350, Nov. 2011, doi: 10.1049/cp.2011.0906.
[15] H. Lee, K. Lee, and Y. Shin, "AES Implementation and Performance Evaluation on 8-bit Microcontrollers," *International Journal of Computer Science and Information Security*, vol. 6, no. 1, 2009, doi: 10.48550/arXiv.0911.0482.
[16] P. Naresh, P. Srinath, K. Akshit, M. S. S. Raju, "Decoding network anomalies using supervised machine learning and deep learning approaches," *in Proc. 2nd Int. Conf. Automation, Computing and Renewable Systems (ICACRS)*, India, pp. 1598–1603, 2023, doi: 10.1109/ICACRS58579.2023.10404866.
[17] M. McLoone and J. McCanny, "High performance single-chip FPGA rijndael algorithm implementations," *in proc. cryptographic hardware and embedded systems workshop (CHES)*, Paris, May 2001, doi: 10.1007/3-540-44709-1_7.
[18] M. I. Hussan, G. V. Reddy, P. T. Anitha, A. Kanagaraj, and P. Naresh, "DDoS attack detection in IoT environment using optimized Elman recurrent neural networks based on chaotic bacterial colony optimization," *Cluster Computing*, pp. 1–22, 2023, doi: 10.1007/s10586-023-04187-4.
[19] Z. Li, D. Du and X. Duan, "Efficient AES side-channel attacks based on residual Mamba-enhanced CNN," *Entropy*, vol. 27, no. 8, p. 853, 2025, doi: 10.3390/e27080853.
[20] Q. Yue, L. Xinqiang, and W. Yadong, "Low-cost round encryption method for embedded system," *International Journal of Security and Its Applications*, vol. 9, no. 4, pp. 117–124, 2015, doi: 10.14257/ijsia.2015.9.4.12.
[21] M. R. Babu and A. R. Reddy, "Optimization of memory for AES Rijndael algorithm implementation on embedded system," *International Journal of Engineering Research & Technology (IJERT)*, vol. 1, no. 7, Sept. 2012.
[22] A. Takielden and A. M. Fanni, "Implementation of AES algorithm in MicroController using PIC18F452," *IOSR Journal of Computer Engineering*, vol. 15, pp. 35–38, Dec. 2013.
[23] B. Alte and A. V. Vidhate, "A hybrid cryptographic protocol for secure and efficient data transmission for wireless body area network," in *2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), IEEE*, 2024, doi: 10.1109/ICCCNT.2024.10726219.

BIOGRAPHIES OF AUTHORS

Ravindra K Reddy currently doing his Ph.D. in VELS University Chennai and completed M.Tech. from RGM College of Engineering and Technology, Nandyal. Currently he is working as an Assistant Professor in Department of ECE, JNTU-A College of Engineering Pulivendula. His ongoing research work focus mainly on network security and cryptography with digital image processing. He can be contacted at email: ravindra.kalvapalli@gmail.com.

Dr. Vijayalakshmi P is an Associate Professor in the department of Electronics and Communication Engineering at VELS University Chennai, she received her Phd from same University and published number of papers in preferred Scoupus and SCI indexed journals. Also, she received funding projects from DST & EDA-MSME. Her current research interests are cognitive radio networks, network security and deep learning techniques. She can be contacted at email: viji.se@velsuniv.ac.in.