Hybrid Encryption Algorithm: Fusion of 3DES and ECC

Tharun A[1], Govardhan M[2], Jayachetan P[3], Abhiram G[4] and Gayathri R[5*]
{bl.en.u4cse22173@bl.students.amrita.edu[1], bl.en.u4cse22170@bl.students.amrita.edu[2], bl.en.u4cse22044@bl.students.amrita.edu[3], bl.en.u4cse22115@bl.students.amrita.edu[4], r_gayathri@blr.amrita.edu[5*]}

Department of Computer Science and Engineering, Amrita School of Computing, Amrita Vishwa Vidyapeetham Bengaluru, Karnataka, India[1, 2, 3, 4, 5]

Abstract. In contemporary cryptographic frameworks, the imperative of achieving secure communication alongside operational efficiency constitutes a fundamental concern. This study introduces an innovative hybrid encryption approach that integrates the advantages of Triple DES (3DES), which is a symmetric encryption technique, with Elliptic Curve Cryptography (ECC), classified as an asymmetric encryption technique. 3DES delivers elevated security levels for the encryption of substantial data quantities, whereas ECC supplies a secure and efficient mechanism for key exchange. The hybrid model uses ECC for secure key exchange and uses 3DES for bulk data encryption, providing both security and speed. The use of two different cryptographic techniques together leads to the improvement in performance of the proposed algorithm, the reduction in complexity of the computations, and strong guarantees for security. This should solve the problems related to scaling issues and the overhead associated with traditional encryption schemes, thus providing a balanced approach to modern cryptographic applications.

Keywords: Hybrid Encryption, 3DES (Triple DES), ECC (Elliptic Curve Cryptography), Symmetric Encryption, Asymmetric Encryption, Secure Key Exchange, Cryptography, Data Confidentiality, Computational Efficiency, Public Key Infrastructure.

1 Introduction

Encryption has been crucial in preventing confidential data from being sent through the digital channels. Most of these algorithms have been developed in more recent times, and significant categories include symmetric encryption schemes and asymmetric encryption algorithms. Of the symmetric algorithms applied mostly, 3DES is typical examples to encrypt large amounts of data for later decryption and are thereby needed with some reliable methods to distribute keys. The issue is addressed by asymmetric encryption, such as that found in Elliptic Curve Cryptography (ECC), using public and private key pairs, though it might be computationally expensive, particularly in encrypting large datasets.

Therefore, the hybrid encryption algorithm proposed in this project combines the merit of 3DES with the strength of ECC. The concept is to apply ECC for secure key exchange, where the asymmetrical algorithm makes sure that the secret keys are transferred over insecure channels safely. After the safe sharing of the secret key, there are bulk encryption and decryption operations utilizing 3DES because it is efficient in handling large amounts of data. This hybrid methodology significantly enhances the overall system security while keeping the performance levels high and thus makes it a good option for the scenarios where security and speed go hand in hand, including financial transactions, secure communication forums, and data storage solutions. This paper establishes a design, implementation, and analysis process of hybrid

ICITSM-Part II 2025, April 28-29, Tiruchengode, India

DOI 10.4108/eai.28-4-2025.2358064

encryption schemes compared with various conventional methods, in terms of its security, speed, and computational efficiency. The results show that the hybrid approach in encryption balances better between security and performance better than conventional forms, making it fit for application on modern cryptographic technologies.

2 Related works

Deen et.al [1] brings growing necessity for secure data transfer through modern digital environment, particularly where personal information is more liable in a progressively interconnected domain. This paper examines incorporating AES (Advanced Encryption Standard) and Blowfish algorithms in order to design an improved hybrid encryption algorithm supporting better data security, consuming minimal power, achieving high performance rate, and providing real time output. The system considered here is designed to provide a reliable mechanism to prevent interception by unauthorized entities, while also making the process of cryptanalysis more complicated. This approach is particularly relevant as it attempts to balance security with computational efficiency, thereby offering a robust response to contemporary cryptographic challenges. Sharma and Kumar et.al [2] has given an analysis on recent advances in hybrid cryptographic algorithms focused on cloud networks. Here, a discussion will be done in this particular timeline between 2021 up to early 2023, as well as how this hybrid technique focuses on multiple different methods used within different encryption techniques and its decryptions. With symmetric algorithms merged into asymmetric ones, it presents an advanced protection strategy for data that gets preserved within cloud systems. It would present a precious resource for beginners, referring to opinions on the performance of various algorithms and providing a base for further development in cloud security. Zhang et.al [3] Describes the detailed analysis of hybrid encryption that uses a combination of symmetric and asymmetric encryption algorithms to counter security issues in the process of information transmission. Its major advantage is that of symmetric encryption to have a fast computation rate in encrypting large sets of data besides security by asymmetric encryption especially for protecting keys. The integration of both methods leads to hybrid encryption, which enhances security while keeping optimal performance levels, and therefore offers a feasible solution for future cryptographic applications. In addition, the paper discusses a variety of algorithms and their use in various systems, demonstrating how hybrid methods enhance data security without adding more complexity. Zhao et.al [4] presents an amalgamation method of hybrid encryption combining DES with RSA. It uses the combination to avoid weaknesses in the algorithms used in symmetric and asymmetric key methods. This algorithm provides greater efficiency without a loss in security: the short DES key is encrypted by the RSA public key and then encypted with the plain- text through the DES algorithm. Hybrid methodology uses RSA to safely exchange keys and DES for efficiently encrypting data and, therefore, delivers fast encryption time along with high reliability. The paper gives performance tests which claim that the algorithm is well-suited for the application of digital signatures as well as secure data communication, hence pro- viding a highly balanced solution for modern crypto- graphic demands. Francis et.al [5] discusses a few hybrid cryptographic approaches used to enhance the information security, with special consideration given to the need for confidential- ity, authentication, and data integrity in open channels of communication. The article presents the vulnerabilities that face the traditional cryptographic systems toward various attacks and the necessity to combine multiple cryptographic algorithms in order to counteract such challenges. This study

demonstrates through the analysis of a number of hybrid cryptosystems that hybridization results in a more robust approach to secure communication. The assessment of current hybrid frameworks provides crucial insight into the benefits and drawbacks of different encryption methods, thus improving the security and efficiency of communication protocols. Subedar and Araballi et al. [6] discuss a few hybrid cryptographic combinations that aim to enhance the security of data and the efficiency of communication. This paper explores the hybridization of symmetric and asymmetric cryptographic methods, in this case, AES, RSA, and ECC with SHA-256 for integrity and authentication. The authors highlight the advantages of hybrid encryption since it has overcome many disadvantages of stand-alone algorithms such as problems in symmetric encryption on key management and slow processing speeds of asymmetric encryption.

From the experimental results, it becomes clear that hybrid combinations make computations more time-efficient while replacing traditional standalone cryptographic methods for securing modern communication. Investigative study on the use of hybrid cryptographic schemes that work towards securing sensitive information while utilizing cloud computing frameworks undertaken by Murad and Rahouma et.al [7] This paper presents a comprehensive comparative analysis of two tier and three tier hybrid set- tings that utilize several cryptographic techniques to enhance security and to improve performance. The simulated Python implementation demonstrates the efficient functioning of different hybrid architectures, with special interest expressed in AES as the quickest encrypting and decrypting program. The study concludes that the two-tier model has higher efficiency, but the three- tier model provides greater security. The paper provides excellent insights into balancing security and performance in cloud data protection. Chowdhary et al. [8] have analyzed various hybrid crypting techniques for image encryption and decryption by relying on symmetric and asymmetric algorithms for security and efficiency improvements. In the article, the study lists the applications of ECC with Hill Cipher (HC), AES, and also ElGamal with Double Playfair Cipher (DPC) designed to discuss comparative analyses of each scheme based on considerations like encryption time, entropy, loss of intensity, PSNR, NPCR, and UACI. The authors show how there is a balance between symmetric algorithms and the amount of security given by asymmetric methods. It can easily be seen that one application of ECC with HC can be for remote or private communication; these applications offer robust image encryption. There are hybrid cryptographic approaches implemented for cloud computing by Reddy et al. [7] but it is not clear how steganography fits in the problem-solving solution. We take this concept forward by integrating both seamlessly. Murugadoss et al. [8] have applied the technique of watermarking that employed chaotic maps and elliptic curve cryptography but these approaches are not suitable for dynamic steganographic purposes. Our method ensures flexibility about all types of scenarios. V. Divyashree et al. [9] introduced multimedia steganography with security conciseness, but the authors failed to implement a robust cryptographic model like AES and RSA, as in our current work. In designing the triple-layer hiding mechanism, Menon and Vaithiyanathan et.al [10] failed to resolve the problem of computational overhead. Our approach decreases such queues without losing security. Similar to Keerthan et al. [11], we have looked at cryptographic algorithms for the IoT, but the integration of steganography is missing from the authors' model. Bhavitha et al. [14] had tested most commonly used encryption methods at the time but focused less on the steganography aspect, which affects data hiding capacity G. Ramasamy et al. [15] suggested a Bash-based simulation environment to simulate multi-process file systems

effectively utilizing light-weight scripting.

3 Methodology

The hybrid encryption algorithm utilizes both symmetric and asymmetric encryption techniques by combining Elliptic Curve Cryptography (ECC) with Triple DES (3DES). It operates in two phases: secure key distribution using ECC and large data encryption via 3DES.

Key Generation

3.1 ECC Key Pair Generation

Each participant (sender and receiver) generates a private-public key pair based on an elliptic curve. The private key remains confidential, while the public key is shared.

3.2 Key Exchange (ECC - ECDH)

The sender and receiver perform the Elliptic Curve Diffie-Hellman (ECDH) key exchange between sender and receiver. Each participant uses its private key and the public key of the counter party to compute a shared secret. This shared secret derives the symmetric 3DES encryption key from this shared secret.

3.3 DES Encryption (Symmetric Encryption)

The sender uses this securely exchanged key to encrypt bulk data with 3DES. This symmetric encryption is efficient for securing large datasets.

3.4 Data Transmission

The data is communicated by sending over the communication channel encrypted. The exchange of key is secured with the help of ECC, while data confidentiality at the time of communication is achieved using 3DES.

3.5 Decryption at the Receiver Side (ECC + 3DES)

The receiver uses his private ECC key and the sender's public key to derive the shared secret via ECDH. The derived key decrypts the ciphertext using 3DES to recover the plaintext.

3.6 Security Guarantee

ECC ensures key exchange is secure, preventing interception by malicious actors. 3DES maintains data confidentiality ensuring it is suitable for large scale encryption.

4 Implementation

The hybrid encryption mechanism combines two different cryptographic algorithms together, namely ECC, which is good at secure key installment, and 3DES, which is useful for encrypting

large size data. The composition achieves the best trade-off between security and computational efficiency, and is suitable for secure communication and cloud storage.

4.1 Elliptic Curve Cryptography (ECC)

ECC thwarts unauthorized key exchange between sender and receiver. With ECDH protocol, two parties can generate a shared secret even over an untrusted medium. ECC provides much stronger security for same size key, such as 256-bit ECC key will have same security level as RSA key.

4.2 Triple DES (3DES)

3DES is used to bulk encrypt data after the key exchange. The encryption applies the DES algorithm three times with distinct keys, hence making it stronger and more resistant against brute-force. 3DES is more useful to process massive amount of data transfer.

4.3 Step-by-Step Implementation

Both the sender and receiver generate an ECC based key pair comprised of a private key and a corresponding public key for encryption and key-exchange. In both cases, a common secret is computed by both parties using their respective private key and the public key of the other party. The shared secret is then fed through a key derivation algorithm (for example: PBKDF2) to get the 24-byte 3DES key. The 3DES key generated is employed to encrypt and decrypt the transmitted and received data respectively. Data is encrypted in CBC mode using the 3DES key produced and an IV to provide uniqueness. The receiver decrypts the data with the same 3DES key and IV, and the plaintext is the result.

4.4 Hybrid Encryption Method

The full hybrid encryption process follows these steps:

4.4.1 Originator:

Generate an ECC key pair. Exchange your ECDH key with the recipient's public key and produce a shared secret. The extracted key for 3DDES is extracted via clicking the document URL. Encrypt the data with 3DES.

4.4.2 Recipient:

Generate an ECC key pair. Now do ECDH encode using the senders public key and receive the same shared secret. Retrieval of the 3DES cipher key. Decrypt the data with 3DES. item Decrypt the data with 3DES.

4.5 Security Considerations

This hybrid process of encryption is based on ECC and 3DES Offers strong security.

The secret of key exchange is protected by ECC (keying material could not be eavesdropped). 19/1/0One 3DES secures traffic (even though the newer AES is faster).

Both 3DES and EC see the trade-off between efficiency and security. This makes them especially suitable for resource-limited contexts such as mobile devices and embedded systems.

5 Results

5.1 Explanation for the ECC Encryption Graphs

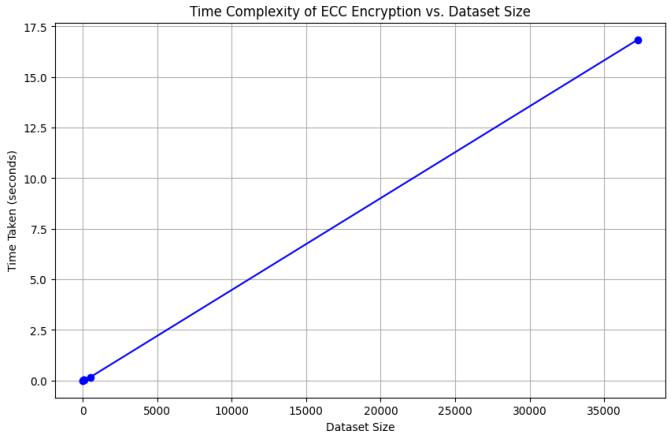

Fig. 1. Time Complexity of ECC Encryption vs. Dataset Size.

Fig 1 and 2 shows the time complexity of ECC encryption is proportional to the size of this dataset. This proves that despite ECC being secure for Key exchange, it is computationally expensive to use in Big Data work-loads. More specifically, this means there is a trade-off between computational efficiency and security, and ECC is predominantly useful for key management rather than bulk data encryption.

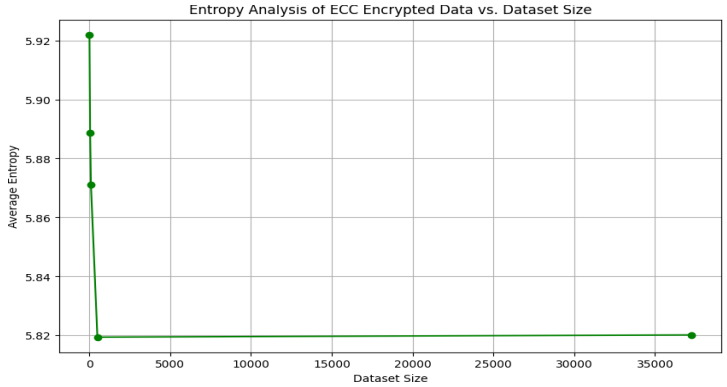

Fig. 2. Entropy Analysis of ECC Encrypted Data vs. Dataset Size.

- ObservationThe entropy begins at high values and converge to it at bigger data sizes, showing the amount of high level strong random when the data was encrypted.
- Meaning: High entropy ensures resistance to attacks like frequency analysis and thereby validates ECC's claim to generate unpredictable, secure ciphertexts. Fig 3 shows the key sensitivity of ECC encryption vs. dataset size.

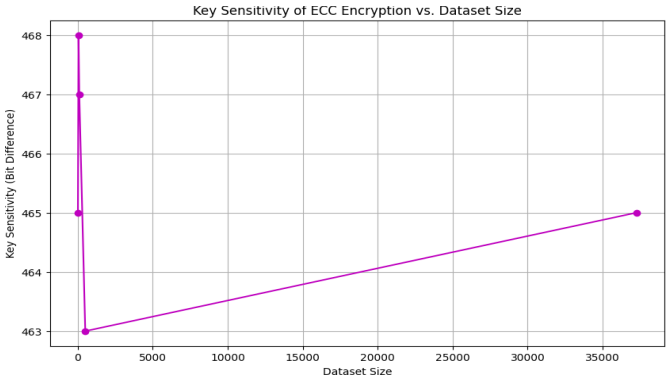

Fig. 3. Key Sensitivity of ECC Encryption vs. Dataset Size.

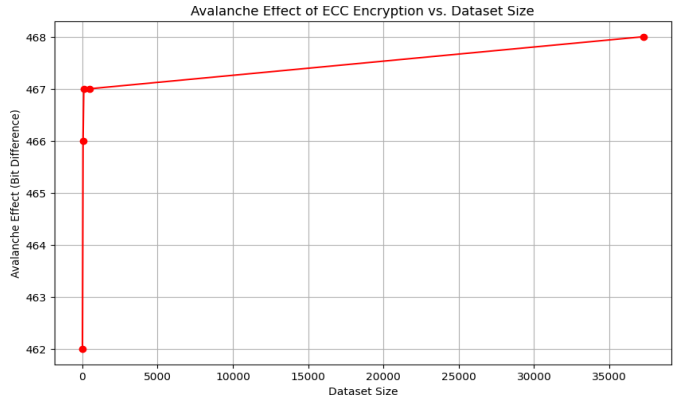

Fig. 4. Avalanche Effect of ECC Encryption vs. Dataset Size.

Fig 4 shows the avalanche effect of ECC encryption vs. dataset size.

- Observation: Avalanche effect in bit differences stabilizes at high values, meaning small input differences correspond to significant output variations.
- Significance: Strong avalanche effect is crucial for secure encryption, where no detectable pattern exists in the ciphertext, ensuring robustness for datasets of any size.

5.2 Explanation for the 3DES Encryption Graphs

- Observation: For 3DES encryption, the time complexity increases linearly with the size of the dataset, similar to ECC.
- Significance: This demonstrates the efficiency of 3DES in encrypting large datasets. Compared to ECC, 3DES has lower computational overhead and is suitable for bulk data encryption in hybrid systems.

Fig 5 and 6 shows the time complexity and entropy analysis of 3DES encrypted data vs. dataset size.

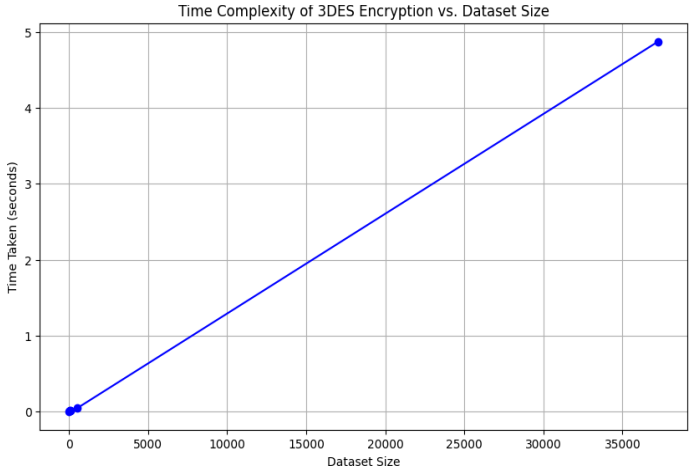

Fig. 5. Time Complexity of 3DES Encryption vs. Dataset Size.

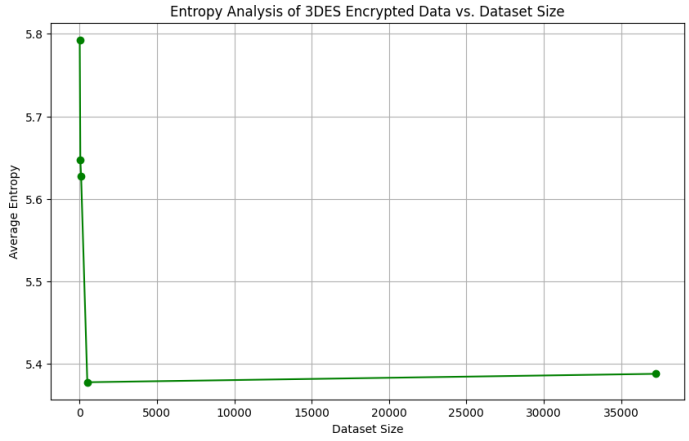

Fig. 6. Entropy Analysis of 3DES Encrypted Data vs. Dataset Size.

- Observation: Entropy values are very high initially and stabilize slightly below as dataset size increases.
- Significance: High entropy guarantees randomness and strong resistance against

cryptographic attacks. The small drop from ECC may indicate the deterministic nature of symmetric encryption like 3DES.

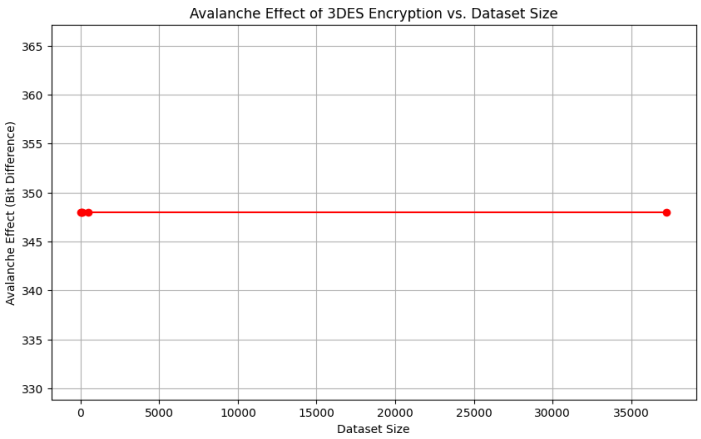

Fig. 7. Avalanche Effect of 3DES Encryption vs. Dataset Size.

Fig 7 shows the avalanche effect of 3DES encryption vs. dataset size.

- Observation: The effect of an avalanche is constant regardless of dataset size.
- Significance: Constant bit differences indicate that 3DES maintains strong encryption strength ensuring input randomness remains consistent across the sizes of datasets.

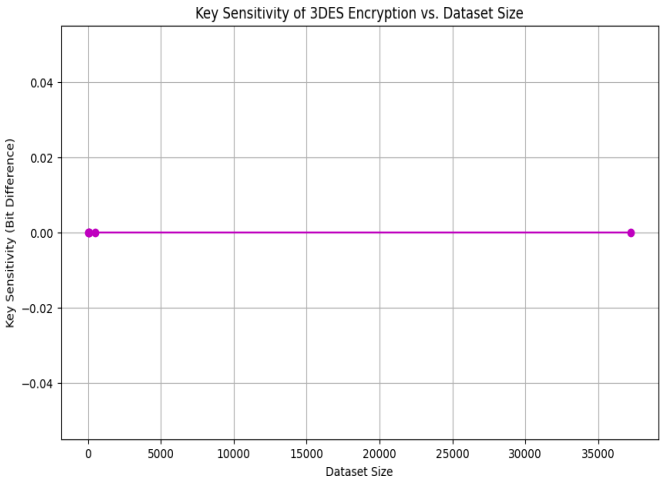

Fig. 8. Key Sensitivity of 3DES Encryption vs. Dataset Size.

Fig 8 shows the key sensitivity of 3DES encryption vs. dataset size.

- Observation: Key sensitivity values remain consistent, with negligible changes in ciphertext for minor key modifications.
- Significance: This work highlights a limitation of 3DES compared to ECC as symmetric encryption generally exhibits lower key sensitivity. This reinforces the need for combining it with ECC in a hybrid system for robust key management.

5.3 Explanation for the Hybrid ECC + 3DES Encryption Graphs

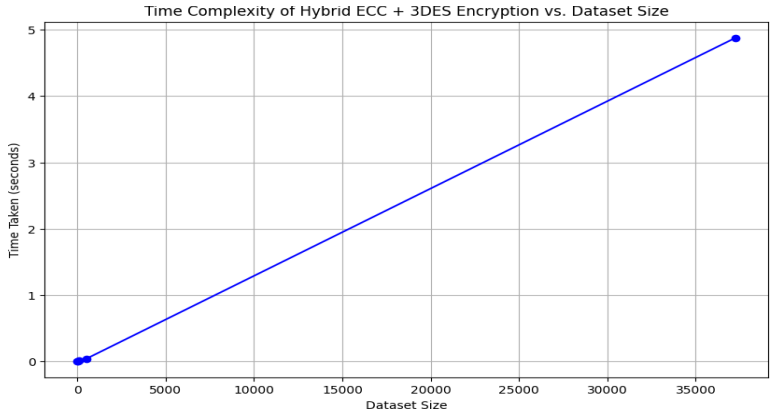

Fig. 9. Time Complexity of Hybrid ECC + 3DES Encryption vs. Dataset Size.

Fig 9, 10, 11 and fig 12 shows the Time Complexity, Avalanche Effect, Key Sensitivity and Entropy Analysis of Hybrid ECC + 3DES Encryption vs. Dataset Size.

- Observation: Time complexity scales linearly with the size of the dataset.
- Significance: This depicts the collective overhead of ECC for secure key exchange and 3DES for efficient data encryption. The linear growth indicates scalability mak- ing the hybrid system suitable for practical scenarios involving datasets of different sizes and with various sizes.

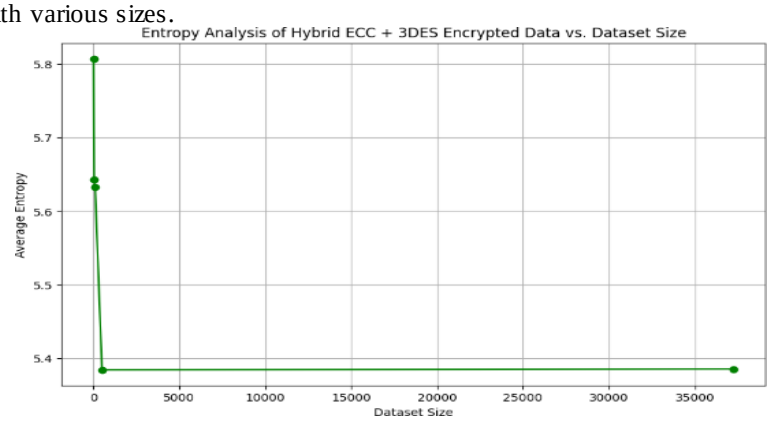

Fig. 10. Entropy Analysis of Hybrid ECC + 3DES Encrypted Data vs. Dataset Size.

- Observation: The entropy stabilizes toward higher values after a temporary drop for smaller datasets.
- Significance: High entropy ensures strong randomness and resistance to crypto graphic attacks. The hybrid approach combines ECC's randomness with 3DES' efficiency to maintain strong encryption.

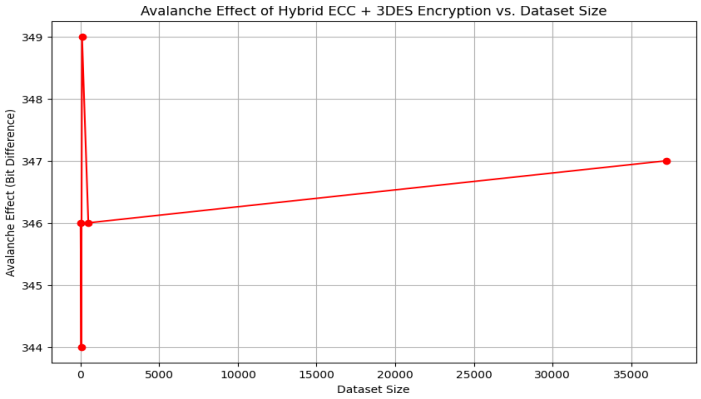

Fig. 11. Avalanche Effect of Hybrid ECC + 3DES Encryption vs. Dataset Size.

- Observation: The avalanche effect stabilizes at high values of bit difference and increases slightly with the dataset size.
- Significance: Small changes in the inputs produce significant differences in the ciphertext, demonstrating the unpredictability and robustness of the hybrid encryption system.

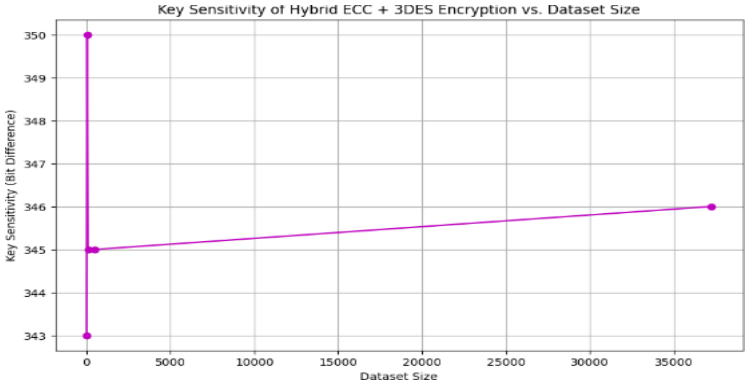

Fig. 12. Key Sensitivity of Hybrid ECC + 3DES Encryption vs. Dataset Size.

- Observation: Key sensitivity remains very high and increases with dataset size.
- Significance: The hybrid system is highly sensitive when key changes, making it robust against brute-force and key-guessing attacks. Together ECC and 3DES enlarge this property.

6 Detailed Analysis

The outcome of multiple and hybrid encryption techniques (ECC, 3DES Hybrid ECC + 3DES) is evaluated against four metrics: time complexity, entropy analysis, avalanche effect and key sensitivity. below is the detailed analysis and conclusion regarding which encryption technique performs best overall.

6.1 Time Complexity

- ECC: The time complexity increases linearly with the size of the dataset but has the highest overhead due to computational complexity.
- 3DES: Demonstrates linear scalability with a much lower time complexity than ECC and is ideal for bulk encryption of data.
- Hybrid ECC + 3DES: The complexity is higher than 3DES but much lower compared to ECC. This happens when ECC is used as a means of key exchange while 3DES is implementation to encrypt the data.
- Best: 3DES is the most efficient approach, but the hybrid brings out a balance between security and computational cost, making it more practical.

6.2 Entropy Analysis

- ECC: Maintains the highest entropy values across all dataset sizes maintaining strong randomness and resistance to cryptanalytic attacks.
- 3DES: Begins with high entropy but stabilizes a little lower than ECC, indicating
- slightly weaker randomness.
- Hybrid ECC + 3DES: Stabilizes at high entropy values but slightly lower than ECC, combining the strengths of both algorithms to maintain strong randomness.
- Best: ECC for pure randomness. However, the hybrid system offers similar performance with better computation efficiency.

6.3 Avalanche Effect

- ECC: Exhibits a strong avalanche effect, where small changes in input result in significant differences in ciphertext, ensuring unpredictability.
- 3DES: Displays a stable avalanche effect, though of lesser magnitude compared to ECC.
- Hybrid ECC + 3DES: Demonstrates a stable and strong avalanche effect, comparable to ECC and greater than 3DES alone.
- Best: Hybrid ECC + 3DES, as it achieves strong unpredictability while balancing the trade-offs between individual techniques.

6.4 Key Sensitivity

- ECC: Highly sensitive to key changes. Even minor modifications yield significant differences in ciphertext, making it robust against brute-force attacks.

- 3DES: Less sensitive to key changes compared to ECC, which is a limitation of symmetric encryption algorithms.
- Hybrid ECC + 3DES: Demonstrates high key sensitivity, comparable to ECC, ensuring strong robustness against key-related attacks.
- Best: Hybrid ECC + 3DES, as it inherits ECC's high sensitivity while maintaining efficiency.

Table 1. Comparison of ECC, 3DES, and Hybrid ECC + 3DES across various metrics.

Metric	ECC	3DES	Hybrid ECC + 3DES
Time Complexity	High overhead	Efficient	Balanced
Entropy	Highest	Moderate	High
Avalanche Effect	Strong	Moderate	Strong
Key Sensitivity	High	Low	High

Table 1 shows the Comparison of ECC, 3DES, and Hybrid ECC + 3DES across various metrics.

7 Conclusion

The proposed Hybrid ECC + 3DES Encryption System puts together the advantages of the two different encryption methods and, thereby, helps eradicate the limitations of using an individual encryption method. By ensuring secure key management using the ECC algorithm and efficient encryption of data using the 3DES algorithm, a balance is achieved between computational efficiency and strong security.

7.1 Key conclusions which the analytical paper reveals:

- Efficiency: The hybrid framework exhibits a linear scalability in relation to dataset dimensions, rendering it appropriate for practical applications that require handling substantial data volumes. The time complexity is markedly reduced in comparison to independent ECC while retaining strong encryption characteristics.
- Security: High entropy, strong avalanche effects, and high key sensitivity val- idate the robustness of the hybrid system against the cryptographic attacks, which include brute-force, key-guessing, and pattern-based attacks.
- Pragmatic: The hybrid system will show adaptability in such applications as secure communications, protecting cloud data and performing financial transactions which would require simultaneous fulfillment of speed and security requirements. The hybrid ECC + 3DES Encryption System in combination with the hybrid encryp- tion techniques described above is thus a highly effective yet secure response to questions This means that hybrid encryption might be a practical approach to the confidentiality

integrity and authenticity of data in digital environments. The current project emphasizes the capabilities of hybrid cryptographic frameworks in the enhance- ment of data security within an increasingly interconnected global perspective. Future research could study the optimization of the hybrid system for resource-constrained environments and its integration into real time encryption architectures.

References

[1] A. E. Taki El Deen, "Design and Implementation of Hybrid Encryption Algo- rithm," IEEE Senior Member, Alexandria University, Egypt, 2020.

[2] H. Sharma and R. Kumar, "A Review Paper on Hybrid Cryptographic Algorithms in Cloud Network," 2nd International Conference for Innovation in Technology (INOCON), 2023. [DOI: 10.1109/INOCON57975.2023.10101044].

[3] Q. Zhang, "An Overview and Analysis of Hybrid Encryption: The Com- bination of Symmetric Encryption and Asymmetric Encryption," 2nd Inter- national Conference on Computing and Data Science (CDS), 2021. [DOI: 10.1109/CDS52072.2021.00111].

[4] J. Zhao, "DES-Co-RSA: A Hybrid Encryption Algorithm Based on DES and RSA," 2023 IEEE 3rd International Conference on Power, Electronics and Computer Applications (ICPECA), 2023. [DOI:10.1109/ICPECA56706.2023.10075771].

[5] N. Francis, "An Analysis of Hybrid Cryptographic Approaches for Information Security," International Journal of Applied Engineering Research, vol. 13, no. 3,

[6] pp. 35-41, 2018.

[7] S. H. Murad and K. H. Rahouma, "Implementation and Performance Analysis of Hybrid Cryptographic Schemes applied in Cloud Computing Environment," 2020 IEEE International Conference on Computing, Networking and Communications (ICNC), 2020. [DOI: 10.1109/ICNC48913.2020.00145].

[8] C. L. Chowdhary, P. V. Patel, K. J. Kathrotia, M. Attique, K. Perumal, and M. F. Ijaz, "Analytical Study of Hybrid Techniques for Image Encryption and Decryption," MDPI Electronics, vol. 9, no. 12, pp. 1876-1886, 2020. [DOI: 10.3390/electronics9121876].

[9] Z. Subedar, A. Araballi, "Hybrid Cryptography: Performance Analysis of Various Cryptographic Combinations for Secure Communication," International Jour- nal of Mathematical Sciences and Computing, vol. 4, pp. 35-41, 2020. [DOI: 10.5815/ijmsc.2020.04.04].

[10] K. K. Reddy, A. R. Chadha, P. S. Nikhil and S. Sountharrajan, "Hybrid Cryptography Techniques for Data Security in Cloud Computing," 2024 IEEE International Conference on Computing, Power and Communication Technologies (IC2PCT), Greater Noida, India, 2024, pp. 1836-1842, doi: 10.1109/IC2PCT60090.2024.10486794.

[11] B. Murugadoss, S. N. R. Karna, J. S. Kode and R. Subramani, "Blind Digital Image Watermarking using Henon Chaotic Map and Elliptic Curve Cryptography in Discrete Wavelets with Singular Value Decomposition," 2021 International Symposium of Asian Control Association on Intelligent Robotics and Industrial Automation (IRIA), Goa, India, 2021, pp. 203-208, doi: 10.1109/IRIA53009.2021.9588744.

[12] D. Divyashree, K. N. Bhanu and M. Anusha, "Secured Communication for Mul- timedia based Steganography," 2020 International Conference on Electronics and Sustainable Communication Systems (ICESC), Coimbatore, India, 2020, pp. 856-861, doi: 10.1109/ICESC48915.2020.9156063.

[13] N. Menon and V. Vaithiyanathan, "Triple Layer Data Hiding Mechanism using Cryptography and Steganography," 2018 3rd IEEE International Con- ference on Recent Trends in Electronics, Information Communication Tech- nology (RTEICT), Bangalore, India, 2018, pp. 407-410, doi: 10.1109/RTE- ICT42901.2018.9012633.

[14] N. K. S. Keerthan, S. P. Marri and M. Khanna, "Analysis of Key Based Cryptographic Algorithms and its Applications," 2023 IEEE 3rd International Conference on Technology,

Engineering, Management for Societal impact using Marketing, Entrepreneurship and Talent (TEMSMET), Mysuru, India, 2023, pp. 1-4, doi: 10.1109/TEMSMET56707.2023.10150061.
[15] M. Bhavitha, K. Rakshitha and S. M. Rajagopal, "Performance Evaluation of AES, DES, RSA, and Paillier Homomorphic for Image Security," 2024 IEEE 9th International Conference for Convergence in Technology (I2CT), Pune, India, 2024, pp. 1-5, doi: 10.1109/I2CT61223.2024.10544282
[16] Ramasamy, G., Shaik, B. A., Kancharla, Y., & Manikanta, A. R. (2025). A Bash-based approach to simulating multi-process file systems: Design and implementation. In Challenges in Information, Communication and Computing Technology (pp. 200-206). CRC Press.