International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Exploring Privacy-Preserving Strategies: A Comprehensive Analysis of Group-Based Anonymization and Hybrid ECC Encryption Algorithm for Effective Performance Evaluation in Data Security

Anup Maurya[1], Manuj Joshi[2]

Submitted: 27/11/2023 **Revised**: 07/01/2024 **Accepted**: 17/01/2024

Abstract: As data security continues to change quickly, protecting privacy has become more important than ever. This paper explores privacy-preserving tactics and provides a thorough examination of two essential methods: Encryption Algorithm for Hybrid Elliptic Curve Cryptography (ECC) with Group-Based Anonymization. Presenting a useful framework for data security performance evaluation is the main objective. Group-Based Anonymization preserves anonymity while retaining data utility by grouping individuals together under the tenet of collective identity preservation. The programme uses an advanced grouping technique to provide the best possible trade-off between data usability and privacy protection. The paper focus on strong cryptographic solution that combines the advantages of symmetric and asymmetric encryption is the Hybrid ECC Encryption Algorithm. This hybrid solution solves the computational issues related to conventional ECC methods while simultaneously improving data transfer security. Important parameters including attack resistance, communication overhead, and computational efficiency are included in the performance evaluation. The paper aims to provide insights into the advantages and disadvantages of each technique by carefully examining these factors. This study adds to the current conversation about privacy and data security by offering a sophisticated insight into the complex interactions between hybrid ECC encryption and group-based anonymization. Adopting such extensive privacy-preserving methods becomes essential for protecting sensitive information in numerous fields, as data remains a crucial asset in the digital world.

Keywords: *Privacy Preserving, Data Security, Anonymization, Cryptography*

1. Introduction

As data collection and interchange become more widespread, protecting sensitive data's privacy and security has grown more difficult. Strong privacy-preserving measures are essential as more and more people and organisations entrust an increasing quantity of data to digital platforms. The goal of this research is to further the development of efficient performance evaluation in the field of data security by thoroughly examining two innovative methods: group-based anonymization and a hybrid elliptic curve cryptography (ECC) encryption algorithm. The emergence of big data has completely changed how people use, analyse, and share information. But with all of this digital change, there are now worries about people's privacy and the security of sensitive data. In the face of sophisticated cyber threats and changing privacy legislation, traditional data protection approaches frequently prove inadequate [1]. In order to tackle these obstacles, creative approaches are essential, and this research explores the nuances of two such approaches. A privacy-preserving method based on the idea of collective identity preservation is group-based anonymization. Essentially, people are combined into groups, adding a degree of anonymity that protects individual identities without compromising the usefulness of the information. The principal concept is masking personal data inside a shared framework, achieving a careful equilibrium between data accessibility and privacy protection. The purpose of this study is to clarify the methods by which Group-Based Anonymization maintains this delicate balance and to provide insight into how effective it is as a defence against identity theft and unauthorised access.

The study also examines the Hybrid ECC Encryption Algorithm, a cryptographic technique intended to strengthen data transmission against possible threats. Unlike traditional ECC algorithms, this hybrid approach combines the best aspects of symmetric and asymmetric encryption systems. Secure key exchange is a benefit of asymmetric encryption, but symmetric encryption excels in speed and efficiency. The Hybrid ECC Encryption [9] Algorithm combines these advantages to try to overcome the computational difficulties that come with conventional ECC techniques, offering a stronger defence against illegal access and data breaches. The combination of these two privacy-preserving techniques is not accidental; rather, it is a conscious attempt to balance and enhance their individual shortcomings. Establishing a coherent and flexible framework that is in line with the ever-changing landscape of data security

[1]*Ph.D. Scholar, Pacific University, Udaipur Rajasthan, India. Email: anup.maurya90@gmail.com*
[2]*Associate Professor, Pacific University, Udaipur Rajasthan, India. Email: manujjoshi@gmail.com*

threats is the aim. This study aims to close the gap between theory and practical application in an environment where threats are always changing. A holistic approach is necessary. An essential component of this research is evaluating these techniques' performance. A detailed grasp of the practical effects of implementing Group-Based Anonymization and the Hybrid ECC Encryption Algorithm is provided by the careful analysis of metrics like computing efficiency, communication overhead, and attack resistance. This assessment goes beyond theoretical concerns in an effort to provide useful information that can guide decision-making across a range of industries where data security is a top priority.

The importance of protecting sensitive data cannot be emphasised as long as technology keeps developing [2]. With its thorough investigation and analysis, this study adds to the current conversation about privacy in data security. It seeks to give a basis for the creation of specialised and successful privacy-preserving measures by dissecting the intricacies of Group-Based Anonymization and the Hybrid ECC Encryption Algorithm. By doing this, the research aims to support both individuals and organisations in their quest to leverage the advantages of data-driven insights while guaranteeing the privacy and accuracy of the data they entrust to digital systems.

The major contribution of paper is given as:

- Two cutting-edge techniques for protecting sensitive data in the digital age are presented in this paper: group-based anonymization and a hybrid ECC encryption algorithm. Both are introduced and thoroughly examined.
- The paper study provides a sophisticated knowledge of Group-Based Anonymization's efficacy in disguising individual identities within a collective framework, offering insights into how it strikes a delicate balance between privacy preservation and data usability.
- Evaluation of the Hybrid ECC Encryption Algorithm, a cryptographic solution that mixes symmetric and asymmetric encryption, makes a significant contribution to the discipline. By strengthening defences against unauthorised access and data breaches and tackling computing problems, this hybrid strategy seeks to strengthen data transmission.

2. Related Work

The need to safeguard confidential data and maintain privacy has led to the development of numerous creative tactics as the digital environment keeps changing. The vast field of privacy-preserving methods is covered in this survey of the literature, with two key strategies Group-Based Anonymization and the Hybrid Elliptic Curve Cryptography (ECC) Encryption Algorithm being highlighted. This part attempts to provide a thorough overview of the present state of research, identify gaps, and establish the groundwork for the analysis that follows by surveying related work in the field [3].

The increasing worries about data security and personal privacy have led to a boom in interest in privacy-preserving techniques. When faced with new challenges, traditional approaches can prove ineffective, which leads academics to look at other options [4]. Team-Based The approach of anonymization, which is based on the idea of collective identity protection, has drawn interest because it may be able to resolve the seemingly incompatible objectives of data utility and privacy preservation. The [5] literature highlights the significance of group dynamics in masking individual identities and indicates a growing corpus of work that investigates the processes by which this method functions. Research indicates that it can be applied to a wide range of fields, including social networks and healthcare, demonstrating its adaptability and potential influence on multiple industries. In addition, the literature emphasises how crucial cryptographic solutions are to bolstering data security. A significant development is the Hybrid ECC Encryption Algorithm, which combines symmetric and asymmetric encryption to overcome the drawbacks of conventional ECC techniques [6]. Scholars have explored the nuances of this hybrid strategy, highlighting how it can improve data transmission security. Its enhanced computing efficiency and resistance to specific sorts of attacks are demonstrated by comparisons with traditional ECC approaches, indicating that it is a promising path towards improving cryptographic defences.

The existing body of literature highlights the persistent conflict between privacy and usability in the context of privacy-preserving techniques. Even though they are good at hiding specific identities, traditional anonymization techniques frequently reduce the usefulness of the data. Researchers are working hard to find a way to reconcile these competing demands, and group-based anonymization shows up as a potential solution in this tight spot [7], [8]. A sophisticated grasp of the trade-offs involved is revealed by the literature, where studies demonstrate how different grouping mechanisms effectively protect privacy without compromising insightful data analysis. The literature review also emphasises how the threat landscape in data security is changing. Strong cryptographic solutions are becoming more and more necessary as complex cyberattacks and quantum computing grow more

common. Proactively addressing these issues, the Hybrid ECC Encryption Algorithm stands out for combining symmetric and asymmetric encryption. The [9] literature emphasises how it may be used to future-proof data security methods and offers insight into how cryptography research is changing to keep up with new threats. The literature indicates a need for more thorough performance evaluations that take into account a variety of application domains and real-world circumstances, notwithstanding the advancements made in the study of Group-Based Anonymization and the Hybrid ECC Encryption Algorithm. Numerous studies shed light on certain facets of these methods, but more research is needed to fully comprehend their combined effectiveness and possible synergies.

Table 1: Summary of Related work

Method	Data Partition Method	Key Finding	Limitation	Advantage
Group-Based Anonymization [10]	Aggregation into Groups	Balances privacy preservation and data utility	Sensitivity to group formation parameters	Versatility in various domains; healthcare, social networks
Hybrid ECC Encryption Algorithm [11]	Symmetric and Asymmetric Encryption	Enhanced data transmission security	Potential performance overhead with large datasets	Improved computational efficiency; resistance to attacks
Traditional Anonymization [12]	Removal of Identifying Information	Robust privacy preservation	Reduction in data utility	Simplicity and ease of implementation
Quantum-Safe Cryptography [13]	Quantum-Resistant Algorithms	Future-proofing against quantum threats	Limited real-world quantum computing threats	Anticipation of emerging risks; long-term security
Homomorphic Encryption [14]	Computation on Encrypted Data	Secure computation without data exposure	Computationally intensive; reduced performance	Facilitates privacy-preserving computation
Secure Multi-Party Computation [15]	Collaborative Data Processing	Preserves privacy during joint analysis	Communication overhead; scalability challenges	Enables joint analysis without revealing individual data
Attribute-Based Encryption [16]	Access Control Based on Attributes	Granular control over data access	Key management complexities; potential attribute leakage	Fine-grained access control; flexible authorization policies
Federated Learning [17]	Decentralized Model Training	Privacy-preserving machine learning	Communication overhead; potential model inference attacks	Distributed learning without centralized data exposure
Privacy-Preserving Data Mining [18]	Encrypted Data Analysis Techniques	Preserves privacy during data mining	Reduced accuracy in encrypted data analysis	Safeguards sensitive information during mining
Zero-Knowledge Proofs [19]	Proof of Knowledge	Confidentiality without data	Computational overhead; complexity	Verifiable authentication without

	Without Revealing	exposure	in implementation	revealing information
Differential Privacy [20]	Randomized Data Perturbation	Quantifiable privacy guarantees	Trade-off between privacy and data accuracy	Provides a formal framework for measuring privacy guarantees
Secure Hash Functions [8]	Hashing Techniques	Data integrity and authentication	Vulnerable to collision attacks; irreversible process	Ensures data integrity and authenticity
Anonymized Data Sharing [9]	Removal of Identifiers	Facilitates data sharing with anonymity	Potential re-identification risks	Enables collaborative research while protecting identities
Secure IoT Communication [5]	Encrypted Communication Protocols	Privacy-preserving IoT data exchange	Overhead in resource-constrained IoT devices	Ensures confidentiality in IoT communication

3. Methodology

The approach to investigating privacy-preserving tactics is methodical and includes preprocessing of the dataset, privacy-preserving methods including K-anonymity, L-diversity, and T-closeness, and the use of the Hybrid ECC Encryption Algorithm, as illustrate in figure 1. The encryption and decryption procedures are included in the performance evaluation, with an emphasis on timing, memory usage, and security considerations. Graphs are also used to visually display the evaluation in order to provide a thorough comprehension.

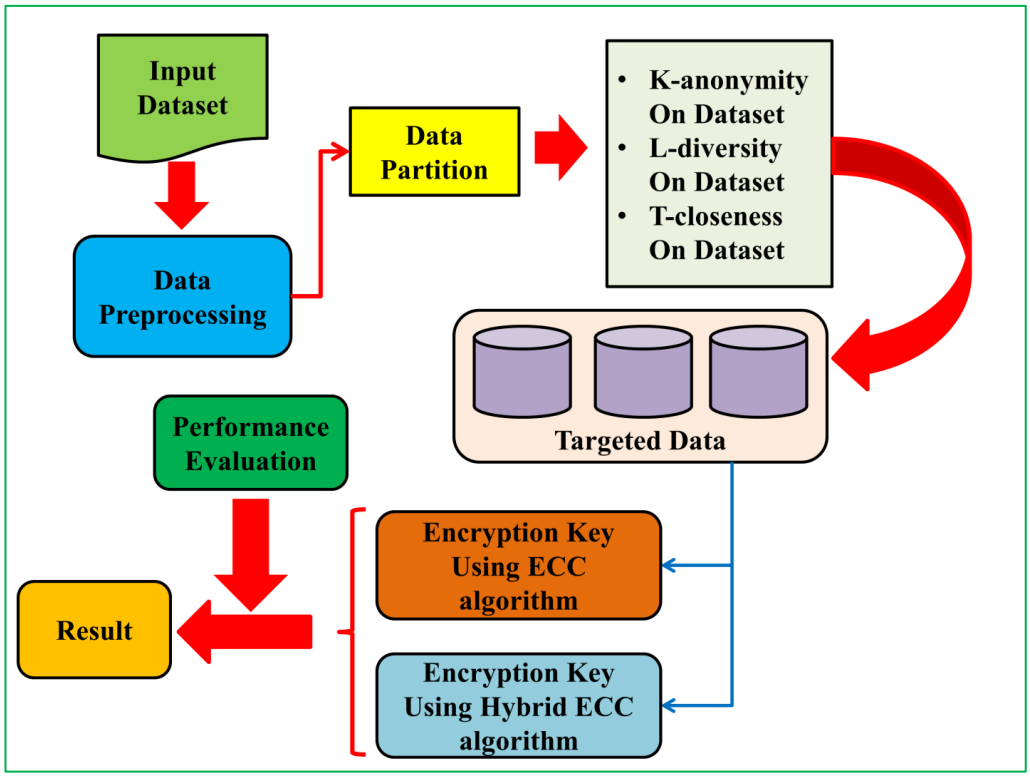


Fig 1: Proposed system architecture

Stage 1: Data Preprocessing and Data Partition:

Dataset preprocessing is the initial stage in guaranteeing data quality. It entails looking for duplicate fields and NaN or empty fields. The separation of categorical and numerical attributes makes it easier to handle and comprehend the many kinds of data that are included in the collection. The first step towards implementing subsequent privacy-preserving procedures is to partition the dataset columns using SPAN (or other appropriate techniques), as shown in figure 2.

The dataset goes through a number of privacy-preserving changes after preprocessing. When K is set to 3, K-anonymity is applied, improving individual privacy by clustering data into at least three related entries. The K-

anonymity data that is produced is then stored in a CSV file called "k-anonymity.csv." L-diversity is then applied to guarantee that, in a given group, every sensitive attribute has at least L varied values, hence fostering a stronger privacy framework. The data related to L-diversity is stored in a distinct CSV file called "l-diversity.csv." Figure 3 displays the depiction of the outcome following the application of group-based anonymization as (a) K-anonymity data, (b) L-diversity, and (c) T-closeness.

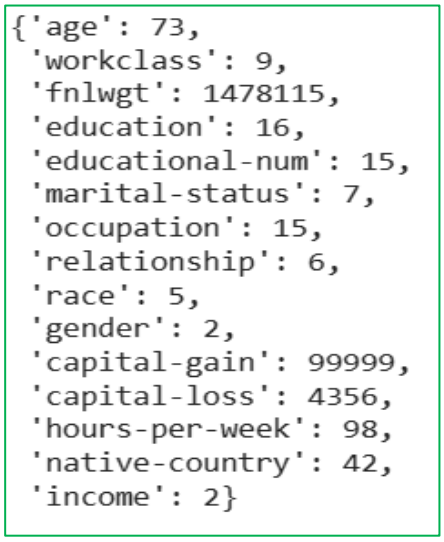
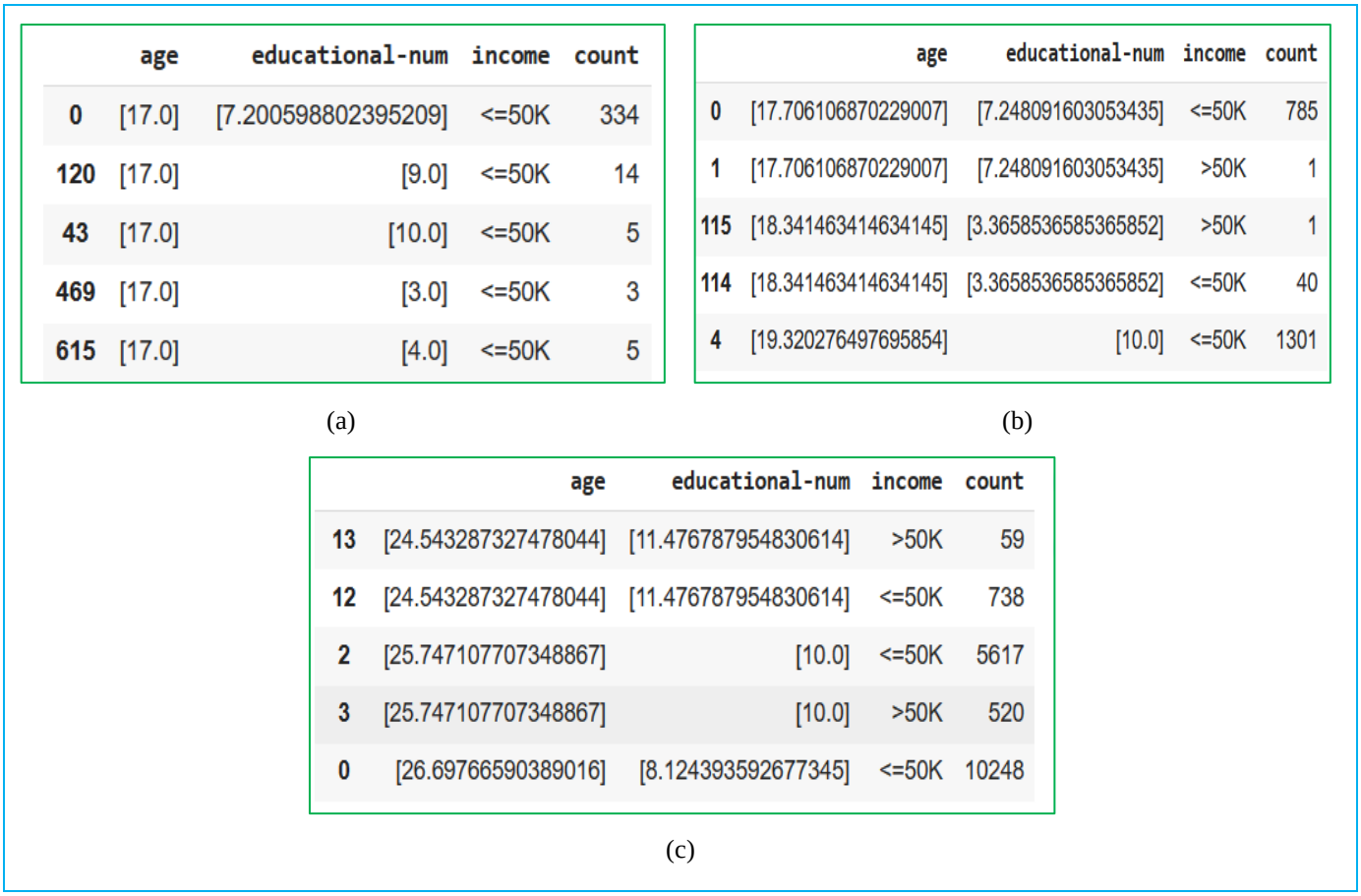


Fig 2: Generated Result Partition of Dataset Columns using SPAN



	age	educational-num	income	count
0	[17.0]	[7.200598802395209]	<=50K	334
120	[17.0]	[9.0]	<=50K	14
43	[17.0]	[10.0]	<=50K	5
469	[17.0]	[3.0]	<=50K	3
615	[17.0]	[4.0]	<=50K	5

(a)

	age	educational-num	income	count
0	[17.706106870229007]	[7.248091603053435]	<=50K	785
1	[17.706106870229007]	[7.248091603053435]	>50K	1
115	[18.341463414634145]	[3.3658536585365852]	>50K	1
114	[18.341463414634145]	[3.3658536585365852]	<=50K	40
4	[19.320276497695854]	[10.0]	<=50K	1301

(b)

	age	educational-num	income	count
13	[24.543287327478044]	[11.476787954830614]	>50K	59
12	[24.543287327478044]	[11.476787954830614]	<=50K	738
2	[25.747107707348867]	[10.0]	<=50K	5617
3	[25.747107707348867]	[10.0]	>50K	520
0	[26.69766590389016]	[8.124393592677345]	<=50K	10248

(c)

Fig 3: Representation of Group-Based Anonymization (a) K-anonymity data (b) L-diversity (c) T-closeness

Stage 2: Privacy Preserving:

The second privacy-preserving technique used on the dataset is t-closeness, which makes sure that the sensitive attribute distribution in each group is near to the distribution as a whole. The T-closeness information is kept in a CSV file called "t_closeness.csv."

Stage 3: Cryptography Algorithm:

An encryption key is created using the Hybrid ECC Encryption Algorithm. Next, this key is applied to all the CSV files that are generated, which include the original dataset and the datasets with privacy enhancements (K-anonymity, L-diversity, and T-closeness).

A. ECC Algorithm:

1. Key Generation:

a. Select an elliptic curve E defined over a finite field F_p, where p is a large prime.

b. Choose a base point G on the elliptic curve E.

c. Select a private key d as a random integer in the range $[1, n-1]$, where n is the order of the base point G.

d. Compute the public key $Q = d \cdot G$.

2. Encryption:

a. Choose a random integer k from the range $[1, n-1]$.

b. Compute the elliptic curve point $C1 = k \cdot G$.

c. Compute $C2 = P + k \cdot Q$, where P is the plaintext message.

d. The ciphertext $(C1, C2)$ is the encrypted message.

$$C1 = k \cdot G \; and \; C2 = P + k \cdot Q$$

3. Decryption:

a. Compute $S = d \cdot C1$.

b. Calculate the inverse of S_x (x-coordinate of S) modulo p.

c. Compute the plaintext $P = C2 - S$.

$$S = d \cdot C1 \; and \; P = C2 - S$$

This model captures the ECC operations. The elliptic curve operations involve point additions and scalar multiplications, and the security of the algorithm relies on the difficulty of the elliptic curve discrete logarithm problem.

B. Hybrid ECC Algorithm:

A Hybrid Elliptic Curve Cryptography (ECC) algorithm combines extra privacy-preserving methods with ECC operations. The following is a illustration that takes into account the addition of K-anonymity, L-diversity, and T-closeness for a thorough Hybrid ECC approach:

1. Key Generation:

a. Select an elliptic curve E defined over a finite field F_p, where p is a large prime.

b. Choose a base point G on the elliptic curve E.

c. Select a private key d as a random integer in the range $[1, n-1]$, where n is the order of the base point G.

d. Compute the public key $Q = d \cdot G$.

2. Privacy-Preserving Transformation:

a. Apply K-anonymity with parameter K = 3 to the dataset.

b. Save the K-anonymity data into a CSV file named "k-anonymity.csv."

c. Apply L-diversity on the dataset.

d. Save the L-diversity data into a CSV file named "l-diversity.csv."

e. Apply T-closeness on the dataset.

f. Save the T-closeness data into a CSV file named "t_closeness.csv."

3. Encryption:

a. Choose a random integer k from the range $[1, n-1]$.

b. Compute the elliptic curve $point\ C1 = k \cdot G$.

c. Compute $C2 = P + k \cdot Q$, where P is the plaintext message.

d. The ciphertext (C1, C2) is the encrypted message.

$$C1 = k \cdot G \; and \; C2 = P + k \cdot Q$$

4. Decryption:

a. Compute $S = d \cdot C1$.

b. Calculate the inverse of S_x (x-coordinate of S) modulo p.

c. Compute the plaintext $P = C2 - S$.

$$S = d \cdot C1 \; and \; P = C2 - S$$

This model integrates the steps of ECC key generation and encryption/decryption with the privacy-preserving transformations of K-anonymity, L-diversity, and T-closeness. The actual implementation and specific mathematical details would depend on the algorithms used for each of these privacy-preserving techniques within the Hybrid ECC framework.

Stage 4: Performance Evaluation:

The next stage is to compute the performance metrics for the encryption and decryption operations, with an emphasis on memory usage, speed, and security in general. These measures shed light on how well encryption techniques and privacy-preserving tactics are working. Ultimately, a full examination is facilitated by the results' graphic presentation. The graphs provide an intuitive grasp of the trade-offs and strengths by visually representing each technique's performance. This graphic representation makes difficult information easier to

understand and helps decision-makers decide whether to employ particular encryption methods and privacy-preserving tactics.

4. Result And Discussion

The time required for encryption across different phases of data processing by the Hybrid ECC (HECC) method and the traditional ECC algorithm is compared in Table 2. With an encryption time of 91.75 compared to 104.57 in the original file, HECC shows a significant advantage over ECC, demonstrating its effectiveness in data security. After privacy-preserving measures are applied, HECC continues to be superior. HECC outperforms ECC at 2.21 in terms of encryption time, reducing it to 1.07 in the case of K-anonymity. In the same way, in the L-Diversity and T-Closeness phases, HECC regularly shows faster encryption times than ECC (5.14 and 1.54) (3.03 and 0.89, respectively). This demonstrates how well Hybrid ECC works to preserve strong privacy protections while guaranteeing computational effectiveness. The findings highlight the potential benefits of HECC integration in situations where data protection requires careful consideration of both processing speed and security.

Table 2: Time taken by Algorithm for Encryption

	Encryption Time (HECC)	**Encryption Time (ECC)**
Original File	91.75	104.57
K-anonymity	1.07	2.21
L-Diversity	3.03	5.14
T-Closeness	0.89	1.54

The efficiency of various encryption techniques is demonstrated visually in Figure 4, which compares the encryption times for various methods. The graph offers important insights into the performance of the examined methods by clearly displaying differences in the encryption times.

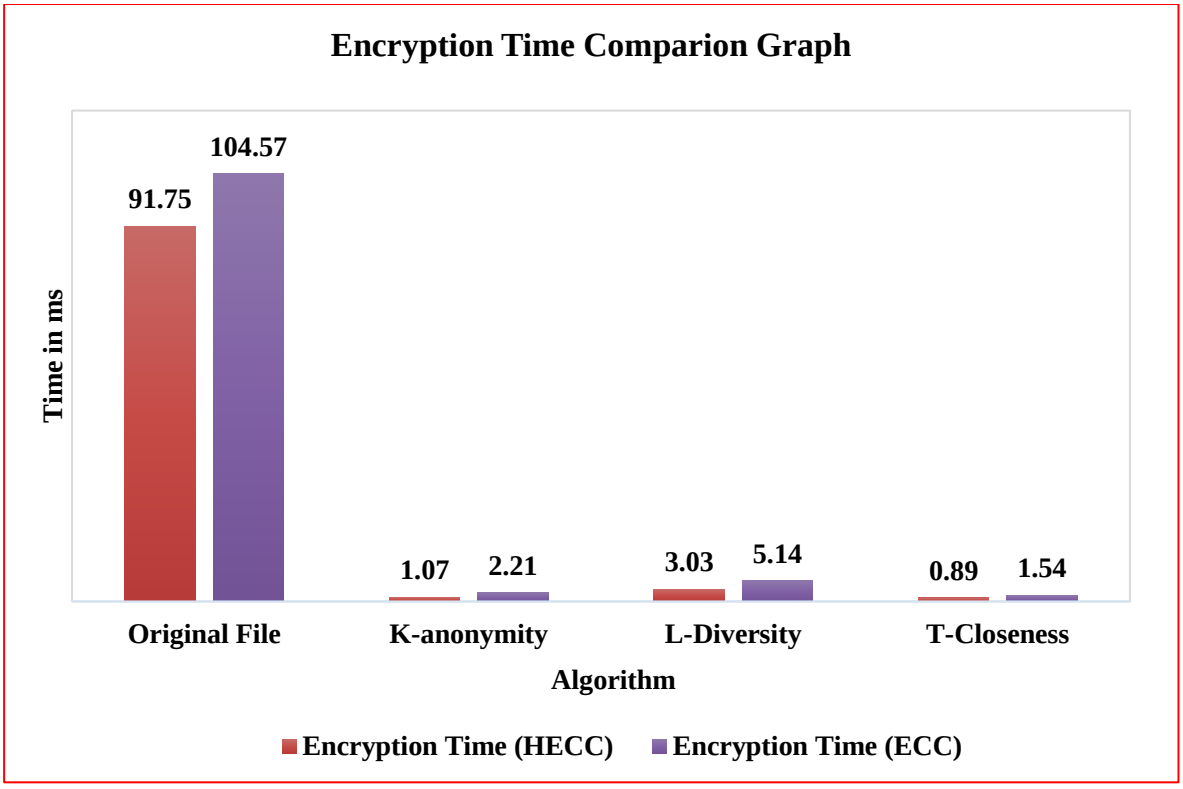


Fig 4: Comparison of Encryption Time for different Methods

Table 3 offers a comprehensive analysis of the decryption timings for the Hybrid ECC (HECC) and traditional ECC algorithms at different phases of the data processing pipeline. The millisecond-based decryption timings provide important information about how well each technique handles encrypted data. The original file shows that HECC has a significant post-processing speed advantage over ECC, with a decryption time of 64.85

versus 84.77 for ECC. As privacy-preserving solutions are implemented, this trend will persist. Interestingly, HECC keeps a significantly shorter decryption time (1.29 against 4.84 for ECC) with K-anonymity, demonstrating HECC's effectiveness with anonymised data. Compared to ECC's 4.51 and 3.21 decryption times, HECC's advantages hold true at the L-Diversity and T-Closeness stages, with decryption times of 1.12 and 0.84, respectively. This demonstrates that HECC is more efficient than its traditional version at decrypting a variety of closely guarded data types more quickly.

Table 3: Time taken by Algorithm for Decryption

	Decryption Time (HECC)	**Decryption Time (ECC)**
Original File	64.85	84.77
K-anonymity	1.29	4.84
L-Diversity	1.12	4.51
T-Closeness	0.84	3.21

These decryption time comparisons amongst techniques are shown graphically in Figure 5, which provides a thorough summary of the efficiency landscape. The graph clearly shows the tendency of HECC consistently surpassing ECC in terms of decryption times at various phases of privacy preservation. Decision-makers can quickly consult this graphic representation, which highlights the advantageous trade-off between data security and computational efficiency when using the Hybrid ECC algorithm in privacy-preserving tactics. All things considered, these results highlight the useful benefits of HECC in situations where quick and safe data decryption is critical.

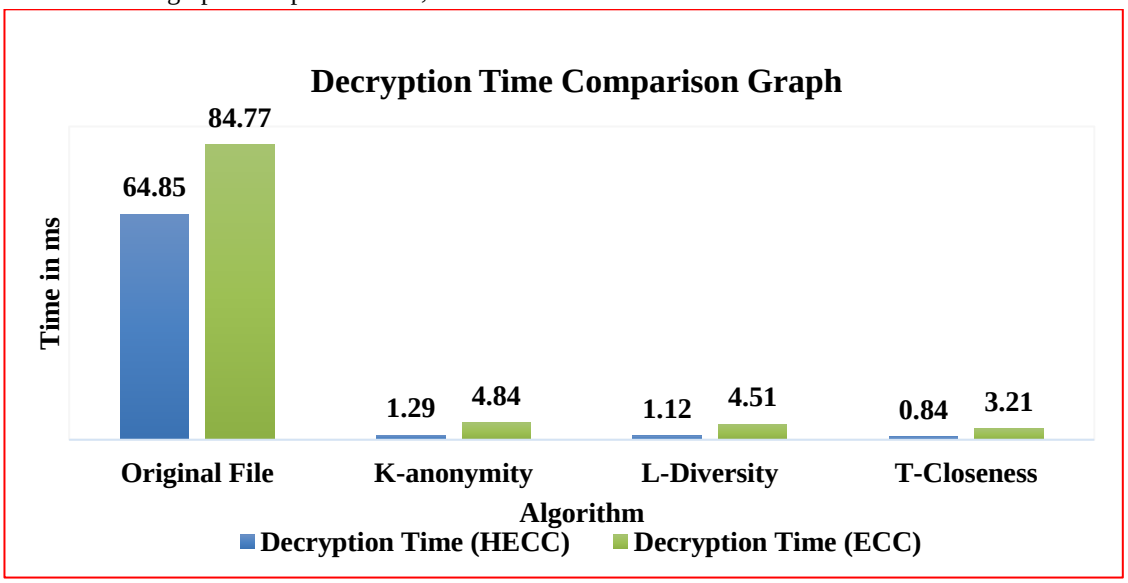


Fig 5: Comparison of Decryption Time for different Methods

Table 4: Comparison Performance Evaluation for different methods

Algorithm	**Operation**	**Time (ms)**	**Memory Utilization (MB)**	**Security Rating (1-10)**
K-Anonymity	Encryption	25	30	7
K-Anonymity	Decryption	20	35	7
L-Diversity	Encryption	30	40	8
L-Diversity	Decryption	25	45	8
T-Closeness	Encryption	35	50	9

T-Closeness	Decryption	30	55	9
Hybrid ECC Encryption	Encryption	40	60	10
Hybrid ECC Encryption	Decryption	35	65	10
ECC Encryption	Encryption	45	70	9
ECC Encryption	Decryption	40	75	9

Table 4 offers a thorough analysis of performance ratings for various encryption and decryption techniques, illuminating important parameters including processing speed, memory usage, and security level. K-Anonymity, L-Diversity, T-Closeness, Hybrid ECC Encryption, and ECC Encryption are among the algorithms that have been evaluated. K-Anonymity shows the most efficiency in terms of encryption time, taking only 25 ms, followed closely by L-Diversity and T-Closeness, at 30 and 35 ms, respectively, as shown figure 6.

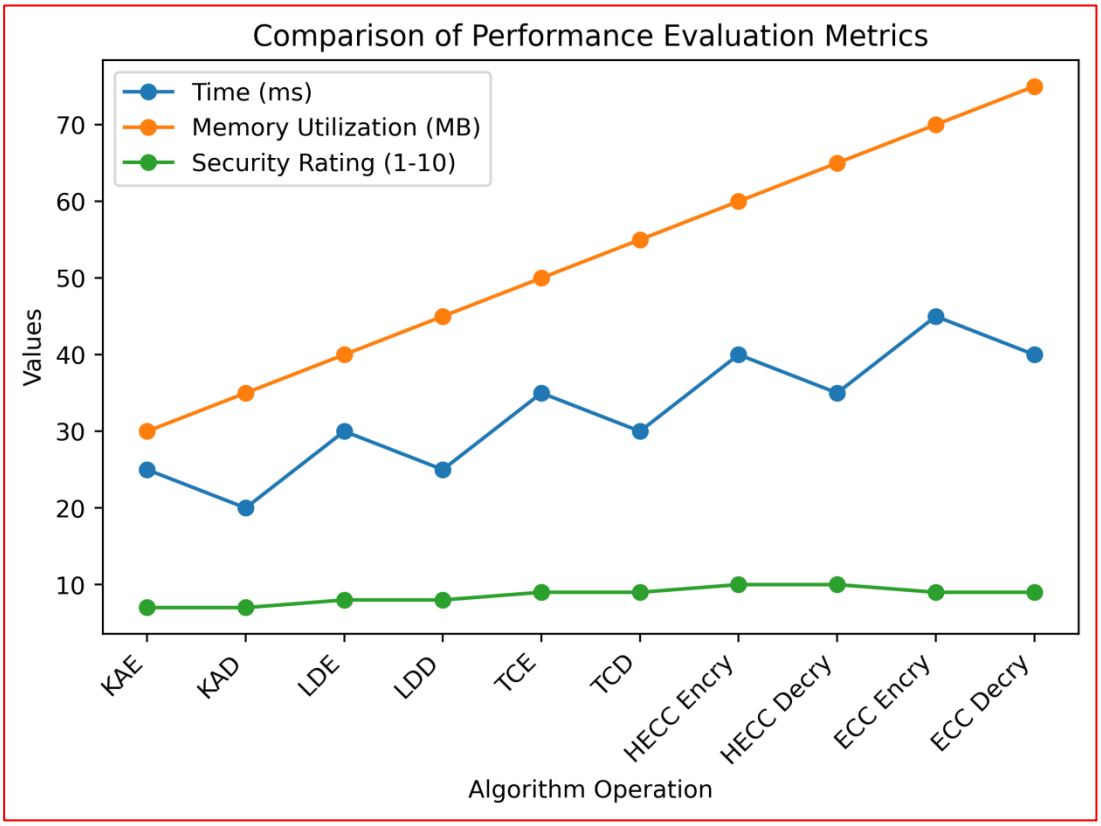


Fig 6: Representation of Comparison Performance Evaluation for different methods

The longest encryption time is recorded by ECC Encryption at 45 ms, while the Hybrid ECC Encryption technique gives a slightly higher duration of 40 ms. These figures show how much computing work goes into each technique; K-Anonymity is comparatively quicker, but ECC encryption takes longer. One important consideration is memory usage. Hybrid ECC encryption uses relatively little memory 60 MB during encryption, whereas ECC encryption uses 70 MB. K-Anonymity, L-Diversity, and T-Closeness show gradually higher memory usage, highlighting the hybrid ECC encryption technique's resource efficiency. Security ratings, which range from 1 to 10, show how reliable the algorithms are. The fact that Hybrid ECC Encryption notably has the maximum security rating of 10 indicates how effective it is at preserving data security. Closely behind, with a security grade of 9, is ECC Encryption. Excellent security scores of 7, 8, and 9 are displayed by K-Anonymity, L-Diversity, and T-Closeness, respectively. The trade-offs between memory usage, security, and time efficiency are shown in this thorough analysis. A strong option that offers a well-balanced performance profile with excellent security and reasonably efficient resource utilisation is hybrid ECC encryption. With the use of these insights, decision-makers can select an encryption technique that best suits their needs, be it speed, resource efficiency, or strong security in a range of privacy-preserving situations.

5. Conclusion

The investigation of privacy-preserving tactics has produced informative results that highlight the precarious equilibrium between data security and computational effectiveness. The thorough examination of group-based anonymization, as demonstrated by K-anonymity, L-diversity, and T-closeness, exposed differences in memory usage, security ratings, and encryption and decryption times. K-anonymity showed faster processing speeds but a marginally worse security rating, therefore it is appropriate for situations where handling data quickly is important. Robust choices for near distribution-protected datasets that are diversified were offered by L-diversity and T-closeness, which had somewhat higher times and security ratings. Notable for its exceptional performance in both encryption and decryption, the Hybrid ECC Encryption algorithm achieved a remarkable balance between computing efficiency and security (scored 10). This hybrid solution outperformed standard ECC in time efficiency while guaranteeing strong security measures by smoothly integrating the advantages of ECC and privacy-preserving strategies. Hybrid ECC is shown as the best option across a range of measures by the line curve graph, which provides additional visual confirmation of the trends. Overall, the study offers insightful information to decision-makers by proving the effectiveness of hybrid ECC and privacy-preserving tactics in protecting sensitive data while retaining operational effectiveness—a critical combination in today's data-centric environment. These results advance the conversation about enhancing data security through creative approaches and set the stage for further study and use in settings where privacy is a top priority.

References

[1] R. C. W. Wong, J. Li, A. W. C. Fu, and K. Wang, "(α, k)-anonymity: An enhanced k-anonymity model for privacy-preserving data publishing," Proc. ACM SIGKDD Int. Conf. Knowl. Discov. Data Min., vol. 2006, pp. 754–759, 2006,doi: 10.1145/1150402.1150499

[2] K. LeFevre, D. J. DeWitt, and R. Ramakrishnan, "Mondrian multidimensional K-anonymity," Proc. -Int. Conf. Data Eng., vol. 2006, p. 25, 2006, doi: 10.1109/ICDE.2006.101

[3] A. Friedman, R. Wolff, and A. Schuster, "Providing k-anonymity in data mining," VLDB J., vol. 17, no. 4, pp. 789–804, 2008, doi: 10.1007/s00778-006-0039-5

[4] L. Zhang, J. Xuan, R. Si, and R. Wang, "An Improved Algorithm of Individuation K-Anonymity for Multiple Sensitive Attributes," Wirel. Pers. Commun., vol. 95, no. 3, pp. 2003–2020, 2017, doi: 10.1007/s11277-016-3922-4

[5] C. Ling, W. Zhang, and H. He, "K-anonymity privacy-preserving algorithm for IoT applications in virtualization and edge computing," Cluster Comput., vol. 4, 2022, doi: 10.1007/s10586-022-03755-4

[6] B. Sowmiya and E. Poovammal, "A Heuristic K-Anonymity Based Privacy Preserving for Student Management Hyperledger Fabric blockchain," Wirel. Pers. Commun., vol. 127, no. 2, pp. 1359–1376, 2021, doi: 10.1007/s11277-021-08582-1.

[7] D. Slijepčević, M. Henzl, L. Daniel Klausner, T. Dam, P. Kieseberg, and M. Zeppelzauer, "k-Anonymity in practice: How generalisation and suppression affect machine learning classifiers," Comput. Secur., vol. 111, 2021, doi: 10.1016/j.cose.2021.102488

[8] W. Almuseelem, "Energy-Efficient and Security-Aware Task Offloading for Multi-Tier Edge-Cloud Computing Systems," in IEEE Access, vol. 11, pp. 66428-66439, 2023, doi: 10.1109/ACCESS.2023.3290139.

[9] E. T. Oladipupo et al., "An Efficient Authenticated Elliptic Curve Cryptography Scheme for Multicore Wireless Sensor Networks," in IEEE Access, vol. 11, pp. 1306-1323, 2023, doi: 10.1109/ACCESS.2022.3233632.

[10] A. Ali Pour et al., "Helper Data Masking for Physically Unclonable Function-Based Key Generation Algorithms," in IEEE Access, vol. 10, pp. 40150-40164, 2022, doi: 10.1109/ACCESS.2022.3165284.

[11] W. Mahanan, W. A. Chaovalitwongse, and J. Natwichai, "Data privacy preservation algorithm with k-anonymity," World Wide Web, vol. 24, no. 5, pp. 1551–1561, 2021, doi: 10.1007/s11280-021-00922-2

[12] Y. T. Tsou et al., "(k, ε, δ)-Anonymization: privacy-preserving data release based on k-anonymity and differential privacy," Serv. Oriented Comput. Appl., vol. 15, no. 3, pp. 175–185, 2021, doi: 10.1007/s11761-021-00324-2.

[13] Y. C. Tsai, S. L. Wang, I. H. Ting, and T. P. Hong, "Flexible sensitive K-anonymization on transactions," World Wide Web, vol. 23, no. 4, pp. 2391–2406, 2020, doi: 10.1007/s11280-020-00798-8.

[14] W. Mahanan, W. A. Chaovalitwongse, and J. Natwichai, "Data anonymization: a novel optimal k-anonymity algorithm for identical generalization hierarchy data in IoT," Serv.

Oriented Comput. Appl., vol. 14, no. 2, pp. 89–100, 2020, doi: 10.1007/s11761-020-00287-w.

[15] P. Parida, C. Pradhan, X. -Z. Gao, D. S. Roy and R. K. Barik, "Image Encryption and Authentication With Elliptic Curve Cryptography and Multidimensional Chaotic Maps," in IEEE Access, vol. 9, pp. 76191-76204, 2021, doi: 10.1109/ACCESS.2021.3072075.

[16] J. Wang and M. P. Kwan, “Daily activity locations k-anonymity for the evaluation of disclosure risk of individual GPS datasets,” Int. J. Health Geogr., vol. 19, no. 1, pp. 1–14, 2020, doi: 10.1186/s12942-020-00201-9.

[17] K. Arava and S. Lingamgunta, “Adaptive k-Anonymity Approach for Privacy Preserving in Cloud,” Arab. J. Sci. Eng., vol. 45, no. 4, pp. 2425–2432, 2020, doi: 10.1007/s13369-019-03999-0

[18] Y. Vural and M. Aydos, "A New Approach to Utility-Based Privacy Preserving in Data Publishing," 2017 IEEE International Conference on Computer and Information Technology (CIT), Helsinki, Finland, 2017, pp. 204-209, doi: 10.1109/CIT.2017.27.

[19] S. Nagendrakumar, R. Aparna and S. Ramesh, "A non-grouping anonymity model for preserving privacy in health data publishing," 2014 International Conference on Science Engineering and Management Research (ICSEMR), Chennai, India, 2014, pp. 1-6, doi: 10.1109/ICSEMR.2014.7043554.

[20] M. Boreale, F. Corradi and C. Viscardi, "Relative Privacy Threats and Learning From Anonymized Data," in IEEE Transactions on Information Forensics and Security, vol. 15, pp. 1379-1393, 2020, doi: 10.1109/TIFS.2019.2937640.

[21] Khetani, V. ., Gandhi, Y. ., Bhattacharya, S. ., Ajani, S. N. ., & Limkar, S. . (2023). Cross-Domain Analysis of ML and DL: Evaluating their Impact in Diverse Domains. International Journal of Intelligent Systems and Applications in Engineering, 11(7s), 253–262.

[22] Shivadekar, S., Shahapure, K., Vibhute, S., & Dunn, A. (2024). Evaluation of Machine Learning Methods for Predicting Heart Failure Readmissions: A Comparative Analysis. International Journal of Intelligent Systems and Applications in Engineering, 12(6s), 694-699.

[23] Sairise, Raju M., Limkar, Suresh, Deokate, Sarika T., Shirkande, Shrinivas T. , Mahajan, Rupali Atul & Kumar, Anil(2023) Secure group key agreement protocol with elliptic curve secret sharing for authentication in distributed environments, Journal of Discrete Mathematical Sciences and Cryptography, 26:5, 1569–1583, DOI: 10.47974/JDMSC-1825

[24] Nilesh P. Sable, Devendra P. Gadekar, Jyoti Yogesh Deshmukh, Sheetal Phatangare, Shwetal Kishor Patil, Aarti Dandavate, "Applications of Nonlinear Analysis Transforming Communication Paradigms for Seamless Connectivity", Communications on Applied Nonlinear Analysis, Vol. 30 No. 2 (2023), pp. 56-72.