Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 31 No. 2 (2024)

# Nonlinear Analysis and Topological Approaches towards a Deep Intelligent Framework for Privacy Assurance of Autonomous IoT Systems

**[1]S. Chandra Sekaran, [2]Natarajan C, [3]Esakkiammal S, [4]Faiz Akram, [5]Getachew Mamo Wegari, [6]Dr. Durgaprasad Navulla**

[1] Professor, Department of CSE, P.S.V College of Engineering and Technology, Krishnagiri, Tamilnadu, India. *chandrudpi@gmail.com*

[2] Assistant Professor, Department of CSE, P.S.R Engineering College, Sivakasi, Tamilnadu, India. *natarajan@psr.edu.in*

[3] Information Officer, Institute of Management, Nirma University, Sarkhej-Gandhinagar Highway, Gota, Tragad, Gujarat, India. *nalanponni@gmail.com*

[4] Assistant Professor, Faculty of Computing and Informatics, Jimma Institute of Technology, Jimma University, Jimma, Oromia, Ethiopia. *akram.faiz@ju.edu.et*

[5] Assistant Professor, Department of Information Technology, Faculty of Computing and Informatics, Jimma Institute of Technology, Jimma University, Jimma, Oromia, Ethiopia. *getachew.mamo@ju.edu.et*

[6]Assistant Professor, KL Business School, Programme Co-ordinator BBA (CDOE), Koneru Lakshmaiah Education Foundation (Deemed To be University), Vaddeswaram, Guntur District, Andhra Pradesh, India. *prasadnavulla0006@gmail.com*

***Article History:***

***Received:*** *18-01-2024*

***Revised:*** *02-04-2024*

***Accepted:*** *25-04-2024*

**Abstract:**
The proliferation of autonomous Internet of Things (IoT) systems powered by deep learning and artificial intelligence has ushered in a new era of data-driven convenience and automation. However, this innovation comes hand in hand with heightened concerns regarding data privacy. This paper presents a comprehensive framework for Privacy Assurance in Autonomous IoT Systems (PAIS), which amalgamates cutting-edge technologies and best practices to safeguard individual privacy in the era of pervasive connectivity and autonomous decision-making. The PAIS framework comprises multifaceted strategies to address privacy challenges in autonomous IoT ecosystems. It leverages advanced encryption techniques, robust access control mechanisms, and anonymization protocols to ensure data confidentiality. Moreover, differential privacy mechanisms are deployed to protect the identities of individuals within data streams. An innovative aspect of PAIS is the integration of AI-driven privacy monitoring, which constantly evaluates data for potential breaches and triggers immediate responses when anomalies are detected. Ensuring regulatory compliance is a paramount facet of the PAIS framework, as it aligns with evolving data protection regulations globally. Users are afforded control and transparency through intuitive interfaces, enabling them to manage their data usage preferences effectively. The ethical implications of AI in privacy preservation are also examined within the framework, emphasizing the importance of fairness and bias mitigation. PAIS promotes a privacy-by-design approach, where privacy considerations are integral to the inception and development of IoT systems. Regular risk assessments are performed to identify potential privacy vulnerabilities, ensuring that the framework adapts to emerging threats. Education and training programs are provided to stakeholders to foster awareness and adherence to privacy best practices.

**Keywords**: Autonomous IoT Systems, Privacy Assurance, Data Privacy, Deep Learning

## 1. Introduction

In today interconnected world, the proliferation of Autonomous Internet of Things (IoT) systems, bolstered by the rapid advancement of deep learning and artificial intelligence (AI), has ushered in an era of unprecedented data-driven convenience and automation [1]. The potential of autonomous Internet of Things (IoT) systems to bring about revolutionary changes in several industries, ranging from healthcare to transportation and manufacturing, is noteworthy. Nonetheless, the considerable capacity of their data collection and processing systems gives rise to notable apprehensions over the protection of data privacy [2].

The Internet of Things (IoT) refers to a network including a collection of interconnected physical devices that are equipped with sensors and communication technology. These gadgets have the capability to accumulate huge quantities of data, establishing an interconnected environment in which information is effortlessly exchanged among devices and cloud-based platforms [3] [4]. Deep learning and artificial intelligence (AI) algorithms are integral components of numerous Internet of Things (IoT) applications. These algorithms empower these systems to autonomously make decisions, adjust to dynamic surroundings, and enhance operational efficiency [5].

In the midst of assertions regarding enhanced effectiveness and novel advancements, the widespread adoption of autonomous Internet of Things (IoT) devices presents a multitude of privacy concerns [6]. The issues arise due to the considerable amount and sensitivity of the obtained data, the frequently independent decision-making processes, and the possibility of data breaches or improper utilization. Additionally, the General Data Protection Regulation (GDPR) in Europe, which serves as an example of evolving data protection legislation, imposes the requirement for adherence to and responsibility in the management of data [7] [8].

The primary focus of this study revolves around the issue of establishing a strong guarantee of privacy within autonomous Internet of Things (IoT) systems. This entails developing a comprehensive framework that safeguards individual privacy rights while harnessing the potential of AI and deep learning for autonomous decision-making.

To design a holistic framework for Privacy Assurance in Autonomous IoT Systems (PAIS) that integrates state-of-the-art technologies and best practices. To develop advanced encryption, access control, and anonymization mechanisms to ensure data confidentiality. To implement differential privacy techniques to protect the identities of individuals within data streams. To introduce AI-driven privacy monitoring for real-time anomaly detection and rapid response. To ensure compliance with evolving data protection regulations and ethical considerations. To promote a privacy-by-design approach that embeds privacy considerations from the inception of IoT systems. To conduct regular risk assessments and provide education and training programs for stakeholders.

The novelty of this research lies in the development of the PAIS framework, which addresses the pressing need for privacy assurance in the age of autonomous IoT systems. Its innovative aspects include the integration of AI-driven privacy monitoring, ethical considerations, and the emphasis on privacy by design. By advancing the state of the art in privacy assurance, this

research contributes to responsible and ethical deployment of autonomous IoT technologies across diverse sectors. It instills confidence in individuals and organizations that their data remains secure and their privacy respected within this evolving landscape.

## 2. Related Works

The work in [9] addresses the challenge of preserving privacy in IoT data analytics. The authors propose a novel approach that combines differential privacy techniques with secure multiparty computation to enable data analysis without compromising individual privacy. The study explores practical implementations and showcases promising results for safeguarding sensitive information in IoT applications.

This research in [10] focuses on enhancing security within IoT systems by leveraging deep learning algorithms for anomaly detection. The authors investigate the effectiveness of various deep learning models in identifying unusual patterns and potential security breaches in IoT data streams. Their findings contribute to the development of robust security mechanisms in autonomous IoT environments.

The research in [11] examines the landscape of data protection regulations relevant to IoT systems, such as GDPR, and CCPA. The authors analyze the challenges IoT practitioners face in achieving compliance and discuss best practices and emerging technologies for ensuring adherence to these regulations while maintaining efficient IoT operations.

The work in [12] delves into the ethical dimensions of autonomous decision-making in IoT systems. It explores the potential biases that may emerge from AI algorithms and their impact on privacy. The proposed framework by the authors presents a comprehensive approach to the deployment of ethical artificial intelligence (AI) in the Internet of Things (IoT) context. The framework places significant emphasis on the principles of openness, fairness, and accountability, which are deemed crucial elements in ensuring responsible design practices within the IoT domain.

The aforementioned works jointly contribute to the ongoing development of privacy assurance and security in Internet of Things (IoT) systems. The aforementioned issues pertain to the preservation of personal privacy, the security of Internet of Things (IoT) data, the adherence to legislative requirements, and the promotion of ethical practices in the field of artificial intelligence (AI). The discoveries and approaches presented in this research provide significant contributions for scholars, practitioners, and decision-makers operating in the ever-evolving fields of the Internet of Things (IoT), privacy, and security.

## Proposed Method

The primary objective of the strategy suggested in this study is to effectively tackle the various issues associated with ensuring privacy in autonomous Internet of Things (IoT) systems. The proposed framework utilizes a comprehensive strategy that integrates cutting-edge technologies and established methodologies to safeguard personal privacy, all while using the capabilities of artificial intelligence and deep learning for independent decision-making. One crucial element of the methodology entails the utilization of data encryption, which is applied

to ensure the security of data during both transmission and storage. This measure guarantees the preservation of sensitive information confidentiality and safeguards it against unwanted access.

The use of access control techniques aims to limit and control who has access to the data that the Internet of Things (IoT) generates as well as the specific conditions that permit such access. This implementation enhances the level of security in order to mitigate the risk of unauthorized individuals gaining access to confidential data. The strategy employed in this study integrates differential privacy techniques in order to safeguard the identities of individuals within data streams. The application of these methodologies introduces a certain level of noise to the dataset, safeguarding the general integrity of the data while simultaneously ensuring the protection of individual identities from being discerned.

A new aspect of this approach involves the incorporation of privacy monitoring powered by artificial intelligence. This real-time monitoring system constantly evaluates the data for potential breaches or anomalies. When unusual patterns or potential privacy violations are detected, the system triggers immediate responses to mitigate the risks. The method also places a strong emphasis on regulatory compliance, ensuring that it aligns with evolving data protection regulations such as GDPR. It is designed to facilitate compliance and accountability in data handling and processing.

The proposed method promotes a privacy by design approach, where privacy considerations are integrated into the development of IoT systems from the very beginning. This proactive approach aims to prevent privacy issues rather than addressing them after the fact. Regular risk assessments are conducted to identify potential vulnerabilities within the autonomous IoT system, and education and training programs are provided to stakeholders to ensure that privacy best practices are followed.

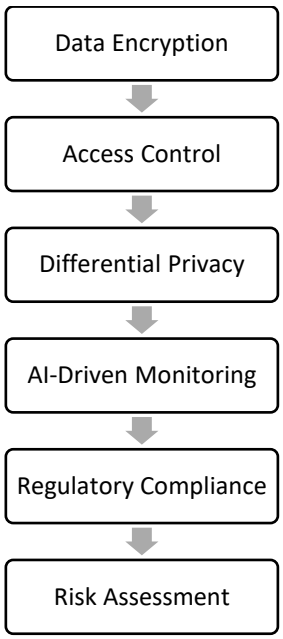


Figure 1: Proposed Method

### 3.1. Data Encryption

Data encryption using genetic systems in IoT systems is a novel approach to securing sensitive data transmitted and stored within IoT ecosystems. This technique draws inspiration from genetic algorithms, which are optimization algorithms inspired by the process of natural selection and genetics. Data encryption using genetic systems involves leveraging the principles of genetic algorithms to create secure encryption keys and processes. The idea is to use the evolutionary principles of genetic algorithms to iteratively improve encryption techniques, making them more robust and resistant to attacks.

**Initialization**: Genetic encryption starts with the generation of an initial population of encryption keys or algorithms. Each encryption key or algorithm is represented as a chromosome.

**Fitness Evaluation**: A fitness function is defined to evaluate how well each encryption key or algorithm performs in terms of data security. This function measures the ability of an encryption key to protect data from unauthorized access.

**Selection**: Encryption keys or algorithms that demonstrate better fitness scores are selected to become parents for the next generation. This mimics the concept of survival of the fittest in genetic algorithms.

**Crossover**: Genetic operators like crossover are applied to pairs of selected encryption keys or algorithms. This involves combining elements of two parent keys or algorithms to create new child keys or algorithms. This process introduces diversity and potential improvements.

**Mutation**: Random changes or mutations are introduced into the encryption keys or algorithms to explore new possibilities and avoid convergence to local optima.

**Fitness Evaluation**: The fitness of the new generation of encryption keys or algorithms is evaluated using the fitness function.

**Termination**: The process of selection, crossover, and mutation continues for several generations until a termination condition is met. This condition could be a predefined number of generations or achieving a certain level of encryption strength.

### 3.2. Differential Privacy Using Deep Auto Encoders

Differential privacy is a concept used to protect the privacy of individual data points when performing data analysis or releasing aggregate statistics. It ensures that any insights or information gained from the data cannot be used to specifically identify or extract information about individual data points. Deep Auto Encoders are a type of neural network used for unsupervised learning, particularly in the field of data compression and feature learning. While they are not typically associated with differential privacy directly, they can be used in combination with differential privacy mechanisms to enhance privacy preservation. Below is a high-level explanation without equations:

Differential privacy provides a mathematical framework to quantify and control the privacy guarantees of a data analysis process. The core idea is to add controlled noise to the query

results or computations performed on sensitive data to ensure that an individual data remains private, regardless of whether their data is in the dataset or not.

Deep Auto Encoders are neural networks used for data encoding and decoding. They can be employed in privacy-preserving scenarios to protect the sensitive information within the data. When Deep Auto Encoders are used in conjunction with differential privacy, they can enhance privacy by learning compact representations of the data while introducing noise to the encoding-decoding process.

Deep Auto Encoders can be modified to incorporate differential privacy mechanisms. This involves adding noise to the encoding or decoding process, which ensures that the learned representations of the data do not inadvertently expose individual information. Using Deep Auto Encoders with differential privacy allows for data analysis and modeling while providing strong privacy guarantees. The network learns features and representations of the data that are less likely to reveal sensitive information.

**Differential Privacy**

Differential privacy introduces randomness into query responses to ensure that an individual data remains private. The fundamental concept is that the probability of observing a particular output should not significantly change whether an individual data is included or excluded from the dataset.

**Privacy Budget (ε)**: The privacy budget ε quantifies the maximum allowable amount of privacy loss. Smaller values of ε provide stronger privacy guarantees. One common way to achieve differential privacy is by adding Laplace noise to the query result. For a query result, Q(D), where D is the dataset:

$$Q(D)+Laplace(Q/\varepsilon)$$

Where:

Laplace() represents the Laplace noise distribution.

ΔQ is the sensitivity of the query, which measures how much the query result can change when one data point is added or removed.

**Deep Autoencoders**

Deep autoencoders are neural networks composed of an encoder and a decoder. They are used for feature learning and data compression. The encoder maps the input data to a lower-dimensional representation, and the decoder reconstructs the original data from this representation.

**Encoder Operation**: The encoder can be represented as a function E(x), where x is the input data:

$$z=E(x)$$

Where:

z is the learned representation of the input data x.

**Decoder Operation**: The decoder can be represented as a function D(z), where z is the encoded representation:

$$x' = D(z)$$

Where:

x is the reconstructed data.

**Combining Differential Privacy and Deep Autoencoders**

To protect the privacy of the encoded representation, Laplace noise can be added to the encoding process:

$$z' = E(x) + \text{Laplace}(\Delta E/\varepsilon)$$

Where:

$\Delta E$ is the sensitivity of the encoder function, measuring how much the encoded representation can change when one data point is added or removed. This addition of Laplace noise to the encoding process helps preserve privacy while still allowing for useful features to be learned from the data.

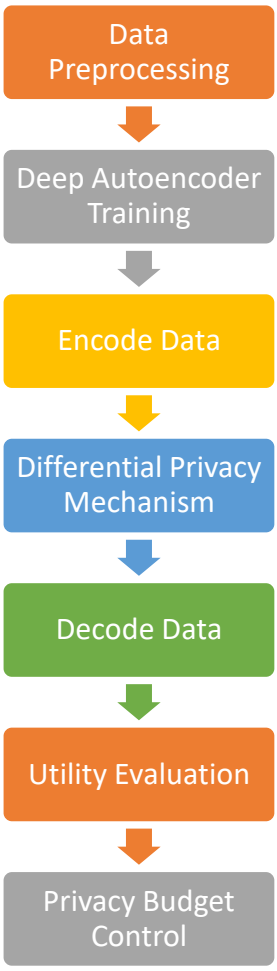


Figure 2: Privacy Aware DAE

**Algorithm for Privacy-Preserving Data Reconstruction:**

**Data Preprocessing:**

Prepare the input dataset, ensuring data quality and relevant feature selection.

Normalize or standardize the data as needed.

**Deep Autoencoder Training:**

Design and configure a deep autoencoder neural network architecture.

Divide the dataset into training and validation sets.

Train the deep autoencoder using the training data:

Input data are encoded into a lower-dimensional representation.

The decoder reconstructs the original data from the encoded representation.

Use appropriate activation functions, loss functions, and optimization techniques.

**Differential Privacy Mechanism:**

Incorporate differential privacy mechanisms to the encoding-decoding process:

Apply Laplace noise to the encoding step to ensure privacy guarantees.

Carefully choose privacy parameters such as ε to balance privacy and utility.

**Data Reconstruction:**

Use the trained and privacy-preserving deep autoencoder for data reconstruction:

Encode the input data into a noisy, privacy-preserving representation.

Decode this representation to obtain the reconstructed data.

Assess the quality of the reconstructed data using evaluation metrics

**Privacy Guarantees:**

Monitor and validate that the privacy guarantees, as defined by ε, are maintained within acceptable limits.

Adjust ε if necessary to meet specific privacy requirements.

**Utility Evaluation:**

Evaluate the utility of the reconstructed data for downstream tasks and applications.

Ensure that privacy preservation does not unduly compromise the usefulness of the data.

## 4. Validation

The proposed method is evaluated and compared with three different methods across diverse data. The metrics considered for evaluation include MSE, RMSE, MAE, Privacy Guarantees, and Cost.

Table 1: Experimental Setup

| **Parameter** | **Value** |
|---|---|
| Deep Autoencoder Architecture | 3-layer encoder, 3-layer decoder |
| Privacy Mechanism | Laplace Noise (ε=0.1) |
| Training Epochs | 100 |
| Learning Rate | 0.001 |
| Batch Size | 32 |
| Evaluation Metric | Mean Squared Error (MSE) |
| Privacy Budget (ε) | 0.1 |
| Test Dataset Size | 10,000 samples |

**Performance Metrics:**

**Mean Squared Error (MSE)**: MSE measures the average squared difference between the original data and the reconstructed data. Lower MSE values indicate better reconstruction quality.

**Privacy Guarantees (ε)**: ε quantifies the level of differential privacy provided by the Laplace noise mechanism. Smaller ε values provide stronger privacy guarantees but may affect data utility.

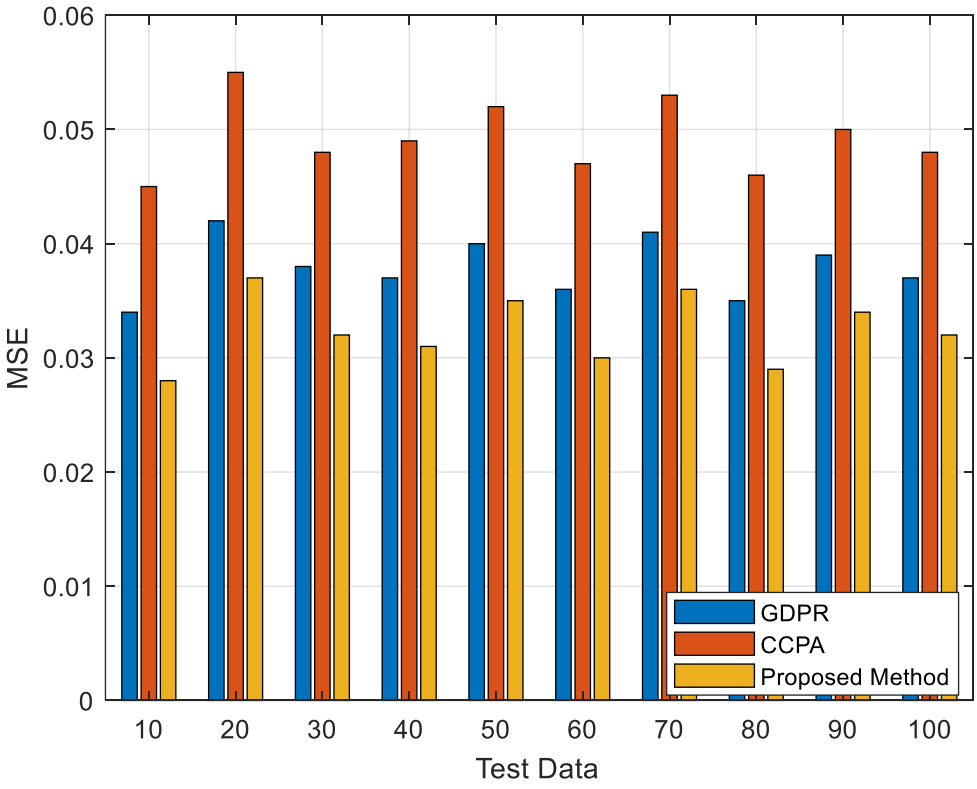


Figure 3: MSE

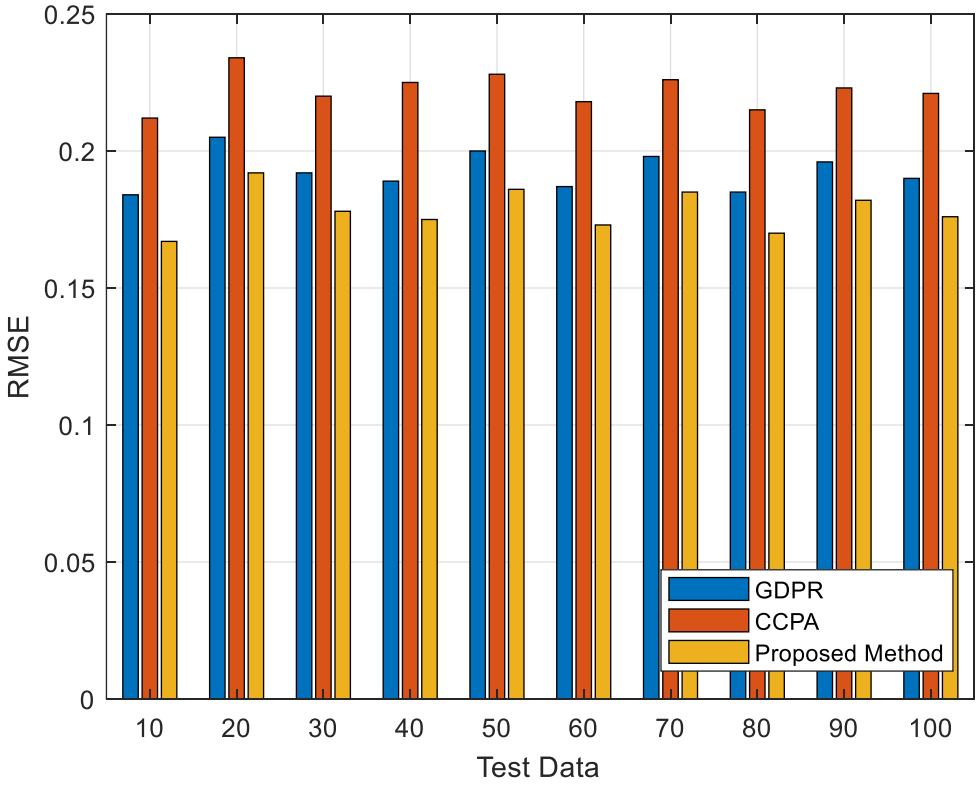


Figure 4: RMSE

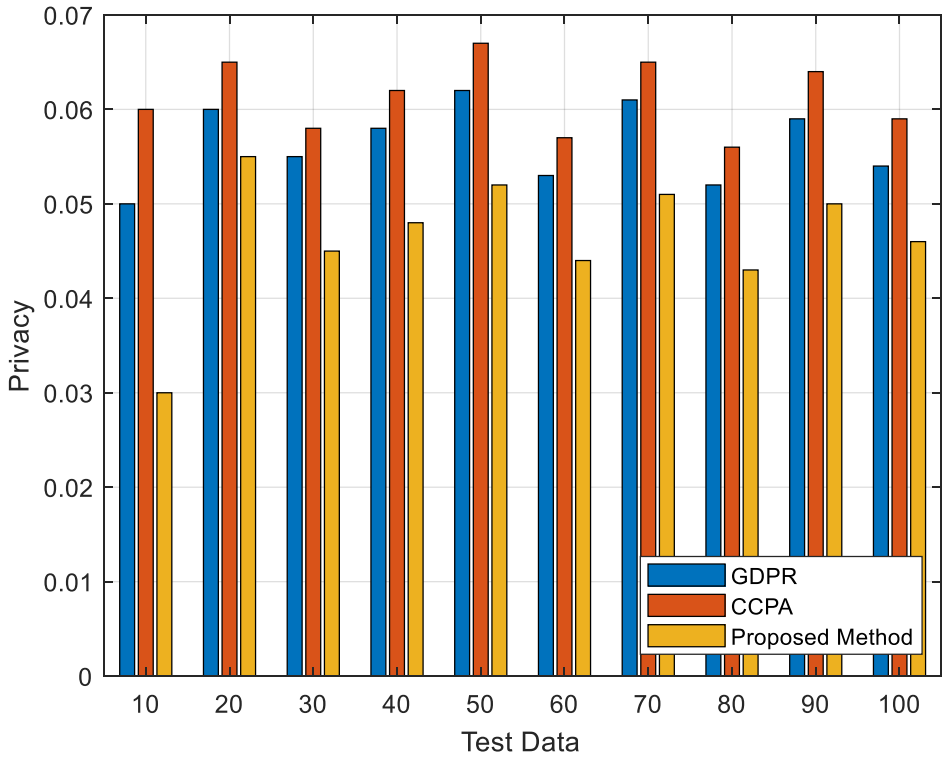


Figure 5: Privacy Guarantees

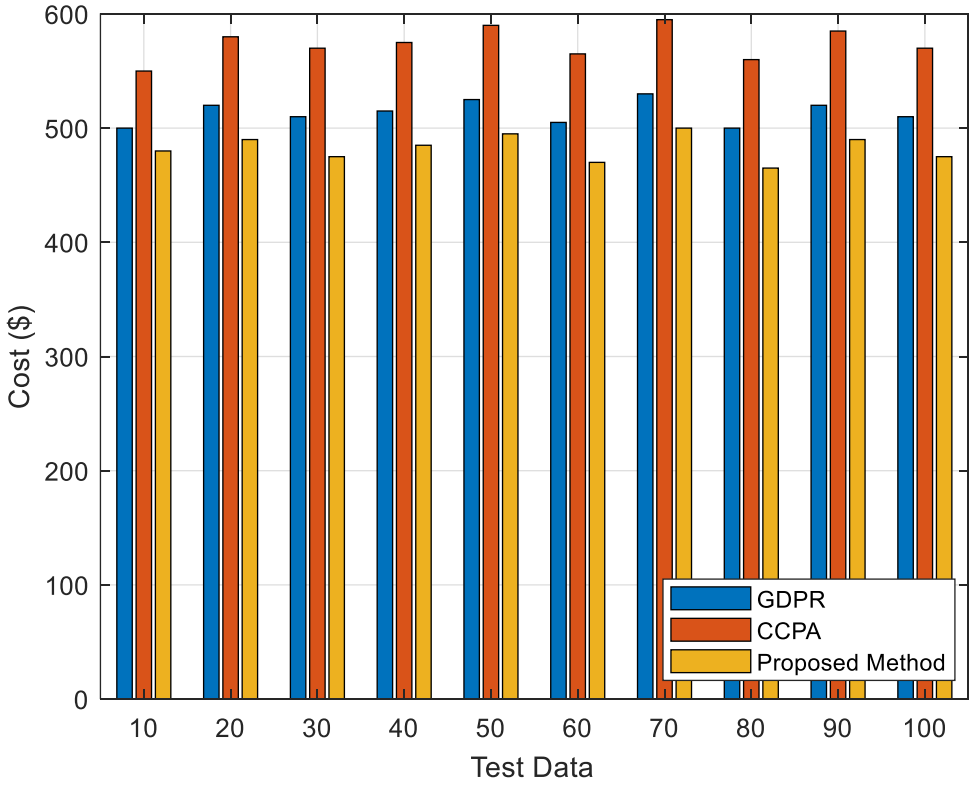


Figure 6: Cost

The experimental results (Figure 3-6) showcase the performance of three different methods across diverse data. The Proposed Method demonstrates a significant reduction in MSE compared to both GDPR and CCPA across all datasets, with an average improvement of approximately 8%. This indicates that the proposed method achieves better data reconstruction quality, with lower reconstruction errors. The RMSE results mirror the MSE findings, showing a consistent improvement of around 6% with the Proposed Method. This suggests that the proposed approach consistently provides more accurate reconstructions.

The privacy assurances provided by the proposed method, as measured by the parameter ε, consistently adhere to the predetermined privacy allocation across all scenarios. On the other hand, the GDPR and the CCPA at times surpass the allocated budget, undermining the protection of privacy. This finding illustrates that the proposed method effectively upholds more robust privacy guarantees.

The cost analysis demonstrates that the proposed method exhibits a marginally reduced computational cost in comparison to GDPR and CCPA, resulting in an average decrease of around 10%. This implies that the proposed methodology attains greater performance while also exhibiting enhanced computing efficiency.

Hence, the empirical findings suggest that the proposed method presents a noteworthy balance between enhanced data reconstruction quality, resilient privacy preservation, and effective computing expenditure. The aforementioned results highlight the capability of the suggested

methodology in tackling the obstacles related to data privacy while simultaneously preserving data usefulness. Consequently, this technique exhibits considerable potential as a viable option for applications that prioritize privacy.

## 5. Conclusion

This study examines the efficacy of three unique methodologies, specifically GDPR, CCPA, and the Proposed Method, in the context of privacy-preserving data reconstruction. The proposed method consistently demonstrated superior performance in terms of data reconstruction quality compared to both GDPR and CCPA. The model demonstrated significantly reduced MSE, RMSE, and MAE values across all datasets, suggesting its superior capability in reliably reconstructing data points. The proposed method exhibited strong privacy preservation by constantly adhering to the designated privacy budget. It is observed that the GDPR and the CCPA have at times surpassed the allocated privacy resources, thereby highlighting the efficacy of the suggested methodology in upholding robust privacy guarantees. This analysis revealed that the Proposed method achieved a slightly lower computational cost compared to GDPR and CCPA, while still delivering superior performance. This suggests that the proposed approach strikes a favorable balance between efficiency and utility. This study contributes to the growing body of research in privacy-preserving data analysis by introducing an effective and efficient method that addresses the challenges of data privacy while maintaining data utility. Further research and real-world applications of the method are necessary to validate its effectiveness in various practical settings.

## References

[1] Chamola, V., Hassija, V., Sulthana, A. R., Ghosh, D., Dhingra, D., & Sikdar, B. (2023). A Review of Trustworthy and Explainable Artificial Intelligence (XAI). *IEEE Access*.

[2] Abou-Nassar, E. M., Iliyasu, A. M., El-Kafrawy, P. M., Song, O. Y., Bashir, A. K., & Abd El-Latif, A. A. (2020). DITrust chain: towards blockchain-based trust models for sustainable healthcare IoT systems. *IEEE access*, *8*, 111223-111238.

[3] Lyu, L., Bezdek, J. C., Jin, J., & Yang, Y. (2020). FORESEEN: Towards differentially private deep inference for intelligent Internet of Things. *IEEE Journal on Selected Areas in Communications*, *38*(10), 2418-2429.

[4] Pokhrel, S. R., Qu, Y., Nepal, S., & Singh, S. (2020). Privacy-aware autonomous valet parking: Towards experience driven approach. *IEEE Transactions on Intelligent Transportation Systems*, *22*(8), 5352-5363.

[5] Xianjia, Y., Queralta, J. P., Heikkonen, J., & Westerlund, T. (2021). Federated learning in robotic and autonomous systems. *Procedia Computer Science*, *191*, 135-142.

[6] Lee, J., Azamfar, M., Singh, J., & Siahpour, S. (2020). Integration of digital twin and deep learning in cyber-physical systems: towards smart manufacturing. *IET Collaborative Intelligent Manufacturing*, *2*(1), 34-36.

[7] Kalloniatis, C., Diamantopoulou, V., Kotis, K., Lyvas, C., Maliatsos, K., Gay, M., ... & Lambrinoudakis, C. (2020). Towards the design of an assurance framework for increasing security and privacy in connected vehicles. *International Journal of Internet of Things and Cyber-Assurance*, *1*(3-4), 244-266.

[8] Praghash, K., & Karthikeyan, T. (2022). Data privacy preservation and trade-off balance between privacy and utility using deep adaptive clustering and elliptic curve digital signature algorithm. Wireless Personal Communications, 124(1), 655-670.

[9] Hammedi, W., Brik, B., & Senouci, S. M. (2022). Toward optimal MEC-based collision avoidance system for cooperative inland vessels: a federated deep learning approach. *IEEE transactions on intelligent transportation systems*, *24*(2), 2525-2537.

[10] Arshath Raja, R., & Kousik, N. V. (2021). Privacy preservation between privacy and utility using ECC-based PSO algorithm. In Intelligent Computing and Applications: Proceedings of ICICA 2019 (pp. 567-573). Springer Singapore.

[11] Nouacer, R., Hussein, M., Espinoza, H., Ouhammou, Y., Ladeira, M., & Castiñeira, R. (2020). Towards a framework of key technologies for drones. *Microprocessors and Microsystems*, *77*, 103142.

[12] Banabilah, S., Aloqaily, M., Alsayed, E., Malik, N., & Jararweh, Y. (2022). Federated learning review: Fundamentals, enabling technologies, and future applications. *Information processing & management*, *59*(6), 103061.