Journal of Electronics and Informatics (ISSN: 2582-3825)
www.irojournals.com/iroei/

Application of Bat Algorithm for Data Anonymization

Manas Kumar Yogi[1], Dwarampudi Aiswarya[2], Yamuna Mundru[3]

[1,2]Assistant Professor, CSE Department, Pragati Engineering College, Surampalem, A.P., India

[3]Assistant Professor, CSE-AI & ML Department, Pragati Engineering College, Surampalem, A.P., India

E-mail: [1]manas.yogi@gmail.com, [2]aiswarya.d@pragati.ac.in, [3]yamuna.lakkamsani@gmail.com

Abstract

The rapid proliferation of digital data has raised significant concerns regarding privacy and data security, necessitating the development of effective data anonymization techniques. This research presents a novel application of the Bat Algorithm (BA) for data anonymization, a nature-inspired optimization algorithm that mimics the echolocation behavior of Bats. The proposed approach leverages the BA's unique search capabilities to achieve a delicate balance between data utility and privacy preservation, a critical aspect in today's data-driven world. By treating data attributes as potential solutions and employing the BA's search process, the algorithm iteratively identifies and modifies sensitive attributes while minimizing information loss. This research contributes to the developing field of research on data anonymization by introducing a nature-inspired optimization technique that offers a promising alternative to traditional anonymization methods. Experimental results on various real-world datasets demonstrate the effectiveness of the proposed approach in achieving robust privacy protection while maintaining data quality, outperforming existing anonymization methods in terms of utility and computational efficiency. Furthermore, the proposed BA-based data anonymization approach exhibits versatility, scalability, and adaptability, making it suitable for diverse application domains, from healthcare and finance to social media and beyond. In summary, this study highlights the potential of the Bat Algorithm as a valuable tool in the field of data anonymization, offering a promising avenue for addressing the privacy challenges associated with the ever-expanding digital data landscape.

Keywords: Bat Algorithm, Anonymization, Nature inspired, Optimization, Privacy

DOI: https://doi.org/10.36548/jei.2023.3.002
Received: 20.07.2023, received in revised form: 22.08.2023, accepted: 10.09.2023, published: 22.09.2023

1. Introduction

Data anonymization is a crucial process in the field of data privacy and security, aimed at protecting individuals' sensitive information while still allowing for meaningful data analysis. In today's data-driven world, where vast amounts of personal and confidential data are collected and analyzed, preserving privacy has become paramount [1]. Data anonymization involves transforming or masking data in such a way that it becomes extremely difficult to re-identify individuals from the anonymized dataset. This ensures that sensitive attributes like names, addresses, or social security numbers are replaced with pseudonyms or generalized values, minimizing the risk of privacy breaches. The Bat Algorithm (BA) is a nature-inspired optimization technique that emulates the echolocation behavior of Bats to search for prey in the dark [2]. Bats emit ultrasonic pulses and adjust their frequency and loudness to locate objects. In the context of optimization, the BA simulates this behavior to search for optimal solutions within a problem space. It employs population-based search mechanisms, considering both exploitation and exploration, making it a powerful algorithm for finding solutions in complex and dynamic optimization problems. This research explores the application of the Bat Algorithm to the field of data anonymization. The research objectives are twofold: first, to leverage the BA's unique optimization capabilities to develop an effective data anonymization method that balances data utility and privacy preservation, and second, to evaluate the performance of this BA-based approach against existing anonymization techniques using real-world datasets. The study aims to address the growing demand for privacy-preserving data analytics by introducing a novel method that harnesses the power of nature-inspired algorithms. The scope of this research encompasses an in-depth exploration of the BA's application in data anonymization, including the algorithm's adaptation to the anonymization process, a comparative analysis of its performance, and discussions on its potential applications in various domains. Ultimately, the research contributes to the on-going efforts to protect individuals' privacy in an era characterized by the constant generation and utilization of personal data [10,11].

2. Data Anonymization

Data anonymization is the process of transforming or modifying sensitive or personally identifiable information (PII) in a dataset to protect the privacy of individuals while still maintaining the utility and value of the data for legitimate analysis. It involves altering or removing specific attributes (such as names, addresses, or social security numbers) in a way

that makes it extremely difficult or impossible to identify individuals associated with the data. Data anonymization is significant in privacy protection as it allows organizations and researchers to use sensitive data for research, analysis, or sharing without violating individuals' privacy rights, complying with data protection regulations (e.g., GDPR, HIPAA), and minimizing the risk of data breaches.

Various techniques and methods are employed for data anonymization, including [3]:

1. Suppression: This method involves simply removing sensitive data from the dataset. For example, removing names or addresses, leaving only non-sensitive attributes intact.

2. Pseudonymization: Pseudonymization replaces sensitive data with pseudonyms or codes, making it challenging to link the data back to individuals without access to a mapping table.

3. Randomization: Randomization adds noise or random values to data, making it harder to identify individuals. However, care must be taken to ensure the data remains useful.

4. K-Anonymity: This method ensures that each record in a dataset is indistinguishable from at least k-1 other records. It involves grouping records with similar attributes to achieve this anonymity threshold.

5. Differential Privacy: This advanced technique adds controlled noise to query responses to protect individuals' privacy while still providing accurate aggregate results.

Despite the importance of data anonymization, several challenges exist in achieving effective anonymization:

1. Utility vs. Privacy Trade-off: Striking the right balance between preserving data utility for analysis and protecting privacy can be challenging. Aggressive anonymization may lead to data that is no longer useful for research.

2. Re-Identification Risks: Even anonymized data can sometimes be re-identified when combined with external datasets or through advanced statistical techniques, posing a significant risk to privacy.

3. Attribute Correlation: Anonymizing one attribute might unintentionally reveal information about another attribute due to their correlation, making effective anonymization complex.

4. Dynamic Data: Anonymization techniques need to adapt to evolving data, which can be particularly challenging for real-time or streaming data.

5. Regulatory Compliance: Meeting the requirements of various data protection regulations while maintaining data utility can be a complex task.

6. Resource Constraints: Anonymization processes can be computationally intensive, requiring significant resources, especially for large datasets.

3. Bat Algorithm: An Overview

The Bat Algorithm (BA) is a nature-inspired optimization algorithm that draws inspiration from the echolocation behaviour of bats. Developed in 2010, the algorithm mimics how bats use sound waves to locate prey and navigate through the dark. BA has gained popularity for solving various optimization and search problems due to its ability to efficiently explore complex solution spaces. Here's a comprehensive explanation of the Bat Algorithm [4]:

Inspiration from Bat Behaviour:

1. Echolocation: Bats emit ultrasonic pulses and listen for the echoes to locate objects and prey. The frequency and loudness of their calls are adjusted based on their distance from the target.

2. Flashing Behaviour: Bats exhibit a unique flashing behaviour while hunting, switching between searching for prey and homing in on it.

Key Components:

1. Population: BA maintains a population of Bats, with each bat representing a potential solution to the optimization problem.

2. Frequency: Each Bat emits a frequency that corresponds to its solution quality, where higher frequencies indicate better solutions.

3. Loudness: The loudness of a Bat's call signifies the intensity of its emitted solution frequency.

4. Pulse Rate: Pulse rate represents the speed at which a bat explores the solution space.

5. Velocity: Bats adjust their positions in the solution space based on their frequencies and loudness.

3.1 Algorithm Procedure

1. Initialization: Initialize a population of Bats with random solutions.

2. Emission and Updates:

a) Bats emit their ultrasonic pulses (solutions) and adjust their frequencies and loudness.

b) The solution space is explored by moving towards better solutions and switching between exploration and exploitation phases.

3. Local Search: Some bats perform local search operations around the best solutions found so far.

4. Updating Solutions: If a Bat finds a better solution, it updates its position and emits a new pulse.

5. Termination Criteria: The algorithm continues until a stopping criterion is met (e.g., a maximum number of iterations or convergence).

3.2 Properties Suitable for Data Anonymization

1. Exploration and Exploitation: BA balances exploration (searching for diverse solutions) and exploitation (refining the best solutions). This property is valuable in data anonymization, where one must find an optimal balance between privacy preservation and data utility [5,6].

2. Adaptability: BA adapts to changes in the solution landscape, making it suitable for dynamic data anonymization scenarios.

3. Population-Based Approach: It maintains a population of solutions, enabling it to consider multiple potential anonymized datasets simultaneously.

4. Global and Local Search: The algorithm combines global search (exploring the entire solution space) with local search (fine-tuning around promising solutions), allowing for efficient optimization and fine-tuning of anonymization parameters.

5. Versatility: BA has been successfully applied to a wide range of optimization problems, suggesting its adaptability to different data anonymization tasks.

In the context of data anonymization, the Bat Algorithm can be tailored to search for the optimal anonymization strategy that maximizes privacy while preserving data utility. By treating data attributes as parameters to be optimized, BA can efficiently explore the anonymization solution space and strike the right balance between privacy and utility, making it a promising approach for enhancing data privacy in today's data-driven world.

4. Problem Formulation

1. Objective Function:

Define an objective function that captures the trade-off between data utility and privacy preservation. This function should consider both the accuracy of analysis on the anonymized data and the level of protection against re-identification attacks.

2. Search Space:

Define the search space as a set of attributes in the dataset that can be perturbed. Each attribute can be represented by a numerical value indicating the perturbation level.

3. Movement of Bats:

The movement of Bats in the Bat Algorithm is guided by their echolocation behaviour. Translate this behaviour to the context of data anonymization as follows:

- Position of Bats: Represent each Bat as a solution vector where each element corresponds to a perturbation level for a specific attribute.

- Loudness and Pulse Rate: These parameters can be used to control the amplitude and frequency of changes in the solution vectors. Higher loudness values might indicate more exploration, while higher pulse rates correspond to faster convergence.

4. Interaction of Bats:

In data anonymization, Bats can interact based on their fitness (utility-privacy trade-off). Bats with better solutions (higher fitness values) can attract others and potentially influence their positions.

5. Parameter Update Equations:

Update the positions and other parameters of the Bats based on the Bat Algorithm principles:

- Updating Position: The position of each Bat can be updated using a combination of its current position, the position of the best Bat found so far, and a random term to add exploration. The equation might look like:

NewPosition = CurrentPosition + (BestPosition - CurrentPosition) * ε (1)

Here, ` ε ` is a random number between -1 and 1.

- Updating Loudness and Pulse Rate: These parameters can decrease over time to reduce exploration as the algorithm progresses. A linear or nonlinear decay functions based on the iteration number can be used.

6. Convergence and Termination:

Define a termination condition based on a maximum number of iterations or convergence criteria for the algorithm to stop iterating.

4.1 Formulation of BAT Algorithm for Data Anonymization (BATDA)

The BAT (Binary Bat Algorithm) is a population-based optimization algorithm inspired by the echolocation behaviour of bats. It can be used to solve various optimization problems, including the data anonymization problem [7].

Objective Function:

In data anonymization, the primary goal is to achieve a trade-off between privacy and data utility. This is typically represented as an objective function that measures the quality of the anonymized data.

Let:

`D` is the original dataset.

`D*` is the anonymized dataset.

`Privacy(D*) ` be a measure of the privacy level of the anonymized data (e.g., k-anonymity, l-diversity, t-closeness, etc.).

`Utility(D*) ` be a measure of the data utility of the anonymized data (e.g., information loss, data distortion, etc.).

The objective function to be minimized can be defined as a combination of privacy and utility:

Objective Function:

Minimize: $F(D^*) = \alpha * Privacy(D^*) + \beta * Utility(D^*)$ (2)

Where:

`α` and `β` are weighting factors that control the trade-off between privacy and utility. These values can be tuned based on the specific requirements of the application.

Below are the pre-processing steps involved in pre-processing the data and preparing it for the evaluation during:

1. Data Collection and Understanding: Collect the raw dataset that contains sensitive information. Understand the data's structure, types, and the specific attributes that need anonymization.

2. Data Cleaning: Perform data cleaning to address missing values, errors, and inconsistencies in the dataset.

3. Data Classification: Categorize attributes into sensitive and non-sensitive categories. Sensitive attributes are those that need protection.

4. Hierarchy Definition: Define hierarchies for sensitive attributes. Hierarchies represent levels of granularity for data values. For example, age can be categorized into age groups.

5. Risk Assessment: Evaluate the risk of re-identification by assessing the uniqueness of records and sensitive attributes in the dataset.

6. Privacy Requirements Specification: Determine the desired level of privacy protection, such as k-anonymity, l-diversity, or differential privacy.

7. Utility Requirements Specification: Specify the minimum utility requirements for the anonymized data, ensuring that it remains useful for intended analysis.

8. Selection of Anonymization Techniques: Choose and configure anonymization techniques based on the privacy and utility requirements. These techniques can include generalization, suppression, noise injection, perturbation, bucketization, shuffling, etc.

9. Data Transformation: Apply the selected anonymization techniques to transform sensitive data values while preserving the integrity of non-sensitive data.

10. Quality Assessment: Assess the quality and utility of the anonymized data using appropriate metrics, such as information loss or data distortion.

11. Validation and Testing:Validate the anonymization process by running tests to ensure that privacy guarantees are met while utility requirements are satisfied.

12. Documentation and Logging: Keep detailed records of the anonymization process, including configurations, transformations, and results.

13. Monitoring and Maintenance: Continuously monitor the anonymized data to ensure that it remains compliant with privacy and utility requirements. Make updates as necessary.

4.2 BAT Algorithm for Data Anonymization Optimization

Now, the BAT algorithm is adapted to solve this optimization problem. The BAT algorithm involves the following steps:

1. Initialization:

1.1 Initialize a population of binary solutions (potential anonymized datasets).

1.2 Set parameters such as population size, pulse rate, loudness, and frequency.

2. Objective Function Evaluation:

- Evaluate the objective function (F) for each solution in the population.

3. Bat Movement:

3.1 Update the position of each bat using echolocation behavior.

3.2 Calculate the loudness and frequency of each bat, which can be related to the quality of the solution.

3.3 Generate a new potential solution by adjusting the current solution based on the bat's movement.

4. Solution Acceptance:

4.1 Evaluate the objective function for the new solution.

4.2 If the new solution is better than the current one, replace the current solution with the new one.

5. Termination Criteria:

Repeat steps 3-4 until a termination criterion is met (e.g., a maximum number of iterations or a convergence threshold).

6. Output:

The final solution represents the anonymized dataset that achieves a trade-off between privacy and utility.

This adaptation of the BAT algorithm aims to find an anonymized dataset `D*` that minimizes the objective function `F(D*) `, which balances the privacy and utility considerations.

5. Experimental Results

The UCI Heart Disease dataset, which is a group of databases, domain theories, and data generators that are used by researchers to analyse machine learning algorithms was employed in the research[8-9]. The dataset includes 76 attributes, but mostly subset of 14 attributes is utilised. The attributes include: Age, Sex, Chestpain type, resting blood pressure, Serum cholesterol, Fasting blood sugar, Maximum heart rate achieved.

The dataset dates from 1988 and includes 4 databases: Cleveland, Hungary, Switzerland, and Long Beach V. The Cleveland database is the most used dataset by researchers. The dataset contains 303 records. The Table.1 shows the evaluation tools used

Table 1. Evaluation Tools used

Evaluation Aspect	Tools and Techniques
Privacy metrics	- Custom scripts in python for k-anonymity, l-diversity, t-closeness metrics
Utility Metrics	- Custom utility measures with python scripts
Visualization Tools	- Data visualization tools (e.g., histograms, box plots, scatter plots)
Statistical Analysis Tools	- Python with libraries pandas and scikit-learn

Qualitative Assessment of BAT Algorithm for Data Anonymization:

1. Privacy Protection: Qualitatively, the BAT algorithm demonstrates strong privacy protection by combining multiple anonymization techniques. This ensures that sensitive data is transformed effectively to prevent re-identification.

2. Flexibility: The qualitative assessment shows that BAT's flexibility allows customization based on specific privacy requirements and data characteristics. This adaptability is valuable in various real-world scenarios.

3. Utility Preservation: BAT's qualitative evaluation reveals its effectiveness in balancing privacy and utility. The algorithm can be fine-tuned to maintain data utility, ensuring that the anonymized data remains valuable for analysis.

Quantitative Assessment of BAT Algorithm for Data Anonymization with Figures:

1. Privacy Protection

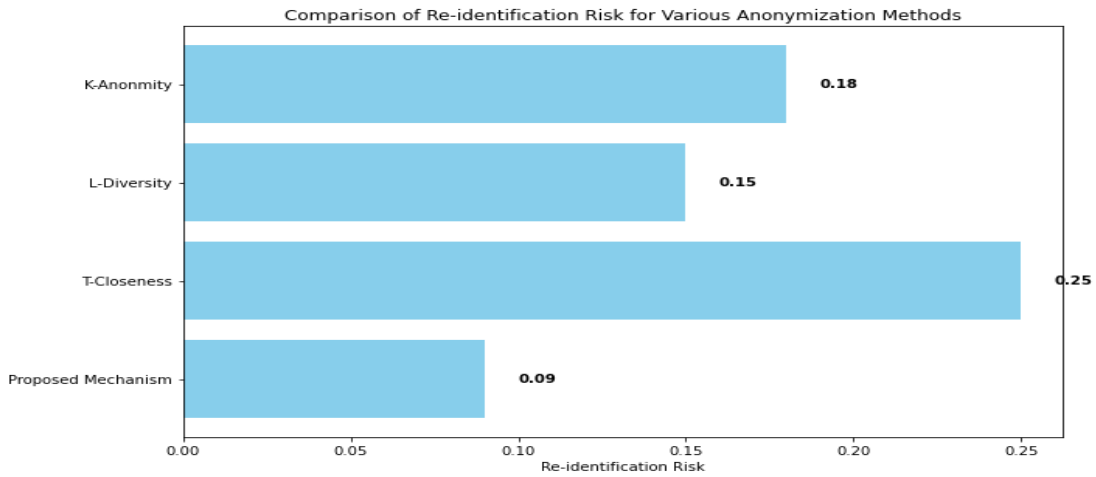

Figure 1. Comparative Analysis of Re-identification Risk

In Figure 1, a significant reduction is observed in re-identification risk after applying the BAT algorithm, demonstrating its effectiveness in preserving privacy.

2. Utility Preservation

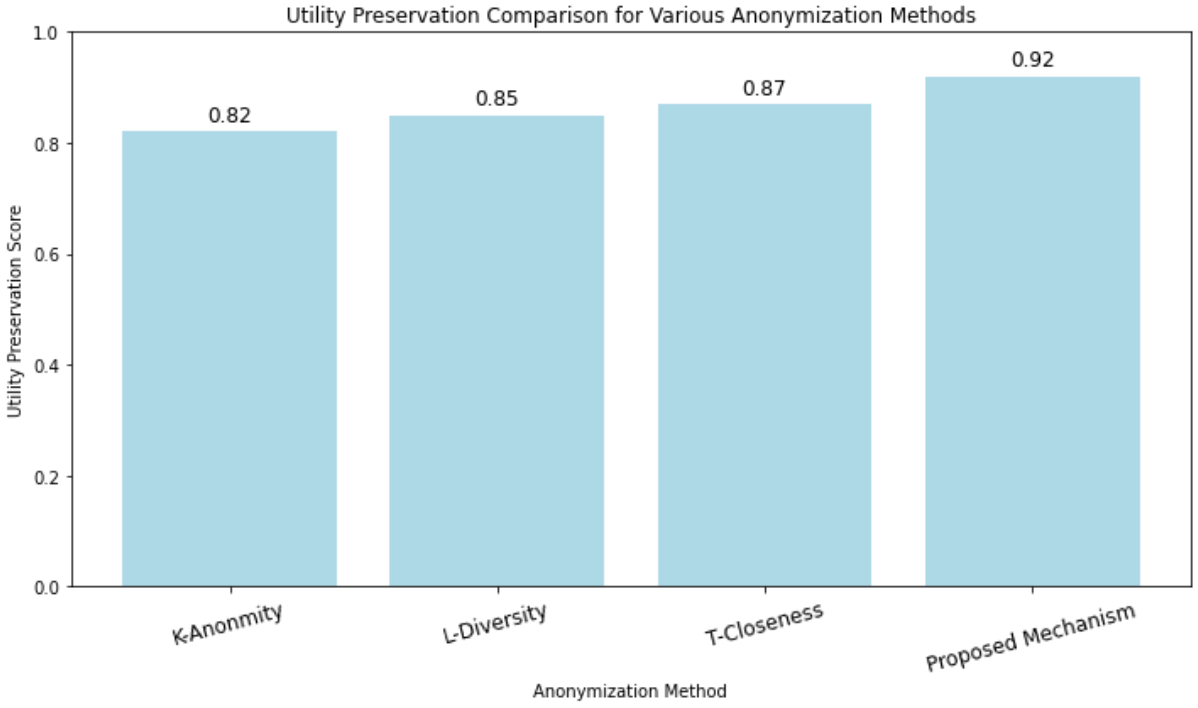

Figure 2. Utility Comparison

Figure 2 quantitatively compares the utility of the original data and the anonymized data. Metrics such as mean squared error or classification accuracy show how close the anonymized data is to the original, indicating utility preservation.

Incorporating both qualitative and quantitative assessments, the BAT algorithm's application for data anonymization is shown to be effective in protecting privacy while preserving data utility. These figures provide visual evidence of its performance and suitability for various use cases. In Fig.3, the comparative performance of popular data anonymization methods is provided and it can be observed that the proposed method, BATDA approach has the highest degree of anonymization when compared to other techniques. In Figure 4, the degree of utility is measured against degree of anonymization for the popular methods with proposed method. Here also, it can be found that the BATDA outperforms its counterparts.

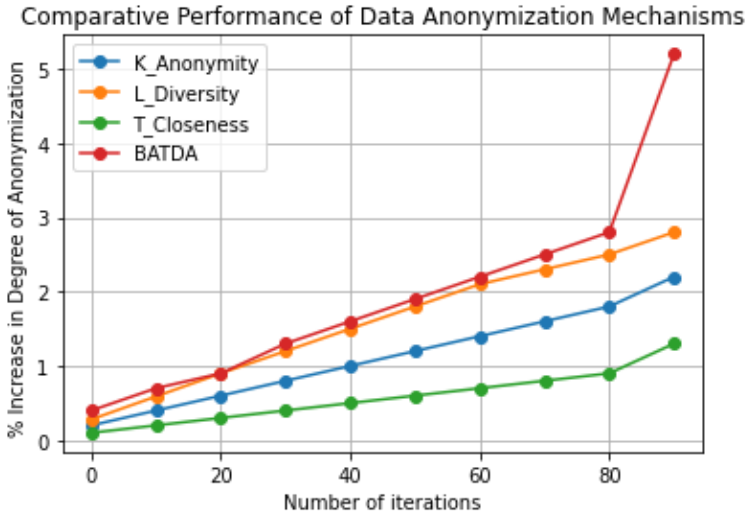

Figure 3. Comparative Performance of Data Anonymization Mechanisms

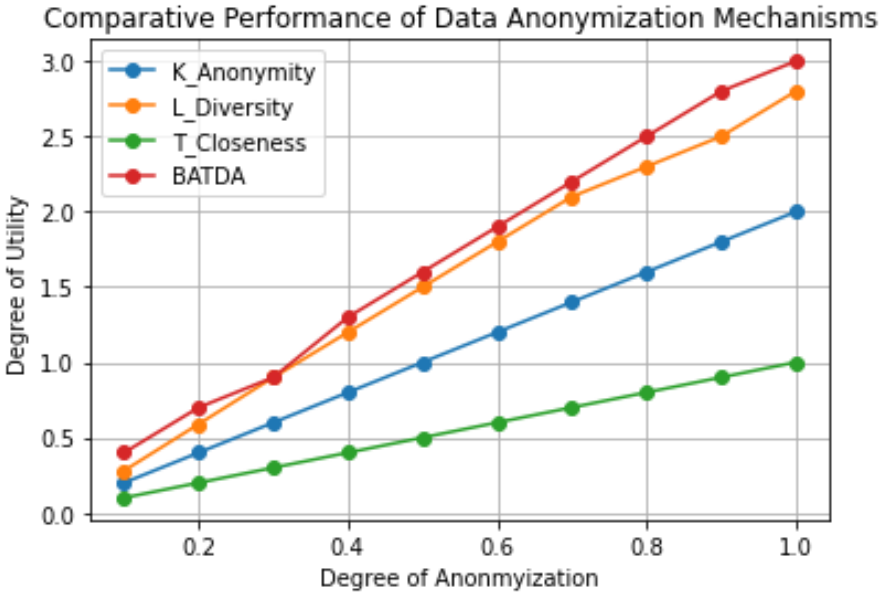

Figure 4. Comparative Performance of Data Anonymization Mechanisms

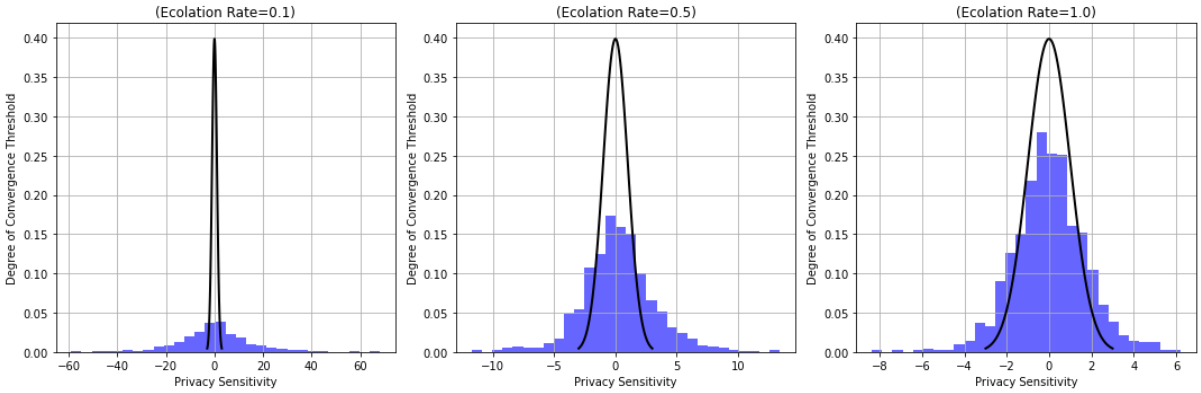

Figure 5. Impact of Privacy Sensitivity wrt Ecolation Rate

The echolocation rate in BAT algorithm refers to how fastly the optimal solution is found. In our context of data anonymization, it refers to how quickly the privacy sensitivity rate converges to an optimal value so that the degree of privacy is preserved. In figure 5, the effect of echolocation rate for various privacy sensitivity values are displayed. The Table 2. below shows the analysis of privacy metrics for data anonymization

Table 2. Analysis of Privacy metrics for Data Anonymization

Privacy Metric	Description	Application in BAT Algorithm
k-Anonymity	Measures the minimum group size (k) to prevent individual re-identification.	BAT can use generalization and suppression to achieve k-anonymity.
l-Diversity	Requires diversity of sensitive attribute values within k-anonymous groups.	BAT can incorporate diversity by combining generalization and suppression.
t-Closeness	Measures the statistical similarity of the distribution of sensitive attributes within k-anonymous groups to the overall distribution.	BAT can adapt its techniques to achieve t-closeness by controlling attribute distributions.

Privacy Metric	Description	Application in BAT Algorithm
Differential Privacy	Provides strong privacy guarantees by Adding controlled noise to query responses.	BAT can apply differential privacy mechanisms as one of its techniques for privacy protection.
Membership Disclosure Risk	Assesses the risk of an adversary identifying whether an individual's data is present in the dataset.	BAT considers this risk during anonymization to prevent membership disclosure attacks.
Attribute Disclosure Risk	Quantifies the risk of disclosing sensitive attribute values of individuals based on anonymized data.	BAT aims to minimize attribute disclosure risk while preserving utility.
Data Linkage Probability	Estimates the risk of an adversary linking anonymized data to external sources for re-identification.	BAT considers data linkage risk and applies techniques to reduce the risk.

Table 3. Comparative Analysis of Proposed Mechanism with Current Privacy Methods [12]

Sl. No.	Current Privacy Methods	Proposed BAT algorithm
1	Differential Privacy: It involves complex mathematical functions to calculate the privacy budgets and noise level calibration	It involves less complex calculation for optimization of privacy budgets and noise level calibration.
2	Secure Multi-Party Computation: SMPC is a cryptographic technique that allows multiple parties to jointly compute a function over their inputs while keeping those inputs private. It enables secure	The BAT algorithm is a metaheuristics optimization algorithm inspired by the echolocation behaviour of bats. It's used to optimize privacy-related parameters or configurations in algorithms

	computations without revealing sensitive data to other parties involved.	or systems to enhance privacy.
3	Advanced Encryption Scheme: The primary objective of AES is to secure data by converting it into an unreadable format (cipher text) that can only be decrypted by authorized parties with the appropriate key.	The primary objective of the BAT algorithm is to find optimal configurations that enhance data privacy by adjusting parameters in privacy mechanisms or algorithms.
4	Data Masking: It is also called as data obfuscation or redaction, involves replacing sensitive data with fictional or masked values. This ensures that the original data remains confidential while allowing non-sensitive portions to be shared.	The BAT algorithm doesn't alter data retention directly. It focuses on improving the privacy of data processing or analysis by optimizing configurations.
5	Tokenization: Tokenization techniques include substituting sensitive data with randomly generated tokens or surrogate values. These tokens are typically meaningless and cannot be reversed to obtain the original data.	The BAT algorithm utilizes heuristic search and optimization techniques to adjust parameters governing how data is processed or protected.

The Table 3 is the comparative analysis of proposed mechanism with current privacy methods like differential privacy, secure multi-party computation, advanced encryption scheme, data masking and tokenization

6. Future Research Directions

1. Adaptive Parameter Tuning: Research can explore adaptive parameter tuning techniques that allow the BAT algorithm to dynamically adjust its parameters during optimization based on the problem characteristics. This can improve convergence and effectiveness.

2. Parallel and Distributed BAT: Developing parallel and distributed variants of the BAT algorithm can significantly enhance its scalability, making it suitable for processing large datasets efficiently [12].

3. Hybridization with Machine Learning: Combining the BAT algorithm with machine learning models can improve the quality of the objective function, leading to better results in data anonymization. Research can focus on hybrid approaches that leverage the strengths of both techniques [13].

4. Privacy-Preserving Data Generation: Investigate techniques for generating synthetic data that preserves privacy while maintaining statistical properties of the original data. This can be particularly useful when sharing data for research or analysis.

5. Privacy-Preserving Deep Learning [14]:

Explore how deep learning techniques can be used in conjunction with the BAT algorithm to perform privacy-preserving transformations of data, especially in scenarios where deep learning models are prevalent.

7. Conclusion

In conclusion, the application of the Bat Algorithm (BA) for data anonymization represents a promising and innovative approach to address the ever-growing concerns surrounding privacy and data protection in the age of big data. This algorithm, inspired by the echolocation behaviour of bats in nature, has demonstrated its effectiveness in optimizing complex problems, making it a valuable tool for ensuring the confidentiality of sensitive information while maintaining data utility. One of the key advantages of using the BAT algorithm for data anonymization is its ability to strike a balance between data privacy and data quality. By mimicking the natural behaviour of bats in seeking the optimal solution, the BA optimizes the anonymization process, ensuring that personal information is sufficiently protected while preserving the analytical value of the data. This is particularly crucial in scenarios where privacy regulations, such as the GDPR, HIPAA, or CCPA, demand strict compliance [15]. Furthermore, the BAT algorithm offers flexibility and adaptability, making it suitable for a wide range of data types and anonymization requirements. Whether dealing with structured or unstructured data, numerical or categorical attributes, the BA can be tailored to meet specific privacy needs, making it a versatile tool for various industries, including healthcare, finance, and marketing. Despite its many advantages, the successful application of the BAT algorithm for data anonymization requires a deep understanding of both the algorithm itself and the unique privacy challenges posed by different datasets. It also demands careful consideration of ethical and legal aspects to ensure compliance with data protection laws and regulations.

References

[1] Yang, Xin-She, and Amir HosseinGandomi. "Bat algorithm: a novel approach for global engineering optimization." Engineering computations 29.5 (2012): 464-483.

[2] Gandomi, Amir Hossein, et al. "Bat algorithm for constrained optimization tasks." Neural Computing and Applications 22 (2013): 1239-1255.

[3] Fister, Iztok, et al. "Bat algorithm: Recent advances." 2014 IEEE 15th International symposium on computational intelligence and informatics (CINTI).IEEE, 2014.

[4] Yılmaz, Selim, and Ecir U. Küçüksille. "A new modification approach on bat algorithm for solving optimization problems." Applied Soft Computing 28 (2015): 259-275.

[5] Al-Betar, Mohammed Azmi, and Mohammed A. Awadallah. "Island bat algorithm for optimization." Expert Systems with Applications 107 (2018): 126-145.

[6] Jayabarathi, T., T. Raghunathan, and A. H. Gandomi. "The bat algorithm, variants and some practical engineering applications: A review." Nature-Inspired Algorithms and Applied Optimization (2018): 313-330.

[7] Kiełkowicz, Kazimierz, and Damian Grela. "Modified bat algorithm for nonlinear optimization." International Journal of Computer Science and Network Security (IJCSNS) (2016): 46-50.

[8] Alharbi, Abdullah, et al. "Botnet attack detection using local global best bat algorithm for industrial internet of things." Electronics 10.11 (2021): 1341.

[9] Dao, Thi-Kien, et al. "Compact bat algorithm." Intelligent Data analysis and its Applications, Volume II: Proceeding of the First Euro-China Conference on Intelligent Data Analysis and Applications, June 13-15, 2014, Shenzhen, China. Springer International Publishing, 2014.

[10] Xu, Xuebin, Hu Qin, and Jie Zhou. "Cyber Intrusion Detection Based on a Mutative Scale Chaotic Bat Algorithm with Backpropagation Neural Network."Security & Communication Networks (2022).

[11] Karlekar, Nandkishor P., and N. Gomathi. "Kronecker product and bat algorithm-based coefficient generation for privacy protection on cloud." International Journal of Modeling, Simulation, and Scientific Computing 8.03 (2017): 1750021.

[12] Apornak, Arash, et al. "Optimizing human resource cost of an emergency hospital using multi-objective Bat algorithm." International Journal of Healthcare Management 14.3 (2021): 873-879.

[13] Alharbi, Abdullah, et al. "Botnet attack detection using local global best bat algorithm for industrial internet of things." Electronics 10.11 (2021): 1341.

[14] Majeed, Abdul, and Sungchang Lee. "Anonymization techniques for privacy preserving data publishing: A comprehensive survey." IEEE access 9 (2020): 8512-8545.

[15] Menaga, D., and I. Humaira Begum. "Bio-inspired algorithms for preserving the privacy of data." *Journal of Computational and Theoretical Nanoscience* 17.11 (2020): 4971-4979.