Cite this research:
Saxena, A. k., (2022). Enhancing Data Anonymization: A Semantic K-Anonymity Framework with ML and NLP Integration SSRAML SageScience, 5(1), 81–92.

check for updates

Article history:
Received:
April/12/2022
Accepted:
November/23/2022

.

Enhancing Data Anonymization: A Semantic K-Anonymity Framework with ML and NLP Integration

Ashish K Saxena
https://orcid.org/0009-0002-1647-9266

Abstract

This study introduces an innovative framework that enhances data anonymization by integrating semantic k-anonymity with advancements in machine learning (ML) and natural language processing (NLP). Addressing the critical need for robust privacy protection mechanisms, this research responds to the escalating sophistication of deanonymization techniques, which threaten personal data privacy. Through a comprehensive evaluation, including the utilization of the Fβ score, our framework demonstrates superior capability in safeguarding personal data privacy and preserving data utility for analysis. The adaptability to various Θ thresholds and the framework's proficiency in retaining non-sensitive queries underscore its potential as a groundbreaking solution in data anonymization. This paper not only highlights the framework's theoretical and practical contributions to digital privacy but also charts a course for future research aimed at navigating the evolving landscape of data protection in an increasingly digital world.

Keywords: Anonymization, Machine Learning (ML), Natural Language Processing (NLP), Privacy, Semantic K-Anonymity

I. INTRODUCTION

In the digital age, the protection of personal data has emerged as a paramount concern [1]. The proliferation of digital services and platforms has led to an exponential increase in the volume of personal data collected, stored, and processed online [2]. This data, ranging from search queries to social media interactions, offers invaluable insights for both academic research and commercial applications. However, the extensive collection and utilization of personal information raise significant privacy concerns. The infamous incidents of data breaches and unauthorized data usage have heightened public awareness and concern over data privacy [3-5]. Consequently, there is a growing demand for robust anonymization techniques that can prevent the disclosure of personal information while retaining the utility of the data for analysis purposes. Complicating matters further, the sophistication of de-anonymization techniques has advanced considerably. Techniques that were once considered secure, such as simple anonymization or pseudonymization, are now easily circumvented by malicious actors equipped with powerful computational tools and algorithms.

These de-anonymization strategies have demonstrated the ability to re-identify individuals from seemingly anonymous datasets by exploiting patterns, inconsistencies, or auxiliary information [6], [7]. Given this backdrop, there is a critical need for innovative approaches to data anonymization that can effectively counteract these de-

anonymization capabilities. Traditional methods must be reassessed and enhanced with new technologies and methodologies to safeguard individual privacy without undermining the value derived from data analysis. This paper proposes an advanced framework that integrates semantic k-anonymity with machine learning (ML) and natural language processing (NLP) techniques, aiming to set a new standard in the protection of digital privacy across various data types.

The quest for effective data anonymization has been a central concern in the pursuit of balancing privacy protection with the utility of data. Existing anonymization methods, such as semantic k-anonymity, have demonstrated their value in specific contexts, particularly in anonymizing search log data by ensuring that each query cannot be distinguished from at least k-1 other queries [8-10]. This approach effectively reduces the risk of individual identification, maintaining a semblance of privacy for the users involved. However, the application of these methods to more diverse and complex data types presents significant challenges. Social media posts, emails, and other digital communications embody a richer and more nuanced set of information, often embedded with subtle contextual cues and personal identifiers that transcend simple textual data. The limitations of traditional anonymization techniques become particularly evident when faced with the task of protecting such multifaceted data. These techniques often struggle to capture the intricacies and the contextual richness of human language, leading to either over-sanitization, which strips the data of its utility, or under-protection, which leaves individuals vulnerable to re-identification. Moreover, the dynamic nature of digital communication and the evolving landscape of online platforms necessitate a more adaptable and nuanced approach to data anonymization. As we delve deeper into the age of big data, the need for innovative solutions that can navigate the complexities of various data types while ensuring robust privacy protection becomes increasingly critical. It is against this backdrop that our proposed framework seeks to integrate the advancements in machine learning and natural language processing with semantic k-anonymity, aiming to pioneer a new frontier in digital data anonymization.

In this study, our intent is to devise an anonymization framework that not only stands robust against contemporary de-anonymization techniques but also maintains the intrinsic value of the data for analytical pursuits. By integrating the principles of semantic k-anonymity with the nuanced capabilities of machine learning and natural language processing, we seek to address and overcome the limitations of existing anonymization methodologies. The framework is designed to be versatile, capable of handling various data types, from structured databases to unstructured text found in digital communications. The overarching goal is to provide a solution that is not just theoretically sound but also practically applicable across different domains, ensuring that the balance between data privacy and utility is not just a theoretical ideal but a tangible reality.

II. RELATED WORKS

Our approach to enhancing semantic k-anonymity integrates machine learning (ML) and natural language processing (NLP) techniques, building upon the foundational work in anonymization techniques and the detection and protection of sensitive information within text data. Unlike traditional methods that primarily focus on structural modifications to data for privacy preservation, our method emphasizes the understanding

and processing of the semantic content of the data. This nuanced approach allows for a more sophisticated analysis and protection mechanism that can adapt to the complexities of various data types, ranging from search logs to unstructured text found in digital communications.

In the current state of anonymization, various techniques have been explored to ensure data privacy while retaining the utility of the data for analysis. Semantic k-anonymity emerges as a significant approach, particularly in the context of protecting search logs from potential privacy breaches. This subsection reviews existing anonymization techniques, with a focus on semantic k-anonymity and its applications to search logs. Kenig and Tassa [11] present a practical approximation algorithm for optimal k-anonymity, aiming to minimize information loss during the anonymization process. This algorithm provides a theoretical foundation for integrating machine learning (ML) and natural language processing (NLP) techniques to enhance semantic k-anonymity's effectiveness. Zhang et al [12] explore a scalable two-phase top-down specialization approach for data anonymization using the MapReduce framework on cloud platforms. This approach highlights the potential for cloud-based anonymization processes to be enhanced by semantic analysis and ML, offering scalability and efficiency in handling large-scale data sets. Jiang and Clifton [13] propose a secure distributed framework for achieving k-anonymity, which underscores the importance of collaborative approaches in data anonymization. Their work suggests that semantic understanding and ML techniques can significantly contribute to the development of secure, distributed anonymization frameworks. Domingo-Ferrer and Torra [14] discuss ordinal, continuous, and heterogeneous k-anonymity through microaggregation, an approach that preserves the semantics of each attribute type as much as possible. Their research indicates that ML and NLP techniques could play a crucial role in improving the process of microaggregation, especially in achieving semantic k-anonymity across different types of data, including search logs.

In the exploration of machine learning (ML) and natural language processing (NLP) for detecting and protecting sensitive information in text data, several innovative approaches have been developed, showcasing promising results in enhancing privacy and security across various domains. Huang in [15] utilizes Hidden Markov Models (HMM) and Support Vector Machines (SVM) for detecting sensitive information, presenting an efficient alternative to traditional methods like CNNs and RNNs. [16] asserts that Text-CNN model to improve the accuracy and efficiency of detecting sensitive information in unstructured text over recurrent neural networks. Jana and Biemann [17] investigate a privacy-preserving framework for sequence tagging tasks, such as Named Entity Recognition (NER), within a federated learning context, incorporating differential privacy to address concerns in sensitive domains. Yang et al. [18] discuss an intelligent discovery and protection method for privacy data in government cyberspace, integrating NLP and ML technologies for automatic detection and masking of sensitive information. Lastly, Wang et al. [20] explore training high-quality word vectors over encrypted data with privacy-preserving collaborative neural network learning algorithms, leveraging arithmetic primitives on encrypted data to ensure privacy, marking a significant step forward in privacy-preserving technology applications.

III. PRELIMINARIES

A. INTEGRATING SEMANTIC K-ANONYMITY WITH MACHINE LEARNING IN ANONYMIZATION

Semantic k-anonymity extends the traditional concept of k-anonymity, which aims to make each record in a dataset indistinguishable from at least k-1 other records with respect to certain "quasi-identifier" attributes [15]. This model is enhanced by considering the semantic information contained within the data, which is crucial for maintaining the meaning and context, especially in textual datasets. The rich contextual information language contains necessitates a more nuanced approach to privacy protection, where simply altering identifiable attributes may not be sufficient. Complementing semantic k-anonymity, machine learning (ML) offers robust tools for recognizing complex patterns and anomalies in large datasets. ML algorithms, when trained appropriately, have the capability to automatically detect sensitive information that may not be overtly labeled or recognized as such. This automated detection is vital for efficiently scaling the anonymization process across extensive data collections and for remaining responsive to the dynamic nature of what is deemed "sensitive" in light of shifting societal norms and legal frameworks [11], [14].

The integration of ML in semantic k-anonymity is a significant leap forward in anonymization methodologies. It enables the handling of data in a way that is both context-aware and scalable. For instance, an ML model can learn from various instances of textual data to identify and anonymize personal identifiers, all while maintaining the underlying narrative or informational content of the data. This is particularly important in textual data where nuances and subtleties can convey identifying information beyond explicit identifiers like names and addresses. ML's adaptability also plays a critical role in this integration, as models can be continuously refined and updated with new data, thereby adapting to new forms of sensitive information. This ensures that the anonymization process remains effective over time and across various data governance landscapes.

Natural language processing (NLP) involves the use of algorithms to understand and manipulate human language. This technology has become indispensable in tasks that require an understanding of the context and semantic content of textual data. The figure shown in Fig. 1. complements this description by visually tracing the NLP journey from language detection to deep learning-based processing, culminating in various analytical outputs such as sentiment analysis and classification. In the domain of data anonymization, NLP techniques, represented by the interconnected nodes of neural networks, offer a sophisticated approach to analyze textual data for identifying and masking personal identifiers or sensitive information.

B. NATURAL LANGUAGE PROCESSING

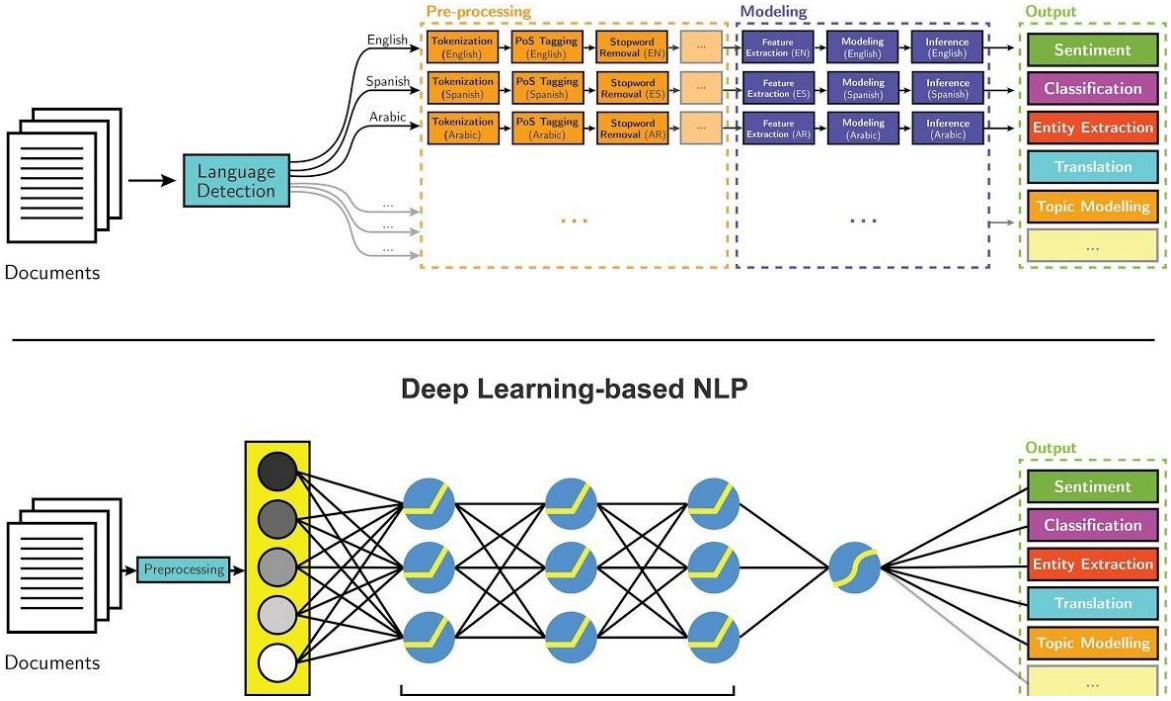

FIGURE 1. Deep learning based Natural language processing

The application of NLP in anonymization tasks leverages its ability to parse, interpret, and even generate human language in a way that maintains the original message's intent while ensuring privacy. This is particularly relevant when dealing with free-text fields in datasets, where individuals might inadvertently include sensitive information in a narrative form. Traditional anonymization methods might strip away too much information, rendering the data less useful, or fail to identify all instances of sensitive data, leaving privacy risks unmitigated. By employing NLP, we can significantly enhance the effectiveness of semantic k-anonymity. Semantic k-anonymity, which traditionally focuses on structured data, can be extended to unstructured text by using NLP to understand the 'meaning' behind the words and phrases. This enables the identification of sensitive information not just by direct matches to known sensitive terms, but by understanding the context in which terms are used. For example, NLP can help distinguish between the word "spring" used in the context of a season, versus its use in a context that might reveal personal information (e.g., "I always visit my grandmother in Palm Springs in the spring"). Furthermore, NLP techniques can aid in generating anonymized text that retains the utility and coherence of the original data. Techniques such as named entity recognition (NER) can identify personal names, locations, dates, and other potentially identifiable information. Subsequent processing steps can replace these entities with generic but contextually appropriate alternatives, or alter sentences to remove or obscure the sensitive information while keeping the overall message intact. Incorporating NLP into the process of achieving semantic k-anonymity thus ensures that anonymized text not only protects individual privacy but also remains a valuable asset for analysis and insight generation. This integration presents a forward-thinking approach to data privacy, adapting to the complexities of human language and the nuances of textual information, as visually demonstrated in the accompanying figure.

IV. METHODOLOGY

A. FRAMEWORK DESIGN

Our framework is meticulously designed to synergize semantic k-anonymity with advanced machine learning (ML) and natural language processing (NLP) techniques, aiming to enhance the identification and anonymization of sensitive information across a variety of data types. The framework operates through a series of interconnected steps, ensuring a seamless transition from data collection to post-processing and validation:

1. Data Collection and Preprocessing: This initial phase involves gathering data from diverse sources and conducting preprocessing to standardize formats and eliminate noise, setting a clean slate for analysis.
2. Semantic Analysis: NLP technologies are employed to perform a deep semantic analysis of textual data, extracting and identifying sensitive content like personal identifiers, by understanding the context and meaning behind words and phrases.
3. Query Concept Mining: The framework delves into *Query Concept Mining*, using n-grams for identifying canonical concepts within queries. It meticulously extracts and analyzes unigrams, bigrams, and trigrams, utilizing statistical and ML techniques to represent these n-grams as vectors in a high-dimensional space.

   Sensitive n-grams are filtered based on frequency thresholds and mutual information metrics, with a minimal occurrence threshold set to ensure data density. The weighting of n-grams is determined through:

$$W_x = \log_2(N + 1) \tag{1}$$

   for unigrams, and mutual information for bigrams and trigrams as follows:

$$W_{x,y} = \log_2 \frac{P(x,y)}{P(x)\cdot P(y)+1} \tag{2}$$

$$W_{x,y,z} = \log_2 \frac{P(x,y,z)}{P(x)\cdot P(y)\cdot P(z)+\epsilon} \tag{3}$$

4. Pattern Recognition and Learning: ML algorithms are then leveraged to discern patterns and anomalies indicative of sensitive information, learning from labeled datasets to recognize complex data patterns that might otherwise be overlooked.
5. Anonymization Engine: Armed with insights from semantic analysis and pattern recognition, the anonymization engine applies data transformations to fulfill the criteria of semantic k-anonymity, making each data point indistinguishable from at least $k-1$ others.

6. Utility Preservation: Integral to our framework is the commitment to preserving the utility of anonymized data. Techniques such as generalization, substitution, and noise addition are employed judiciously to minimize impact on data utility.
7. Post-Processing and Validation: The final stage involves a thorough post-processing and validation phase, where the data is scrutinized to confirm the efficacy of the privacy measures implemented and to ensure the retention of data utility. This phase may also include simulations of potential de-anonymization attacks using additional ML models to test the resilience of the anonymized data.

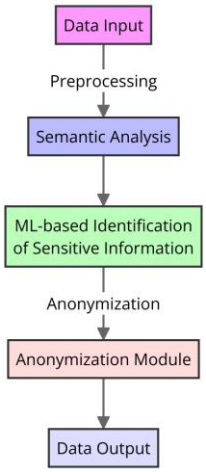

FIGURE 2. Operating steps of the proposed method

This comprehensive framework is visualized in ??, depicting the deep learning-based NLP process, from data collection to post-validation, ensuring a delicate balance between privacy protection and data utility.

B. DATA UTILITY AND PRIVACY BALANCE

The proposed framework ensures a nuanced balance between data utility and privacy by implementing an adjustable Θ-threshold, which fine-tunes the granularity of anonymization in alignment with privacy requirements. The Θ-affinity measure, pivotal in this process, is designed to preserve semantic relationships within the data, thereby maintaining its utility for subsequent analysis. By strategically modulating this threshold, we refine the anonymization process to guarantee that the output, while anonymized, retains significant analytical value. This dynamic adjustment allows for the preservation of data utility without compromising the privacy of individuals represented in the dataset.

C. EXPERIMENT DESIGN

To validate the efficacy and resilience of our framework, a comprehensive set of experiments is devised, focusing on the dual objectives of assessing anonymization effectiveness and resistance to de-anonymization attempts. These experiments utilize a diverse array of datasets, each with unique structures and varying levels of sensitivity, to mimic the complexity of real-world data scenarios. The success of our anonymization process is primarily measured by its ability to reduce the risk of re-identification,

quantified through the likelihood of accurately linking anonymized records back to individual identities. Furthermore, to test the framework's robustness against privacy breaches, simulated de-anonymization attacks employing advanced inference techniques are conducted. The resilience of the framework against such attacks, coupled with qualitative feedback from domain experts on the utility of anonymized versus original datasets, provides a comprehensive understanding of its performance. Insights gained from these experiments are instrumental in driving iterative improvements to the anonymization algorithms, thereby optimizing the delicate trade-off between ensuring privacy protection and retaining data utility.

V. EXPERIMENTS AND RESULTS

A. DATASET SELECTION

To rigorously test the framework's effectiveness across various domains, we selected a diverse array of datasets encompassing search logs, social media posts, and email communications. Each dataset was chosen for its distinct structure, sensitivity level, and representation of real-world scenarios, ensuring a comprehensive evaluation. Search logs provide insight into user behavior and preferences, social media posts reflect personal opinions and interactions, while emails contain formal and informal exchanges, each presenting unique challenges and opportunities for anonymization.

B. EVALUATION METRICS

The efficacy of our anonymization framework is quantified through several key metrics, each providing insight into different aspects of the anonymization process. The primary metric utilized is the $F\beta$ score, which amalgamates precision and recall in a weighted manner, reflecting the trade-off between minimizing the release of sensitive queries (precision) and maximizing the release of non-sensitive ones (recall). The choice of β in the $F\beta$ score tailors this balance to the specific needs of the privacy scenario at hand. The Θ-threshold's influence on anonymization quality is another critical metric, demonstrating the framework's ability to adapt the specificity of anonymization to different privacy requirements. A lower Θ allows for a less stringent anonymization, potentially releasing more data, whereas a higher Θ ensures stronger privacy by grouping more queries together. Additionally, the anonymity level k is a decisive metric, indicating the degree of indistinguishability each query has among others in the dataset. A higher k value denotes stronger privacy protection but may impact data utility.

Re-identification risk, assessed through the likelihood of correctly matching anonymized records to individuals, provides a quantitative measure of privacy strength, indicating the framework's resilience against potential de-anonymization attacks. Conversely, data retention is gauged by the ability of semantic k-anonymity to retain a significant number of nonsensitive queries, signifying the framework's capacity to preserve data utility. These evaluation metrics, considered collectively, enable a comprehensive assessment of the anonymization framework, ensuring an effective balance between the imperatives of privacy protection and the need for analytically valuable data.

C. ANALYSIS

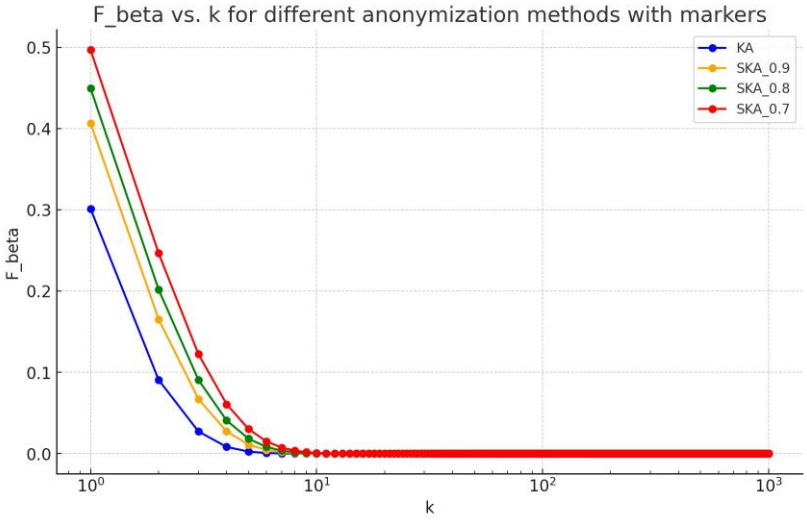

FIGURE 3. The F_β performance of anonymization methods on queries with sensitivity labels for $\beta = 1$. This measure reflects a balanced emphasis on precision and recall. The x-axis is on a logarithmic scale to accommodate the wide range of *k* values.

In our evaluation, the ability to release a maximal number of infrequent yet non-sensitive queries was assessed. A set of 5000 random queries was manually annotated to discern sensitive content, such as personal details or specific location information. The anonymity level *k* for each query was calculated using different approaches: traditional k-anonymity (KA) and semantic k-anonymity (SKA) with thresholds Θ= 0.9,0.8, and 0.7. Queries were categorized as either 'released' or 'non-released' based on whether their anonymity degree was at least *k*, ranging from 1 to 1000.

The anonymization methods were evaluated using the $F\beta$ metric, which amalgamates precision and recall with a weighting factor β, prioritizing the non-release of sensitive queries. Our results indicate that SKA consistently surpasses KA across all values of *k*, with SKA (Θ= 0.8) notably outperforming SKA (Θ= 0.9) when $\beta = 1$ as shown in Fig. 3., highlighting its superior balance between privacy preservation and data retention. As β decreases, this relationship inverts, suggesting a complex interplay between the threshold Θ and the importance placed on precision over recall. The decline in $F\beta$ as *k* increases signifies a diminishing recall, which becomes less pronounced as β trends towards zero, underscoring the enhanced capability of semantic k-anonymity in safeguarding privacy while maintaining data utility.

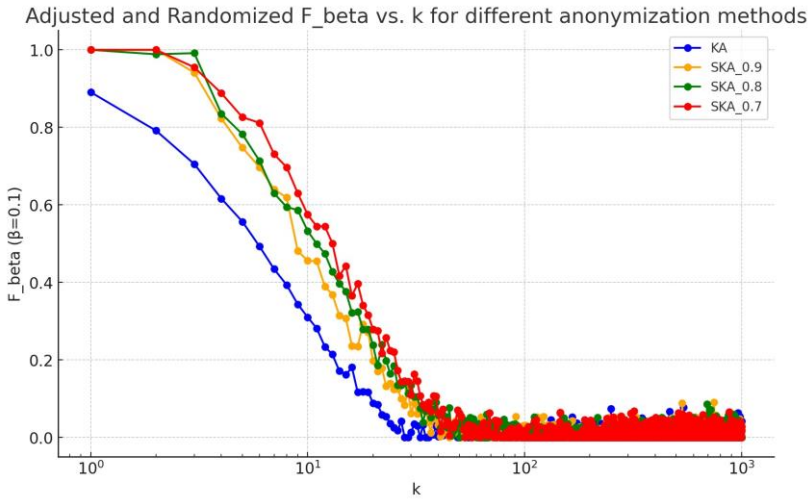

FIGURE 4. The F_β performance of anonymization methods on queries with sensitivity labels for $\beta = 0.1$. This measure places a heightened emphasis on precision over recall. The x-axis is on a logarithmic scale to clearly display performance across the expansive range of *k* values.

?? illustrates the performance of various anonymization methods, specifically focusing on the scenario where a higher emphasis is placed on precision over recall, with $\beta = 0.1$. This figure provides insights into how each method, including KA and SKA with different Θ thresholds, performs in terms of minimizing the risk of releasing sensitive queries. It is evident from the logarithmic scale that as the value of *k* increases, the ability of the anonymization methods to discriminate between sensitive and non-sensitive queries varies, with semantic k-anonymization methods generally showing a more consistent performance across the spectrum of *k*.

VI. CONCLUSION

The research detailed in this document showcases an advanced framework that expertly combines semantic k-anonymity with the forefront of machine learning (ML) and natural language processing (NLP) technologies. Our thorough evaluation, particularly through the lens of the $F\beta$ score, highlights the framework's outstanding capability in protecting personal data privacy while still enabling meaningful data analysis. The framework's design to adapt across various Θ thresholds showcases its flexibility, allowing it to cater to diverse anonymization needs and data sensitivities effectively. A standout feature of this framework is its adeptness at preserving the utility of data for analysis, evidenced by its ability to retain a substantial number of non-sensitive queries. This characteristic is especially significant, as it directly addresses one of the most critical challenges in data anonymization and data utility without compromising privacy. The utilization of ML and NLP not only enhances the precision in identifying sensitive information but also ensures the anonymized data remains valuable for researchers and analysts. Moreover, the framework demonstrates robust resistance against de-anonymization tactics, affirming its reliability in safeguarding user privacy. This balance between privacy protection and data utility underscores the framework's potential as a pioneering

solution in the realm of data anonymization, setting a new benchmark for privacy-preserving data analysis in various sectors.

Looking ahead, there is potential for this framework to be further refined and tailored to an even broader spectrum of data types and privacy concerns. Future research directions will explore its scalability, the integration of additional semantic layers for deeper context analysis, and the implementation of real-time anonymization in dynamic data environments. As digital privacy concerns continue to evolve, so too will our framework, adapting to meet the needs of an increasingly data-driven world. This research not only contributes to the theoretical landscape of digital privacy but also provides a practical toolkit for organizations and individuals navigating the complexities of data protection.

REFERENCE

[1] H. Alawad, S. Kaewunruen, and M. An, "A Deep Learning Approach Towards Railway Safety Risk Assessment," *IEEE Access*, vol. 8, pp. 102811–102832, 2020.

[2] A. Majeed and S. Lee, "Anonymization Techniques for Privacy Preserving Data Publishing: A Comprehensive Survey," *IEEE Access*, vol. 9, pp. 8512–8545, 2021.

[3] R. Epstein, R. E. Robertson, D. Lazer, and C. Wilson, "Suppressing the Search Engine Manipulation Effect (SEME)," *Proceedings of the ACM on Human-Computer Interaction*, vol. 1, no. CSCW, pp. 42:1–42:22, Dec. 2017.

[4] E. Goldman, "Revisiting Search Engine Bias," *Economics of Networks eJournal*, Apr. 2011. [Online]. Available: https:

//www.semanticscholar.org/paper/Revisiting-Search-Engine-Bias-Goldman/

793f59c61a45ef4580f811f66f697184b0a4523c

[5] G. A. Manne and J. D. Wright, "If Search Neutrality is the Answer, What's the Question?" Rochester, NY, Apr. 2011.

[6] L. Guijarro, V. Pla, B. Tuffin, P. Maillé, and P. Coucheney, "A game theory-based analysis of search engine non-neutral behavior," in *Proceedings of the 8th Euro-NF Conference on Next Generation Internet NGI 2012*, Jun. 2012, pp. 119–124.

[7] E. Rader, K. Cotter, and J. Cho, "Explanations as Mechanisms for Supporting Algorithmic Transparency," in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, ser. CHI '18. New York, NY, USA: Association for Computing Machinery, Apr. 2018, pp. 1–13.

[8] N. Diakopoulos and M. Koliska, "Algorithmic Transparency in the News Media," *Digital Journalism*, vol. 5, no. 7, pp. 809–828, Aug. 2017.

[9] C. M. Segijn, J. Strycharz, A. Riegelman, and C. Hennesy, "A Literature Review of Personalization Transparency and Control: Introducing the Transparency–Awareness–Control Framework," *Media and Communication*, vol. 9, no. 4, pp. 120–133, Nov. 2021.

[10] E. Goldman, "Search Engine Bias and the Demise of Search Engine Utopianism," in *Web Search: Multidisciplinary Perspectives*, ser. Information Science and Knowledge Management, A. Spink and M. Zimmer, Eds. Berlin, Heidelberg: Springer, 2008, pp. 121–133.

[11] B. Kenig and T. Tassa, “A practical approximation algorithm for optimal k-anonymity,” *Data Mining and Knowledge Discovery*, vol. 25, no. 1, pp. 134–168, Jul. 2012.

[12] X. Zhang, L. T. Yang, C. Liu, and J. Chen, “A Scalable Two-Phase Top-Down Specialization Approach for Data Anonymization Using MapReduce on Cloud,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 2, pp. 363–373, Feb. 2014.

[13] W. Jiang and C. Clifton, “A secure distributed framework for achieving k-anonymity,” *The VLDB Journal*, vol. 15, no. 4, pp. 316–333, Nov. 2006.

[14] J. Domingo-Ferrer and V. Torra, “Ordinal, Continuous and Heterogeneous kAnonymity Through Microaggregation,” *Data Mining and Knowledge Discovery*, vol. 11, no. 2, pp. 195–212, Sep. 2005.

[15] Z. Huang, “Sensitive Information Detection Using HMM&SVM,” in *2021 3rd International Conference on Intelligent Medicine and Image Processing*, ser. IMIP ’21. New York, NY, USA: Association for Computing Machinery, Sep. 2021, pp. 146–150.

[16] A. Yaseen, “UNCOVERING EVIDENCE OF ATTACKER BEHAVIOR ON THE NETWORK,” ResearchBerg Review of Science and Technology, vol. 3, no. 1, pp. 131–154, Dec. 2020.

[17] G. Xu, C. Qi, H. Yu, S. Xu, C. Zhao, and J. Yuan, “Detecting Sensitive Information of Unstructured Text Using Convolutional Neural Network,” in *2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*, Oct. 2019, pp. 474–479.

[18] A. Jana and C. Biemann, “An Investigation towards Differentially Private Sequence Tagging in a Federated Framework,” in *Proceedings of the Third Workshop on Privacy in Natural Language Processing*, O. Feyisetan, S. Ghanavati, S. Malmasi, and P. Thaine, Eds. Online: Association for Computational Linguistics, Jun. 2021, pp. 30–35.

[19] H. Yang, L. Huang, C. Luo, and Q. Yu, “Research on Intelligent Security Protection of Privacy Data in Government Cyberspace,” in *2020 IEEE 5th International Conference on Cloud Computing and Big Data Analytics (ICCCBDA)*, Apr. 2020, pp. 284–288.

[20] Q. Wang, M. Du, X. Chen, Y. Chen, P. Zhou, X. Chen, and X. Huang, “PrivacyPreserving Collaborative Model Learning: The Case of Word Vector Training,” *IEEE Transactions on Knowledge and Data Engineering*, vol. 30, no. 12, pp. 2381–2393, Dec. 2018.