mathematics

MDPI

Article

Comprehensive Evaluation Method of Privacy-Preserving Record Linkage Technology Based on the Modified Criteria Importance Through Intercriteria Correlation Method

Shumin Han [1,*], Yue Li [1], Derong Shen [2] and Chuang Wang [1]

[1] School of Artificial Intelligence and Software, Liaoning Petrochemical University, Fushun 113001, China; liyue@stu.lnpu.edu.cn (Y.L.); wangchuang@lnpu.edu.cn (C.W.)

[2] School of Computer Science and Engineering, Northeastern University, Shenyang 110819, China; shenderong@ise.neu.edu.cn

* Correspondence: hanshumin@lnpu.edu.cn

Abstract: The era of big data has brought rapid growth and widespread application of data, but the imperfections in the existing data integration system have become obstacles to its high-quality development. The conflict between data security and shared utilization is significant, with traditional data integration methods risking data leakage and privacy breaches. The proposed Privacy-Preserving Record Linkage (PPRL) technology, has effectively resolved this contradiction, enabling efficient and secure data sharing. Currently, many solutions have been developed for PPRL issues, but existing assessments of PPRL methods mainly focus on single indicators. There is a scarcity of comprehensive evaluation and comparison frameworks that consider multiple indicators of PPRL(such as linkage quality, computational efficiency, and security), making it challenging to achieve a comprehensive and objective assessment. Therefore, it has become an urgent issue for us to conduct a multi-indicator comprehensive evaluation of different PPRL methods to explore the optimal approach. This article proposes the use of an modified CRITIC method to comprehensively evaluate PPRL methods, aiming to select the optimal PPRL method in terms of linkage quality, computational efficiency,and security. The research results indicate that the improved CRITIC method based on mathematical statistics can achieve weight allocation more objectively and quantify the allocation process effectively. This approach exhibits exceptional objectivity and broad applicability in assessing various PPRL methods, thereby providing robust scientific support for the optimization of PPRL techniques.

Keywords: Privacy-Preserving Record Linkage; CRITIC method; weight allocation; multi-indicator comprehensive evaluation

MSC: 68P27

check for updates

Citation: Han, S.; Li, Y.; Shen, D.; Wang, C. Comprehensive Evaluation Method of Privacy-Preserving Record Linkage Technology Based on the Modified Criteria Importance Through Intercriteria Correlation Method. *Mathematics* **2024**, *12*, 3476. https://doi.org/10.3390/math12223476

Academic Editors: Jonathan Blackledge and Antanas Cenys

Received: 19 September 2024
Revised: 2 November 2024
Accepted: 4 November 2024
Published: 7 November 2024

1. Introduction

The era of big data has led to an explosive growth in data, which is deeply intertwined with people's lives and extensively utilized across various fields [1,2]. The linkage and integration of data [3,4] provide a robust foundation for the efficient operation and development of diverse industries and society as a whole. Record linkage, also referred to as record matching, constitutes a core technology in data integration, facilitating the identification and classification of identical or similar records from diverse sources to disclose corresponding real-world entities. It is typically employed in combination with truth discovery [5] when addressing complex data integration tasks. Entity alignment [6], also known as entity matching or ontology alignment, is a key step in the knowledge graph. It involves cross-language and cross-domain knowledge graphs. The goal is to identify and map together nodes describing the same real-world entity in different graphs. In practice, record linkage is often a subtask or pre-step in entity alignment. However, as we proceed with the implementation of record linkage, we must also confront a series of challenges. Nowadays, hosting database services on cloud systems has become a common practice characterized by highly dynamic data that possesses substantial capacity and is susceptible to loss [7]. These characteristics pose significant challenges to privacy and security. They also hinder inter-system information exchange, leading to low utilization rates and high circulation costs. How do we address the critical concern of privacy protection in the process of record matching? For instance, we can select the appropriate privacy protection methods based on the varying sensitivity of the data, thereby ensuring both the availability of the data and safeguarding sensitive information to prevent privacy breaches when disseminating interval value data [8]. And an efficient privacy-preserving semantic-aware multi-keyword-ranked search scheme in the cloud to meet users in the cloud environment for efficient, accurate, privacy and security search needs [9]. Henceforth, Privacy-Preserving Record Linkage technology emerged [10], aiming to identify matching records without compromising the privacy or confidentiality of unmatched entities by only sharing final results between sources [11]. This effectively enables data linkage and integration without exposing personal sensitive information. PPRL finds wide application in medical care, government departments, educational institutions, social networks among other fields, for instance, protecting the privacy of patients' medical records [12,13] while facilitating accurate analysis for personalized treatment plans in healthcare settings; similarly safeguarding user privacy on social platforms while enabling personalized service recommendations based on interest and behavior analysis.

The existing PPRL technology has achieved many results [14], such as Bloom Filters, Homomorphic Encryption algorithms, Secure Multi-Party Computation, and Differential Privacy Mechanisms. So choosing a secure and efficient PPRL method according to the requirements of scenarios has become an urgent problem to be solved. The current evaluation of PPRL methods is mainly evaluated by focusing on a single metric, such as linkage quality or computational efficiency [15,16], and it fails to fully consider the balance among security, efficiency and linkage quality of PPRL methods. There is a lack of a comprehensive evaluation and comparison framework for PPRL methods that consider multiple indicators. For example, Dinusha Vatsalan's group proposed a general framework equipped with standardized measures [17]. This framework aims to provide an overall evaluation criterion for PPRL methods, evaluating their performance in terms of scalability, linkage quality and privacy protection. However, it has limitations as it emphasizes adjusting the weights of these indicators according to users' specific needs and preferences but does not clearly provide a specific quantitative method for calculating these weights.

Aiming at the above problems, we propose a comprehensive evaluation method of privacy protection record chaining technology based on the modified Criteria Importance Through Intercriteria Correlation(CRITIC) method [18–22]. This method can comprehensively consider a variety of key performance indicators according to the needs of business scenarios. It adaptively modifies the assessment methodology in response to the intrinsic connections within the indicator data. By accounting for the differences and conflicts among the indicators within PPRL methods, it clearly outlines the process for assigning weights to each indicator. This enables a comprehensive evaluation of its various aspects [23–26], culminating in the identification of the method with the superior overall performance. Consequently, it offers a more secure and efficient solution for safeguarding privacy in the digital era.

The key contributions of our method are as follows:

- We meticulously select a series of key indicators tailored to the specific business scenario. By employing the forward and backward normalization methods, we effectively mitigate the discrepancies caused by varying dimensions and value ranges among different indicators. This refined approach makes the evaluation results more precise and objective.

- We use the coefficient of variation to quantify the variability among indicators. By considering their average values and the extent of their dispersion, we achieve a more objective and rational weight allocation.
- According to the internal relationship between the selected indicators, Pearson correlation coefficient calculation formula or Spearman correlation coefficient calculation formula can be used to flexibly and accurately quantify the correlation between indicator variables, so that the subsequent evaluation and analysis results are more accurate and objective.

The experimental findings indicate that the improved CRITIC method can more precisely and objectively identify the approach or framework that exhibits the most superior comprehensive performance across several pivotal indicators. This refined CRITIC method not only aids researchers and decision-makers in conducting a more comprehensive and precise analysis and comparison of the performance of various framework models, thereby facilitating the selection of the optimal solution for a given scenario, but it also exerts a profound influence on advancing the progress and fostering the application development within related technological fields. It is noteworthy that the scope of application of this improved CRITIC method is not limited to PPRL method, and it can be extended to encompass a wide array of indicator framework models, inclusive of time series prediction models. The integration of time series forecasting models, which is a technology that leverages historical time data to anticipate future events or trends [27]. Its integration further broadens the application field and practical value of CRITIC method.

The structure of the subsequent parts of this paper is as follows: Section 2 outlines the preliminary work related to the methods proposed in this study. Section 3 introduces the problem definition and related background knowledge. Section 4, as the methodology section, illustrates the implementation process of this method by enumerating a concrete example. Section 5 comprehensively evaluates and summarizes several mainstream PPRL methods. Section 6 summarizes the article and points out some deficiencies as well as future research directions.

2. Related Work

The section primarily discusses the current challenges in evaluating PPRL methods, focusing on both single indicator evaluation and comprehensive evaluation. Subsequently, we propose a research direction for conducting multi-indicator comprehensive evaluation [28–30] of various PPRL methods to address these challenges.

Currently, numerous solutions have been engineered to address the challenges posed by PPRL technology. However, the assessment of these methods predominantly revolves around the evaluation of individual metrics, with only a few comprehensive evaluation frameworks having been suggested. The constraints inherent in these evaluation approaches hinder a clear determination of the relative merits and flaws of the various methods. The limitations of both single-indicator evaluations and multi-indicator comprehensive assessments are primarily centered on the following aspects:

The delicate balance between privacy preservation and data utility is often overlooked: The fundamental objective of PPRL technology is to effectively utilize data while simultaneously upholding privacy standards. An evaluation that relies solely on a single metric may fail to capture the nuanced equilibrium between these two critical aspects. For instance, a method might excel in safeguarding privacy yet fall short in terms of accurate data matching or maintaining data integrity, and the converse can also be true.

Inadequacy in Handling Diverse Scenarios: Various application contexts impose distinct demands on PPRL. A single metric may not adequately capture performance across different scenarios. In healthcare data linkage, privacy concerns might be paramount, whereas in commercial data integration, the focus could be on matching accuracy and efficiency [31,32].

Insufficient Comprehensive Performance Analysis: Evaluations based on a single metric often concentrate on one performance dimension, such as linkage accuracy, privacy protection level, or computational efficiency. However, assessing PPRL technology necessitates a multifaceted approach due to the inherent trade-offs between privacy and accuracy. A single metric may not provide a holistic view of a technique's performance.

Challenges in Comparing Methods: Different PPRL methods may employ varied privacy protection strategies, algorithmic designs, or implementations. A single metric evaluation might not facilitate an accurate comparison of their respective strengths and weaknesses. Some methods may prioritize privacy protection, while others optimize for linkage accuracy.

Lack of Standardized Evaluation Criteria: PPRL spans several domains, including privacy, data mining, and information security, but lacks unified evaluation criteria. Consequently, single-indicator assessments can vary based on the assessor's background and objectives, compromising comparability and credibility.

Potential Inaccuracy in Evaluation Results: Single-indicator evaluations can be influenced by factors such as dataset choice and parameter settings, leading to unstable or biased outcomes. Employing a multi-indicator evaluation approach, complemented by statistical tests, can provide a more precise assessment of the PPRL performance.

Nonetheless, implementations of comprehensive, multi-indicator evaluation and comparison frameworks for PPRL methods are relatively scarce, for instance, Dinusha Vatsalan's group introduced a universal framework accompanied by standardized metrics [17], which is designed to offer a holistic evaluation benchmark for PPRL methods. This framework aims to assess their performance across dimensions such as scalability, linkage quality, and privacy protection. Nevertheless, this framework has its limitations; for example, the selected evaluation metrics may not be exhaustive enough to thoroughly gauge the performance of PPRL methods, frameworks may display a hint of inflexibility in the face of rapid changes in privacy protection requirements and application scenarios, and the experimental datasets utilized might not be diverse enough to encapsulate the full spectrum of potential real-world scenarios. Similarly, Nanayakkara Charini's team presented a comprehensive and robust set of evaluation indicators and methodologies [33] within the context of group-based record linkage (GBRL) to assess the efficacy of group-based record linkage techniques. However, while group-based record linkage has broad applicability across various domains, our method focuses on a subset of these scenarios, which could compromise the generality of the findings. Consequently, the evaluation outcomes might be skewed or constrained, failing to capture the full range of performance characteristics in different contexts.

The current evaluation methods are constrained to assessing PPRL methods from various angles but fall short of achieving a holistic evaluation. To overcome these deficiencies, we adopt a multi-indicator comprehensive evaluation methodology when evaluating PPRL methods, which strikes a balance among multiple indicators like runtime, linkage quality, and security [34]. We adjust the most suitable evaluation benchmarks [35] in accordance with the specific requirements and constraints of the application scenario. Such an evaluation facilitates a thorough consideration of the advantages and disadvantages of PPRL methods within a particular application context, enabling us to identify the method that performs best across several key indicators and thereby providing secure and efficient decision-making support for practical applications. Hence, developing a comprehensive evaluation method applicable to various indicators and different application scenarios is an urgent matter that we need to tackle.

3. Preparation Work

3.1. Problem Definition

Definition 1 (Privacy-Preserving Record Linkage)**.** *Suppose each of the P parties $P_1, P_2, \ldots, P_P (P \geq 2)$ owns the dataset $D_1, D_2, \ldots, D_P$. Parties want to determine which of their records $R_{1,i} \in D_1, R_{2,j} \in D_2, \ldots, R_{p,k} \in D_p$ match (corresponding to the same entity) based on record encryption or encoding of Quasi Identifiers (QIDs): attributes that have the potential to identify a record. The decision model $C(\cdot)$ classifies the record$(R_{1,i}, R_{2,j}, \ldots, R_{p,k})$ set into two classes: match* *and mismatch. In the above process, only the records classified as matching are shared among the participants, and the information of other unmatched records is not leaked.*

Definition 2 (Spearman's rank correlation coefficient)**.** *The Spearman's rank correlation coefficient, proposed by Charles Spearman, measures the correlation between the ranks (orders) of two variables. It depends on the order of the data rather than the specific values. Ranging from* -1 *to 1, a coefficient of 1 indicates a perfect positive correlation,* -1 *indicates a perfect negative correlation, and 0 indicates no linear correlation.*

Definition 3 (Pearson correlation coefficient)**.** *The Pearson correlation coefficient, devised by Karl Pearson, quantifies the strength of the linear relationship between two continuous variables. It operates under the assumption that these variables are normally distributed and continuous in nature. Similar to Spearman's rank correlation coefficient, the Pearson correlation coefficient occupies a spectrum from* -1 *to 1. A coefficient of +1 signifies a perfect positive linear relationship,* -1 *a perfect negative linear relationship, and 0 indicates no discernible linear association between the variables.*

3.2. CRITIC Introduction

Typically, when assigning weights to indicators, there is a tendency to focus on the data itself. However, the fluctuations between data points or the correlations among them also convey valuable information. We can leverage the extent of data volatility or the correlation between data points to calculate the weight for each indicator.

The CRITIC weighting method is an objective approach that considers data volatility. It is based on two key measures: volatility, also known as contrast strength, and conflict, which is a measure of correlation. Volatility is quantified by the standard deviation—a higher standard deviation signifies greater fluctuation and thus a higher weight. Conflict is captured by the correlation coefficient; a higher degree of correlation between indicators implies less conflict and consequently a lower weight. The underlying principle is to determine the objective weight of an indicator by assessing the balance between contrast strength and conflict, thereby achieving an objective weight distribution for the evaluation scheme. This method is particularly useful for assessing the stability of data and is well-suited for analyzing datasets where indicators or factors exhibit a certain degree of correlation. The exhaustive steps of the method are as follows:

Constructing data matrices: We construct the initial data matrix according to the collected indicator data.

Dimensionless Processing: To eliminate the influence of varying dimensions on the evaluation outcomes, dimensionless processing is essential for each indicator. Depending on the type of indicator, the CRITIC weighting method typically employs either direct or indirect normalization techniques.

Indicator variability: Within the CRITIC methodology, the standard deviation is employed to capture the disparity and fluctuation among the internal values of each indicator. A higher standard deviation indicates a greater numerical spread within the indicator, signifying that it encapsulates more information and possesses a stronger intrinsic evaluation power. Consequently, such indicators should be allocated a higher weight in the overall assessment.

Indicator conflict: The correlation coefficient is utilized to represent the interdependence among indicators The stronger the correlation with other indicators, the less conflict there is between the indicator in question and the others. This high correlation suggests that the indicators reflect similar information, leading to a degree of repetition in the evaluation content. Consequently, the intrinsic evaluation strength of the indicator is somewhat diminished, warranting a reduction in the weight assigned to it.

Information carrying capacity: The larger C_j is, the greater the role of the j-th evaluation indicator in the whole evaluation indicator system, and more weight should be assigned to it.

Weight assignment: According to the obtained information bearing capacity, the weight w_j of the indicator is calculated.

4. Methodology

To address the issue that current evaluation methods fall short of providing a holistic assessment of PPRL methods, this project employs an modified CRITIC approach to examine the interplay among multiple indicators, discern the relational model between these indicators, and subsequently devise an appropriate solution method. By aggregating the information from various indicators of the PPRL method, a comprehensive indicator is derived, which serves to encapsulate the overall performance of the PPRL method.

In the following sections, in conjunction with the multiple indicators within the PPRL method, a detailed exposition of the three modules of the comprehensive evaluation methodology for privacy-preserving record linkage technology based on the improved CRITIC method will be provided. These modules include the construction of a standardization matrix, the allocation of indicator weights, and the comprehensive evaluation. The entire processing flow is depicted in Figure 1, with Algorithm 1 offering a detailed breakdown. Table 1 delineates the parameters utilized in the proposed method and their respective significance.

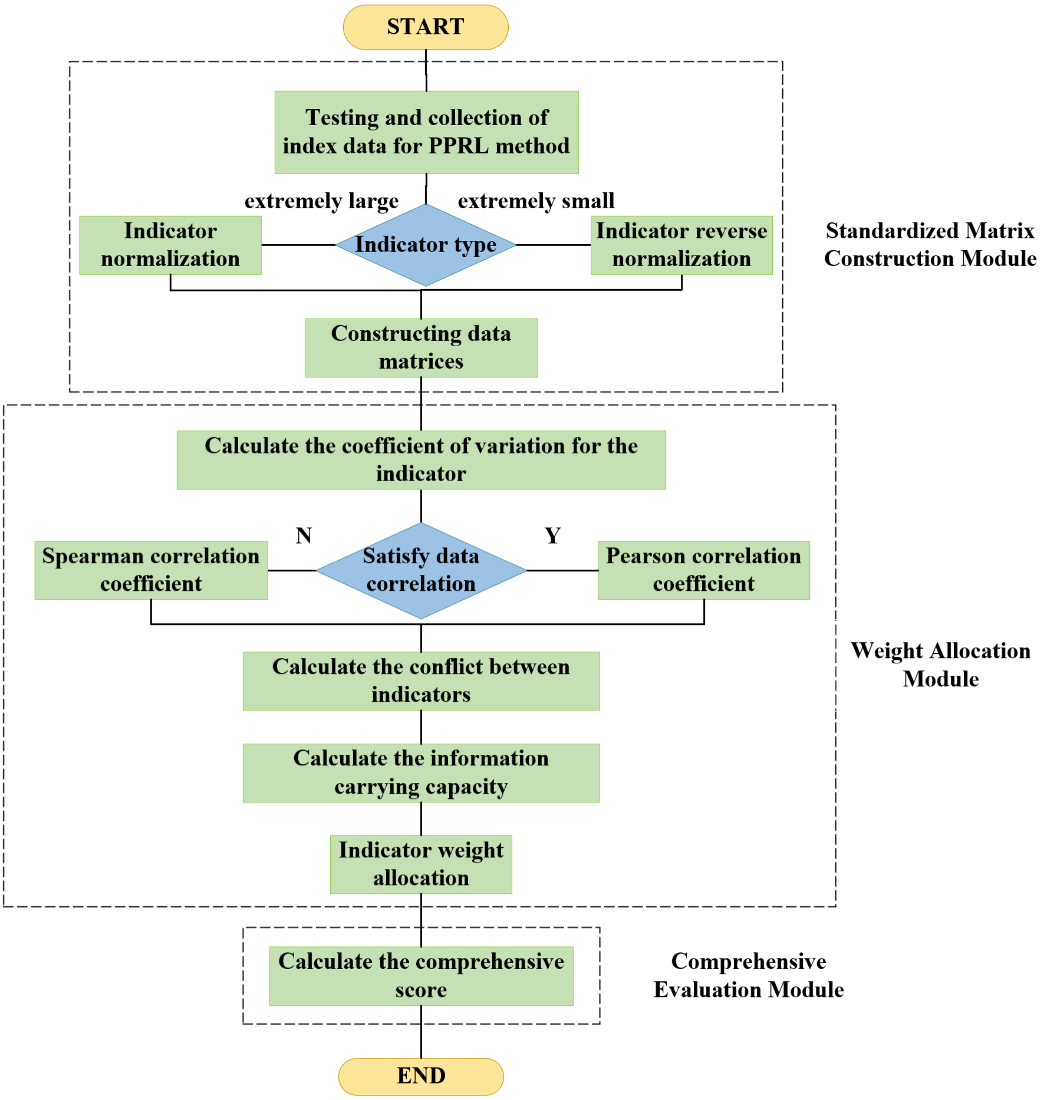
START
Testing and collection of index data for PPRL method
extremely large
extremely small
Indicator normalization
Indicator type
Indicator reverse normalization
Standardized Matrix Construction Module
Constructing data matrices
Calculate the coefficient of variation for the indicator
N
Y
Spearman correlation coefficient
Satisfy data correlation
Pearson correlation coefficient
Calculate the conflict between indicators
Weight Allocation Module
Calculate the information carrying capacity
Indicator weight allocation
Calculate the comprehensive score
Comprehensive Evaluation Module
END

Figure 1. Flowchart of comprehensive evaluation of privacy-preserving record linkage techniques based on the modified CRITIC method.

Table 1. Parameter table of PPRL multi-indicator comprehensive evaluation algorithm based on improved CRITIC method.

Parameters	Meaning
m	The number of PPRL methods involved in the evaluation
M_i	The i-th PPRL method $(1 \leq i \leq m)$
B	The data source for each method
S_i	The security of method i
L_i	linkage quality of method i
R_i	The runtime of method i
j	indicator $j(1 \leq j \leq 3)$
$\bar{x}_j$	The mean of the indicator j
s_j	The standard deviation of the indicator j
v_j	Coefficient of variation of the indicator j
r_{ij}	Correlation coefficient between indicator i and indicator j
f_j	The conflict of the indicator j
C_j	The information carrying capacity of the indicator j
w_j	The weight of the indicator j

Algorithm 1: PPRL Multi-indicator comprehensive evaluation algorithm utilizing the enhanced CRITIC approach

```
Input:$(M_1, M_2, ..., M_i, ..., M_m, B)$
Output:$(E_1, E_2, ..., E_i, ..., E_m)$
$S_i$=security_test$(P_i, B)$;
$L_i$=linkQuality_test$(P_i, B)$;
$R_i$=runtime_test$(P_i, B)$;
for y in range(3):
    $j$=[]
    for x in range($m$):
        $j$.append(m[x][y])
        IF type($j$)==maximal_type:
            RETURN $j$=positive_standardization($j$)
        Elif type($j$)==minimal_type:
            RETURN $j$=reverse_standardization($j$)
  for i in range($m$):
      matrix.append([$S_i$, $L_i$, $R_i$]);
  $\bar{x}_j = \frac{1}{m}\sum_{i=1}^{m} x'_{ij}$
  $s_j = \sqrt{\frac{1}{m-1}\sum_{i=1}^{m}\left(x'_{ij} - \bar{x}'_{ij}\right)^2}$
  $v_j = \frac{s_j}{\bar{x}_j}$
  IF is_correlation($i, j$)==1 :
      RETURN $r_{ij}$=pearson_correlation($i, j$)
  ELSE:
      RETURN $r_{ij}$=spearman_correlation($i, j$)
$f_j$=indicators_conflict($r_{ij}$)
$C_j = v_j f_j$
$w_j = \frac{C_j}{\sum_{j=1}^{m} C_j}$
$E_i = \sum_{j=1}^{n} w_j x'_{ij}$
```

The function of the standardization matrix construction module is to gather and analyze various indicator data related to the PPRL method. This involves normalizing the collected indicator data using direct and indirect normalization techniques, subsequently creating the standardization matrix.

The weight allocation module is designed to assign weights to indicators in a scientifically sound and rational manner. It begins by utilizing the coefficient of variation to quantify the variability among indicators, taking into account the impact of both the average level and the degree of dispersion of the indicators on the weight distribution. Next, depending on the characteristics of the indicator data, either the Pearson correlation coefficient formula or the Spearman correlation coefficient formula is applied to calculate the conflict among indicators. Finally, the weights are determined by integrating the information-carrying capacity derived from these two approaches.

The comprehensive evaluation module is responsible for calculating the ultimate score for each PPRL method based on the assigned weights and provides a comparative summary of the results.

4.1. Standardized Matrix Construction Module

This module primarily aggregates indicator data pertaining to three key aspects of the PPRL method: security, linkage quality, and runtime. It then employs a suite of standardization techniques to normalize the indicator data, ultimately constructing a standardization matrix (Algorithm 1, line 4–13).

4.1.1. Data Collection

The evaluation indicator data for the PPRL method can be gathered across three key dimensions [17,36]: (1) security assessment, (2) linkage quality assessment, and (3) runtime assessment. Among these three aspects, security is a pivotal factor that influences both linkage quality and runtime. A higher level of security necessitates more intricate encryption (or encoding) methods, which in turn increase runtime and diminish computational efficiency. Additionally, enhanced security often results in more complex encryption (or encoding) processes, leading to a wider discrepancy between the encrypted (or encoded) ciphertext (or code) and the original plaintext, thereby reducing linkage quality.

Security

Security is typically appraised through various lenses, such as privacy leakage risk assessment, differential privacy testing, and mock attack testing. The subsequent section delves into the evaluation of the risk of privacy disclosure (line 1 of Algorithm 1).

Suppose the dataset processed by privacy-preserving technology is referred to as the Masked Database (D^M), while the global dataset is labeled as B. D^M may match successfully with records in B that possess identical attribute values, potentially resulting in information disclosure. In this context, the concept of Disclosure Risk (DR) is defined. DR is a numerical value ranging from 0.0 to 1.0, where 0.0 signifies absolute security, with no information leakage, and 1.0 denotes complete exposure, where all information is compromised.

Suppose a^M is an attribute within dataset D^M, and n_g represents the count of a^M attribute values in D^M that share the same value with B. In this case, the probability that a^M is disclosed is $1/n_g$, which is expressed in Equation (1) following normalization.

$$P_s(a^M) = \frac{1/n_g - 1/N}{1 - 1/N} \tag{1}$$

DR Is usually divided into three types: maximum leakage risk, marketing leakage risk, and average leakage risk.

The maximum leakage risk refers to the highest leakage risk value among all attributes of D^M. The maximum leakage risk helps to limit the leakage risk value to ensure data privacy, and its calculation process is shown in Equation (2).

$$DR_{Max} = \max_{a^M \in D^M} (P_s(a^M)) \tag{2}$$

Marketing leakage risk is the proportion of attributes whose leakage risk is 1, which is of great significance for the statistics of fully leaked attributes, and its calculation process is shown in Equation (3).

$$DR_{Mark} = |\{a^M \in D^M : P_s(a^M) = 1.0\}|/n \tag{3}$$

The average leakage risk is used to evaluate the average leakage probability, and the calculation process is shown in Equation (4).

$$DR_{Mean} = \frac{1}{n} \sum_{a^M \in D^M} P_s(a^M) \tag{4}$$

Then, the calculation process of the security indicator in this paper is shown in the following Equation (5).

$$Security = 1 - DR \tag{5}$$

Linkage Quality

Linkage quality is commonly assessed across three dimensions: Precision, Recall, and F-Measure [14] (line 2 of Algorithm 1). The True Duplicates (Tds) denote the set of actual matching records within the dataset, while the Declared Duplicates (Dds) refer to the set of matched records identified by the method. True Positive (TP) denotes instances where records representing the same entity are correctly identified as matches; True Negative (TN) occurs when records representing distinct entities are correctly identified as non-matches; False Positive (FP) arises when records representing different entities are erroneously identified as matches; and False Negative (FN) occurs when records representing the same entity are incorrectly identified as non-matches. Consequently, Precision, Recall, and F-Measure are computed as follows.

Precision: The ratio of the number of true matching record groups in the candidate record group to the number of candidate record groups, the higher the ratio, the more accurate the result of the method, which is calculated by the following Equation (6).

$$Precision = \frac{|Td| \cap |Dd|}{|Dd|} = \frac{|TP|}{|TP| + |FP|} \tag{6}$$

Recall: Regarding the ratio of the number of true matching record groups in the candidate record group to the number of true matching record groups in the data set, the higher the ratio, the more comprehensive the true matching records found by the method, and it is calculated by the following Equation (7).

$$Recall = \frac{|Td| \cap |Dd|}{|Td|} = \frac{|TP|}{|TP| + |FN|} \tag{7}$$

F-measure: The value of F is the harmonic mean of recall and precision and is usually expressed as the following Equation (8).

$$F - Measure = \frac{2 \times Recall \times Precision}{Recall + Precision} \tag{8}$$

Runtime

Runtime serves as a primary metric for assessing the scalability of the PPRL method. To evaluate the scalability of the PPRL method, this paper employs the runtime generated during the linkage process as the basis for evaluation (Algorithm 1, line 3). We apply the PPRL method to the data source B, under identical other conditions, for n iterations, and record the runtime for each iteration. The average of these runtimes is then taken as the runtime for the PPRL method, which is calculated using Equation (9).

$$\bar{t} = \frac{1}{n}\sum_{i=1}^{n} t_i \tag{9}$$

4.1.2. Construction of the Normalized Matrix

In this paper, we evaluate it from three aspects: security, runtime and linkage quality. The security of the PPRL method is tested by the DR (Disclosure Risk), and the F-Measure is used to represent the linkage quality of the PPRL method. We apply the PPRL method to the same data source B, and on the basis of ensuring the same participants and other variables, we use the above measurement methods to collect data on the three indicators of the PPRL method: runtime, linkage quality and security. For example, there are three existing PPRL methods, M_1, M_2, and M_3, and we collect data on their three metrics: runtime, linkage quality, and security. The collected results are as follows: the performance metrics for runtime are recorded as 50, 18, and 100, while the metrics for linkage quality are 0.85, 0.9, and 0.95. Additionally, the security metrics are 0.85, 0.8, and 0.9. The compiled data are presented in Table 2 below.

Table 2. Each evaluation indicator of the three PPRL methods.

Indicators Methods	Runtime	Linkage Quality	Security
M_1	50	0.85	0.85
M_2	18	0.9	0.8
M_3	100	0.95	0.9

We formulate the initial data matrix utilizing the gathered data in conjunction with Equation (10), and the construction result is shown in Equation (11).

$$X = \begin{pmatrix} x_{11} & \cdots & x_{1n} \\ \vdots & \ddots & \vdots \\ x_{m1} & \cdots & x_{mn} \end{pmatrix} \tag{10}$$

$$X = \begin{pmatrix} 50 & 0.85 & 0.85 \\ 18 & 0.9 & 0.8 \\ 100 & 0.95 & 0.9 \end{pmatrix} \tag{11}$$

The primary objective of data standardization is to eliminate the discrepancies in dimension and value range between various indicators, thereby enhancing the reliability and precision of analytical outcomes. By transforming the indices to a common dimension and value range, more precise comparisons and comprehensive analyses can be conducted across different indices. Furthermore, standardization aids in mitigating the impact of outliers, reducing the likelihood of distortion and inaccuracy in the analysis results.

Each metric falls into a specific category: extremely large, extremely small, intermediate, or interval type. The runtime is an extremely small type, aligning it with the reverse indicator category, where a smaller value indicates higher computational efficiency. Linkage quality and security, on the other hand, are extremely large types, categorized as positive indicators. Higher values signify superior linkage quality and security within the range of 0 to 1: a higher value signifies superior performance. It is essential to convert these metrics to a uniform type for comparison purposes. Additionally, given the varying magnitude of each metric, it is necessary to normalize them to a common metric range for meaningful comparison. This article employs both forward and reverse normalization techniques to standardize the data.

Reverse Normalization: The inverting process is used to convert an inverse metric (smaller is better) into a positive metric, while also dimensioning the compressed data in the [0, 1] range. A negative indicator usually represents a bad state or risk, which needs to be reversed into a positive indicator, so that it can be analyzed and compared with other positive indicators.

Direct Normalization: The forward process is mainly used to keep the positive indicator (that is, the indicator with higher values is better) positive and convert it to a dimensionless relative value in the range [0, 1]. This processing helps to eliminate the dimensional differences between different indicators so that different indicators can be compared and analyzed.

We apply the reverse calculation method to the data associated with the reverse indicator runtime, Its calculation formula is shown in the following Equation (12).

$$x'_{ij} = \frac{max(x_{ij}) - x_{ij}}{max(x_{ij}) - min(x_{ij})} \tag{12}$$

We utilize a positive calculation method for the data associated with the two positive metrics of linkage quality and security. Its calculation formula is shown in the following Equation (13).

$$x_{ij}^{'} = \frac{x_{ij} - min(x_{ij})}{max(x_{ij}) - min(x_{ij})} \tag{13}$$

Here, x_{ij} represents the j-th indicator value of the i-th method, while $x_{ij}^{'}$ is the normalized value. $max(x_{ij})$ denotes the maximum value of the j-th indicator, and $min(x_{ij})$ is the minimum value of the j-th indicator.

By employing the aforementioned processing method, the element of x_{ij} in matrix $X = \left(x_{ij}\right)_{m \times n}$ after normalization processing is denoted as $x_{ij}^{'}$, and the matrix formed by these normalized elements is referred to as the normalized matrix $X^{\star} = \left(x_{ij}^{'}\right)_{m \times n}$. The results are shown in Equation (14).

$$X^{\star} = \begin{pmatrix} 0.6097561 & 0 & 0.5 \\ 1 & 0.5 & 0 \\ 0 & 1 & 1 \end{pmatrix} \tag{14}$$

4.2. Weight Allocation Module

In this section, the weights of the three indicators of the PPRL method are assigned using the modified CRITIC method. Balancing the relationship between these indicators and ensuring a reasonable distribution of their weights is crucial for the comprehensive evaluation of the PPRL method. Building upon the CRITIC method, we employ the coefficient of variation rather than the coefficient of standard deviation to gauge the variability between indicators (lines 14–16 of Algorithm 1). The coefficient of variation addresses the impact of disparate units and/or mean values on the comparison of variability levels, making it suitable for comparing the dispersion of datasets with distinct units or means. Moreover, being a relative number, the coefficient of variation is not influenced by the measurement unit of the original data, thus enhancing its universality and comparability.

Additionally, when assessing the conflict between indicators, we utilize different correlation coefficients depending on the interrelationship between indicators (lines 17–20 of Algorithm 1). This approach allows for a more precise quantification of the correlation between indicator variables, thereby enhancing the accuracy of subsequent evaluation and analysis. The following outlines the detailed process for calculating the coefficient of variation, assessing conflict, and determining the weights [37,38].

4.2.1. Coefficient of Variation

The coefficient of variation (CV) is defined as the ratio of the standard deviation to the mean. This measure eliminates the influence of varying units and/or means on the comparison of variability levels, allowing for the comparison of the dispersion of datasets with different units or means. Since the coefficient of variation is a dimensionless quantity, it should be used as the reference when comparing two sets of data with different dimensions or mean values, rather than the standard deviation. A smaller coefficient of variation indicates a smaller degree of variation (deviation), implying lower risk, and thus a lower weight should be assigned to the corresponding indicator. Conversely, a larger coefficient of variation suggests a greater degree of variation (deviation), indicating higher risk, and thus a higher weight should be assigned to the indicator.

Let the standard deviation of the j indicator be s_j, the mean be $\bar{x}_j$, and the coefficient of variation be v_j. The calculation process is shown in the following Equations (15)–(17).

$$s_j = \sqrt{\frac{1}{m-1}\sum_{i=1}^{m}\left(x'_{ij} - \bar{x}'_{ij}\right)^2} \tag{15}$$

$$\bar{x}_j = \frac{1}{m}\sum_{i=1}^{m} x'_{ij} \tag{16}$$

$$v_j = \frac{s_j}{\bar{x}_j} \tag{17}$$

By solving the aforementioned formula, one can determine the standard deviation and coefficient of variation for each indicator. Table 3 presents the standard deviations and coefficients of variation for each indicator of the three PPRL methods, using Equations (15)–(17).

Table 3. The contrast intensity of each indicator.

Indicators	Runtime	Linkage Quality	Security
Standard deviation	0.41151385	0.40824829	0.40824829
Coefficient of variation	0.76691217	0.81649658	0.81649658

4.2.2. Conflictibility

The inter-indicator conflict can be quantified by computing the correlation coefficient between the indicators (line 21 of Algorithm 1). The correlation coefficient is a statistical metric used to gauge the strength and direction of the linear association between two variables. In the assessment of indicator conflict, the correlation coefficient serves as a tool to assess the degree of correlation between different indicators, thereby capturing the conflict between them. When a strong positive correlation is observed, a smaller conflict value suggests a lower weight should be assigned. The magnitude of the conflict between the j indicator and the remaining indicators is denoted as f_j, and r_{ij} represents the correlation coefficient between the i indicators and the j indicators. It is calculated as shown in Equation (18) below.

$$f_j = \sum_{i=1}^{m}(1 - r_{ij}) \tag{18}$$

The measure of indicator conflict is achieved by computing the correlation coefficient between them. Consequently, the exploration of indicator conflict hinges on the selection of an appropriate correlation coefficient. For instance, there exists a certain linear relationship between runtime and security, and hence the Pearson correlation coefficient is employed when calculating the correlation coefficient between these two. In contrast, when calculating the correlation coefficient between runtime and linkage quality, or between linkage quality and security, where no linear relationship is present, the Spearman correlation coefficient is used.

The Pearson correlation coefficient is denoted as r_ρ, and the Spearman correlation coefficient is denoted as r_s. The formulas for calculating them are provided in Equations (19) and (20), respectively.

$$r_\rho = r_{xy} = \frac{cov(x,y)}{\sigma_x \sigma_y} = \frac{\sum_{i=1}^{n}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{n}(x_i - \bar{x})^2}\sqrt{\sum_{i=1}^{n}(y_i - \bar{y})^2}} \tag{19}$$

$$r_s = 1 - \frac{6\sum_{i=1}^{n} d_i^2}{n^3 - n} \tag{20}$$

In the context of calculating the Spearman correlation coefficient, x and y represent the indicator vectors, $\sigma_x \sigma_y$ is the covariance of x and y, σ_x and σ_y are the standard deviations of x and y, respectively, and d_i is the rank difference between the two indicator vectors.

The rank difference for the Spearman correlation is computed as follows:

- Sort the observations of the two variables by magnitude and assign a rank (i.e., the sorted position) to each observation. If there are identical observations, their ranks are averaged.
- Calculate the squared difference between the rank of each variable and its corresponding position, d_i^2, where d_i is the rank difference for the i-th observation, that is, the rank of x_i minus the rank of y_i. The calculation progress is shown in Table 4 below.

Table 4. Indicator element rank difference.

Variable x_i	Element Position (Desc)	Rank	Variable y_i	Element Position (Desc)	Rank	Rank Difference
0.609756	1	1	0	3	3	2
0	3	3	0.5	2	2	1
0.5	2	2	1	1	1	1

By solving the above method, we can obtain the correlation coefficient between the indicators, as shown in Table 5 below.

Table 5. Correlation coefficient between indicators.

Indicators	(Runtime, Linkage Quality)	(Runtime, Security)	(Linkage Quality, Security)
Correlation Coefficient	−0.5	−0.99206453	0.5

Table 6 shows the conflict obtained by using Equation (18) for each indicator of the three PPRL methods.

Table 6. The contrast intensity of each indicator.

Indicators	Runtime	Linkage Quality	Security
Conflict	3.49206453	2	2.49206453

4.2.3. Calculated Weight

Let the information carrying capacity of indicator j be denoted as C_j (line 22 of Algorithm 1), and the weight assigned to indicator j be w_j (line 23 of Algorithm 1), which can be computed as shown in Equations (28) and (29) below.

$$C_j = v_j f_j \tag{21}$$

$$w_j = \frac{C_j}{\sum_{j=1}^{m} C_j} \tag{22}$$

Table 7 shows the weight assignments obtained by using Equations (28) and (29) for each indicator of the three PPRL methods (the outcome is retained precisely to six decimal positions).

Table 7. Weight allocation of each indicator.

Indicators	Runtime	Linkage Quality	Security
Weight	0.422024	0.257332	0.320644

4.3. Comprehensive Evaluation Module

4.3.1. Calculate Score

There are numerous approaches to comprehensive evaluation. Currently, the most commonly employed model for multi-index comprehensive evaluation is the index scoring method based on weighted averages. The core of this method is to aggregate the results of the various indices into a single comprehensive evaluation value through the weighted average technique. This approach is straightforward, easy to understand, and provides clear conclusions, with strong operational capabilities. We compute the final evaluation score for the PPRL method using the weighted average method. Let the final evaluation score of PPRL method M_i be E_i (line 24 of Algorithm 1), and its calculation formula is as shown in Equation (23) below.

$$E_i = \sum_{j=1}^{n} w_j x'_{ij} \tag{23}$$

Table 8 shows the final evaluation scores obtained by using Equation (23) for each index of the three PPRL methods (the outcome is retained precisely to six decimal positions).

Table 8. Evaluation scores for each PPRL method.

Methods	M_1	M_2	M_3
Evaluation score	0.417654	0.550690	0.577976

4.3.2. Discussion

In this section, we have assessed three approaches via a practical case, concentrating on three crucial aspects: linkage quality, runtime, and security. The final scores are relative measures derived from internal comparisons among the methods. Here is the detailed analysis of the results:

Method 3 emerged as the top scorer in the comprehensive evaluation, highlighting its significant advantage in linkage quality. Although it is not the most efficient in terms of runtime, its robust performance in security contributes to its overall outstanding performance. This result indicates that Method 3 is the preferred choice when projects demand high precision in linkage analysis and strong security; Method 2 excelled in runtime, significantly enhancing the efficiency of data processing. While it may fall slightly short of Method 3 in terms of linkage quality, its exceptional runtime performance is sufficient to meet the needs for rapid response. Consequently, Method 2 demonstrates its unique strengths in scenarios where both processing speed and linkage quality are of paramount importance; Method 1 displayed a moderate level across all three evaluation dimensions, with no single metric standing out significantly, nor any noticeable weaknesses. Its composite score reflects a balance in performance, offering stable and reliable linkage quality, reasonable runtime, and ensured security without the pursuit of extreme performance. For projects seeking a comprehensive balance and versatility, Method 1 provides an ideal balanced solution.

In summary, each of the three methods has its distinct features, and their comprehensive evaluation scores reflect their overall performance across different dimensions. Method 3 is suitable for scenarios with stringent requirements for linkage quality and security, Method 2 for occasions where processing speed is crucial while maintaining linkage quality, and Method 1 for applications that prioritize a well-rounded balance in performance.

5. Experiment and Analysis

5.1. Preparatory Work

The dataset employed in this experiment is the North Carolina Voter Registration List (NCVR), which can be downloaded from the FTP address ftp://alt.ncsbe.gov/data/, accessed on 3 September 2024. The data utilized in our method were extracted from genuine public voter record information, ensuring the authenticity and reliability of the dataset. This article implemented the methods discussed using PyCharm (2023.3). The experimental configuration included an Intel Core i5-12600KF CPU, 32 GB of memory, a 1 TB hard drive, and was operated on a 64-bit Windows 10 system. The development environment was PyCharm (2023.3), and the dataset used was the North Carolina Voter Registration List (NCVR).

This section will comprehensively evaluate the current four mainstream PPRL methods, which are Randall et al.'s PPRL method based on homomorphic encryption (HE-PPRL) [39], Durham et al.'s PPRL method based on composite bloom filter (RBF-PPRL) [40], Karapiperis et al.'s PPRL method based on the FEDERAL framework (F-PPRL) [41], and the PPRL method (MD-PPRL) proposed by Vatsalan et al., which combines a bloom filter, secure summation, and Dice coefficient similarity calculation protocol [42].

5.2. Experimental Data Collection

5.2.1. Scalability Testing

Firstly, the scalability of each PPRL method was assessed by examining how the runtime of the method varied with the increase in the size of the data source. We maintained a fixed number of parties, $p = 5$, and measured the runtime of each method as a function of the data source size (5 k, 10 k, 50 k, 100 k, 500 k, 1000 k). The test results are presented in the following Figure 2.

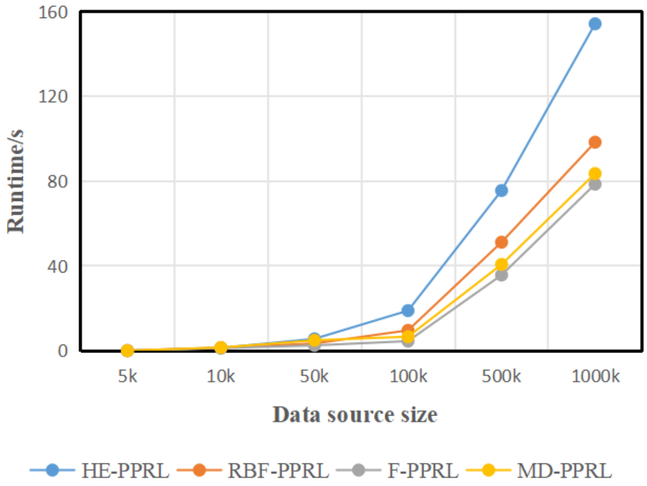

Figure 2. Runtime versus data source size.

Secondly, to assess how the runtime of each PPRL method is affected by the increase in the number of parties, we fixed the data source size at B = 5 k. We then tested the runtime of each method as the number of parties varied (3, 5, 7, 9), and the results are depicted in the following Figure 3.

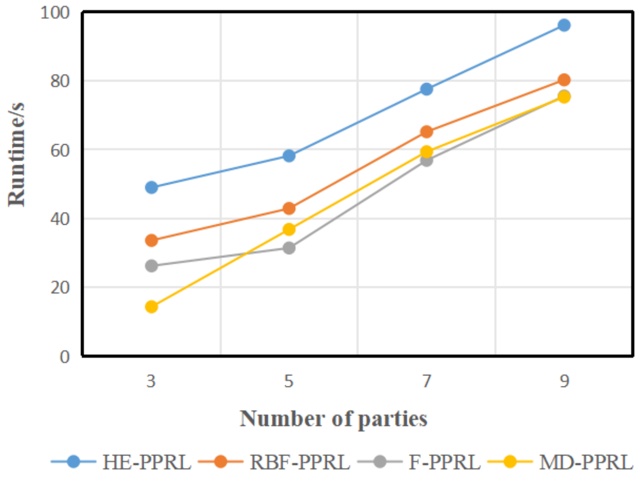

Figure 3. Runtime versus number of participants.

5.2.2. Method Performance Testing

The performance evaluation of each PPRL method encompasses three key aspects: Precision, Recall, and F-Measure. We set the size of the data source to B = 5 k and examined how the Precision, Recall, and F-Measure of each method evolved with the number of participants (3, 5, 7, and 9, respectively). The test outcomes are illustrated in the Figures 4–6 below.

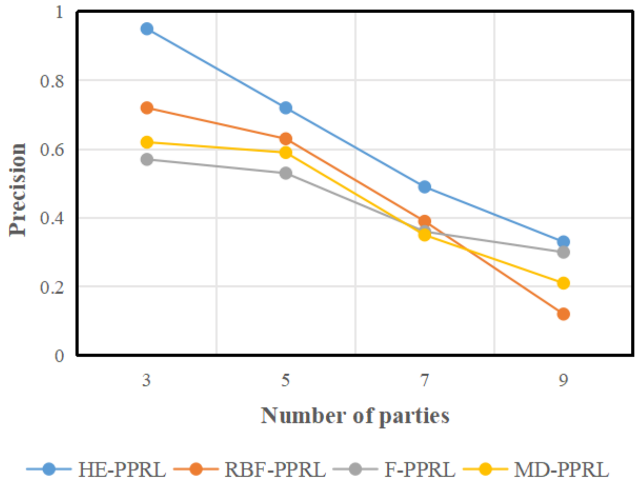

Figure 4. Precision versus number of participants.

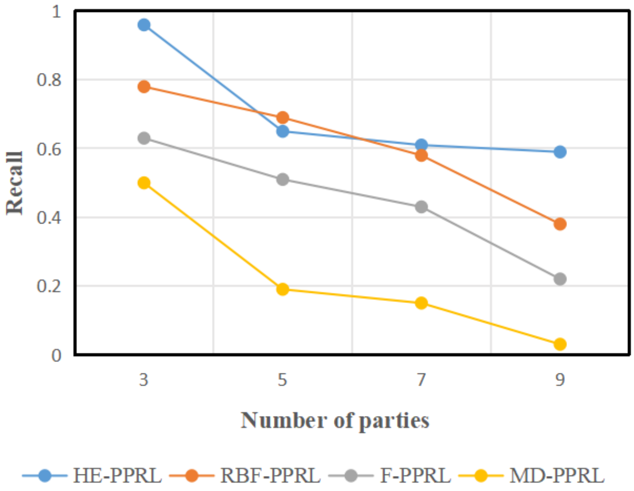

Figure 5. Recall versus number of participants.

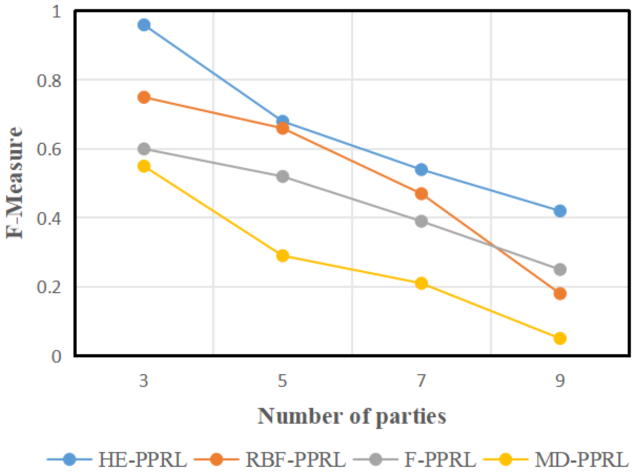

Figure 6. Recall versus number of participants.

5.2.3. Security Testing

The security assessment of each PPRL method involves quantifying the risk of data privacy leakage. With a fixed data source size of B = 5 k and a set number of participants p = 5, the security test results for each method are presented in the following Figure 7.

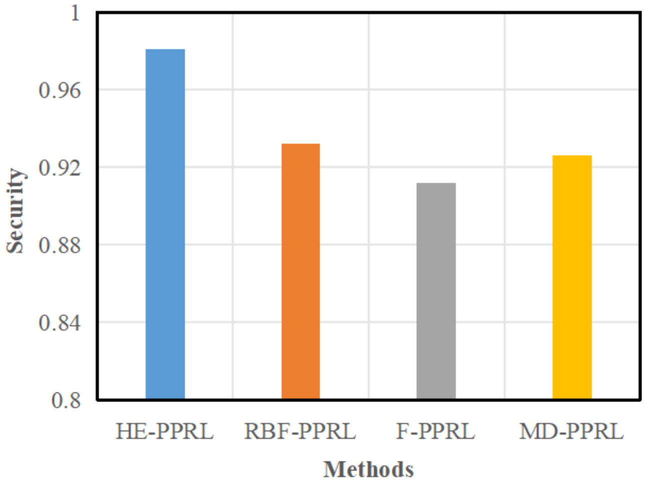

Figure 7. Security of each method.

5.3. Experimental Results and Analysis

Drawing on the comprehensive test data for each PPRL method, we extract the critical index data for each method under the specific conditions of a data source size of $B = 5$ k and a participant count of $p = 5$. As depicted in the following Table 9, to conduct a comprehensive evaluation of these methods, we consider three fundamental metrics: runtime, linkage quality (with the F-Measure serving as a reference metric for linkage quality), and security. This comprehensive evaluation aims to provide a more accurate understanding of the performance characteristics of each method, thereby laying a solid foundation for subsequent optimization and selection.

Table 9. Indicator data of each method.

Indicators / Methods	Runtime(/S)	Linkage Quality	Security
HE-PPRL	58.2	0.68	0.981
RBF-PPRL	42.9	0.66	0.932
F-PPRL	31.4	0.52	0.912
MD-PPRL	36.8	0.29	0.926

Based on the correlation analysis of the data, runtime is categorized as a negative indicator, while linkage quality and security are considered positive indicators. It is worth noting that there is a certain linear relationship between runtime and security. Considering these data characteristics, we standardize them to enhance analysis and application. Table 10 displays the data after normalization.

Table 10. Standardized indicator data.

Indicators / Methods	Runtime	Linkage Quality	Security
HE-PPRL	0	1	1
RBF-PPRL	0.570895522	0.948717949	0.28985507
F-PPRL	1	0.58974359	0
MD-PPRL	0.798507463	0	0.20289855

As illustrated in Figure 8, the safety index exhibits a higher degree of data dispersion, indicating a more significant variation in its values. This substantial variation highlights the importance of the safety index in the overall evaluation, justifying the allocation of a correspondingly higher weight to accurately reflect its impact on the overall results.

The following Table 11 displays the coefficient of variation calculated for each index based on its degree of variation, which will serve as a crucial reference for weight allocation and aid in more accurately measuring the relative importance of each index in the overall evaluation. This ensures the accuracy and reliability of the data analysis and processing results.

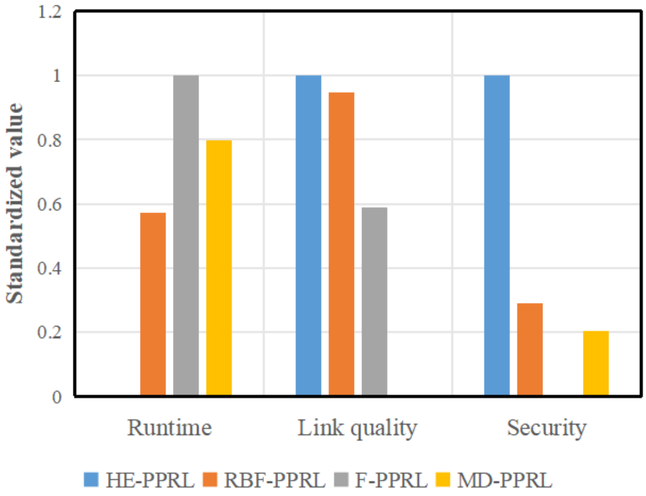

Figure 8. The standardized index data of each method.

Table 11. Coefficient of variation of each indicator.

Indicators	Runtime	Linkage Quality	Security
Standard deviation	0.4320564158	0.4607662106	0.4351648886
Coefficient of variation	0.729392878267	0.726055846831	1.16607290774

Spearman correlation coefficient and Pearson correlation coefficient were used based on the correlation between each index, and the correlation coefficient between them was calculated, respectively. The calculation results are shown in Table 12 below.

Table 12. Correlation coefficient between indicators.

Indicators	Runtime	Linkage Quality	Security
Correlation coefficient	−0.8	−0.987046135	0.8

Based on the data presented in Table 12 above, the conflictivity between the indicators can be determined, and the corresponding calculations are summarized in Table 13 below.

Table 13. The contrast intensity of each index.

Indicators	Runtime	Linkage Quality	Security
Conflict	3.787046135	2	2.187046135

To balance the discrepancies and contradictions between different indicators, it may be advisable to assign greater weight to those indicators that exhibit higher conflict and coefficient of variation. This approach ensures a more comprehensive consideration of all aspects of the decision-making or evaluation process, thereby enhancing the accuracy and reliability of the outcomes. Table 14 below presents the index weight assignments obtained in this experiment for the four PPRL methods (the outcome is retained precisely to six decimal positions), and Figure 9 provides a visual representation of the weight ratio for each indicator.

Table 14. Weight allocation of each indicator.

Indicators	Runtime	Linkage Quality	Security
Weight	0.408337	0.214663	0.377000

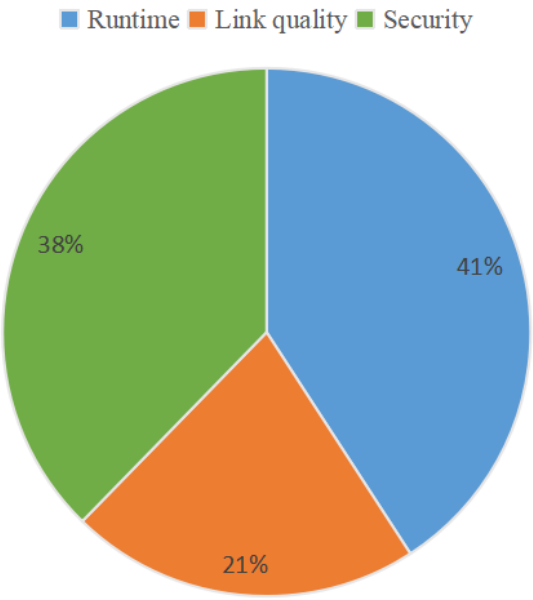

Figure 9. Each index weight distribution proportion chart.

According to the experimental results in the above Table 15, the PPRL method based on homomorphic encryption (HE-PPRL) demonstrates superior performance in this experiment. This indicates that under the data set chosen in this paper, especially under the specific conditions of data source size B = 5 k and the number of participants p = 5, the comprehensive performance of the HE-PPRL method holds a significant advantage over the other three methods, thereby further confirming the superiority and effectiveness of the HE-PPRL method in such scenarios. It is also essential to recognize that the other three methods did not demonstrate an advantage in this experiment, but this does not imply that they are inferior to the HE-PPRL method in other scenarios or conditions. Consequently, when assessing various methods, it is crucial to consider multiple factors comprehensively to avoid reaching one-sided conclusions.

Table 15. Final score for each method.

Methods	HE-PPRL	RBF-PPRL	F-PPRL	MD-PPRL
Evaluation scores	0.591663	0.546048	0.534934	0.402553

The evaluation method adopted in this paper, building on the research achievements of Dinusha Vatsalan's team, delves into the deep mining and utilization of data characteristics, achieving the quantification of index weighting. This has led to significant advancements in exploring and comparing the comprehensive performance of PPRL methods. Given the diversity of data sources, the level of interference factors, and the impact of environmental conditions, which may all lead to variations in experimental outcomes and profoundly affect the final assessment, we have meticulously maintained a uniform experimental environment throughout the testing phase. This has been done to eliminate potential influences of various environmental factors on our results, ensuring their fairness and credibility. This method not only provides strong support for the optimization of PPRL methods but also offers a scientific basis for decision-making. After extensive experimental repetitions and in-depth analysis, the consistency between the experimental results and the PPRL methods chosen in actual decision-making approaches 80%, indicating that the method proposed in this paper holds tremendous practical value and significance in the field.

In order to further verify the effectiveness and advancement of the improved CRITIC method, we compare and analyze it with the existing evaluation methods. For example, Ma Huimin and Li Qiang (2006) used AHP analytic hierarchy process to assess the risk of ERP projects [43]. Our quantitative analysis reveals that AHP, when dealing with complex decision-making problems, exhibited a high degree of variability due to subjective judgment, with a consistency ratio (CR) exceeding the acceptable threshold of 0.1 in 60% of the cases studied.In repeated experiments, the consistency of results obtained through AHP reached only 70%, whereas our proposed method achieved a consistency rate of 95%. At the same time, we also use the fuzzy analytic Hierarchy Process model based on fuzzy logic proposed by Zhang Jijun [44]. Our results indicate that the improved CRITIC method achieves a mean accuracy of 85% in identifying performance differences between PPRL methods, compared to the 70% accuracy rate of the fuzzy AHP model. Additionally, the improved CRITIC method has a lower standard deviation in the evaluation outcomes, suggesting greater stability. Table 16 shows the comparative analysis between the proposed method and AHP method.

Table 16. Comparison of evaluation methods.

Indicators	Result Consistency	Accuracy	Adoption Rate
Improved CRITIC	0.95	0.85	0.80
AHP	0.70	0.70	0.85

6. Conclusions

This paper innovatively proposes a comprehensive evaluation framework based on an improved CRITIC method, aimed at thoroughly and deeply assessing the performance of PPRL techniques. The framework meticulously constructs a multi-dimensional evaluation system, enabling the scientific and systematic identification of the optimal PPRL technique. Experimental results demonstrate that the framework exhibits extremely high accuracy and objectivity in evaluating the merits and demerits of PPRL techniques, and the evaluation results are highly consistent. This not only robustly validates the scientificity and effectiveness of the evaluation framework but also fully showcases its immense practical value and profound societal significance in the field of PPRL technique evaluation. While our research method can identify optimal PPRL methods, theoretical best choices may not align with practical ones due to factors like implementation costs, operational complexity, and application requirements. Our evaluation results, which reveal the theoretical advantages of a PPRL approach, should only serve as a basis for decision-makers to make comprehensive and balanced decisions considering practical constraints and specific needs. Based on this, integrating two or more evaluation methods has become the latest trend in comprehensive evaluation. Not only overcomes the limitations of a single evaluation method but also brings out the synergistic advantages of multiple methods, making the evaluation process more scientific, objective, and accurate. Looking to the future, our research will continue to refine the comprehensive evaluation system of PPRL technologies for different audiences and diverse scenarios within the framework of integrating subjective and objective methods, and strive to find more suitable PPRL solutions.

Author Contributions: Conceptualization, S.H. and Y.L.; methodology, S.H. and Y.L.; software, S.H. and Y.L.; validation, S.H. and Y.L.; formal analysis, S.H., C.W. and D.S.; investigation, S.H., D.S. and C.W.; resources, S.H. and Y.L.; data curation, S.H. and Y.L.; writing—original draft preparation, S.H. and Y.L.; writing–review and editing, S.H. and Y.L.;visualization, S.H., Y.L. and D.S.; supervision, S.H. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the National Natural Science Foundation of China (62172082) and the Education Department of Liaoning Province, Youth Project (LJKQZ20222440).

Data Availability Statement: The datasets and codes used and/or analyzed during the current study are available from the corresponding author (Shumin Han; Email: hanshumin_summer@yeah.net) upon reasonable.

Acknowledgments: The authors would like to thank the National Natural Science Foundation of China (62172082) and the Education Department of Liaoning Province, Youth Project (LJKQZ20222440). All persons and institutes who kindly made their data available for this research are acknowledged.

Conflicts of Interest: The authors declare no competing interests.

References

1. Li, T.; Chen, L.; Jensen, C.S.; Pedersen, T. TRACE: Real-time Compression of Streaming Trajectories in Road Networks. *Proc. VLDB Endow.* **2021**, *14*, 1175–1187. [CrossRef]
2. Li, T.; Huang, R.; Chen, L.; Jensen, C.S.; Pedersen, T. Compression of uncertain trajectories in road networks. *Proc. VLDB Endow.* **2020**, *13*, 1050–1063. [CrossRef]
3. Yao, S. Research on Privacy Record Linkage Technology for Data Integration. Master's Thesis, Hangzhou Dianzi University, Hangzhou, China, 2023.
4. Gu, M. Research on a Multi-Party Verifiable Privacy-Preserving Record Linkage Mechanism Based on Blockchain. Master's Thesis, Zhejiang Gongshang University, Hangzhou, China, 2019.
5. Li, T.; Gu, Y.; Zhou, X.; Ma, Q.; Yu, G. An Effective and Efficient Truth Discovery Framework over Data Streams. In Proceedings of the International Conference on Extending Database Technology, Venice, Italy, 21–24 March 2017.
6. Wu, J.; Li, T.; Chen, L.; Gao, Y.; Wei, Z. SEA: A Scalable Entity Alignment System. In Proceedings of the 46th International ACM SIGIR Conference on Research and Development in Information Retrieval, Taipei, Taiwan 23–27 July 2023; SIGIR '23; pp. 3175–3179. [CrossRef]
7. Wang, J.; Li, T.; Wang, A.; Liu, X.; Chen, L.; Chen, J.; Liu, J.; Wu, J.; Li, F.; Gao, Y. Real-time Workload Pattern Analysis for Large-scale Cloud Databases. *arXiv* **2023**, arXiv:2307.02626. [CrossRef]
8. Zhang, S. Research on Multi-Level Sensitivity Model and Privacy Protection Method in the Publication of Interval-Valued Data. Ph.D. Thesis, Guangxi Normal University, Guilin, China, 2016.
9. Liu, Y.; Dai, H.; Zhou, Q.; Li, P.; Yi, X.; Yang, G. EPSMR: An efficient privacy-preserving semantic-aware multi-keyword ranked search scheme in cloud. *Future Gener. Comput. Syst.* **2024**, *159*, 1–14. [CrossRef]
10. Dong, D.; Shen, D.; Han, S.; Nie, T.; Kou, Y.; Yu, G. Multi-Party Strong-Privacy-Preserving Record Linkage Method. *J. Front. Comput. Sci. Technol.* **2019**, *13*, 394–407.
11. Han, S.; Shen, D.; Nie, T.; Kou, Y.; Yu, G. A method for multi-party record linkage under privacy protection. *J. Softw.* **2017**, *28*, 2281–2292. [CrossRef]
12. Kelty, E.; Hansen, M.; Randall, S.; Gration, D.; Baynam, G.; Preen, D.B. Use of privacy-preserving record linkage to examine the dispensing of pharmaceutical benefits scheme medicines to pregnant women in Western Australia. *Pharmacoepidemiol. Drug Saf.* **2024**, *33*, e5845. [CrossRef]
13. Tanveer, M.; Chelloug, S.A.; Alabdulhafith, M.; El-Latif, A.A.A. Lightweight authentication protocol for connected medical IoT through privacy-preserving access. *Egypt. Inform. J.* **2024**, *26*, 100474. [CrossRef]
14. Thilina, R.; Dinusha, V.; Sean, R.; Peter, C. Evaluation of advanced techniques for multi-party privacy-preserving record linkage on real-world health databases. *Int. J. Popul. Data Sci.* **2017**, *1*. [CrossRef]
15. Silva, A.; Bellala, G. Privacy-Preserving Multi-Party Clustering: An Empirical Study. In Proceedings of the 2017 IEEE 10th International Conference on Cloud Computing (CLOUD), Honolulu, HI, USA, 25–30 June 2017; IEEE: New York, NY, USA, 2017.
16. Li, T.; Chen, L.; Jensen, C.S.; Pedersen, T.B.; Gao, Y.; Hu, J. Evolutionary Clustering of Moving Objects. In Proceedings of the 2022 IEEE 38th International Conference on Data Engineering (ICDE), Virtual, 9–12 May 2022; pp. 2399–2411. [CrossRef]
17. Vatsalan, D.; Christen, P.; O'Keefe, C.M.; Verykios, V.S. An Evaluation Framework for Privacy-Preserving Record Linkage. *J. Priv. Confidentiality* **2014**, *6*. [CrossRef]
18. Nie, Y.; Ma, X.; Xiao, X. Research on the development evaluation of China's digital supply chain: Based on the CRITIC-G1 method and Bonferroni operator. *Logist. Res.* **2024**, 15–28.
19. Wu, L.; Zhao, G. Weighting method and comparison of academic journal evaluation indicators based on structural CRITIC method. *Stat. Decis.* **2024**, *40*, 56–62. [CrossRef]
20. Zhan, Q.; Zhou, W.; Li, W.; Zhang, X.; Qin, X. Comprehensive Evaluation of Intelligent Obstacle Avoidance Function by Changing Lanes of Vehicle Based on an Improved Evaluation Index System. In Proceedings of the International Conference on Wireless Communications and Applications, Kuala Lumpur, Malaysia, 2–3 January 2022.
21. Yuan, X.; Zhang, P.; Li, N.; Li, Y.; Hou, Y.; Xiong, S. Comprehensive quality evaluation method of smart meters based on AHP-Critic. *J. Phys. Conf. Ser.* **2021**, *1920*, 012010. [CrossRef]

22. Guo, L.; Wang, S.; Chen, H.; Yang, A.; Liang, B. Comprehensive evaluation method of micro-energy harvesters for power supply of outdoor wireless sensors. *IOP Conf. Ser. Earth Environ. Sci.* **2021**, *645*, 012017. [CrossRef]
23. Xiao, C.; Ye, J.; Esteves, R.M.; Rong, C. Using Spearman's correlation coefficients for exploratory data analysis on big dataset. *Concurr. Comput. Pract. Exp.* **2016**, *28*, 3866–3878. [CrossRef]
24. Alsaqr, A.M. Remarks on the use of Pearson's and Spearman's correlation coefficients in assessing relationships in ophthalmic data. *Afr. Vis. Eye Health* **2021**, *80*, 10. [CrossRef]
25. Hauke, J.; Kossowski, T. Comparison of Values of Pearson's and Spearman's Correlation Coefficients on the Same Sets of Data. *Quaest. Geogr.* **2011**, *30*, 87–93. [CrossRef]
26. Rebeki, A.; Lonari, Z.; Petrovi, S.; Mari, S. Pearson'S or Spearman's Correlation Coefficient—Which one to use? *Poljoprivreda* **2015**, *21*, 47–54. [CrossRef]
27. Yao, Y.; Li, D.; Jie, H.; Jie, H.; Li, T.; Chen, J.; Wang, J.; Li, F.; Gao, Y. SimpleTS: An Efficient and Universal Model Selection Framework for Time Series Forecasting. *Proc. VLDB Endow.* **2023**, *16*, 3741–3753. [CrossRef]
28. Zhong, X.; Zhong, H. Multi-index comprehensive evaluation method and its application. *J. Inn. Mong. Univ. (Humanit. Soc. Sci. Ed.)* **2004**, 107–111. [CrossRef]
29. Wang, H.; Chen, L.; Chen, K.; Xue, M.; Liang, Q. Multi-index comprehensive evaluation method and the selection of weight coefficients. *J. Guangdong Pharm. Univ.* **2007**, 583–589. [CrossRef]
30. Zhao, H.; Boliqao, A.; Huang, X. Research on the Indicator Weight of Multi-level and Multi-index Performance Evaluation System. *J. Inn. Mong. Univ. (Humanit. Soc. Sci. Ed.)* **2006**.
31. Song, Y.; Gu, Y.; Li, T.; Qi, J.; Liu, Z.; Jensen, C.S.; Yu, G. CHGNN: A Semi-Supervised Contrastive Hypergraph Learning Network. *IEEE Trans. Knowl. Data Eng.* **2024**, *36*, 4515–4530. [CrossRef]
32. Li, Yu-Shuai; Li, Tian-Yi; Zhou, Jian-Guo; Huang, Bo-Nan Double-Consensus Based Distributed Optimal Energy Management for Multiple Energy Hubs. *Appl. Sci.* **2018**, *8*, 1412.
33. Nanayakkara, C.; Christen, P.; Ranbaduge, T.; Garrett, E. Evaluation measure for group-based record linkage. *Int. J. Popul. Data Sci.* **2019**, *4*, 1127. [CrossRef]
34. Mohammadi, S.; Balador, A.; Sinaei, S.; Flammini, F. Balancing privacy and performance in federated learning: A systematic literature review on methods and metrics. *J. Parallel Distrib. Comput.* **2024**, *192*, 104918. [CrossRef]
35. Hu, D.; Chen, L.; Fang, H.; Fang, Z.; Li, T.; Gao, Y. Spatio-Temporal Trajectory Similarity Measures: A Comprehensive Survey and Quantitative Study. *IEEE Trans. Knowl. Data Eng.* **2024**, *36*, 2191–2212. [CrossRef]
36. Durham, E.; Xue, Y.; Kantarcioglu, M.; Malin, B. Quantifying the correctness, computational complexity, and security of privacy-preserving string comparators for record linkage. *Inf. Fusion* **2012**, *13*, 245–259. [CrossRef]
37. Hu, H.; Zhang, J.; Chen, C.; Lu, G.; Zhang, G.; Lin, H.; Chen, X. Slope stability evaluation and prediction model based on an improved CRITIC-weighted machine learning algorithm. *Highw. Eng.* **2023**, *48*, 74–83. [CrossRef]
38. Yang, C.; Bing, H.U. Supportability Grey Comprehensive Evaluation of Radar Equipment Based on Improved AHM-CRITIC. *Telecommun. Eng.* **2019**, *59*, 229–236.
39. Wang, J.H.; Huang, Q.; Jao, D. Privacy-Preserving Data Aggregation Using Homomorphic Encryption. U.S. Patent No. 7,856,100, 21 December 2010.
40. Ashley, D.E.; Murat, K.; Yuan, X.; Csaba, T.; Mehmet, K.; Bradley, M. Composite Bloom Filters for Secure Record Linkage. *IEEE Trans. Knowl. Data Eng.* **2014**, *26*, 2956–2968.
41. Dimitrios, K.; Aris, G.D.; Verykios, V.S. FEDERAL: A Framework for Distance-Aware Privacy-Preserving Record Linkage. *IEEE Trans. Knowl. Data Eng.* **2018**, *30*, 292–304.
42. Vatsalan, D.; Christen, P. Scalable Privacy-Preserving Record Linkage for Multiple Databases. In Proceedings of the CIKM'14: 2014 ACM Conference on Information and Knowledge Management, Shanghai, China, 3–7 November 2014.
43. Ma, H.; Li, Q. Applying AHP to assess ERP project risk. *Comput. Digit. Eng.* **2006**, *34*, 4.
44. Zhang, J. Fuzzy Analytic Hierarchy Process (FAHP). In *Fuzzy Systems and Mathematics*; CRC Press: Boca Raton, FL, USA, 2000.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.