Journal of Contemporary Educational Research, 2025, Volume 9, Issue 4
http://ojs.bbwpublisher.com/index.php/JCER
ISSN Online: 2208-8474
ISSN Print: 2208-8466

# Research on Classification and Desensitization Strategies of Sensitive Educational Data

**Chen Chen[1], Caixia Liu[1,2]***

[1]School of Smart Education, Jiangsu Normal University, Xuzhou 221116, Jiangsu, China
[2]Jiangsu Education Informatization Engineering Technology Research Center, Xuzhou 221116, Jiangsu, China

**Author to whom correspondence should be addressed.*

**Copyright:** © 2025 Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), permitting distribution and reproduction in any medium, provided the original work is cited.

**Abstract:** In the era of digital intelligence, data is a key element in promoting social and economic development. Educational data, as a vital component of data, not only supports teaching and learning but also contains much sensitive information. How to effectively categorize and protect sensitive data has become an urgent issue in educational data security. This paper systematically researches and constructs a multi-dimensional classification framework for sensitive educational data, and discusses its security protection strategy from the aspects of identification and desensitization, aiming to provide new ideas for the security management of sensitive educational data and to help the construction of an educational data security ecosystem in the era of digital intelligence.

**Keywords:** Data security; Sensitive data; Data classification; Data desensitization

**Online publication:** April 28, 2025

## 1. Introduction

With the rapid advancement of information technology and the realization of the significant data era, data has become a driving force behind socio-economic and educational innovation. Technologies like big data, cloud computing, and artificial intelligence have accelerated the digital transformation of education, generating vast amounts of sensitive data. This data covers many areas, such as students' personal information, academic research, etc. Due to its multi-source, heterogeneous, and dynamic nature, classifying and desensitizing sensitive information is challenging. The 2024 National Conference on the Digitization of Education emphasized that safety is essential for digital education, stressing the need to secure content, data, AI algorithms, and ethical standards [1]. This underscores the critical importance and urgency of securing educational data.

The secure management of sensitive educational data is complex. Firstly, its sensitive nature makes categorization and identification difficult. Secondly, dynamic and complex data requires flexible management strategies. Additionally, the multi-source, heterogeneous nature of the data poses challenges in integration and sharing. Ensuring data security while enabling data sharing and utilization is also a key issue. Existing research

mainly focuses on fields like healthcare, industry, and finance, with less attention given to classification and desensitization strategies in education. Therefore, developing desensitization strategies based on data sensitivity and usage scenarios while balancing security and usability is an urgent problem.

To address the challenges outlined above, this paper develops a multi-dimensional classification framework for sensitive educational data and explores desensitization strategies suited to educational contexts. The goal is to provide theoretical and technical support for secure educational data management, balancing security and usability, reducing the risk of data leakage, and offering insights for future management and application of educational data.

## 2. Classification of sensitive educational data

Sensitive educational data refers to information that, if disclosed or misused, could harm students, schools, and educational institutions [2]. This data is large in volume and complex, with classification being the first step in desensitization. The Data Security Law [3], enacted in China in 2016, provides guidelines for the categorization, management, and protection of educational data. Based on this, a classification framework for sensitive educational data has been developed, covering the following dimensions.

### 2.1. Data sources and uses

Sensitive educational data encompasses information related to students, teachers, and administrators. It is derived from various sources and serves a wide range of purposes. Sensitive educational data comes from various sources and serves multiple purposes, including data generated in teaching, information gathered in educational management, research data, and data from campus life [4].

### 2.2. Data structure

Sensitive educational data can be classified into structured, semi-structured, and unstructured data. Structured data includes personal information, test scores, etc., which are organized in tables with clear formats and rules. Semi-structured data includes class notes, lesson plans, etc. While lacking a strict tabular structure, they provide rich data expression. Unstructured data consists of images, audio, video, and other media used in teaching and learning. These data do not follow a fixed format or clear structure and are typically stored in raw form.

### 2.3. Data association

Sensitive data can be classified into high and low correlation based on their internal relationships. High-correlation data are closely linked and often tied to core educational activities, so the leakage of one piece may expose others. Low-correlation data are more loosely connected and have less impact on core activities. For example, learning attitudes, behaviors, and teaching methods are highly correlated with academic performance, while family background and teaching resources are less so.

### 2.4. Data sensitivity

Data can be categorized as sensitive, more sensitive, or less sensitive based on their level of sensitivity. Personal information, psychological records, etc., are sensitive data, and their leakage can severely impact privacy and safety. Academic results, teaching evaluations, etc., are more sensitive data, and their leakage can negatively affect individuals, schools, and institutions, disrupting teaching and learning. Teaching resources, learning activity records, etc., are less sensitive, typically causing minimal impact if leaked.

## 3. Identification of sensitive educational data

The identification of sensitive educational data refers to the process of detecting sensitive information that may pose security risks from the categorized educational data using specific techniques and methods. Structured sensitive data is usually identified through rule-based and dictionary-based methods, while unstructured sensitive data is typically identified using machine learning and deep learning techniques.

### 3.1. Rule-based and dictionary-based identification

Rule-based identification involves detecting specific sensitive data based on predefined rules. Texts that match patterns, such as student and ID numbers, can be identified using regular expressions in a rule set. This method can be adjusted to meet specific needs, but it requires expert knowledge to set the rules. Dictionary-based identification uses a sensitive word dictionary to match data items containing sensitive information. By comparing content with dictionary entries, this method is efficient and cost-effective, requiring no complex calculations. However, an incomplete or incorrect dictionary can result in missing sensitive data [5].

### 3.2. Machine learning methods

Machine learning methods involve using algorithms to train models for identifying sensitive data. Traditional methods often struggle with the complexity and diversity of unstructured data, while machine learning techniques, such as natural language processing and image recognition, can effectively identify various types of unstructured data and extract sensitive information [6]. Algorithms like text similarity, Word2Vec, and K-Means clustering have improved recognition accuracy. However, these methods typically require large amounts of annotated data and have limited ability to recognize new sensitive words [7].

### 3.3. Deep learning methods

Deep learning methods use deep neural networks to recognize and classify sensitive data. Models like convolutional neural networks, generative adversarial networks, recurrent neural networks, and long short-term memory networks are key in sensitive data identification. These methods have strong learning abilities, good adaptability, and powerful automatic feature extraction, allowing them to learn complex patterns from large datasets. Deep learning excels in tasks like entity and image recognition, eliminating the need for manual feature design. However, they require large amounts of data for training, which increases computational costs.

## 4. Desensitization of sensitive educational data

Data desensitization (**Figure 1**) is the process of transforming sensitive information with specific rules while maintaining its essential characteristics. This aims to remove sensitive content, prevent unauthorized access, and allow relevant data processing [8].

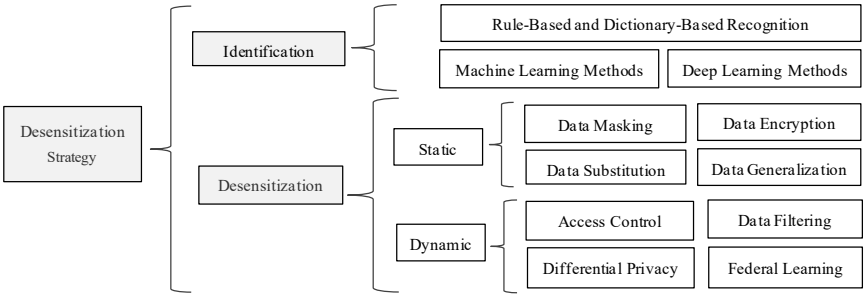


**Figure 1.** Desensitization strategy

## 4.1. Static desensitization

Static desensitization involves processing sensitive data before storage or use while preserving the original data's characteristics and structure. It is typically used in non-production environments, such as development, testing, and analysis. It mainly includes the following techniques.

### 4.1.1. Data masking

Data masking is the process of obscuring sensitive data by replacing some or all of its content with specific characters. For example, a student's home contact number "13912345678" may be replaced with "139****5678." Data masking allows the data to remain identifiable and usable for subsequent storage and processing without changing its format.

### 4.1.2. Data encryption

Sensitive data is encrypted using encryption algorithms, with the original data recoverable only through a specific key. For example, student files can be stored and transmitted using encryption algorithms like AES and RSA. The original data can only be decrypted and restored with the correct key. Data encryption ensures that only authorized users can decrypt and access the data, ensuring both data integrity and privacy.

### 4.1.3. Data substitution

Data substitution involves replacing original sensitive data with fictitious but plausible data that preserves the statistical properties. For example, a student's real name may be replaced with a randomly generated name or code (S001, S002, e.g.). This ensures data availability while protecting personal information during statistical analysis.

### 4.1.4. Data generalization

Data generalization is a technique that hides sensitive information by transforming specific data into more abstract and generalized forms. For example, a student's specific test scores may be generalized into achievement levels (excellent, good, etc.). The data generalization technique hides specific data and provides only general information, reducing the risk of privacy exposure to some extent.

## 4.2. Dynamic desensitization

Dynamic desensitization involves real-time masking of sensitive data during access, with the desensitized results returned immediately. It can be applied directly in production environments, ensuring system operation and data availability. The details are as follows.

### 4.2.1. Access control

Access control technology dynamically regulates access to sensitive data based on user permissions, ensuring that only authorized users can view specific data. Techniques include RBAC, ABAC, and DAC. For example, a teacher, based on their privileges, logs into their account to access the learning data of students in their class and receives real-time feedback to adjust their teaching approach.

### 4.2.2. Data filtering

Data filtering involves real-time filtering or desensitization of sensitive data through SQL rewriting or middleware techniques before returning query results. For example, to filter students' gender data, the query

could be rewritten as "SELECT * FROM students WHERE gender = 'male';." This technology allows efficient data queries to filter sensitive information, protecting privacy while helping educators perform their tasks more effectively.

#### 4.2.3. Differential privacy

Differential privacy is a privacy protection method that allows statistical analysis of data while preserving individual privacy by adding noise or perturbations before data release [9]. For example, schools or organizations can introduce noise to raw grades before publishing them, thus protecting student privacy. This technique can provide privacy protection and ensure data availability at the time of data collection, release, and analysis.

#### 4.2.4. Federated learning

Federated learning is a privacy-preserving distributed machine learning framework that keeps user data local and uses intermediate parameters for co-optimization between client and server, ensuring both privacy and model performance [10]. For example, schools with their student data can collaborate in model training via federated learning without sharing the data, enhancing education prediction and analysis. This approach reduces the risk of raw data leakage during transmission, protecting data owners' privacy.

## 5. Conclusion

This paper systematically analyzes the characteristics of sensitive educational data and proposes a multi-dimensional classification framework. Based on this framework, identification and desensitization of sensitive educational data are discussed in detail. The study primarily focuses on the application of static and dynamic desensitization techniques in the field of education. The purpose of this study is to provide new insights and methods to address the security challenges faced by educational data, reduce the risk of data leakage, and maximize data availability. Additionally, it is hoped that this study will offer valuable insights for enhancing the security and privacy protection of educational data.

## Funding

Education Science planning project of Jiangsu Province in 2024 (Grant No: B-b/2024/01/152); 2025 Jiangsu Normal University Graduate Research and Innovation Program school-level project "Research on the Construction and Desensitization Strategies of Education Sensitive Data Classification from the Perspective of Educational Ecology"

## Disclosure statement

The authors declare no conflict of interest.

## References

[1] Ministry of Education of the People's Republic of China, 2024, Ministry of Education Convenes 2024 National Digitization of Education Work Summary Conference, viewed January 20, 2025, http://www.moe.gov.cn/jyb_xwfb/gzdt_gzdt/moe_1485/202412/t20241227_1171791.html

[2] Lu C, 2021, Research on Data Desensitization Technology for Internet of Things, Master's thesis, Nanjing University of Posts and Telecommunications. https://doi.org/10.27251/d.cnki.gnjdc.2021.000420

[3] The Central People's Government of the People's Republic of China, 2021, Data Security Law of the People's Republic of China, viewed December 24, 2024, https://www.gov.cn/xinwen/2021-06/11/content_5616919.htm

[4] Yang X, Tang S, Li J, 2016, The Definition, Potential Value and Challenges of Big Data in Education. Modern Distance Education Research, 1: 50–61.

[5] Wu J, Su Y, Jiang Z, et al., 2022, Analysis of Sensitive Data Storage Security Technology in Power Monitoring Systems. Electronic Technology and Software Engineering, (05): 188–191. https://doi.org/10.20109/j.cnki.etse.2022.05.045

[6] Yuan M, Xu X, Zhang Y, 2023, Research on AI-Based Method for Data Masking of Unstructured Operational Data. Cybersecurity and Data Governance, 42(S1): 184–190.

[7] An M, 2022, Research and Implementation of a Sensitive Content Recognition Mechanism for Big Data Security, Master's thesis, Beijing Jiaotong University.

[8] Shen C, Xu Y, 2023, Research and Prospect of Data Masking Technology. Information Security and Communications Confidentiality, (02): 105–116.

[9] Cai B, 2024, Research on Multi-Dimensional Data De-Identification Method Based on Differential Privacy. Information Recording Materials, 25(05): 160–162.

[10] McMahan B, Moore E, Ramage D, et al., 2017, Communication-Efficient Learning of Deep Networks from Decentralized Data, Proceedings of the 20th International Conference on Artificial Intelligence and Statistics, PMLR 54: 1273–1282.

**Publisher's note**

Bio-Byword Scientific Publishing remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.