STM JOURNALS

International Journal of
Computer Science Languages

ISSN: 3048-944X
Volume 3, Issue 1, 2025
January–June
DOI (Journal): 10.37591/IJCSL

https://journals.stmjournals.com/ijcsl

Review IJCSL

# Differential Privacy-Aware Data Sanitization for Multi-Level Security

Manas Kumar Yogi*

***Abstract***

*Multi-level security (MLS) models are fundamental for enforcing mandatory access control in high-security environments such as government, military, healthcare, and finance. However, traditional MLS frameworks, including the Bell-LaPadula and Biba models, often create rigid data silos, preventing efficient data utilization. Differential privacy (DP) presents a novel solution by enabling controlled information leakage while preserving confidentiality. By injecting statistical noise into query results, DP allows lower-clearance users to access sanitized versions of higher-classified data without violating security policies. This paper explores advancements in privacy-preserving MLS, emphasizing hybrid models that integrate DP with homomorphic encryption for enhanced security. Additionally, machine learning–driven adaptive noise mechanisms are discussed as a means to dynamically adjust privacy protections based on query sensitivity and user behavior. These innovations not only strengthen data security but also improve operational efficiency in multi-tiered access systems. We examine policy implications, advocating for DP-aware MLS frameworks in national security and intelligence-sharing contexts. Ethical concerns such as privacy-utility trade-offs, bias in DP mechanisms, and adversarial risks are also addressed. By balancing security and controlled data access, DP-enhanced MLS models offer a future-ready approach to secure data-sharing architectures, fostering both confidentiality and collaboration.*

**Keywords:** Security, Bell-LaPadula model, differential privacy, encryption, malware

## INTRODUCTION

### Understanding Multi-Level Security

Multi-level security (MLS) is a security framework used in computer systems and networks to enforce mandatory access control (MAC) based on hierarchical classification levels. It ensures that users can only access data for which they have the appropriate security clearance. MLS is widely used in military, government, and critical infrastructure systems where strict information compartmentalization is essential [1].

***Author for Correspondence**
Manas Kumar Yogi
E-mail: manas.yogi@gmail.com

[1]Assistant Professor, Department of Computer Science and Engineering, Pragati Engineering College (A), Surampalem, Andhra Pradesh, India

Received Date: February 26, 2025
Accepted Date: February 28, 2025
Published Date: March 10, 2025

**Citation:** Manas Kumar Yogi. Differential Privacy-Aware Data Sanitization for Multi-Level Security. International Journal of Computer Science Languages. 2025; 3(1): 42–52p.

### Key Multi-Level Security Principles: Bell-LaPadula and Biba Models

Two foundational models define the principles of MLS enforcement: the Bell-LaPadula model, which focuses on data confidentiality, and the Biba model, which emphasizes data integrity.

#### *Bell-LaPadula (BLP) Model (Focus: Confidentiality)*

- *The simple security property (no read up – NRU):* A subject at a lower security level cannot read data at a higher level (e.g., a "Secret"-cleared user cannot access "Top Secret" data).

 

- *The star () property (no write down – NWD):* A subject at a higher security level cannot write to a lower level to prevent information leaks (e.g., a "Top Secret"-cleared user cannot write to a "Secret" document).
- This model is used in environments where preventing unauthorized data disclosure is the primary goal.

***Biba Model (Focus: Integrity)***

- *The simple integrity property (no read down – NRD):* A subject at a higher integrity level cannot read data from a lower level to prevent contamination (e.g., a trusted administrator cannot read unverified user input) [2].
- *The star () integrity property (no write up – NWU):* A subject at a lower integrity level cannot write to a higher level to avoid corrupting critical data (e.g., a standard user cannot modify a kernel file).
- The Biba model ensures data integrity by preventing untrusted modifications.

**Challenges in Balancing Data Access and Security in Multi-Level Security**

Despite its theoretical strengths, MLS faces significant challenges in real-world implementations.

***Rigidity in Access Control***

- MLS enforces strict isolation, which can hinder collaboration. Users often need data from different levels but cannot access it due to NRU restrictions.
- This limitation is particularly problematic in intelligence and healthcare systems, where cross-level data analysis is crucial.

***Data Utility Versus Security Trade-offs***

- Ensuring absolute confidentiality often reduces data availability and usability.
- Analysts and researchers working with aggregated data may face restrictions even when no sensitive details are directly exposed.

***Performance Overhead and Complexity***

- Implementing MLS in modern distributed systems is computationally expensive.
- Managing multi-tiered access policies requires additional system resources and administrative effort.

These challenges create a security-usability paradox, where ensuring strict security often reduces the practical value of the system. To address these limitations, a more adaptive approach is required, integrating modern privacy-preserving techniques like differential privacy (DP).

**Need for Differential Privacy in Multi-Level Security**

***Traditional "No Read Up" (NRU) Restriction Versus Adaptive Data Access***

The Bell-LaPadula model's NRU restriction is designed to prevent unauthorized access to higher-level classified information [3]. However, strict NRU enforcement results in inefficient data utilization in multi-user environments.

**Example Problem**

- A military intelligence officer at a Secret level needs statistical insights from Top Secret reports but cannot access them directly due to NRU.
- Even though raw classified details must remain confidential, the officer could still benefit from generalized insights without exposing sensitive content.

To overcome this limitation, DP can be employed to sanitizing high-clearance data before granting lower-clearance access.

 

## How Differential Privacy Enables Controlled Information Flow

### *What Is Differential Privacy?*

Differential privacy (DP) is a mathematical framework that enables privacy-preserving data analysis by introducing controlled noise into query results. It ensures that individual contributions remain anonymous, preventing attackers from extracting sensitive information even if they have partial knowledge of the dataset.

### *Applying Differential Privacy to Multi-Level Security Systems*

By integrating DP with MLS policies, we can introduce adaptive data access mechanisms that allow lower-clearance users to derive insights from higher-classified data without direct access.

## Key Advantages [4, 5]

### *Enabling Secure Information Flow*

- Instead of outright denying access, DP allows lower-clearance users to query statistical summaries of classified datasets.
- *Example:* A Secret-level analyst can query military deployment numbers, but exact figures are obfuscated using DP to ensure confidentiality.

### *Mitigating Risk of Information Leakage*

- DP ensures that even if an attacker gains access to the data, noise injection prevents them from inferring precise details.
- This reduces the risk of covert channels, which are a common concern in MLS enforcement.

### *Improving Data Utility Without Violating Security Policies*

- Unlike traditional MLS approaches that completely restrict access, DP allows controlled data aggregation and trend analysis while maintaining strict security guarantees.
- This makes DP-enhanced MLS more practical for real-world applications in government, finance, and healthcare.

## Example Implementation: Military Intelligence Analysis

### *Scenario*

A military intelligence system uses DP to allow Secret-level analysts to run statistical queries on Top Secret battlefield reports.

*Without Differential Privacy (Traditional Multi-Level Security)*

- Analyst at Secret level is completely denied access to any battlefield reports.
- No insights can be obtained, leading to operational inefficiencies.

*With Differential Privacy–Enhanced Multi-Level Security*

- Analyst can query "How many enemy units were deployed in Region X?"
- The system adds DP noise (e.g., Laplace or Gaussian noise) to obfuscate exact values before providing an approximate answer.
- Analyst gains useful intelligence while ensuring classified details remain protected.

By combining DP with MLS models, security systems can evolve from strict isolation policies to controlled access mechanisms that balance security with usability. This approach ensures that confidentiality remains intact while enabling valuable data-driven decision making. Future research should focus on optimizing DP techniques for MLS systems, particularly in high-risk, real-time environments such as military operations and critical infrastructure security.

## DIFFERENTIAL PRIVACY MECHANISMS IN MULTI-LEVEL SECURITY SYSTEMS

DP is a mathematical framework designed to enable statistical analysis of datasets while preserving the privacy of individual entries. DP ensures that the inclusion or exclusion of any single data point

 

does not significantly affect the overall results, making it nearly impossible to infer specific details about any individual [6].

Formally, ϵ-differential privacy (ϵ-DP) is defined as follows:

A randomized function M provides ϵ-differential privacy if for any two adjacent datasets D and D' (differing by at most one record) and for any output S, the probability of M(D) producing S is close to the probability of M(D') producing S, controlled by a privacy budget ϵ:

$$Pr[M(D) \in S] \leq e\epsilon \cdot Pr[M(D') \in S]$$

where:

- ϵ (epsilon) controls the privacy level—lower values indicate stronger privacy guarantees.
- δ (delta) (in some relaxed variants) represents the probability of small privacy violations.

The key takeaway is that DP introduces controlled randomness, ensuring that no adversary can confidently distinguish whether a particular data point was included in the dataset or not.

**Key Techniques: Laplace Mechanism, Gaussian Mechanism, Exponential Mechanism**

Several noise-injection mechanisms enable DP while maintaining data usability [7, 8].

***Laplace Mechanism***

- Used for numerical data.
- Adds noise sampled from a Laplace distribution (centered at zero, with scale proportional to 1/ϵ).
- Ideal for queries like average salary, total population counts, etc.
- *Example:* When querying a military casualty report, instead of providing an exact number, the system adds random noise (±20) before displaying results.

***Gaussian Mechanism***

- Used when differential privacy is relaxed to (ϵ, δ)-DP (allowing small probability of privacy violations).
- Adds noise sampled from a Gaussian distribution.
- Suitable for high-dimensional data, for example, machine learning (ML) models.
- *Example:* In battlefield analytics, Gaussian noise can ensure broader uncertainty in exact troop deployment numbers while retaining overall statistical accuracy.

***Exponential Mechanism***

- Used for categorical data, where direct noise addition is not feasible.
- Selects an output probabilistically based on a scoring function (higher probability for more relevant results).
- *Example:* If a military officer queries "Which region has the most supply chain disruptions?" the system returns a probable answer without revealing exact classified logistics data.

These mechanisms enable controlled data leakage within defined security parameters, making them well-suited for MLS environments where access needs to be carefully managed.

**Application of Differential Privacy in Multi-Level Security Data Access**

***Obfuscating Sensitive Statistics for Lower-Clearance Users***

Traditional MLS systems operate on a binary access control mechanism—a Secret-level analyst is either granted full access or completely restricted from querying Top Secret data. This leads to inefficiencies in information flow.

 

DP enables an adaptive model, where lower-clearance users can access sanitized statistical insights without directly reading classified reports.

***Example Scenario: Military Intelligence Reports***

- Traditional MLS (Bell-LaPadula)
- A Secret-level analyst cannot access any troop deployment report from a Top Secret database.

***Differential Privacy–Enhanced Multi-Level Security***

- The analyst can run a query like "How many units are stationed in Region A?"
- Instead of returning an exact value (e.g., 1042 units), the system applies Laplace noise and returns $1030 \pm 25$ units.
- This preserves confidentiality while providing usable insights.

By introducing query-dependent noise, DP ensures that sensitive details are blurred while still maintaining operational usability.

**Ensuring Query-Based Access Control Without Violating Multi-Level Security Rules**

The integration of query-based DP controls in MLS addresses key challenges.

***Preventing Covert Channels***

- Traditional MLS risks side-channel inference attacks, where adversaries infer sensitive data from allowed responses [9].
- DP counters this by adding randomization, preventing attackers from making accurate inferences.

***Role-Specific Noise Injection***

- Different clearance levels can be assigned different noise budgets ($\epsilon$ values).
- A Top Secret analyst gets more precise results, while a Secret analyst receives more obfuscated data.

***Restricting Query Frequency***

- DP mechanisms limit the number of queries before privacy degradation occurs.
- This prevents repeated querying from reconstructing exact details.

By embedding DP into query-based MLS access controls, useful intelligence can be shared without compromising classified data [10].

While DP introduces some performance overhead, it greatly enhances data utility while preserving confidentiality.

**Strengths and Weaknesses of Differential Privacy Versus Role-Based Filtering**

- Strengths of DP in MLS
- More flexible than strict access controls
- Enables secure cross-clearance information sharing
- Provides quantifiable privacy guarantees ($\epsilon$-DP)
- Prevents inference attacks via controlled noise

**Weaknesses and Challenges**

- Computational cost—DP mechanisms (Laplace/Gaussian noise) require additional processing power.
- Tuning privacy budgets ($\epsilon$) is complex—too high = data leaks, too low = unusable insights.
- May still require traditional MLS enforcement for critical information (e.g., nuclear launch codes).

 

The integration of DP into MLS systems offers a balanced approach to confidentiality and usability. While traditional MLS models enforce strict isolation, DP enables controlled information sharing, allowing lower-clearance users to access sanitized insights without violating security policies. A hybrid approach combining DP-enhanced MLS with role-based discretionary access control (RBAC) can further improve security and operational efficiency. Future research should focus on:

- Optimizing DP noise injection for military and governmental datasets.
- Developing adaptive privacy budgets based on risk analysis.
- Enhancing performance efficiency to support real-time MLS analytics.

By modernizing MLS with DP, organizations can achieve both security and practicality, ensuring better intelligence sharing while upholding confidentiality standards.

## CASE STUDIES AND PRACTICAL IMPLEMENTATIONS

### Government and Military Use Cases

***Example: Military Troop Deployment Statistics with Differential Privacy Noise Injection***

In military operations, sensitive data such as troop deployment numbers, strategic asset locations, and operational readiness are strictly classified. Traditional MLS models enforce rigid "No Read Up" (NRU) restrictions, preventing lower-clearance personnel from accessing highly classified reports [11]. However, this rigid control can sometimes hinder operational efficiency, as analysts at lower clearance levels may require broad statistical insights without accessing precise classified details.

### How Differential Privacy Helps

By applying DP noise injection, a controlled amount of information can be shared while ensuring that specific details remain protected.

- Instead of blocking access entirely, the system can allow Secret-level analysts to query troop deployment statistics but inject Laplace or Gaussian noise into the numerical results.
- If an analyst queries "How many personnel are currently stationed in Base Alpha?", the system may return $1030 \pm 25$ rather than the exact 1042, ensuring that while strategic insights are available, the precise number remains obfuscated.
- This prevents adversaries from accurately inferring classified troop movements while still allowing mid-tier personnel to make informed decisions.

This approach enhances information flow without compromising security, making military data access more flexible and adaptable.

### Case Study: U.S. Census Bureau's Differential Privacy Approach Adapted for Multi-Level Security

The U.S. Census Bureau was one of the first major government agencies to adopt differential privacy to protect individual identities in publicly released data. It introduced DP noise injection in its 2020 census, ensuring that no individual's information could be inferred while preserving overall statistical accuracy [12]. This concept can be adapted for MLS military and governmental applications:

- *Population census reports in conflict zones:* Military intelligence agencies conducting demographic analyses in sensitive regions can apply DP, allowing intelligence officers to extract useful statistics while preventing adversaries from exploiting precise population counts.
- *Defense budget allocation summaries:* When sharing high-level budget breakdowns between departments, DP can obfuscate exact spending figures to prevent intelligence leaks while ensuring internal transparency.
- *Cyber threat intelligence sharing:* Government agencies can sanitize threat reports using DP before sharing with private cybersecurity firms, ensuring classified vulnerabilities remain protected while providing valuable insights into attack patterns.

 

This case study highlights how differential privacy bridges the gap between security and transparency in government analytics.

**Healthcare and Finance Applications**

***Sharing Medical Records with Privacy-Preserving Access Levels***

In the healthcare sector, MLS is used to enforce role-based access to electronic health records (EHRs).

- Doctors may require access to full medical histories.
- Nurses might only see medication and allergies.
- Medical researchers could benefit from anonymized patient statistics while being restricted from identifiable records.

**Challenges of Traditional Multi-Level Security in Healthcare**

- Hard access restrictions make it difficult for medical researchers to conduct studies on disease patterns without violating patient privacy.
- Overly restrictive policies prevent junior doctors or emergency responders from accessing life-saving information in critical situations.

**How Differential Privacy Enhances Multi-Level Security in Healthcare**

By integrating differential privacy into MLS-based medical data access, hospitals can [13]:

- Provide statistical insights on diseases (e.g., "How many COVID-19 patients in Region A?") while preventing leaks of specific patient data.
- Ensure that disease progression models can be developed using privacy-preserving aggregation, ensuring medical innovation without violating confidentiality.
- Allow pharmaceutical companies to access sanitized patient demographics to guide clinical trials while ensuring patient-level anonymity.

Thus, DP enhances privacy-preserving medical data sharing, ensuring both security and scientific progress.

**Banking Fraud Detection with Multi-Level Security + Differential Privacy Integration**

Financial institutions use MLS to restrict access to transaction histories, credit reports, and fraud detection systems.

**Limitations of Traditional Multi-Level Security in Banking**

- Bank analysts at lower levels may be blocked from fraud detection insights, delaying responses to suspicious activities.
- Regulatory reporting requirements often require banks to share transaction summaries without revealing customer details, posing a privacy challenge.

**How Differential Privacy Helps**

- Transaction monitoring systems can apply differential privacy to detect fraud patterns without exposing sensitive customer details.
- Regulatory compliance teams can query aggregated risk statistics while ensuring individual transaction details remain confidential.
- Banking fraud artificial intelligence models can be trained using differentially private financial datasets, ensuring model robustness without violating privacy laws like GDPR (General Data Protection Regulation).

By integrating DP with MLS, banks can balance fraud detection, regulatory compliance, and customer privacy more effectively.

 

### Challenges in Real-World Implementations [14]

#### *Computational Overhead of Differential Privacy in High-Security Systems*

A major challenge of integrating DP in MLS-based environments is the computational cost of noise injection.

- DP mechanisms (Laplace, Gaussian, and Exponential) require additional randomization computations before responding to queries.
- High-security systems, such as military intelligence servers or financial fraud detection engines, process millions of queries daily.
- Adding DP to every request can significantly increase processing time and memory overhead.

#### Possible Solutions

- *Hybrid DP approaches:* Implement selective noise injection only for queries crossing security clearance boundaries.
- *Hardware acceleration:* Use artificial intellegence–powered DP mechanisms to optimize real-time noise computation.
- *Efficient query batching:* Precompute sanitized statistical summaries instead of injecting DP noise in real-time queries.

These optimizations can reduce the computational burden while maintaining security.

#### Risk of Privacy-Utility Trade-offs in Multi-Tiered Access

Another challenge is balancing privacy protection vs. data utility.

- *Too much noise:* Makes the dataset useless for analysts (e.g., if military reports contain excessively obfuscated numbers, analysts may make incorrect strategic decisions).
- *Too little noise:* Increases the risk of sensitive data leaks, potentially violating national security or privacy laws.

#### Potential Approaches

- *Dynamic privacy budgets:* Assign different $\epsilon$-values based on data sensitivity (e.g., troop deployment data gets higher noise, while medical statistics get lower noise).
- *Query-rate limiting:* Prevent excessive queries from reconstructing sensitive details.
- *Artificial intelligence–driven privacy monitoring:* Use machine learning to detect abnormal access patterns and adjust DP noise levels dynamically.

By fine-tuning DP settings, organizations can maximize both security and usability in real-world applications.

## FUTURE DIRECTIONS

### Advancements in Privacy-Preserving Multi-Level Security

#### *Hybrid Models Combining Differential Privacy and Homomorphic Encryption*

While DP ensures data sanitization by adding noise to sensitive statistics, it does not inherently protect raw data storage or computation on encrypted datasets. To address this limitation, integrating homomorphic encryption (HE) with DP can enhance MLS frameworks by enabling computations on encrypted data without decryption, preserving both confidentiality and analytical utility [15, 16].

- DP ensures that query outputs remain differentially private, while HE ensures that data remains encrypted throughout computation, reducing exposure risks.
- *Use case:* In a military intelligence system, a Secret-level analyst may need aggregated battlefield statistics from Top Secret databases.
- DP ensures statistical privacy by injecting controlled noise into troop deployment reports.
- HE ensures secure computations without exposing raw data, even to the system administrator.

 

This hybrid approach strengthens privacy guarantees by ensuring that even high-clearance personnel only receive sanitized outputs without ever decrypting the original sensitive data.

**Adaptive Noise Mechanisms Using Machine Learning**

One of the key limitations of static DP mechanisms is that they apply fixed noise levels across all queries, often leading to suboptimal privacy-utility trade-offs. Machine learning–driven adaptive noise mechanisms can dynamically adjust noise injection based on:

1. *Query sensitivity:* More noise is added for queries accessing highly classified data, while lower noise is applied to less critical queries.
2. *User behavior analysis:* If a user frequently queries similar data, the system can increase noise to prevent inference attacks.
3. *Real-time risk assessment:* Machine learning models can analyze system logs to detect suspicious query patterns and adjust DP settings accordingly.

**Example**

- A finance sector MLS system may allow regional managers to access branch-level financial reports.
- If a user tries repeated queries on specific high-value transactions, the machine learning–driven DP mechanism will increase noise, preventing potential privacy breaches while maintaining overall statistical accuracy.

Such adaptive DP mechanisms improve data access flexibility while ensuring robust privacy protection across multi-tiered security levels.

**Policy Implications for Secure Data Sharing**

***Need for Differential Privacy–Aware Multi-Level Security Frameworks in National Security***

Governments and intelligence agencies rely on MLS to safeguard national security data, but traditional access control models often lead to data silos, preventing timely inter-agency collaboration. Implementing DP-aware MLS frameworks can enable secure data sharing across agencies while ensuring confidentiality.

***Key Policy Recommendations Include***

- Standardizing DP integration in MLS systems for military, intelligence, and law enforcement agencies.
- Enforcing DP compliance in inter-agency data exchanges to minimize data leakage risks while facilitating collaboration.
- Implementing DP-aware auditing mechanisms to monitor access patterns, ensuring compliance with national security policies.

By incorporating DP, policymakers can strike a balance between security and information sharing, enabling more efficient decision-making in high-stakes environments.

**Ethical Concerns and Risk Mitigation Strategies**

While DP-enhanced MLS improves security, it also raises ethical concerns related to data accuracy, bias, and fairness.

***Privacy Versus Decision-Making Accuracy***

- Excessive DP noise can distort critical data, leading to misinformed military, healthcare, or financial decisions.
- *Solution:* Implement privacy-adaptive policies that optimize DP settings based on data sensitivity and real-world impact.

 

***Bias in Differential Privacy Mechanisms***

- If DP noise disproportionately affects specific user groups or datasets, it may introduce biases in policy decisions.
- *Solution:* Develop fairness-aware DP models to ensure equitable data access across different MLS levels.

***Risk of Adversarial Exploits***

- Sophisticated attackers may attempt reconstruction attacks by correlating DP outputs across multiple queries.
- *Solution:* Implement query auditing and rate-limiting strategies to detect and prevent cumulative information leakage.

By addressing these ethical risks, governments and organizations can ensure responsible deployment of DP-enhanced MLS frameworks, maximizing both security and societal trust.

## CONCLUSION

The integration of DP into MLS models represents a transformative shift in mandatory access control. Traditional MLS frameworks, while effective in hierarchical security enforcement, often lead to data isolation and inefficiencies in decision-making. DP offers a paradigm shift by allowing controlled, statistically secure access to sensitive data through noise injection techniques, ensuring that lower-clearance users can derive meaningful insights without compromising confidentiality. Innovative advancements, such as hybrid DP-HE frameworks, further enhance security by enabling encrypted computations without exposing raw data. Additionally, machine learning-driven adaptive noise mechanisms introduce a dynamic approach to privacy preservation, optimizing security-utility trade-offs based on query sensitivity and user behavior. These solutions address key challenges in high-stakes environments like defense, intelligence, healthcare, and finance, where both security and operational agility are paramount. From a policy standpoint, DP-aware MLS frameworks must be institutionalized to standardize secure data-sharing while ensuring compliance with national security mandates. Ethical considerations, including bias in DP mechanisms, adversarial exploitation risks, and fairness in data access, must be carefully mitigated through robust auditing and adaptive privacy policies. Ultimately, privacy-preserving MLS architectures offer a balanced approach to data security, collaboration, and informed decision-making in multi-tiered systems. By embracing DP innovations, organizations can future-proof their security models, ensuring both confidentiality and controlled accessibility in an era of increasing cyber threats and data-driven operations.

## REFERENCES

1. Ghazi B, Golowich N, Kumar R, Manurangsi P, Zhang C. Deep learning with label differential privacy. Adv Neural Inform Process Syst. 2021; 34: 27131–27145.
2. Wu X, Zhang Y, Shi M, Li P, Li R, Xiong NN. An adaptive federated learning scheme with differential privacy preserving. Future Generation Computer Syst. 2022; 127: 362–372.
3. Jiang B, Li J, Yue G, Song H. Differential privacy for industrial internet of things: opportunities, applications, and challenges. IEEE Internet of Things J. 2021; 8 (13): 10430–10451.
4. Zhao Y, Chen J. A survey on differential privacy for unstructured data content. ACM Comput Surveys. 2022; 54 (10s): 1–28.
5. Yousefpour A, Shilov I, Sablayrolles A, Testuggine D, Prasad K, Malek M, Nguyen J, Ghosh S, Bharadwaj A, Zhao J, Cormode G. Opacus: user-friendly differential privacy library in PyTorch. arXiv preprint. arXiv:2109.12298. September 25, 2021.
6. Li Z, Wang B, Li J, Hua Y, Zhang S. Local differential privacy protection for wearable device data. PLoS One. 2022; 17 (8): e0272766.
7. Wang J, Han H, Li H, He S, Sharma PK, Chen L. Multiple strategies differential privacy on sparse tensor factorization for network traffic analysis in 5G. IEEE Trans Indus Informatics. 2021; 18 (3): 1939–1948.

 

8. Jia B, Zhang X, Liu J, Zhang Y, Huang K, Liang Y. Blockchain-enabled federated learning data protection aggregation scheme with differential privacy and homomorphic encryption in IIoT. IEEE Trans Indus Informatics. 2021; 18 (6): 4049–4058.
9. Ziller A, Usynin D, Braren R, Makowski M, Rueckert D, Kaissis G. Medical imaging deep learning with differential privacy. Sci Rep. 2021; 11 (1): 13524.
10. El Ouadrhiri A, Abdelhadi A. Differential privacy for deep and federated learning: a survey. IEEE Access. 2022; 10: 22359–22380.
11. Demelius L, Kern R, Trügler A. Recent advances of differential privacy in centralized deep learning: a systematic survey. ACM Comput Surveys. 2025; 57 (6): 1–28.
12. Ponomareva N, Hazimeh H, Kurakin A, Xu Z, Denison C, McMahan HB, Vassilvitskii S, Chien S, Thakurta AG. How to dp-fy ML: a practical guide to machine learning with differential privacy. J Artif Intell Res. 2023; 77: 1113–1201.
13. Adnan M, Kalra S, Cresswell JC, Taylor GW, Tizhoosh HR. Federated learning and differential privacy for medical image analysis. Sci Rep. 2022; 12 (1): 1953.
14. Zhang W, Li X. Federated transfer learning for intelligent fault diagnostics using deep adversarial networks with data privacy. IEEE/ASME Trans Mechatron. 2021; 27 (1): 430–439.
15. Jiang H, Pei J, Yu D, Yu J, Gong B, Cheng X. Applications of differential privacy in social network analysis: a survey. IEEE Trans Knowledge Data Eng. 2021; 35 (1): 108–127.
16. Wylde V, Rawindaran N, Lawrence J, Balasubramanian R, Prakash E, Jayal A, Khan I, Hewage C, Platts J. Cybersecurity, data privacy and blockchain: a review. SN Computer Sci. 2022; 3 (2): 127.

 