Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 02, NCRTCS - 2026

Data Security and Privacy in Artificial Intelligence Systems

Sakshi Deepak Hatte
Department of Computer Science
Prof. Ramkrishna More ACS College Akurdi, Pune - 44

Abstract - Artificial Intelligence systems depend on large volumes of data to enable intelligent decision making, prediction, and automation. These datasets frequently contain sensitive personal and organizational information, making data security and privacy critical issues. Artificial Intelligence introduces specific risks such as data leakage, inference attacks, and unauthorized model exploitation. This paper examines security and privacy challenges across the Artificial Intelligence data lifecycle and presents protection mechanisms including encryption, access control, differential privacy, and federated learning. The study emphasizes the need for privacy by design principles to ensure secure and trustworthy Artificial Intelligence systems.

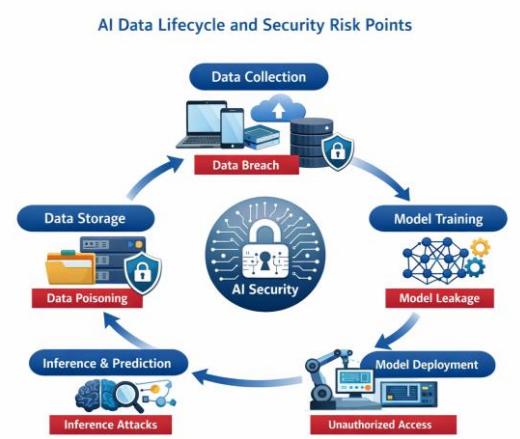
Keywords - Artificial Intelligence, Data Security, Data Privacy, Machine Learning, Differential Privacy

I. INTRODUCTION

Artificial Intelligence has become an essential technology in modern digital systems such as healthcare diagnostics, financial analytics, smart transportation, and intelligent automation. Artificial Intelligence models require large datasets to achieve accuracy and efficiency. However, the extensive use of sensitive data increases the risk of data breaches, unauthorized access, and privacy violations. Conventional security approaches are insufficient to address the complex threats faced by Artificial Intelligence systems. Therefore, robust data security and privacy mechanisms are necessary to ensure ethical and secure deployment.

II. ARTIFICIAL INTELLIGENCE DATA LIFECYCLE AND SECURITY RISKS

Artificial Intelligence systems operate through a structured data lifecycle consisting of data collection, storage, preprocessing, model training, deployment, and inference. Each stage presents unique security challenges. Data collection from user inputs, sensors, and online sources may expose systems to data poisoning and unauthorized access. Insecure data storage can lead to large scale data breaches. During model training, models may memorize sensitive information, which can be exploited through inference and extraction attacks.



III. DATA PRIVACY CHALLENGES IN ARTIFICIAL INTELLIGENCE

Artificial Intelligence systems raise significant privacy concerns due to automated decision making and large-scale data analysis. Many models operate as black boxes, limiting transparency and user understanding of data usage. Improper handling of data may also introduce bias, exposing sensitive attributes and resulting in unfair outcomes.

IV. SECURITY AND PRIVACY PRESERVATION TECHNIQUES

Encryption ensures confidentiality of data during storage and transmission. Access control mechanisms restrict data usage to authorized entities. Differential privacy protects individual data records by introducing controlled noise. Federated learning enables decentralized model training without sharing raw data, thereby preserving privacy.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 02, NCRTCS - 2026

Table 1. Comparison of Artificial Intelligence Security and Privacy Technique

Technique	Purpose	Security / Privacy Benefit	Limitations
Encryption	Protects data during storage and transmission	Ensures confidentiality and prevents unauthorized data access	Does not protect data while in use; key management complexity
Access Control	Restricts system and data access to authorized users	Prevents unauthorized usage and internal misuse	Insider threats still possible
Differential Privacy	Adds controlled noise to datasets or outputs	Prevents disclosure of individual data records	May reduce model accuracy
Federated Learning	Trains models across decentralized devices	Raw data never leaves local devices, enhancing privacy	Communication overhead and system complexity
Secure Multi-Party Computation	Enables joint computation without data sharing	Ensures privacy across multiple data owners	High computational cost
Model Anonymization	Removes sensitive attributes from training data	Reduces bias and privacy leakage	Risk of reduced data utility
Audit Logging & Monitoring	Tracks data access and system activity	Helps detect security breaches and misuse	Requires continuous monitoring

Encryption provides confidentiality, differential privacy limits data exposure, access control prevents unauthorized usage, and federated learning preserves user data.

V. REGULATORY AND COMPLIANCE CONSIDERATIONS

Data protection regulations such as the General Data Protection Regulation emphasize transparency, user consent, data minimization, and accountability. Compliance with these regulations is essential for organizations deploying Artificial Intelligence systems.

VI. FUTURE DIRECTIONS

Future Artificial Intelligence systems are expected to adopt advanced privacy preserving techniques such as homomorphic encryption and secure multi party computation, enabling data processing without revealing sensitive information.

VII. CONCLUSION

Data security and privacy are fundamental requirements for Artificial Intelligence systems. Artificial Intelligence specific threats require advanced protection mechanisms beyond traditional security solutions. Integrating encryption, differential privacy, access control, and federated learning supports secure and ethical deployment.

ACKNOWLEDGMENT

The author sincerely thanks the faculty members of the Department of Computer Science for their guidance and support during the preparation of this research work.

REFERENCES

[1] C. Dwork, Differential privacy, International Colloquium on Automata, Languages, and Programming, 2006.
[2] A. Shokri et al., Membership inference attacks against machine learning models, IEEE Symposium on Security and Privacy, 2017.
[3] K. Bonawitz et al., Practical secure aggregation for privacy preserving machine learning, ACM CCS, 2017.
[4] European Union, General Data Protection Regulation, Official Journal of the European Union, 2018.