Cryptography in AI Data Security

1st Navyaa Jain
Department of Computer Engineering
JIIT
Noida, India
2401030114@mail.jiit.ac.in

2nd Aradhya Singh
Department of Computer Engineering
JIIT
Noida, India
2401030100@mail.jiit.ac.in

3rd Nishika
Department of Computer Engineering
JIIT
Noida, India
2401030116@mail.jiit.ac.in

***Abstract*—The recent boom in Artificial Intelligence and Large Language Models has raised serious concerns about data security and privacy. Models like ChatGPT and Gemini get better when they have a lot of information from people using them. When these systems have information they work better but this also means there is a bigger risk. This risk is that people might share things about themselves without realizing it when they talk to these systems or upload files. Since many people use these systems a huge amount of information is collected, which makes it really important to store it safely and protect it. Artificial Intelligence and Large Language Models need to be able to do this to keep people's information safe. This paper studies how data is stored and processed in AI and LLM pipelines and highlights the main security risks involved, such as data breaches, privacy leakage, and model manipulation. We examine cryptography as a practical approach for protecting AI datasets through encryption, integrity checks, and secure access control. The focus is on balancing model improvement with stronger data protection so that AI systems can be developed more safely and responsibly.**

***Index Terms*—Artificial Intelligence, Large Language Models, Data Security, Cryptography, Privacy Protection, AI Data Storage**

I. Introduction

Modern AI systems and LLMs need storage systems that can handle a lot of information and give them what they need quickly. When it comes to AI workflows the data is usually stored in three stages: collection storage, processing storage, and model artifact storage. User inputs such as prompts, replies, uploaded files, and activity records are first stored in secure cloud storage or large databases. These systems keep multiple copies of the data and split it across servers so it stays safe and easy to access even if one system fails. Before training the AI model, the data is cleaned and converted into a structured form that the computer can understand, such as small word units and number-based representations. This processed data is then stored in fast storage systems so it can be used quickly during training.

AI models do not keep exact copies of user conversations inside the model itself. Instead, they learn general patterns from the data and store those patterns as numbers. This means the model remembers relationships in language, not the original text itself. However, other supporting data, such as activity logs, extra training data, and testing data, can still include private or sensitive information. So this data also needs strong security and protection.

Cryptography helps reduce these security risks by protecting stored and shared data using encryption. It is a way of securing information with mathematical methods so that only authorized users can read or use it. It converts normal readable data into an unreadable form using keys and encryption techniques. This helps reduce damage from data breaches, prevents misuse, and keeps sensitive information safer. Since AI systems now work with very large amounts of personal and confidential data, using cryptographic protection has become necessary.

II. Methodology

Cryptography suits our requirements to prevent data breaches and enhance data security due to its multi-layered, complex nature of working. It comprises of the following:

A. Encryption

Data is converted from readable form to unreadable form called ciphertext. This is done using a key- something which encodes the conversion process from readable data to ciphertext and vice versa. In context of LLMs, this can be used for storing the data set of any language model. This can also be used to prevent data breach by encrypting data in transit so that it cannot be accessed by unauthorised users on a network, which can be as big as the internet itself.

B. Key based access

Only entities with the correct cryptographic key can decrypt data. Without the key, data remains useless, which prevents misuse even by insiders. By insiders, we mean any entity which doesn't have authorization over the data but has access to LLM technology at development level.

C. Integrity verification

Cryptographic hashes and signatures ensure that data has not been modified, AI training data remains authentic, model inputs are not tampered with.

D. Authentication

Cryptography verifies identities of systems and users interacting with AI pipelines, preventing impersonation or spoofing attacks.

E. Efficacy of cryptography

In distributed AI environments, multiple services communicate across networks to perform tasks such as data collection, processing, and model deployment. Cryptographic authentication ensures that only verified entities are allowed to participate in these interactions. Cryptography tests use Zephyr Test Framework (Ztest) to run the tests. The tests are executed if the cryptographic functionality is enabled in Kconfig. Various modes- AES, AEAD, ECDH, ECDSA and Hash- can be tested for different AI models. By preventing spoofing and impersonation attacks, authentication mechanisms help maintain the reliability and security of AI systems.

III. Result

This research paper explores the use and storage of massive amounts of data by AI and Large Language Models (LLM). Though models do not store actual conversations, data, and training information may hold private information, which can be risky if security measures are not in place.

Cryptography appears to be an effective means of improving data security in AI systems. Encryption makes data unreadable without keys, key-based access controls data use, data hashing ensures data integrity, and authentication prevents unauthorized access. These processes occur at various levels to prevent data leaks and tampering. Thus, cryptographic processes should be a fundamental security component of AI and LLM data systems to ensure that model development and usage are secure and trustworthy.

IV. Conclusion

In this paper, we looked at how AI and Large Language Model systems use and store very large amounts of data during training and operation. Because these systems are heavily dependent on user inputs and datasets, there is always a risk that sensitive information can be exposed, misused, or modified if proper protection is not applied. Although the models themselves do not store exact conversations, related storage such as logs, datasets, and training records can still contain private data, which makes security an important requirement.

From the study and references reviewed, cryptography stands out as one of the most practical ways to improve data security in AI environments. Methods like encryption make data unreadable without proper keys, key-based access limits who can use the data, hashing helps detect unwanted changes, and authentication prevents unauthorized system access. These protections work at multiple levels and reduce common risks such as data leaks and tampering. Based on this, it can be concluded that cryptographic techniques should be included as a basic security layer in AI and LLM data pipelines so that model development and usage can be safer and more trustworthy.

References

[1] Hamed Taherdoost, Tuan-Vinh Le and Khadija Slimani , “Cryptographic Techniques in Artificial Intelligence Security: A Bibliometric Review, March 2025.

[2] https://docs.nordicsemi.com/bundle/ncs-2.9.2/page/nrf/tests/crypto/README.html.

[3] Ogbodo, M. U., et al. (2025). Cryptographic Techniques in Artificial Intelligence Security: A Bibliometric Review. ResearchGate.

[4] Yan, B., Li, K., Xu, M., Dong, Y., Zhang, Y., Ren, Z., Cheng, X. (2024). On Protecting the Data Privacy of Large Language Models (LLMs): A Survey. arXiv preprint arXiv:2403.05156.