The Unbreakable Trio Protection From LLM's

Jovana Latinovic and Bharat S. Rawal
Department of Computer Science and Digital Technologies, Grambling State University, Grambling, LA 71245

The Problem

AI is Powerful, But Privacy Is at Risk

AI (LLMs) makes life easier:
it solves problems, automates tasks, finishes jobs faster.
But: there's a big problem → **Data Privacy**.
Real-world examples: companies like Samsung leaked confidential data into ChatGPT.
Challenge: AI is double-edged — it can be good, but also dangerous if misused.
As a computer scientist, I asked: how do we protect people's data from this misuse?

First Step: Protecting and Encrypting Data

Starting with Encryption

The first defense: **Learning With Errors (LWE)**.
LWE is futuristic and already used in post-quantum cryptography.
It works by adding *small noise* → data looks scrambled to attackers.
Only the person with the key can "unscramble" it.
Result: Hackers face an almost impossible problem.
(And don't worry, that's just the beginning!)

What is LWE?

Learning With Errors Explained Simply

Think of LWE as adding "fake letters" into your diary.
To outsiders: the diary looks messy and unreadable.
To the owner (with the key): you know which letters are real.
Key point: Easy to use if you have the secret, impossible if you don't.
Strong enough to resist even quantum computers.

Double Protection: Homomorphic Encryption

Adding a Second Lock

Now we add **homomorphic encryption** → a *second layer*.
Analogy: the diary is locked, and then placed inside a locked box.
You can *work on* the diary (write notes, change text) while it's still in the locked box.
But you can't remove or expose it without the key.
Result: Data is doubly hard to steal or misuse.

The Next Problem

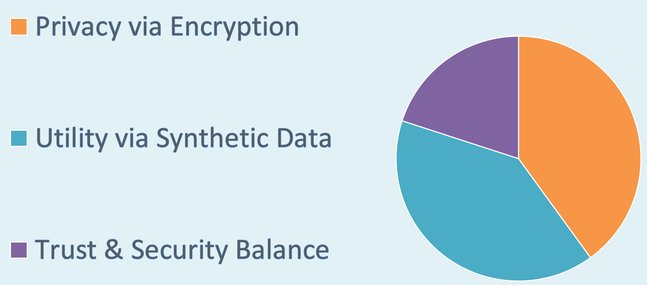
But What About AI Training?

LLM companies want data to keep models smart.
If everything is encrypted, they may say: *"We can't improve our AI."*
This creates a conflict: **Security vs. Model Improvement**.
How do we allow AI to learn *without* exposing private data?

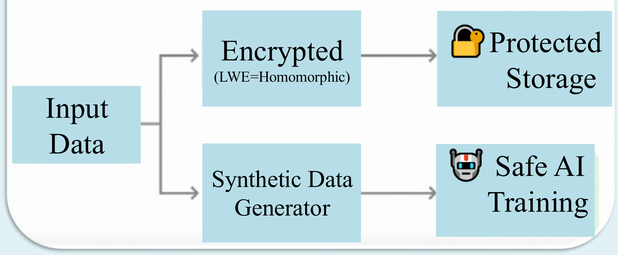
The Trio in Action

The Unbreakable Trio

Step 1: Learning With Errors → noise as armor.
Step 2: Homomorphic Encryption → locked diary in a locked box.
Step 3: Synthetic Data → fake-but-useful data for AI training.
Together, they form an **Unbreakable Trio**.
Protects users **and** still helps AI grow.



How The Trio Works



The Solution: Synthetic Data

AI Protecting Against AI

Idea: split the data flow into **two paths**:
Private Data → stays encrypted (LWE + homomorphic).
Synthetic Data → generated from private data (fake but realistic).
LLMs get the synthetic version for training.
Users keep their real private data fully encrypted.
Result: Privacy protected + AI still improves.

Conclusion

A Future of Trustworthy AI

AI is here to stay, but privacy must not be optional.
With the **Unbreakable Trio**, we:
Keep real data safe.
Let AI keep learning responsibly.
Give users control + give companies growth.
Final thought:
"We use AI to protect against AI."

References

[1] J.-W. Lee, H. Kang, Y. Lee, W. Choi, J. Eom, M. M. Deryabin, E. Lee, J. Lee, D. Yoo, Y.-S. Kim, and J.-S. No, "Privacy-Preserving Machine Learning With Fully Homomorphic Encryption for Deep Neural Network," *IEEE Access*, vol. 10, pp. 30039–30054, 2022. doi: 10.1109/ACCESS.2022.3159694
[2] G. Lloret-Talavera, M. Jorda, H. Servat, F. Boemer, C. Chauhan, S. Tomishima, N. N. Shah, and A. J. Peña, "Enabling Homomorphically Encrypted Inference for Large DNN Models," *IEEE Trans. Comput.*, early access, 2023. doi: 10.1109/TC.2023.3292574
[3] C. Gentry, S. Halevi, and N. P. Smart, "Homomorphic Evaluation of the AES Circuit," in *Advances in Cryptology – CRYPTO 2012*, Berlin, Heidelberg: Springer, 2012, pp. 850–867. doi: 10.1007/978-3-642-32009-5_49
[4] V. Lyubashevsky, C. Peikert, and O. Regev, "On Ideal Lattices and Learning With Errors Over Rings," in *Advances in Cryptology – EUROCRYPT 2010*, Berlin, Heidelberg: Springer, 2010, pp. 1–23. doi: 10.1007/978-3-642-13190-5_1
[5] J. Beutel, J. Kohne, and T. Schneider, "Syntfhe: Privacy-Preserving Synthetic Data Generation Using Fully Homomorphic Encryption," *IEEE Access*, vol. 11, pp. 115624–115639, 2023. doi: 10.1109/ACCESS.2023.3307180

GRAMBLING STATE UNIVERSITY