Hybrid Design for Enhanced Privacy

This chapter introduces Nesa's cutting-edge hybrid approach to privacy enhancement. The essence of this hybrid design lies in the thoughtful integration of hardware-based and cryptographic-based solutions, each selected and optimized for varying scenarios within our ecosystem through what we call the Split-Flow Protocol.

The Split-Flow methodology for hybrid privacy is grounded in the recognition that privacy concerns manifest in different forms—users may wish to conceal their input data or the results of their inferences, while node owners might seek to protect the confidentiality of their model parameters. Our hybrid design acknowledges the unique requirements of these use cases by deploying the most appropriate privacy-preserving technologies.

Through the synergy of the robust, hardware-centric protections of Trusted Execution Environments (TEEs) and the advanced cryptographic techniques of Zero-Knowledge Proofs (ZKPs) and Secure Multi-Party Computation (SMPC), we ensure that privacy is a foundational pillar of the system.

This chapter elucidates the rationale behind Nesa's hybrid strategy, offering a comprehensive blueprint for achieving the highest standards of privacy using Split-Flow while maintaining the usability and efficiency of the decentralized inference process.

Previous
Step-by-Step Process of Decentralized Inference

Next
Challenges in Achieving Confidentiality and Verifiability

Last updated 1 month ago