Challenges in Achieving Confidentiality and Verifiability

In engineering a privacy-centric decentralized inference architecture, the primary challenge lies in reconciling the twin imperatives of data confidentiality and computational verifiability. These concurrent objectives, each indispensable, represent an intrinsic paradox that proves difficult to harmonize.

While conventional encryption techniques are adept at bolstering confidentiality, they incapacitate the data that they encrypt for substantive analytical processing. So in environments like Nesa's where the system's operational utility is contingent upon the facilitation of intricate data computations on private data, encryption doesn't work.

Confidentiality typically involves encrypting data to prevent unauthorized access. While encryption secures the data when static or during exchange, it also obscures the data from the very systems that need to process it. Standard computation on encrypted data is not feasible, as the process of encryption changes the data format and structure, making it indecipherable and inoperative for standard computation.

This necessitates the development of the specialized techniques of Homomorphic Encryption (HE) and Secure Multi-Party Computation (SMPC), which are designed to enable computations on encrypted data without ever needing to decrypt it.

However, the introduction of such techniques to enable computation on encrypted data engenders a second challenge: verifiability. Users and node owners inherently desire not just the confidentiality of their data or models but also the assurance that the computations performed are correct and trustworthy.

Verifiability means providing a way to prove that the computation was executed as intended and that the results are accurate reflections of the computation on the expected data. Zero-knowledge proofs (ZKPs) can be employed to demonstrate the correctness of computations without revealing the underlying data. But integrating this into a system already grappling with encrypted data adds layers of complexity.

The intersection of these challenges—ensuring confidentiality while enabling computation and providing verifiability—requires a sophisticated balance of cryptographic innovation and system design. Any proposed solution must be sufficiently secure to guard against breaches and robust enough to withstand the scrutiny of verification without compromising on performance or scalability.

As we proceed through this section, we will dissect these challenges in detail and explore Nesa's Split Flow Protocol that harnesses composite architectures to address the combined imperative of confidentiality and verifiability within the inference framework.

Previous
Hybrid Design for Enhanced Privacy

Next
Split-Flow

Last updated 1 month ago