ZCube: A Zero-Trust, Zero- Knowledge, and Zero-Memory Platform for Privacy and yet Secured Access

Department of Computer Science and Engineering, University of North Texas, Denton, TX

Vinh Quach, Ram Dantu, Sirisha Talapuru, Shakila Zaman, Apurba Pokharel

UNT UNIVERSITY OF NORTH TEXAS EST. 1890

Introduction

Traditional trust management systems rely on past interactions and network referrals to calculate trust scores, requiring extensive storage. This creates memory dependence, increases vulnerability to attacks, and heightens the risk of data exposure due to breaches, which are becoming more frequent and severe.

We propose a lightweight, memoryless, trustless protocol that eliminates the need to store previous interactions or request confidential information. Each request begins with a fresh plan, which is rigorously monitored during execution, with each hop linked similarly to blockchain blocks, requiring honesty and adherence to the plan for proof assembly.

We implemented the proposed idea and evaluated its performance and functionality by measuring response time and failure rate along a specific path. Our results show that this novel memoryless approach maintains trust on the fly, eliminating the need for confidential information in access control.

Proposed Solution

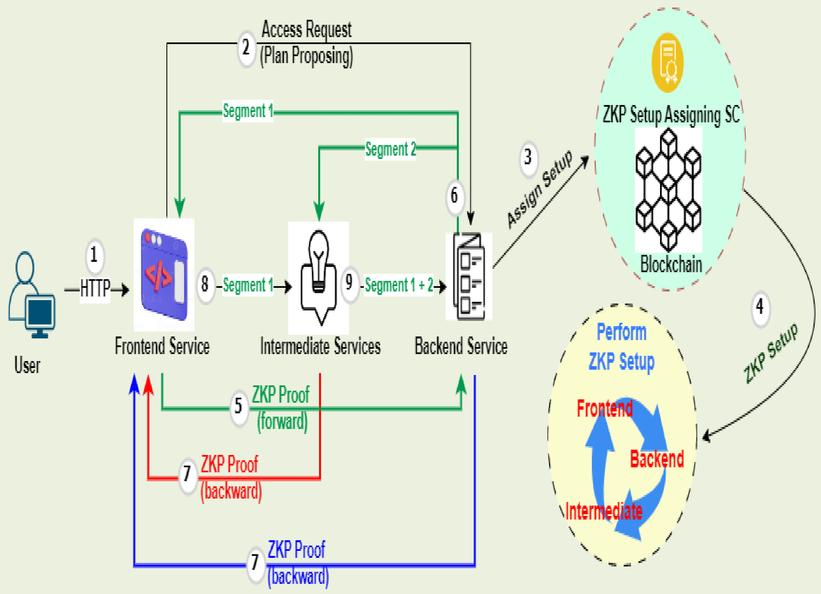
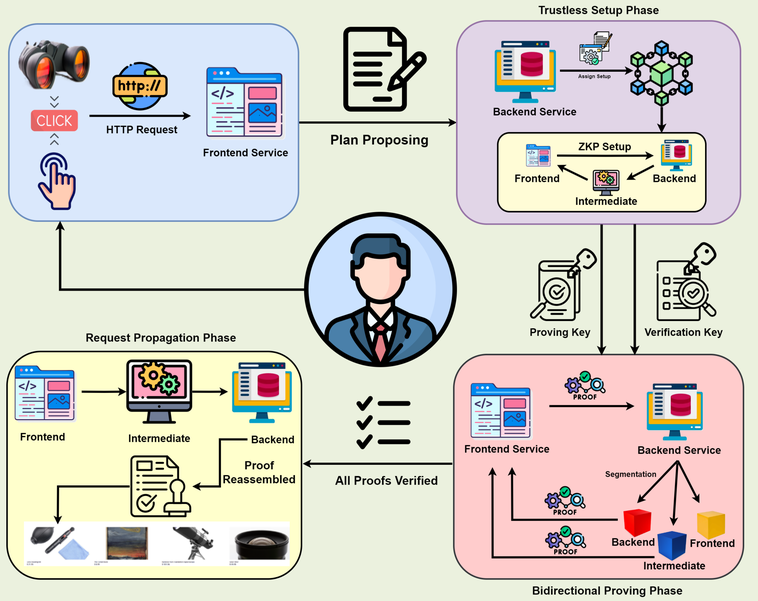


Figure 1: Memoryless Zcube Event Flow

Using OpenTelemetry Demo, we demonstrate the ability to create a memoryless network that can handle hundreds of independent transactions simultaneously.

Methodology

- We evaluate performance and functionality based on response time and failure rate. OpenTelemetry Demo consists of microservices writing in different languages.
- After user authentication, a plan is presented for approval, triggering the Trustless Setup phase, which involves plan proposal, pair setup, setup execution.
- Once the proving key is received by the requesting service, the Bidirectional Proving phase begins by sending a proof to the terminal service. This involves proof segmentation and backward proving.
- In the Request Propagation phase, after all proofs have passed verification, the requesting service begins sending the actual request. following the proposed plan to assemble the correct proof.



Results

The platform was load tested with 1 to 150 users. Response times remained consistent up to 100 users, but latency increased with higher user counts. Figure 2 shows that our memoryless platform is suitable and practical for this use case.

Various time durations were analyzed, and the percentage contribution of each phase to the total response time was calculated, as shown in Figure 3. As the system approaches failure, phase 3 increases significantly.

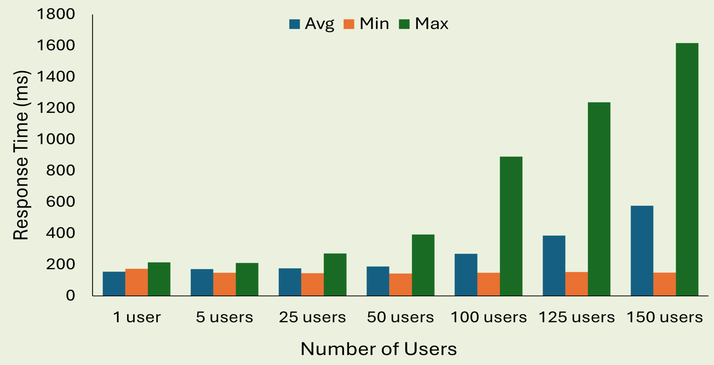


Figure 2: Response Time for Varying Number of Users

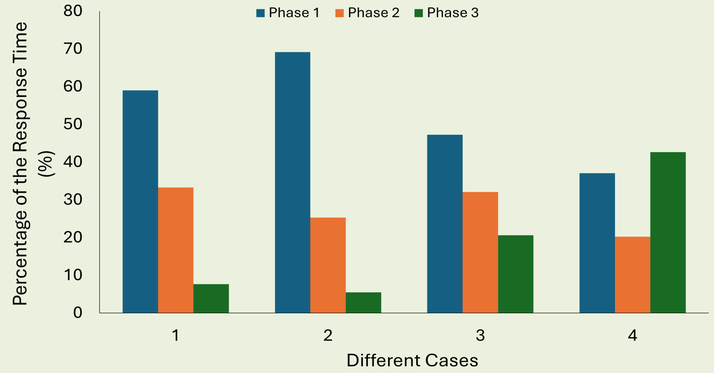


Figure 3: Percentage of Total Response Time for Each Phase of the Platform

Conclusions

We focus on developing a continuous, decentralized, memoryless game plan platform that can be implemented within a microservice architecture. This goal is achieved by leveraging the concepts of blockchain and plan presentation.

In our platform, every step of plan presentation and execution is verified and monitored. In summary, the security and efficiency of the proposed platform demonstrate that our protocol is practical and can potentially be used by a wide range of applications..

Acknowledgments

This research was partially supported by the National Centers of Academic Excellence in Cybersecurity, housed in the Division of Cybersecurity Education, Innovation and Outreach, at the National Security Agency (NSA) grants H98230-20-1-0329, H98230-20-1-0414, H98230-21-1-0262, and H98230-22-1-0329.