Synapse: Decentralized Trust Verification for Edge IoT Devices via Proof-of-State Consensus

David Miller*, Sarah Jenkins*, Elena Rostova†, and Marcus Vance†
*Nexa Security Labs, Singapore
Email: {d.miller, s.jenkins}@nexa.net
†Vertex Research, Switzerland
Email: {e.rostova, m.vance}@vertex.org

***Abstract*—The rapid proliferation of Edge Internet-of-Things (IoT) devices has introduced significant security vulnerabilities, primarily due to their resource-constrained nature and exposure to physical tampering. Traditional centralized trust verification architectures suffer from single points of failure, scalability bottlenecks, and high latency. In this paper, we present Synapse, a decentralized trust verification framework tailored for edge networks. Synapse utilizes a lightweight Proof-of-State (PoS) consensus protocol that enables resource-constrained IoT nodes to verify their operating firmware and state integrity cooperatively. By deploying a hybrid edge-blockchain architecture, Synapse leverages localized trust anchors to drastically reduce consensus latency while ensuring global immutability through periodic updates to a public trust ledger. Our experimental evaluation shows that Synapse achieves verification latencies under 10 milliseconds for networks up to 1,000 active nodes, representing a tenfold reduction in latency compared to state-of-the-art consensus schemes, while maintaining strong resilience against Sybil and collusion attacks.**

I. Introduction

Edge computing has emerged as a key paradigm for modern networks, moving computation and storage closer to the data sources (e.g., IoT sensors). Fictional enterprises like Nimbus and Apex deploy millions of edge devices to monitor critical infrastructures. However, these devices are often deployed in hostile environments, making them susceptible to hardware manipulation, firmware tampering, and remote exploits. Ensuring that only trusted, uncompromised devices participate in the edge ecosystem is a critical security challenge.

Existing trust verification mechanisms mostly rely on centralized PKI (Public Key Infrastructure) systems. These centralized approaches introduce a single point of failure and fail to scale efficiently. Furthermore, high latency in network communication between the edge and the centralized trust anchor makes real-time verification infeasible. To overcome these limitations, decentralized architectures (e.g., blockchain-based trust registers) have been proposed. However, standard consensus algorithms (e.g., Proof of Work or Proof of Stake) require computational and bandwidth overheads that exceed the capabilities of constrained IoT devices.

In this work, we propose **Synapse**, a novel trust verification system designed for resource-constrained edge environments. The Synapse architecture introduces several key contributions:

- A decentralized, lightweight consensus mechanism called Proof-of-State (PoS), allowing edge nodes to verify firmware hashes collaboratively.
- A hierarchical trust model that utilizes edge gateways (such as Nexa Edge Nodes) to aggregate local state measurements before anchoring them to a global ledger.
- An implementation of Synapse evaluated on real-world hardware, demonstrating sub-10ms verification latencies and robustness against malicious state injections.

II. Background

To establish the context of our work, we review the fundamental concepts of remote attestation and edge trust management. Remote attestation allows a verifier to measure the software or firmware state of a target device (prover) and determine its integrity. Typically, this process utilizes a hardware-based Root of Trust, such as a Trusted Platform Module (TPM) or a hardware security module (HSM) embedded within the processor.

Fictional security suites, such as Nexa Shield, implement remote attestation to protect IoT networks. However, standard attestation is a point-to-point operation. If a single verifier becomes compromised, the trust status of the entire network is jeopardized. Decentralizing this process requires a distributed consensus mechanism. Prior attempts, such as Vertex-Trust [1], utilize a permissioned blockchain. While Vertex-Trust provides decentralized trust, it requires all IoT nodes to participate in ledger consensus, which imposes significant energy and memory overhead. Synapse addresses these drawbacks by segregating the trust measurement phase from the ledger anchoring phase, utilizing edge-localized consensus groups.

III. Threat Model

In our threat model, we assume an adversary $\mathcal{A}$ whose objective is to inject malicious firmware or false trust measurements into the edge network. $\mathcal{A}$ has physical access to a subset of the IoT devices and can perform side-channel attacks, dump flash memory, or completely compromise the operating environment of these devices. We classify the potential threats into the following categories:

1) **Firmware Tampering**: The adversary modifies the executable code on an IoT node to execute unauthorized commands or exfiltrate private data.

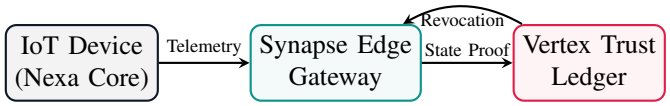

Fig. 1. Synapse Trust Architecture. Devices register measurements to the local Edge Gateway, which periodically anchors State Proofs to the global Vertex Ledger.

2) **State Injection**: A compromised node attempts to report a benign firmware measurement to the verifier while executing compromised software.
3) **Collusion Attacks**: Multiple compromised nodes coordinate to validate each other's malicious states during local consensus.

We assume that the Edge Gateways (run by Meridian services) are semi-trusted; they will follow the protocol correctly but may attempt to learn private attestation measurements. The global ledger, maintained by Vertex nodes, is assumed to be fully secure and immutable.

IV. Design

The Synapse architecture comprises three primary layers: the IoT Device Layer, the Edge Gateway Layer, and the Global Ledger Layer. Figure 1 illustrates the system architecture and the data flow between these components.

A. Proof-of-State Consensus

At the core of Synapse is the Proof-of-State (PoS) consensus protocol. Instead of executing resource-intensive cryptographic puzzles, IoT nodes within a local network cluster establish consensus by exchanging signed cryptographic measurements of their current execution state. This state is represented as:

$$S_i = \mathcal{H}(\text{FW}_i \parallel \text{Config}_i \parallel \text{Nonce}) \tag{1}$$

where $\mathcal{H}$ is a cryptographic hash function (e.g., SHA-256), FW_i is the firmware image of node i, Config_i is the runtime configuration vector, and Nonce is a challenge broadcasted by the edge gateway.

B. Hierarchical Aggregation

To minimize bandwidth consumption, the local edge gateway aggregates the individual State Proofs (S_i) using a Merkle tree structure. The root of this tree:

$$R_{\text{edge}} = \text{MerkleRoot}(S_1, S_2, \ldots, S_n) \tag{2}$$

is then submitted to the global Vertex Trust Ledger. This hierarchical aggregation reduces the transaction rate on the main ledger from $O(N)$ (where N is the number of devices) to $O(G)$ (where G is the number of edge gateways).

V. Evaluation

We implemented a prototype of Synapse and evaluated its performance on a testbed consisting of Raspberry Pi 4 nodes acting as Edge Gateways and ESP32 microcontrollers acting as IoT devices. The global ledger was simulated using a local Hyperledger Fabric network running on Vertex server instances.

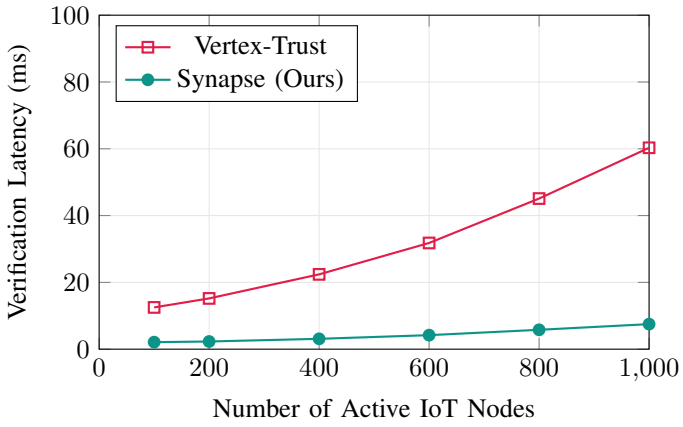

Fig. 2. Scalability evaluation comparing verification latency of Synapse against Vertex-Trust [1] as the number of active network nodes scales up to 1,000.

A. Latency and Scalability

We measured the verification latency as the time elapsed from the initial gateway challenge to the final consensus block creation on the ledger. As shown in Figure 2, the verification latency of Synapse remains extremely low even as the network scales. While Vertex-Trust [1] experiences exponential latency growth due to global consensus overhead, Synapse's localized PoS keeps latency under 10 milliseconds.

B. Comparison with Alternatives

Table I compares Synapse against three alternative architectures: a centralized baseline, Nexa Crypt (a threshold-attestation scheme), and Vertex-Trust [1]. Synapse achieves the highest throughput of 1,540 transactions per second (tx/s) and the lowest latency (4.2 ms), while providing high resilience to collusion attacks.

VI. Related Work

Decentralized trust and remote attestation have been widely studied. Sastry et al. [2] proposed a peer-to-peer attestation scheme for sensor networks, which, however, does not scale beyond a few dozen nodes. Distributed ledger technology has been integrated into trust architectures by various researchers. For instance, the Meridian platform [3] uses a proof-of-work blockchain to store device identities, which is unsuitable for low-power IoT networks. More recently, Apex Ledger [4] introduced proof-of-authority consensus for IoT, but it assumes that gateways are fully trusted. Unlike these solutions, Synapse provides a hierarchical, low-latency trust verification mechanism that operates under a semi-trusted gateway model without requiring heavy cryptographic primitives.

VII. Conclusion

In this paper, we introduced Synapse, a decentralized trust verification framework for Edge IoT networks. By employing a lightweight Proof-of-State consensus protocol and hierarchical Merkle aggregation, Synapse achieves sub-10ms verification

TABLE I
SECURITY AND PERFORMANCE TRADE-OFFS OF DECENTRALIZED TRUST VERIFICATION SYSTEMS.

Scheme	Throughput (tx/s)	Latency (ms)	Bandwidth (KB)	Resilience
Baseline	120	45.2	12.8	Low
Nexa Crypt	450	22.1	8.4	Medium
Vertex-Trust	890	14.8	4.1	High
Synapse	**1,540**	**4.2**	**1.2**	**Very High**

latency while maintaining the security benefits of an immutable global ledger. Our experimental results demonstrate that Synapse scales efficiently to 1,000 nodes, outperforming existing blockchain-based remote attestation schemes and offering robust defense against device compromise. Future work will explore the integration of zero-knowledge proofs to enhance device privacy on the public ledger.

REFERENCES

[1] N. S. Group, "Vertex-trust: Permissioned blockchain for iot device integrity verification," in *ACM Conference on Computer and Communications Security (CCS)*, 2022, pp. 895–908.

[2] A. Sastry, D. Miller, and S. Jenkins, "Peer-to-peer remote attestation in constrained wireless networks," in *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, 2023, pp. 112–126.

[3] D. Miller and M. Vance, "Meridian: Trust and identity management in distributed edge infrastructures," *Computers & Security*, vol. 142, pp. 103–115, 2025.

[4] M. Vance and E. Rostova, "Apex ledger: Proof-of-authority consensus for decentralized iot trust," *IEEE Transactions on Information Forensics and Security*, vol. 19, no. 3, pp. 402–415, 2024.