DHTee: Decentralized Infrastructure for Heterogeneous TEEs

Rabimba Karanjai*, Zhimin Gao§,Lin Chen‡ Xinxin Fan¶, Teweon Suh‖, Weidong Shi*, Lei Xu†
*University Of Houston,USA, †Kent State University,USA , ‡ Texas Tech University,USA
{rkaranjai, wshi3}@uh.edu, xuleimath@gmail.com, lin.chen@ttu.edu
§ Auburn University at Montgomery,USA, ¶ IoTeX,USA, ‖ Korea University,South Korea
xinxin@iotex.io, suhtw@korea.ac.kr

2023 IEEE International Conference on Blockchain and Cryptocurrency (ICBC) | 979-8-3503-1019-1/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICBC56567.2023.10174906

Abstract—**Trusted execution environment (TEE) technology has many uses, such as protecting data in the cloud and improving security for industrial IoT. However, there are technical challenges that limit its widespread adoption. These challenges include the fact that different TEE vendors have incompatible solutions, and devices equipped with the same TEE technology may belong to different owners, making it difficult to establish trust between them. To address these challenges and fully utilize TEE technology, a decentralized coordination mechanism called DHTee is proposed. DHTee uses blockchain technology to support key TEE functions in a heterogeneous TEE environment, especially attestation service. Devices equipped with TEE can interact securely with the blockchain to determine whether potential collaborating devices meet the requirements. DHTee is also flexible and can support new TEE schemes without affecting existing TEEs.**

Index Terms—**TEE, blockchain, heterogeneous**

I. Introduction

New computing paradigms and application scenarios such as cloud computing and edge computing, smart manufacturing [1], federated machine learning [2], and general data trading [3] emphasize resource sharing and collaboration, leading to improved system efficiency, flexibility, and robustness. However, collaborative computing brings security and privacy challenges. Various techniques have been developed to mitigate these challenges, including cryptographic tools like fully homomorphic encryption [4] and secure multi-party computation [5], and access control and isolation mechanisms. Trusted execution environment (TEE) technology offers a good balance between security assumptions, functionality, and performance. Several TEE solutions have been proposed, such as Intel SGX [6], AMD SEV [7], ARM TrustZone [8], RISC-V [9], and Nvidia H100 GPU TEE [10]. However, the fragmentation of the TEE ecosystem makes it hard to build a heterogeneous TEE system, which reduces the capability of resource sharing and collaborative computation. A straightforward approach to mitigate this challenge is to modify each device to add support for other devices' TEE systems.

To overcome these limitations and further unleash the potential of TEE technology, we propose DHTee, which utilizes blockchain as the coordination and storage backbone to support the interoperation of devices with different TEE technology. A device only needs to be modified to support this common format to interact with other devices in the ecosystem. When a new type of TEE scheme is introduced, only the blockchain system needs to be updated and will not affect existing devices. DHTee brings several benefits: (i) It offers a unified framework to support heterogeneous TEE systems; (ii) It reduces the system management complexity and can easily support new TEE systems; (iii) It eliminates the single point of failure in the attestation process; and (iv) It protects information stored on the blockchain without affecting the function to support heterogeneous TEEs. In summary, our contributions in the paper include:

- We clarify the essential requirements on the design of a heterogeneous TEE system.
- We propose the detailed design of DHTee that leverages blockchain technology to support the collaboration of multiple TEE schemes.
- Analysis and evaluations are done to demonstrate the security and practicability of DHTee.

II. Overview of DHTee

This section provides an overview of DHTee and outlines its design goals.

A. Major Participants

Fig. 1 provides an overview of the abstract structure of DHTee, and there are mainly two types of participants involved:

- *Devices*. The system consists of multiple computation devices equipped with different TEE solutions, owned and managed by different entities. They work together to complete a secure computing task, exchanging results between TEEs without leakage to non-TEE devices, as required by the task.
- *Blockchain*. The system uses a blockchain as a coordinator between devices and for attestation services. Blockchain nodes run a consensus protocol, and only authorized nodes maintain the permissioned blockchain, which has a public/private key identity system.

B. Assumptions and Design Goals of DHTee

Design goals of DHTee. DHTee is designed to support the interoperation of heterogeneous TEE schemes, and devices

979-8-3503-1019-1/23/$31.00 ©2023 IEEE

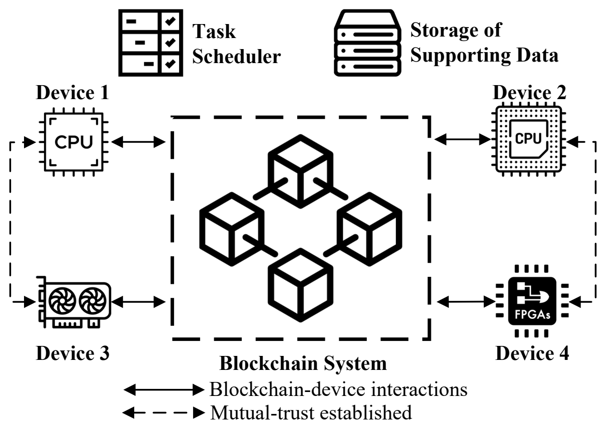

Fig. 1. High level architecture of DHTee. Each computation device has its own TEE hardware and protocols. These TEE schemes are not compatible with each other for different reasons. When two devices need to collaborate to finish a computation task, they establish mutual trust with the help of the blockchain system and TEE schemes, i.e., the devices verify each other's execution environment even if they use different TEE schemes, and establish a shared secret key for information exchange. After mutual trust is established, the two devices can interact directly without relying on the blockchain.

of the same TEE but managed by different stakeholders. Concretely, the design goals of DHTee include: (i) Multiple devices with different TEEs can collaborate to provide a unified trusted execution environment to finish a computation task; (ii) Devices with new TEEs can be added to DHTee easily to work with existing devices, and existing devices do not need to be modified; and (iii) The unified TEE created by DHTee offers all security features supported by a typical TEE scheme.

Technical challenges of DHTee. There are two major challenges for DHTee to support a heterogeneous TEE system and achieve the design goals, both of which are related to the remote attestation process. (i) Compatibility of the root of trust. A TEE is identified by a public/private key pair, which is issued and endorsed by a corresponding root-of-trust (RoT). However, two identities issued by different RoTs for two TEEs cannot be recognized by the other device. Therefore, they cannot establish mutual trust. (ii) Compatibility of data formats. A TEE solution has its own format to describe the execution environment (e.g., software stack and hardware information), which is used for attestation reports. Two devices equipped with different TEEs cannot understand each other's attestation report.

Assumptions. The design of DHTee relies on several assumptions, which are summarized as follows:

- *Permissioned blockchain.* The blockchain stores various device information and only permissioned blockchain is considered in the design of DHTee.
- *Attribute equivalence.* The attestation report of a TEE includes software/hardware attributes. Equivalent relationships exist between attributes of different TEE schemes, such as two attributes that represent the same software on different hardware platforms.
- *Common cryptographic suites.*All devices support symmetric encryption (e.g., AES) and key exchange (e.g., Diffie-Hellman) for secure direct information exchange after mutual trust is established.
- *Simplified TEE key architecture.*A TEE scheme can have multiple key pairs derived from various sources, but DHTee assumes a device uses a single key pair for identification and attestation endorsement.

III. Analysis and Evaluation

This section analyzes the security features of DHTee and evaluates its performance.

A. Security Analysis

Compared with existing TEE schemes that work for the same type of devices, DHTee mainly modifies three places in the TEE design: enrollment, the attestation report verification, and verification of the verification result. Assuming all existing TEE schemes involved in DHTee are secure, we only need to argue that these modifications do not introduce new vulnerabilities.

Security of the enrollment. DHTee offers two methods for device enrollment: (i) Vendor-provided public key, assuming an honest vendor who supports third-party attestation service, or (ii) Physically obtaining the public key from the device, provided the device hardware is free of trojans and backdoors and the physical connection is secure against attacker control.

Security of attestation report verification. When a device generates an attestation report, it is submitted to the blockchain for verification. Each blockchain node verifies the report's validity using the associated public key and digital signature. The consensus mechanism ensures that only correct verification results are included in the trusted blockchain.

Security of the verification result. For a classical TEE scheme, the device obtains the result from the attestation service and verifies its digital signature on the result. With DHTee, the major difference is that the device fetches the result directly from the blockchain, which is a distributed system. DHTee guarantees that a transaction the device obtained has been included in the blockchain.

In summary, DHTee achieves the design goals of supporting heterogeneous TEE without sacrificing security.

IV. Conclusion

Providing a unified and transparent TEE that includes various computation devices is important for a large range of security-sensitive tasks that require the collaboration of multiple types of devices. In the cloud environment, this capability also gives the service provider more flexibility to schedule tasks. The design of DHTee addresses two major obstacles in the construction of a heterogeneous TEE by utilizing the emerging blockchain technology. Furthermore, DHTee minimizes the modification of existing TEE schemes and only relies on a small set of assumptions.

References

[1] L. Xu, L. Chen, Z. Gao, H. Moya, and W. Shi, "Reshaping the landscape of the future: Software-defined manufacturing," *Computer*, vol. 54, no. 7, pp. 27–36, 2021.

[2] Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated machine learning: Concept and applications," *ACM Transactions on Intelligent Systems and Technology (TIST)*, vol. 10, no. 2, pp. 1–19, 2019.

[3] F. Liang, W. Yu, D. An, Q. Yang, X. Fu, and W. Zhao, "A survey on big data market: Pricing, trading and protection," *Ieee Access*, vol. 6, pp. 15 132–15 154, 2018.

[4] Z. Brakerski and V. Vaikuntanathan, "Efficient fully homomorphic encryption from (standard) LWE," in *IEEE 52nd Annual Symposium on Foundations of Computer Science - FOCS 2011*, R. Ostrovsky, Ed. IEEE Computer Society, 2011, pp. 97–106.

[5] Q. Ma and P. Deng, "Secure multi-party protocols for privacy preserving data mining," in *Wireless Algorithms, Systems, and Applications - WASA 2008*, ser. LNCS, Y. Li, D. Huynh, S. Das, and D.-Z. Du, Eds., vol. 5258. Springer Berlin Heidelberg, 2008, pp. 526–537.

[6] *Intel Software Guard Extensions Programming Reference*, October 2014. [Online]. Available: https://software.intel.com/sites/default/files/managed/48/88/329298-002.pdf

[7] J. P. David Kaplan and T. Woller, "Whitepaper: AMD memory encryption," April 2016.

[8] ARM, "Arm security technology building a secure system using trustzone technology," 2009.

[9] T. Lu, "A survey on risc-v security: Hardware and architecture," *arXiv preprint arXiv:2107.04175*, 2021.

[10] A. C. Elster and T. A. Haugdahl, "Nvidia hopper gpu and grace cpu highlights," *Authorea Preprints*, 2022.