PRIVACY AND SECURITY

This column delves into privacy risks of the IoT using risk concepts that are more native to the security domain in order to conceptually bridge our collective understanding, articulation, and management of privacy concerns in the IoT which otherwise might not be sufficiently considered or foreseen by existing legal and technical controls.

INTRODUCTION

COLUMN EDITOR
Erin Kenneally

This issue's guest column takes a crack at resolving tension between privacy, security, and pragmatic innovation in the IoT using Distributed Ledger technology. The described Off-Chain Trusted Computing solution is a promising path forward- it is based on a standard specification and addresses the scalability criticisms that hinder DLT deployment. Testing, evaluating, and implementing these types of trust-by-design approaches put forth by the authors are critical to achieving the promise of IoT innovation.

OFF-CHAIN TRUSTED COMPUTING

by Lei Zhang, Sanjay Bakshi, and John K. Zao

Trustworthiness and privacy are of primary concern as companies connect their manufacturing and logistic infrastructures to the Internet of Things (IoT). They want to reap the benefit of automated asset management, process control and predictive maintenance. However, to do so effectively, companies need to facilitate information sharing among trustworthy partners while complying with data protection and privacy preserving regulations. In this respect, Distributed Ledgers (a.k.a. Blockchains) offer a viable solution by enabling their participants to discover one another and establish peer-to-peer trust relations without a centralized intermediary. Nonetheless, this approach comes with a caveat: Blockchains may not scale well. Since each Blockchain-based transaction must be attested by multiple Blockchain participants, it may take time to complete a transaction. Besides, since each transaction is processed by multiple participants, information privacy is sacrificed in exchange for Byzantine fault tolerance and trustworthiness of the results. To overcome these shortcomings of on-chain computing, *Off-Chain Trusted Computing* was devised to offload the bulk of transaction workload to the Trusted Execution Environments (TEEs) established in the off-chain computing nodes that are trusted by the Blockchain participants, leaving only the execution of business logic to on-chain computing. This hybrid approach greatly increases the efficiency and speed of the transactions. Moreover, by concealing the input and output of the TEEs with data encryption and verifying the states of transaction execution in the TEEs through remote attestation, Off-Chain Trusted Computing can preserve the information privacy of data providers and confirm the proper execution of the business logic. This column provides an introduction to this new technology by explaining its operation, surveying its standardized application programming interfaces (APIs) and mentioning an example application.

HOW DOES OFF-CHAIN TRUSTED COMPUTING WORK?

In on-chain computing, application programs are encapsulated in Smart Contracts and executed by multiple Blockchain participants. Trustworthiness of the computing results depends on the majority consensus reached among the participants. As mentioned, such a process can be resource draining and time consuming; besides, information privacy is hard to maintain as multiple participants are involved in the computation. Off-Chain Trusted Computing is a new hybrid computing paradigm, in which the profiles of the application programs, the trusted computing nodes (a.k.a. the *Workers*) capable of establishing Trusted Execution Environments (TEEs), and the available datasets are all maintained by the Blockchain. Execution of the application programs is performed by the trusted Workers, instead of the Blockchain participants. The roles of the participants are mainly to monitor and coordinate the application program execution as well as to audit and conduct the financial transactions to pay for these on-line services. Instead of encapsulating the application programs, the Smart Contracts are used to specify the business logic such as the use policies of the datasets and process the transaction tokens such as the Work Order and the *Work Order Receipts* that initiate the transaction and the payment process.

In an Off-Chain Trusted Computing (TC) system, *Workers* capable of establishing TEEs and offering TC services are grouped into Pools, each managed by a Blockchain participant, known as a *Worker Pool Administrator*. Each Worker possesses a pair of asymmetric keys: the private key shall be kept within its cryptographic hardware while the public key, in the form of a signed certificate, shall be registered with the Blockchain and can be fetched by any user of the TC services. Together, the key pair can be used to authenticate the Worker and perform key management on behalf of its TEEs.

In order to protect information privacy, each dataset shall be encrypted with a random symmetric key. The encrypted dataset can then be kept in a public storage. The data encryption key, on the other hand, shall be dispatched to the Worker chosen to perform the trusted computation under the protection of the Worker's asymmetric key pair.

Once the Workers and the datasets are in place, a user may go through the following steps to obtain a privacy-preserving TC service using a chosen application program, running in a chosen Worker's TEE, processing the encrypted datasets.

1. To start a transaction, a user must submit a Work Order specifying the requested TC service and its execution conditions; the user must also deposit sufficient credits to pay for the service.
2. Blockchain participants execute a Smart Contract with the user's Work Order as input in order to verify whether the requested TC service satisfies the use policies of the application programs, the Workers and the datasets.
3. If the request satisfies the use policies, then:
   a. The user's credits are reserved to pay for the TC service.
   b. A Blockchain Event is issued to a Worker Pool Administrator to trigger the TC operation.
   c. A Worker is assigned by the Worker Pool Administrator to perform the trusted computation; a TEE is then established in the Worker to carry out the computation.
   d. The encrypted datasets are moved into the TEE and then decrypted using the data encryption keys.
   e. After verifying its authenticity, the chosen application program is also imported and executed in the TEE. The program shall process the decrypted data and produce the results within the confines of the TEE so that its execution cannot be tampered by any entity, including the Worker and its Administrator.

f. When the execution is completed, the results are encrypted within the TEE using the result encryption key, another symmetric key established with the user. The Worker then issues a Work Order Receipt through the Worker Pool Administrator.
g. The Work Order Receipt, which includes a hash of the final state of the program execution, shall be verified by the Blockchain participants in order to confirm the successful completion of the TC operation.
h. If the successful completion of the TC operation is confirmed, then the Smart Contract shall proceed to complete the payment process. The user shall be able to download and decrypt the results of the TC operation.

4. If the Work Order fails to satisfy the use policies or the Work Order Receipt fails to confirm a successful completion of the TC operation, then the user's request is cancelled and the deposited credit is refunded.

Since the application program is verified and executed in a TEE established within a verified and trusted Worker under the instructions of Smart Contracts executed collectively by the Blockchain participants, the *trustworthiness* of the computing process is assured. Furthermore, since the data going into and the results coming out of the TEE are concealed by encryption, the *privacy* of the information is preserved.

What is in the EEA Off-Chain Trusted Compute Specification?

In May 2019, Enterprise Ethereum Alliance (EEA) released its Off-Chain Trusted Compute Specification v.1.0[1] laying down the foundation for Off-Chain Trusted Computing operation. The specification offers a set of standardized application programming interfaces (APIs) to create, inspect, share and re-use application programs for Blockchain transactions that require privacy, oracle services or computation-intensive workload. The specification is compatible with Trusted Execution Environments (TEE), Zero-Knowledge Proofs (ZKP) and Trusted Multi-Party-Compute (MPC).

Relevant to our topic, this specification also lays out the following workflows aiming at preserving trustworthiness and privacy:

1. Register Pools of Trusted Workers with the Blockchain based on asymmetric cryptography.
2. Specify the Work Order APIs for offloading on-chain computing to off-chain trusted execution environments (TEEs) while maintaining a high degree of trustworthiness.
3. Preserve the privacy of the processed data and the program execution states when the program is executed in the off-chain TEEs.
4. Specify the Work Order Receipts APIs for generating hardware-based attestation of execution states within the TEEs, which can be verified by the Blockchain participants to verify the trustworthiness of the off-chain execution.

An Example Application

Since the release of the EEA Off-Chain Trusted Computing specification, several Trusted Worker pools have been created for applications in smart factories, smart cities, AI model sharing, medical data sharing and 3D rendering data protection. At the Mobile World Congress 2019, Intel and iExec, two main contributors to the specification, demonstrated a decentralized service that helps a fleet of rescue robots to find the safe paths to search for and reach two lost robots. A Marketplace of Smart Contracts was created to aid trusted discovery and transaction settlement. The Smart Contracts enabled mutual authentication among the robots and ensured the reach of a decentralized consensus on the result of the transactions. To ensure scalability and data privacy, the Smart Contracts offloaded the AI computing to an Intel SGX enclave. Upon the completion of the rescue task, the marketplace carried out a payment from the users owning lost robots to those with the rescue robots for the services they offered.

Conclusion

Off-Chain Trusted Computing offers viable ways to offload computation intensive execution from Blockchain participants to trusted computing nodes. With the aid of Confidential Computing,[2] it can also support privacy-preserving information processing. This and other emerging applications will foster the advent of data economy.

Biographies

Lei Zhang is currently leading the security team at iExec, France, to build blockchain-based trusted cloud computing. He is one of the main editors of the worldwide trusted compute standard: EEA (Enterprise Ethereum Alliance) Trusted Computing specification. He leads/participates in several Working Groups on Security and Blockchain in IEEE. He received his Ph.D. degree in computer science from the Universite de Toulouse and NICTA (National ICT of Australia) in 2009. He has multiple U.S./international patents on Security and wireless communications. His expertise focuses on cyber-security, cloud computing, and Internet of Things. He participates and leads several International and European projects on cloud and cyber-security.

Sanjay Bakshi (sanjay.bakshi@intel.com) is a board member and a Co-chair of the Technical Steering Committee at the Enterprise Ethereum Alliance. At work, he is a Principal Engineer at Intel leading the Edge Data Privacy innovation team. He is an expert in Edge computing, Blockchain, Internet of Things, Confidential Computing, Privacy and Cyber Security. He holds 37 issued patents.

John K. Zao [SM]] (jkzao@ieee.org) is the founding chair of the IEEE Standard Working Group on Edge/Fog Computing and Networking Architecture Framework and the founding vice-chair of the IEEE Standard Committee on Edge/Fog/Cloud Communications with IoT and Big Data. He is also a co-chair of the Security Working Group and the Distributed Computing Task Group of the Industrial Internet Consortium (IIC). He is the Director of the Intelligent Edge/Fog Computing Research Center at National Chiao-Tung University in Taiwan. He is also a founder of NGoggle Inc. in San Diego, USA, which developed an EEG augmented VR goggle for neural monitoring and rehabilitation based on visual stimulation. He received his PhD in Computer Science at Harvard University in 1995 and was elected a Senior Member of IEEE in 2001.

Footnotes

[1] https://entethalliance.org/enterprise-ethereum-alliance-releases-dff-chain-trusted-compute-specification-1-0/

[2] https://searchcloudcomputing.techtarget.com/definition/confidential-computing.

Column Editor Biography

Erin Kenneally (erin@elchemy.org) is the Director of Cyber Risk Analytics at Guidewire-Cyence, where she provides cyber risk strategic advisement for data-driven research innovation, risk analytics and modeling technology solutions. She most recently transitioned from Portfolio Manager in the Cyber Security Division for the U.S. Department of Homeland Security, Science & Technology Directorate. She previously served as Technology-Law Specialist at the International Computer Science Institute (ICSI) and the Center for Internet Data Analysis (CAIDA) and Center for Evidence-based Security Research (CESR) at UC San Diego. She also founded and is CEO of Elchemy, Inc.. She is a licensed attorney specializing in information technology law, including privacy technology, data protection, AI and autonomous systems ethics and legal risk, trusted data sharing and governance, technology policy, and emergent IT legal risks. She holds Juris Doctorate and Masters of Forensic Sciences degrees and is a graduate of Syracuse University and the George Washington University.