Blockchain-enabled IoT for Privacy-Preserving Computation Capabilities in Untrusted Environments

Youakim Badr
youakim.bdr@insa-lyon.fr
INSa de Lyon

Context:
The Internet of Things (IoT) as a concept is fascinating and exciting, but one of the major challenging aspects of IoT remains its cyber-security. The key to secure the IoT relies on our understanding of different IoT building blocks and how to assess vulnerabilities in each block in order to mitigate risks. A typical IoT architecture can be represented by four building blocks: Things or connected devices, which are defined as uniquely identifiable nodes (sensors or actuators); Gateways, which act as act as intermediaries between things and the cloud and ensure connectivity, security, and manageability; Network infrastructure which include routers, gateways, repeaters and other devices that control and secure data exchange; Cloud infrastructure which comprises virtualized servers to ensure storage, computing and analytical capabilities.

Existing security technologies will play a role in mitigating IoT risks at each building block but they raise several challenges when we attempt to exchange data securely and enable computation in untrusted environments. Challenges are due, and not limited to [5, 6]:

**Limited resources:** IoT devices have unconventional characteristics such as limited and constrained resources (computational and storage resources, connectivity and batteries). Many “IoT devices” and platforms use simple processors and operating systems. As a result, they may not support sophisticated security approaches and thus cannot be protected from information attacks, physical tampering, denial-of-service attacks and impersonating “things” or denial-of-sleep attacks that drain batteries.

**Centralized IoT networks:** IoT platforms are often built on centralized communication models relying on the server/client paradigm. All devices are thus identified, authenticated and connected through cloud servers. As a result, connections between devices have to exclusively go through the internet, even if devices are located closely. While this model has connected small-scale IoT networks as we see them today, it will not be able to scale to large IoT networks of tomorrow in which tens of billion of devices are connected. In addition, IoT devices and platforms have to reply on third-party service providers to manage device identities, authentication and access controls. Thus, centralized clouds and large server farms become not only point of failure that can disrupt the entire network but also subject censorship and security attacks since they retain confidential information about devices and/or user credentials. They also become significantly very expensive due to the costs associated with their installation and maintenance.
Objective:
A decentralized approach to IoT networking that relies on the peer-to-peer communication model would solve many of the before mentioned challenges. It can process hundreds of billions of transactions between devices that form IoT networks, distributes computation and storage needs across the billions of devices and prevents censorships and failure in any single node in a network from bringing the entire network to a collapse.

However, establishing peer-to-peer communications in huge IoT networks that maintains privacy and security will present its own set of challenges, such as:

1) Offering some form of computational capabilities to securely exchange data between devices or compute any functionality in a privacy-preserving manner;
2) Providing some form of validation and consensus for transactions to prevent spoofing and theft.
3) Offering a trustless environment in which the IoT does not rely on third-party providers to manage devices' identity, authentication and access control and thus avoid the leak of sensitive data and censorship.
4) Preventing failure in any single node in a network from bringing the entire network to a halting collapse.

In our research team, we are addressing challenges related to IoT trustless environment in which devices can manage identity, authentication and access controls based. We are developing a blockchain-based identity Management system and access controls without relying on third-party providers.

In this thesis, we focus on developing an IoT computational platform to securely exchange data between devices and extend connected device capability to compute any functionality in a privacy-preserving manner. For example, a set of apartments’ electrical meters in a smart building can jointly compute their maximum power consumption over their inputs while keeping those inputs private. To this end, we would like to develop a platform that settles privacy-preserving computation (a.k.a secure multi-party computation) and enforces security concerns in trustless and peer-to-peer IoT networks.

Any decentralized privacy-preserving computational platform, must support foundational functions:

- Peer-to-peer messaging;
- Autonomous device coordination
- No centralized authority control
- Perform privacy-preserving operations on devices’ data while keeping the inputs private at all times.
- Ensure operation scalability with distributed computing;
- Privacy-preserving operations’ automation based on devices’ shared states
Research Methodology
In order to build such privacy-preserving platform in peer-to-peer IoT networks, we are particularly interested in challenges related to the application of two different, yet complementary topics: the secure computation paradigm [4] and blockchain technology [3]. The goal in this research is to simultaneously take secure multi-party computation from the realm of theory to practice and blockchain technology from finance to the IoT era. Our motivations behind the secure multi-party computation and blockchain are following:

1) Blockchain is the underlying technology of crypto-currencies and presents today an object of intense interest in the finance industry and beyond (IoT, ownership, ...). Roughly speaking, blockchain is a database for decentralized and transactional data sharing across a large network of untrusted participants who find agreements on their shared states without trusting a central authority. Blockchain maintains a continuously growing set of data records. A blockchain consists of: transactions, which are the actions created by the participants and blocks, which record transactions and make sure they have not been tampered with. The blockchain has many remarkable characteristics such as tamper-proof, immutable records, decentralized, autonomous, and trustless capabilities. These capabilities open the door to a series of IoT security mechanisms that were remarkably difficult, or even impossible to implement without blockchains.

2) The secure multi-party computation is a subfield of cryptography with the goal of jointly conducting computation tasks based on private inputs. Cryptographic applications, such as encryption or signatures are the foundation of Blockchain but they are not sufficient to ensure securely cooperative computation operations that can be computed, with security against malicious adversaries. One of the most exciting capabilities of the secure multi-party computation is dealing with different adversarial powers (semi-honest or malicious connected devices) that are willing to deviate from the secure multi-party computation protocol.

Recent initiatives attempt to couple Bitcoin and secure computation. Bentov et al. propose a "model of fairness in secure computation in which an adversarial party that aborts on receiving output is forced to pay a mutually predefined Bitcoin monetary penalty [1]. Guy Zyskind develops a general-purpose secure computation platform that relies on blockchain (Bitcoin) for efficiency and scalability [2]. In these works, utilizing the blockchain technology is only limited to secure multi-party computing MPC and not applied to IoT platforms.

A privacy-preserving computational platform needs to be built as a foundation of trustless and scalable peer-to-peer IoT networks, with unprecedented collaboration, coordination, and secure connectivity for each block of the IoT architecture and without centralized controls.
Bibliography:


