Proposition de recherche doctorale

Etude et mise en ouvre de formalismes à base de Blockchain pour la protection de données en environnement distribué

Mots clés :
- Directeur de thèse : salima BENBERNOU
- Co-encadrant(s) :
- Unité de recherche : Laboratoire d'Informatique PAris DEscartes
- Ecole doctorale : École Doctorale Informatique, Télécommunications, Électronique de Paris
- Domaine scientifique principal: Divers

Résumé du projet de recherche (Langue 1)

The massive growth of digital universe is promoting various types of risks. Of all types, security is critically important and becoming significant concern to different types of users including industries and individuals. Security includes several entities: hardware, software, network, and data. The increasing trend of using a wide variety of devices increased security threats because these devices provide an opportunity to the adversaries to access these devices. Additionally, the paradigm such as Internet of Things (IoT) are used today to build hyper-connected ecosystem that includes these applications and physical devices. This essentially has increased vulnerability of digital ecosystem or data security threats because the hyper-connection has opened affluent gateways for adversaries to access to user data. This project concerns of data security. Security has drawn an enormous interests to researchers and industry practitioners. They are investigating state of the art technologies to find shortcomings and develop new approaches for guaranteeing security of data. However, the advent of Big Data has given rise to different security challenges concerning data: securing computations in distributed programming framework, securing relational data stores, secure data storage and transactions logs, End-point input validation/filtering Real - time security, compliance monitoring, Scalable and composable privacy - preserving data mining and analytics, cryptographically enforced access control and secure communication, granular access control, Granular audits, data provenance. Although there is an exhaustive list of technologies for securing data, it remains a problem specifically if data is distributed collected multiple heterogeneous sources, distributed within and across a large number of nodes, and accessed by massive number of users. Technologies such as Blockchain is gaining popularity within the realm of security to specifically to secure large volume of data stored in different data centers. Blockchain is perceived as a promising technology for securing data distributed in different data centers. In Blockchain, unlike conventional approaches where security of data are certified by single third party authority is not allowed, the approval any changes has to be agreed by multiple distributed authorities. Such decentralized authentication approach would prevent any unauthorized access, modification in data. However, there are several challenges that must be addressed to adopt block in data intensive distributed systems including performance and complexity. This project focuses on how to leverage the power of blockchain in securing data that are stored in decentralized/distributed cluster and accessed by number of users.

Résumé du projet de recherche (Langue 2)

Blockchain offers various opportunities for guaranteeing data security such as immutability of ledger. However, there are several limitations of Blockchain technology which must be addressed to exploit it for data security in distributed environment. Some of the major challenges are enlisted in the following: performance, privacy, immutability, etc. we will focus on privacy. Blockchain is believed to be safe as users only make transactions with generated addresses rather than real identity. Users also could generate many addresses in case of information leakage. However, that blockchain cannot guarantee the transactional privacy since the values of all transactions and balances for each public key are publicly visible. Moreover, Multiple methods have been proposed to improve anonymity of blockchain. But it is still a challenging issue.