* Security / Identity
* IoT & Blockchain

Blockchain & IoT

With the consequent explosion in the volume of data produced by smart devices have led to the outsourcing of data to designated data centers. To manage the huge data stores, centralized data centers such as cloud storage cannot afford auspicious rapid growth in the diversity and number of devices connected to the internet. Also, the cloud storage’s convenience has blinded us to the extent that we now place too much trust in third parties. Due to a lack of good points of reference and low costs, we are obliged to trust these third parties to secure our most private and sensitive data, which are mostly unencrypted.

The author builds a novel block chain-based distributed cloud architecture with a software defined networking enable controller fog nodes at the edge of the network to meet the required design principles

The second article author want to construct a secure and auditable IoT data management system. He divides the system into 3 levels, Data plane (DHT, Cloud), Control plane(BlockChain), IoT devices & Services.

I want to talk about the DHT (Distributed Hash Table), it serve as a scalable, self-managing storage with high availability. I think in this field, this technology is very suitable to be the store interface to store the private key.

How to improve the system:

Full decentralization and true redundancy:

build a distributed cloud data storage across the globe, it is extremely difficult to cause significant disruptive.

Facilitates resource usage:

running the on-demand resource algorithm from the smart contract to facilitate the use of resources on demand simply.

Complete privacy:

It is possible to achieve complete privacy without any third party having access to and control of the data.

Improves the quality-of-services:

Offer traceability of the use of resources in order to properly verify the service level agreement by both the client and the service provider.

Cost reduction:

Efficiency

In my opinion, it should add some incentive mechanisms into the smart contract, also they should think about the block size of the system, there must be huge amount of data in the system, how to keep the system run efficiently, maybe they should use private block chain to accelerate the speed of confirmation.

Reference:

[1] Xu Q., Aung K.M.M., Zhu Y., Yong K.L. (2018) A Blockchain-Based Storage System for Data Analytics in the Internet of Things. In: Yager R., Pascual Espada J. (eds) New Advances in the Internet of Things. Studies in Computational Intelligence, vol 715. Springer, Cham

[2] Hossein Shafagh, Lukas Burkhalter, Anwar Hithnawi, and Simon Duquennoy. 2017. Towards Blockchain-based Auditable Storage and Sharing of IoT Data. In Proceedings of the 2017 on Cloud Computing Security Workshop (CCSW '17). ACM, New York, NY, USA, 45-50. DOI: https://doi.org/10.1145/3140649.3140656

[3] Sharma, Pradip & Chen, Mu-Yen & Hyuk Park, Jong. (2017). A Software Defined Fog Node based Distributed Blockchain Cloud Architecture for IoT. IEEE Access. PP. 1-1. 10.1109/ACCESS.2017.2757955.

Blockchain & security

In the first article, it mainly talk about the security of the data in the IoT which I described in the first part, I will pay more attention on ways to enhance the security. The main method used by the attacker is they will make various attempts to access a user’s personal key stored in the user’s computer or smartphone.

The author want to combine blockchain with cloud computing environment. User anonymity can be ensured if the blockchain method is used when saving the user information in the cloud computing environment.

In my opinion, I do not prefer the way to use cloud computing as the environment of a blockchain-based electronic wallet. It need blockchain method to be used to remove the information of the user who uses cloud computing, it is not safe to the data, there still some possible that someone may steal the information from the system.

The second article talk about the tradeoff between provable security and transaction processing speed. It introduces a new formal property of blockchain protocols, called chain growth which based on trees and it shows its power by substantially improving the security bounds of the bitcoin backbone, also it did analyze of the GHOST backbone protocol.

During reading this article, I learned a lot from the function and terminology the author list, I think it is a great article which need me to read it several times to understand it.

Reference:

[1] Park, J.H.; Park, J.H. Blockchain Security in Cloud Computing: Use Cases, Challenges, and Solutions. *Symmetry* **2017**, *9*, 164.

[2] Kiayias, A., & Panagiotakos, G. (2015). *Speed-Security Tradeoffs in Blockchain Protocols*.