Proposal 4

Instigators: Abderrahim Benslimane and Julio Perez, Avignon University, France

Title: BlockChain to secure Internet of Things: FPGA implementation

Summary of the proposal

Due to the increasing number of Internet-connected devices, their high connectivity, diversity, heterogeneity, and inability to support complex and cumbersome security protocols, a number of security and privacy challenges arise. So, we consider using BlockChain for the security of Internet of Things (IoT) since we think it will bring a lot of benefits. However, there are still several challenges to be raised regarding security, storage and privacy. We proposed a new generic IoT architecture BlockChain-based to provide robust security with unlimited cloud storage capacity that can be adapted to IoT resource constraints by introducing a new security and storage management component into the BlockChain.
Furthermore, consensus protocols, used in the mining of BlockChain to find the right hash and to preserve the integrity of the network, spend a lot of time, energy and resources. Low-capacity IoT equipment is unable to perform these BlockChain actions. We plan to implement a new consensus protocol light and fair for IoT devices with an intermediate layer above IoT layer.

Our objective in this project is to use FPGA (Field Programmable Gate Arrays) to implement computational solutions and simplify the complexity related to the Blockchain in IoT.

Related Work

Authors in [1] have proposed a decentralized IoT data management using BlockChain and trusted execution environment “Intel SGX”, to ensure data security and privacy for the system. However, the disadvantage of using SGX is its limited memory. SGX is a set of processor extensions to Intel's x86 design that allows the creation of isolated execution environments called enclaves, and these enclaves reside in a hardware guarded area of memory called the Enclave Page Cache (EPC). The EPC is currently limited to 128 MB [2]. Moreover, their solution doesn’t resolve the scalability concern, so their system may be applied only if the data are not needed immediately and the functions are executed at a later time in the BlockChain. Also, The IoT gateways are the ones which store the hash of the data in the BlockChain and the main data in SGX. So, it is like if the data is sent from the IoT devices to the SGX without passing throughout the BlockChain.

Therefore, our proposed work differs from their architecture since our research work sends the data to the BlockChain and the new component (SSM) which reside in the BlockChain is the one who manages and stores the data in unlimited place which is the cloud.

Work in [3] introduces for IoT-BlockChain applications, a distributed data storage framework, which ensures that the ownership of the IoT data stays with the stakeholders.

Work in [4] presents the gaps in the current methods of security and privacy, and propose LSB which is a scalable and lightweight BlockChain for IoT, relating to security and privacy. Those lightweight LSB protocols reduce the bandwidth and computation costs.

However, in both [3] and [4], architectural details and performance implications are not addressed particularly, for the resource-constrains of IoT platforms.

Authors in [5] have proposed a new distributed BlockChain cloud architecture which is based on BlockChain, fog computing and SDN. It provides an efficient solution for managing the data which are produced by the IoT devices in the distributed cloud and also at the edge of the network. However, their model lacks to explore the several energy technique aspects.

Therefore, in our previous work we proposed a different architecture since it sends the data to the Blockchain and the new component that resides in the Blockchain is the one that manages and stores, securely, data in the cloud with unlimited storage space [6].

Plan

- Use the FPGA for hash calculation and secure communication, knowing that FPGA allows better flexibility than the CPU and GPU. Various FPGA hardware alternatives will be studied, from tinyFPGA to Soc FPGA for IoT devices, and Netfpga for high-end infrastructure nodes. FPGAs are designed to consume less energy than other integrated circuits, making mining very cost-effective. In addition, FPGA can be configured to compute different cryptocurrency-specific algorithms, allowing miners to switch from extracting one type of currency to another. The mains issues to be lifted are mainly concerned with the performance of the system and the costs of installation.
- The FPGA model will be communicate to the students to prepare the algorithms and the programming language to be used.
- Implementation on the FPGA

  Evaluations taking into account different parameters such as latency, capacity, processing, energy, etc.
- Final report and prototype demonstration.

References

1. F. A. Alaba, M. Othman, I. A. Targio Hashem, and F. Alotaibi, “Internet of things security: A survey,” Journal of Network and Computer Applications, vol. 88, pp. 10–28, 2017.
2. G. Ayoade, V. Karande, L. Khan, and K. Hamlen, “Decentralized IoT Data Management Using BlockChain and Trusted Execution Environment”, IEEE International Conference on Information Reuse and Integration (IRI), 6-9 July 2018.
3. Ben A Fisch, Dhinakaran Vinayagamurthy, Dan Boneh , and Sergey Gorbunov, “Iron: Functional Encryption using Intel SGX”, ACM SIGSAC Conference on Computer and Communications Security, October 2017.
4. H. Shafagh, L. Burkhalter, A. Hithnawi, and S. Duquennoy, “Towards BlockChain-based Auditable Storage and Sharing of IoT Data,” *NSDI 2017 - 14th USENIX Symposium* on *Networked Systems Design* and. *Implementation*, Mar *2017*, Boston, USA.
5. A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, “LSB: A Lightweight Scalable BlockChain for IoT Security and Privacy,” IEEE Symposium on Security and Privacy, 2017.
6. Pradip Kumar Sharma, Mu-Yen Chen, Jong Hyuk Park, “A Software Defined Fog Node based Distributed BlockChain Cloud Architecture for IoT”, IEEE Access, Volume 6, Pages: 115 – 124. September 2017.
7. S. Benouar, A. Benslimane, “Robust Blockchain for IoT Security”, IEEE Globecom 2019, CISS - Communication & Information Systems Security Symposium, IEEE Global Communications Conference, 9-13 December 2019, Waikoloa, HI, USA.