SHORT TERM SCIENTIFIC MISSION (STSM) – SCIENTIFIC REPORT

The STSM applicant submits this report for approval to the STSM coordinator

Action number: CA15127 (Resilient communication services protecting end-user applications from disaster-based failures (RECODIS)

STSM title: Blockchain based Proxy re-encryption scheme for IoT

STSM start and end date: 16/04/2018 to 27/04/2018

Grantee name: Mr Krzysztof Gierlowski

PURPOSE OF THE STSM/

Internet of Things (IoT) is one of the most exciting paradigms in emerging technology. It is experiencing exponential growth in both, research and industry. IoT is connecting billions of devices and sensors to automate networks and has considerable applications in virtually all mechanically intensive industries. In spite of all the advancements, privacy and security remains a top concern for the IoT ecosystem as it exposes huge amounts of data to security breaches. Decentralized architecture and resource constrained devices make IoT incapable to use conventional security approaches.

Blockchain, a distributed ledger technology has gained a lot of attention in areas beyond the cryptocurrency. It has been used to provide security and privacy in peer-to-peer networks with similar topologies to IoT. Internet of Things applications follows decentralized architecture by definition, it's normal that blockchain will play a role in how devices will communicate directly between each other. The distributed architecture of blockchain can help solve many of the IoT security and trust challenges. Blockchain is also well suited to provide IoT device identification, authentication and seamless secure data transfer. It eliminates a single source of failure within the ecosystem, protecting an IOT device's data from tampering. Blockchain can be used to track the sensor data measurements and prevent duplication with any another malicious data. IoT sensors can exchange data though a blockchain instead of going through a third party. The deployment and operation costs of IoT can also be reduced through blockchain since there is no intermediary.

IoT security and privacy are critical success factors for meeting the high expectations of the technology to transform many aspects of our society and economy. So, there is a requirement to build an IoT system using the blockchain which can provide authentication and secure data sharing between the entities. To solve these issues, the decentralized and consensus driven Blockchain and the combination of cryptographic processes behind it can offer an intriguing alternative.

DESCRIPTION OF WORK CARRIED OUT DURING THE STSMS

During the STSM, we discussed the different aspects of the implementation of this use case. We focused on developing a blockchain based architecture to securely store and share the sensor data between the entities. We considered five entities in the system: sensors' owner, user, cloud provider and the blockchain. The sensors' owner activates the sensors and provides each sensor smart contract with the required key material. The cloud server securely stores data from the sensors and transaction containing the address of the stored data is generated on the blockchain. This smart contract manages the financial transaction and also checks the corresponding requirements related to the data. When a user requests access to one of the sensors, the specific data is re-encrypted and decryption key along with address is provided using the smart contract.

After the architecture was finalized, I started the implementation of the proposed architecture. In the first part, blockchain related work was completed. Ganache client[1] was used as blockchain for Ethereum development. After its configuration, smart contracts rules were defined and implemented using the Solidity[2] v0.4.20. Truffle framework[3] was used to compile and deploy the smart contract on the Ethereum blockchain. Using Ganache, we can quickly see how our smart contract affects the blockchain, and also provides introspect details like accounts, balances, contracts interaction and gas costs.

In the second part, I focused on the implementation of the security mechanisms to be used as defined in the use case. The re-encryption scheme is based on Elliptic Curve Cryptography (ECC) allowing to offer lightweight public key cryptographic solutions. ECC was implemented on the Python v3.6.4 using the library pyca/cryptography[4]. After its implementation, pyethereum[5] library was used to connect to the Ethereum blockchain and to interact with the smart contracts deployed.

Links: -

1. https://github.com/trufflesuite/ganache-cli
2. https://solidity.readthedocs.io/en/v0.4.23/
3. https://github.com/trufflesuite/truffle
4. https://cryptography.io/en/latest/
5. https://github.com/ethereum/pyethereum

DESCRIPTION OF THE MAIN RESULTS OBTAINED

The main goal of the STSM was to define the blockchain based architecture for re-encryption of sensor data and its prototype implementation. After the minimum requirement for the implementation were completed the next phase was to layout the plan for evaluation of the prototype. We discussed the evaluation of the system. A detailed security and performance analysis was defined to demonstrate the scalability of the approach. In particular, we show how a very efficient proxy re-encryption scheme allows that the data is only visible by the owner and the person present in the smart contract.

The evaluation of the system will be divided into three main parts as following:

1. Security Analysis
   In this part we will list down benefits of using re-encryption scheme, Blockchain, possible attacks on the system and their prevention.
2. Scenario based performance evaluation
   The performance of the system will be evaluated by comparing the central authority system with the implemented prototype on the bases of time, packet overhead and throughput.
3. Regression Analysis
   The data collected from the performance evaluation will be used to perform the regression analysis using R studio.

The next phase of the project will be to evaluate the implemented prototype and publish conference article as soon as possible.

FUTURE COLLABORATIONS (if applicable)

After the successful implementation and evaluation of the idea. The main focus will be to publish the work in a renowned conference. There is also a possibility to extend this research work into a journal or publish more conference article by adding features such as

1. Access control List for the blockchain transactions.
2. Use of blockchain as an auditing service for the cloud servers.
3. Integration of more cryptographic functions in the blockchain.