Proof-of-Authentication for Scalable Blockchain in Resource-Constrained Distributed Systems

Problem:

Resource-constrained distributed systems such as the Internet of Things (IoT) are deployed for real-time monitoring and evaluation. Several security solutions involving cryptography exist for their applications mainly under asymmetric and symmetric cryptography. But in either case, there is always a central entity to initialize or process these security mechanisms. As a result, a single-point failure could compromise the whole system.

Motivation:

Current security solutions are problematic when there is a centralized controlling entity. Although the blockchain provides decentralized security architectures using proof-of-work (PoW) but Proof-of-work is an expensive process for IoT and edge computing due to the deployment of resource-constrained devices. The **Proof-of-Authentication** (PoAh) consensus algorithm presented in this paper tries to replace Proof-of-Work and introduce authentication in such environments to make the blockchain application-specific.

Methodology:

The Proof-of-Authentication system evaluates its sustainability and applicability for the IoT by conducting the evaluation process in both *simulation* and *real-time testbeds*. First, individual nodes in the network generate transactions (Trx) with the data or processes and combine them into a block. The nodes broadcast the blocks for further evaluation. Individual nodes are responsible for public and private key generation (PuK andPrK). This model uses the *ElGamal* method of encryption i.e. **y = g^x(mod p)**, where y is the *public key* and x is the *private key*.

Before node broadcast, the source node uses its private key PrK, i.e. x, to sign the block and makes its public key PuK, i.e. y, available to everyone. Once the block is received by the trusted node, it is processed to evaluate its authenticity by getting the source node public key, i.e. y. After signature validation, the trusted node also checks the MAC value for a second round of evaluation. After successful authentication, the trusted nodes broadcast the block to the network with PoAh identification. Following this, individual nodes in the network find the PoAh information from the block to add in the chain. Individual nodes compute the hash of the block and keep it to link the next block and the previously computed hash value is stored in the current block to maintain the chain

Results:

A. Simulation Evaluation

For this experiment, there is a total of five participants in the network with two miner/trusted nodes and the block size is fixed to 35 bytes, where multiple transactions are kept in one block. The simulation results indicate an average time for the Proof-of-Authentication of **3.34 seconds**. The average is computed from the PoAh time from 10 iterations.

B. Testbed Evaluation

The proposed Proof-of-Authentication is implemented in a real-time testbed to evaluate its sustainability. The testbed implementation includes five Raspberry Pis, where three Pis are associated with multiple sensors and the other two work as the trusted nodes to the network. With the process of Proof-of-Authentication, the Pis take an average of **3.8 seconds** while the total end-to-end time from block formation to becoming a part of blockchain is **4.4 seconds** concluded from 15 operations.

Future Work:

In the future work, the proposed PoAh algorithm can be analysed with bigdata sets in larger systems. The security of the proposed algorithms for various benchmark attacks could also be undertaken in future work.