INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY
HYDERABAD

R&D SHOWCASE 2021

SMART CONTRACT-BASED BLOCKCHAIN-ENVISIONED AUTHENTICATION SCHEME FOR SMART FARMING

ABSTRACT

A blockchain-based smart farming technology provides the agricultural data to the farmers and other users associated with smart farming on a single integrated platform. Moreover, persistence and auditability of stored data in blocks into the blockchain provide the confidence of using the correct data when needed later and adds transparency, anonymity and traceability at the same time. To fulfill such a goal, in this paper, we design a new smart contract-based blockchain-envisioned authenticated key agreement mechanism in a smart farming environment. The device-to-device (D2D) authentication phase and device-to-gateway (D2G) authentication phase support mutual authentication and key agreement between two Internet of Things (IoT) enabled devices and between an IoT device and the gateway node in the network, respectively. The blocks are created by the edge servers on the authenticated data of IoT devices received from the gateway nodes and then sent to the cloud server. The smart contract-based consensus mechanism allows verification and addition of the formed blocks by a Peer-to-Peer (P2P) cloud servers network. The security of the proposed scheme is done through formal and informal security analysis, and also using the formal security verification tool. A detailed comparative study reveals that the proposed scheme offers superior security and more functionality features as compared to existing competing authentication protocols. Finally, the blockchain based simulation has been conducted to measure computational time for a varied number of mined blocks and also a varied number of transactions per block.

REGISTRATION & AUTHENTICATION SCHEME

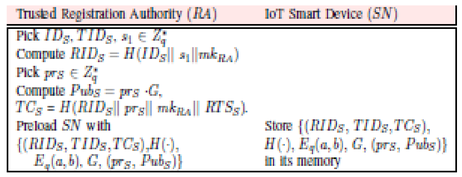


Fig. 2: Summary of IoT smart device registration phase

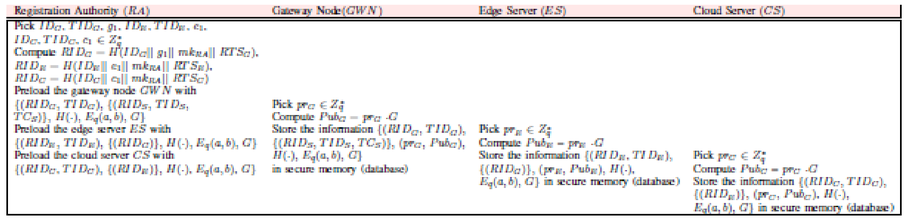


Fig. 3: Summary of registration phase of GWN, ES and CS

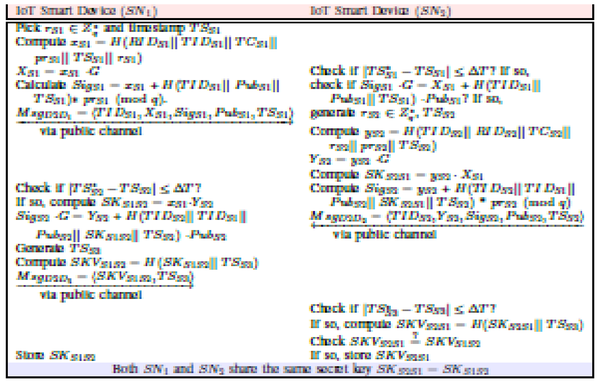


Fig. 4: Summary of D2D authentication phase

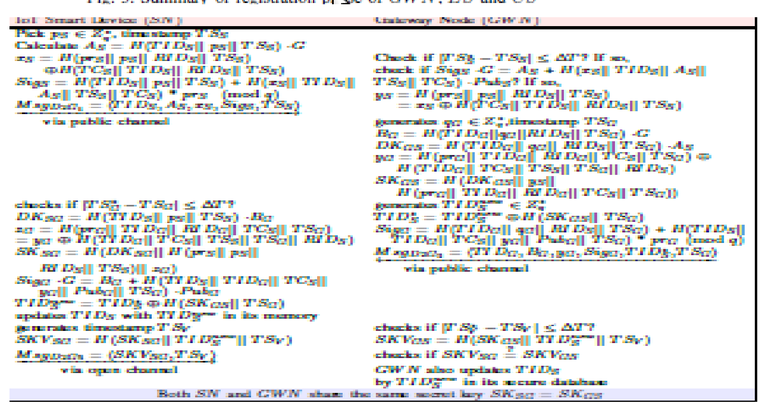


Fig. 5: Summary of D2G authentication phase

BLOCKCHAIN CONSENSUS ALGORITHM

Algorithm 1 Smart contract processing and consensus work-flow of the blockchain

Input: $Block_i$: A full block having the structure as given in Fig. 6 that is to be added to the blockchain, N: Total number of P2P nodes (cloud servers) in the blockchain network
Output: Block commit status (YES/NO)

1: Set $Magic\_Number = 2 * (N-1)/3 + 1$
2: $CMP_i \leftarrow \Phi$ (empty)
3: Broadcast $Block_i$ to the replica nodes in the network to peers
4: **for** each replica cloud server node CS_j **do**
5: /* Smart contract processing */
6: Set $Consensus\_Vote_j = NO$
7: Compute $Block\_Hash = H(Block_i)$
8: **if** ($Block\_Hash = Curr\_Block\_Hash$) **then**
9: **if** (validation of $Sig_{parBlock}$ using Pub_{ES} is successful) **then**
10: Generate Merkle tree root (MTR_{i_x}) using the n_x transactions stored in the block payload
11: **if** ($MTR_{i\_x} = MTR_{rx}$) **then**
12: Set $Consensus\_Vote_j = YES$
13: **end if**
14: **end if**
15: **end if**
16: Add $Consensus\_Vote_j$ to CMP_i
17: **end for**
18: Set $App_{Count} \leftarrow 0$
19: **for** each vote V reply in CMP_i **do**
20: **if** (V is YES) **then**
21: Set $App_{Count} = App_{Count} + 1$
22: **end if**
23: **end for**
24: **if** ($App_{Count} \ge Magic\_Number$) **then**
25: Add block $Block_i$ into the blockchain
26: Broadcast block commit status as YES to the blockchain network
27: **end if**

RESULTS

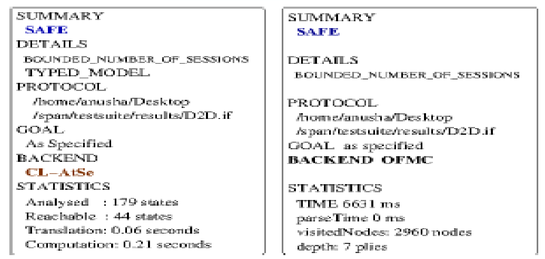


Fig. 8: AVISPA simulation results for D2D authentication

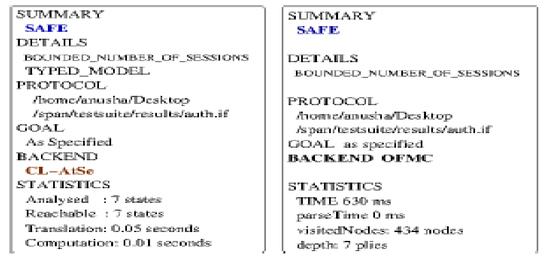
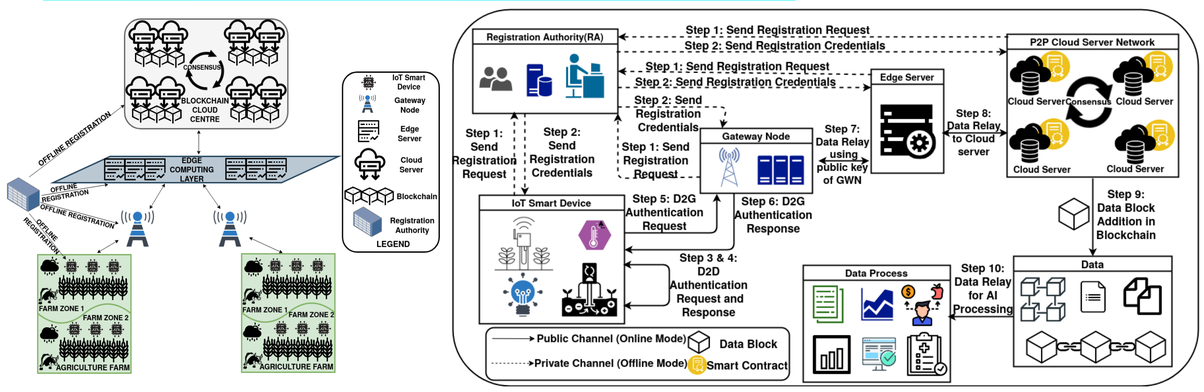


Fig. 9: AVISPA simulation results for D2G authentication

NETWORK MODEL & ACCESS MODEL



Research Centre: Centre for Security, Theory and Algorithmic Research (CSTAR), IIIT-Hyderabad

Anusha Vangala, Anil Kumar Sutrala, Ashok Kumar Das, Minho Jo, "Smart Contract-Based Blockchain-Envisioned Authentication Scheme for Smart Farming" in Internet of Things Journal, 2021, DOI: 10.1109/JIOT.2021.3050676. (SCI Impact Factor 9.936).