INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY
HYDERABAD

R&D SHOWCASE 2021
Technology, Social Impact

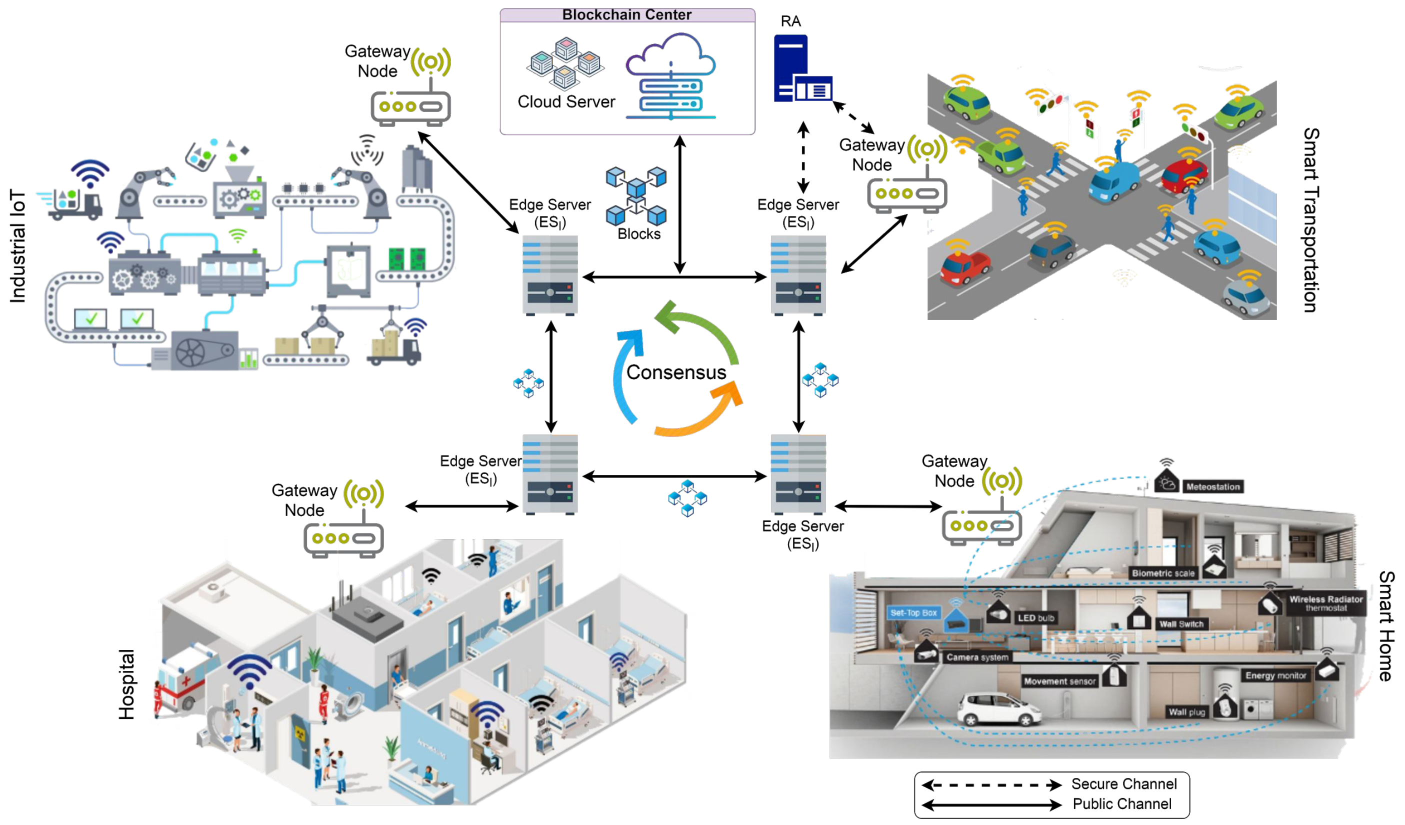
Consortium blockchain-enabled access control mechanism in edge computing based generic IoT environment

ABSTRACT

Internet of Things (IoT) is the latest era of connecting smart devices to exchange data with other objects. However, it has several security challenges such as privacy, integrity, confidentiality, authenticity and active & passive attacks. The access control mechanism plays a very crucial role as IoT devices require to send/receive data securely to their nearby gateway node and its associated edge server(s). In blockchain, once the blocks are added it can not be further modified, updated or deleted. It is required to design a blockchain-enabled access control scheme for edge computing based generic IoT environment.

CONTRIBUTION

- ❖ A consortium blockchain-enabled access control scheme is designed in edge computing based generic IoT (CBACS-EIoT). CBACS-EIoT offers access control among IoT smart devices and its associated gateway nodes & edge servers.
- ❖ Key management process is designed among the edge servers and the cloud servers in the blockchain center.
- ❖ The blocks created by the edge nodes are mined and put in their respective local ledgers. Then the blocks are added in the global ledger.
- ❖ A detailed security analysis has revealed that the proposed CBACS-EIoT is robust and secure against various potential active and passive attacks.
- ❖ Finally, the performance analysis shows that CBACS-EIoT offers superior security and supports more functionality features with less communication and computational overheads as compared to existing relevant schemes.



Block Header	
Block Version	BV
Previous Block Hash	PBHash
Merkle Tree Root	MTR
Block Type	Public
Timestamp	TS
Owner of Block	ES_l
Public key of signer (ES_l)	Pub_{ES_l}
Block Payload (Transactions)	
Transaction #1 Transaction #2 ⋮ Transaction #n_t	Tx_1 Tx_2 ⋮ Tx_{n_t}
Current Block Hash	CBHash
Signature on block using ECDSA	BSign

a) Formation of a block on public blockchain

Block Header	
Block Version	BV
Previous Block Hash	PBHash
Merkle Tree Root	MTR
Block Type	Private
Timestamp	TS
Owner of Block	ES_l
Public key of signer (ES_l)	Pub_{ES_l}
Block Payload (Encrypted Transactions)	
Encrypted Transaction #1 Encrypted Transaction #2 ⋮ Encrypted Transaction #n_t	$E_{Pub_{ES_l}}(Tx_1)$ $E_{Pub_{ES_l}}(Tx_2)$ ⋮ $E_{Pub_{ES_l}}(Tx_{n_t})$
Current Block Hash	CBHash
Signature on block using ECDSA	BSign

b) Formation of a block on private blockchain

Block Header	
Block Version	BV
Previous Block Hash	PBHash
Merkle Tree Root	MTR
Block Type	Hybrid
Timestamp	TS
Owner of Block	ES_l
Public key of signer (ES_l)	Pub_{ES_l}
Block Payload	
Encrypted Transaction #1 Transaction #2 ⋮ Encrypted Transaction #n_t	$E_{Pub_{ES_l}}(Tx_1)$ Tx_2 ⋮ $E_{Pub_{ES_l}}(Tx_{n_t})$
Current Block Hash	CBHash
Signature on block using ECDSA	BSign

c) Formation of a block on consortium blockchain

METHOD

- We have considered certificate-less access control mechanism for establishing a session key between gateway nodes and its respective IoT smart devices based on their application types.
- Dolev-Yao and CK-adversary are adopted for threat model.
- The designed scheme containing registration phase then followed by the access control between “smart device and gateway node” and “gateway node and edge server”.
- Key management phase between edge server and cloud server, and dynamic nodes addition phase for new IoT smart device addition and new gateway node addition.
- Consensus protocol for block verification and addition in blockchain is discussed, also the formation of a block (public, private or hybrid) was elaborated.
- Finally, the formal and informal security issues was discussed.

CONCLUSION

- A novel consortium blockchain-enabled access control scheme in edge computing based generic IoT environment was introduced.
- A detailed security analysis including the formal security under the random oracle model. Comparative study reveals that the CBACS-EIoT provides better security and functionality attributes, and low communication and computation cost.

REFERENCES

- Lin C, He D, Kumar N, Huang X, Vijaykumar P, Choo KR. HomeChain: A Blockchain-Based Secure Mutual Authentication System for Smart Homes. IEEE Internet of Things Journal 2020; 7(2): 818-829.

S. Saha, D. Chattaraj, B. Bera, A. K. Das, “Consortium blockchain-enabled access control mechanism in edge computing based generic IoT environment” in Transactions on Emerging Telecommunications Technologies (Wiley), http://doi.org/10.1002/ett.3995

Presented by: Sourav Saha
Supervisor: Dr. Ashok Kumar Das, Associate Professor, CSTAR Lab, IIIT Hyderabad