Webology (ISSN: 1735-188X)
Volume 18, Number 6, 2021

Blockchain Based Device Authentication For The Internet Of Things

[1] **D. Janet Ramya ,** [2] **Dr. L. Arockiam**

[1] Research Scholar in Computer Science.

[2] Associate Professor in Computer Science.

[1] [2] St. Joseph's College(Autonomous) [Affiliated to Bharathidasan University], Tiruchirappalli, Tamilnadu, India.

ABSTRACT - The technologies such as Internet of Things have contributed rapidly to transform the environment in a smarter way. Each thing connected in this environment has its own identity which is standardised yet vulnerable in many ways. Blockchain- the decentralised, distributed, immutable ledger technology is an alternative solution to visualise the connected network in a more secured way. By combining these two technologies, the identities of each device are made rigid and tamper proof. In this paper, the advantages of anonymity of blockchain technology is inculcated to the "things" through identity based encryption algorithm and smart contracts. The proposed work integrates key management and makes it unalterable and Smart contracts automate the membership of devices in a network thus ensuring secure identities to devices.

Index Terms: Blockchain, Ethereum Smart contracts, Internet of Things, Key management.

I. INTRODUCTION

Internet of Things (IoT) and Blockchain are considered emerging technologies placing roots in many application areas. These two technologies are transforming concepts to create new possibilities. Opportunities are rising day by day to create innovative applications that can share the intrinsic features of both technologies, exploring how the IoT can profited from the decentralized nature of the Blockchain. The term IoT refers to the on-going effort that awaits to connect a wide variety of physical things to the communication networks.

In today's scenario in the IoT, security risks go far beyond than just theft of information or denial of services. The rise of emerging technologies like IoT has also brought an increase in the amount of data being shared among connected devices. Security and privacy solutions should be implemented with respect to the heterogeneous nature of IoT devices. Blockchain falls under the same roof, because this technology also placed its roots in authenticating, authorizing, and auditing devices and also protects data generated in a well-defined manner. The decentralized nature of Blockchain eliminates the concept of centralized trust and avoids single point failures. Blockchain has a function to create a global index for all the transactions generated in the network and makes it immutable. As a result, device and data will become

more secure by infusing blockchain technology to IoT. Therefore, a new means to authenticate, authorize, audit devices and data generated by these devices will pave way to transform the digital world in a more secure way [13].

II. BACKGROUND STUDY

A. The Internet of Things

"Things", denote, valuable resources, either as material value, or in the form of the service they offer. Resources need to be managed throughout their lifecycle, and access to these resources need to be controlled and audited periodically. The identity of resources, maybe a device should be managed, protected and maintained by an identity management (IdM) system. An IdM offers services for authentication, which means some kind of mechanism to assure identity and through the mechanism the system could identify the entity which operates on a resource. Authentication is considered as a prerequisite for auditing, accounting and access control and other services not related to security or accountability. An authentication operation of a thing may be disrupted if the token is lost or stolen, or if the password is revealed to others. This makes the thing vulnerable and easy to tamper [1]. Nowadays, Authentication of things is turning out to be the biggest challenge.

IdM could [2];

- Define the identity of an entity
- Store the relevant information of entities
- Make that information accessible in a public or private environment
- Provide resilient services in a distributed environment
- Help in managing the connectivity within the prescribed environment

B. Blockchain

Bitcoin's public ledger, the blockchain, was first introduced in 2009 by Satoshi Nakamoto. Bitcoin was the first implementation to be used widely for peer-to-peer trustless electronic cash. Since then, similar structures are used to create many forms of electronic cash or cryptocurrencies. At the same time, Blockchain technology has been implemented in various application scenarios.

Some potential properties include;

- Blockchain decentralises the services it offers and there is no central authority to control the network.
- Data transparency and auditability ensures that all transactions in a network is available and known to all peers in the network
- Distributed information where every node has the copy of the entire chain
- Decentralised Consensus mechanisms assure the transactions be validated by all the nodes in the network.
- The Blockchain is immutable i.e. Tamperproof, hence it cannot be manipulated.

When it comes to decentralised consensus in distributed systems, they require majority of nodes to mutually agree on a given value, needed for computational purposes. Blockchain uses various consensus mechanisms like proof of work (PoW), proof of stake (PoS), etc. [8]

The PoW of every block is a mathematical puzzle which introduces a specific level of difficulty to generate a new block. Every block in the network is validated through the decentralised consensus. If

there is maximum consensus to accept a new block, then the new block will be added into the blockchain. All the miners will then have to start mining using that block as a reference. The block once added cannot be modified as it is immutable else the entire blockchain would have to be regenerated.

Proof of stake (PoS) is a proposed alternative to PoW, since PoW method forces miners to repeatedly run expensive hashing algorithms to validate transactions, PoS determines users to prove ownership of a certain amount of currency or through some means of majority. This reduces the complexity of block generation [12].

Blockchain implementations first started with Bitcoin for financial transactions in a peer to peer network. Public key cryptography was used and PoW was the consensus mechanism. Hyperledger is a project hosted by Linux foundation as a cross industry product with customizable benefits to serve multiple application domains. It follows PoW consensus. Ethereum was designed in 2013 to facilitate the development of decentralized applications on top of the blockchain. Ether is the cryptocurrency owned by Ethereum and there is an internal pay for computations and block generations which causes a transaction fee called gas fee. The decentralized applications are programmed with the help of a built-in Turing complete language called Solidity. Ethereum uses PoS as its consensus mechanism. In this paper, Ethereum implementation is taken under study.

Therefore from the above said, blockchain can offer;

- Tamperproof hashes as identity alternatives for a distributed environment like IoT
- Transparent and auditable services to store the relevant information of things
- Make that information accessible to everyone in the network
- Decentralised, Distributed ledger which can be accessed anytime
- Manages and monitors each device in its entirety

C. Blockchain based Identity for IoT:

David W. Kravitz et al. [3] proposed ways to secure user identity and transactions symbiotically with respect to transaction longevity. The following were factors considered to ensure transaction longevity such as, Asymmetric key rotation, Device group membership, Hash function agility, Transaction Expiration. Cryptographic constructs such as authorization key management and attribute management were discussed. The author applied the above method to Asset transfer example and concluded by stating on how to improve the robustness of user identity against fraud by privately referencing the user's blockchain transactions.

Paul Dunphy et al. [5] discussed the various distributed ledger Technology benefits to identity management. He quoted the various identity management schemes which are sorted into two categories. They were self-sovereign identity and decentralized trusted identity. Various identity management schemes like UPort, Sho Card, Sovrin were listed. The design and analysis of each IdM scheme was compared and tabulated with the laws of distributed ledger technology.

George C. Polyzos et al. [6] discussed the blockchain-assisted information distribution for the internet of things. The author enforced the importance of how blockchains and smart contracts can help in overcoming the security and privacy challenges. The advantages on how blockchains enable novel security mechanisms and how blockchains contribute to the sustainability of a system and help in building new trust models were elaborated. The method consisted of the following phases such as identification and trust management, Provenance verification and information tracking, Authentication and access

control. The author concluded by stating that the efficiency and scalability of blockchains would be enhanced if the gateway is secured.

Abdallah Zoubir Ourad et al. [7] has proposed an Access Control and Authentication management for IoT using blockchain in which a sample ethereum smart contract scenario is explained. Blockchain based authentication models such as Auth0 has introduced a method which authenticated the server directly. The proposed system design was to One Time Authentication which Authenticated once directly to the Blockchain then accessed the Resource Using Smart Contract Tokens.

Qun Lin et al. [11] proposed identity based cryptosystems which used public keys to derive user identities. The author developed security model for ID-based linearly homomorphic signature. The signer can produce an identity based cryptosystem using bilinear groups as tool to design ID based linearly homomorphic signature. An ID-based linearly homomorphic signature scheme is a tuple of five PPT (Probabilistic Polynomial-Time) algorithms such as H Setup, HExtract, HSign, HVerify, HEval to avoid the shortcomings of the use of public-key certificates. Moreover, the scheme is proved secure against existential forgery on chosen message and ID attack under the random oracle model.

Mohamed Tahar HAMMI et al. [15] designed a decentralized authentication blockchain-based mechanism called BC Trust. BC Trust is based on the principal of "The friend of my friend is my friend", which means that, if a device is authenticated in one cluster, it becomes trustful and accepted by all the other clusters. The blockchain ensures that the stored information is available for all the participating nodes, and protected from modifications. Elliptic Curve Digital Signature Algorithm was used in the experiment and power consumption by communication and process power consumption in migration through BC layers was measured. The results were compared with the classical method and BC Trust method and BC Trust resulted in low consumption of power.

Otto Julio Ahlert Pinno et al. [9] developed Control Chain, using Blockchain as a Central Enabler for Access Control Authorizations in the IoT. It is based on principles like Decentralization, Resilience, Off-line working, Low processor usage for authorizations. A comparative study was made on architectures such as XACML, OAuth, UMA, Fair Access and Control Chain. Control Chain focused mainly on access control which was scalable, user friendly, transparent, fault tolerant and compatible with wide range of IoT models.

Chan Hyeok Lee et al. [10] implemented the IoT System using Block Chain to ensure authentication and to protect data by applying Zero-Knowledge proof to a smart meter system to prove that a user is authentic without disclosing information such as public key. Privacy protection was ensured using the anonymous nature of block chain for privacy protection. IoT device authentication and data tampering was ensured. It was proved that using smart contracts which have Zero-knowledge proof, transactions can be convenient and safe.

III. PROPOSED WORK

The objective of the AROJAN algorithm is to assign unique identity to the IoT device. This registration is done when the IoT device wants to connect with the Blockchain. The Device would then send a request to the blockchain with its device number. The Miner, on receiving the request will generate the public and private key for the device using the device's unique identity (could be device number, serial number, etc.) after verifying the device information. If the device identity is valid then keys are sent to the device and stored in the blockchain.

Later the valid device can communicate with the peers in the network through Smart contracts. The smart contracts are signed between the peer devices and it holds the public key of the device. Once the membership of the device is validated through the Smart Contract the device can exchange information.

In Fig.1, the proposed work to authenticate devices consists of two phases such as Identity Based Encryption (IBE) and Smart Contract Based Identity (SCBID) is shown.

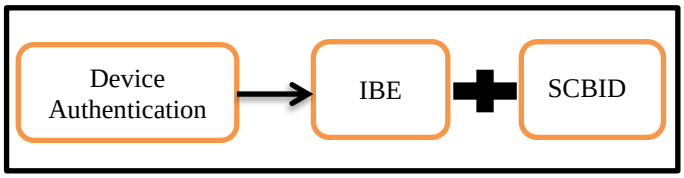

Fig. 1. The Two Phases in Device Authentication

A. Identity Based Encryption (IBE)

Identity Based Encryption (IBE) is one alternative that enables a user's public key to be created using his identity, so that other entities can verify the user's identity through the public key. IBE suffers from the key Escrow problem: the Key Generation Centre (KGC) is aware of the user's private key, and there is no way to authenticate a user. This is where Certificateless Cryptography comes around. For example, an IoT device can append its public key to his data access request and send the request to the blockchain where the blockchain miners are able to verify the public key of the device.

Notations:

A_1, A_2 - IoT devices
DID_1 - Device IDentifier of device A_1
PK_1 - Public Key of device A_1
SK_1 - Secret or Private Key of device A_1
M_1 - Miner of device A_1
SC_1 - Smart Contract of device A_1

***Algorithm*: AROJAN**
INPUT : System Parameter DID_1 – Device Number
PROCESS : Generating PK_1, SK_1 for Device A_1
OUTPUT : PK_1, SK_1

Step 1: Start
Step 2: Read DID_1 for A
Step 3: Call Procedure *Blockchain Based Identity (BID)*
Step 4: Stop

***Procedure*: Blockchain Based Identity (BID)**

BEGIN
Step 1: The A_1 sends request to KGC
//Device registration
Step 2: The Miner in KGC verifies the request from IoT device *//Device verification*
Step 3: If DID_1 is valid *//Key Generation*
M_1 generates PK_1 and SK_1 for device A_1
M_1 signs the message
Sends the signed message to device A_1
Step 4: If the DID_1 is invalid
M_1 rejects the device request
Step 5: A_1 wants to communicate to device A_2
Step 6: A_1 creates SC_1 using PK_1
//Smart Contract Generation
Step 7: A_2 verifies membership of device A_1 using PK_1
Step 8: If PK_1 exists
Registered device communicates to exchange information
Step 9: If PK_1 does not exist
Device is not registered
END

Once the device is authenticated the transactions are authorised by miners.
To verify a transaction T_A, the miners have to check the following requirements:

1) If the public key PK_A is derived from the identity ID_A associated with it.
2) If the signed transaction can be verified with the public key PK_A.

By checking the two requirements above, the miners will be able to verify whether a transaction T_A is created from ID_A or not. The procedure BID would ensure authenticity of devices which have full control over their identity once registered. An integrated key management scheme is applied for each device in the blockchain.

B. Smart Contract Based IDentity (SCBID):

a) Ethereum

A new and increasingly popular implementation of this Blockchain is Ethereum. Ethereum is maintained and extended constantly, through a group called the Ethereum Foundation. The cryptocurrency associated with Ethereum is called Ether. Ethereum additionally offers the users the possibility to save Turing-

complete code called Smart Contracts (SCs) into the blockchain. These SCs are simultaneously evaluated by multiple blockchain users to ensure everyone has the same state of the contracts.

b) Smart Contracts and Solidity

A Smart Contract (SC) is a digital program which is evaluated in the blockchain and should produce the same result whenever executed in any system. SCs are written in a programming Language called Solidity. Solidity has been described as a contract-oriented and high-level language whose syntax and usage feels similar to JavaScript and runs on the Ethereum Virtual Machine (EVM). This virtual machine is a consensus-based globally executed virtual machine. This EVM is what executes the SCs and guarantees that its code is evaluated correctly [14].

c) Ethereum Identity Standards

ERC 725: a Proposed Ethereum Identity Standard:

Integrating Blockchain with IoT would bring in identity concepts in a network such as;

- An Identity of a device is known by the address of an Ethereum Smart Contract implementing ERC 725
- An integrated key management scheme is applied for each device

Any identity is represented using the DID (Decentralized IDentifier) consisting of;
did:[method]:[method specific identifier]
Eg: did:uport:2nQviQG6Cgm1GYTBaaKAgr76uY7iSeiUkqX
Each DID has a DID document which contains its public keys [4] [15].

d) Prototyping a Blockchain Smart Contract:

In the proposed SCBID technique, the public key of the device is added in the smart contract and published in the blockchain network. At the receiving end the receiver, to whom the contract is intended for receives the smart contract. The receiver checks;

- Whether the public key is derived from the device's identity
- Whether the device is registered to the blockchain to ensure device membership

Once these conditions are satisfied, the smart contract is deployed at receiver's end and the information exchange takes place. This ensures that only authentic devices can communicate to exchange information and exist in the blockchain network.

```
pragma solidity >=0.4.22 <0.6.0;
contract Domain {
        address private owner;
        mapping (address => bool) private member;

        function checkOwner() public {
           owner = msg . sender;
        }

        function setMember (address id, bool include)
public {
          require (msg . sender == owner);
          member [id] =  include ;
        }

        function query (address id) public view returns
(bool) {
          return member[id];
        }
}
```

In the above code, the owner (creator) of the domain can add and remove members with the setMember function. With the query function, it is then possible to check if an address is a member or not.

In Fig. 2, the smart contract is executed in REMIX IDE. The contract is written in solidity programming language. The contract checks the device ID and Hash exists in the blockchain network or not. If the device is a member, then a Boolean value **True** is returned when query function is called in the contract as shown in Fig.3. If the device is not a member of the blockchain then the Boolean value **False** is returned on calling the query function as shown in Fig. 4.

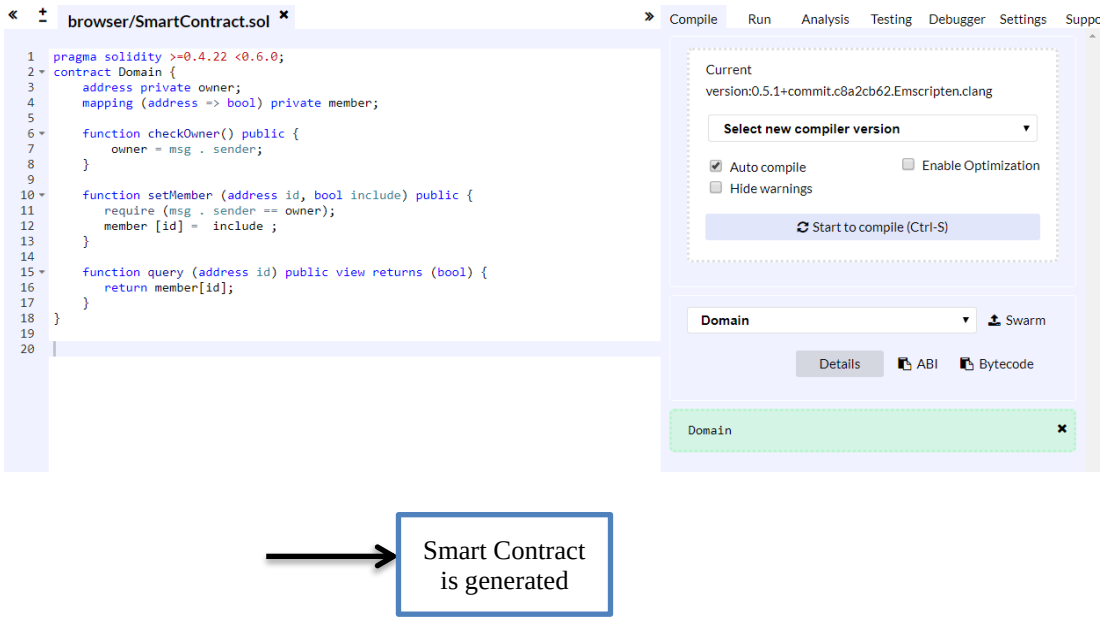

Fig. 2 Deployment of Smart Contract- Domain

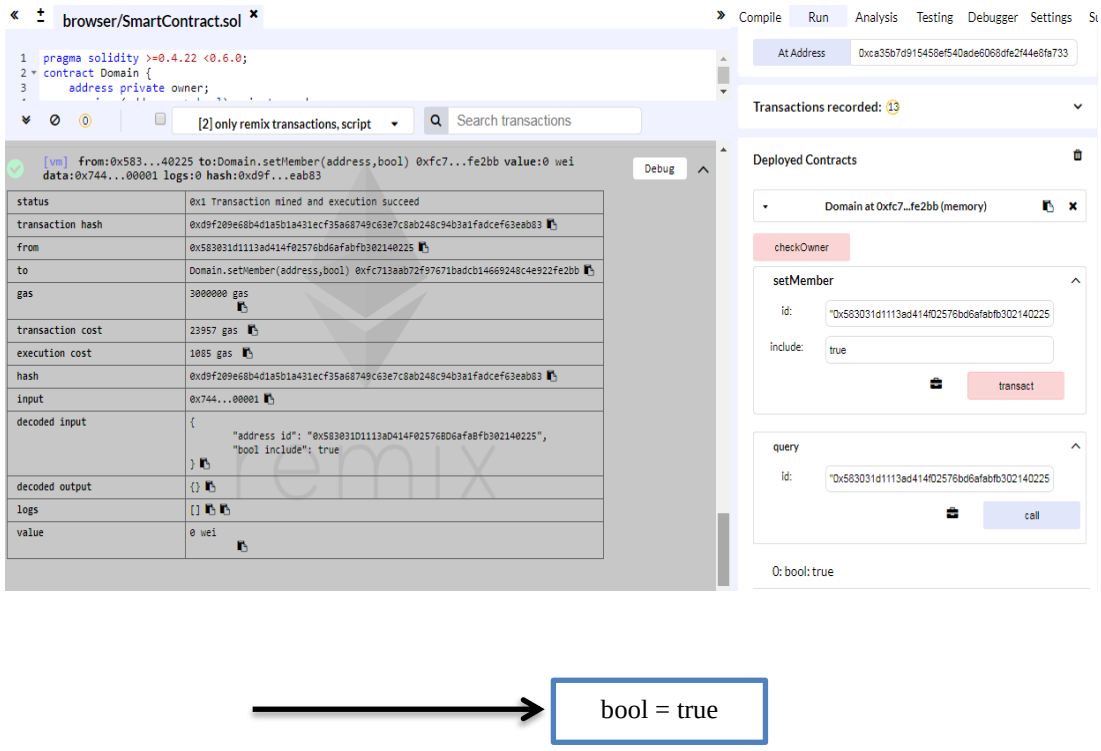

Fig 3. The membership of devices is verified and if memberID exists bool value returns true

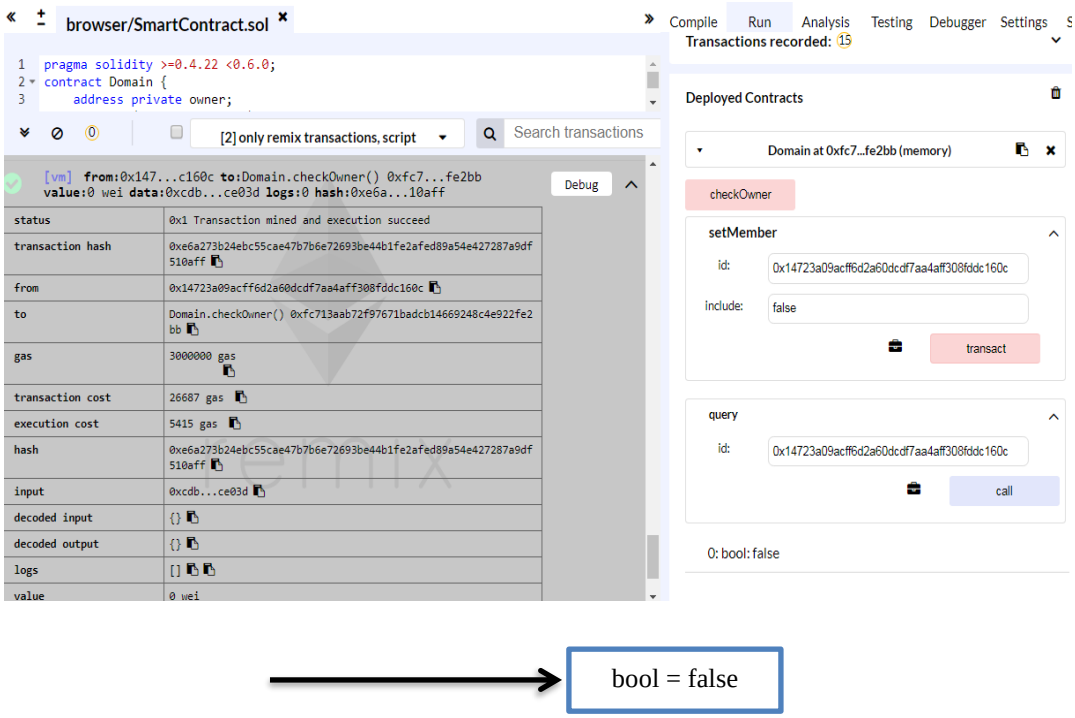

Fig 4. The membership of devices is verified and if memberID does not exist bool value returns **false**

IV. CONCLUSION

The need for device authentication is booming in this internet age. In this paper, blockchain based device authentication for the "things" in the IoT environment is stated to ensure secure, tamper proof devices to exist in a network. For this, BID technique does identity based encryption and smart contract based membership verification for devices is proposed. Thus anonymity feature of blockchain is imparted to the things in their distributed, connected environment to ensure security, robustness, and immutability. In future, this work can be enhanced by applying the proposed work with other consensus mechanisms and blockchain implementations and can be compared to provide the optimal one for an IoT environment.

REFERENCES

[1] Fongen, Anders, "Identity management and integrity protection in the internet of things", In 2012 third international conference on emerging security technologies, pp. 111-114, IEEE, 2012.

[2] Mahalle, Parikshit, Sachin Babar, Neeli R. Prasad, and Ramjee Prasad, "Identity management framework towards internet of things (IoT): Roadmap and key challenges", In International Conference on Network Security and Applications, pp. 430-439, Springer, Berlin, Heidelberg, 2010.

[3] Kravitz, David W., and Jason Cooper, "Securing user identity and transactions symbiotically: IoT meets blockchain", In 2017 Global Internet of Things Summit (Gio TS), pp. 1-6, IEEE, 2017.

[4] Jacobovitz, Ori, "Blockchain for identity management", The Lynne and William Frankel Center for Computer Science Department of Computer Science, Ben-Gurion University, Beer Sheva (2016).

[5] Dunphy, Paul, and Fabien AP Petitcolas, "A first look at identity management schemes on the blockchain", IEEE Security & Privacy 16, no. 4 (2018): 20-29.

[6] Polyzos, George C., and Nikos Fotiou, "Blockchain-assisted information distribution for the Internet of Things", In 2017 IEEE International Conference on Information Reuse and Integration (IRI), pp. 75-78, IEEE, 2017.

[7] Ourad, Abdallah Zoubir, Boutheyna Belgacem, and Khaled Salah, "Using Blockchain for IOT Access Control and Authentication Management", In International Conference on Internet of Things, pp. 150-164, Springer, Cham, 2018.

[8] Hammi, Mohamed Tahar, Patrick Bellot, and Ahmed Serhrouchni, "BC Trust: A decentralized authentication blockchain-based mechanism", In 2018 IEEE Wireless Communications and Networking Conference (WCNC), pp. 1-6, IEEE, 2018.

[9] Pinno, Otto Julio Ahlert, André Ricardo Abed Grégio, and Luis CE De Bona, "Control chain: Blockchain as a central enabler for access control authorizations in the iot", In GLOBECOM 2017-2017 IEEE Global Communications Conference, pp. 1-6, IEEE, 2017.

[10] Lee, Chan Hyeok, and Ki-Hyung Kim, "Implementation of IoT system using block chain with authentication and data protection", In 2018 International Conference on Information Networking (ICOIN), pp. 936-940, IEEE, 2018.

[11] Lin, Qun, Hongyang Yan, Zhengan Huang, Wenbin Chen, Jian Shen, and Yi Tang, "An ID-based linearly homomorphic signature scheme and its application in blockchain", IEEE Access 6 (2018): 20632-20640.

[12] Christidis, Konstantinos, and Michael Devetsikiotis, "Blockchains and smart contracts for the internet of things", IEEE Access 4 (2016): 2292-2303.

[13] Jesus, Emanuel Ferreira, Vanessa RL Chicarino, Célio VN de Albuquerque, and Antônio A. de A. Rocha, "A survey of how to use blockchain to secure internet of things and the stalker attack", Security and Communication Networks 2018 (2018).

[14] Hanada, Yuichi, Luke Hsiao, and Philip Levis, "Smart Contracts for Machine-to-Machine Communication: Possibilities and Limitations", In 2018 IEEE International Conference on Internet of Things and Intelligence System (IOTAIS), pp. 130-136, IEEE, 2018.

[15] Hammi, Mohamed Tahar, Patrick Bellot, and Ahmed Serhrouchni, "BC Trust: A decentralized authentication blockchain-based mechanism", In 2018 IEEE Wireless Communications and Networking Conference (WCNC), pp. 1-6, IEEE, 2018.