Pakistan Journal of Engineering and Technology, PakJET
Multidisciplinary | Peer Reviewed | Open Access
Volume: SI, Number: 01, Pages: 51- 58, Year: 2020

Blockchain Authentication Mechanism for Securing Internet of Things

Khadija Fazal[1,*], Adeel M.Syed[1]

[1]Software Engineering Department, Bahria University Shangrilla Road E-9, Islamabad, Pakistan
*Corresponding Author's email: khadijafazal98@yahoo.com

***Abstract*- Internet of Things is a recent potential advancement in an IT arena, consists of multiple smart things (devices) which are connected through a physical network. Cisco incorporation predicts that IoT network will connect 50 billion devices by 2020. Most of the industries are adopting IoT technology, and because of its fast-spreading, massive adoption and deployment, current authentication mechanisms have serious disadvantages. For numerous reasons, the security issues are the major hurdle in the adoption and deployment of IoT on a large scale since it is highly vulnerable to attacks. In this paper, a Blockchain-based authentication mechanism is proposed called Ethereum. It is a public blockchain mechanism. It has emerged as a technology that possesses great capabilities of providing secure authentication, management and access control for IoT devices in a decentralised, trusty and flexible manner by creating a safe environment. The devices can identify and trust each other, and only authenticated users are given permission to access them.**

***Index Terms*--** Blockchain, Ethereum, Internet of Things (IoT), Security

I. INTRODUCTION

Internet of things (IoT) is an emerging technology. IoT aims at interconnecting devices and people to the internet [1]. It represents a network where ''things'' or embedded devices having sensors are interlinked through a private or a public network providing a wide range of services to its users [2]. The smart connected devices or 'things' range from simple wearable accessories to large machines, each containing sensor chips. However, only authenticated and authorised users must be granted access to the system. Otherwise, the IoT ecosystem will be prone to numerous attacks. Whereas, the rapid increase in requirements for deploying IoT on a large scale results in significant security issues. Various security issues are considered to be the significant challenges in an IoT ecosystem that includes authentication, authorisation, privacy, access control, information storage, management and system configuration [3].

Recently, the Gartner study concluded that approximately 20 billion devices, things or physical objects are going to be connected to the internet by 2020 [4]. Such physical objects acquire useful information and communicate with software systems through the internet [5]. As a result of such extensive and rich interaction, these devices produces enormous amounts of data, enabling dependent services. Other than the benefits which are provided by these services, numerous critical security and privacy issues may arise. To this point, some efficient security and privacy measures need to be taken to avoid IoT ecosystem from being at a risk of failure. For handling transactions or sensitive data in a trustworthy online system, authentication is considered to be the critical component, as it is the process of proving identity or determining whether something or someone is actually what or who it is trying and declaring to be [6]. Blockchain was proposed for the very first time by Satoshi Nakamoto in 2008, and its implementation was started in 2009 [7]. Blockchain is a distributed, decentralised ledger (database) technology, mostly regarded as a public ledger that stores all the transactions in a chain of blocks. The chain of blocks includes a timestamp and cryptographic hashes which are used to link these blocks [8]. When new blocks are added to the chain, the chain as a result grows. For preventing a single point of failure in Blockchain, a copy of the ledger is maintained by each node which is kept updated and validated simultaneously [7]. These blocks consist of two parts, one is the transaction or record that is stored by the database and the second part is known as a header which includes block information such as hash, a nonce, timestamp of block transaction and hash of the previous block [9].

All the participating nodes involved in the blockchain ecosystem have to generate and maintain the ledger [8]. The participating nodes are of two types: the read-only nodes which can only read the transactions and the other one are read-write nodes which are usually known as miners that can read and write the transactions. Miners are allowed for adding transactions to the chain and are termed to be as unique nodes [9]. Blockchain is a trusted technology with a lot of potential merits. It is considered to be one of the core techniques in a decentralised network environment, as it is distributed, decentralised and unchangeable [7]. Miners need to complete proof of work (PoW) so that the block is accepted by the peers included in the blockchain network [10]. The basic structure of the Blockchain is shown in Fig 1.

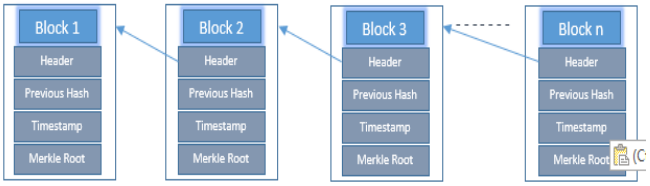

FIGURE 1. Basic structure of Blockchain

Many researchers have believed that Blockchain provides a promising solution for ensuring the security of IoT. We also have taken benefits from this technology to guarantee the security of IoT ecosystem. The main goal of our study is to propose an authentication mechanism based on blockchain type Ethereum, which is a public blockchain and ensures the security of IoT in a distributed and decentralised manner. The mechanism intends for creating secure zones where user and devices can communicate with each other securely. The rest of the paper is organised as follows: Section II is the Related Work which comprises of the blockchain introduction in detail and includes the work done by other authors in ensuring the security of IoT using Blockchain, section III is the Proposed Technique, section IV includes Results and Discussion, and finally, section V is comprised of conclusion, which concludes the paper.

II. RELATED WORK

This section holds a detailed review and contributions of the authors on how Blockchain is integrated with Internet of Things to address the security challenges arises in the context of IoT. Many researchers concluded IoT as a system of 'things' where only trusted users would be given access. However, existing solutions to address security are not fully adapted to such a system due to some limitations and heterogeneity of the devices [11]. Often, a hybrid or a combination of security solutions and techniques are needed, which incurs a huge cost. Secondly, an ecosystem comprised of multiple nodes may result in enormous scalability issues as existing efficient security solutions, e.g. Public Key Infrastructure (PKI) are often centralised [12]. Finally, it becomes difficult to integrate new services and scenarios as each application uses a different security architecture, approach and deployment. Therefore, it becomes necessary to propose a new security mechanism for an IoT ecosystem. To meet the security requirements in an IoT ecosystem, many researchers believe that Blockchain provides a promising solution. A solution that 1) allows new devices and services integration easy, 2) provides full adaption to needs and requirements of IoT and 3) Independent of device type and application's design and architecture [12].

Recently, a lot of work has been done in integrating blockchain technology in IoT infrastructure. Taking benefits of Blockchain's resiliency and power, the authors [13] proposed an efficient decentralised authentication mechanism based on Blockchain called bubbles of trust. The authors [14] have proposed an access control policy which is dynamic and is based on blockchain technology to be truly distributed with taking benefits from machine learning for the internet of things. The authors [15] proposed a user authentication scheme based on the Blockchain without involving any third part to analyse and ensure the security of IoT devices. Only authorised and secure access must be granted to IoT resources and to ensure this, [16] has proposed a solution called IoT Chain which is a security architecture based on blockchain technology for securing the internet of things. The authors [17] have presented and discussed many state-of-the-art techniques and mechanisms that are available in the existing literature. The authors [18] have proposed a Blockchain connected gateway design, which in the blockchain network securely maintain the user privacy for IoT devices in terms of sensitive data.

The authors [19] realised to propose a Blockchain-based data security framework for introducing tamper-proof and transparent data storage and its retrieval in IoT systems. Most of the IoT devices are lightweight and low energy, and they dedicate most of their computation and energy for the execution of some core functionalities, which makes the task of moderately supporting security much tricky. To overcome such challenges, the authors [20] have proposed a Blockchain-based security and privacy architecture to fulfil IoT demands to a scalable, distributed and lightweight security and privacy mechanism.

The authors of [21] have proposed a decentralised scheme for data storage based on a public blockchain and certificate-less cryptography. The author [22] proposed a Blockchain-based solution to enable secure communication, access control and authentication to IoT devices. The authors [23] have proposed a hyper ledger fabric-based secure blockchain technique for data transmission in Industrial IoT. The authors [24] have proposed a decentralised access control framework based on Blockchain for the internet of things called Fair-Access. The authors [25-30] have proposed an identity framework based on Blockchain for IoT. They have applied this framework to smart homes based on IoT to achieve self-management identity by the end-users. The authors [26] have proposed an authentication model by combining Physical Unclonable Function (PUF) and Blockchain. The authors [27-35] have proposed an out-of-band two-factor authentication system based on Blockchain infrastructure for securing Internet of Things. IoT and Blockchain are integrated and the integrated system were implemented with Eris Blockchain platform and emulator devices. The summary of the related work is mentioned in Table 1 below:

TABLE 1
SUMMARY OF THE RELATED WORKS

Proposed Approach	Authentication Consideration	Blockchain's Type	Implementation
Mohamed Tahar Hammi et al.	Yes	Ethereum	Yes
Aissam Outchakoucht et al.	Partial	Not Specified	No
Ali Dorri et al.	Yes	Bitcoin	Simulations
DongXing Li et al.	Yes	Hyperledger Fabric	No
W. Liang et al.	Yes	Hyperledger Fabric	Simulations
Aafaf Ouaddah et al.	No	Bitcoin	Yes

III. PROPOSED MECHANISM

The primary goal of our proposed approach is to secure IoT ecosystem by virtually creating a secure environment where devices can trust and communicate with each other and user may grant access to any IoT device after successful authentication. All the devices exist in that environment will communicate with every other device belonging to that environment and considers the rest of the devices as malicious. We are creating an environment of trust and call such an environment as "Trusted Vicinity". Thus, all the devices or members that belong to these "Trusted Vicinities" can trust each other, and such an environment is kept inaccessible and protected from non-member devices. For achieving our proposed system, we rely on a blockchain type Ethereum, which is a public blockchain, and it implements a smart contract. The proposed approach implements both user-to-device and device-to-device access after successful authentication process using a smart contract.

A. INITIALISATION PHASE

The initialisation phase is comprised of two phases, mentioned and discussed below:

PHASE 1: USER-TO-DEVICE AUTHENTICATION

In the case of user-to-device authentication, the identity of the user is verified by the smart contract. The user is an end-user, or a customer wanted to gain access to particular IoT devices to carry out their respective tasks. The smart contract determines if the user is legitimate and is allowed to gain access to their required IoT devices. Admins and End users have a unique Ethereum Address and are directly interfaced with the smart contract using the Ethereum wallet.

PHASE 2: DEVICE-TO-DEVICE AUTHENTICATION

In case of device-to-device authentication, each "Trusted Vicinity" consists of multiple IoT devices, where a particular device is designed as Master node of that vicinity, and this Master node is the owner of a private/public key pair. The Master node looks more like a certification authority. Any device from the trusted vicinity can be termed as master and the rest of the devices in that vicinity are called as Followers. An Elliptic Curve Cryptography is used for key exchange, and a private/public key pair is generated by each follower. After that, each follower in the vicinity is given with a structure called the ticket.

This ticket is basically a lightweight certificate consists of 64 bytes and contains three parameters, i.e. 1) A Group Identifier (Grp_Id), which is the identity of a particular vicinity to which a device belongs or is part of. 2) An Object Identifier (Obj_Id), which represents the unique identity of each object/device that belongs to a particular vicinity. 3) Public Address (Pub_Addr), which shows the public address of the follower. IoT devices have unique object identifiers, but they don't have a direct interface with the smart contract. The first 20 bytes of the follower's public key are represented as Secure Hash Algorithm 3 (SHA-3) [28] and 4) A Signature Structure, it uses master's private key of a particular vicinity to represent Elliptic Curve Digital Signature Algorithm (ECDSA). In user-to-device authentication, the user sends an authentication request to Blockchain using Ethereum wallet address which checks for the user's validity. For concatenation of Group Identifier, Object Identifier and the Public Address the signature includes SHA-3 hash and the structure of the ticket is given below:

Signature (SHA-3 (Group Identifier | Object Identifier | Public Address))

B. SYSTEM'S ARCHITECTURE AND FUNCTIONALITY

The working and life cycle of our proposed mechanism is detailed in FIGURE 3, FIGURE 4, FIGURE 5 and FIGURE 6. First of all, the connected things in an IoT ecosystem may belong to various sectors such as, industry, house, city, hospital etc. and are shown in Fig 2, whereas Algorithm# 1 shows various parameters and functions that used in our proposed mechanism. FIGURE is the initialisation Phase1 which represents the authentication scenario which includes that the end-user when wants to access a particular device(s), it first initiates an authentication request that is sent to the smart contract specifying the unique user's Ethereum Address, Obj_Id of the device user wants to access and its respective Grp_Id to which that device belongs.

Variables:

Obj: Object

Sender: Object

Receiver: Object

Admin

User

Master

Follower

Functions:

Function 1: UserIdExists (Integer User_Id, Blockchain BC)

//Check if user identifier exists on Blockchain or not

Function 2: ObjectIdExists (Integer Obj_Id, Blockchain BC)

//Check if object identifier exists on Blockchain or not

Function 3: GroupIdExists (Integer Grp_Id, Blockchain BC)

//Check if group identifier exists on Blockchain or not

Function 4: ObjectAddressExists (Integer Obj_Address, Blockchain BC)

//Check if address of the object exists on Blockchain or not

Function 5: Error ();

//Return Error Message

ALGORITHM#1 Variables & Function Definition

If the user is legitimate, the smart contract broadcast a message to both user and device which includes an Access token and sender's (user) Ethereum address. When this message is received at the user end, the user creates a package which is signed by Ethereum private key and it includes Access Token, User's IP Address, Ethereum Public Key and Access Duration.

The package is sent to the corresponding device using its public key. When the package is received by that device, its contents are verified and upon success the user is granted access by the device from sender's (user) IP address for the specified duration. And in Fig 4 Phase 2, master chooses the Group Identifier (Grp_Id).

FIGURE 2. Things in an IoT Network

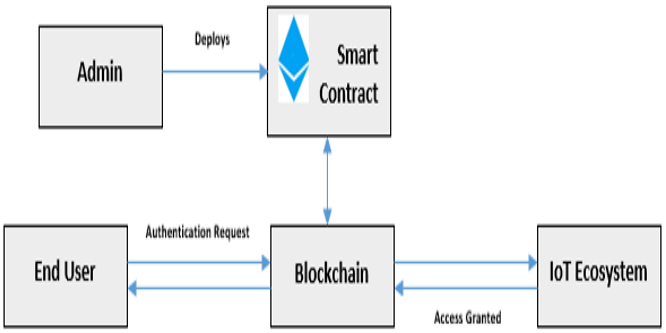

FIGURE 3. Initialisation Phase 1

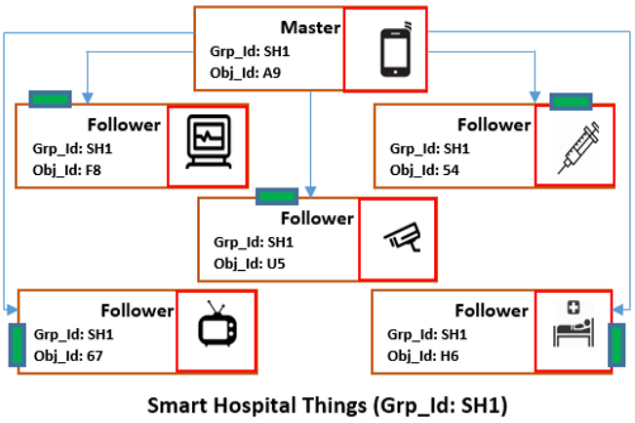

FIGURE 4. Initialisation Phase 2

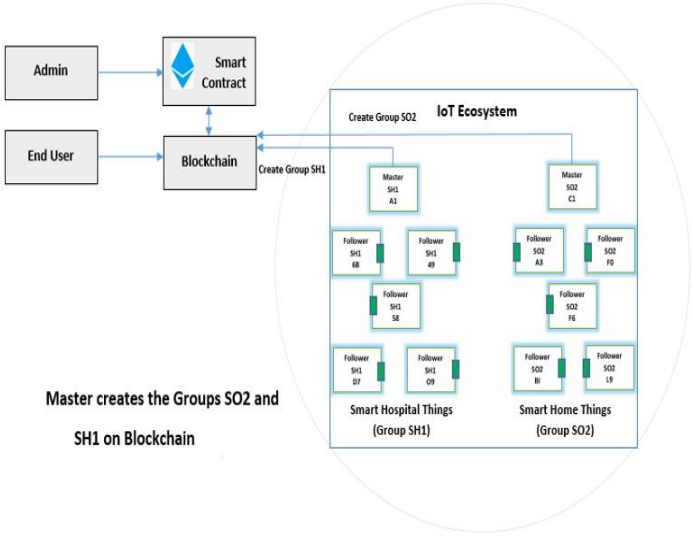

FIGURE 5. Master Creates Groups on Blockchain

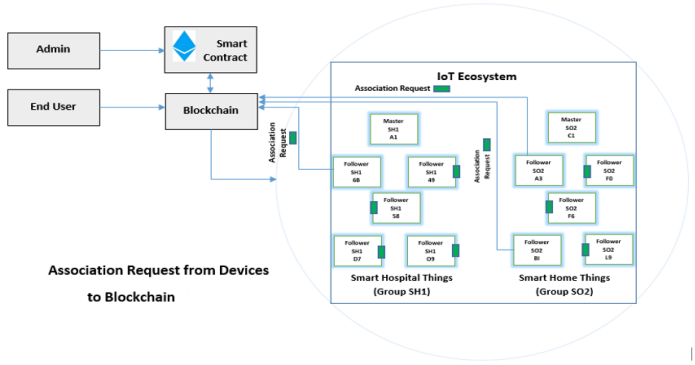

FIGURE 6. Association Request from Devices to Blockchain

Furthermore, all the objects included in the Group are provided with a ticket which is signed by the master. After when the Group is prepared, a 'trusted vicinity' will be created at the blockchain level and is shown in Fig 5. As we have chosen a public blockchain so any user can create a 'trusted vicinity'. For the creation of 'trusted vicinity' at blockchain level, master has to send a transaction which includes the identifier of the master (i.e. Obj_Id of the Master) along with the Group identifier the master wishes to create. Blockchain is responsible for verifying both Master's Obj_Id and Grp_Id. 'Trusted Vicinity' is created after being transaction is considered valid.

```
begin
if (ObjectIdExists (Obj_Id, BC) == True) then
return error ();
if (ObjectAddressExists (Obj.Grp_Id, BC) == True) then
return error ();
if (Object. Type = User) then
if (UserIdExists (Obj.User_Id, BC) == True) then
return error ();
if (Object. Type = Master) then
if (GroupIdExists (Obj.Grp_Id, BC) == True) then
return error ();
else if (Object. Type = Follower) then
if (GroupIdExists (Obj.Grp_Id, BC) == False) then
return error ();
if (BC.TicketVerification (obj.Ticket) == Failed) then
return error ();
else
```

ALGORITHM# 2 Association Rules of Proposed Mechanism

Followers in turn (the objects which are part of the system) associate themselves to their corresponding groups or 'trusted vicinities' by sending the transaction to the Blockchain. The smart contract at blockchain level verifies their Obj_Id and then their ticket's validity is checked following the master's public key of that particular Group or 'trusted vicinity, as shown in FIGURE 6. If any of the above-mentioned condition fails to satisfy, the follower cannot be associated with the Group or 'trusted vicinity'. Algorithm# 2 describes the association rules of the objects involved in the mechanism.

But if the first association request by follower is successful, it do not need to use its ticket in future for authenticating itself. Followers or master of two or more 'trusted vicinities' that are associated or stored on a blockchain can exchange messages and transactions.

We also have defined some key points for blockchain access control upon various objects and transaction, which are mentioned below:

1) After the association request, if any group or 'trusted vicinity' wants to join, it can, after when the master sends 'create' request to the Blockchain but it should be with a unique Grp_Id.
2) All the Masters with duplicate name or Grp_Id cannot create the Group.
3) The objects belonging to the same Group can communicate and send data and transactions.
4) The objects belonging to different authenticated groups can also exchange data and transactions, but through their respective Masters'.
5) Any external entity/object/group that does not exist on the Blockchain (i.e. No Master has created the Group on the Blockchain) and wants to access or carry out transaction with any of the authenticated Group or 'trusted vicinity' is rejected.
6) Any object that do not have a ticket or with a fake one cannot be associated with any group or 'trusted vicinity' and thus they are not allowed to communicate with any object of 'trusted vicinity'. Algorithm# 3 shows the communication rules for the objects involved in the proposed mechanism.

ALGORITHM#3 Communication Rules of Proposed Mechanism

```
begin
if (ObjectIdExists (sender_Id, BC) == False)
or (ObjectIdExists (receiver_Id, BC) == False) then
return error ();
if (BC.SignatureVerfication (sender. Message) == Failed)
then
return error ();

// Secure Communication of objects and data exchange
completed with success
```

Due to transaction's signature, the authentication of objects and integrity if exchanged messages are ensured. The miners must validate the smart contract once it is created and sent by a transaction to the Blockchain. An address (e.g. 0x89f78fa9f456dbd0a1bc22a09befc56ada04d6b3) which always starts with '0x', is received by the owner of the contract as a result of successful validation that addresses basically refers to the contract that resides on Blockchain. This address is accessible to any user as it is made public and can be used without a single constraint.

Following a consensus algorithm, the proposed smart contract has the following rules based on the type of the object.

If the Object Type is "Master" it has to consider the following rules, mentioned below:

1) Master is allowed for signing tickets only.
2) It is responsible for the creation of the Group at blockchain level with only a unique identifier of the Group which does not already exist on the Blockchain.
3) Master being out of service, should not affect the functionality of rest of the Group or 'trusted vicinity'.
4) Any object can be master.

If the Object Type is "Follower" it has to consider the following rules, mentioned below:

1) The follower cannot be associated with more than one Group.
2) It only exists or is associated if its Group exists.
3) It is not allowed for the creation of a new Group.
4) The first transaction of follower requires authentication done by using a ticket that is signed by the group identifier's (Master) private key.

If the Object Type is "End User" it has to consider the following rules, mentioned below:

1) End users are customers who generate access request to access certain IoT devices through a smart contract.
2) They can access one or more IoT device upon successful authentication.

If the Object Type is "Admin User" it has to consider the following rules, mentioned below:

1) The first Admin is the creator or owner of the smart contract.
2) Admin owns one or more IoT devices.
3) Admin is the entities who manage access control list of end-users and their permissions to access IoT devices.
4) They are also responsible for adding, registering and de-registering of IoT devices to their respective vicinities.
5) Upon successful authentication, Admins through smart contract allows end-users to access their required IoT devices.

If the Object Type is both "Master and Follower" they have to consider the following rules, mentioned below:

1) The Obj_Id of both Master and Follower must be unique but same Grp_Id if they belong to the same Group or 'trusted vicinity'.
2) Their key-pair and public addresses must be unique.
3) Messages must be communicated between the objects of the same Group as well as other groups that exist on the Blockchain, and rest are considered malicious.
4) All the exchanged transaction and messages should be signed and verified.

IV. RESULTS AND DISCUSSION

Implementation of IoT requires lots of privacy and security related issues to be addressed. We have proposed an authentication mechanism using Blockchain which provides a decentralised solution, overcoming the issues of centralised or central authority (CA), which causes huge scalability issues, being single point of failure, expensive

and etc. The proposed authentication mechanism increases the network connectivity of IoT and builds trust between all the devices. This mechanism is useful in both user-to-device and device-to-device communication in an IoT network. The user, when authenticated by following the mentioned protocols, is given access to any IoT device, ensuring secure access and the devices in an IoT network are allowed to communicate with each other once a trusted vicinity is created and devices are authenticated, and they can also communicate with the devices of other trusted vicinities but considers those devices malicious which are non-member devices. However, the implementation of the proposed mechanism is to be done in future.

In an IoT network, we not only ensure the secure flow of data and information but also to identify authenticated devices. In the Blockchain based authentication system every device is connected in a peer-to-peer manner following a consensus protocol. Every device is identified using their unique public key, which is generated by the system.

Our proposed mechanism ensures the security of the IoT network without relying on a centralised system and keep the system secure against the following attacks mentioned below:

Man-In-The-Middle (MITM) Attack: Following our proposed mechanism, MITM attack is guaranteed to not happen as messages or transactions are sent to devices using their public/ private key and hash technique, so only authorised users and devices will receive the message. Messages on the receiver side will be ignored in case of any modification made to the message. None the less message exchange in Blockchain also uses a digital signature concept which makes it more secure.

Impersonation Attack: All the transactions that took place in the blockchain network are mined and verified by the Blockchain using digital signature and mining process. Each user and device has their own unique identity in the system using process of authentication.

Replay Attack: the network power in the blockchain environment cannot be captured more than half by any device. Every sent or received transaction is recorded in the blockchain ledger after being verified and mined. So none of the transaction can be transmitted in the network for multiple times.

Denial of Service (DoS) Attack: Every broadcasted transaction goes through a verification process in the network, to check if the transaction is valid or not. So DoS attack is almost impossible to occur.

Most of the existing approaches relies on Bitcoin, which basically takes 10mins for block creation and validation, a huge interval of time which is not tolerated by some IoT devices. Whereas some approaches uses Ethereum but address other security goals such as access control, authorisation etc. as mentioned in [14] [24]. However, the author [13] have proposed an authentication mechanism in which the devices are allowed to communicate with each other in their respective bubble only, whereas IoT requires the devices to communicate in overall IoT ecosystem where needed. Still, Blockchain implemented security mechanisms have various issues, and most of the efficient existing solutions are often centralised, e.g. Public Key Infrastructure (PKI) [12] which has its own problems like a single point of failure, expensive etc.

V. CONCLUSION

Security is and will always remain an essential aspect of software and hardware products. Any security breach to devices, networks and people can cause catastrophic consequences. Internet of Things (IoT) is an innovative technology, consists of multiple devices and has many applications. Each device must be reachable and produce content that can be retrieved by any authorised user. In many cases, access to these devices and their communication exchanges should be secure. For numerous reasons, the security issues are the major hurdle in the adoption and deployment of IoT on a large scale since it is highly vulnerable to attacks. In this paper, we propose an Ethereum based Blockchain authentication mechanism to secure the internet of things environment by creating secure zones. Our proposed approach can be applied to various contexts of IoT, their services and scenarios. As our approach relies on a public type of Blockchain, therefore, all the security properties are ensured. In the future, we intend to implement the proposed mechanism by writing the smart contract in solidity language using Remix IDE and to evaluate its performance in terms of cost and time.

REFERENCES

[1] K. Fazal, H. Shehzad, A. Tasneem, A. Dawood, and Z. Ahmed, "A Systematic Literature Review on the Security Challenges of Internet of Things and their Classification," *Int. J. Technol. Res.*, 2017.

[2] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of things: The road ahead," *Computer Networks*. 2015.

[3] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of Things security: A survey," *Journal of Network and Computer Applications*. 2017.

[4] C. Stamford, "Gartner Says By 2020, More Than Half of Major New Business Processes and Systems Will Incorporate Some Element of the Internet of Things," *Gartner.com*, 2016. .

[5] M. Conoscenti, A. Vetro, and J. C. De Martin, "Blockchain for the Internet of Things: A systematic literature review," in *Proceedings of IEEE/ACS International Conference on Computer Systems and Applications, AICCSA*, 2016.

[6] M. Alizadeh, S. Abolfazli, M. Zamani, S. Baaaharun, and K. Sakurai, "Authentication in mobile cloud computing: A survey," *Journal of Network and Computer Applications*. 2016.

[7] Z. Zheng, S. Xie, H. N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *Int. J. Web Grid Serv.*, 2018.

[8] Y. Yu, Y. Li, J. Tian, and J. Liu, "Blockchain-Based Solutions to Security and Privacy Issues in the Internet of Things," *IEEE Wirel. Commun.*, 2018.

[9] A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito, "Blockchain and iot integration: A systematic survey," *Sensors (Switzerland)*. 2018.

[10] M. Vukolić, "The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2016.

[11] M. Ma, S. M. Preum, W. Tarneberg, M. Ahmed, M. Ruiters, and J. Stankovic, "Detection of Runtime Conflicts among Services in Smart Cities," in *2016 IEEE International Conference on Smart Computing, SMARTCOMP 2016*, 2016.

[12] R. Alur *et al.*, "Systems Computing Challenges in the Internet of Things: A white paper prepared for the Computing Community Consortium committee of the Computing Research Association," *Comput. Community Consort.*, 2015.

[13] M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, "Bubbles of Trust: A decentralised blockchain-based authentication system for IoT," *Comput. Secur.*, 2018.

[14] A. OUTCHAKOUCHT, H. ES-SAMAALI, and J. Philippe, "Dynamic Access Control Policy based on Blockchain and Machine Learning for the Internet of Things," *Int. J. Adv. Comput. Sci. Appl.*, 2017.

[15] R. Almadhoun, M. Kadadha, M. Alhemeiri, M. Alshehhi, and K. Salah, "A User Authentication Scheme of IoT Devices using Blockchain-Enabled Fog Nodes," in *Proceedings of IEEE/ACS International Conference on Computer Systems and Applications, AICCSA*, 2019.

[16] O. Alphand *et al.*, "IoTChain: A blockchain security architecture for the Internet of Things," in *IEEE Wireless Communications and Networking Conference, WCNC*, 2018.

[17] E. F. Jesus, V. R. L. Chicarino, C. V. N. De Albuquerque, and A. A. D. A. Rocha, "A Survey of How to Use Blockchain to Secure Internet of Things and the Stalker Attack," *Secur. Commun. Networks*, 2018.

[18] S. C. Cha, J. F. Chen, C. Su, and K. H. Yeh, "A Blockchain Connected Gateway for BLE-Based Devices in the Internet of Things," *IEEE Access*, 2018.

[19] P. Angin, M. B. Mert, O. Mete, A. Ramazanli, K. Sarica, and B. Gungoren, "A blockchain-based decentralised security architecture for Iot," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2018.

[20] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in *2017 IEEE International Conference on Pervasive Computing and Communications Workshops, PerCom Workshops 2017*, 2017.

[21] R. Li, T. Song, B. Mei, H. Li, X. Cheng, and L. Sun, "Blockchain for Large-Scale Internet of Things Data Storage and Protection," *IEEE Trans. Serv. Comput.*, 2019.

[22] A. Z. Ourad, B. Belgacem, and K. Salah, "Using blockchain for IOT access control and authentication management," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2018.

[23] W. Liang, M. Tang, J. Long, X. Peng, J. Xu, and K. C. Li, "A secure FaBric blockchain-based data transmission technique for industrial internet-of-things," *IEEE Trans. Ind. Informatics*, 2019.

[24] A. Ouaddah, A. Abou Elkalam, and A. Ait Ouahman, "FairAccess: a new Blockchain-based access control framework for the Internet of Things," *Secur. Commun. Networks*, 2016.

[25] X. Zhu and Y. Badr, "A survey on blockchain-based identity management systems for the internet of things," in *Proceedings - IEEE 2018 International Congress on Cybermatics: 2018 IEEE Conferences on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart Data, Blockchain, Computer and Information Technology, iThings/Gree*, 2018.

[26] Jamil, Mohsin, Asim Waris, Syed Omer Gilani, Bilal A. Khawaja, Muhammad Nasir Khan, and Ali Raza. "Design of Robust Higher-Order Repetitive Controller Using Phase Lead Compensator." IEEE Access 8 (2020): 30603-30614.

[27] Bashir N, Jamil M, Waris A, Khan MN, Malik MH, Butt SI. Design and Development of Experimental Hardware in Loop Model for the Study of Vibration Induced in Tall Structure with Active Control. Indian Journal of Science and Technology. 2016 Jun;9:21.

[28] Khan MN, Jamil M, Gilani SO, Ahmad I, Uzair M, Omer H. Photo detector-based indoor positioning systems variants: A new look. Computers & Electrical Engineering. 2020 May 1;83:106607.

[29] Kashif H, Khan MN, Altalbe A. Hybrid Optical-Radio Transmission System Link Quality: Link Budget Analysis. IEEE Access. 2020 Mar 18;8:65983-92.

[30] Zafar K, Gilani SO, Waris A, Ahmed A, Jamil M, Khan MN, Sohail Kashif A. Skin Lesion Segmentation from Dermoscopic Images Using Convolutional Neural Network. Sensors. 2020 Jan;20(6):1601.

[31] Uzair M, D DONY RO, Jamil M, MAHMOOD KB, Khan MN. A no-reference framework for evaluating video quality streamed through wireless network. Turkish Journal of Electrical Engineering & Computer Sciences. 2019 Sep 18;27(5):3383-99.

[32] Khan MN, Gilani SO, Jamil M, Rafay A, Awais Q, Khawaja BA, Uzair M, Malik AW. Maximizing throughput of hybrid FSO-RF communication system: An algorithm. IEEE Access. 2018 May 25;6:30039-48.

[33] K. Rahim, H. Tahir, and N. Ikram, "Sensor Based PUF IoT Authentication Model for a Smart Home with Private Blockchain," in *ICAEM 2018 - 2018 International Conference on Applied and Engineering Mathematics, Proceedings*, 2018.

[34] L. Wu, X. Du, W. Wang, and B. Lin, "An Out-of-band Authentication Scheme for Internet of Things Using Blockchain Technology," in *2018 International Conference on Computing, Networking and Communications, ICNC 2018*, 2018.

[35] S. Chauhan, R. Sobti, G. Geetha, and S. Anand, "Cryptanalysis of SHA-3 candidates: A survey," *Res. J. Inf. Technol.*, 2013.