International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-11 Issue-1, October 2021

Rethinking Blockchain for Access Control in the Internet of Things

Poonam Ninad Railkar, Parikshit Narendra Mahalle, Gitanjali Rahul Shinde

Abstract: ***IoT is a network of interconnected heterogeneous devices which sense, accumulate the data and forward the same to the cloud platform for analytical purposes. There are various IoT verticals in which huge research is going on. IoT security is the most challenging research area in which researchers are investing a huge number of efforts. The challenges in IoT security include access control, trust management, authentication, authorization, privacy, and secured device to device communication. To overcome these, this paper gives an overview of proposed trust based distributed access control approach in IoT. Some of the challenges and threats can be controlled by blockchain technology. Basically, blockchain is an open and distributed ledger of records that can be verified efficiently and stored permanently. This paper checks the feasibility study of the applicability of blockchain in the IoT ecosystem to apply access control mechanism and privacy-preserving policies. This paper discusses how access control and privacy can be addressed by blockchain without compromising security. This paper consists of rigorous gap analysis which is done on the top of comprehensive literature survey. The paper also addresses the challenges and issues which can be faced while applying access control mechanism using blockchain in the context of IoT.***

Keywords: Access Control, Attack, Blockchain, Internet of Things, Security, Threats.

I. INTRODUCTION

Nowadays, use of the Internet of Things (IoT) is increasing vertically and horizontally in every industry and almost used in all fields like medical area, smart home, transport, offices, school, smart grid to provide easy life and automation services. IoT is a communication network of heterogeneous devices which are manageable over the internet and now become a constraint technology. The embedded technology enables devices to interact with each other via the internet. In view of this, a lightweight and scalable trust-based Access Control is needed in resource constraint IoT environment [1]. In IoT ecosystem, any devices can connect to anything anywhere using any network path. IoT gives us comfort and convenience at the same time, various IoT threats are emerging. These threats can be a big challenge in the privacy and security of collected data. For securing access to these devices there is need to take specific requirements into consideration such as, resource constrained nature of devices. IoT application provides services worldwide to millions of devices. These devices can be resource constrained or powerful devices and to provide secure access to these devices is a critical task to handle. In this digital distributing era granting/denying access to IoT device is top security concerns. It is critical for distributed IoT devices, as most of devices are resource constrained in nature. There are various access control policies present for IoT but most of them are based on a centralized model. However, this approach may not be suitable for ubiquitous access. In case of frequent updates in access control permissions; this centralized model can become a bottleneck and a single point of failure. To overcome these problems some distributed access control solutions are also available like capability-based access control, role-based access control, and attribute-based access control systems. Access control systems like access control list, role-based access control, attribute-based access control are not able to support all features like concurrency, scalability, interoperability, consistency, attack resistant, and decentralized to meet requirements of IoT ecosystem. Distributed access control in IoT network is one of the major challenges as resource constraint and heterogeneous devices are there. Decentralized approach of access control allows us to govern a large variety of heterogeneous devices in scalable mode. If an attacker is able to hack the access control mechanism of devices, the sensitive information of the IoT ecosystem may be compromised. So, the efficient and distributed access control mechanism needs to be provided for IoT devices due to resources constraints characteristics of IoT ecosystem. Blockchain Technology is gaining much more attention from various business domains, due to its wide variety of applicability and security. Basically, blockchain is an immutable ledger of transaction records that can be maintained in a distributed manner and also used a decentralized model. Blockchain provides high reliability and honesty. The transaction made with the help of the blockchain broadcasts in the whole blockchain network. Blockchain technology uses a hash function to make block immutable. Hash code is attached to every block to validate a block. Majority in the network has a copy of the valid block, so no one tampers or modifies this block. This technology is built on the top of cryptography, peer to peer network and blockchain protocol.

Manuscript received on August 31, 2021.
Revised Manuscript received on September 26, 2021.
Manuscript published on October 30, 2021.
*Correspondence Author
Poonam N. Railkar*, Assistant Professor, Department of computer Engineering, STES's Smt. Kashibai Navale College of Engineering, Pune (Maharashtra), India.
Parikshit Mahalle, Professor and Head, Department of Artificial Intelligence and Data Science, Vishwakarma Institute of Information Technology, Pune (Maharashtra), India.
Dr. Gitanjali Rahul Shinde, Assistant Professor, Department of Computer Engineering, Vishwakarma Institute of Information Technology, Pune (Maharashtra), India.

The blockchain has its own special design data storage structure and the transactions can be made without involving third-party verification. It does not require any central authority which lowers centralized cost for administration and verification. It records every transaction that was made. Same entry of transaction will be updated in all ledger copies of the network. Blockchain has the ability to overcome challenges like distributed and trustworthy access control and privacy in a distributed IoT network [2]. This is one side of Blockchain. However, this technology also faces few challenges like heavy computation and storage. So, it is a challenging task to integrate blockchain with a resource constrained environment. This paper covers possible dimensions in the context of access control of blockchain technology, including security, limitations, and challenges. In this paper technical aspects of blockchain technology in IoT are also presented. This paper also discusses access control for secure machine to machine communication and highlights the required characteristics and common architectures of IoT. In addition to this, application and characteristics of blockchain in IoT are also highlighted. The key challenges and issues that need to be taken into consideration while implementing blockchain in resource constraint environment are discussed. How challenges of traditional centralized and distributed access control schemes can be resolved with the blockchain technology are discussed in this paper and gives a complete survey whether blockchain will be useful for access control in IoT or not? The emphasis of this paper is also elaborating basic terminology of blockchain including smart contracts and crypto currency and the role of smart contracts in the context of IoT is also elaborated.

II. MOTIVATION

A. Submission of the paper

Nowadays billions of smart devices are connected to the internet and it is continuously growing, so by 2022 95% products will have IoT in our daily life. These large numbers of devices are continuously generating and exchanging data which are confidential and if any attacker is successful to access this data, then the user's data gets compromised which leads to many consequences. For example, Banking data, Military information etc. Applying security to this vast information and protect it from the attacker is a big challenge.

IoT supports distributed architecture and hence centralized access management is another problem. If this central management is failed because of any attack, suppose by DDoS attack then services getting by these devices will stop. Generally, central cloud service provider is used in IoT environment. So, there is need for decentralized and dynamic access management.

III. INTERNET OF THINGS OVERVIEW

In the current era, IoT becomes a buzzword of information technology. The IoT has the ability to change the real-world objects into intelligent objects that can sense, communicate and compute the data. Based on these parameters, devices can take the decisions.

IoT is acting as the umbrella under which various technological stack resides which strengthen the IoT stack. Now, IoT is becoming a well- known concept in various verticals and horizontals of various domains including common individual's everyday life, agriculture, and military and so on [3]. IoT is the convergence of various technologies so technological revolution of IoT depends on the various underlying technological stack which can range from the wireless sensor network to nanotechnology

A. IoT Architecture

IoT created endless opportunities in various domains, hence every business organization wants to include IoT products or smart devices in their business process. But when we try to fit these products in business scenarios it becomes a challenging task because of a number of devices and a variety of conditions or requirements make them work. This scenario occurs due to the inability to develop the architecture of IoT that satisfy the business as well as technical requirements. The application specific architecture of IoT remains limited to that particular domain. This becomes one of the hurdles in understanding the scope of IoT centric approaches. There is a need of generic architecture of IoT that will help to improve technical understanding, implementation methodology and identifications of various tools for IoT application developers, such architecture directly or indirectly helps to solve challenging real time problems. The overall idea of IoT can be described by looking it in a layered way as shown in figure 1.

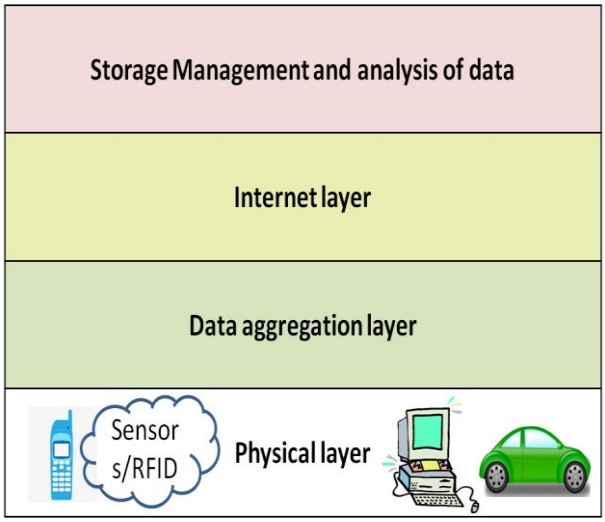

Figure 1: Layered IoT Architecture

3.1.1 Physical layer

At the physical layer, all the sensors, actuators and smart devices are placed. These sensors have the ability to convert information obtained from real world to data which is useful for data analysis. Sensors have very much significant in IoT architecture framework because these sensors actually provide all time information that actually processed. The actuators are the devices which have the ability to convert electrical energy to mechanical energy. These actuators help to perform an action based on a decision made with the data analysis. The actuating and sensing provide the facility to collect the data and perform the required actions. These sensors sense the environmental parameter and send the information to middleware or data aggregation system.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

3.1.2 Layer 2: Data aggregation layer:

When sensors collect real-time information, the information is forwarded to Data aggregation layer which can also be called as middleware. Actually, this layer is working very closely with the physical layer. The sensor network is connected to gateway devices or middleware. The gateway devices and middleware devices generally work through Wi-Fi, LAN. When middleware devices get the data from sensors, generally middleware devices pre-process that data. The data getting from the previous stage is very huge. The middleware squeezes that huge amount of data into an optimal size of data and this data is put into the dataset for further analysis. This layer is responsible for taking decision based on the data that devices have. This layer is also responsible for data conversion. This layer helps to convert the data in required format. This conversion is required in terms of timing and structure of data.

3.1.3 Layer 3 Internet layer:

Now at the middleware, we have data which is structured and ready for analysis. This data needs to be forwarded to the cloud for storage and processing. We cannot make a decision at the gateway or middleware because gateway or middleware has a limited amount of memory and computational power. So, middleware performs its task and forwards the data to cloud through the internet. Actually, we cannot use the traditional protocol stack for data transmission because the traditional protocol has more overhead and require more computation power for processing. So, it is always recommended to use a lightweight protocol which will minimize the overhead packet processing. There are various IoT protocols used like MQTT, COAP etc that really help to transfer data. JSON objects can be used for data transmission which are widely used as network supported format.

3.1.4 Layer 4 storage management and analysis of data:

Before this layer, whatever data is prepared will be provided to edge technologies for analysis and visualization purpose. Most of the time cloud platform will be the estimation place for the data. At the same time, some additional operations may be performed before data reached to the data centre. After this, data is received to the data centre or cloud. Here in-depth processing of the data is done. This in-depth processing of data is in repetitive manner. This affects the quality of data which enhance decision and prediction making. In this layer both IT and operational professionals are required. After checking all quality parameters this information will be brought back to the real world in the form of reports, actions, decisions or predictions.

B. IoT applications

IoT has tremendous possibilities due to which IoT has a wide variety of applications in various domain. There are various IoT applications out of which only a few applications are deployed. In the next future, we can see various IoT applications ranging from smart home to smart cities. The following section describes the various application areas.

3.2.1. Aerospace and defense

The traffic in the air is also increasing day by day. Airbus global market forecast that in next each year air traffic will be increased by at least 4.5 % and almost 30000 aircraft will be required in the next 20 years. So, we need to consider this business domain also. IoT has the ability to provide solutions to the aerospace industry based on data. Airbus companies collect, manage and analyse the data which is generated by sensors and smart devices. This data also helps to find faults in the aircraft. The smart and connected devices help Airbus manufacturers and operators to lookout for vertical performance by concentrating on fuel consumption, downtime, and optimization in route. The Airbus manufacturers now in search of the security of products or systems and also increased investment in IoT technologies. Identification of potential applications and relative mature IoT system is key to design and develop IoT products in the aerospace industry.

3.2.2. Healthcare Industry

Nowadays IoT becomes a fundamental building block of any healthcare application. The objective of any IoT enabled healthcare system is to provide real-time data of the patient to its associated doctors. The healthcare project named Ewall is developed in European countries under the FP7 program. This project is developed for elder adults who are living independently. The sensors are deployed over the wall of the house and some sensors are placed on the body which collects to make the activity of the patient. If some abnormal behaviours or readings are observed, then message will be sent to both caretaker and caregivers i.e., doctors and family members. IoT devices enable the possibility of monitoring patient remotely at the same time there are security and privacy issues which need to be addressed. IoT helps to keep patients healthy and also improve the delivery of care [4].

3.2.3. Agriculture domain

IoT has implemented in agricultural domains which helps to improve the productivity of the farm. IoT has the ability to transform this sector from farm to folk by contributing to food safety, reducing agricultural input and food waste. IoT based large scale pilots can be used in entire supply chain management. Hydroponic is a new agricultural methodology can be efficiently used to improve the productivity of the farm. In this type of farming, all the crops are planted in materials call media and these seeds which are planted in media put into the plastic pipe by making a hole on the pipe. We need to provide required nutrition through the water. The plants absorb the nutrition from the flowing water[5]. We can completely automate end to end process with IoT. This technology can help the farmers to improve productivity.
Likewise, IoT can be implemented in various domains including the media entertainment industry, insurance industry, recycling, environment monitoring, transportation, process industry, manufacturing industry, retail, logistics, supply chain management, and pharmaceutical industry and so on. There is a huge list of IoT applications that help to make human life better.

C. Issues and challenges

Although IoT has spread in various domains and successfully solved numerous problems still facing few issues and challenges. The most important challenges are the security and privacy of data. There are some applications like healthcare, military, aerospace, atomic research centre, etc, which generate sensitive data. If the security of such data gets compromised,

in that case it may lead to huge financial loss or death of an individual user. So, there is a need for efficient lightweight algorithms and protocols that ensure security as well as privacy of any IoT application.

The next challenge is data management. The IoT ecosystem is generating a huge amount of data and we are collecting this huge amount of heterogeneous data from various sensors to make strongly connected system. This data is too huge for the current computer system, so many resources are attracted towards big data IoT.

Resource constraint devices are also a major issue in IoT. In IoT ecosystems at one end, we have resources constraint devices. These resource constraints devices are having very low memory, low processing capacity and low computational power in IoT ecosystems. We need to make sure that those resources constraints device synchronizes with high-end devices. In such use cases, high-end devices are underutilized due to resource constraints environment. Data is travelling from one end to another end over the internet. There are some open issues like standardization of IoT that are not integrated into some specific comprehensive frame. The existing infrastructure is not suitable for IoT ecosystems, there is a need for IPV6 enabled network infrastructure. The IoT open issues can be viewed in different perspectives i.e., infrastructural perspective, data management perspectives, and computational intelligence perspective.

In the infrastructural perspective, a generic framework is expressed within which IoT applications can be developed easily. There is a need for a more flexible way of communication that will enhance the capability of the IoT ecosystem. The decentralization and heterogeneity have their own impact on IoT application. But we must decide which part needs to be centralized or decentralized and up to what extent decentralization can be done. At the same time, there is a need for protocol stack, a number of IP addresses, etc. From data management perspective extraction of useful data out of the huge amount of data is a challenging task. Processing of this big data in resource constraints environment is also challenging. Memory, computation and bandwidth requirement are must for analyse IoT ecosystems.

From a computational intelligence perspective, the problem is that how to make system smart and make useful decisions. The current data mining and machine learning algorithms is still lagging to calculate correct inferences for the heterogeneous dataset.

Many times, data produced by IoT devices are private and sensitive, but some traditional access control systems cannot have control on the leakage of data or some access control methods improve privacy and security of data as well. Depending on the importance of data, strong access methods are needed on resource constraint devices as well as on powered devices, otherwise data will be compromised and leads to many consequences.

IV. ACCESS CONTROL

A. Overview of Access Control

Access control provides a way of limiting access to computational physical or virtual resources. It is granted to a user to access these resources. Before providing an access control list to the user, the user must be authenticated and authorized. There are various access control policies or methods are present. There are various access control policies like mandatory access control, discretionary access control, role-based access control, attribute-based access control, etc [6]. Before deciding access control policy, we must consider below measures:

1. Try to analyze the information in terms of its confidentiality level, sensitivity, privacy and integrity relate to organizations and users. Consider worst-case use cases.
2. Determine the way of communication between the data creator and data owner.
3 Specify the way of providing access control list i.e., manual or automatic based on account creation.
4. Decide the role of user in application.
5. Align closely access control policies with organization access control policies.
6. Describe the way of granting permissions [7].

B. Access control and IoT

In IoT, ecosystem device collects the information and interact with each other. During the exchange of information with other devices puts the security and privacy of data at risk. We have to make sure the digital identity of billions of devices on the internet should not be exposed.

Existing access control mechanism:

The access control mechanism ensures that shared resources will be accessed by only legitimate users. Access to the resource is protected by limiting the rights of users. Comparative summary of some of access control models is summarized in table 1.

Some access control mechanism is presented here:

1) Mandatory Access Control: In Mandatory Access Control (MAC) the administrator of the system provides access control list (ACL) to each user to access resources. The security permissions are assigned to users and resources independently. Only the administrator has privileges to modify security permissions associated with both the user and resources. This model is very expensive to implement, but such models can be used in military applications [16].

2) Access Control Matrix:

Access control matrix (ACM) is a two-dimensional matrix in which the first dimension is users and another dimension is resources and there is a mapping of permission on that particular object. The permission can be read, written and executed. The user can have any subset of this permission set. Access control matrix has a good mapping of who can access what. The size of the matrix and the complexity of the matrix could be the two great challenges of this access control mechanism. Due to these challenges, this access control mechanism, we cannot use in the context of IoT. Many access control mechanisms are developed on the top of this mechanism.

3) Access Control List:

Access Control List (ACL) is developed on the top of the ACM and can be implemented by using linked list data structure, here the list starts with the object and these objects are linked to subjects. In some scenario, ACL can be referred as identity-based access control because the identity of the user is used as a characteristic. ACL object contains the rights associated with subject which range from empty set to {R, W, X, D}.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

In IoT ecosystem, access control mechanism depends on various parameters like type of device, time and location but ACL considers identity as a fundamental parameter.
This is a limitation of Access control list. Revocation of any privileges is time consuming and not secure in IoT environment.

Table- I: Comparative summary of the state of art for access control

Access Control Model	Scalabi-lity	Hetero-geneity	Privacy	Trust	Selective Disclosure	Principle of least privileges	lightweight calculation	Distributed
TAACS [42]	H	H	M	Yes	No	No	Yes	Yes
ABAC using blockcha in [43]	H	H	L	Yes	No	No	Yes	Yes
RBAC [8,9]	M	H	L	No	No	No	No	No
	M	H	L	Yes	No	No	Yes	No
ABAC [10]	M	M	M	Yes	No	No	Yes	Yes
UCON [11]	L	M	H	Yes	No	No	No	Yes
CAPBAC [12, 13]	H	L	M	Yes	No	No	Yes	Yes
	H	L	M	No	No	Yes	Yes	Yes
LCap [44]	H	H	No	No	No	No	Yes	No
Fabic IoT [45]	Yes	Yes	-	-	No	No	No	Yes

H: High, M: Medium, L:Low

4) Capability based Access Control:
This access control also depends on ACM. Here capability is token. In this scheme, access control mechanism uses a list in which each subject is associated with set of one or more pair of objects and its set of permissions. Capability-based access mechanism is handled by accessor, not by resources. Various variations of capability-based access control are provided as a solution for access control in IoT [17][18].
5) Role based Access Control:
Role based Access control (RBAC) is used as one of the oldest access control mechanism studied in 1990 and become standard in 1996. In RBAC, the role is a key criterion for accessing resources. Each role is linked with a set of operations which defines access rights. RBAC has various advantages like scalability, central library for policy, but it is very difficult in IoT environments [16].
6) Relationship-based Access Control:
It is one of the latest access control mechanism which introduces the idea of a binary relationship. This scheme uses a binary relationship between accessor and resources. Authors claimed that this methodology can be used for general purposes but mostly this methodology is used for social media application. But we can implement this scheme by defining friendly relation between devices.
7) Attribute Access Control:
Attribute Access Control (ABAC) is more abstract than RBAC. This scheme uses attributes like name, job, title, responsibilities or other attributes like time, location for access permission. System-wide updating is difficult in ABAC [19] [20].

C. Issues and Challenges

1. Principle of least privileges: Deciding limiting access rights to perform particular task is challenging.
2 Inter-organisational access control is challenging in distributed environment.
3. Need to provide the optimum solution for access control for the different use case.
4. Dynamic access control for IoT devices are a challenging task.
5. If a central server is used for worldwide access control for billon of IoT devices, then it will be a challenging task to manage them [2].
6. There are challenges like interoperability, and scalability to address in resource constraint devices [21]

V. BLOCKCHAIN

A. Overview of blockchain

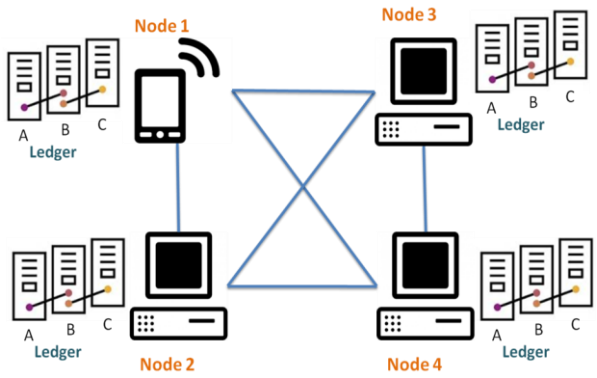

Figure 2: Overview of Blockchain

As IoT is changing many vertical markets and industry, the same way blockchain is emerging technology which is going to affect next three to five years. Satoshi Nakamoto invented blockchain technology in 2008 to build bitcoin and implemented in 2009. Bitcoin is digital crypto-currency worked on peer-to-peer network in distributed environment using blockchain technology. Currently when you want to transfer money from one account to another account you require banks in between, but in bitcoin exchange there is no need of any central management and third party. In blockchain to achieve security cryptography is used. Blockchain is distributed database which consists of blocks, each of which contains encrypted data and have unique hash which is generated by selecting any hash algorithm. In blockchain network as per figure 2 every node has same copy of ledger. If any device tries to modify the ledger, it will be easily detected as the hash will change. Before adding a new block in the network one of the nodes validate that block and once validated, it is broadcasted to other nodes.

Without consent of others nodes no one can alter block, as each block has hash value. So, blocks in ledger are immutable and tamper proof.

B. Building blocks of blockchain

Following are main building blocks of blockchain. Sample of distributed blockchain is shown in figure 3. Valid and verified transactions are stored in form of block that is linked to previous one. A blockchain starts with genesis block which is nothing but initial block. To create new block hash value of the previous block is entered. In distributed blockchain, as shown in figure 3 Peer B has the exact copy of blockchain peer A has. So, any changes to any block would result in different hash code and thus immediately visible to all participants in the blockchain.

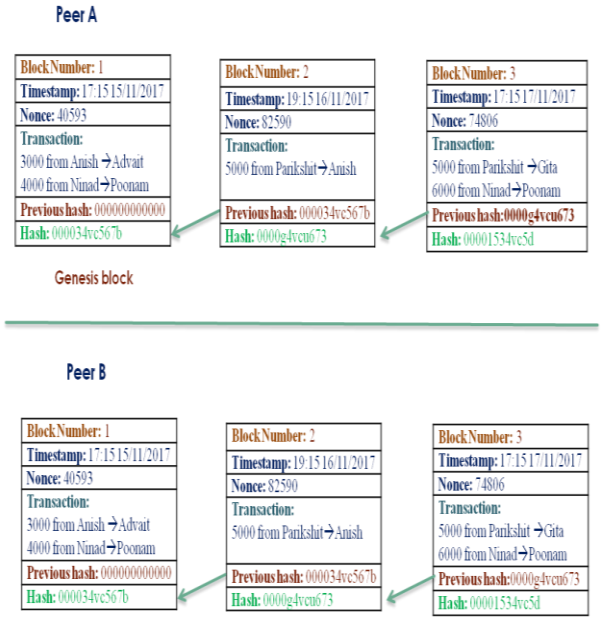

Figure 3: Sample of distributed blockchain

1. Block: In blockchain technology, data is stored in forms of blocks. They form a chain of blocks. Blocks are assembled in chronological order. The first block is called genesis block. Each block consists of a header and a set of transactions. Size of block header is 80 bytes long string [22][23]. Block header stored information as follows:

i) Timestamp: Require 4 byte to store. It records at what time block created.

ii) Version: Require 4 byte to store. As there are different versions of blockchain, there is need to mention which version is used

iii) Merkle root: Require 32 byte to store. It is similar to binary tree. In first step for every transaction hash value is created. In next step each pair of hashes of two transactions are combine and find new hash value for it. It continues till top to get one hash which is at merkle root [24] as shown in figure 4. If there are odd number of transactions then last transaction hash combine with itself to create new hash value.

iv) Nonce: Require 4 byte to store. Nonce stands for number used once. It is used to create different hash. Miners in blockchain solve puzzle to get nonce value.

v)Difficulty target: Require 4 byte to store. This is proof of work algorithm. Here difficult target is decided. To achieve this target nonce value gets changed by miners.

vi)Previous hash: Require 32 byte to store. It stores hash value of previous block which is used to link the blocks.

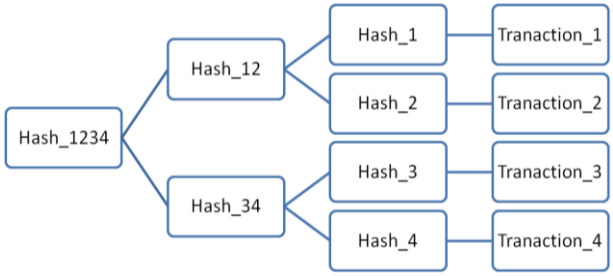

Figure 4 Merkle root

2. Transaction:

It is a small unit of task or operation stored in the block. After executing some set of operations and before store it to block it get validated from majority nodes in the network. After validation only, these set of transactions are stored in blockchain. These records stored permanently in the block. You can view these records any time but cannot modify these records.

3. Hash:

Hash function is a mathematical function which takes an arbitrary length of data as input and returns fixed length of hash. Hash is digital finger print for each block which is fixed in length. Input can be any certain amount of data; it can be 100 of pages. After applying the hash function on this data, that function generates a fixed-length hash value. There are multiple hash algorithms available. Mostly SHA256 hash algorithm is used to produce a hash value. This algorithm generates a 256-bit length hash value. Each block contains its own hash value and the previous hash value which are used to link blocks sequentially. The hash table is also maintained for fast retrieving.

4. Consensus Mechanism:

Blockchain is distributed ledger as it stored over multiple nodes in the network. To stored blocks in the ledger, it should validate first by the majority of nodes. To approve these blocks consensus mechanism is required. There are multiple consensus mechanisms are available. Some of the consensus mechanisms are Proof of Work (PoW), Proof of stake (PoS), Proof of Space (PoSp), Proof of Capacity (PoC), Proof of Elapsed Time (PoET), Proof of Deposit (PoD).

C. IoT and Blockchain integration approaches:

It can be used in following application:

1. Smart city can be secured using blockchain [25].

2. In IoT ecosystem, resource constraint devices are connected to the gateway and this gateway is connected to the blockchain network for secure access control management [26].

3. To provide decentralization and maintain privacy between peer to peer blockchain is also used[27]

4. To provide security and privacy in smart home application blockchain concept is used [28]. Proof of Work is eliminated to avoid extra computational power.

5. In [29] system they have managed IoT system using Blockchain. More than thousands of devices are managed using blockchain technology.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

They have used RSA public key cryptosystem. They are storing public keys in Ethereum and private keys on devices

D. Blockchain platforms

Multiple blockchain platforms are available in nowadays. Some of them are explained are as follows:

1. Ethereum: Ethereum is open source. It has distributed computing capability and it is more for decentralised application. The inventor of Ethereum is Vitalik Buterin. Ethereum is a platform where Ether cryptocurrency is used. It supports smart contract that is scripting functionality. If programming code references any contract then we called it as smart contract. Smart contract is plan of codes run on Ethereum network which provides trust.

2. Hyperledger: Hyperledger is global collaboration open source blockchain based project [30]. Main contributors of this projects are IBM, SAP Ariba, and Intel and hosted by Linux Foundation. It is not Ethereum blockchain. Hyperledger got so many members from different field like banking, supply chain, aviation technology. All these companies came together and working on this open-source project.

3. BigchainDB: BigchainDB is a database which supports features of Blockchain. BigchainDBis open-source distributed database combination of big data and blockchain [31]. It supports characteristics of blockchain like an immutable ledger, decentralization control. This supports federation consensus model [32]. It used in both public and private network. It also provides transaction privacy and supports smart contracts.

E. Applications of blockchain

1. Healthcare: Using blockchain technology Patients personal records can be stored in an encrypted format. Only those individuals who have the private key can access that data. Receipt of operations can easily be transferred to medi-claim or to insurance companies. These companies also keep trust on these receipts as it uses tamperproof blockchain ledgers.

2. Smart property: Property like land, patent, car and house can use blockchain technology for small contracts. Once property transfer is recorded in blockchain ledger no one can modify it. Any flaws can also be found in property ownership using this distributed ledger.

3. Cryptocurrency: Many Cryptocurrency uses blockchain technology. This technology is used in Bitcoin, Ethereum, Peercoin, Litecoin and so on.

4. Supply chain management: Tracking and tracing of goods can be handled very properly using blockchain.

F. Challenges

1 Lower-power devices-

Implementing a Blockchain mechanism with lower-power devices (like IoT gadgets) required a light weight platform. IoT has light-weight protocol stack which has been used to sense the action, compute the decision and communicate with the concerned thing. To provide security at network layer using Blockchain requires a high computing server where action will be evaluated and depending on that decision will be taken care. This is the fundamental challenge developers will face while working with light-weight platforms.

2.Efficiency-

In general, the mathematical hash function used to calculate hash value for each block in block-chain consumes 2-3 minutes. This challenge can be overcomed via high performance computing platform, but ultimately it leads to more Power Consumption. More research opportunity is available for geeks in this area.

3. Implementation Cost-

One of the recently built leading programmed Blockchain is Ethereum and currency that has been used to get access to open banking system is Ether (ETH). Develop the system using this Blockchain methodology to protect our sensitive data is depend on two factors-

i). Platform support required to perform minimum 15 operations per second is expensive and

ii). Skilled developers are required to design the secured systems, which also costs more money. As per the 2018 data published by Burning Glass Technology, there is huge increase (i.e., 316%) for Blockchain developer positions primarily in United States [33].

4. Scalability-

Blockchain mechanism is scalable for small size and medium size P2P network where less than thousand numbers of operations have been performed. For public blockchain processing rate is 7-15 TPS for Ethereum [34]. So scalability becomes an issue where more than numerous operations (like Visa application) have been involved [34].

VI. ACCESS CONTROL USING BLOCKCHAIN TECHNOLOGY

A. Design issues

Looking over a blockchain implementation in real time, points out the following design issue.

1. Design Issue with respect to Blockchain Implementation:
To incorporate blockchain mechanism to provide security for data in real time change is required in existing features and that needs to be collaborated at some common place.

2. Deciding appropriate Consensus Algorithm-
This is a building block for using blockchain in real time, because it provides a security solution on distributed platform through which node connected in peer-to-peer network can perform an agreement regarding inclusion of new block in the current chain. If decision made in selecting Consensus algorithm is not accurate then it will lead to increase the rework cost for environment setup.

3. Attack 51%: There is one unavoidable security threat comes in picture i.e., attack 51%, if more than 50% of nodes in P2P network delivering incorrect data then the provided data becomes correct.

4. Energy: More energy has been utilized to perform specified actions in blockchain network [24]

B. Challenges of Access control in IoT using blockchain:

1. Designing access control using blockchain technology is a challenging task as blockchain requires powerful devices to execute proof of Work to validate and store block in a blockchain network [35].

2. To create a generic model to make compatible with a different access control mechanism [36]

C. How blockchain useful for access control in IoT:

Internet of Things (IoT) and Blockchain are two trending giants of the recent industrial and products world. Amalgamation of these two will result out into a big revolution, which will help to establish a Smart Life. The more focused domain for IoT applications is Security and it can achieved through combining IoT and Blockchain together. In simple way, there is high possibility to create a Smartly Secured Sensor based Computing and Connected solutions. Also, another considerable plus here is encrypted data and data stored in distributed network provides security to end-to-end communication in real-time IoT applications without third party or human interventions [37]. This way Security hurdle will get resolved.

Currently working IoT applications (such as Home Automation to control power consumption) are using third-party solutions to achieve security benefits. However due to presence of third-party tool/person the sensitive data is not completely secured, there is still options for grey-code hackers to tamper the system and steal the data. IoT applications are using various access control mechanism to secure the data and end-to-end communication. Access control models are usually being used to enable the identity management and authentication methods. [38] The decentralized access control models like Access Control List (ACL), Role Based Access Control (RBAC), Attribute Based Access Control (ABAC) can be used to enhance the security in IoT application that to without involving third party vendors solution [39]. In decentralized systems end-users has directly connection with IoT gadgets, but users can access those gadgets with token based authorization. And these tokens have been shared with trusted personnel. Apart from ACL other two access control models i.e., RBAC and ABAC do not require updating the user list rather it needs to update the user access rights and access policies. Downside of using these models to provide security is risky as it difficult to handle access rights and policies. Smart thing in IoT are low powered, low memory and also not able to perform complex computation on its own.

Which is why the new smart era requesting for simplistic way to provide the trustworthy secure solution for developing IoT applications? To fill this gap, Blockchain is playing a role of helping hand to do the same. Through the usage of Blockchain only the authorized resources can access the data stored on smart things. And this way data as well as end-to-end message delivery will be protected. With this approach security has been achieved but it slows down the overall performance of the system. There is still more awareness and new best optimal methods required to provide better support to use Blockchain for establishing efficient access control mechanism for IoT.

In [2] designed architecture for scalable access control in IoT using blockchain. They stored access control information in distributed environment using blockchain technology. Here resource constrained devices are not part of blockchain network. But management hub is there to handle communication between these IoT devices with blockchain network. Manager entity is there who decide access control policies and it interacts with smart contract to define these policies.

System [36] uses controlchain blockchain approach for access control in IoT. This system is decentralized which does not require third-party, compatible with many access control model present in literature. It also supports offline working, avoid the central point of failure and resilient to data corruption.

Tamper-proof Identity-based Access Management is implemented using blockchain technology [21]. This system supports scalability in terms of number of client connection and avoids the central point of failure.

[40] Implements contract based distributed and trusted access control mechanism for IoT ecosystem. This system includes multiple access control contract (ACC), one register contract (RC) and one judge contract (JC). JC judges the misbehaving of subject to decide the penalty accordingly. ACC support static access control based on previously defined policies and also support dynamic access control based on misbehaviour of subject. RC registers all information of misbehaving, smart contract and access control.

New Fair Access mechanism using blockchain technology is introduced in [41] This system is decentralized and preserving the privacy of data.

VII. TRUST BASED DISTRIBUTED ACCESS CONTROL MODEL FOR IOT:

This section gives overview of proposed trust based distributed access control approach in IoT. Basic operation of proposed approach is shown in figure 5.

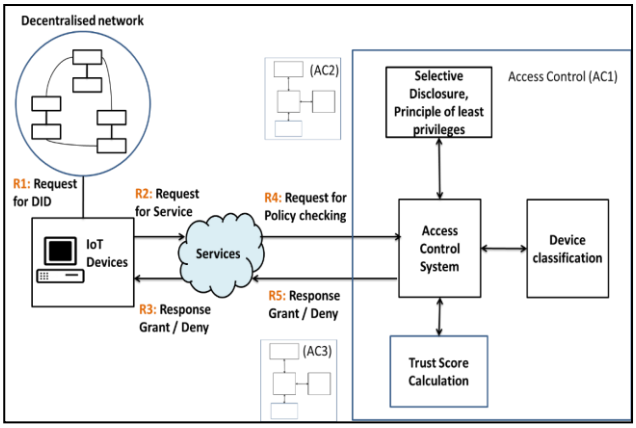

Figure 5: Trust Based Distributed Access control Model for IoT

In this proposed system all devices have Distributed Identifier (DID). Based on DID authentication takes place which will provide selective disclosure. Smart-device sends request to access the resources of device or service. Each device is classified as Expedient devices, semi- Expedient devices, or Non-Expedient devices. When the device receives an access request, it checks the trust score of the subject device and also checks device type.

According to device classification and trust score calculation permission mappings will happen dynamically. This approach will support the principle of least privileges means the only required resources will allocate to provide service as per request.

VIII. CONCLUSION

IoT Security getting more and more attention from its initial phase of network evolution because the security of data becoming more challenging.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

With the exponential growth of IoT devices, the security threats to data, devices, and communication are also increasing in all directions. To secure the IoT ecosystem there is the need for strong access control policies, privacy-preserving policies, and trust management mechanisms. From the security perspective blockchain technology can become a solution to the IoT ecosystem. IoT and blockchain are distributed in nature. From an architectural perspective integration of both may be possible but from the implementation perspective, resource constraint environment can be the problem. The resource constraint devices in IoT unable to fulfill the requirement of computational power. This paper also talks about the challenges and issues which can be faced while implementing blockchain in the resource constraint environment of IoT. It is necessary to optimize the blockchain working principle for the resource constraint environment. In view of these issues and challenges in the access control mechanism, we proposed architecture for distributed, and dynamic access control that will be scalable, attack resistant and trustworthy.

REFERENCES

1. P. N. Railkar, P. N. Mahalle and G. R. Shinde, "Access Control Schemes for Machine to Machine Communication in IoT: Comparative Analysis and Discussion," 2018 IEEE Global Conference on Wireless Computing and Networking (GCWCN), Lonavala, India, 2018, pp. 59-63, doi: 10.1109/GCWCN.2018.8668639.
2. Novo, Oscar. "Blockchain meets IoT: An architecture for scalable access management in IoT." IEEE Internet of Things Journal 5.2 (2018): 1184-1195.
3. Madakam, S., Ramaswamy, R., & Tripathi, S. (2015). "Internet of Things (IoT): A literature review". Journal of Computer and Communications, 3(05), 164.
4. Dewangan, K., & Mishra, M. "Internet of Things for Healthcare: A Review." nternational Journal of Advanced in Management, Technology and Engineering Sciences, ISSN NO : 2249-7455, Volume 8, Issue III, MARCH/2018.
5. Brewster, C., Roussaki, I., Kalatzis, N., Doolin, K., & Ellis, K. (2017). "IoT in agriculture: Designing a Europe-wide large-scale pilot" IEEE communications magazine, 55(9), 26-33.
6. Sara Sinclair "Access Control In and For the Real World", Technical Report TR2013-745, Department of Computer ScienceDartmouth College November 2013 https://pdfs.semanticscholar.org/0c20/c5a1cd5fc19a58938bd6aad09990eb58abed.pdf
7. https://www.cgisecurity.com/owasp/html/ch08.html
8. Zhang, Guoping, and Jiazheng Tian. "An extended role based access control model for the Internet of Things." Information Networking and Automation (ICINA), 2010 International Conference on. Vol. 1. IEEE, 2010.
9. Jindou, Jia, Qiu Xiaofeng, and Cheng Cheng. "Access control method for web of things based on role and sns." Computer and Information Technology (CIT), 2012 IEEE 12th International Conference on. IEEE, 2012.
10. Ye, Ning, et al. "An efficient authentication and access control scheme for perception layer of internet of things" Applied Mathematics & Information Sciences 8.4 (2014): 1617.
11. Guoping, Zhang, and Gong Wentao. "The research of access control based on UCON in the internet of things." Journal of Software 6.4 (2011): 724-731.
12. Anggorojati, Bayu, et al. "Secure access control and authority delegation based on capability and context awareness for federated iot." River Publishers 5 (2013): 135-160.
13. Hernández-Ramos, José L., et al. "DCapBAC: embedding authorization logic into smart things through ECC optimizations." International Journal of Computer Mathematics 93.2 (2016): 345-366.
14. Kim, Ji Eun, et al. "Seamless integration of heterogeneous devices and access control in smart homes." Intelligent Environments (IE), 2012 8th International Conference on. IEEE, 2012
15. Fremantle, Paul, et al. "Federated identity and access management for the internet of things." Secure Internet of Things (SIoT), 2014 International Workshop on. IEEE, 2014.
16. Ravidas, S., Lekidis, A., Paci, F., Zannone, N., "Access control in internet-ofthings:A survey", Journal of Network and Computer Applications (2019), doi: https://doi.org/10.1016/ j.jnca.2019.06.017
17. Gusmeroli, Sergio, Salvatore Piccione, and Domenico Rotondi. "A capability-based security approach to manage access control in the internet of things." Mathematical and Computer Modelling 58.5-6 (2013): 1189-1205
18. Andaloussi, Y., et al. "Access control in IoT environments: Feasible scenarios." Procedia computer science 130 (2018): 1031-1036.
19. E. Yuan and J. Tong. "Attributed Based Access Control (ABAC) for Web Services" In Proceedings of International onference on Web Services, pages 561–569. IEEE, 2005.
20. V. C. Hu, D. Ferraiolo, R. Kuhn, A. Schnitzer, K. Sandlin, R. Miller, and K. Scarfone. "Guide to Attribute Based Access Control (ABAC) Definition and Considerations", NIST Special Publication 800, NIST, 2014.
21. Nuss, Martin, Alexander Puchta, and Michael Kunz. "Towards blockchain-based identity and access management for internet of things in enterprises." International Conference on Trust and Privacy in Digital Business. Springer, Cham, 2018.
22. https://www.fundera.com/blog/blockchain-explained
Atlam, Hany F., and Gary B. Wills. "Technical aspects of blockchain and IoT." Role of Blockchain Technology in IoT Applications 115 (2019): 1.
23. https://www.coindesk.com/information/blockchains-issues-limitations
24. Biswas, K.; Muthukkumarasamy, V. "Securing smart cities using blockchain technology", In Proceedings the 18th IEEE International Conference on High Performance Computing and Communications; 14th IEEE International Conference on Smart City; 2nd IEEE International Conference on Data Science and Systems (HPCC/SmartCity/DSS 2016), Sydney, Australia, 12–14 December 2016; pp. 1392–1393.
25. Cha, S.C.; Chen, J.F.; Su, C.; Yeh, K.H. "A blockchain connected gateway for BLE-based devices in the internet of things", IEEE Access 2018, 6, 24639–24649.
26. Conoscenti, M.; Vetrò, A.; De Martin, J.C. "Peer to peer for privacy and decentralization in the internet of things", In Proceedings of the 39th International Conference on Software Engineering (ICSE 2017), Buenos Aires, Argentina, 20–28 May 2017; pp. 288–290.
27. Dorri, A.; Kanhere, S.S.; Jurdak, R.; Gauravaram, P. "Blockchain for IoT security and privacy: The case study of a smart home", In Proceedings of the IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom 2017), Kona, HI, USA, 13–17 March 2017; pp. 618–623.
28. Huh, S.; Cho, S.; Kim, S. "Managing IoT devices using blockchain platform", In Proceedings of the 19th IEEE International Conference on Advanced Communications Technology (ICACT 2017), PyeongChang, Korea, 19–22 February 2017; pp. 464–467.
29. Dameron, Micah. "Beigepaper: An Ethereum Technical Specification." (2017).
30. McConaghy, T., Marques, R., Müller, A., De Jonghe, D., McConaghy, T., McMullen, G., ... & Granzotto, A. "BigchainDB: a scalable blockchain database", white paper, BigChainDB (2016)..
31. Panarello, A., Tapas, N., Merlino, G., Longo, F., & Puliafito, A. "Blockchain and iot integration: A systematic survey", Sensors, 18(8), 2575 (2018)..
32. https://www.computerworld.com/article/3345998/demand-for-blockchain-engineers-is-through-the-roof.html
33. https://medium.com/coinmonks/blockchain-scaling-30c9e1b7db1b
34. Ourad, A. Z., Belgacem, B., & Salah, K. "IOT Access control and Authentication Management via blockchain", Conference: 2018 International Conference on Internet of Things (ICIOT 2018)At: Seattle, USA, June 25 - June 30, 2018
35. Pinno, Otto Julio Ahlert, Andre Ricardo Abed Gregio, and Luis CE De Bona. "Controlchain: Blockchain as a central enabler for access control authorizations in the iot." GLOBECOM 2017-2017 IEEE Global Communications Conference. IEEE, 2017.
36. https://www.forbes.com/sites/bernardmarr/2018/01/28/blockchain-and-the-internet-of-things-4-important-benefits-of-combining-these-two-mega-trends/#701b089e19e7

37. P.N.Mahalle, P. N. Railkar “Identity Management for Internet of Things”, River Publications, Aalborg, Denmark. ISSN Number: 978-87-93102-90-3(Hard copy) 978-87-93102-91-0(Ebook)
38. https://intopalo.com/blog/2015-05-25-access-control-for-internet-of-things/
39. Zhang, Y., Kasahara, S., Shen, Y., Jiang, X., & Wan, J. Smart contract-based access control for the internet of things. IEEE Internet of Things Journal, 6(2), 1594-1605, (2018)..
40. Ouaddah, Aafaf, Anas Abou Elkalam, and Abdellah Ait Ouahman. “FairAccess: a new Blockchain-based access control framework for the Internet of Things”, Security and Communication Networks 9.18 (2016): 5943-5964.
41. Thirukkumaran, R., and P. Muthukannan. "TAACS-FL: trust aware access control system using fuzzy logic for internet of things." International Journal of Internet Technology and Secured Transactions 9, no. 1-2 (2019): 201-220.
42. Ding, Sheng, Jin Cao, Chen Li, Kai Fan, and Hui Li. "A novel attribute-based access control scheme using blockchain for IoT." IEEE Access 7 (2019): 38431-38441.
43. Buschsieweke, Marian, and Mesut Güneş. "Securing critical infrastructure in smart cities: Providing scalable access control for constrained devices." In 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), pp. 1-6. IEEE, 2017.
44. H. Liu, D. Han and D. Li, "Fabric-iot: A Blockchain-Based Access Control System in IoT," in IEEE Access, vol. 8, pp. 18207-18218, 2020

AUTHORS PROFILE

Prof. Poonam N. Railkar received her Master in Computer Engineering (Computer Networks) from Pune University Maharashtra, India in the year 2013. From September 2012, she is currently working as an Assistant Professor in Department of Computer Engineering, STES’s Smt. Kashibai Navale College of Engineering, Pune, India. She has published 20 plus papers at national and international journals and conferences and authored 1 book. She has guided more than 15 plus under-graduate students and 3 plus postgraduate students for projects. Her research interests are Internet of Things, Identity Management, Security and Database Management System Applications.

Dr. Parikshit N. Mahalle graduated from Sant Gadge Baba Amravati University in Amravati, India, with a B.E. in Computer Science and Engineering and an M.E. in Computer Engineering from Savitribai Phule Pune University in Pune, India. Aalborg University in Aalborg, Denmark, awarded him a Ph.D. in Computer Science and Engineering with a specialty in Wireless Communication. He has been teaching and conducting research for almost 18 years. He is currently a Professor and Head of the Department of Artificial Intelligence and Data Science at the Vishwakarma Institute of Information Technology India in Pune, India. He's mentored over 150 undergraduates and 35 post graduate students. students and 30 plus post-graduate students for projects. 3 PhD students. His recent research interests include Algorithms, Inter- net of Things, Identity Management and Security

Dr. Gitanjali Rahul Shinde has obtained his B.E degree in Computer Engineering from Savitribai Phule Pune University, Pune, India and M.E. degree in Computer Engineering from Savitribai Phule Pune University, Pune, India. She completed her PhD from Aalborg University Denmark. From September 2008, she is currently working as an Assistant Professor in Department of Computer Engineering, Vishwakarma Institute of Information Technology, Pune, India. She has published 40 plus papers at national and international journals and conferences. She has guided more than 25 plus under-graduate students and 7 plus postgraduate students for projects. Her research interests are Internet of Things, System Programming, Operating System, Theory of computation and Wireless Communication.