Trust Management in IOT Enable Healthcare System using Ethereum based Smart Contract

Bhabendu Kumar Mohanta, Debasish Jena, Utkalika Satapathy

Abstract: Internet of Things (IoT) is one of the most promising areas for research in the last decade. The numbers of IoT enabled devices developed makes the application of IoT more interesting. The application areas are Insurance sector, Smart Environment Monitoring, Smart City, Healthcare Sector, Smart Transportation, and Agriculture Sector among many other smart device enabled applications. IoT implementation relays on different security and privacy challenges. To make use of IoT in real-life application confidentiality, integrity, authentication, authorization, trust, verification, information storage, and management, availability challenges need to be addressed. In this work, authors have used the decentralized Blockchain technology to address security and privacy issues in IoT enabled applications. Initially, the paper identifies and explained the security and privacy challenges that currently exist in IoT applications. Ethereum virtual machine is used to implement the Blockchain distributed network and healthcare insurance claims is taken as an example to test the proposed solution. Results show that the distributed Blockchain technique provides trust management and address some of the existing security and privacy challenges of IoT enable healthcare insurance sector.

Keywords: Blockchain, Ethereum, Healthcare Insurance, IoT, Smart Contract, Privacy, Security, Trust Management.

1. INTRODUCTION

The number of Internet of Things (IoT) smart devices connected to the different network is already cross the world population. The development of smart devices making easier to implement the real-time application. As shown in figure 1. different applications of IoT. The healthcare sector is one of the most important sectors where a patient condition is monitor using different smart things deployed in the patient body. The patient's health data collection based on IoT-Cloud architecture already explained in paper [1]. The health insurance sector is gradually increasing all around the world. The traditional insurance sector is a centralized system where all these transactions are not known to each other. In a health insurance system, the patient already registered to any insurance company with satisfying all constants by the insurance company. When patients got treatment in hospital and claim the insurance policy there are some issue arises like treatment types, financial claims, time of settlement and trust among. Recently the development of IoT devices has the potential to collect, processing, storage, and analysis the information of patients in real-time. The benefits of using IoT in medical are faster treatment, reduce cost and easy diagnosis. The integration of Blockchain technology with IoT improves and addresses some security issues [2]. The Blockchain technology derived from Bitcoin cryptocurrency proposed by Satoshi Nakamoto one decade ago [3]. In that white paper, Satoshi Nakamoto first time explains the concept of peer to peer transaction of cryptocurrency without involving any third party. All the transactions are also recorded in digital format and stored in all the nodes presents in that network. The users in an IoT application need to build trust among them. The authors explained the trust properties, the importance of trust management and goals of in terms of IoT system in papers [4] [5]. In smart healthcare system different IoT devices are used to monitor the patient condition. Then the collected information are process either in fog computing or in cloud computing depending on the system architecture.

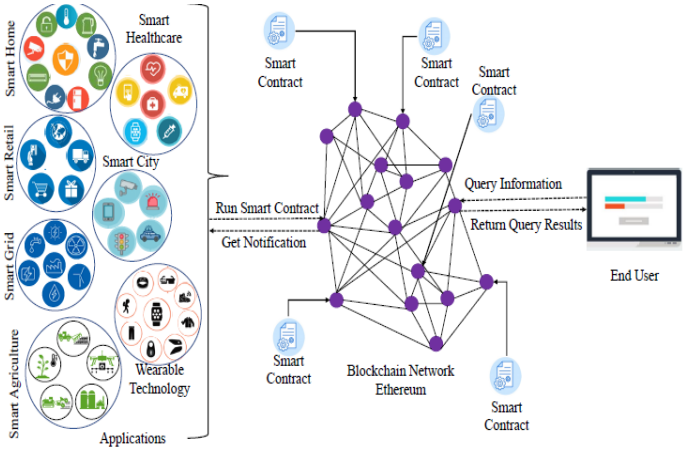

Figure 1. *IoT Applications integrated with Blockchain Based Architecture*

This article explores the following contributions:

- The paper identifies the recent work on healthcare insurance system Integration with Internet of Things.
- The different security and privacy issues are investigated in IoT applications.
- The paper proposed the decentralized Blockchain technique to addresses the exiting security and privacy issues of IoT system.
- The proposed framework uses smart contract for each entity and deployed in the Ethereum network.
- The results show that the proposed model is computationally efficient in decentralized manner for tracking and monitoring the health insurance claims in real time

- *Bhabendu Kumar Mohanta is currently pursuing Ph.D. degree program in Computer science and engineering,IIIT,Bhubaneswar, India,9438658892 E-mail: C116004@iiit-bh.ac.in*
- *Debasish Jena ,Associate Professor, Department of computer Science and enginnering,IIIT, Bhubaneswar, India, debaish@iiit-bh.ac.in, 9437230284*
- *Utkalika Satapathy has master. degree in Computer science and engineering,IIIT,Bhubaneswar, India,8637251732 E-mail: A117010@iiit-bh.ac.in*

Rest of the paper is organized as follows: Literature review regarding the current research on health insurance explains in Section 2. The security and privacy issues of Internet of Things application are identifies in Section 3. In Section 4, the solution approach is analyzed in term of Blockchain concept integration with the IoT. The proposed framework for based on Blockchain concept is shown in Section 5.The implementation details are explained in Section 6.Finally, the paper concludes in Section 7 along with future scope.

2. LITERATURE SURVEY

Since the evolution of the Internet of Things technology, the healthcare sector becomes smart in term of monitoring the patient in real-time or processing the information in quick time. Today health insurance is an important sector associated with medical. Each of the insurance claims passes through a different phase and need lots of documentation as well as time. The traditional system of health insurance claims has lots of uncertainty and there is no trust between the patients, insurance company and hospital. The emerging technology IoT makes the application smart by its associated technologies. Similarly, the Blockchain technology which is a distributed digital ledger can make the system tamper-proof. In recently some of the research articles addressed the Blockchain and IoT uses in the health insurance sector. The insurance sector has moved from traditional based approach to the new approach using the techniques like IoT, Big data and Artificial Intelligence [6]. The fraud claims detection technique using machine learning in health insurance application was proposed in [7]. Since IoT has already used in the healthcare system for monitoring the patients in real-time. In the internet era where everything is stored in digital format, leakage of personal information or privacy of the patients is in real risk. The sharing of information and computing of data need to be done securely. The challenges to implementing the healthcare sector in a distributed way where everything is securely shared and compute explained in [8]. The Blockchain has the potential to share the digital information to all the, not in distributed structure and all the transactions are immutable once recorded. Some of the research articles already available which addressed the use of Blockchain technology in the health sector for security and privacy issue [9], [10], [11].

3. SECURITY AND PRIVACY ISSUE IN IOT

IoT becomes a most emerging technology and its use cases are many. The recent development of sensors, actuator, and sensors enable device. The application of IoT is almost each and every filed. Because of lightweight, real-time data read, easy connectivity and lots of application are being developed using IoT. The application of IoT becomes really be implemented and deployed if all the issues are addressed. As IoT devices are low processing power, limited storage existing encryption technique or security protocols are impossible to apply. Here challenges are to be developed a lightweight security protocol or design architecture in such a way that IoT device work securely and available always. The basic IoT architecture consists of the three-layer physical layer, network layer, and application layer. Each of these layers has security and privacy issue exist. In the following subsection, the details security and privacy issue of the IoT Systems are discussed.

3.1. Security challenges in IoT

IoT devices are developed by the manufacturer mostly ignoring the security aspect of the device. If an attack occurs in the IoT device like during communication network means if Zigbee device is a hack then all the sensors connected to that network can be compromised. In that situation, replacing the Zigbee device or manufacturer again that hardware device makes expensive and not recommend also. So here\the challenge is developed secure system architecture in such a way that all the hardware devices are accessed by properly authenticated users. Beside this there is different security threads are available in IoT.

3.1.1. Authentication

Authentication problem is one of the major issues in the IoT system. As for authentication purpose, existing techniques are used password based, smart card based, or fingerprint based but none of the authentication technique work for the low-end devices. In an IoT application, every node needs to be properly authenticated to the system for secure data access or transfer.

3.1.2. Authorization

Authorization means the devices must have permission from a Central authority or from a decentralized network to receive or send the data in a network. The permission must be given to process any data in the network. In an IoT decentralized architecture authorization is one of the challenges, how to authorizes each node in the network.

3.1.3. Confidentiality

In an IoT network as large numbers of sensors and IoT enable devices like fog node or edge node are used for real-time processing of data at the edge of the network. The confidentiality of each node must be maintained. Otherwise sensitive information of the nodes may be hack by the attacker.

3.1.4. Non-Repudiation

Non-Repudiation means denying the authenticity of any transaction or operation done in a system. This type of attack possible when there is no proper authentication orlog file maintained in a system. In an IoT system, lots ofsensitive information flows between different nodes, sothe system needs to have proper authenticate process.

3.1.5. Data Leakage

Data Leakage simply means the transmission of sensitive information from within an organization to external parties via an electronic medium or a physical medium. The types of information that is leaked are: Intellectual properties, Health records, confidential information, and customer data.

3.1.6. Trust Management

In an application associated users must trust each other. In a traditional based system, central server is the trusted party. Each and every transactions detail is stored in that party. The trust management is one of the issues in traditional base system.

3.2. Privacy Challenges in IoT

In an IoT system users unaware of his/her data use. The means how the IoT devices values are collected and who

has the accessing power. The most the application end user not knew the data processing and transfer. As personal information involves like health care system, smart home application, or smart transportation system if the attackers get access to the network he/she can monitor the system and predict the future event. In a decentralized IoT, architecture privacy becomes more difficult to achieve.

4. Integration of Blockchain with IoT

Since its development, IoT is providing some interesting application like smart city, smart home and smart healthcare system. The living quality of the people has increased through automation and digitization of the system. Most of the application share data communicate and perform computation in a centralized system or untrusted way. The application needs to address the security, privacy, reliability and scalability issues. So Blockchain being the decentralized system having properties like scalability, autonomy, reliability, secure, immutable and trusted can solve the issue of IoT application. IoT can benefit from the Blockchain concept if integrated in a proper way. The block details are shown in Figure 2.

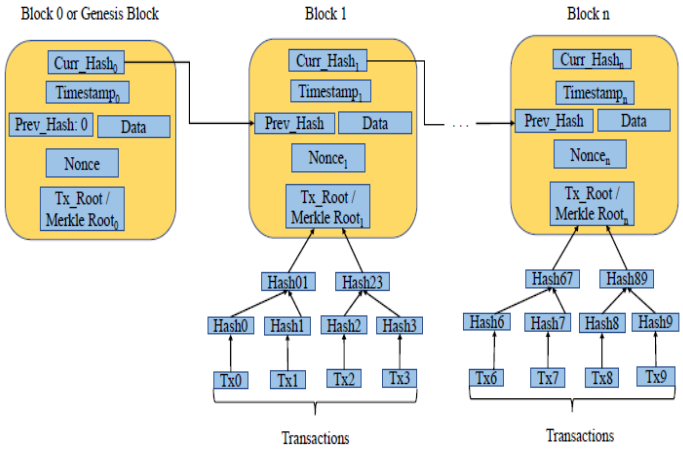

***Figure 2**. Details attributes of a Block in a Blockchain system.*

4.1. Solution Approach using Blockchain on Different Attacks

4.1.1. Authentication and Authorization of IoT Devices

In a traditional way, authentication is performed using a central server. The Blockchain-based smart contract has the ability to provide IoT devices authentication in a decentralized way like multiparty authentication. The Bubbles of Trust is a technique proposed where IoT device are authenticated in a decentralized way in [12]. Smart contract based Blockchain can do the authorization of IoT devices in less complexity compared with traditional authorization technique. The smart contract is also used to update software or hardware, even put some policy control for authorization of devices.

4.1.2. Confidentiality and Non-Repudiation

In a Blockchain system, each transaction is encrypted and goes through a verification process before adding to the block format. Each node has a unique hash address and using ECC based digital signature node are authenticated and using smart contract different authorization are given to the nodes. So in a blockchain system user confidentiality maintained. Non-repudiation is not possible in the Blockchain system. As each node send a message and its digital signature(Private key) to another node. So the identity of the transaction owner is validated by decrypting the message with the sender public key. later part no one can deny that transaction is not done by him/her. During the registration process, each node gets a unique identification number which is recorded in the blockchain so node tampering is also not possible. Blockchain uses the Public key cryptographic concept to deals with authentication. Once proper authentication is done non-repudiation and node tampering can be avoided.

4.1.3. Data leakage and Trust Management

In a Blockchain system based IoT system, all the data arecryptographically secure and digitally signed by the sender. All the data flow in the network are stored in a digital ledger format. So there is no chance of data leakage or performed data transit attack in Blockchain based system. As al, the nodes have the same copy of transaction so they can verify any other transaction. The node identity can be identify using the unique key and their digital signature which increases the trust among all users,

4.2. IoT Applications a Blockchain Solution Approach

In figure 1. smart IoT based applications are design in Blockchain concept. Blockchain architecture may be a permissioned model or permissionless model. IoT devices are connected to the different intermediate system, it may be fog nodes. These intermediate nodes are connected in s distributed way for communication and computation purpose. For efficient and reliable decision making process multiparty computation is better than single node taking a decision. As per the application requirement need to developed the smart contract and deployed in the Blockchain based platform. Presently two widely use Blockchain platform are available Ethereum and Hyperlegder fabric. A smart contract is a self-executable program as per requirement if that program runs it gives the corresponding output. In many applications like smart home monitoring system if a fire occurs alarm or notification can be sent to the responsible user. similarly in the smart healthcare system, if any collected information needs quick response using fog computing and blockchain based smart contract, immediate action can be taken place once get the alert. In some smart application, action can be taken quickly if the event is known before it takes place. Finally, as Blockchain system is secure, tamper-proof, distributed and immutable makes the IoT system more secure and robust.

5. PROPOSED FRAMEWORK FOR HEALTHCARE INSURANCE

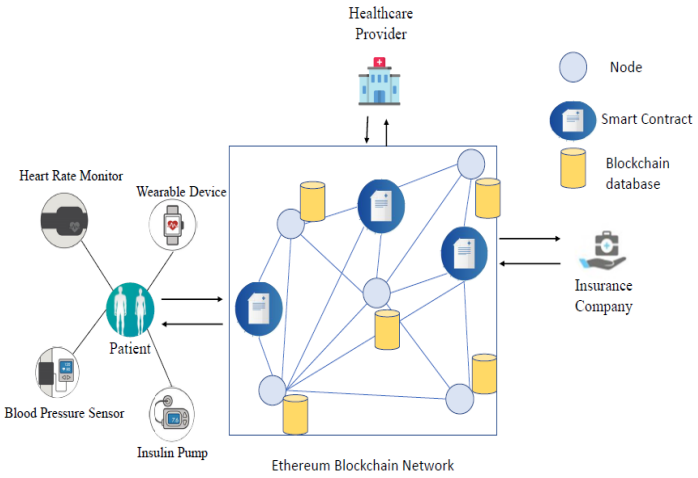

Figure 3. *The proposed framework for Healthcare Insurance Claims in Distributed Blockchain Network.*

The insurance sector is one of the most demanding sectors nowadays. As insurance may be health, vehicle, home, any electronic instrument, there are many different types of insurance coverage type are exist.. A patient can start the health cover insurance by register through the hospital or by directly through an online system. Insurance company verified the claim insurance and approve accordingly. Lastly, hospital after patient treatment is over put the final money claim to the insurance company directly. Once the hospital gets the approval from the insurance company, the patient is discharged. In traditional system some of the problems are:

- Patient never knows actually how much amount paid by the insurance company and date and time of released.
- Communication is between mostly two-party these more than two parties involved.
- There is no transparent way of information communicated.
- There is no trust between the users.

6. IMPLEMENTATION DETAILS

Ethereum is an open-source decentralized public and permissionless blockchain based platform providing computer application to run on top of it. It lets developers program their own smart contract using solidity language without needing to build their own blockchain. The applications running on the Blockchain can communicate in the Blockchain network with each other and the complete network of an interconnected application called decentralized applications (Dapps) is being developed using this. The Ethereum platform has a shorter block time than bitcoin which makes it more convenient to run applications on top of it. Blocks and the record of cryptocurrency transaction are done by Ethereum, which is done very quickly and leads to quicker transactions. Ethereum processes a large number of the transaction happening on the network without the user waiting too long.

6.1. Experimental Environment Details

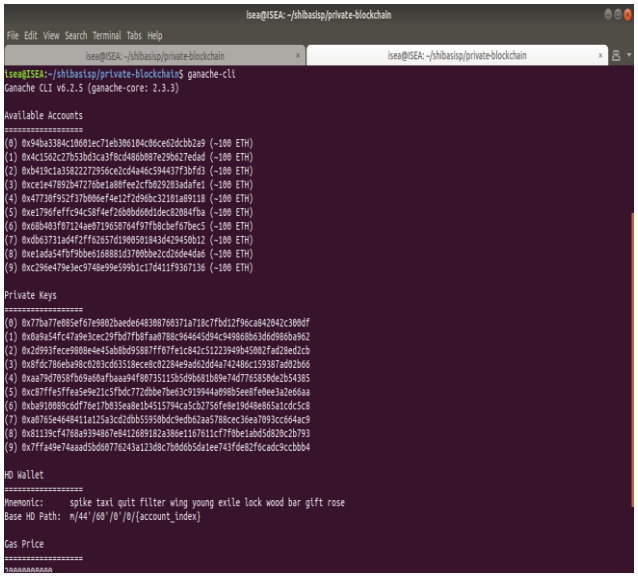

Figure 4 *Ethereum Decentralized Virtual Machine Platform*

For Ethereum deployment to create the Blockchain virtual network one system is used having configuration 2.2GHz Intel Core i5-5200U processor with 8GB of RAM Linux as the operating system. As shown in figure 4 Ethereum platform of ten users having unique hash identity created for network communication. Using the unique identity, nodes can transfer message from one to another digital by signature concept. Digital signature means to add a digital code with the electronically transmitted message so that others can verify. The advantages of using digital signature are authenticating the content, user identity is verified, and it prevents non-repudiation. The uniqueness with the digital signature is that each document has a unique code. The Blockchain system uses a digital signature so that each node can transmit the message using its own signature and other nodes can verified it.

6.2. Smart Contract for IoT application

A smart contract is a tiny computer program that runs on the blockchain. It is just like a physical contract but it doesn't require trusting a 3rd party for operating. It enables a certain task to be automatically executed once some pre-defined conditions are triggered.Because the smart contract is stored inside a Blockchain, it runs in a completely decentralized manner. With this technique, no one in the network can gain control of the assets. As they are stored on a Blockchain, they inherit some interesting properties:

- It is immutable i.e the smart contract can never be changed once it is deployed into the blockchain. So, no one can tamper the code of the smart contract behind your back.
- It is distributed i.e everyone in the network validates the output of the smart contract. So, an attacker can't force the contract in a certain way because this attempt will be spotted by the other nodes in the blockchain network and they will mark this attempt as invalid.

- It can work as multi-endorsement accounts, such that smart contract is executed only when a required number of nodes endorses.
- It can store useful information about an application such as registration and domain information.

The smart contract uses in different IoT application and challenges are explained in paper [13]. As shown in the Figure 3. smart contract can be written and deployed in Blockchain based Ethereum network.

6.3. Smart Contract based Healthcare Insurance system for experimental purpose

In this paper, after Blockchain based Ethereum platform is created in a system. For validation and verification purpose healthcare Insurance system is taken as an IoT application. As shown in figure 3. in healthcare system three entities are patient, insurance company, Healthcare system. The smart contract for each of these entities are written using solidity and deployed in the Blockchain network. In this example initially patient smart contract will automatically execute whenever the patient input condition are satisfied and the message is transfer in the network. The message is shown by both hospital and insurance company. Then subsequently all the events took place are recorded in digital format and available for all three entity in the Blockchain network. The security and privacy issue address by this system are Address space of IoT devices, Authentication, authorization, secure communication, trust management, data authentication, integrity, secure computation.

6.3.1. Smart contract code

```
……
pragma solidity >=0.4.21 <0.6.0;
address [ ] insurance;  // admins of the system
struct Token
        {
        byte32 UID;
        address insurance;
        address patient;
        address hospital;
}struct insurance
                {
                address patient;
                address hospital;
                }
mapping( address=>patients[ ] ) public patients_insurance
mapping( address=>hospitals[ ] )public hospitals_insurance
modifier onlyinsurance {
        bool insurance=false;
      for(uint256 i=0; i<insurance.lenth; i++)
        {
         If( msg.sender==insurance[i])
                {
Insurance=true;
      break;}
    }
}
Function addPatientInsuranceMapping (address patient, address hospital) public onlyinsurance{
        Bool patientExists=false;
 For(uint256 i=0; i<hospital_insurance[hospital].length; i++ )
        {
          If (hospital_insurance[hospital][i]==insurance)
                {
Hospital=patients_insurance[msg.sender][i].hospital;
                insuranceExists=true;
                break;
          }
        }
  If(insuranceExists)
{
Patient_insurance[patient].push(insurance(insurance,hospital);
patientinsuranceMappingAdded(patient,insurance,msg.sender,hospital):
}
Else
    insuranceDoesnotExist(insurance,hospital,msg.sender);
}
 Function addInsuranceHospitalMapping(address hospital, address insurance) public  onlyinsurance{
Hospital_insurance[hospital].push(insurance);
HospitalInsuranceMappingAdded(hospital,insurance,msg.sender)
}
  event Create(string login);
   event ClaimInitiate(string login, address from, address to);
   event ClaimApprove(string login, address from, address to);
    event ClaimSettlement (string login, address from, address to);
  event ClaimClose(string login, address from, address to);
……
```

6.3.2. Results and security analysis

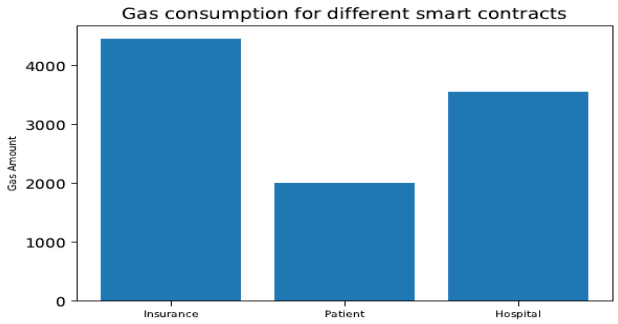

Figure 5. *Gas consumption for different Smart Contract in Ethereum network in deployed state.*

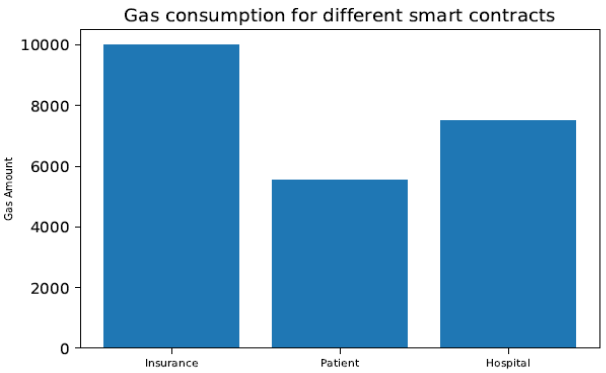

Figure 6.. *Gas consumption for different Smart Contract in Ethereum network during execution state.*

As shown in figure 5 and figure 6 the gas utilization of the Ethereum virtual machine during different smart contracts execution. The smart contracts are deployed in the blockchain network and execute automatically when any event gets triggered. As per the proposed distributed network all the transactions are recorded in digital format with only authorized users. In this work as private Blockchain is used for implementation purpose. All the nodes are initially authenticated to the system. The input data collected from different sensors devices are forwarded for further processing in the Blockchain network. Each entity has a smart contract for all the functionality. The smart contract executes as per the functionality and triggers the corresponding events. During message transmission digital signature is used along with the message so the non-repudiation is avoided.

7. CONCLUSION AND FUTURE WORK

IoT is one of the most promising areas of research in the last decade. Using the concept of IoT many applications are developed such as smart home, a smart environment monitoring smart traffic management, and so on. All these applications are great to use as without human interaction. The application can run in real-time using different sensors, actuator, and smart devices. Healthcare insurance is one of the most promising sectors across the world. In traditional insurance, the system has an issue like trust management, insurance claims clarity, processing delay, and settlement issue. In this paper, the authors proposed a framework based on Blockchain technology where all the participants entity are connected in a distributed way. The Ethereum virtual machine was used as a Blockchain platform for implementation purpose. As it is private Blockchain al entities are registered initially. The smart contract designs for each entity for different functionality. The results shown the smart contract are run using less gas during execution. Here all the insurance claims process are recorded in digital ledger format using the digital signature which built the trust among the associated users. In future authors will like to implemented in public Blockchain environment so that more users participant in the network and multiparty computation can be address.

REFERENCES

[1] Jaiswal, Kavita, Srichandan Sobhanayak, Bhabendu Kumar Mohanta, and Debasish Jena. "IoT-cloud based framework for patient's data collection in smart healthcare system using raspberry-pi." In 2017 International Conference on Electrical and Computing Technologies and Applications (ICECTA), pp. 1-4. IEEE, 2017.

[2] Reyna, Ana, Cristian Martín, Jaime Chen, Enrique Soler, and Manuel Díaz. "On blockchain and its integration with IoT. Challenges and opportunities." Future Generation Computer Systems 88 (2018): 173-190.

[3] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008.

[4] Z. Yan, P. Zhang, and A. V. Vasilakos, “A survey on trust management for internet of things,” Journal of network and computer applications, vol. 42, pp. 120–134, June, 2014.

[5] G. Lize, W. Jingpei, and S. Bin, “Trust management mechanism for internet of things,” China Communications, vol. 11, no. 2, pp. 148–156, February, 2014.

[6] Silvello, A. "IoT and Connected Insurance Reshaping The Health Insurance Industry. A Customer-centric" From Cure To Care" Approach." ICST Trans. Ambient Systems 4, no. 15 (2017): e5.

[7] Sun, Chenfei, Qingzhong Li, Hui Li, Yuliang Shi, Shidong Zhang, and Wei Guo. "Patient cluster divergence based healthcare insurance fraudster detection." IEEE Access 7 (2018): 14162-14170.

[8] McGhin, Thomas, Kim-Kwang Raymond Choo, Charles Zhechao Liu, and Debiao He. "Blockchain in healthcare applications: Research challenges and opportunities." Journal of Network and Computer Applications (2019).

[9] Nguyen, Dinh C., Pubudu N. Pathirana, Ming Ding, and Aruna Seneviratne. "Blockchain for Secure EHRs Sharing of Mobile Cloud based E-health Systems." IEEE Access (2019).

[10] Dwivedi, Ashutosh Dhar, Gautam Srivastava, Shalini Dhar, and Rajani Singh. "A decentralized privacy-preserving healthcare blockchain for iot." Sensors 19, no. 2 (2019).

[11] Siyal, Asad, Aisha Junejo, Muhammad Zawish, Kainat Ahmed, Aiman Khalil, and Georgia Soursou. "Applications of Blockchain Technology in Medicine and Healthcare: Challenges and Future Perspectives." Cryptography 3, no. 1 (2019).

[12] M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, “Bubbles of trust: A decentralized blockchain-based authentication system for IoT,” Computers & Security, vol. 78, pp. 126–142, September, 2018.blockchain cloud architecture for IoT,” IEEE Access, vol. 6, pp. 115–124, February, 2018.

[13] Fotiou, Nikos, and George C. Polyzos. "Smart contracts for the internet of things: Opportunities and challenges." In 2018 IEEE European Conference on Networks and Communications (EuCNC), Ljubljana, Slovenia,2018,pp. 256-260.