EAI Endorsed Transactions
on Internet of Things
Research Article EAI.EU

Systematic Literature Review of Security Solution Using Blockchain in Internet of Things (IoT)

Sana Zeba[1,*] and Mohammad Amjad[2]

[1]Research Scholar, Dept. of Computer Eng. Jamia Millia Islamia, New Delhi, India
[2]Professor, Dept. of Computer Eng. Jamia Millia Islamia, New Delhi, India

Abstract

Advanced computerization and quick growth Internet of Things (IoT) System used sensors for functioning according to sense. The fast growth and evaluation of the IoT environment, increased security challenges and security problems of the system because of its wireless connectivity and centralized architectures, etc. In the current situations, Blockchain technology is the most emerging and growing technology in the security area of Internet of Things applications, because of its Peer-to-Peer and decentralized nature. In this paper, our goal line is to performed Systematic Literature Review with summarized existing problems and solution related to the securities in the Blockchain based Internet of Things and the IoT system. Research questions are used to declared problems in the SLR. Through the contribution of research questions and literature survey conclude the actual security problems on the Internet of things and mechanisms of solutions with Blockchain.

Keywords: IoT Architecture, Internet of Things (IoT), Blockchain in IoT, Security and Privacy in IoT, Types of Blockchain

Received on 31 May 2020, accepted on 15 June 2020, published on 25 August 2020

doi: 10.4108/eai.17-8-2020.166002

*Corresponding author. Email: sanazeba.mau@gmail.com

1. Introduction

In the recent era, the wireless Internet of Things (IoT) becomes a rich courtesy field in the smart environment. It's rapidly increased the bigger number of intelligent devices in the system and it is effectively emerged devices and physical environments through the Internet and create a smart system. Firstly, the Internet of Things network was invented in 1998 and developed in 1999 by Kevin Asthon [1]. The market of Internet of things, will increase from $547 in 2018 to $841 million in 2020 according to the report of Gartner. Internet of Things well-defined as a framework or environment where intelligent devices or things are connected and communicating and transferring the data between devices at anytime and anywhere. In the IoT, intelligent devices have circumscribed sources of power and limited storage capacity in the network. Its rapid growth, complexity and heterogeneity of the objects of the systems creates more security concerns and issues related to security in the IoT system [2]. These objects might be sensors, RFID, actuators, mobile phones and other smart devices. This IoT system used in different applications or domains like Smart City, Smart Home, Smart Traffic Systems, Smart Parking Systems, Smart Enterprise, Smart Health Monitoring System, Smart Education Systems etc. [3], [4]. Security is the biggest concern in all the applications of the Internet of Things system because of its open structure and nature.

Recently, many researchers worked on Blockchain Technology for curing the threats which occurred in Internet of Things. The Blockchain Technology perceived by Satoshi Nakamoto in 2008 [1], [14], [17] and it has a distributed immutable and public ledger of transactions. In the current IoT system scalability problem occurs due to its centralized nature where intelligent devices are identified, authenticated and managed centrally in the system. Hence, Blockchain provides the concept of distributed ledger, Peer-to-Peer network [23], management and authentication mechanisms in the system which ensure the authenticity, privacy, integrity as well as the security of the system. Therefore, the

need of Blockchain's integrated IoT application in the future.

In this Systematic Literature Review (SLR) paper, directed a SLR for studying about the Internet of Things, integrated solutions of security problem in the IoT system with Blockchain technology, Security Challenges and Security preserving methods and approaches in the atmosphere of the Internet of Things and used of Blockchain in IoT.

The outline of this SLR paper is as: Section II is the research background in which discussed the Internet of Things system, Blockchain technology, Integration of Blockchain with Internet of things, Section III discussed related work about it, Security and Blockchain, Section IV, discuss Comparison of various solutions. In V, Section draw the discussion portion of Research Questions, Section VI, represent concluding comments and future scopes of this research.

2. Research Background

Research Questions are used to identify the security problems of the IoT system and its solutions. Below table shows the Research Questions of the literature study:

Table 2. Research Questions of SLR

S.N.	Question's	Motivations
RQ1:	What is the security related issues have been arrived within IoT System?	Aim of this RQ's are to find out different security related issues and challenges of IoT systems which are facing.
RQ2:	What kinds of security solutions have been discussed to improve the IoT System?	Aims to find out the solution of RQ1 for improve the functioning the IoT system.
RQ3:	What kinds of Blockchain solutions have been presented to improved Security of IoT System?	Aim to find out solution of RQ1 with the help of Blockchain.

2.1. Internet of Things

Every day, smart objects or devices increased in the IoT system. Internet of Things is the internetworking of items like smart vehicles, smart phones or any smart devices which are embedded with sensors, actuators, software, electronics and internet connectivity [27]. Internet connectivity enables the things or objects, collect the data's and performed an operation accordingly. The architecture of the Internet of Things used different protocols for the purpose of routing the data's, management the infrastructures, keys, intelligent devices and security threats. Due to the open nature of architecture of IoT, these architectures are vulnerable to security threats and different attacks. Security threats are the main concerns for its system [30]. Here are some reasons discussed:

- It is not a secure environment because of the Internet networking of objects in the IoT. There is much possibility of executing any malware or any threats activities.
- In its system, things are communicated with each other in the network that's why there is an opportunity of hindering the privacy and integrity of data.
- The IoT system are promoted versions of different technologies similar to Mobile Ad-hoc Network (MANET), VANET, Wireless Sensor Network (WSN), 2G, 3G, 4G communication. Hence, it is also vulnerable all threats and attacks of these technologies.

2.1.1. Security Requirements in IoT

Security is the main concern in its system because of its open nature [30]. Different Security parameters which are discussed in the below:

- **Integrity:** Preventing the unauthorized nodes for modifying the information's.
- **Confidentiality:** Confidentiality means protecting the information's to unauthorized nodes from leaks.
- **Availability:** Availability refers that information's are available for accessing when it's needed.
- **Authenticity:** Sensitive data's or system should not be accessed by any unauthorized users.
- **Authorization:** Authorization refers to the process of giving permission to someone or something for doing anything's.

Figure 1. Security Requirement in IoT System

2.1.2. Layered Architecture of IoT

In Internet of Things system, according to the operations of devices categorized the IoT system into different layer architecture of the IoT system [1], [33]. There are many opinions for the layered architecture of its system like 3 Layer IoT Architecture, 4 Layer IoT Architecture, 5 Layer IoT Architecture. However, in this literature review discusses 4 Layer IoT Architecture with each layer like Perception, Middleware, Network Layer and Application Layer.

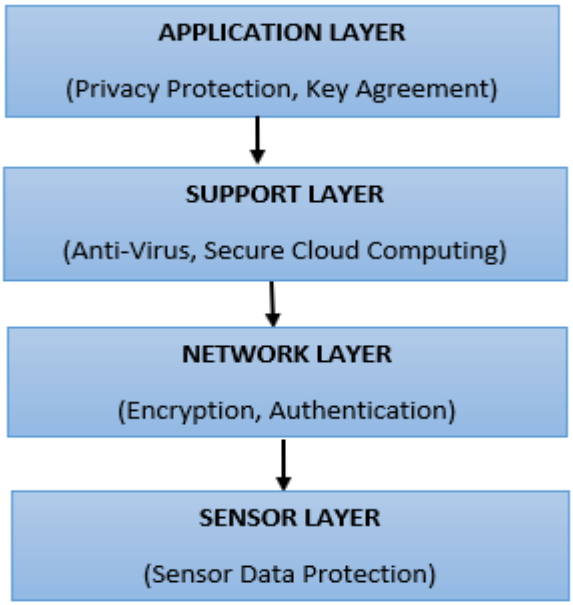

Figure 2. IoT system Architecture [1] []

1.The Sensor Layer [1]: In the IoT system sensor layer is the top most layer because firstly data's or information's are entered into the system through it. Sensor layer is also called as "Perception Layer" of architecture. Acquisition of data from the physical environment's through sensor devices and actuators is the functioning which is performed in it. For the acquisitions of data's different devices like RFID [1] reader, sensors, GPS etc. used in this layer.

2.The Network Layer [33]: This Network Layer of Internet of Thing plays the function of routing and transferring of the data across the network. The operations of this layer like routing, switching, internet gateway etc. performed by using different latest technologies like 3G, 4G, Zigbee, Wi-Fi, Bluetooth, etc.

3.The Support Layer [1]: Support Layer in the IoT system, is responsible to process and manipulation of data's in the network. The Support layer acts as the border between the network and application layers. Middleware layer is also called as "Middleware layer" in the IoT system.

4.The Application Layer [33]: In the IoT system, Application layer is the furthermost significant layer. This layer ensures the integrity, authenticity and confidentiality of the data. The purpose of the IoT system is achieved at this last layer purpose of the IoT system is achieved at this last layer.

2.2. Blockchain Technology

Blockchain concept is act as database which is used for storage in the network as decentralized manner. Blockchain is an arrangement of blocks, which store the complete list of records of transactions in the network [17]. Every block has one parent block and every first block is called as a genesis block in the Blockchain and it has no parent block. Blockchain Technology has peer-to-peer and distributed ledger concepts. This distributed ledger has three concepts like block, chain and transaction. The Block is the storage part which contains the transactions, hash values and records, etc. The Chain is linking part of Blockchain which is used for connecting the blocks and create chain. Any valuable information which is circulated in the network is called as the Transactions. Overall Blockchain concept is mainly defined with the four terms which are [17]:

- **Peer-to-Peer Network:** Blockchain technology removes central dependencies of all nodes from any central party within the network.
- **Distributed and Open Ledger:** Each node in the network validated individually and act as transparent.
- **Synchronization of ledgers copies:** Ledger copies shared among all nodes in the network. Hence, synchronization of ledgers is required in the network when the new transactions occur then validate the new transaction and add into the validated ledgers of transactions.
- **Mining Operation:** Mining operation of Blockchain adds the transaction in the public ledger of a past transaction.

2.2.1: Types of Blockchain: Blockchain categorized on the basis of access controlling power of the network [38]. There are four types of network, which are:

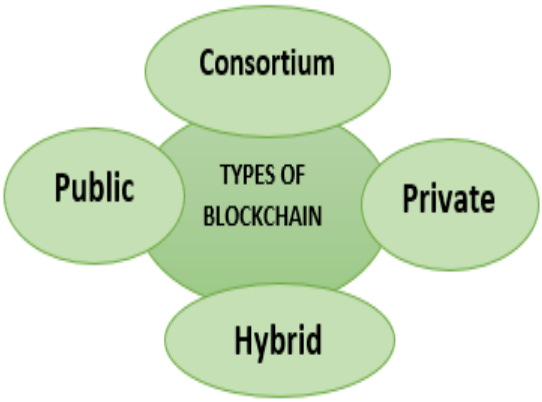

Figure 3. Types of Blockchain

1. Public Blockchain: For accessing purpose, In Public Blockchain there is no restriction on the network. The Proof

of work is the consensus algorithms of public Blockchain. Proof of Stake (PoS) consensus and Delegated Proof of Stake are also coming in this Blockchain [41]. Examples of Public Blockchain are Monero, Litecoin, Dash, Bitcoin, Ethereum.

2. Private Blockchain: In this Blockchain there is restriction for accessing the network. Nodes cannot join in the network unless network administrators invited it. RAFT, the Practical Byzantine fault tolerance (PBFT) consensus algorithms are coming under the Private Blockchain [44]. Examples of the Private Blockchain are Multichain, MONAX.

3. Consortium or Federated Blockchain: In this Blockchain, the semi-decentralized concept used. Its controlled and restricted by more than one organization. This type of Blockchain used by mainly government organizations like banks, etc. Examples of Consortium Blockchain are Corda, B3i (Insurance), EWF(Energy), R3(Bank).

4. Hybrid Blockchain: This type of Blockchain is the mixture of both the private and the public Blockchain. This Blockchain used the features or characteristics of both Blockchain.

2.2.2 Integration of Blockchain with Internet of Things

In the integrated Blockchain Internet of Things applications, all the transactions with lots of information go through Blockchain network for storing immutable and persistence records of data. The IoT system has vulnerable to security in system. Blockchain technology has the features of decentralized, immutable, anonymity etc. which merge with the IoT system and become a secure Blockchain based the IoT system. The different authoritative features of Blockchain technology are [17], [41], [54]:

- **Decentralized:** Blockchain technology make the systems, decentralized, it means there is no need of third centralized parties for validation of any transaction in the system.
- **Persistency:** Persistency is the quality which means determined to ensure or accomplish something. Due to this quality Blockchain network can be validated transactions quickly and find out the invalid transaction immediately in the system.
- **Anonymity:** With address, any user can interact directly with Blockchain. That's why Blockchain don't give the assurance of privacy.
- **Immutability:** Blockchain technology offers the concept of distributed ledger and this distributed ledger are immutable, it means that majority of nodes verified the data modification in the network. Immutable distributed ledger enhances the privacy and security of systems.
- **Security:** Blockchain uses the cryptographic technologies like public key, private key and hash concept in the system which increase the security concern automatically.

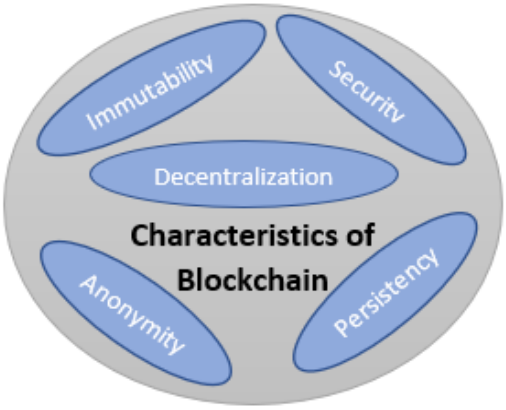

Figure 4. Key Characteristics of Blockchain

3. Related Work

In this segment, we will shortly present a summary of any works of the previous published literature related to the security problems of the IoT system, Blockchain Technology in IoT and solutions of the IoT problems using Blockchain.

3.1 Security Issues in IoT System

Mikail Mohammed Salim et.al. [24], has presented a survey of comprehensive approach which includes general DDoS attack motivations and specific reasons why attackers prefer the IoT devices to launch DDoS attacks. The author listed different types of tools that are available for attacking it devices to form a botnet and further tools are discussed which allow using it bots to launch DDoS attacks and presented a detailed and systematic classification of different types of DDoS attacks that take place on the cloud.

Chao Li et.al. [28], has presented the study of privacy defense problem in the IoT system through a broad review of the state-of-threat by mutually considering three major dimensions, namely the state-of-the-art principles of privacy laws, the IoT system architecture and representative privacy enhancing technologies (PETs).

Wei Zhou et.al. [62], has discussed "IoT Feature" concepts for the better recognize the necessary details of new IoT threats and the challenges which were focused in recent research. In this paper also discussed security and privacy effects on IoT system on the basis of different IoT features including the threats and different existing solutions.

Lulu Liang et.al. [72], has exposed a denial of service attack of an Internet of Things. Different attacks tools have discussed in this paper for QoS attacks. Like the Quality of service attack tool is Kali Linux, which is launched by using many methods and also compare different methods.

Mario Frustaci et.al. [81], has tried to monitor on the IoT security scene and providing a taxonomical monitoring from the view point of main layered architecture of IoT system model. It has also introduced about a new model as Social Internet of things (SIoT) where IoT system merges with different social networks, which allowing devices and people to facilitate information and interact.

Benz Arti et.al. [92], has presented a categorization of attacks from a variety of networks involved in the IoT system. This categorization discriminates common and specific attacks from each network and use several criteria like the congestion, security attributes, disturbance. Also, several existing security solutions are presented for the purpose to expose the security requirements to protect IoT.
\

3.2 Solutions of IoT Security Problem

Laphou Lao et.al. [5], has given an overview of Blockchain-IoT architecture and also analyzing protocols and their structures. Discussed various consensus protocols for Blockchain IoT and compare among various consensus algorithms of Blockchain. In this paper also analyses the model for Peer to Peer traffic model. They have provided a traffic model for Blockchain based it system for traffic distribution.

Krishna Prasad Satamraju et.al. [16], has discussed a model which used the concept of Blockchain to lead the security problem and authentication problem in the IoT system. They were used various factors in Blockchain and IoT systems which effects in the integration of both. They were concluded the hybrid model is more powerful across distributed platforms.

Mohammad Dabbagh et.al. [25], has analyzed the bibliometric conference papers of Block chain's and related articles, and review papers that have been indexed in WoS from 2013 to 2018. They have analyzed those collected papers against five research questions. The results revealed some valuable insights, including yearly publications and citation trends, the hottest research areas, and top-ten in influential papers, favorite publication venues, and most supportive funding bodies.

Christy Varghese et.al. [26], has proposed system forms a decentralized network offering transparency and security. It also guarantees authentication, synchronization and data integrity. To overcome the limitations and issues in the IoT system, the author proposed IoT system using Blockchain.

Lei Hang et.al. [38], has proposed unified platform for IoT with Blockchain which were focused on the integrity of sensitive data. There were used another layer in its architecture called as IoT Blockchain Service layer which manage the Blockchain network. Raspberry Pi devices used for creating IoT network, which submit the sensor data's to Blockchain network. A Smart contract written in solidity language and this smart contract discussed the rules and logic of Unified IoT Blockchain platform.

Bo Tang et.al. [39], has proposed decentralized it passport for trust cross-platform using Blockchain technology. Arbitrary trust relation established among each other using this Blockchain based platform.

Mohammad Salar Arbabi et.al. [40], has proposed a decentralized based novel system using Blockchain technology. This system used smart contract concept in the implementation of the Internet of Things system to overcome the high cost and centralized problem. An Ethereum BC tool used in the merged platform of IoT and Blockchain.

Tareq Ahram et.al. [91], has focused on break the ground for presenting and demonstrating the use of Blockchain in numerous industrial applications. A health care industry IoT application, Health chain its application, is formalized and developed on the foundation of Blockchain using IBM Blockchain inventiveness.

4. Comparison of Various Solutions

Many earlier projected solutions are deliberated for the Internet of Things applications with the help of different latest types of technologies. For example, in the paper [33], the author proposed trust-based mechanism in smart manufacturing, which uses trust tax as necessary information on the transactions between any physical system, human, because the lack of confidence and reliability. In [38], the author worked on the integrity of the sensing data of its systems and for securing the integrity of the data they proposed the Blockchain based platform of Internet of Things system. For implementation scenario used Raspberry Pi devices and Hyperledger fabrics. In the paper [56], the author developed a BlendCAC scheme in which devices are self-controlled of resources and there is no centralized monitoring of the devices. This scheme is based on the private Blockchain. In [58], the author investigated the security concern of Blockchain base its systems and developed a framework for dealing with privacy problems with Internet of Things system. In this paper, also discoursed some solutions for the Security of IoT using the Blockchain and Ethereum tool. The author in [59], assured the security related to the Internet of Things applications during the time synchronization in the system. Blockchain scheme used for the time verification and convenience synchronization of the distributed ledger in the network. In this paper [61], the author proposed a Home automation system which sends alarms to the owner for when of any intrude activity. This project used the micro controller TI-CC3200 and send voice calls for alarm to the owner. In this paper [89], author developed a model of Home Security System, which is focused on detection of intruders, identification and authentication of unknowns.

Table 1. Analysis of Pervious Security Solution of Smart Home IoT

Paper Title	Consensus Algorithms / Approaches	Parameters Considered / Solution	Blockchain Types	IoT Devices	Future Work
BIFF: A Blockchain-based IoT Forensics Framework with Identity Privacy [4]	Modified Merkel Signature Scheme	Identification and Privacy of Evidence	Public Blockchain	Similar Smart Devices	Test the reliability with heterogeneous Devices
A Secured and Authenticated Internet of Things Model using Blockchain Architecture [16]	Binary Merkel Tree Scheme	Authentication Problem	Permission less or private Blockchain	Smart Devices	Improve Privacy Security
IoT DEVICE MANAGEMENT USING BLOCKCHAIN [26]	Proof of Work Concept	Authentication and Data Integrity	Ethereum Blockchain	Smart Phone and Raspberry Pi	Not Mention
A Secured and Authenticated Internet of Things Model using Blockchain Architecture [33]	Any Prototype of B.C.	Privacy and Authenticity	Public Blockchain	Cameras, GPS Sensors	Not Mention
Design and Implementation of an Integrated IoT Blockchain Platform for Sensing Data Integrity [38]	Proof of Concept consensus algorithm	Sensing Data Integrity	Hyperledger Blockchain	Raspberry Pi Device	Used other consensus algorithms for improving transaction rate
BlendCAC: A Blockchain Enabled Decentralized Capability-based Access Control for IoTs [56]	Proof of Concept Prototype	Scalable and lightweight Access Control,	Local Private Blockchain	Raspberry Pi Device	Still long way complete decentralized security and Used in Real type application
Blockchain-Based Solutions to Security and Privacy Issues in the Internet of Things [58]	Not Discuss	Scalability, Authentication, Integrity, Privacy	Public Blockchain (Bitcoin, Ethereum)	Smart IoT devices	Used GHOST Protocol and DAG model alternative to Blockchain

Paper Title	Consensus Algorithms / Approaches	Parameters Considered / Solution	Blockchain Types	IoT Devices	Future Work
Blockchain-based Secure Time Protection Scheme in IoT [59]	Practical Byzantine Fault Tolerance (PBFT) consensus mechanism	Time Synchronization of IoT	Public Blockchain	RFID, Smart Home Appliances	Improve accuracy of time, reduce offset
IoT Based Smart Security and Home Automation System [61]	Used standard IoT model	Motion detection	Not Used	TI CC3200 Launch Pad	Lack in synchronization of alarm, Make more synchronized
A Denial of Service Attack Method for an IoT System [72]	Not Used	Denial of Service Attack	Not Used	Arduino, Kali Linux	More Attacks Study
Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT [85]	PoC Prototype	Generic, Scalable and Access Control Management System	Private Blockchain	Smart Sensor device	Not Mention
IoT Application Development: Home Security System [89]	Based on fundamental IoT Architecture	Lower Power System, Detection and Authentication	Not Used	Raspberry Pi Device	Similar Concept used for face detection using ML & AI

5. Discussion of Research Questions

RQ1: What is the security related issues have been arrived within IoT System?
Overall, in the Systematic literature process identified the major security issues of the Internet of Things based applications. The main issue of the IoT systems is data integrity, privacy, authentication, different types of attacks and centralized monitoring of IoT systems.

RQ2: What kinds of security solutions have been discussed to improve the IoT System?
There are so many researchers have provided the security issues and solutions of that issue. The researchers have used many technologies (DAG, IOTA etc.), approaches and cryptographic algorithms (RSA, SHA, etc.) for solutions for the security of IoT system.

RQ3: What kinds of Blockchain solutions have been presented to improved Security of IoT System?
Most of the papers have discussed the problems of the IoT system and discussed solutions of the corresponding problems. Some researchers are given the solutions of the security problem with the help of Blockchain Technology. Some of the solutions to privacy problems and some of the solution to the integrity problem in general.

Overall, most of the researchers were focused on the only one security issue in the research. Many researchers were considered any one of the security issues among privacy, authentication, data integrity, etc. Security solutions of the IoT system have projected without using the Blockchain technologies. There were also so many researchers which proposed the solutions of the Internet of Things applications with the support of Blockchain. Security problems are discussed over-all in detail and the researchers were approaching the advanced solution by using Blockchain but solutions of the problems are not discussed in details.

6. Conclusion & Future Work

Goal of conduct Systematic Literature review (SLR) of the IoT system is to provide the analysis of the automated and smart Internet of Things applications. Subsequently, the systematic literature review analyzed that researchers have attentive in the security concerns of the IoT network

and move the latest technologies for solutions of the security measures on it. Firstly, main focused on the research solutions for the security which basically for privacy and integrity or attacks in the network. Secondly, focused on the Blockchain solutions of the researchers for the security problems of IoT system. Blockchain based platforms were used in IoT implementations, which were dealing anyone security parameters. Future work will be providing model for any IoT application with the help of Blockchain which will deal with the different security parameters.

References

[1] Sana Zeba, Daniyal Khan, Md Hussain Ahmad " Security Threats and Technologies in Internet of Things System " IJSRD - International Journal for Scientific Research & Development| Vol. 7, Issue 07, 2019 | ISSN (online): 2321-0613 page no 64- page no 69

[2] Chaoran Guo, Haiyan Zheng, "A Brief Analysis of Privacy Protection Strategy for Block Chain-based Internet of Things System " ICBDR 2019: Proceedings of the 2019 3rd International Conference on Big Data Research November 2019 page no 94- page no 97

[3] Sana Zeba, Md Hussain Ahmad "SURVEY ON ATTACKS IN MANET BASED INTERNET OF THINGS SYSTEM" in IJSRD -Vol. 7, Issue 06, 2019 | ISSN (online): 2321-0613 page no 96- page no 102

[4] Duc-Phong Le, Huasong Meng, " BIFF: A Blockchain-based IoT Forensics Framework with Identity Privacy " 2018 IEEE Region 10 Conference (Jeju, Korea, 28-31 October 2018) https://ieeexplore.ieee.org/document/8650434 page 2372- page 2377

[5] Laphou Lao, Zecheng Li, " A Survey of IoT Applications in Blockchain Systems: Architecture, Consensus, and Traffic Modeling " ACM Computing Surveys February 2020 Article No.: 18

[6] Rong Wang, Wei-Tek Tsai, " A Video Surveillance System Based on Permissioned Blockchains and Edge Computing "2019 IEEE

[7] Pietro Danzi, Anders E. Kalør, " Delay and Communication Tradeoffs for Blockchain Systems with Lightweight IoT Clients " 2019 IEEE page 1- page 12

[8] Ramazan Yetis, Ozgur Koray Sahingoz, " Blockchain Based Secure Communication for IoT Devices in Smart Cities " 2019 IEEE page 134- page 138

[9] Marten Sigwart, Michael Borkowski, " Blockchain-based Data Provenance for the Internet of Things " IoT 2019: the 9th International Conference on the Internet of Things October 2019 page no 1- page no 8

[10] Elizabeth Reilly, Matthew Maloney, " An IoT Integrity-First Communication Protocol via an Ethereum Blockchain Light Client " 2019 IEEE/ACM (SERP4IoT) page 53- page 56

[11] Zhibin Lei, Chao Feng, Tony Tsang, " Next Generation Blockchain Network (NGBN) " 2019 20th IEEE International Conference (MDM) page 452- page 456

[12] Abdur R. Shahid, Niki Pissinou, " Sensor-Chain: A Lightweight Scalable Blockchain Framework for Internet of Things " 2019 International Conference on Internet of Things (iThings) and IEEE Smart Data and Green Computing and Communications and IEEE Cyber, Physical and Social Computing on page 1154- page 1161

[13] LIXIA XIE, YING DING, " Blockchain-Based Secure and Trustworthy Internet of Things in SDN-Enabled 5G-VANETs " 2019 IEEE Volume 7 See on page 56656 - page 56666

[14] Qilei Ren, Ka Lok Man, "Using Blockchain to Enhance and Optimize IoT based Intelligent Traffic System " 2019 IEEE International Conference on Platform Technology and Service (PlatCon)

[15] Roberto Di Pietro, Xavier Salleras, " A blockchain-based Trust System for the Internet of Things " SACMAT '18: June 2018 on page no 77-page no 83

[16] Krishna Prasad Satamraju, " A Secured and Authenticated Internet of Things Model using Blockchain Architecture " 2019 IEEE on page 19- page 23

[17] Zibin Zheng, Shaoan Xie, " An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends " 2017 IEEE 6th International Congress on Big Data page no 557- page no 564

[18] Jun Lin, Wen Long, " Using Blockchain and IoT Technologies to Enhance Intellectual Property Protection " ICCSE'19: October 2019 page no 44- page no 49

[19] Mohammad Maroufi, Reza Abdolee, " On the Convergence of Blockchain and Internet of Things (IoT) Technologies "2019

[20] Jonayet Miah, Razibhayat Khan, " Service Development of Smart Home Automation System: A Formal Method Approach " CIIS 2019: November 2019 page no 161- page no 167

[21] Riya Thakore, Rajkumar Vaghashiya, " Blockchain - based IoT: A Survey "2019 ELSEVIER on page 704 -page 709

[22] Chinazaekpere Ngubo, Mischa Dohler, " Blockchain, IoT and Sidechains " 2019 IMECS conference of Engineers and Computer Scientists

[23] SIN KUANG LO, YUE LIU, " Analysis of Blockchain Solutions for IoT: A Systematic Literature Review " 2019 IEEE for more information page no 58822 -page no 58835

[24] Mikail Mohammed Salim, Shailendra Rathore "Distributed denial of service attacks and its defences in IoT: a survey", Springer Science Business Media, LLC, part of Springer Nature 2019

[25] MOHAMMAD DABBAGH 1, MEHDI SOOKHAK2, "The Evolution of Blockchain: A Bibliometric Study", Volume 7, 2019 IEEE

[26] CHRISTY VARGHESE, JISHA JOSE, "IoT DEVICE MANAGEMENT USING BLOCKCHAIN" 2019 IJSETR 2019, ISSN: 2278 -7798

[27] Nazrul M. Ahmad, Siti Fatimah Abdul Razak, " Improving Identity Management of Cloud-based IoT Applications using Blockchain " 2018 IEEE on ICIAS

[28] Chao Li, Student Member, "Privacy in Internet of Things: from Principles to Technologies" 2018 IEEE. See http://www.ieee.org/publications_standards/publications/rights/index.html

[29] Jawad Ali, Toqeer Ali, " Blockchain-based Smart-IoT Trust Zone Measurement Architecture " COINS '19: International Conference on Omni-Layer Intelligent Systems May 2019 page no 152- page no 157

[30] Jaychand, Nishant Behar "A Survey on IoT Security Threats and Solutions" 2017 Vol. 5, Issue 3, March 2017 www.ijircce.com

[31] Qianwei Zhuang, Yuan Liu, " Proof of Reputation: A Reputation-based Consensus Protocol for Blockchain Based Systems " IECC '19: Proceedings of the 2019

International Electronics Communication Conference July 2019 page no 131- page no 138
[32] Abdur R. Shahid, Niki Pissinou, " Quantifying location privacy in permissioned blockchain-based internet of things (IoT) " MobiQuitous '19: Proceedings of the 16th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services November 2019 page no 116- page no 125
[33] Yongping Zhang, Xiwei Xu, " Blockchain-Based Trust Mechanism for IoT-Based Smart Manufacturing System "2019 IEEE TRANSACTIONS ON COMPUTATIONAL SOCIAL SYSTEMS on page 1- page 9
[34] Boulkamh Chouaib, Derdouri Lakhdar, " Smart Home Energy Management System Architecture Using IoT " icist 2019: 9th International Conference on Information Systems and Technologies March 2019 page no 1- page no 5
[35] Abid Sultan, Muhammad Azhar Mushtaq, " IOT Security Issues Via Blockchain: A Review Paper " ICBCT March 2019 page no 60- page no 65
[36] Pankaj Mendki, " Blockchain Enabled IoT Edge Computing " ICBCT 2019: Proceedings of the 2019 International Conference on Blockchain Technology March 2019 page no 66- page no 69
[37] Said El Kafhali, Chorouk Chahir, " Architecture to manage Internet of Things Data using Blockchain and Fog Computing " BDIoT' 4th International Conference on Big Data and Internet of Thing October 2019 page no 1- page no 8
[38] Lei Hang, Do-Hyeun Kim, " Design and Implementation of an Integrated IoT Blockchain Platform for Sensing Data Integrity " 2019 MDPI on page 1- page 26
[39] Bo Tang, Hongjuan Kang, " IoT Passport: A Blockchain-Based Trust Framework for Collaborative Internet-of-Things " SACMAT 24th, May 2019 page no 83- page no 92
[40] Mohammad Salar Arbabi, Mehdi Shajari, " Decentralized and secure delivery network of IoT update files based on Ethereum smart contracts and blockchain technology " CASCON '19: November 2019 Pages 110–119
[41] Jin-ho Park, Mikail Mohammed Salim, " CIoT-Net: a scalable cognitive IoT based smart city network architecture " 2019 Springer page 1- page 20
[42] Aleksandr Lepekhin, Alexandra Borremans, " A systematic mapping study on internet of things challenges " SERP4IoT '19: May 2019 page no 9- page no 16
[43] Rishabh Jain, Aniket Dogra, " Solar Energy Distribution Using Blockchain and IoT Integration " International Electronics Communication Conference July 2019 page no 118- page no 123
[44] Yuchen Yang, Longfei Wu "A Survey on Security and Privacy Issues in Internet-of-Things" 2016 IEEE. See http://www.ieee.org/publications_standards/publications/rights/index.html
[45] Mayra Samaniego, Cristian Espana, " Access Control Management for Plant Phenotyping Using Integrated Blockchain " BSCI '19: July 2019 page no 39- page no 46
[46] Nallapaneni Manoj Kumara, Pradeep Kumar Mallickb, "Blockchain technology for security issues and challenges in IoT " 2019 Science Direct page no 1815 -page no 1823
[47] KoenTange, Michele De Donno, " Towards a Systematic Survey of Industrial IoT Security Requirements: Research Method and Quantitative Analysis " 2019 ACM
[48] Sana Zeba, Shish Ahmad, "DETECTION AND VERIFICATION OF MALICIOUS NODE IN BLACK HOLE ATTACK USING DSA" in International Journal for Research in Technological Studies
[49] Volkan Dedeoglu, Raja Jurdak, " A trust architecture for blockchain in IoT " Mobi Quitous '19: Proceedings of the 16th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services November 2019 page no 190- page no 199
[50] Charalampos S. Kouzinopoulos, Konstantinos M. Giannoutakis, " Implementing a Forms of Consent Smart Contract on an IoT-based Blockchain to promote user trust " 2018 IEEE https://ieeexplore.ieee.org/document/8466268
[51] Xiaoyang Zhu, Youakim Badr, " A Survey on Blockchain-based Identity Management Systems for the Internet of Things " 2018 IEEE page 1568 - page 1573
[52] Zijiang Hao, Raymond Ji, " FastPay: A Secure Fast Payment Method for Edge-IoT Platforms using Blockchain " 2018 Third ACM/IEEE Symposium on page 410 - page 415
[53] Miguel Pincheira Caro∗, Muhammad Salek Ali, " Blockchain-based Traceability in Agri-Food Supply Chain Management: A Practical Implementation " 2018 IoT Vertical and Topical Summit on Agriculture - Tuscany (IOT Tuscany)
[54] Lijing Zhou, Licheng Wang*, " BeeKeeper: A Blockchain-based IoT System with Secure Storage and Homomorphic Computation " 2018 IEEE on page 1- page 17
[55] Rahul Agrawal, Pratik Verma, " CONTINUOUS SECURITY IN IOT USING BLOCKCHAIN " 2018 IEEE https://ieeexplore.ieee.org/document/8462513 page 6423- page 6427
[56] Ronghua Xu, Yu Chen, " BlendCAC: A Blockchain Enabled Decentralized Capability-based Access Control for IoTs "2018 IEEE https://ieeexplore.ieee.org/document/8726680 page 1027 - page 1034
[57] Shanto Roy∗, Md. Ashaduzzaman, " Blockchain for IoT Security and Management: Current Prospects, Challenges and Future Directions " 2018 IEEE
[58] 58) Yong Yu, Yannan Li, " Blockchain-Based Solutions to Security and Privacy Issues in the Internet of Things "2018 IEEE https://ieeexplore.ieee.org/document/860075 page 12- page 18
[59] Kai Fan, Shangyang Wang, " Blockchain-based Secure Time Protection Scheme in IoT " 2018 IEEE on page 1- page 9
[60] Juah C Song, Mevlut A Demir, " Blockchain Design for Trusted Decentralized IoT Networks " 2018 IEEE https://ieeexplore.ieee.org/document/8428720 page 169- page 174
[61] Ravi Kishore Kodali, Vishal Jain, " IoT Based Smart Security and Home Automation System " 2016 IEEE International Conference page no 1286- page no 1289
[62] Wei Zhou, Yuqing Zhang, "The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved", IEEE https://ieeexplore.ieee.org/document/8386824
[63] Sheng Ding, Jin Cao, Chen Li, " A Novel Attribute-Based Access Control Scheme Using Blockchain for IoT " 2018 IEEE on page 1- page 10
[64] Abinaya.E, Aishwarya.K, "A Performance Aware Security Framework to Avoid Software Attacks on Internet of Things (IoT) Based Patient Monitoring System " 2018 IEEE https://ieeexplore.ieee.org/document/8550955
[65] Uzair Javaid, Muhammad Naveed Aman," BlockPro: Blockchain based Data Provenance and Integrity for

Secure IoT Environments " BlockSys'18: November 2018 page no13- page no 18
[66] Lingjun Fan, J. Ramon Gil-Garcia, " Investigating blockchain as a data management tool for IoT devices in smart city initiatives " May 2018 page no 1- page no 2
[67] Sumathi Balakrishnan, Hemalata Vasudavan, " Smart Home Technologies: A Preliminary Review " ICIT 2018: December 2018 page no 120- page no 127
[68] Bahtijar Vogel, Rimpu Varshney, " Towards designing open and secure IoT systems: insights for practitioners " IOT '18: page no 1-page no 6
[69] Diego M. Mendez Mena, Baijian Yang, " Blockchain-Based Whitelisting for Consumer IoT Devices and Home Networks " SIGITE '18: page no 7- page no 12
[70] Uzair Javaid, Ang Kiang Siang, " Mitigating loT Device based DDoS Attacks using Blockchain " CryBlock'18: June 2018 on page no 71- page no 76
[71] Saravid A/L Suchaad, Koichiro Mashiko, " Blockchain Use in Home Automation for Children Incentives in Parental Control " MLMI2018: September 2018 page no 50- page no 53
[72] Lulu Liang, Kai Zheng "A Denial of Service Attack Method for an IoT System" 2016 8th International Conference on Information Technology in Medicine and Education
[73] Kimheng Sok, Jean Noël Colin," Blockchain and Internet of Things Opportunities and Challenges " SoICT 2018: December 2018 page no 150- page no 154
[74] Aarti Rao Jaladi, Karishma Khithani " Environmental Monitoring Using Wireless Sensor Networks (WSN) based on IOT "International Research Journal of Engineering and Technology page no 1371- page no 1378
[75] Mohammad Hasanzadeh Mofrad, Daniel Mossé, " Speech recognition and voice separation for the internet of things " IOT '18: page no 1- page no 8
[76] Roberto Casado-Vara, Fernando De La Prieta, " Blockchain framework for IoT data quality via edge computing " BlockSys'18: November 2018 page no 19- page no 24
[77] R Gurunath, Mohit Agarwal, " An Overview: Security Issue in IoT Network " Second International conference on (I-SMAC 2018) IEEE Xplore page no 104- page no 107
[78] Trusit Shah, S. Venkatesan " Authentication of IoT Device and IoT Server Using Secure Vaults " 2018 17th IEEE International Conference
[79] I. A. Alameri " MANETS and Internet of Things: The Development of a Data Routing Algorithm " Engineering, Technology & Applied Science Research Vol. 8, No. 1, 2018, 2604-2608 on page no 2604- page no 2608
[80] Pinyaphat Tasatanattakool, Chian Techapanupreeda, "Blockchain: Challenges and Applications", 2018 IEEE https://ieeexplore.ieee.org/document/8343163
[81] Mario Frustaci, Pasquale Pace "Evaluating Critical Security Issues of the IoT World: Present and Future Challenges", IEEE INTERNET OF THINGS JOURNAL, VOL. 5, NO. 4, AUGUST 2018 page 2483- page 2495
[82] Tianzhi Yang, Yuan Liu, "A Blockchain based Smart Agent System Architecture " ICCSE'19: 4th International Conference on Crowd Science and Engineering October 2019 on page no 33- page no 39
[83] Francesco Restuccia, Salvatore D'Oro, "Blockchain for the Internet of Things: Present and Future" IEEE INTERNET OF THINGS JOURNAL, VOL. 1, NO. 1, JANUARY 2018
[84] TIAGO M. FERNÁNDEZ-CARAMÉS, PAULA FRAGA-LAMA, " A Review on the Use of Blockchain for the Internet of Things " 2018 IEEE on page no 32979- page no 33001
[85] Oscar Novo, " Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT " 2018 IEEE on page no 1184- page no 1195
[86] Daniel Minoli, Benedict Occhiogrosso, " Blockchain mechanisms for IoT security " 2018 ELSEVIER www.elsevier.com/locate/iot page no 1- page no 13
[87] AnaReyna*, CristianMartín, " On blockchain and its integration with IoT. Challenges and opportunities "2018 SPRINGER on page no 173- page no 190
[88] Jyoti Deogirikar, Amarsinh Vidhate " Security Attacks in IoT: A Survey "2017 IEEE International conference on I-SMAC https://ieeexplore.ieee.org/abstract/document/8058363/ page no 32- page no 37
[89] Raj G Anvekar, Dr. Rajeshwari M Banakar " IoT Application Development: Home Security System "2017 IEEE International Conference on Rural Development page no 68- page no 72
[90] Jos´e Santos, Tim Wauters, "Resource Provisioning for IoT application services in Smart Cities" 2017 IFIP2017 IEEE. https://ieeexplore.ieee.org/document/8255974
[91] Tareq Ahram1, Arman Sargolzaei2, "Blockchain Technology Innovations" 2017 IEEE Technology & Engineering Management Conference (TEMSCON)
[92] BENZ ARTI, Bayrem TRIKI "A Survey on Attacks in Internet of Things Based Networks" 2017 IEEE https://ieeexplore.ieee.org/document/8273006
[93] Dr Y Raghavender Rao " Automatic Smart Parking System using Internet of Things (IOT)" International Journal of Engineering Technology Science and Research IJETSR May 2017 page no 225- page no 228