IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 6 Issue 3, March 2019
ISSN (Online) 2348 – 7968
www.ijiset.com

Employing Blockchain in Internet of Things: A Comparative Analysis

Priyanka Dongre
Assistant Professor
Priyadarshini College of Engineering
Nagpur, (M.S), India.
priyankadongre@gmail.com

Dr. Pushpneel Verma
Associate Professor
Bhagwant University Ajmer, Rajasthan, India.
pushpneelverma@gmail.com

***Abstract*—To secure data in Internet of Things (IoT), implementation of Blockchain algorithm is becoming popular and its widespread use and applications in industries are increasing day by day and rapidly. It is believed that by 2020, Over 25 billion devices are expected to be connected to the Internet. The Internet of Things (IoT) enabled applications that offer socioeconomic benefits, because of exponentially increasing number of connected devices. A variety of IoT applications have different operational requirements and constraints.**

The issues like user authentication, device identity, data security, and so on are posing limitation on implementing IoT. Security and data privacy are significant concern in IT industry where network of computers share the data among several and different users. Depending on the application and usage, IT industry has implemented and continued to implement a variety of data privacy and security tools.

These tradition nature security solutions are not always applicable to "Internet of Things" due to many reasons like IOT contains a network of heterogeneous devices that run on varied embedded devices, operating systems, number of devices connected in IOT and so on. Unfortunately, like any other industry in IOT industry data privacy and security is often disregarded.

On the other hand, with the introduction of cryptocurrency called "Bitcoin" which is tracked securely using Blockchain technology is becoming popular and accepted worldwide. The blockchain technology has proved its potential to identify and trace each transaction irrespective location and network and helps in identification of device, secures data transfer and immutable data storage.

The aim of this research paper is to provide comparative analysis of some of the works available in literature. The paper summarizes the existing work on employing blockchain technology in Internet of things.

Keywords— Blockchain Techonology, Internet of Things, Data Security in IoT, Data Exchange in Internet of Things. .

I. INTRODUCTION

This section briefly introduces the Internet of Things and Blockchain Technology.

A) Internet of Things:

The Internet of Things (IoT) is comprises devices that has abilities for generating, communicating and processing the data as well. As shown in the figure 1., the internet of things is rapidly growing in all industrial sectors and day to day life. With the introduction of internet and smartphones people are more inclined towards easy to use things. In near future IoT will completely shift the paradigm to a new world where things will not only communicate with other things but will also communicate with human. The IoT network not only contains the sensors, mobiles, laptops or computers but also the devices like television, fridge, transport vehicles, aeroplanes and so on. In near future these devices will exchange the data among themselves, manufacturers, administrators and users due which they are more likely to prone for cyber-attacks and the attacker may steal private information or sensitive safety critical data. Hence there is need to think on securing data before it becomes publicly available. Apart from data security there are other challenges also like data privacy, authentication, access rights and challenges related to hardware and software implementation.

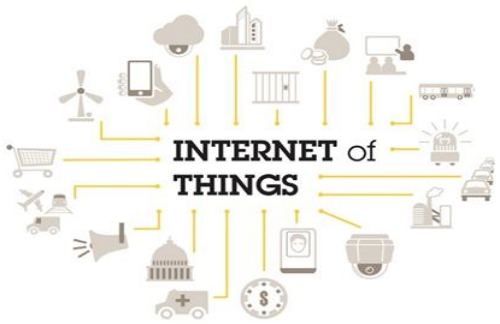

Fig. 1. Internet of Things [26]

B) Blockchain:

Blockchain is also referred as ledger containing records of transaction between two parties which is growing continuously and it uses cryptography to securely link the blocks. Every block contains information like link to previous block in the form of cryptographic hash, timestamp and data of transaction. It is an integral part of the "bitcoin" a digital cryptographic currency invented in 2008. The characteristics of block chain are shown in figure 2. It is decentralized, distributed, cryptographically secured, immutable and non repudiable,

reduces third party dependencies, verifiable etc. It does need a trusted authority or central server system to work. It is managed using peer to peer inter-node communication protocol and validating new blocks. The block header and block body are the two parts of each block in blockchain technology. The header includes information such as version, Merkle tree root hash, timestamp, nBits, Nonce, and parent block hash. The body contains transaction and transaction counter. Transaction storing capacity is dependent on the size of the block. The transaction is authorized by validation mechanism implemented in the form of asymmetric cryptography and digital signatures.

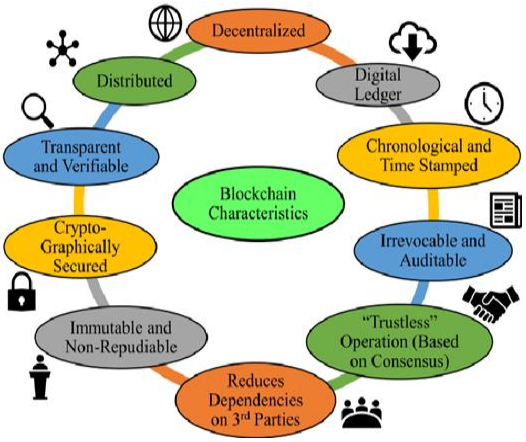

Fig. 2: Characteristics of Blockchain.

II. LITERARTURE SURVEY

Ali Dorri et. al. (2017) proposed a framework to address the security, privacy, and performance of the IoT based smart home and presented the simulated results of traffic overhead & processing overhead in blockchain. It is a hierarchical architecture that contains three tiers as Smart Home, Overlay Network and Cloud Storage. The Smart home contains several IoT devices like thermostat, smart bulbs, an IP camera, sensors etc. The authors ensured decentralized topology is maintained through methods that are distributed and trustworthy. At each tire the authors used local, shared and private Blockchain to securely access the data, control and monitor the devices in IoT smart home network. In this framework the symmetric encryption is used to maintain confidentiality, hashing technique is used to achieve integrity, logging transactions in local Blockchain ensures user control, policy holder and shared keys are used for authorization purpose. However, the authors stated that in worst case for a query-based store transaction the time overhead is 20ms and it increases the energy consumption by 0.07 (mj) of IoT devices [1], [2].

Rawia Bdiwi et. al. (2017) proposed a ubiquitous learning environment (ULE) that is implemented and secured by combing the features of IoT and Blockchain. The learning environment contained devices like IP Camera, integrated sensors, Smart TV, interactive white board, sensors and devices that collects the data and transmit it over internet for analysis and processing. These devices act as the contact point between student and teacher in the ubiquitous learning environment. The cloud-based BC platform allows students and teachers to access the data and services securely. Transaction reliability is ensured using cryptographic hashes. The authors used "consensus protocol" to verify the ledger and transaction sharing is efficient. This distributed architecture helps to decentralize the system [3].

Zhe Yang et. al. (2017) proposed reputation system that allows to judge the message received from sender based on his reputation score. The system is implanted using Blockchain technology for vehicular network. The reputation value of a sender / vehicle is calculated using the historical ratings. The building blocks of proposed systems are the entities involved and procedures. The four entities in the system are trusted authority (TA), ordinary vehicle (OV), malicious vehicle (MV), and miner. The trusted authority (TA) is responsible for registration and allocation of ID, public key and private key. TA also certifies the sensing capacity of vehicle. Ordinary Vehicles remain in vehicle cluster till it is selected by miner. These vehicles can send and receive messages, provide ratings, and can receive raging packages from miner. Malicious Vehicles may exist in the network which may try to disturb the network operation, broadcast false messages, fake ratings etc. The miner is a temporary center node elected among vehicles using specific rules. The procedure includes Data credibility assessment, Rating, Miner election, Block generation and validation, Distributed consensus, Reputation calculation. The authors claimed that the system is able to improve the security of vehicular networks after conducting number of experiments for verifying the reliability of system [4].

Jung, M. Y., & Jang, J. W. (2017), used ECDSA digital signature and SHA-256 hash function in Blockchain to ensure security in data management and data searching system for IoT network. The authors used security properties of Blockchain includes authentication, non-repudiation and data integrity. The Blockchain contains the IP address and data name of the owner. Block hash value is analyzed to implement data management and searching. Based on the simulation results the authors claims that the system is able to prevent IP spoofing, Sybil attack and single point failure. The system is easy to manage [5].

Tian, F. (2017, June) discussed general challenges in scaling blockchains and proposed a decentralized traceability system employing IoT & Blockchain. The author explained the working of proposed system with an example scenario of food supply chain based on Hazard Analysis and Critical Control Points. The theoretical and application concept proposed by author may improve the efficiency and transparency in supply chain as well provide real time information to gain the consumer's confidence in the food industry [6].

Han, D., Kim, H., & Jang, J. (2017) implemented a Smart Door Lock system based on Blockchain using CPU, TCP/IP, Bluetooth / Zigbee, GPS and sensors. The system is able to identify the unauthorized access, inside and outside intruders, immediately. The system also implements security features

like non-repudiation and data integrity implemented through proof of work. The first receiver block is added to chain when miner completes (n+1) rounds and all nodes creates and broadcasts (n+1) blocks. Authors also suggest that 3 to 4 zero bits are required to establish a real-time blockchain network [7].

Xie, C., Sun, Y., & Luo, H. (2017) proposed a three-layer scheme for storing tracking data of agriculture products using Blockchain technology. The sensing layer is the internet of things comprising several sensors like temperature, humidity, pressure, acceleration, GPS and GPRS modules. These IoT devices write the data to Data Storage Layer when a certain action is sensed by sensors. The double chain data storage system is implemented in Ethereum blockchain framework. The system automatically performs encapsulation and data analysis on the data received from sensors and writes it to blockchain. To secure the database transaction hash is used and for improving I/O data efficiency auxiliary database is used. Application Layer enables the user to access data system services through specific applications designed for the specific service [8].

To manage the privacy preference in IoT network Shi-Cho Cha et. al. (2017) proposed the design of a Blockchain based connected Gateway called BC Gateway. To explain the functionality of BC Gateway authors used three types of participant. The first participant is the either owner of IoT Device or Administrator of IoT Device. The second participant is the administrator of BC Gateway and third is the end user. In this system the user can access the IoT device through BC Gateway by obtaining the device information and accepting the privacy policy and the preference is stored on Blockchain network. To resolve the disputes between IoT service provider and user the user preference data can be utilized. Every IoT device is registered on BC Gateway through a device binding where device manager stores the device information and privacy policies using smart contracts. The authors conducted experiment on Etherum network by simulating the BC Gateway and client application on android mobile phone. To implement security features authors used Raspberry PI III Model B for implementing a six "Setup", "Set-Partial-Private-Key", "Set-Secret-Value", "Set-Public-Key", "Sign" and "Verify" phase Digital Signature Scheme. The computational cost of each security module is obtained as shown below [9].

TABLE I: COMPUTATIONAL COST OF SECURITY MODULE [9]

Security Module	Cost
Random number generator (96 bits)	0.5ms
Hash function (SHA-512 with input 1000 bits)	7ms
ECC Pairing (384 bits)	240ms
ECC point multiplication (384 bits)	4ms
ECC point addition (384 bits)	2ms

Ozymaz, K. R., & Yurdakul, A. (2017) configured IoT Gateway in a private etherum network using LoRa nodes as blockchain node for low power IoT devices. As the low power IoT devices can not afford to run complex and long duration blockchain calculations the authors implemented event-based messaging mechanism. End device and a Gateway is implemented using LoRa with Raspberry Pi2 and Pi 3 connected to Dragino LoRa/GPS Hat and iC880A from IMST. A smart contract termed as "Bridge" having two events and two functions enables the communication between end devices and gateway. The two events process and notify whereas the functions are request and activate [10].

Zhu, X., Badr, Y., Pacheco, J., & Hariri, S. (2017) introduced a method for extracting unique signatures which uniquely identifies each IoT device used in Smart Homes. The authors also proposed a distributed and trustworthy Identity Management System based on Blockchain Identity Framework (BIFIT). The system implements two phases, first training the system offline and the second test the system online. Using this method user can monitor and control the various sensors embedded with the appliances like LED Light, AC Lamp, Ventilator, Door Lock, Television etc. [11].

Ning Zhou, Menghan Wu, and Jianxin Zhou (2017), presented a study that utilizes blockchain technology and internet of things to record, store and secure the volunteer service time so that the volunteer's personal data remain secure using smart contracts of blockchain and they are rewarded to keep them motivated for volunteering [12].

Zheng. Z. et. al (2017) explained the overview of Blockchain architecture, its characteristics, consensus algorithms and its comparison in detail along with few challenges and suggestions for future work. The table below describes the comparison among public, consortium and private blockchain [13].

TABLE II: COMPARISON AMONG PUBLIC, CONSORTIUM AND PRIVATE BLOCKCHAIN

Property	Public blockchain	Consortium blockchain	Private blockchain
Consensus determination	All miners	Selected set of nodes	One organization
Read Permission	Public	Public or Restricted	Public or Restricted
Immutability	Impossible to tamper	Can be tampered	Can be tampered
Efficiency	Low	High	High
Centralized	No	Partial	Yes
Consensus process	Permission less	Requires permission	Requires permission

The table below shows the comparison among consensus algorithms [13].

TABLE III: COMPARISON AMONG CONSENSUS ALGORITHMS

Property	PoW	PoS	PBFT	DPOS	Ripple	Tendermint
Node Identity Management	Open	Open	Permissioned	Open	Open	Permissioned
Energy Saving	No	Partial	Yes	Partial	Yes	Yes
Tolerated power of adversary	<25% Computing power	<51% stakes	<33% faulty replicas	<51% Validators	<20% faulty nodes	<33% byzantine voting power
Example	Bitcoin	Peercoin	Hyperledger Fabric	Bitshares	Ripple	Tenermint

Pradip Kumar Sharma, Mu-Yen Chen, and Jong Hyuk Park (2017) proposed an architecture based on fog computing, software defined networking (SDN) and blockchain to address the issues in IoT network like availability, data delivery in real time, security, scalability, latency and resiliency. IoT devices generate the raw data streams in distributed cloud and at the edge of IoT network considering this things authors designed a new distributed cloud architecture based on blockchain. As compared with traditional IoT network the authors model reduces traffic load, computing resources and end to end delay among devices in the distributed blockchain cloud network. The authors evaluated the model on several parameters like throughput, response time, delay-incurred performance metrics, accuracy rate of attack detection and presence of different traffic [14].

Zonyin Shae and Jeffrey J. P. Tsai (2017) discussed design aspects, technology requirements and challenges for a blockchain based architecture aimed to analyze clinical trial and precision medicine data using big data analytics and IoT. The authors identified four different components and discussed requirements and challenges for implementation in the proposed architecture [15]. The four components are listed below.

1. Distributed and parallel computing based on blockchain to devise and study parallel computing methodology for big data analytics.
2. blockchain application data management component for data integrity, big data integration, and integrating disparity of medical related data,
3. verifiable anonymous identity management component for identity privacy for both person and Internet of Things (IoT) devices and secure data access to make possible of the patient centric medicine, and
4. trust data sharing management component to enable a trust medical data ecosystem for collaborative research [15].

According to Salahuddin, M. A. et. al. (2017) IoT networks has a potential to be applied in implementing smart health care solutions as the IoT devices has ability to generate large amount of data in the form of text, audio and video. To utilize this data in health care we will require an effective mechanism for collecting, aggregating, batch processing and pseudo-real or real time processing as the data comes from heterogeneous sources on IoT network. To overcome these issues the authors proposed a cost effective, flexible and secure software architecture build using cloud computing, fog computing and blockchain that can be employed in private IoT for smart health care applications. The architecture provides features such as machine to machine (M2M) messaging, rule base for data management, data and decision fusion so that the smart health care applications and services can be used effectively [16].

Rifi, N., Rachkidi, E., Agoulmine, N., & Taher, N. C. (2017) has proposed a method to secure IoT network using Publisher Subscriber data sharing mechanism with blockchain technology. The method is based on smart contracts between provider and a consumer. The authors used off chain database technology to deal with data storage problems. The block stores the information of contract and reference to where the data is stored. To study the mining process performance with respect to overall system response time the authors presented a data analytic model. A decentralized applications (DApps) framework called Embark is used with Etherum blockchain, IPFS database and Whisper protocol to exchange messages between applications. The authors implemented their private blockchain with two gateways implemented on Raspberry Pi & laptop and a go etherum (geth) client, that notifies when the new smart contract is generated or updated. The smarts contracts are implemented using SolidityC programming whereas the frontend and GUI is implemented using HTML, Javascript and JQuery [17].

Pinno, O. J. A., Gregio, A. R. A., & De Bona, L. C. (2017) proposed an architecture called "ControlChain" which is decentralized, resilience, and capable of working offline to control and authorize access in IoT network. The ControlChain is different from traditional architectures in the sense that it is a completely decentralized and provides transparency in authorization process also it compatible with other access control models used in IoT. The architecture provides a secure way to create relationships, assign attributes and use them in access control. According to authors the traditional access control architectures XACML, OAuth, UMA and FairAccess are unable to provide the full stack of features as compare to ControlChain. The authors presented a comparison as shown in table below [18].

TABLE IV: ARCHITECTURE COMPARISON

Architecture Features	XACML	OAuth	UMA	FairAccess	ControlChain
Scalability	-	-	-	+	+
Fault Tolerant	-	-	-	+-	+
No third parties	-	-	-	+	+
New authorization	+	+	+	-	-(*)
Get authorization	+	+	+	-(*)	+
Integr. Relationship	-	-	-	-	+
Compatibility	+	-	-	-	+
Low object overhead	+	+	+	+	+

(*) dependent on the type of proof and dissemination speed of blocks [18].

Park, J., & Kim, K. (2017) presented a model called "TM-Coin" for trustworthy, efficient remote attestation and decentralized management of Trusted Computing Base (TCB) in IoT devices based on blockchain technology. TM-Coin has taken maximum advantage of ARM TrustZone and blockchain

to securely manage the TCB measurement of IoT devices. It implements miners and verifiers to remotely attest the data received from IoT devices that use TCB measurement method and publish them in Blockchain. The authors implemented the prototype using ARM TrustZone based development board [19].

Considering the potential of drones to be used in future IoT applications, Liang, X., Zhao, J., Shetty, S., & Li, D. (2017) has designed a general architecture using blockchain. The architecture aims to methods for identifying "Trusted Data Origin", "Instant and Permanent Data Integrity", "Trusted Accountability" and "Resilient Backend" while employing drone as an IoT device. The architecture contains important system elements as "Drone", "Control System", "Blockchain Network", "Cloud Database", and "Cloud Server". The authors claim that the system is reliable and accountable for real time data collection and drone control and at the same time it reduces potential attacks and data losses [20].

Li, C., & Zhang, L. J. (2017) presented a model that employs blockchain technology using wide area networking in IoT. The basic idea is to divide the IoT network in decentralized multiple levels and implement the blockchain across each level to ensure the security. The authors enlisted four advantages of using this model are 1) Using a centralized local instrument to coordinate with other IoT devices ensures safety. 2) Computational load, network load and concentrated risks are reducing with the presence of multiple centers. 3) Peer-to-peer communication is established between centers. 4) Contracts record in multiple blockchains ensure secure and reliable IoT network. Authors mention that the total cost of network may increases due to decentralization and additional resources also longer processing time is required to maintain contracts [21].

Ao Lei et. al. (2017) proposed a method that works with heterogeneous networks for secure key management. The authors presented a novel network topology for vehicular communication systems (VCS) based on blockchain to simplify the distributed key management in VCS. The security managers (SMs) captures the vehicle information, encapsulates the block to issue keys, and executes the rekeys to vehicles present in the same security domain. The framework utilizes dynamic transaction collection period to reduce timing of key transfer and handover to other vehicles. The authors presented a simulation of the proposed framework [22].

Huang Z. et. al. (2017) presented an analysis of requirements for data exchange in IoT network. From the security perspective the data exchange must meet three major requirements i.e. trusted privacy preserving policies, trusted access to data and trusted trading. The authors developed a prototype using Etherum blockchain for data exchange in IoT. The prototype includes 10 Etherum nodes as a Blockchain network on an Ubuntu system. Out of these two nodes are used for mining and are deployed in Aliyun servers while others are utilized for IoT data exchange using PC. SolidiyC is used to implement smart contracts which are compiled on any of the miner nodes [23].

Urien, P. (2018) has discussed about integrating secure elements for the blockchain transaction processing in a trusted way. The author also planned to develop Blockchain IoT platform leverage the blockchain technology. According to author the blockchain transaction processing based on ECDSA signature is prone to attack and can be stolen. To eliminate this risk author suggested to use javacard secured elements [24].

Christidis, K., & Devetsikiotis, M. (2016) has examined the fitness of blockchain in the field of Internet of things. The authors reviewed the working mechanism of blockchain and explored the whether its combination with IoT is helpful in creation of the market in which services of devices, and resources can be shared through a cryptographically secured and automated mechanism. The authors also identified and discussed several implantation issues of these technology and concluded that the combination of blockchain and IoT will definitely contribute in introducing the new business models and distributed applications [25].

III. National & International Scenario:

The proposed work is in its early stage where the focus more oriented towards studying the Blockchain technology, Internet of Things. The study is also trying to analyze how the combination of both can be done to secure the data exchanged among IoT devices through maintaining privacy preferences of users, IoT devices and administrators. At this point of study, a thorough literature survey of 25 papers published in year 2017 is carried out. Some of the observations are listed below.

A. International Scenario:

•Most of the researchers across the globe are trying to find out how blockchain can help in securing the data access and transfer among IoT devices and other heterogenous networks.

•In most of the studies researchers proposed either the framework / architecture / method or prototype to utilize blockchain for data security, privacy, data access etc. in IoT.

•Few studies simulated or implemented the prototype to test the proposed framework or architecture.

•Most of the studies used Raspbery Pi family of boards for implementation of prototypes.

•Etherum framework of blockchain technology is more commonly used by the researchers.

B. National Scenario:

Out of these 25 studies none of the national studies were present. Whereas few national researchers are working jointly with the international researchers to solve the issues for combining blockchain and IoT technology.

IV. Results of Learning Object Evaluation:

The comparative analysis is shown in Appendix-I

V. CONCLUSIONS:

Blockchain and Internet of Things are comparatively new technologies and industries are finding the ways to introduce in common market place for the use. The studies available in literature are more prototype oriented and less practical oriented. Most of the studies has considered Smart Home Scenario for their prototypes / frameworks of implementation there are other areas also where IoT network and devices can bring the drastic change in our daily lives or in industries. Hence there is need to study and implement other IoT application scenarios. At the same time IoT network contains heterogeneous devices having less computing abilities for data processing and power / energy constraints. The blockchain is a decentralized technology and can be able to provide security in data exchange among IoT and other devices but still it is not explored in more detail. Most of the researchers used Etherum Blockchain frameworks hence there is need to compare the any other frameworks if available and then employ it with IoT for data security.

REFERENCES

[1] Dorri, A., Kanhere, S. S., & Jurdak, R. (2017, April). Towards an optimized blockchain for IoT. In Proceedings of the Second International Conference on Internet-of-Things Design and Implementation (pp. 173-178). ACM.

[2] Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017, March). Blockchain for IoT security and privacy: The case study of a smart home. In Pervasive Computing and Communications Workshops (PerCom Workshops), 2017 IEEE International Conference on (pp. 618-623). IEEE.

[3] Bdiwi, R., de Runz, C., Faiz, S., & Cherif, A. A. (2017, July). Towards a New Ubiquitous Learning Environment Based on Blockchain Technology. In Advanced Learning Technologies (ICALT), 2017 IEEE 17th International Conference on (pp. 101-102). IEEE.

[4] Yang, Z., Zheng, K., Yang, K., & Leung, V. C. (2017, October). A blockchain-based reputation system for data credibility assessment in vehicular networks. In Personal, Indoor, and Mobile Radio Communications (PIMRC), 2017 IEEE 28th Annual International Symposium on (pp. 1-5). IEEE.

[5] Jung, M. Y., & Jang, J. W. (2017, October). Data management and searching system and method to provide increased security for IoT platform". In Information and Communication Technology Convergence (ICTC), 2017 International Conference on (pp. 873-878). IEEE.

[6] Tian, F. (2017, June). A supply chain traceability system for food safety based on HACCP, blockchain & Internet of things. In Service Systems and Service Management (ICSSSM), 2017 International Conference on (pp. 1-6). IEEE.

[7] Han, D., Kim, H., & Jang, J. (2017, October). Blockchain based smart door lock system. In Information and Communication Technology Convergence (ICTC), 2017 International Conference on (pp. 1165-1167). IEEE.

[8] Xie, C., Sun, Y., & Luo, H. (2017, August). Secured Data Storage Scheme Based on Block Chain for Agricultural Products Tracking. In Big Data Computing and Communications (BIGCOM), 2017 3rd International Conference on (pp. 45-50). IEEE.

[9] Cha, S. C., Chen, J. F., Su, C., & Yeh, K. H. (2018). A Blockchain Connected Gateway for BLE-based Devices in the Internet of Things. IEEE Access.

[10] Özyılmaz, K. R., & Yurdakul, A. (2017, October). Integrating low-power IoT devices to a blockchain-based infrastructure: work-in-progress. In Proceedings of the Thirteenth ACM International Conference on Embedded Software 2017 Companion (p. 13). ACM.

[11] Zhu, X., Badr, Y., Pacheco, J., & Hariri, S. (2017, September). Autonomic Identity Framework for the Internet of Things. In Cloud and Autonomic Computing (ICCAC), 2017 International Conference on (pp. 69-79). IEEE.

[12] Zhou, N., Wu, M., & Zhou, J. Volunteer Service Time Record System Based on Blockchain Technology. (2017). IEEE.

[13] Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017, June). An overview of blockchain technology: Architecture, consensus, and future trends. In Big Data (BigData Congress), 2017 IEEE International Congress on (pp. 557-564). IEEE.

[14] Sharma, P. K., Chen, M. Y., & Park, J. H. (2018). A software defined fog node based distributed blockchain cloud architecture for iot. IEEE Access, 6, 115-124.

[15] Shae, Z., & Tsai, J. J. (2017, June). On the Design of a Blockchain Platform for Clinical Trial and Precision Medicine. In Distributed Computing Systems (ICDCS), 2017 IEEE 37th International Conference on (pp. 1972-1980). IEEE.

[16] Salahuddin, M. A., Al-Fuqaha, A., Guizani, M., Shuaib, K., & Sallabi, F. (2017). Softwarization of Internet ofThings Infrastructure for Secureand Smart Healthcare. Computer, 50(7), 74-79.

[17] Rifi, N., Rachkidi, E., Agoulmine, N., & Taher, N. C. (2017, September). Towards using blockchain technology for IoT data access protection. In Ubiquitous Wireless Broadband (ICUWB), 2017 IEEE 17th International Conference on (pp. 1-5). IEEE.

[18] Pinno, O. J. A., Gregio, A. R. A., & De Bona, L. C. (2017, December). ControlChain: Blockchain as a Central Enabler for Access Control Authorizations in the IoT. In GLOBECOM 2017-2017 IEEE Global Communications Conference (pp. 1-6). IEEE.

[19] Park, J., & Kim, K. (2017, March). TM-Coin: Trustworthy management of TCB measurements in IoT. In Pervasive Computing and Communications Workshops (PerCom Workshops), 2017 IEEE International Conference on (pp. 654-659). IEEE.

[20] Liang, X., Zhao, J., Shetty, S., & Li, D. (2017, October). Towards data assurance and resilience in IoT using blockchain. In Military Communications Conference (MILCOM), MILCOM 2017-2017 IEEE (pp. 261-266). IEEE.

[21] Li, C., & Zhang, L. J. (2017, June). A Blockchain Based New Secure Multi-Layer Network Model for Internet of Things. In Internet of Things (ICIOT), 2017 IEEE International Congress on (pp. 33-41). IEEE.

[22] Lei, A., Cruickshank, H., Cao, Y., Asuquo, P., Ogah, C. P. A., & Sun, Z. (2017). Blockchain-based dynamic key management for heterogeneous intelligent transportation systems. IEEE Internet of Things Journal, 4(6), 1832-1843.

[23] Huang, Z., Su, X., Zhang, Y., Shi, C., Zhang, H., & Xie, L. (2017, December). A decentralized solution for IoT data trusted exchange based-on blockchain. In Computer and Communications (ICCC), 2017 3rd IEEE International Conference on (pp. 1180-1184). IEEE.

[24] Urien, P. (2018, February). Towards secure elements for trusted transactions in blockchain and blochchain IoT (BIoT) Platforms. Invited paper. In Mobile and Secure Services (MobiSecServ), 2018 Fourth International Conference on (pp. 1-5). IEEE.

[25] Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. IEEE Access, 4, 2292-2303.

[26] https://www.axis.com/blog/secure-insights/internet-of-things-reshaping-security/ accessed on 17/06/2018.

[27] Puthal, D., Malik, N., Mohanty, S. P., Kougianos, E., & Yang, C. (2018). The blockchain as a decentralized security framework. IEEE Consumer Electronics Magazine, 7(2), 18-21.

Appendix - I
Comparative Analysis of Existing Research Work

Paper No.	Aim / Objective	Approach to implement solution	Technique / Methods / Technology Applied / Explained	Findings / Results / Remarks
[1], [2]	Case study to address the security, privacy, and performance in terms of traffic & processing overhead in IoT based Smart Home.	Simulated IoT Network of 50 Nodes out which 13 are Cluster Heads.	1) Symmetric Encryption to maintain data confidentiality 2) Appending blocks without POW 3) Distributed trust method 4) Signature based verification for authorization 5) Hashing technique for data integrity	1) A simulation having 60 Seconds run time created 960 transactions. 2) Proposed architecture reduces traffic & processing overhead compare to BC in bitcoin. 3) On the other hand, in worst case scenario is overhead is increased by 20ms and it increases the energy consumption by 0.07 (mj) of IoT devices
[3]	To design secured collaborative learning system using IoT & Blockchain	The authors used IP Camera, integrated sensors, Smart TV, interactive white board etc.	1) Cloud based Blockchain platform. 2) Cryptographic Hashes 3) Consensus protocol	1) Authors claimed that integration of IoT with Blockchain feature can enhance the next generation IoT applications. 2) **Explained Theoretical Concepts** 3) **It can be considered as a prototype as no practical results are presented**
[4]	To build a reputation system that allows to judge the message received from sender based on his reputation score	Simulated a Vehicular Network as an IoT	1) Data credibility assessment, 2) Rating, 3) Miner election, 4) Block generation and validation, 5) Distributed consensus, 6) Reputation calculation	Simulation Results: 1) Message Detection Accuracy (MDA) increases when reputation threshold (RTH) reaches peak and drops gradually when it reaches to 0. 2) MDA of blockchain-based scheme drops rapidly when the ratio of malicious capacity (ROM) exceeds 0.325 3) MDA degrades when the Number of zero (NOZ) exceeds the proper range. 4) **Can be considered as a prototype.**
[5]	to ensure security in data management and data searching system for IoT network	Network of Data owner nodes identified using IP address	7) ECDSA digital signature 8) SHA-256 hash function	1) Authors claim that simulation results are better than existing system. 2) **Explained Theoretical Concepts** 3) **It can be considered as a prototype as no practical results are presented**
[6]	To discuss general challenges in scaling blockchains. To propose a decentralized traceability system employing IoT & Blockchain	Example scenario of food supply chain based on Hazard Analysis and Critical Control Points	Explained key characteristics of 1) Blockchain 2) DistributedDBS 3) BigchainDB.	1) The theoretical and application concept proposed by author may improve the efficiency and transparency in supply chain as well provide real time information to gain the consumer's confidence in the food industry. 2) **Explained Theoretical Concepts**
[7]	To identify unauthorized access, inside and outside intruders. To implement security features non-repudiation and data integrity	Smart Door Lock system based on Blockchain using CPU, TCP/IP, Bluetooth / Zigbee, GPS and sensors	1) Cryptography (Public Key and Private Key) 2) SHA-256 (Proof of Work)	3) Practical Results are not available 4) **Explained Theoretical Concepts**
[8]	To design a scheme to store data tracking of agriculture products using Blockchain technology	IoT of sensors like temperature, humidity, pressure, acceleration, GPS and GPRS modules	1) Double-chain storage structure 2) Hashing technique	1) This scheme spends about 130% the time of non-chain mode in data writing. 2) 200-300 sensor data per second is written to blockchain.
[9]	To manage the privacy preference in IoT network using Blockchain Technology	The first participant is the either owner / Admin of IoT Device The second participant is the administrator of BC Gateway and third is the end user	1) Device Binding 2) Smart Contracts 3) Random number generator (96 bits) 4) Hash function (SHA-512 with input 1000 bits) 5) ECC Pairing (384 bits) 6) ECC point multiplication (384 bits) 7) ECC point addition (384 bits) (elliptic curve algorithm)	Computational cost for each security module is indicated in front of it. 1) Random number generator (96 bits) – 0.5ms 2) Hash function (SHA-512 with input 1000 bits) – 7ms 3) ECC Pairing (384 bits) – 240ms 4) ECC point multiplication (384 bits) – 4ms 5) ECC point addition (384 bits) – 2ms

[10]	To create a proof of concept to enable low-power, resource-constrained IoT end-devices accessing a blockchain-based infrastructure	IoT gateway is configured as a blockchain node and an event-based messaging mechanism for low-power IoT end-devices	1) Smart Contract 2) LoRa protocol software 3) Etherum Blockchain	1) Practical Results are not available 2) **Explained Theoretical Concepts**
[11]	To identify attacks like Replay, Delay, Denial of Service (DoS), Flooding, Impersonation, Pulse DoS, and Noise injection in Smart Home using Blockchain	IoT network of device LED Light, AC Lamp, Ventilator, Door Lock, Television equipped with sensors.	1) five levels of decomposition for DWT 2) jRip algorithm	1) most of the attacks are detected with more than 97% of accuracy 2) replay attack the detection rate is 88.75%.
[12]	To record, store and secure the volunteer service time in IoT using Blockchain.	application example to illustrate the usage of volunteer service time system for tree plantation	1) Smart contracts 2) ECDSA elliptic curve algorithm	1) Proposed solution enables every participant to have an access to monitor the procedure of voluntary activities and as the owner of their personal data. 2) Practical results are not available
[13]	To explain overview of Blockchain architecture, its characteristics, consensus algorithms and its comparison in detail along with few challenges and suggestions for future work	NA	NA	1) **Theoretical Explanation**
[14]	to address the issues in IoT network like availability, data delivery in real time, security, scalability, latency and resiliency	Proposed distributed cloud architecture based on blockchain	1) fog computing, 2) software defined networking (SDN) 3) 2-hop blockchain technique 4) Classified advertisement (classad) matchmaking technique 5) CLOUDRB for managing and scheduling performance computing application 6) TFN2K tool to generate real-time attacks	7) The results of evaluation show that performance is improved by reducing the induced delay, reducing the response time, increasing throughput, and the ability to detect real-time attacks in the IoT network with low performance overheads.
[15]	To discuss design aspects, technology requirements and challenges for a blockchain based architecture aimed to analyze clinical trial and precision medicine data using big data analytics and IoT	Developed a blockchain platform to investigate (a) peer verifiable data integrity, and (b) data sharing and trust collaboration	1) semantic computation and text exploration techniques 2) smart contracts	1) Real identities of more than 60% users is identified. 2) Discussion on data analytics, privacy, security and data integration mechanism is given.
[16]	To identify effective mechanism for collecting, aggregating, batch processing and pseudo-real or real time processing as the data comes from heterogeneous sources on IoT network.	Authors proposed a cost effective, flexible and secure software architecture build using cloud computing, fog computing and blockchain with private IoT for smart health care applications.	1) data fusion and decision fusion. 2) Smart contracts	1) The architecture provides features such as machine to machine (M2M) messaging, rule base for data management, data and decision fusion so that the smart health care applications and services can be used effectively
[17]	To develop a method to secure IoT network with blockchain technology	Raspberry Pi & laptop and a go etherum (geth) client, that notifies when the new smart contract is generated or updated. The smarts contracts are implemented using SolidityC programming whereas the frontend and GUI is implemented using HTML, Javascript and JQuery	1) Publisher Subscriber data sharing mechanism 2) smart contracts 3) (DApps) framework 4) Whisper protocol 5) off-chain database technology	1) The objective of this work was to consider the possibility to use blockchain technology in the area of security in IoT. We have presented an architecture solution designed for that purpose that is based on contract model between a provider and a consumer of data. 2) **Theoretical Explanation**
[18]	To implement a Blockchain based architecture for IoT access authorizations	divided the database of the ControlChain in 4 different Blockchains: Context Blockchain, Relationships Blockchain, Rules Blockchain and Accountability Blockchain for IoT	1) NA	1) The architecture is fully decentralized (requiring no third-party), scalable, user transparent, user friendly, fault tolerant and compatible with a wide range of access control models employed in the IoT. 2) **Theoretical Explanation**

[19]	To present a model called "TM-Coin" for trustworthy, efficient remote attestation and decentralized management of Trusted Computing Base (TCB) in IoT devices based on blockchain technology.	ARM TrustZone and blockchain to securely manage the TCB measurement of IoT devices	1) It implements miners and verifiers to remotely attest the data received from IoT devices that use TCB measurement method and publish them in Blockchain	1) The authors implemented the prototype using ARM TrustZone based development board 2) **Theoretical Explanation**
[20]	To design a general architecture using blockchain for Drones as IoT network and data exchange.	The architecture contains important system elements as "Drone", "Control System", "Blockchain Network", "Cloud Database", and "Cloud Server"	1) Discussion on methods for identifying "Trusted Data Origin", "Instant and Permanent Data Integrity", "Trusted Accountability" and "Resilient Backend	1) The authors claim that the system is reliable and accountable for real time data collection and drone control and at the same time it reduces potential attacks and data losses 2) **Theoretical Explanation**
[21]	To divide the IoT network in decentralized multiple levels and implement the blockchain across each level to ensure the security	Layered Network of IoT Devices.	1) The mapping between logical layer and practical address 2) compare Sum 3) asymmetric encryption	1) The multi-layer network model based on block-chain technology provides a feasible solution for the establishment of wide-area secure IoT network 2) **Theoretical Explanation**
[22]	To identify a method that works with heterogeneous networks for secure key management	Simulated network topology for vehicular communication systems (VCS) based on blockchain to simplify the distributed key management in VCS.	1) The security managers (SMs) captures the vehicle information, encapsulates the block to issue keys, and executes the rekeys to vehicles present in the same security domain. The framework utilizes dynamic transaction collection period to reduce timing of key transfer and handover to other vehicles	1) The authors presented a simulation of the proposed framework 2) The results of simulation for each scheme is given in milliseconds. ECIES Encryption 0.51027 ECIES Decryption 0.73996 ECDSA Signing 0.51011 ECDSA Verifying 1.10171 Block Mining 4.11046
[23]	To analyze of requirements for data exchange in IoT network in terms of trusted privacy preserving policies, trusted access to data and trusted trading	The prototype includes 10 Etherum nodes as a Blockchain network on an Ubuntu system. Out of these two nodes are used for mining and are deployed in Aliyun servers while others are utilized for IoT data exchange using PC. SolidiyC is used to implement smart contracts which are compiled on any of the miner nodes	1) access contracts, communication contracts and auto exchange contracts	1) Provided deeply **theoretical** analysis of current trusted requirement in IoT data exchange and divides them into three categories: trusted trading, trusted data access and trusted privacy preserve
[24]	To discuss about integrating secure elements for the blockchain transaction processing in a trusted way	The author also planned to develop Blockchain IoT platform leverage the blockchain technology	1) javacard secured elements	1) According to author the blockchain transaction processing based on ECDSA signature is prone to attack and can be stolen. 2) To eliminate this risk author suggested to use javacard secured elements. 3) **Theoretical Explanation**
[25]	To examine the fitness of blockchain in the field of Internet of things	The authors reviewed the working mechanism of blockchain and explored the whether its combination with IoT is helpful in creation of the market in which services of devices, and resources can be shared through a cryptographically secured and automated mechanism	1) Smart Contracts	1) The authors also identified and discussed several implantation issues of these technology and concluded that the combination of blockchain and IoT will definitely contribute in introducing the new business models and distributed applications. 2) **Theoretical Explanation**