International Journal of Engineering, Management, Humanities and Social Sciences Paradigms (IJEMHS)
(Volume 31, Issue: Special), June 2019
An Indexed and Referred Journal with Impact Factor: 2.75
ISSN (Online): 2347-601X
www.ijemhs.com

Security issues in Blockchain Applications using IOT

Jyotikanta Jena, Assistant Professor, Department of Computer Science & Engineering, Krupajal Engineering College, Bhubaneswar
Karishma Singh, UG Student, Department of Computer Science & Engineering, Krupajal Engineering College, Bhubaneswar
Raj Krishna Jha, UG Student, Department of Computer Science & Engineering, Krupajal Engineering College, Bhubaneswar
Bhola Kumar, UG Student, Department of Computer Science & Engineering, Krupajal Engineering College, Bhubaneswar

Abstract:- **As we all know that Blockchain is a distributed and decentralized ledger that contains connected blocks of transactions. where it guarantees tamper-proof storage of approved transactions, Unlike other ledger approaches. The blockchain is being used within IoT due to its distributed and decentralized organization, e.g. to store sensor data and enable micro-payments or manage device configuration. A key challenge in the deployment of Blockchain technology is the hosting location. The Blockchain is distributed in nature which makes the system more robust and immune to a single point of failure [2]. IOT devices either it be a smart home device, smart phone, tablet or any wearable technology are being connected to the internet. These IOT devices are becoming a very major part of our daily life. We can use many forms without being aware that we have started depending on them like for security purpose we us security systems in our house, like smarts locks on our doors to keep our self-safe from the Hackers. Now the latest trending IOT devices security has become one of the major concerns of the IT Industry. In this paper we are going to discuss about the latest block chain technique application to develop a framework for security and management of data on the internet [1]. I have also researched about various application and there uses in this paper.**

Keywords: Blockchain; Centralized & Decentralized; IOT; Blockchain Applications;

I. INTRODUCTION

The IOT or we can say Internet of things is changing almost everything single thing in our surroundings the way we way we communicate or get power or shop with each other with different devices [5]. Usually Iot devices have Small chips and sensor are embedded in physical devices which transmit valuable information. These information gives us a better understanding how these devices work and how they are becoming essential for our day to day life.

Iot devices usually share a large amount of data either it can be our health data or our day to day money transaction data, this large amount of data is shared between different devices over the common platform i.e., internet of things. The IOT platform allows different applications to communicate with each other by combining the data from different devices and applying analytics on the data to share the valuable information among the applications.

Most of the smart devices in our house are connected to the smart-hub. Where most of these smart hubs contain serious vulnerabilities where the hacker can easily access to come to our front door and can unlock the lock the door which is connected to the smart-hub. If successfully access is gained by the attacker of our wireless network this will allow the cyber criminals to spot the smart-hubs which they can hack easily giving them access to our house security devices resulting in compromising our security or may be these moonlighters could walk up to our front door as a trespasser.

II. CIA TRAID

In CIA Traid C-Confidentiality I-Integrity A-Availability is a model which is designed to guide policies for information security within an organization [1].

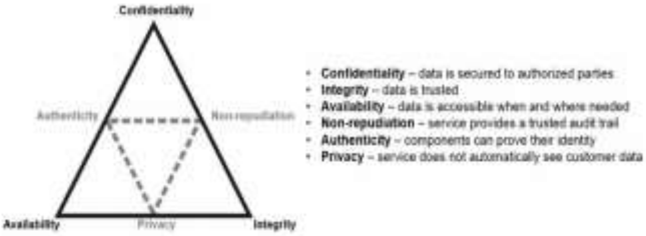
Confidentiality
Authenticity
Non-repudiation
Availability
Privacy
Integrity
Confidentiality – data is secured to authorized parties
Integrity – data is trusted
Availability – data is accessible when and where needed
Non-repudiation – service provides a trusted audit trail
Authenticity – components can prove their identity
Privacy – service does not automatically see customer data

Fig:1 Cia Traid

III. CHALLENGES IN IOT

Scalability- Many types of devices working together on the IOT platform it is very difficult to provide same security level among the entire network [1].

Manageability-Managing the details of all data is very difficult which leads to may authority issues.

Reliability – As we know that IOT consist of huge networks and it is very difficult to authorize reliability of all the sources of data such as in case of data attacks like man in middle attack.

Capability – Implementation of any secure algorithm is very tough due to its Availability of limited size of memory and limited amount of computing resources

Privacy – Securing the data of participants from the exposure and falling of data in the hands of unwanted parties.

IV. APPLICATIONS OF BLOCKCHAIN

Here are some applications where Blockchain has been applied and this table also shows how Blockchain applications are useful [4]

Application	Examples	Description
Cryptocurrency	Bitcoin Litecoin Namecoin	These all are digital coins used for payments. Here Bitcoin is the first and most widely used decentralized ledger currency with the highest market capitalization. Litecoin is the first cryptocurrency to use Scrypt as a hashing algorithm. Namecoin is the first cryptocurrency to use scrypt as a hashing algorithm.
Smart contract	Blockchain HealthCare, Blockchain music, property law etc.	In the Blockchain HealthCare Personal health records could be encoded and stored on the blockchain with a private key which would grant access only to specific individuals. One of the major problems in the music industry include ownership rights, royalty distribution, and transparency. Here the digital music industry focuses on monetizing productions, while ownership rights are often overlooked.
Food Industry	Consumers, Food security Department	Blockchain could be used to create a Digital Certificate for each piece of food proving from where it has come from and where it has been. How it has been transported? Where it was harvested /processed? What batch does it belong to? If the contamination is detected we can trace it back to its roots and instantly notify other people who has brought the same batch of the bad food. Who has been in contact with it? Where was it sold? Was it kept at the right temperature?
Energy markets	Smart grids by LO3 energy Wien energy Innogy	Local trading of solar energy Trading of energy between Utilities Wien energy are the solution for automated billing of electrical vehicle charging stations
Smart Property	Chromaway. SBAB. Telia. Lantmateriet	Transfer of property right for assets such as land or other tangible assets using blockchain.
Blockchain Identity	Passport, Digital Id’s	It could help owners identify themselves online and off. Here we you have to take a picture of yourself stamp it with a public and private key, both of which are encoded to prove it is legitimate. Here the passport is stored on the ledger, given a Bitcoin address with a public IP, and confirmed by Blockchain users. In the future you’ll be able to use the one digital ID for signing up at any registrar. It’s an open source secured by the blockchain, and protected by a ledger of transparent account.
Blockchain Financial Services	Insurance: Claims processing Payments: Cross-Border Payments	Here the blockchain provides a perfect system for risk-free management and transparency. Here Its encryption properties allow insurers to capture the ownership of assets to be insured and It will help customers from getting cheated from fraud claims As we know that the global payments sector is error-prone, costly, and open to money laundering. It would take days if not longer for money to cross the world In 2004, Santander became one of the first banks to merge blockchain to a payment’s app, enabling customers to make international payments 24 hours a day, while clearing the next day.

V. BLOCKCHAIN AND IOT

Blockchain technology is one of the best ways to solve major privacy and scalability concerns in the Internet of Things. IoT industry must use blockchain technique which could be used for tracking billions of connected devices or enabling the process of transactions and coordination between devices and allowing for significant savings to IoT industry manufacturers. There is no single point failure due to its decentralized approach. Blockchain mainly uses cryptographic algorithms which would make consumer data more private [7]. As we know IOT is a distributed system, but Today most of these work with support from a centralized infrastructure. Here the sensors and the actuators can talk to each other, but cannot execute coordinated tasks, without trust. A smart contract can be used and executed across a peer group of devices, with trust. Can form a low cost and low maintenance trusted ecosystem. There are Some features where the privacy and security challenges in Iot are the best.

Decentralization not only eliminates many to one traffic flows but also overcomes the problem of a single point failure where it ensures the scalability and robustness by using resources of all participating nodes in the blockchain. Anonymity: Identity of the users must be kept private where the inherent anonymity is afforded which is suited for most of the Iot use cases.

Security in blockchain ensures a very secure network over untrusted third parties which would be very beneficial in IoT with numerous devices.

VI. PROBLEMS USING BLOCKCHAIN USING IOT

No matter how much benefits we have from the blockchain model but there will definitely be some flaws and shortcomings. Here are some flaws which I have listed below

Scalability issues – which relates to the size of Blockchain ledger that may or might lead to centralization as it's grown over time and it would require some **kind of** record management which depends over the future of the Blockchain technology.

Processing power and time – It is required to perform encryption algorithms for all the objects involved in Blockchain based IoT system given the fact that IoT systems are very comprised of the devices that have very different computing capabilities, not all of them will be capable of running the same systems.

Storage will be a hurdle - Blockchain eliminates the need for a central server to store all the transactions and device IDs, the ledger will increase in size as time passes but the ledger has to be stored on the nodes themselves. Which is beyond the capabilities of a wide range of smart devices such as sensors, that have a very low storage capacity [1].

V. LITERATURE SURVEY

Security issues has become widespread nowadays here a literature survey on various security issues occurring in IoT devices and applications and how blockchain plays a role in it as a savior. There are many related conferences, workshops and symposiums around the world [3].

The concept of bit coin is in a way difficult to theorize but can be implemented in practice [1]. Though it has not been extensively researched and documented it still can prove to be a very strong form of online currency. Bitcoin has its own perks when it comes in comparison to the traditional old bank transactions. It is a decentralized form of currency, in simple terms it means that nobody rules over it. The presence of many redundant copies of the transaction database eliminates any third-party rule over the money you own and lets you exercise total control over it, the government can’t freeze your money [3]. Transactions are practically

Table: Shows various security applications used in blockchain

AUTHOR	TITLE	YEAR	OBJECTIVES	METHODOLOGY	TOOLS

Himanshu Gupta	A Security Framework for IOT Devices Against Wireless Threats	2017	In this paper, block chain technique is being used to develop a framework for security and management of data over the internet. The developed a framework which shows how smart devices communicate with each other with block chain posing as the backbone. The framework serves as a scalable and robust solution, in order to address identity and security concerns of IOT.	Block chain uses the decentralized method to secure the data rather than having a dedicated system. No individual or the company is able to control the information which is contained on the Public blockchain or the rules governing the blockchain. Here it is not possible for the "owner" of the blockchain to change the rules of the blockchain at his own wish. SHA-256 Algorithm is being used for more security	Database, Sensors, IoT devices, Wi-fi router, internet connectivity, Python

Bayu Adhi Tama, Bruno Joachim Kweka, Youngho Park, Kyung-Hyune Rhee	A Critical Review of Blockchain and Its Current Applications	2017	In this paper, it thoroughly reviews the applications used in the Blockchain technology which has been known as a digital currency platform since the emergence of Bitcoin, the first and the largest of the cryptocurrencies. The decentralized transaction ledger of blockchain could be employed to register, confirm, and send all kinds of contracts to other parties in the network.	Various applications are being used with help of blockchain which will be giving us more security and privacy over the internet. For e.g. Health care In the Blockchain HealthCare Personal health records could be encoded and stored on the blockchain with a private key which would grant access only to specific individuals. Or in energy markets Transfer of property right for assets such as land or other tangible assets using blockchain can be done	RFID, sensors, routers, C++
Mayra Samaniego, Uurtsaikh Jamsrandorj, Ralph Deters	Blockchain as a Service for IoT	2017	This paper evaluates the use of cloud and fog as hosting platforms. Blockchain guarantees tamper proof storage of approved transactions. Due to its distributed and decentralized organization, blockchain is being used within IoT e.g. to manage device configuration, store sensor data and enable micro-payments. A key challenge in the deployment of blockchain technology is the hosting location.	The fog and the cloud are two equally suited hosting platforms for a blockchain as a service. Cloud and fog are mirror images of each other regarding computational resources and latency. While the fog has limited resources, it exhibits low latency. On the other hand, cloud hosted applications can scale out and thus overcome resource constraints at the price of significant latency issues evaluates the use of the fog and the cloud as possible platforms. The performance analysis clearly indicates that the network latency is the dominant factor. Consequently, the fog outperforms the cloud	Intel Edison Arduino boards, Python, Python servers, cloud,
Rahul Agrawal, Pratik Verma, Rahul Sonanis, Umang Goel, Dr. Alok Nath De, Sai Anirudh Kondaveeti, Suman Shekhar	Continuous Security in Iot Using Blockchain	2018	This paper proposes a blockchain based IoT security solution where trust is established through the immutable and decentralized nature of blockchain. The distributed nature of blockchain makes the system more robust and immune to single point of failure. A unique digital crypto-token is required for a user interaction to be legitimate. This token is used as an access control mechanism to prevent any unauthorized access to the system. Tokens are pre-generated using a prediction model based on user’s IoT-trail in the blockchain. By using blockchain as an underlying framework in IoT environment and through the method of continuous security, we made the system more secure, robust and interoperable.	Continuous security is achieved primarily through IoT-Zone identification, IoT-Token generation for next valid zones and Token validation. IoT-Zone identification needs active monitoring of user IoTtrails. Every user in the IoT system has to register with Enrolment Certificate Authority (ECA) which provides an Enrolment Certificate (ECert) to the user. User’s public key is used to gather transactions from blockchain establishing his/her trail. GPS system and locations of surrounding IoT-devices in the network along with mined user trail helps in establishing his current zone. Once IoT-token has been generated, an action is triggered which is being analysed by a nearby IoT-hub. IoT-hub queries the particular token from digital wallet of nearby user devices via API and verifies it with the help of blockchain network. Each user has unique private-public key pair. Token is signed using RSA Digital Signature algorithm [12] by user’s private key. Digital Signature is verified first on blockchain network using user’s public key. This ensures that token is not used by another user in the network in case of token theft.	JASON Objects, LSTM (Long Short-Term Memory), Iot Devices

Seyoung Huh, Sangrae Cho, Soohyung Kim ETRI, Daejeon	Managing IoT Devices using Blockchain Platform	2017	Using blockchain, we can control and configure IoT devices. We manage keys using RSA public key cryptosystems where public keys are stored in Ethereum and private keys are saved on individual devices. Specifically, we choose Ethereum as our blockchain platform because using its smart contract, we can write our own Turing-complete code to run on top of Ethereum. Thus, we can easily manage configuration of IoT devices and build key management system.	In this paper we have deployed smart contracts on Ethereum. Once we deployed contracts, we started to provide inputs after encoding. Once we have successfully updated/registered values on Ethereum, we were able to retrieve values from Ethereum. we used Raspberry Pi to simulate IoT system. We set up meter, which updates to Ethereum network periodically. We used a smartphone to set up the policies of air conditioner and LED. And those two devices respond according to policies given from Ethereum	Raspberry Pi, LED, Sensors, IoT Devices
Arman Pouraghily, Md Nazmul Islam, Sandip Kundu, Tilman Wolf	Privacy in Blockchain-Enabled IoT Devices	2018	In this work, we propose an architectural guideline for blockchain enabled IoT devices which facilitates sharing them between multiple blockchain ecosystems and at the same time, ensures the exclusive access to them seamlessly through blockchain smart contracts.	Proposed method which is based on Ethereum blockchain network, the shared resources are directly connected to the blockchain and are controlled by a smart contract through which they receive and update their security parameters as well as the serving user's information. presented the design guidelines for such IoT devices and the smart contracts controlling them.	Raspberry Pi, IoT device, Smart Contract**,**
Supriya Thakur Aras, Vrushali Kulkarni	Blockchain and Its Applications a Detailed Survey	2017	This detailed survey intends to bring together all the key developments so far in terms of putting blockchain to practice. While the most common adoption of blockchain is in finance and banking domain, there are experiments being conducted by many big players in various other domains. This paper will explore the various domains where blockchain has had an impact and where future implementations may be expected.	Proof of Work E.g.: Bitcoin, Litecoin, Dogecoin, Namecoin • Considered very secure, as less prone to Sybil attack unless a mining node acquires • 51% of the pools computing power. • Miners get rewards (as Bitcoins) • Prevents unlawful forking of the chain Proof of Stake • Less wasteful in terms of energy consumption • Less chance of hardware centralization • Potentially faster than Proof-of-work protocol • Possibly reduced possibility of selfish mining attack (assuming already rich miners are less likely to attack!)	Raspberry Pi, IoT device, Smart Contract,

Li Shuling	Application of Blockchain Technology in Smart City Infrastructure	2018	This paper, first introduces the role of the big data, IoT, and the energy Internet in the construction of smart city and Blockchain technology. By analysing their respective characteristics and comparing their similarities, corresponding solutions are put forward to aim at the problems such as poor security of IoT, upgrading of equipment maintenance and upgrading, construction and	Blockchain 1.0 refers to cryptographic currency, such as the most famous bitcoin. Blockchain 2.0, on the other hand, is a contract that can cover economic, marketing and financial applications and can be extended to more areas such as equities, debt, insurance, title, smart assets and contracts only. Blockchain 3.0, on the other hand, transcends the fields of money, finance and markets, especially in the	Smart home appliances, internet, Python, Database,

			operation cost of large data centre, poor flexibility in anti-attack, difficulty in establishing trust in energy Internet users, user privacy leakage and inapplicability of trading market mode. A kind of architecture of P2P light-heavy backup is put forward to overcome the high cost of Blockchain data storage.	areas of government, health, science, culture and the arts, and builds a decentralized and cooperative society. Blockchain is an integrated technology, which includes Hash, asymmetric encryption, workload proof, Merkel tree, timestamp, P2P and other technologies. It also presents a solution to the problem of increasing storage pressure in the late blockchain. The solution proposed a P2P light - heavy backup architecture, hoping to be able to provide practical help for the future.	
Afreen Fatima Mohammed	Security Issues in IoT	2018	This paper discusses about various vulnerabilities and threats against IoT and what actions could be taken to provide a more secure IoT. As more and more IoT devices are coming in the market, securing IoT systems represents a number of challenges. The connectivity then helps to capture more data from more places, ensuring more ways of increasing efficiency and improving safety and IoT security. Data privacy, confidentiality data integrity is at potential risk when these devices are connected.	In the near future Internet of Things will be an essential element of our daily lives. Numerous energy constrained devices and sensors will continuously be communicating with each other the security of which must not be compromised. Cryptographic algorithms can be applied. Choose an appropriate cryptographic algorithm which is best suitable to be adopted in IoT applications Various iot threats like ddos and malware attacks are occurred so in order to overcome them various techniques are being used like Change your default passwords and usernames, Update to the latest software, create a second network for IoT devices, Download security applications	SHA-256, cloud, wi-fi, Smart Devices.
Chao Qu, Ming Tao, Jie Zhang, Xiaoyu Hong, Ruifen Yuan	Blockchain Based Credibility Verification Method for IoT Entities	2018	In this paper, to establish the relationship between IoT and BC for device credibility verification, we propose a framework with layers, intersect, and self-organization Blockchain Structures (BCS). In this new framework, each BCS is organized by Blockchain technology. We describe the credibility verification method and show how it provide the verification. The efficiency and security analysis are also given in this paper, including its response time, storage efficiency, and verification. The conducted experiments have been shown to demonstrate the validity of the proposed method in satisfying the credible requirement achieved by Blockchain technology and certain advantages in storage space and response time.	In this paper, we have presented an IoT device credibility verification method based on Blockchain technology and discussed it in detail. The validity of the proposed model and method can reach the credible requirement by Blockchain technology and also has certain advantages in regard to storage space and response time. Although the proposed method has some advantages, there are still some problems to be resolved. For example, an attack on the MS cannot verify the credibility of all the nodes under it, which does not achieve complete decentralization. The 51% of the computation problem is still not effectively addressed and still threatens the entire network under such an attack. In addition, for a large scale IoT environment, determining how to choose the number of BCS nodes and how to control the height of the tree is still a problem requiring further study.	The smart devices and sensors in the IoT, Wi-Fi

VI. METHODOLOGY

We have limited our systematic review to the field of IoT security where trust is established through the immutable and decentralized nature of blockchain. As we know that the distributed nature of blockchain makes the system more robust and immune to single point of failure [10].

Data Sources:

The systematic review included the following electronic databases:

- Google Scholar
- IEEE explorer
- Springer Link
- Elsevier ScienceDirect

Selection of Studies: The selection process started with various publications gathered from online digital libraries and based on that criteria's, the publications were either included in the systematic review or not. The selection process was divided into four phases:

Phase 1: The search results were filtered according to the various criteria. We included studies from the years 20016 to 2018.Since we are working on blockchain so knowing about the latest trend will be very beneficial and as we know that 2008 was the of the introduction of Bitcoin and it is known as the first published application of the blockchain technology.

Phase 2: We have searched and accessed various research questions by going thoroughly by the title and abstract. We excluded 40 results.

Phase 3: The duplicates from 12 different databases were removed. 28 publications were left for the next phase.

Phase 4: The remaining results were read in more detail by reading thoroughly through it. The remaining results also had to include a novel and sufficient contribution to the field of various applications by the means of a blockchain. Many results were blacklisted as the introduced idea was very general and no further details on its design or implementation were given. In the end we were left with only 15 papers that were most suitable for our study.

Data Gathering:

We were interested for which purpose or field a blockchain included in IoT security. As blockchain technology can be used for multiple purposes. We found that a blockchain is usually used in the following fields: data sharing, access control, health care, smart Contracts and food industries. From the contents of the publications, we identified a blockchain platform like Ethereum, Hyperledger Fabric etc., a consensus algorithm (e.g., PoW, PoS, etc.), and a blockchain type. Finally, we identified if the proposed solutions incorporated smart contracts.

Tools Required

OS: Windows 10

Editor: Visual Studio Code

Package to be installed in editor:

```
npm i sha256 --save, npm i solidity --save, npm i express --save, npm i nodemon --save
```

Other Tools which can be used to create a blockchain are:

- Eris
- Mist
- Coinbase's API
- Tierion
- Embark
- Ether Scripter

CONCLUSION

Sharing IoT devices introduces new opportunities for innovation but at the same time, it ensures private access to the resources being shared. In order to avoid and not depending on the third party supervising the private access to the resource [12]. We will be proposing the alternative solution of using blockchain technology. We have here discussed more about what are the techniques and methodology used. We are planning to implement working applications on blockchain for our further research paper and to explore more security issues and how to overcome them. Future work will focus on implementing Blockchain technology for use where we will be creating a blockchain and making it more secure by using Proof of Work algorithm and then we will be building an API which will allow the user to interact with our Blockchain with our API [8]. Once our API is built, we will be making it as a decentralized network because the API which we build is very centralized which is not good because this API is totally control of our Blockchain, therefore making it decentralized would be the best option. So, to build this decentralized Blockchain network we are going to take our API and make many different instances of it and each instances of our API is going to be a network node in our Blockchain network.

REFRENCES

[1] Himanshu Gupta, Garima Varshney ‘A security framework for IoT devices against wireless threats’, 2017 2nd International Conference on Telecommunication and Networks (TEL-NET 2017) https://www.techbullion.com/blockchain-definition-origin-history/

[2] Parul Datta, Bhisham Sharma ‘A survey on IoT architectures, protocols, security and smart city-based applications’,2017International Journal of Computer Applications (0975 – 8887) Volume 180 – No.3, December 2017 https://ieeexplore.ieee.org/document/8203943/

[3] Supriya Thakur Aras, Vrushali Kulkarni, ‘Blockchain and Its Applications – A Detailed Survey’, 2017 13th International Computer Engineering Conference (ICENCO) https://ieeexplore.ieee.org/document/8289760/

[4] Petar Radanliev, Dave De Roure, Stacy Cannady, Rafael MantillaMontalvo, Razvan Nicolescu, Michael Huth, ‘Economic Impact ofIoT Cyber Risk - Analyzing past and present to predict the futuredevelopments in IoT risk analysis and IoT cyber insurance’, Living in the Internet of Things: Cybersecurity of the IoT – 2018 https://ieeexplore.ieee.org/document/8379690/

[5] Mario frustaci, Pasquale pace, Gianluca aloi, Giancarlo Fortino dimes, ‘Evaluating critical security issues of the IoT world: Present

and Future Challenges', IEEE Internet of Things Journal (Volume: 5, Issue: 4, Aug. 2018)
https://ieeexplore.ieee.org/document/8086136/

[6] S. Sridhar, 'Intelligent Security Framework for IoT Devices Cryptography based End -To- End security Architecture',2017 International Conference on Inventive Systems and Control (ICISC)
https://ieeexplore.ieee.org/document/8068718/

[7] Thomas MAURIN, Laurent-Frédéric DUCREUX, George CARAIMAN, Philippe SISSOKO, 'IoT Security Assessment through the Interfaces P-SCAN Test Bench Platform',2018 Design, Automation & Test in Europe Conference & Exhibition (DATE)
https://ieeexplore.ieee.org/document/8342159/

[8] K Poyner, R S Sherratt, 'Privacy and security of consumer IoT devices for the pervasive monitoring of vulnerable people', Living in the Internet of Things: Cybersecurity of the IoT - https://ieeexplore.ieee.org/document/8379730/

[9] J M Blythe, S D Johnson, 'The consumer security index for IoT: A protocol for developing an index to improve consumer decision making and to incentivize greater security provision in IoT devices', Living in the Internet of Things: Cybersecurity of the IoT - 2018 https://ieeexplore.ieee.org/document/8379691/

[10] Irina Brass, Leonie Tanczer, Madeline Carr, Miles Elsden & Jason Blackstock, 'Standardising a Moving Target: The Development and Evolution of IoT Security Standards', Living in the Internet of Things: Cybersecurity of the IoT – 2018
https://ieeexplore.ieee.org/document/8379711/

[11] Aqeel-ur-Rehman1, Sadiq Ur Rehman2, Iqbal Uddin Khan, Muzaffar Moiz and Sarmad Hasan, 'Security and Privacy Issues in IoT', International Journal of Communication Networks and Information Security (IJCNIS)
http://ijcnis.org/index.php/ijcnis/article/view/2074

[12] Afreen Fatima Mohammed, 'Security Issues in IoT', 2017 IJSRSET | Volume 3 | Issue 8 | Print ISSN: 2395-1990 | Online ISSN: 2394-4099
http://ijsrset.com/paper/3369.pdf

[13] Iuon-Chang Lin and Tzu-Chun Liao, 'A Survey of Blockchain Security Issues and Challenges', International Journal of Network Security, Vol.19, No.5, PP.653-659, Sept. 2017 (DOI: 10.6633/IJNS.201709.19(5).01)
https://pdfs.semanticscholar.org/f61e/db500c023c4c4ef665bd7ed2423170773340.pdf

[14] Yoad Lewenberg, Yonatan Sompolinsky, Aviv Zohar, 'Inclusive Block Chain Protocols', International Conference on Financial Cryptography and Data Security
https://link.springer.com/chapter/10.1007/978-3-662-47854-7_33

[15] Ruiguo yu1, Jian Rong wang1, Tianyi xu1, Jie gao1, yongli a gong zhang1, and mei yu1, 'Authentication with Block-Chain Algorithm and Text Encryption Protocol in Calculation of Social Network', IEEE Access (Volume: 5)
https://ieeexplore.ieee.org/document/8100712

[16] Chih-Wen Hsueh, Chi-Ting Chin, 'EPoW: Solving Blockchain Problems Economically', 2017 IEEE Smart World, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (Smart World/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)
https://ieeexplore.ieee.org/document/8397612

[17] Yuang Chen, Thomas Kunz, 'Performance evaluation of IoT protocols under a constrained wireless access network', 2016 International Conference on Selected Topics in Mobile & Wireless Networking (MoWNeT)
https://ieeexplore.ieee.org/abstract/document/7496622

[18] Ye Guo, Chen Liang, 'A Critical Review of Blockchain and Its Current Applications', International Conference on Electrical Engineering and Computer Science (ICECOS) 2017
https://link.springer.com/article/10.1186/s40854-016-0034-9

[19] Ahmet EKİN, Devrim Ünay, 'Blockchain applications in healthcare',2018 26th Signal Processing and Communications Applications Conference (SIU)
https://ieeexplore.ieee.org/document/8404275

[20] Shuling Li, 'Application of Blockchain Technology in Smart City Infrastructure',2018 IEEE International Conference on Smart Internet of Things (SmartIoT)
https://ieeexplore.ieee.org/document/8465562

[21] Pinyaphat Tasatanattakool, Chian Techapanupreeda 'Blockchain: Challenges and applications', 2018 International Conference on Information Networking (ICOIN)
https://ieeexplore.ieee.org/document/8343163

[22] Nir Kshetri, 'Can Blockchain Strengthen the Internet of Things?', IT Professional (Volume: 19, Issue: 4, 2017) https://ieeexplore.ieee.org/document/8012302

[23] Arman Pouraghily, Md Nazmul Islam, Sandip Kundu, Tilman Wolf, 'Poster Abstract: Privacy in Blockchain-Enabled IoT Devices',2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoT)
https://ieeexplore.ieee.org/document/8367006

[24] Mayra Samaniego, Ralph Deters, 'Blockchain as a Service for IoT',2016 IEEE International Conference on Internet of Things (things) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)
https://ieeexplore.ieee.org/document/7917130

[25] Dennis Miller, 'Blockchain and the Internet of Things in the Industrial Sector', IT Professional (Volume: 20, Issue: 3, May. /Jun. 2018)
https://ieeexplore.ieee.org/document/8378971

[26] YouTube
Proof of Work
https://www.youtube.com/watch?v=HneatE69814
Proof of stake
https://www.youtube.com/watch?v=EWfGzeF3Xmw