Secure IoT via Blockchain

Secure IoT via Blockchain

Ms. Ruchi Garg[1], Ms. Poonam Gupta[2] and Dr. Amandeep Kaur[3]

[1]Assistant Professor, Electronics and Communication Engineering Department, M.M.(Deemed to be University), Mullana, Ambala, Haryana, India.
garg.330@gmail.com

[2]Assistant Professor, Computer Science and Engineering Department, M.M.(Deemed to be University), Mullana, Ambala, Haryana, India.
guptapoonam2311@gmail.com

[3]Associate Professor, Computer Science and Engineering Department, M.M. University, Sadopur, Ambala, Haryana. India
amandeepkaur@mmumullana.org

Email: amandeepkaur@mmumullana.org

Abstract. Block chain technology had gained popularity because of its use in crypto-currencies like bitcoin. Today uses of blockchain are growing in number of areas like banking, industries, health centers and even security of IOT. Moreover, the use of IOT is growing exponentially every year with its aim in 5G technologies like e- health, smart homes, distributed intelligence etc. but it faces challenges in security and privacy. The privacy of a user data is at a risk because of its (i.e. IoT) centralized client-server model. This centralized approach of the server poses a serious vulnerability to the data security. This data at the server attracts the attackers to enter into the network and invade through the data and schedule attacks or inject a malware. It indicates that the central architecture of IoT possess a compromised confidentiality, integrity, and security of data which disrupts its use as the widespread adoption of this technology. Therefore, it is essential to evade the hostile centralized server architecture for IoT to enhance its security. It implies a need for decentralized architecture to maintain the data. The data can be kept at the different users without any central control with the help of blocks as suggested by Blockchain. This paper addresses the various security issues in IOT and how block chain helps in solving these issues.

Keywords: Internet of Things (IoT), Security Issues in IoT, Security, Privacy, Blockchain

1. Introduction

As the wireless communication technologies, networks and circuit integration are gaining maturity; many researchers as well as many countries put their attentiveness towards the IoT. The key infrastructure behind this technology is Internet that consists of many IoT devices and data. But the devices connected as IoT nodes are heterogeneous in nature **[1]**. These different types of devices can be structured, semi-structured or unstructured and they employ different interconnecting technologies like RFID (Radio Frequency Identification) and WSAN (Wireless Sensor and Actor-Network) etc. to

interchange information. These physical and smart IoT devices are controlled remotely and can communicate directly without human intervention. They have the capability of not only monitor their environment, but they can also execute shared tasks with coordination with each other. IoT plays a very important role in society as it changes life into smarter life by increasing the intelligence level of a society. Even though it seems to become a future technology where different devices or machines can communicate or interact with each other but there exists lot of challenges in the present architecture of IoT network that needs to be addressed. The present architecture is based on centralized client-server model. There is no doubt that information transmission leads to the development of society but with the development in IoT, it cannot be denied that it is difficult to handle heavy network traffic, expensive devices and human labour costs by centralized networks. Hence the centralized feature of IoT is one of the major issues to treat. This centralized approach of the server poses a serious vulnerability to the data security. This data at the server attracts the attackers to enter into the network and invade through the data and schedule attacks or inject a malware. Moreover, this centralization results in the increased cost in maintaining the large centralized data centres and there is also a single point of failure in centralized architecture **[2]**.

To overcome the security drawbacks due to centralized data in IoT, there is a need to maintain data at various levels. This decentralization of data looks towards maintenance of the data at users' level but in a secured manner only. Here cryptography is an already well-known technique is available to serve the purpose. The crypt solution at different users' levels is similar to the concept of crypt currency. There are various crypt currency solutions like bit coin, Litecoin etc. are successfully existing. The technology which emerges from this crypt currency is familiar as Blockchain **[3]**.

In recent years blockchain has originated as a technology with many features that helps in clearing path for the future of IoT. Blockchain is a distributed database that enables the transactions to occur and these transactions are shared among the communicating parties in the network **[4]**. All the finished transactions are recorded in a list of blocks. This chain of blocks grows continuously with new blocks when they are added. Therefore, it is also referred to as the distributed ledger or public ledger. As it uses decentralized approach, it allows a copy of every transaction to remain with every communicating party without the intervention of any trusted third party. So, it solves the issue of single point of failure that exists in the centralized architecture of IoT. This further reduces the development cost and server cost. It acts as a security mechanism against intruders. Also, the immutable nature of Blockchain maintains the integrity of the data because once the record has been declared valid, the transactions cannot be changed. No doubt, Blockchain was initially designed for crypto-currencies transactions with a merit of decentralized digital phase, which invites the integration of blockchain with IoT **[5]**. This integration of IoT with Blockchain can be highlighted with the assistance of the following advantages as shown in **Figure1**.

In recent years blockchain has originated as a technology with many features that helps in clearing path for the future of IoT. Blockchain is a distributed database that enables the transactions to occur and these transactions are shared among the communicating parties in the network [4]. All the finished transactions are recorded in a list of blocks. This chain of blocks grows continuously with new blocks when they are added. Therefore, it is also referred to as the distributed ledger or public ledger. As it uses decentralized approach, it allows a copy of every transaction to remain with every communicating party without the intervention of any trusted third party. So, it solves the issue of single point of failure that exists in the centralized architecture of IoT. This further reduces the development cost and server cost. It acts as a security mechanism against intruders. Also, the immutable nature of Blockchain maintains the integrity of the data because once the record has been declared valid, the transactions cannot be changed. No doubt, Blockchain was initially designed for crypto-currencies transactions with a merit of decentralized digital phase, which invites the integration of blockchain with IoT [5]. This integration of IoT with Blockchain can be highlighted with the assistance of the following advantages as shown in Figure1.

- Decentralization: Traditionally, transactions are authenticated through a central trusted third party. This centralization results in the increased cost to keep alive the large centralized data centers. Further, the centralized architecture establishes a single point of failure also. But decentralization in blockchain permits a copy of every transaction to remain with every communicating party without the involvement of any third party. So, it resolves the issue of single point of failure that exists in the centralized architecture. This further decreases the development cost due to the centralized server, which acts as a security tool against intruders [5].

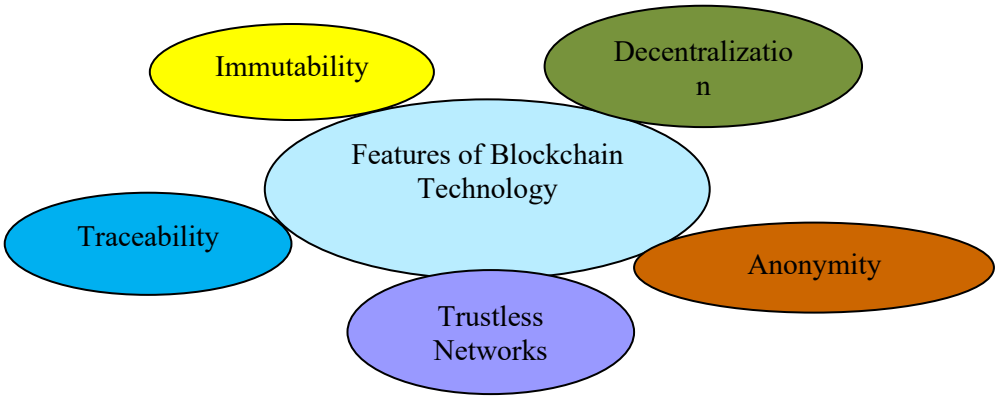

Figure1. Advantages of Blockchain Technology

- Anonymity: Blockchain is capable of hiding the characteristics of the users. It keeps the identities of the user's private as there is no central party that requires the identities of the users [5].
- Immutability: All the transactions in Blockchain are stored in a distributed network, so it is quite difficult to alter the transactions. As every block is a cryptographic hash of the previous block. More and more blocks are added to the chain then going back to modify some data within the previous block required the re-computation of the hash of that block as well all the blocks after it. This leads to the high financial cost also. In this way it assures the integrity of the data [6].
- Trustworthy Networks: Blockchain has eliminated the concept of trusted third party. No two users need to get verified from the middle party. Any user on the blockchain can verify the identity of any other party thus there is no need of authentication from third party. So, this brings a faster and secure means of transactions [7].
- Traceability: The transactions in the blockchains are saved with the timestamp i.e. a sequence number that shows when that particular transaction occurs. So that each user can verify the historical data related to any transaction with the help of these timestamps [8].

On the other hand, some other features of blockchain are little suitable for IoT applications. The first and the major problem are Processing Power and time required to perform encryption algorithms for all the objects involved in Blockchain-based IoT system. This is due to the diverse nature of IoT systems as it consists of devices that are heterogeneous and have different computing capabilities, and not all of them are capable of running the same encryption algorithms at the desired speed. The second hurdle is the storage capacity. Blockchain removes the need for a central server to store transactions and device IDs, but the ledger has to be stored on the nodes themselves, and the ledger is bound to increase its size as time passes. That is outside the capabilities of a wide range of smart devices such as sensors, which have very low storage capacity. The third factor is scalability issue relating to the size of Blockchain ledger

that might lead to centralization as it's grown over time and required some record management which is casting a shadow over the future of the Blockchain technology [9].

But the decentralized nature and the security features overwhelm its (i.e. Blockchain) weaknesses and it can still be considered as a hopeful solution for IoT. Therefore, IoT system makes communication possible between various nodes without any central system with the help of blockchain [10]. Hence it arises a need to analyze the security issues of IoT so that these can be discussed to plug with Blockchain.

2. Security Evaluation of IoT system

Since IoT connects the internet to the physical world, it leads to some new privacy and security problems. Some of them are due to internal architecture of IoT and its variance to earlier networks, while others are because of using internet. **Figure 2** shows the various points from which the various intruders come to attack IoT systems. Therefore, at this stage, protection implies to examine the security problems by considering the information flows and the main points of control.

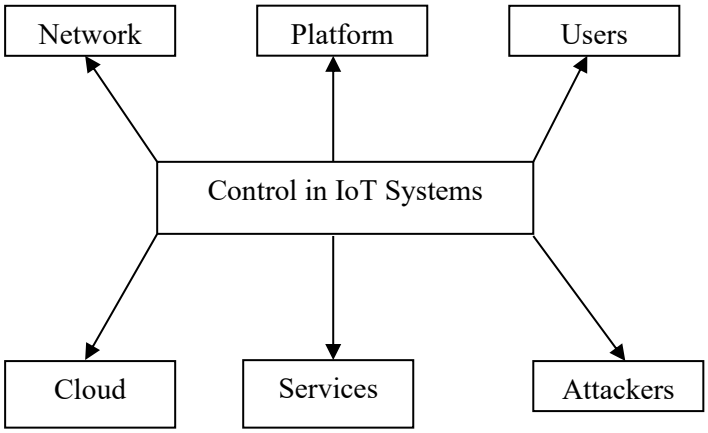

Figure 2. Main Points of Control in IoT Systems

The foundation of any IoT system lies on network, cloud, platform and services along with its users and attackers or intruders as shown in Figure2.

- **Network-**IoT network is modified form of conventional network as the devices connected can be of different hardware performances (e.g. CPU computation, platforms, policies etc.) which leads to weakens inter-operability and increased cost to understand each other. Also, framing security related framework for these systems are very complicated. But as the infrastructure of both the networks i.e. IoT and conventional networks is almost same, hence the nature of problems must be same in both **[11]**.
- **Cloud -** IoT devices use cloud as a centralized server to save the data as the memory capacity of IoT devices is very low. In some applications the data is very sensitive and if at any instance the centralized server does not work then there is a difficulty in saving the data which may cause to halt those applications. As a result, IoT is highly dependent on cloud and the devices must have back up servers to be swapped with original cloud **[12]**.
- **Users-** User is an important as well as the most vulnerable element of the IoT system as he/she has to manage the system and has to take decisions regarding all important aspects related to communication. The casual behavior of user/ system engineer leads to failure of any well implemented security system. For example, if in any application, password-based authentication is used, and the careless user makes the guessable passwords then it can be easily cracked with the common security attacks by the invader. Therefore, the user should

be intelligent enough in knowing all the common attacks and should be able to follow the security policies strictly. Moreover, the user should have knowledge about social engineering also **[13]**.

- **Attacker -**Since IoT devices are connected through internet, therefore these devices can be accessed and hence attacked at any time. Also, the security services in these are designed considering the constraints on the resources used. Moreover, services provided by IoT, at present, are not fully authenticated. As a result, IoT systems are very much vulnerable to attacks. The threats that attack on network comes under nonphysical and all other attacks can be considered as physical. As the environment around IoT devices is not secure, any malicious user could attack it easily and can gain the access of vulnerabilities of the system. The attacks which affects the CIA triads of the network like spoofing, buffer overflow etc. are treated as nonphysical threats and it is very difficult to prevent these attacks as the devices in IoT system are heterogeneous. Moreover, as discussed earlier strong security policies cannot be implemented due to resources constraints. Hence IoT devices are very much susceptible to attacks. So, using these vulnerabilities an attacker can easily attack these systems and these, should be minimized by any method **[14]**.

3. Effective of Blockchain in IoT

IoT is able to draw a network of versatile assets to share their resources only without any dimension to consider the network security. Therefore, IoT presents a network with lot of open-ended links, which are vulnerable. Some common vulnerable points which must be plugged are listed as-

i). Inherent privacy and security threats of using the existing WSN technology.
ii). Distributed attack due to unsecure scalability.
iii). IoT depends upon cloud environment which adds single-point-of-failure due to centralized architecture.
iv). No measure for data authentication.

These vulnerabilities make IoT an unreliable platform for secure transactions. Therefore, a welcome solution to IoT must add a sense of security by performing some basic functions to the transactions, like- non-repudiation, integrity, and confidentiality **[15]**.

Hence IoT is looking for its missing link to reliability and privacy. This missing link can be established with the help of autonomous, trust-worthy, and decentralized competences of Blockchain. Therefore, Blockchain may meet out the security challenges of IoT effectively. The effectiveness to deal with the challenges is performed individually on each layer of IoT architecture below in Figure 3 **[15]**.

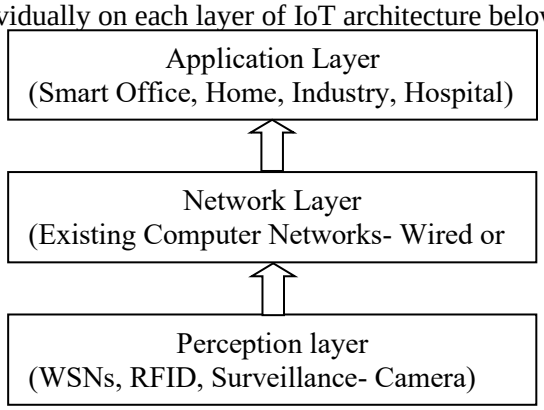

Figure 3. Layered Architecture of IoT

- **Application Layer:** This layer is the most sensitive layer for the implementation in terms of the security. The whole network may be compromised due to various attacks at this layer, like- malicious code injection, sniffing attack, cross site scripting, phishing, denial of service attack

etc. These attacks can be answered with the help of some security measures, like- data security, risk assessment, authentication, intrusion detection etc. At this layer, therefore the decentralized architecture of Blockchain accomplishes IoT by using cryptography for data security with the login authentication modules. Every transaction is validated by all the network users to assess the risk of any kind of malicious act [16]. The intrusion is curbed due to the decentralized ledgers for the transactions in terms of blocks. The significance of security aspects of blockchain for IoT at application level can be enlightened with the assistance of Figure 4.

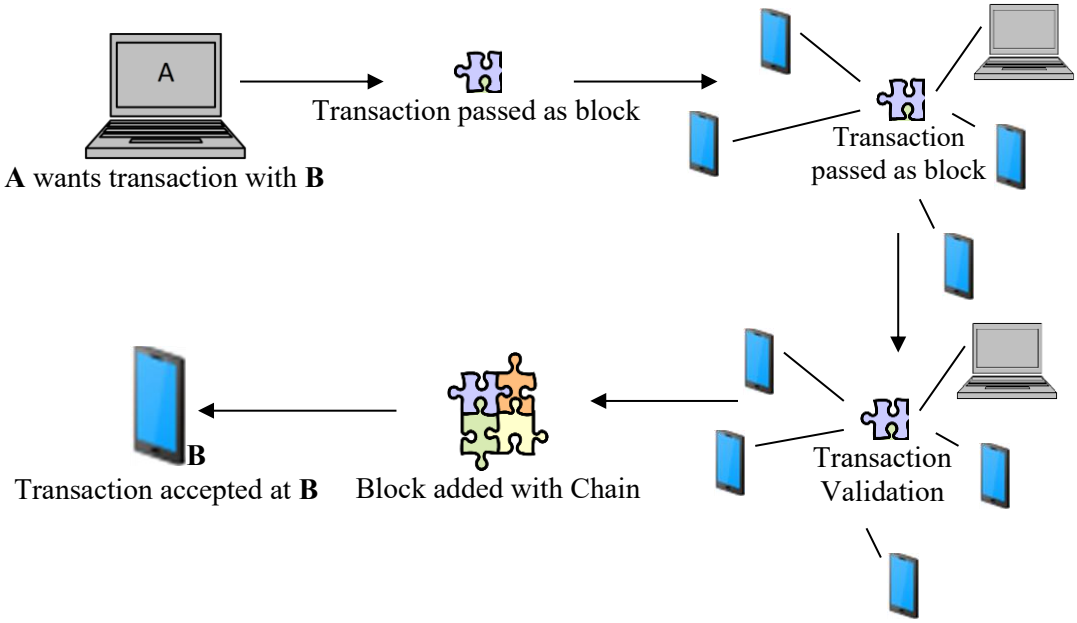

Figure 4: Implementation of transaction in Blockchain.

- **Network Layer:** This layer is responsible to connect various smart devices with each other through any existing network among them. This layer lacks to ensure data integrity and authentication that is being transported from perception layer to it. Therefore, IoT is prone to bear storage attack, man-in-middle attack, and denial-of-service attack etc.
  These attacks can defy with Blockchain. Since blockchain authenticate a user before gaining access to the network resources therefore storage devices or cloud may be protected from the attackers to go for storage attack. The possibility of unauthorized access to the network is plugged by Blockchain which hinders intruding evader to act as man-in-middle attack **[17]**. Hence Blockchain ensures that both the receiver and the sender is able to exchange unaltered data with due privacy. Similarly, denial-of-service is corked because of the blockchain security access policy which never allows an authenticated user to flood the resources with malicious access calls.

- **Perception Layer:** Attackers act on this layer either by replacing the existing or putting new smart devices here. By placing some outside sensors or smart devices, invaders try to gain access of IoT resources and perform some attacks like- timing attack, replay attack, energy-burn out, eavesdropping, node capturing etc. These attacks are caused just because of no security element of IoT. The timing attack performed by decoding the timing need of a node to perform specific action. Here, an attacker observes the timing needs of the nodes carefully and approximate the possible vulnerabilities of the implemented methods at the computational week nodes. In the other form that is replay attack, the attacker captures the authentication information of a sender and act as a legitimate node in the network. This further allows the attacker to add fake nodes to the network and may cause energy burn out stage for others by indulging them in some

spurious transactions. Thereby, the attacker is able to capture the rightful nodes and interfere in the ongoing communication between a receiver and sender to act as an eavesdropper **[18]**.

All these attacks highlight the vulnerabilities of IoT at perception layer, whereas Blockchain can act as a security module for IoT to plug these vulnerabilities. The Blockchain secures IoT by proposing distributed validation process of a transaction. In Blockchain, any node can leave or join the network at any moment but without its validation it can't go for network resources as shown by **Figure 4**.

4. Fault Analysis of Blockchain

Though fundamental application of Blockchain has various key points to prove its strength to IoT, still its implementation causes some concerns to IoT also. The application of consensus method to perform a transaction is shown in **Figure 4**, which causes some faults to IoT also, as explained following:

- **Proof-of-Work:** Every new block generated by a potential miner has to perform a computationally intensive algorithm to gain the access of the network by a fair competition. Now if the algorithm to perform at the potential miner is less complex then it compromises the network security and vice-versa. At this point the weak computational capability of IoT nodes with less- memory and poor power backup aggravate it so much so that the node acting as a potential miner may die before its actual useful life **[19]**.
- **Proof-of-Stake:** All the participating nodes in Blockchain have a capability to validate a new block. This validation is a weighted validation process in proportion to the coins; a node has at any point of time. Therefore proof-of-stake presents a biased network, where a mighty miner can dictate all other participants. It goes against the flexible and impartial scalability of any network may be IoT **[20][21]**.
- **Proof-of-Authority:** The blockchain authorize some of the participating nodes to validate every new block in the network. Therefore, a closed network is required to form where some nodes can be identified as validation nodes. Thus proof-of-authority advocates small network with limited number of nodes where all the nodes must be well known to each other before joining the network. Again proof-of-authority goes against the "no central authority" of IoT architecture **[22]**.
- **Proof-of-Elapsed Time:** The Blockchain network allows all the participating nodes to wait for random period of time and the first one to complete its waiting time captures the opportunity to generate a new block. This elapsed time is bound to add delay in the network throughput. Some hard-real time applications of IoT like- disaster management, military operations, industrial surveillance etc. has a marginal scope for such delay **[23][24]**.
- **Multi-Signature Authentication:** To enhance the security of the Blockchain operations, each transaction is authorized by multiple users of the network. It is a security overhead for battery ridden, tiny size, less computational and with poor storage capacity sensors in IoT **[25]**.

5. Conclusion and Future Scope

Blockchain has various features which go well with IoT, but the integration of these two technologies together is not so easy. Lot of things are to be considered during this implementation. This paper discussed some of the issues of IoT systems and how Blockchain helps in solving these issues. Lot of other issues is also need to be addressed. Since there are lot of other issues that still have to be considered, so at this stage it cannot be concluded that Blockchain best suits IoT, but if the above issues and the effectiveness of Blockchain will be considered, then in future integrating these two will definitely help. Also, there are some challenging areas for Blockchain also. With the elimination of those challenges and the assistance of the advanced technology in other fields, a trustworthy, well-organized, and scalable IoT blockchain will overshadow the IT industry soon.

References

[1] L.Atzori, A. Iera and G. Morabito, 2010, 'The internet of Things: a survey', Computer Networks 54 pp 2787-2805
[2] M.A. Khan and K. Salah, 2018, 'IoT security: Review, blockchain solutions, and open challenges', Future Generation Computer Systems 82 pp 395-411
[3] Melanie Swan, 2015 'Blockchain Blue Print for a new economy' O'Reilly Media, USA.
[4] K. Christidis and M. Devetsikiotis, 2016, 'Blockchains and smart contracts for Internet of Things', IEEE Access, Volume 4, pp 2292-2303
[5] Z.Zheng, S. Xie, H. Dai, X. Chen and H. Wang, 2017 'An overview of blockchain technology: Architecture, consensus, and future trends', IEEE 6thInternational Congress on Big Data, pp 557-564
[6] X.Liang, J. Zhao, S. Shetty and D. Li, 2017, 'Towards data assurance and resilience in IoT using blockchain , IEEE Military Communications Conference (MILCOM) paper
[7] Yu Zhang and Jiangtao Wen, 2015 'An IoT electric business model based on the protocol of bitcoin', ICIN, IEEE 18th International Conference on Intelligence in Next Generation Networks, pp 184-191
[8] T. Chollet , J. Castiaux, M. Bruneton and L. Sainlez, 2017 'Continuous interconnected supply chain using blockchain and internet of things supply chain traceability', deloitte blockchain
[9] Sonali Chandel, Song Zhang, and Hanwen Wu, 2020, 'Using Blockchain in IoT: Is it a Smooth Road Ahead for real? ', Advances in Information and Communication, pp 159-171
[10] Ben Dickson, 2016, 'The benefits and challenges of using blockchain in IoT development', BD Techtalks
[11] Xiruo Liu, Meiyuan Zhao, Sugang Li, Feixiong Zhang and Wade Trappe, 2017 'A Security framework for the Internet of Things in the Future Internet Architecture', Future Internet
[12] JunZhou, Zhenfu Cao, Xiaolei Dong and Athanasios Vasilakos, 2017, 'Security and Privacy for Cloud-Based IoT: Challenges', IEEE Communications Magazine Volume 55, Issue1 pp 26-33
[13] Lohana Santos Medeiros, Fabio Zuvanov, Flavio Luis de Mello and Edilberto Strauss, 2018 'IoT Information Security Evaluation for Developers and Users', Journal of Information Security and Cryptography(Enigma), Volume 4 No.4
[14] Ismail Butun, Patrik Osterberg and Houbing Song, 2020 'Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures', IEEE Communications Surveys & Tutorials 22(1), pp 616-644
[15] K. Zhao and L. Ge. 'A survey on the Internet of Things security',2013, International Conference on Computational Intelligence and security (CIS) pp 663-667
[16] R. Vignesh and A. Samydurai, 2017, 'Security on Internet of Things (IoT) with Challenges and Countermeasures', International Journal of Engineering Development and ResearchVolume 5, Issue 1, pp 417-423
[17] M. Leo, F. Battisti, M. Carli and A. Neri, 2014 'A federated architecture approach for Internet of Things security', Euro Med Telco Conference (EMTC) 1-5
[18] L. Atzori, A. Iera, G. Morabito and M. Nitti, 2012, 'The Social Internet of Things (SIoT) - when social network meet the internet of things: Concept, architecture and network characterization', Computer Networks Volume 56, Issue 16, pp 3594-3608
[19] A. Baliga. 'Understanding Blockchain consensus models', 2017, Persistent 4:1-14
[20] A. Poelstra. 'Distributed consensus from proof of stake is impossible', 2015, Blockstream, Austrin, TX, USA, Self-Published Paper.
[21] A. Kiayias, A. Russell, B. David and R. Oliynykov, 2017, 'Ouroboros: A Provably secure proof-of-stake blockchain protocol', CRYPTO 2017: 37th Annual International Cryptology Conference Santa Barbara, CA, USA: Springer, pp 357-388
[22] Toqeer Ali Syed, Ali Alzahrani, Salman Jan, Muhammad Shoaib Siddiqui, Adnan Nadeem and Turki Alghamdi, 2019, 'A comparative Analysis of Blockchain Architecture and its

Applications: Problems and Recommendations', IEEE Access Volume 7, pp 176838-176869
[23] L. Chen, L. Xu, N. Shah, Z. Gao, Y. Lu, and W. Shi, 2017, 'On security analysis of proof-of-elapsed-time (poet)', International Symposiumon Stabilization, Safety, and Secuity of Distributed Systems Lyon, France: Springer 282–297
[24] W. Wang et al., 2019, 'A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks', IEEE Access 7, pp 22328-22370
[25] Dipankar Dasgupta, John M. Shrein and Kishore Datta Gupta, 2019 'A survey of blockchain from security perspective', Journal of Banking and Financial Technology 3, pp 1-17