A Security Architecture for a Smart Home Ecosystem using Permissioned Blockchain

[1]George Gabriel Richard Roy, [2]S. Britto Ramesh Kumar

[1]Assistant Professor, [2]Assistant Professor
[1]Department of Information Technology, [2] Department of Computer Science
[1,2] St. Joseph's College, Tiruchirappalli, India

Abstract: Internet of Things (IoT) has come a long way of being as some jargon to an everyday household term where everyone seems to know something of it**.** This in a way is good where everyone gets to know about technology which would make life easier but there is also a risk or a threat of people or organizations who wish to create chaos and be menacing. These organizations or people are the main reason behind the data on networks which are subject to being attacked, eavesdropped, intercepted, malformed or stolen. Hence there is an ever present need to secure the data transmission and the integrity of the information present in the IoT networks from such threats. This paper proposes an Architecture to secure the devices as well as the transactions on an IoT Smart Ecosystem using Permissioned Blockchain technology to prevent data loss and to uphold confidentiality and integrity of the devices and the data transactions.

IndexTerms **– IoT, Blockchain, Permissioned, Smart Ecosystem, Security**

I. INTRODUCTION

The world as we know it has evolved into altogether a different one since the past century, gone are the times where the priority of communication was within person to person. The complexity of communication relied only on the language used and the behavior of the person whom it was to be communicated. Now as of recent times people have state of the art technology at their disposal to do the communication for them. The priority now has shifted from person to person towards machine to machine (m2m) and now its things to things (t2t). The evolution of networks has exponentially increased from just a simple Local Area Network to an "All" Area Network where every possible scenario could be transformed into a network. One such network is the Internet of Things (IoT). Gone are the days where the mention of IoT was an alienated word where people were astonished by the idea of it, now IoT has become a household term where people recognize it and many of them even have access to IoT devices.

The "things" in IoT stands for any living or non-living object which can be uniquely identified on the Internet, so data which is transferred to and from that thing could be easily identified that it is coming from that "thing". A thing could be a person, a plant, a table, a pen, a thermostat etc., just to name a few. So IoT can be summarized as a Network of Things that is able to communicated between each other and transmit information over the Internet for a specific purpose.

The application of IoT is vast in number, many present-day sectors can accommodate IoT in various degrees of complexity. These sectors are Industrial, Vehicular, Human, Homes, Medical, Environment etc. The data in IoT is gathered with the help of a variety of sensors which serves various purposes, if that sensor can process data, send and receive requests then it is said to be a smart sensor.

The IoT network is made up of sensors and actuators in a preliminary level which is responsible for sensing the surrounding and performing actions based on the sensed data. The next level is the addition of devices, these devices are called Smart Devices because it can connect to other devices in the network, share information and interact with users or other devices. The combination of these devices, sensors and actuators make up an IoT environment.

One of the most predominant IoT applications is the concept of a Smart Home (SH) where everyday household activities are automated with the help of sensors and smart devices. Smart Homes need to work in an environment that can send requests to other smart services outside of the home to be a wholesome Smart Environment. The SH will work more efficiently if they are in an ecosystem where every task will be automated with minimal to no intervention from humans. This ecosystem will contain the SH itself along with all the registered services pertaining to the SH. The services along with the SH can be addressed as a Smart Home Ecosystem (SHE).

The SHE is beneficial in many ways regarding to accessibility, ease of use and improved automated tasks, but it also invites a plethora of threats and has room for many vulnerabilities. As IoT is not a standard where only a certain set of protocols should work within a constrained environment, it works as a non-standardized invitee of many methodologies and protocols which can be made to work in unison with other protocols and methods, thus providing security to this network seems to be a daunting task.

This is where Blockchain comes to play. The word "Blockchain" rings falsely in the ears of the masses as it relating to only cryptocurrencies such as Bitcoin, Ethereum or the likes of it. As a matter of fact, Blockchain is the driving technology behind Bitcoin and much other cryptocurrencies. Simple put cryptocurrencies are just applications of The Blockchain Technology [10].

Blockchain is a Distributed Ledger Technology (DLT). IT is made up of many blocks which links to a previous block thus creating a chain of blocks thus the name Blockchain. Transactions on a Blockchain takes place between peers. These peers are decentralized. When a transaction takes place between A and B, a set of participating peers come to a consensus agreeing upon the validity of the transaction thereby committing the transaction on to a block on the validation of the transaction. The blocks are then stored locally on each of the participating peers in a ledger which is immutable. The blocks are stored with a write once, read many permissions, this makes the transactions secure on the Blockchain [9].

This paper proposes a convergence of the IoT Smart Home Ecosystem with Permissioned Blockchain technology to prevent the attacks and to secure transactions on the Eco System.

This paper is organized as I – Introduction, II – Literature Review, III – Proposed Architecture, IV – Conclusion and V – Future Direction.

II. Literature Review

A Smart Ecosystem relies on the infrastructure, applications, management of the devices and services and the stakeholders. Dario et al. presented an overview of how a Smart City Ecosystem could function on a city block. They have utilized low cost sensors and sensor powered devices to act as the base of their network. An open stack was used to facilitate as the middleware. They proceeded to explain about the infrastructure of the Ecosystem which was made up of various development boards along with sensors attached to them. The most important part of their study was the Stack4Things framework which acted as the middleware controlling and monitoring the devices and services. Security was provided through Stack4Things with AES algorithms for integrity and security of the devices. The focus of that article was to provide adequate quality services using the devices and Stack4Things but they did not focus much on the security aspect of the network [1].

Sujit et al. proposed a scalable framework to secure IoT transactions on a blockchain network using a local peer method. The focus of the paper was completely on increasing the transactions per second and increasing the storage requirements on the peer. With more focus towards the transaction rate and not towards individual device security [2].

IoT is a promising disruptive technology, presented Minhaj et al. in their paper which dealt with review of security issues in IoT and the emerging trends of how those security loops holes could be filled in. They did an extensive study on the issues and the possible solutions that could be optimal for the problems stated. They also studied the possibility of Blockchains being used as a measure for securing an IoT network. Although this was only a study and only a parametric analysis of the IoT attacks were proposed, thereby setting the stage for future directions to provide solutions based on their studies [3].

The most complex and dauting challenge faced by IoT implementations are the likes of cybersecurity challenges propose Kenneth et al. Where the devices, sensors, gateways and the network itself facing constant probes from multiple malicious sources on the internet, espionage, theft of data and even destruction of nodes. They mentioned that the attacks on IoT networks will continue to grow as the networks grow and these cyber attacks will be nerve ending where the networks are most vulnerable at, which would bring devastating blows on the financial and service of the country itself [5].

According to Dorri et al. IoT security and privacy are the major challenges when it comes to the distributed nature of the IoT nodes on the networks. They say that approaches based on Blockchain provides that security and privacy at the cost of momentous delay between transactions, heavy energy consumption and usage of resources. They have used Ethereum as the blockchain technology which is not very efficient and heavily relies on mining. The miners must work on a consensus based on Proof of Work where an always on device to handle all the communication within and outside the home. Their Smart Home system consisted of a cloud storage and overlay and the smart home itself. Results were shown by taking security, privacy and integrity into effect [6].

Kan et al. presents Blockchain as a new technology which is used for data sharing where there are lots of untrusted peers in the network. They propose that when there are huge transactions the existing systems are not optimal and they have high barriers. A component-based framework was introduced by them to exchange information across random but connected blockchains calling it an inter-blockchain communication. The focus of their paper was to facilitate routing management and message transfer. They have not included IoT neither spoke about securing the transactions of services [8].

IoT devices have progressed to accommodate many domains mentioned Seyoung et al. in their paper. They said that as in a normal network those IoT devices have the necessity to communicate and to be in sync with other devices as well. They have moved away from the traditional client server model, which was not adequate to house this network for its optimal performance so they used peer to peer networks. They have proposed that Blockchain would be a good candidate to build the network of IoT devices. Ethereum was used to configure and to control the devices. Public key infrastructure was used to authenticate the devices using RSA public key cryptosystems where the Blockchain will store the public keys and the private keys were stored in the devices itself. The choice of Ethereum even though fine-grained, is not stable and not scalable to accommodate massive number of devices. A proof of concept was made only with a limited number of devices [7].

III. Proposed Work

The proposed work progressed from a previous work on IoT which is present in **Fig 1.** This architecture dealt with how data and services on an IoT network could be controlled and monitored using user devices and other devices. This Architecture solely was based on the traditional Client and Server Model where every data which is processed and received was done through centralized servers.

The components of this architecture are End Users, LTE network, Processing Server, Low Powered Wide Area Network (LPWAN), IoT Readers, Wi-Fi Access Point and Sensors. This architecture follows the more traditional approach of client/server data lies on a central point of interest.

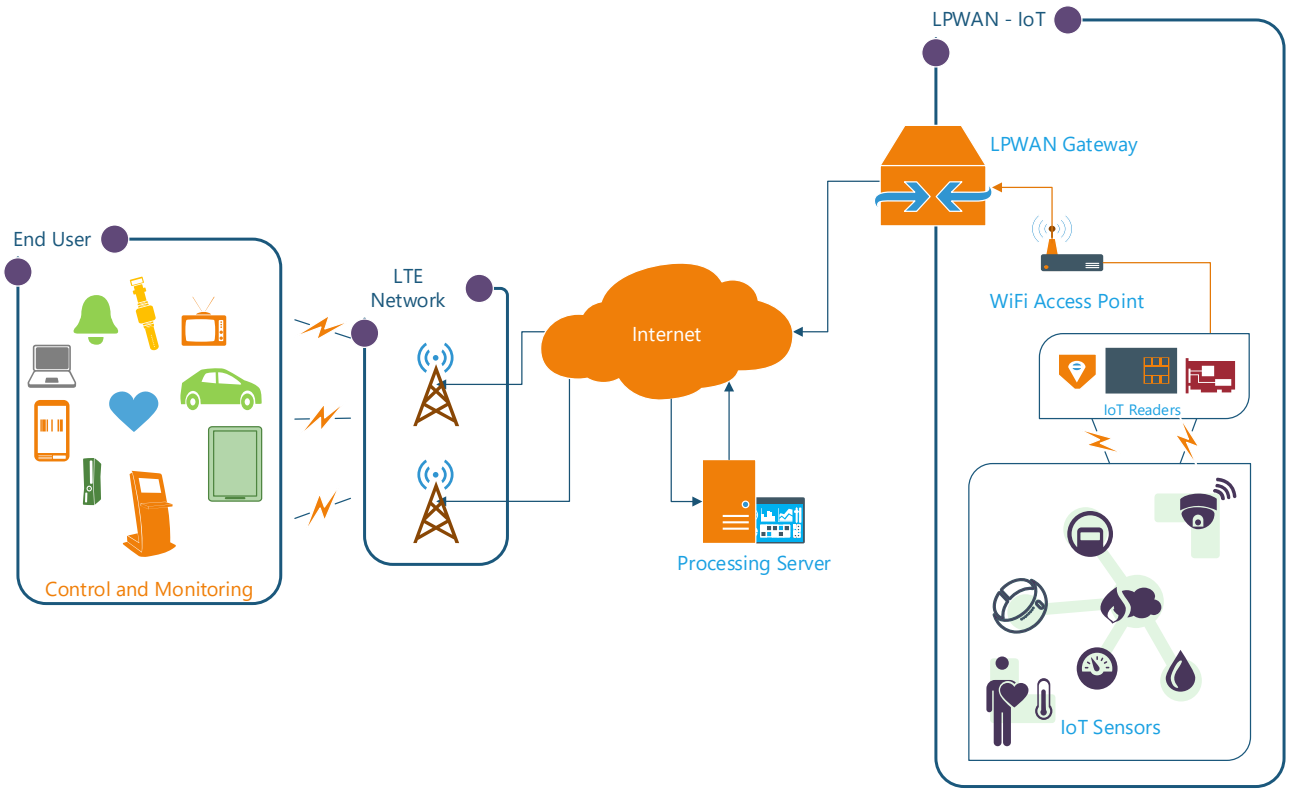

Figure 1. An Architecture for Control and Monitoring Activities on an IoT Network (CMAIN)

The data flowed from the sensors to the control and monitoring devices in a regular fashion, where data was sensed by the sensors at the premises, then later sent to the IoT Readers which in turn connected to the Wi-Fi access point proceeding to the LPWAN gateway. From the LPWAN gateway it was sent to the processing server to send appropriate data to End User devices for control and monitoring purposes.

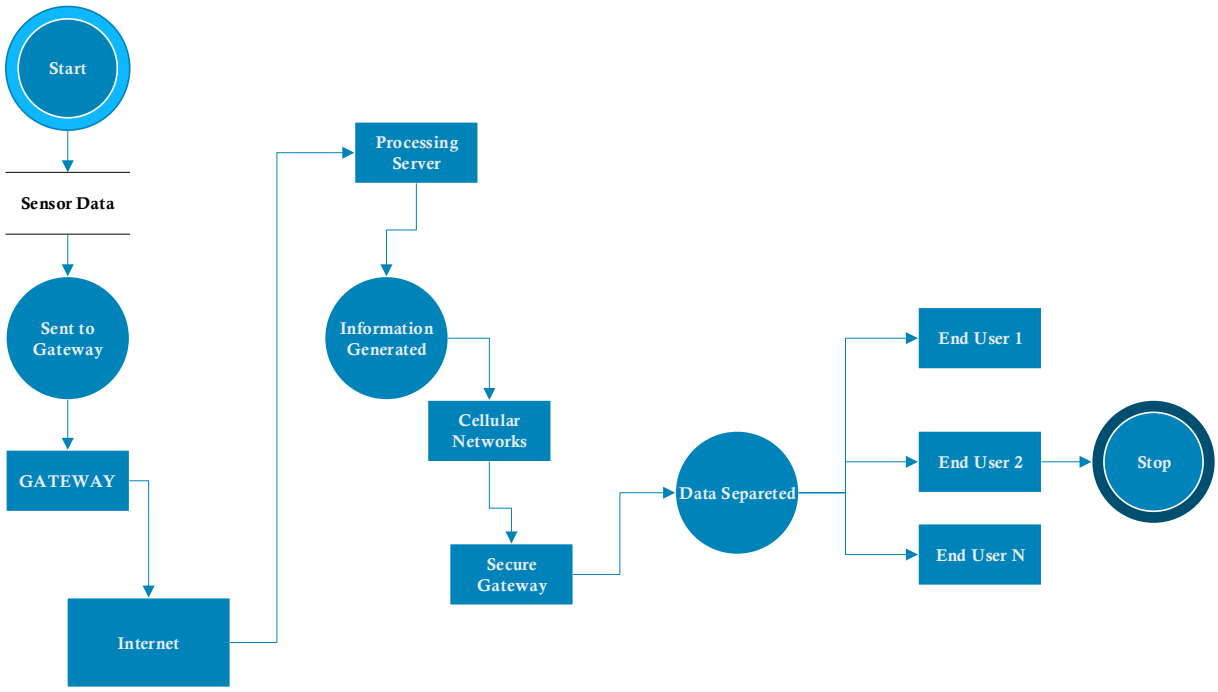

Figure 2. Data Flow of CMAIN

CMAIN was susceptible to many attacks such as DDOS, Man in the middle (MITM), Eavesdropping, Device Spoofing [3,5] and was considered too risky to be implemented for a Smart Home Ecosystem.

To protect the confidentiality and privacy of the data transferred, along with protection of the nodes on the network turning into bots the architecture was required to be modified in a way where all services and the Smart Homes could communicate with each other securely with minimum intervention from the user and it should be secure as well. The complexity of the system should be hidden from the user thus providing ease of use as well. Thus, a Security Architecture for a Smart Ecosystem using Permissioned Blockchain was needed to be formed as evident in Fig 3.

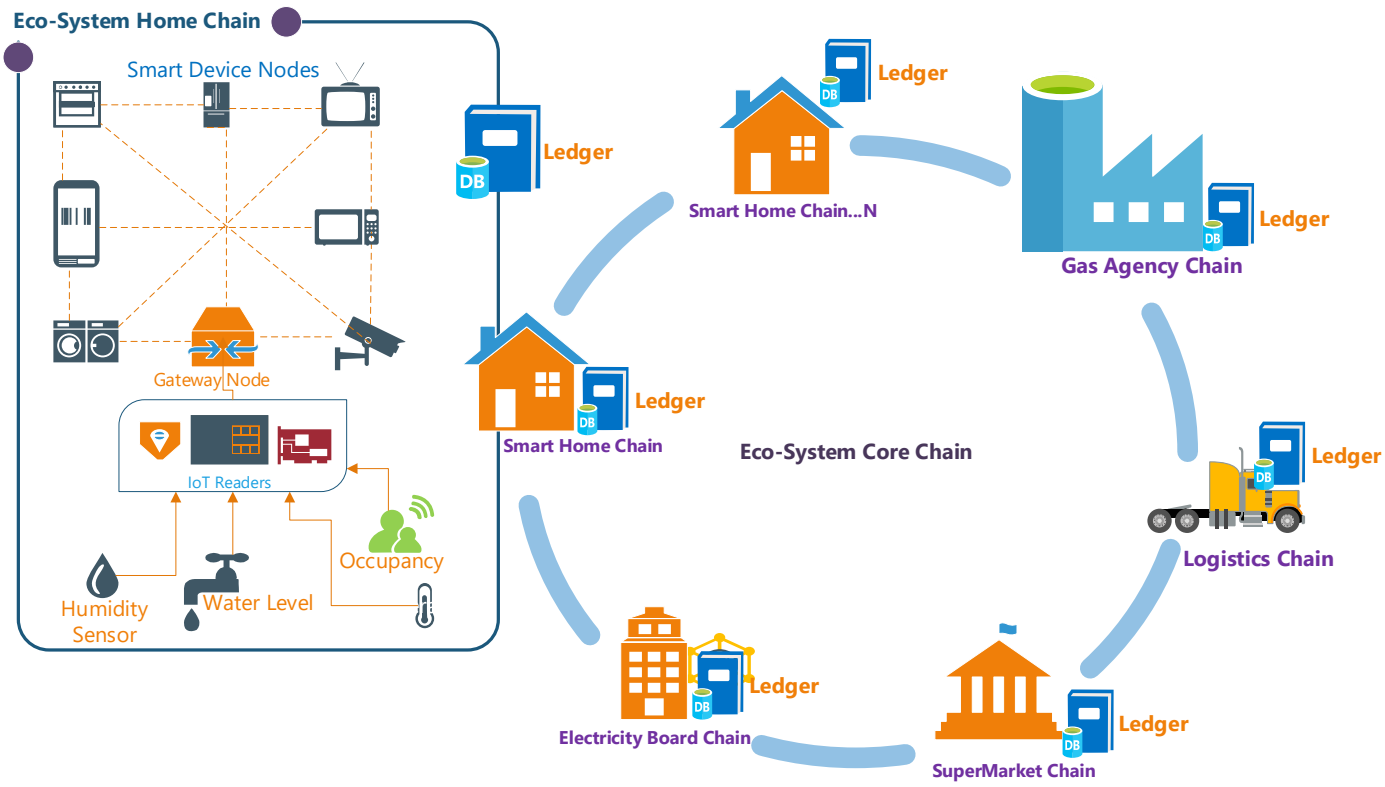

Figure 3. Security Architecture for a Smart Home Ecosystem using Permissioned Blockchain

The proposed architecture incorporated most of the features from the CMAIN and added new features to it. The components of the proposed architecture are divided into three main divisions i) Eco-System Home Chain, ii) Eco-System Core Chain and iii) Eco-System Services Chain. Under these three divisions there are various other components that make up this architecture.

3.1 Ecosystem Home Chain (ESHC)

3.1.1 Smart Device Nodes (SDE)

The ESHC houses a variety of devices, sensors and actuators which communicate with each other, out of them the most important are the SDEs. These SDEs can range anywhere from smart - washing machines, television sets, refrigerators, cameras, ovens etc., these SDEs are said to be smart because they are capable of interacting, transferring data and sending requests to other devices and services with little to no intervention of the end user. These SDEs are responsible to send requests to Smart Services and get response from them.

3.1.2 Sensors

Sensors are the basic building blocks of any IoT network, there are various types of sensors which have distinct purpose to sense various happenings in the surrounding. The sensors cannot send data to the Internet on its own, it needs an IoT reader to perform this action. Sensors can transmit Analog and Digital signals as well.

3.1.3 IoT Readers (IoTR)

Data sensed from the sensors are sent to the IoT Readers, theses node are responsible to capture the signals and process them accordingly. The data will be sent to the Gateway node to be connected further to the cloud or it could be used to perform other actions locally depending on the type of input it receives.

3.1.4 Actuators

The Actuators gets their information from the IoTR, the data sensed by the sensor which is sent to the IoTR is processed immediately and sent to the appropriate authorized Actuator to perform physical actions. The Actuators are connected to the IoTR to avoid data being sent to malicious nodes or actuators.

3.1.5 Gateway Nodes (GN)

The GNs are responsible to route the traffic from the IoT Readers to the Internet. The GNs contains an Identity Ledger of all the registered devices on the network, it has the role to authenticate and authorize data transfer including sending and receiving data. It also plays a crucial role when it comes to update the firmware on all the other devices securely.

3.1.6 Home Ledger (HL)

The Home Ledger houses the authentication information of all the registered services, the registered users and devices all in an immutable ledger. The transactions from the GNs and the SDEs are also stored as blocks in this ledger too. All requests and responses, from and too the ESHC are stored here locally and at the Eco-System Core Chain in parallel.

3.2 Ecosystem Core Chain (ESCC)

3.2.1 Core Ledger (CL)

The Core Ledger contains all Identity of all the participating nodes stored in blocks, this information is received from other ESHCs of the Ecosystem and the registered service providers and their identity from the Eco-System Service Chain along with the services they offer.

3.2.2 Smart Contracts (SMC)

SMCs are programs that are running on top of the Blockchain which can be called as a protocol between two parties, where the rules the protocol imposes are agreed upon both parties as a contract. The Smart Contract is automatically executed when the rules are met. The SMC does away with the need of trusted third-party nodes or middle men. An SMC is responsible to define the decree and penalties of an agreement and automatically administer the deed or sequence of actions to which the parties are legally bound through that contract.

3.3 Ecosystem Service Chain (ESSC)

3.3.1 Services

In an Eco System there are many services which a Smart Home would require, there are n number of services which can be added to the ESSC. All these services should be registered on the ESCC.

3.3.2 Service Ledger (SL)

The SL is contained in every service, it houses the list of all the Smart Homes that have been registered with the service, and it also contains the transactions of all the participating nodes stored as blocks. These transactions are also committed on the ESHC for added security.

IV. Conclusion

In this paper, an Architecture is set as a Proof of Concept which is proposed to secure a Smart Home Ecosystem using permissioned Blockchains. Various components come together in a way to manage IoT devices and their services using a permissioned Blockchain. There are three major chains, the Eco-System Home Chain, the Eco-System Core Chain and the Eco-System Service Chain. These three works in unison to provide the user a holistic automated approach with little or not intervention from the user. Using this Distributed Ledger Technology will provide protection from the attacks that work against the IoT networks.

V. Future Direction

This paper the architecture is set to many possibilities, future work will expand on this architecture to facilitate a framework and the network will be implemented real time with results and comparisons to show to the effectiveness of this model.

References

[1] Dario Bruneo, Salvatore Distefano, Maurizio Giacobbe, Antonino Longo Minnolo, Francesco Longo, Giovanni Merlino, Davide Mulfari, Alfonso Panarello, Giuseppe Patanèc , Antonio Puliafito, Carlo Puliafito and Nachiket TapasAli. 2019. An IoT service ecosystem for Smart Cities: The #SmartME project. Internet of Things; Engineering Cyber Physical Human Systems, 5: 12–33.

[2] Sujit Biswas, Kashif Shaif, Fan Li, Boubakr Nour, and Yu Wang. 2018. A Scalable Blockchain Framework for Secure Transactions in IoT. IEEE Internet Of Things Journal, Early Access.

[3] Minhaj Ahmad Khan, Khaled Salah 2018. IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems, 82, 395–411.

[4] Marco Conoscenti, Antonio Vetr`o and Juan Carlos De Martin 2017. Blockchain for the Internet of Things: A systematic literature review. International Symposium on Internet of Things: Systems, Management and Security, IEEE Xplore.

[5] Kenneth Kimani, Vitalice Oduol and Kibet Langat. 2019. Cyber Security Challenges for IoT-based Smart Grid Networks. International Journal of Critical Infrastructure Protection.

[6] Ali Dorri, Salil S. Kanhere, Raja Jurdak and Praveen Gauravaram. 2017. Blockchain for IoT Security and Privacy: The Case Study of a Smart Home. IEEE Percom Workshop on Security Privacy and Trust in The Internet of Things.

[7] Seyoung Huh, Sangrae Cho and Soohyung Kim. 2017. Managing IoT Devices using Blockchain Platform. IEEE International Conference on Advanced Communications Technology, 464-467.

[8] Kan Luo, Siyuan Wang, Wei Yu, LingChao Gao, Hafiz Muhammad Amjad and Kai Hu 2018. A Multiple Blockchains Architecture on Inter-Blockchain Communication. IEEE.

[9] Zhang, Y. and Wen J. 2017. The IoT electric business model: Using blockchain technology for the Internet of Things, Peer-to-Peer Networking and Applications, (10) 4, 983–994.

[10] Nir Kshetri, 2010. Can Blockchain Strengthen the Internet of Things? IEEE IT Professional (19) 4, 68-72.