DECENTRALIZED APPROACH TO SECURE IOT BASED NETWORKS USING BLOCKCHAIN TECHNOLOGY

Urooj Waheed
Ph.D. Scholar, Department of Computer Science, University of Karachi, Karachi (Pakistan)
E–mail: urooj050@hotmail.com

M. Sadiq Ali Khan
Associate Professor, Department of Computer Science, University of Karachi, Karachi (Pakistan)
E–mail: msakhan@uok.edu.pk

Samia Masood Awan
Research Associate, Department of Computer Science, University of Karachi, Karachi (Pakistan)
E–mail: samia_masood@hotmail.com

M. Ahsan Khan
Chief Research Officer, Go4Blockchain, Karachi (Pakistan)
E–mail: mahsankhan0@gmail.com

Yusra Mansoor
Post – Graduate Student, Department of Computer Science, National University of Computer and Emerging Sciences (FAST), Karachi (Pakistan)
E–mail: k180877@nu.edu.pk

Recepción: 05/03/2019 **Aceptación:** 09/04/2019 **Publicación:** 17/05/2019

Citación sugerida:
Waheed, U., Ali Khan, M. S., Awan, S. M., Ahsan Khan, M. y Mansoor, Y. (2019). Decentralized Approach to Secure IoT based Networks using Blockchain Technology. *3C Tecnología. Glosas de innovación aplicadas a la pyme. Edición Especial, Mayo 2019*, pp. 182–205. doi: http://dx.doi.org/10.17993/3ctecno.2019.specialissue2.182–205

Suggested citation:
Waheed, U., Ali Khan, M. S., Awan, S. M., Ahsan Khan, M. & Mansoor, Y. (2019). Decentralized Approach to Secure IoT based Networks using Blockchain Technology. *3C Tecnología. Glosas de innovación aplicadas a la pyme. Special Issue, May 2019*, pp. 182–205. doi: http://dx.doi.org/10.17993/3ctecno.2019.specialissue2.182–205

ABSTRACT

Emerging Technologies of Fourth Industrial Revolution such as Internet of Things has the potential to change the way we are living today and interact with information systems and devices. From a small device like a simple glucose monitor of healthcare sector to Autonomous cars from transportation industry, IoT plays a vital role in connected information, human interaction and data. At the same instance, IoT deals with personalized human and quite important data from various types of devices, a small loophole can be a reason to bring disastrous impact on human lives, a minor vulnerability in IoT networks may challenge the complete cycle of IoT network. It may generate calamity type of event, not only in information systems but also on the physical human lives as well, because of a single point of failure as IoT based networks usually deployed on centralized systems. In this paper, we are proposing a decentralized approach to remove single point of failure with the help of new layer of security based on Blockchain technology as advancement in securing IoT networks.

KEYWORDS

Internet of Things, Decentralized Network of IoT, IoT Security, Convergence of IoT & Blockchain, IoT Data Security and Privacy, IoT Authentication, IoT Network Distribution.

1. INTRODUCTION

1.1. INTERNET OF THINGS (IOT)

The concept of IoT came into existence in 1980's but in 1990's this concept become talk of the town (Farooq, *et al.*, 2015). Internet of Things evolved rapidly with the advancement in many related industries (Brody & Pureswaran, 2014). Through Internet of things we can reshape our standards of living, because of its important role in everyday life like in medical science, home appliances automation, transport management system (Farooq, *et al.*, 2015). The research conducted by Federal Trade Commission (TFC), the ratio between number of IoT devices and number of people has increased tremendously (Alphand, *et al.*, 2018). It is also stated that wireless device which will be connected to Internet of Thing will approximately reach the count of above 26 billion by the end of 2020, this number will exceed the devices worked as hub (Dorri, *et al.*, 2017).

The state of the art nature of the IoT services are based on the usage and combination of different data extracted from various heterogeneous devices. (Axon, 2015). IoT application system is multi farious because of its capability to: sense and extract information from environment, collect data operated by machines, classify humans, animals, information and other ongoing happenings (Brody & Pureswaran, 2014).

Figure 1. Block Diagram of Internet of Thing.

IoT also has ability to convert data into programmed instructions that "feedback through the communication networks to other things with actuating capabilities". The ability of conversion eliminates the need of human interference at every state of computation. Due to the extension in the internet boundary which now focuses on the connectivity of traditional computing devices as well as nontraditional devices, this fills the gap of connecting real and virtual world more tightly (Bahga & Madisetti, 2016). On the other hand, the Internet of Things model has diversity and complexity which brings the challenges like security, naming, privacy, mobility etc. Through studying the management and security aspect of IoT we will grasp the distinctive and innovative nature of IoT (Farooq, *et al.*, 2015). There also rises the need to cope the count of connected devices and generating large traffic. New solutions were proposed to overcome mentioned challenges.

1.2. BLOCKCHAIN

A Blockchain consists of records arranged in crypt graphical joined list that maintains a publicly empirical ledger which doesn't require a centralized authority; intrinsically, it's a replacement paradigm of assurance between units in varied application domains (Hammi, *et al.*, 2018). It consists of blocks of information in a chain like structure that automatically update whenever a new block is attached. The Blockchain utilizes "elliptic bend cryptography (ECC)" and "SHA–256 hashing" to give solid cryptographic confirmation to information verification and honesty (Xu, *et al.*, 2018). The Historically Blockchain has all things worldwide–dispersed trust. Confided in Third Parties or unified specialists and administrations can be upset, bargained or hacked. They can likewise get rowdy and wind up degenerate later on, regardless of whether they are reliable at this point. Each transaction of Blockchain's shared public ledger is checked by a majority consent of the mining nodes who are actively involved in transaction verification and validation. Blockchain initially is the technology originated from cryptocurrency, while their progress in existing architectures has led researchers to use them in areas that rank security. The advantages of new structure are localized nature, inherent darkness, resilience, security, security, autonomy (Khan, 2018).

1.3. CHARACTERISTICS OF BLOCKCHAIN

The different factors involved in making Blockchain a promising Technology are described below.

Table 1. Characteristics of Blockchain.

Decentralization	In centralized transaction processing environment, each transaction needs to be validated through the centralized trusted party (e.g., banking system), that resulting to the cost and the performance decrees at the central point. With respect to the centralized IOT model, third party is no longer needed in Blockchain. Consensus algorithms in Blockchain are used to maintain data integrity and consistency (Qian, *et al.*, 2018).
Persistency	Once a transaction record is validated by a miner node (special nodes that validate the transaction) in a Blockchain network its copy is broadcasted on the entire network and that record is not deleted or rolled back from entire Blockchain (Christidis & Devetsikiotis, 2014).
Anonymity	In Blockchain nodes interact with the network using public key that use to addresses the node on entire Blockchain network but not acknowledge the real identities of the user (Xu, *et al.*, 2018).
Security	Blockchain use the asymmetric cryptographic technique to secure the entire network. Asymmetric or public key cryptography contain 2 keys one public key and second private key. Public key is used by the node to addresses in Blockchain network and private key is use by the node to signs the transaction that it initiates. Other nodes use their public key and compare it after hashing to their signature for checking the initiator node identification (Banerjee, *et al.*, 2018).
Scalability	Blockchain address space consists of 160–bit on the other hand IPv6 address space contains 128–bits, A Blockchain address is 20 bytes or 160–bit hash of the general public key generated by ECDSA (Elliptic Curve Digital Signature Algorithm). Blockchain have 4.3 billion more Addresses over IPv6 (Otte, *et al.*, 2017).
Resilient backend	Every distributed node within the Blockchain IOT network maintains a replica of the whole ledger. This helps in safeguarding the network form any potential failures and attacks (Ouaddah, *et al.*, 2016).
High efficiency	Since the transaction removes the involvement of the third party and may proceed in Low–trust condition, the number of your time spent is obviously decrees whereas the efficiency is clearly increases (Qian, *et al.*, 2018).
Transparency	Changes made to public Blockchain network are publicly viewable by all participants in the network. Moreover, all transactions are immutable, meaning they cannot be altered or deleted (Otte, *et al.*, 2017).

2. LITERATURE REVIEW

2.1. INTERNET OF THINGS ARCHITECTURE

Two word, “Internet” & “Things” composed idea of IoT (Bahga & Madisetti, 2016). But putting these words together gives an idea of a huge network connected with different types of objects, addressed uniquely and established on standard communication protocols (Zhang & Wen, 2015).

A normal IoT system include diversified devices with built–in sensors interconnected through a system (Zyskind, *et al.*, 2015). The devices in IoT are particularly recognizable and are for the most part portrayed by low power, little memory and restricted preparing ability (Di Pietro, *et al.*, 2018, June). The passages are conveyed to associate IoT gadgets to the outside world for remote arrangement of information and administrations to IoT clients (Wörner & Bomhard, 2014). Its architecture based on layers, every layer has different functions. IoT mainly operates on three layered structure according to many researchers (Hammi, *et al.*, 2018). The IoT layers include Perception Layer, Network Layer, and Application Layer (Kouzinopoulos, *et al.*, 2018).

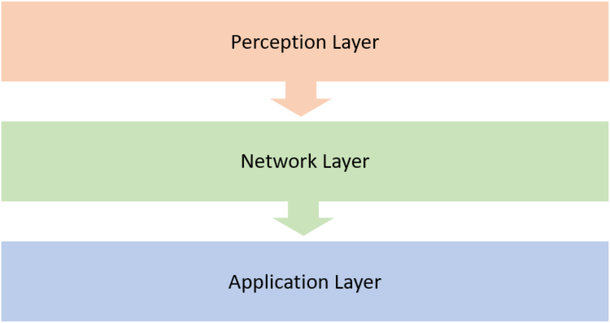

Figure 2. Layers of IoT.

Architecture Layers	Description
Perception Layer	It is also to be known as "Sensors" layer. With the assistance of actuators & sensors. It accumulates information from the surroundings. It transmits gathered and processed data to the network layer (Hammi, *et al.*, 2018).
Network Layer	The motivation behind this level is to forward the data received from the observation level to a frame of explicit logical order through existing correspondence systems such as the web, the mobile network or the other very solid system (Christidis & Devetsikiotis, 2014).
Application layer	This layer is the most surprising and most terminal layer. The application level affects organizations modified according to the client's prerequisites. With the application of television, PC or compact equipment, etc. The purpose of this level is to transfer the collected information from the perceptual level to explicit information, taking care of the structure through existing correspondence structures, such as the Internet, the mobile network or some other type of reliable structure (Mahmoud, *et al.*, 2015).

Table 2. IoT Layer based Architecture.

DOI: http://dx.doi.org/10.17993/3ctecno.2019.specialissue2.182-205

2.2. DECENTRALIZED NETWORKS

Many questions above are easy to address through a decentralized approach in IoT networks by adopting P2P communication in a standardized way (Farooq, *et al.*, 2015). This decentralized model in IoT will be able to process many transactions, up to billions between interconnected devices of IoT networks (Khan & Salah, 2018). It dramatically reduces the cost of installation and maintenance of centralized data centers (Di Pietro, *et al.*, 2018). Decentralized practically divide the overall computations and storage across connected devices across IoT networks (Brody & Pureswaran, 2014). Failure of a single node still prevent or halt the whole network (Ouaddah, *et al.*, 2016). P2P approach has its own challenges and measures of security (Conoscenti, *et al.*, 2016). IoT security is not only about securing data but providing security for the data belongs to a very personalized form (Di Pietro, *et al.*, 2018). The solution we are proposing have to support the security of that type of network dealing with thousands of nodes and billions of devices, privacy is also be equally entertained, additionally, the consensus among network participants are required to deal with data theft and spoofing (Antonopoulos, 2014). To achieve the characteristics and functionalities of seasoned IoT systems without a single point failure and centralized control, P2P messaging, distributed environment and automated coordination among devices are required (Kouzinopoulos, *et al.*, 2018).

2.3. BLOCKCHAIN ARCHITECTURE

IoT can also be made secure by the emerging technology known as Blockchain. The Blockchain technology transform the traditional mechanism of management and securing the operation technology. Because the device, sensor and controller are not changeable when in usage (Yousuf, *et al.*, 2015). With known vulnerabilities of securities as well it is not possible to fix the problem of avoid the problem because the problem may occur somewhere else in the system (Dorri, *et al.*, 2017). As described by researchers the Cloud Computing shows may failure when it operates on very large amount of data. It is very difficult to tackle data of large scale that are fragile and not resilient to failure – "as is the case with many current industrial IoT and OT systems" (Friese, *et al.*, 2010). This problem can be solved by allowing the constant arrangement of updating software, as well as Blockchain technology after devices have been deployed, with little or no downtime through an over–the–air update system (Dorri, *et al.*, 2017). Using this solution system will be available to the network most of the time (Banerjee, *et al.*, 2018). "Therefore, a cost and operationally efficient way of providing over–the–air updates and patching to IoT devices and sensors would greatly benefit the industry as a whole" (Kouzinopoulos, *et al.*, 2018).

3. THE PROBLEMS OF A CENTRALIZED IOT NETWORK

The centralized model considers as the backbone and supporting element of IoT environments. Connect and validate different types of devices by means of a group consisting of cloud–based servers, without physically connected, both devices communicate with each other over the Internet. A network is responsible for providing a domain to identify, connect and validate over cloud on the base of large storages of data centers. The maintenance cost of a centralized environment is hefty and to integrate IoT based solutions are somewhat required high–end budgets. Economic is a point need to be addressed at the designing phase before the implementation phase to understand the number of upcoming devices, the data they will share with each other and the volume of bandwidth required to support the massive network of IoT to encounter beforehand the issues may arise due to technical and non–technical ends such as scalability.

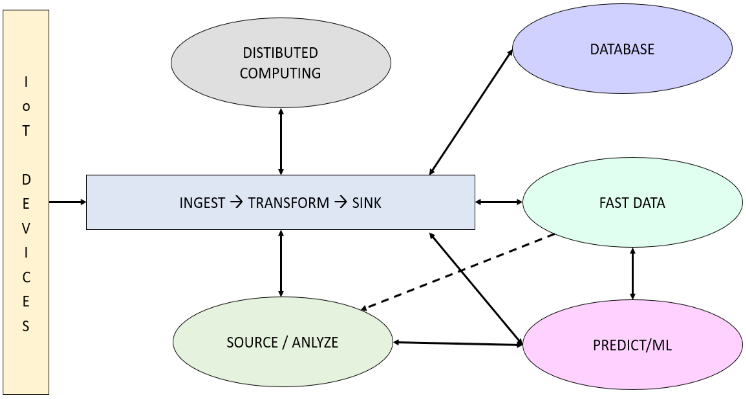

Figure 3. Centralized IoT Architecture.

The fact and attraction of IoT are whether the devices placed nearby or far from it, they are supposed to communicate over the internet using the server–client approach. A server act and privileges to each device such as identification, authentication and then allow to communicate and interact with the IoT network. Full cycle permissioned network by means of high storage data and communication processing e.g. Genetic Computing devices, which we are using for decades. As it is a generic and decade long, so is only possible to provide support for very small IoT networks, several basics and unforeseen reasons may occur when we deploy IoT networks on large scale projects such as Autonomous Cars, Smart Cities and etc. which is the growing need of tomorrow. About ultra–computation, availability of network, bandwidth and huge data storages at the time of deployment and at maintained, IoT infrastructure are high in costs. Additionally, it is also clearly explained that the cloud server's vulnerabilities and loopholes are still there, and the points discussed so far in single point failure which can fail the whole network that's the critical tasks. M2M Communications are not as easy as by definition its elaborate, there is no assurance of manufacturers about compatibility and interoperability of IoT devices, also there is not a single platform which provides a multi–manufacturer device connection hub. These are unignorably factors, which enforces us to think out of the box design and deployment strategy to maintain sustainability.

4. DEALING WITH CHALLENGES & THREATS

Accessibility can be compromised with the threats defined below:

4.1. DENIAL OF SERVICE (DOS) ATTACK

A DOS, the attacker's objective is to render the service or data unaccusable to the valid users. In the anticipated architecture, an overlay network or for a specific smart home can be attacked by sending false transactions or blocks. The effects of such an attack can however be minimized by the usage of requester and requestee PK lists in CHs. If PKs of both the requester and the requestee's of a multisig transaction are absent in these two lists, then the transaction is passed along to other CHs. A PK is blocked and remains inoperable if numerous failed access attempts are received by the CH. However, an adversary using various PKs to launch an attack can succeed.

4.2. MODIFICATION ATTACK

The assailant would have to elude the cloud storage security to launch this attack. The aim of this attack is to modify or delete the saved data of a certain user. However, by comparing hashes of the cloud data and its local BC the user would be able to realize if his data has been altered. In case of a data breach, a transaction is generated by the user that firstly references the valid multisig transaction that contains the actual hash of the data and is signed by both the user and the cloud storage and secondly it references the access transaction containing fabricated hash of the data and is signed by both the cloud storage and the user. Once various CHs receive this transaction, they authenticate the valid transactions referenced in it. If the two hashes are found inconsistent, the CH notifies its nodes of malicious activities by the cloud storage. Unfortunately, the data is unrecoverable for the user.

4.3. DROPPING ATTACK

Initiating a dropping attack requires the assailant to take over a CH or a group of CHs. The CHs controlled by the adversary drops every single transaction and block it receives. However, such an attack would be detected by the nodes in the constituent clusters since no transactions or service would be acknowledged from the network. If such a scenario arises, all the nodes in a cluster of our suggested architecture are informed about an unresponsive CH and they elect a new CH.

5. CHALLENGES TO SECURE IOT DEPLOYMENTS

Internet of Things ecosystem is diversified, and a single deployment required multiple

roles such as manufacturers, solution providers, researchers, programmers, vendors and cloud centers (Christidis & Devetsikiotis, 2014). Together, they create an environment and give necessary support for the deployments. Each role must be aware of to get the greatest benefit from IoT technologies, which is changing and expanding rapidly.

IoT systems are all about data, the data that is highly personalized or a highly sensitive, security, data management, network management and there are many complexities are involved to handle the enormous volume of users. To transform data into actions are seemingly impossible, as a number of challenges are present at the time of deployment and maintenance. These challenges turn IoT systems towards vulnerable and risky (Ouaddah, 2016). The aim of data security is all about such system availability, security and adaptability.

6. BLOCKCHAIN TECHNOLOGY AND ITS ADVANTAGES

Blockchain technology is the cornerstone of decentralized and data handling using cryptography on the distributed ledger. Each transaction done by network nodes or peers in a sequential block–by–block way with time stamping and few headers and relevant information for the reference and retrieval purposes. No central authority or no specific users across a network may act as an administrator (Conoscenti, *et al.*, 2016). This type of network or systems never responsible for any approval of transactions, participants across network develop consensus to accept any new block into the chain. Through Blockchain, the traditional and conventional centralized system will have no future especially those systems based on escrow service or intermediaries. High security, cost reduction, immutability, time savings are firsthand benefits through Blockchain (Hammi, 2018). Blockchain is based on cryptography algorithms developed to prevent data manipulation but make sure high security. Each block has a hash of the previous block so any hacker cannot temper any block in between any two blocks. Blockchain is high immutable so it's impossible to delete or revert changes.

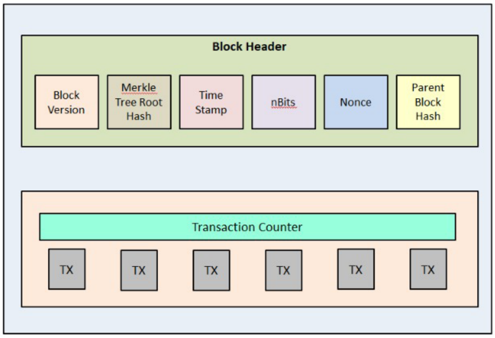

Figure 4. Blockchain Architecture.

"The Blockchain is an incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but almost everything of value." (Farooq, *et al.*, 2015). Investments from government, public and private sectors injected and capital is rising into the global Blockchain. It is greatly predicted that many more industries and thousands of new applications will be introduced to start a new era of Blockchain technology.

7. SECURITY NECESSITIES FOR IOT

7.1. DATA PRIVACY

It is necessary because of a diversified integration of services and network the data recorded on a device is vulnerable to attack by compromising nodes existing in associate IoT network. Moreover, attacker Access the data without owner permission.

7.2. DATA INTEGRITY

It is required in centralized client server model the attacker may gain unauthorized access to the network and change the original data or information and forward it. For example, Alice sends data to Bob. Watson the middle guy might get data first and forward the data after modification.

7.3. THIRD PARTY DATA COLLECTED

It is primary concern in centralized environment is stored and controlled by a third centralized entity that may miss use this data or provide it to someone else.

7.4. TRUSTED DATA ORIGIN

It based in IOT environment it is difficult to know generated data come from which device that is stored in the entire network and can be altered by anyone.

7.5. ACCESS CONTROL

It is one off the main issue in IoT network. To define which node have the right to access and perform different function in entire IOT network may be difficult.

7.6. SINGLE POINTS OF FAILURE

It requires for continuous growth of centralized networks for the IoT based infrastructure could expose single–points–of–failure. Because all data of entire network store and verified by a central authority. If the central point is failing or down the whole network is down.

7.7. SCALABILITY

Internet of thing connects many sensors and other devices for information sharing and a large number of applications via internet. It challenges the structure and the rapid growth of the system to meet scalability.

8. METHODOLOGY

There is an issue, presented because of the architectural model, the issue is really seasoned and traditional in centralized servers, it acts as single authority to grant access and verify the identity of all devices and entities that interact and transact on a network. One problem arises if someone would like to exploit the system, it must do the less hard job into hacking the system. Once the system is compromised, a hacker may act like existed devices and impersonate within the system to do dangerous activities. Usually, in IoT networks, the data from devices considered as highly sensitive. In IoT network single point of failure is unignorably arises because of centralized approach. It may create many loopholes and make IoT systems vulnerable to be hacked or crashed. To provide better security, privacy and scalability following factors are involved. The role of Blockchain is diversified and highly recommends being used in IoT networks by security experts. Blockchain is a problem–solving element if it revamps with IoT networks. Authentication, Distribution and Shared responsibilities are a few key benefits of Blockchain into IoT networks.

Suppose Device A, B and C would like to access IoT environment. These three devices need to interact with following three factors; Authentication, Distribution – Child Chain, Distribution – Parent Chain Thoroughly defined as Decentralized IoT Network using Blockchain Technology. The first factor "Authentication" ensure access to the system completely based on Distributed Ledger Technology (DLT) to have data security, privacy, immutability and resistance of censorship. Each device to follow criteria of DLT based encrypted Authentication. Once device granted access by Authentication factor. Blockchain is the cornerstone of the decentralized strategy. It acts as a distribution model and support two–way P2P communication. The centralized system provides a point, which is vulnerable and exploitable by hackers, but Blockchain gives us a unique model of authentication and distribution. This helps us to give to attacks because it is difficult to attacks hundreds and thousands of nodes at the same time. It freely entering into environment, DLT based Authentication maintains complete information of devices, such as device unique identification number and demographics related information into public ledger. It will help traceability among all participants accessed to IoT network.

When Device A would like to communicate with Device B, our architecture designed in such a way that a separate child chain will create to provide independent, on network, safe and secure P2P communication between Device A and Device B. Both devices can exchange standardized operations (hashing is simultaneously be performed) in a decentralized way. After size of Block, communication end trigger or some trigger defined already in child chain operations, generate a new Block into Parent Chain. In this way, whenever any device communication to any other device, separate child chain be created to facilitate the communication by hashing and when triggered out, the information recorded to the Parent Chain through newly generated Block.

The function of Parent Chain is to maintain record, logs, tracks, act as a Master Ledger. Web Blockchain Explorer will be provided to trace and audit the complete communication authentication pattern among the devices. These factors will help to operate and maintain Decentralized IoT Network using Blockchain Technology. Ensure better security, privacy, availability, scalability, auditing, traceability and interoperability of IoT systems. This type of architecture has an ability and feasibility to resolve many issued discussed so far in this paper. In depth study, research outcomes and simulation will be provided in the next paper.

DDoS attacks and data tampering are general issues to every other application. Because centralized systems open to many vulnerabilities itself. Single point of failure provides a chance to attackers. Blockchain is the key answer to safeguarding the systems against hackers. Authentication based in a decentralized way allows each device to find, validate and grant access to interact with IoT system.

Blockchain already proved its security, privacy and resistance against hacking and data tampering. Blockchain based decentralized authentication way of more so–called secure layer enable IoT devices to the communication directly with each other than a central point. This is the future of connected devices.

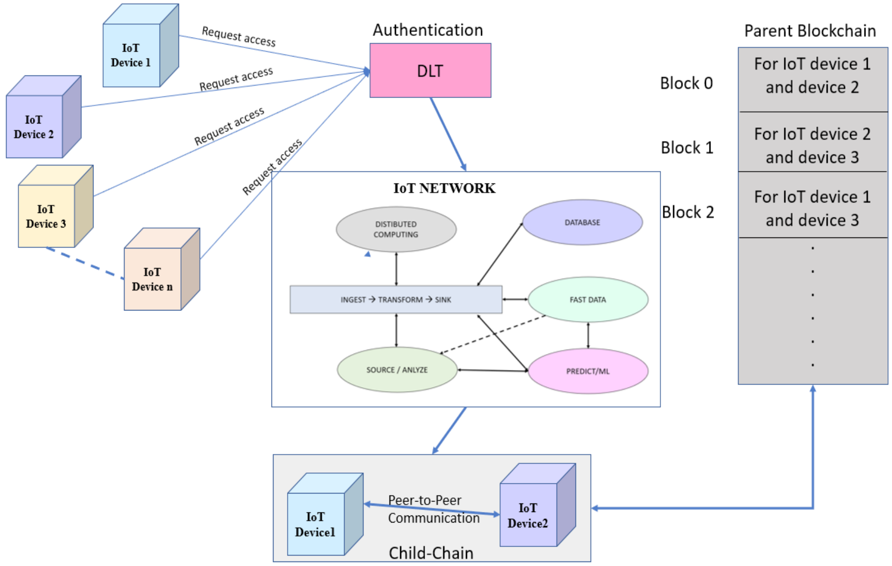

Figure 5. Proposed Blockchain based IoT Architecture.

9. CONCLUSION

Internet of Things is the key to provide us a futuristic lifestyle of automated homes and intelligent devices from transportation to healthcare industries. Even a minor vulnerability in the processing and security needs of the personalized data generated by the IoT devices can have a severe impact on human lives. In the centralized IoT networks, a single point of failure may lead to disastrous effects on information systems but can also cause catastrophic real–life incidents. In this paper, we propose to decentralize the IoT networks through Blockchain technology to overcome the susceptibilities of a centralized network. This paper reviews the literature to recognize the integral parts of IoT and Blockchain, their primary characteristics for integrating both into a solitary environment. We have examined the decentralized networks and how Blockchain will cater the challenges and threats for a more secure deployment of IoT networks to provide a better understanding for our readers. The proposed architecture not only provides decentralization but also improves the scalability, security, transparency, anonymity and efficiency of IoT networks. The paper ends with our complete proposed Blockchain architecture based on uniform scheme, authentication and distribution.

10. FUTURE WORK

To check and ensure the impact and quality assurance in lieu of security, privacy, scalability, feasibility, storage and interoperability, Hyperledger Fabric and Swath will be used for Authentication and Distributing factors. Provided a Blockchain explorer to track parent chain. Sort of simulation will be presented in a detail manner to determine the contrast and possible outcomes from this scheme. However, conventional model of IoT – M2M data transportation remain unchanged. Main objective will be practically making possible of additional layer of security using a new scheme of authentication and distribution on top of Blockchain and Distributed Ledger.

REFERENCES

Alphand, O., Amoretti, M., Claeys, T., Dall'Asta, S., Duda, A., Ferrari, G. & Zanichelli, F. (2018). IoTChain: A blockchain security architecture for the Internet of Things. *In 2018 IEEE Wireless Communications and Networking Conference (WCNC)* (pp. 1–6). IEEE.

Antonopoulos, A. M. (2014). Mastering Bitcoin: unlocking digital cryptocurrencies. *O'Reilly Media, Inc.*

Axon, L. (2015). Privacy–awareness in Blockchain–based PKI. *University of Oxford.*

Bahga, A. & Madisetti, V. K. (2016). Blockchain platform for industrial internet of things. *Journal of Software Engineering and Applications,* 9(10), p. 533.

Banerjee, M., Lee, J. & Choo, K. K. R. (2018). A blockchain future for internet of things security: A position paper. *Digital Communications and Networks*, 4(3), pp. 149–160.

Brody, P. & Pureswaran, V. (2014). Device democracy: Saving the future of the internet of things. *IBM*, September.

Christidis. K. & Devetsikiotis. M. (2014), Blockchains and smart contracts for the Internet of Things, *Security and Communication Networks*, pp. 2292–2303

Conoscenti, M., Vetro, A. & De Martin, J. C. (2016). Blockchain for the Internet of Things: A systematic literature review. *In 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA)* (pp. 1–6). IEEE.

Di Pietro, R., Salleras, X., Signorini, M. & Waisbard, E. (2018). A blockchain–based Trust System for the Internet of Things. *In Proceedings of the 23nd ACM on Symposium on Access Control Models and Technologies* (pp. 77–83). ACM.

Dorri, A., Kanhere, S. S., Jurdak, R. & Gauravaram, P. (2017). Blockchain for IoT security and privacy: The case study of a smart home. *In 2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops)* (pp. 618–623). IEEE.

Farooq, M. U., Waseem, M., Khairi, A. & Mazhar, S. (2015). A critical analysis on the security concerns of internet of things (IoT). *International Journal of Computer Applications, 111*(7).

Friese, I., Heuer, J. & Kong, N. (2014). Challenges from the Identities of Things: Introduction of the Identities of Things discussion group within Kantara initiative. *In 2014 IEEE World Forum on Internet of Things (WF–IoT)* (pp. 1–4). IEEE.

Hammi, M. T., Hammi, B., Bellot, P. & Serhrouchni, A. (2018). Bubbles of Trust: A decentralized blockchain–based authentication system for IoT. *Computers & Security*, 78, pp. 126–142.

Khan, M. A. & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, 82, pp. 395–411.

Kouzinopoulos, C. S., Spathoulas, G., Giannoutakis, K. M., Votis, K., Pandey, P., Tzovaras, D. & Nijdam, N. A. (2018). Using blockchains to strengthen the security of internet of things. *In International ISCIS Security Workshop* (pp. 90–100). Springer, Cham.

Mahmoud, R., Yousuf, T., Aloul, F. & Zualkernan, I. (2015). Internet of things (IoT) security: Current status, challenges and prospective measures. *In 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)* (pp. 336–341). IEEE.

Otte, P., de Vos, M. & Pouwelse, J. (2017). TrustChain: A Sybil–resistant scalable blockchain. *Future Generation Computer Systems*. 9(10), p. 433.

Ouaddah, A., Abou Elkalam, A. & Ait Ouahman, A. (2016). FairAccess: a new Blockchain-based access control framework for the Internet of Things. *Security and Communication Networks*, 9(18), pp. 5943–5964.

Qian, Y., Jiang, Y., Chen, J., Zhang, Y., Song, J., Zhou, M. & Pustišek, M. (2018). Towards decentralized IoT security enhancement: A blockchain approach. *Computers & Electrical Engineering*, 72, pp. 266–273.

Wörner, D. & von Bomhard, T. (2014). When your sensor earns money: exchanging data for cash with Bitcoin. *In Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication* (pp. 295–298). ACM.

Xu, Q., Aung, K. M. M., Zhu, Y. & Yong, K. L. (2018). A blockchain–based storage system for data analytics in the internet of things. *In New Advances in the Internet of Things* (pp. 119–138). Springer, Cham.

Yousuf, T., Mahmoud, R., Aloul, F. & Zualkernan, I. (2015). Internet of Things (IoT) Security: Current status, challenges and countermeasures. *International Journal for Information Security Research (IJISR)*, 5(4), pp. 608–616.

Zhang, Y. & Wen, J. (2015). An IoT electric business model based on the protocol of bitcoin. *In 2015 18th International Conference on Intelligence in Next Generation Networks* (pp. 184–191). IEEE.

Zyskind, G., Nathan, O. & Pentland, A. (2015). Enigma: Decentralized computation platform with guaranteed privacy. *International Journal of Computer Applications*, 145(4).

AUTHORS

Urooj Waheed

She is currently a Phd scholar at DCS, UoK, having MSCS (2016) in Computer Science with specialization in Human Computer Interaction and Intelligent System. She is currently working as visiting faculty in Department of Computer Science – UBIT. Her main research interests are Security, Computer Networking, Human Computer Interaction.

Dr. M. Sadiq Ali Khan

M.Sadiq Ali Khan is working as Chairman and Associate Professor at Department of Computer Science University of Karachi since 2014, and currently a chair of IEEE computer society Karachi section. He has done his Ph.D in Computer Science with specialization in Network Security. He has about 20 years of teaching and research experience and his research interest includes Data Communication & Networks, Network Security & Cryptography & Wireless Network Security, IoT. M.Sadiq Ali Khan received his BS & MS Degree in Computer Engineering from SSUET in 1998 and 2003 respectively. He is member of IEEE, CSI, PEC and NSP.

Samia Masood Awan

Samia Masood Awan completed Master of Engineering in Computers and Information Systems with specialization in Computer Networks and Performance Evaluation from NED University of Engineering and Technology (2014). She is currently working as a Research Assistant at Department of Computer Science – UBIT, University of Karachi. Her technical fields today are Computer Networks, Network Security and IoT.

Muhammad Ahsan Khan

Muhammad Ahsan Khan is a Blockchain Evangelist and Cryptocurrency Proponent. His primary domains are Advisory, Consultancy and Research of Blockchain & Cryptocurrency based PoCs, Use Cases and Convergence with 4.0 Technologies. Maintains diversify portfolio in research and development across healthcare, financial and government sectors.

Yusra Mansoor

She is currently doing MSCS from FAST–NU, having BSCS (2016) from PAF–KIET. Currently working as a lab instructor in PAF KIET and visiting faculty in department of Computer science (UBIT), University of Karachi. Research interest computer networking, network security, Algorithms, database.