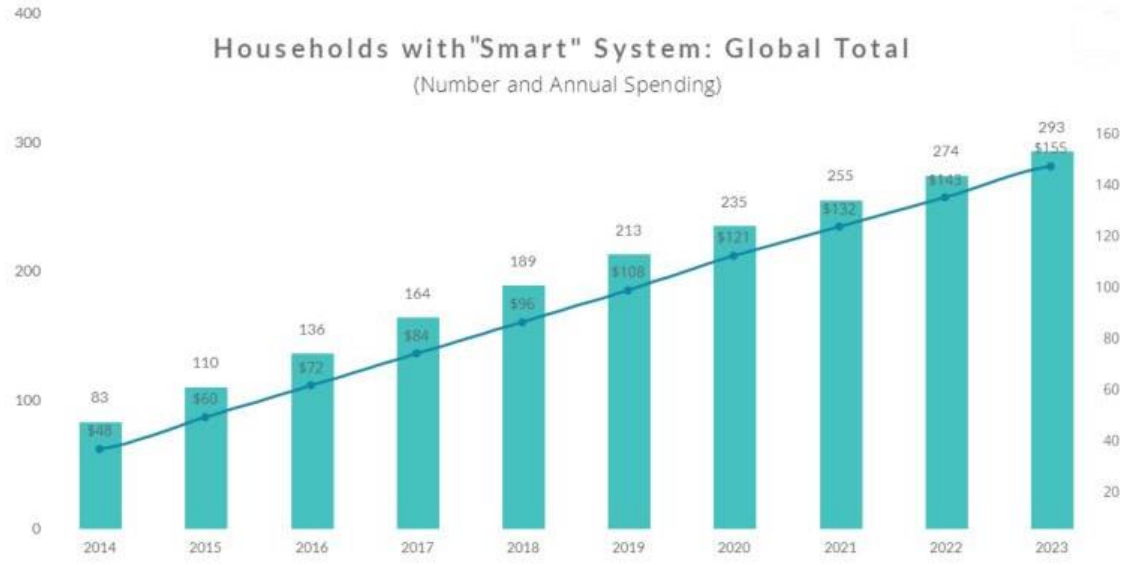
Smart Home's Data Security by Block Chain Technology Approaches

[Word count-2466]

Table of Contents

Introduction

Continuous advancements in technology has become most crucial endeavours so far in bettering the way human live their lives. One such new inducement in to human lives was smart home. A smart home is a conglomerate of heterogeneous interconnected devices such as smart phones, wearable devices and smart meters, over internet with an underlying platform based on Internet of things (IOT). (Moniruzzaman et al., 2020). Home automation has incredible potential in creating change in every aspect of home, and can dramatically enhance living experience at home. Annual spending on smart homes is increasing exponentially which can be seen from Fig.1, and for example UK government has decided to install smart electricity meters in more than 26million homes by 2020. (Lashuk, 2020) This depicts the increased potentiality of smart home market in recent times. This overarching smartness is bringing new challenges in the form of data privacy, security and integrity. Importance and consciousness over data has made individuals to travel in quest of most effective and efficient technologies that can provide data security and privacy.



Average Annual Spending on Smart Homes (with the projections from 2020 to 2023)

Source: Grey services

Figure 1: Average annual spending on Smart Homes

Block chain a synonymous term to crypto currency will be an old school thought, without any hesitation. Unleashed abilities and capabilities it possess had influenced facts of almost all industries across the world. The recent progress would be in to home automation industry to provide transparency, privacy and security of user data.

Block chain Technology is a decentralized, peer to peer transacting technology with immutable properties and a publicly available ledger. Four crucial traits audit ability, persistency, anonymity and decentralization has been the predominant factors in gaining attention from industries and academia. (Mohanta et al., 2019). The internal mechanism and workflow of Block chain technology can be viewed from Fig 2:

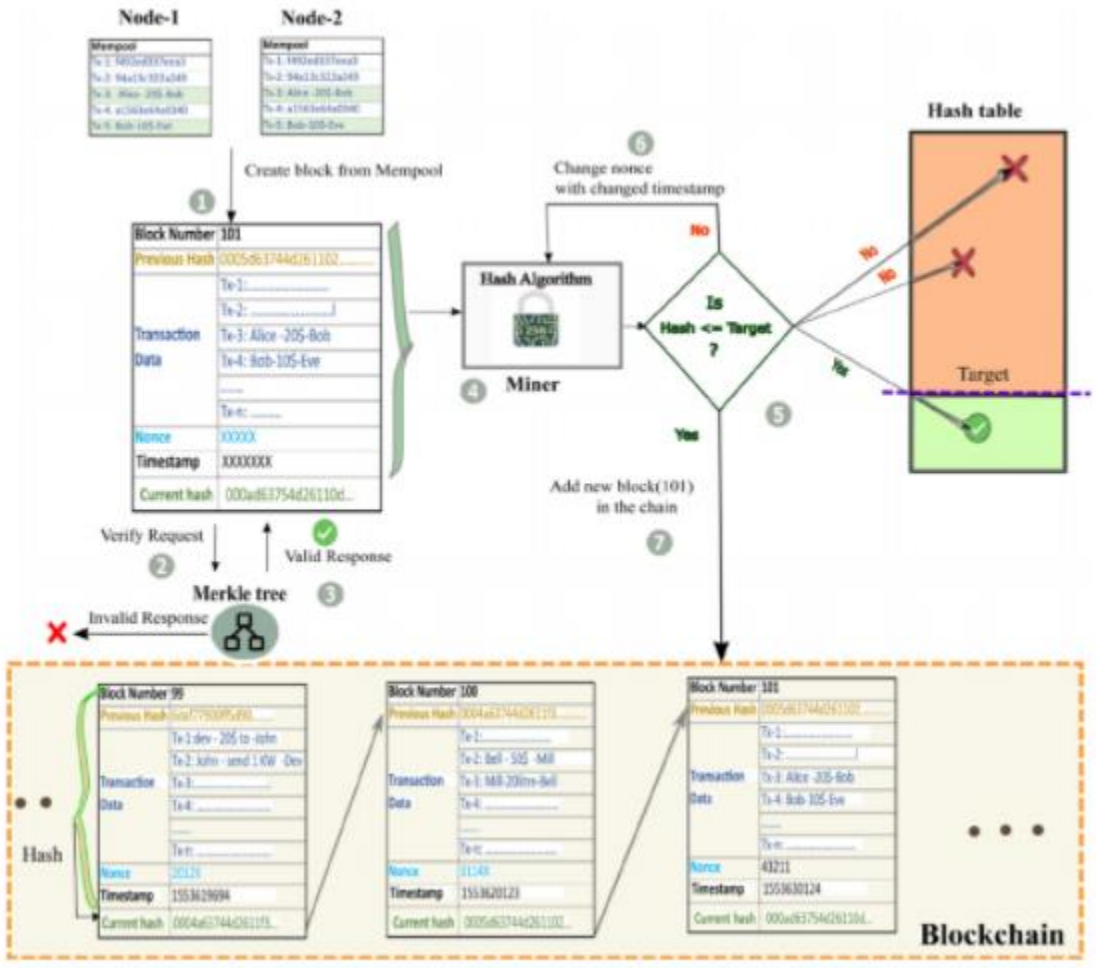


Figure 2: Internal mechanism and Work flow of Block chain technology

Problem space

Cyber security industry has emphasised that data privacy and security in smart homes would become major area of concern by 2020, due it sheer size of implementation which can draw interest of malicious attackers of data. (Maglaras et al., 2020). Due to all devices connected to a central server or cloud, a single-point failure can compromise the availability of entire data. Fault tolerant and Tamper proof environments are necessary. (Hang & Kim, 2019). Basing on emerging challenges and issues that might affect; home automation, three Block chain approaches are discussed in this study to eradicate data security issues and provide more transparency, privacy and integrity. Though, this paper has nothing to address about IoT and life cycle of products in IoT application such as development, integration and usage. But, this will address life cycle of data which include data generation, communication, storage and deletion. Security can be viewed as chief consideration in success of smart homes. First and foremost reason behind these challenges would be nature of network in which smart devices are integrated, secondly interaction among several devices manufactured or provided from diverse sources. This dynamicity surrounded over smart home is yielding larger attack surface area.

Aim

The primary aim of this study is to provide solutions for the challenges faced by the automation in the context of data security by employing Block Chain approaches.

Objective

To provide a long-term sustainable solution in the context of data security for automated homes, with all effectiveness and efficiency.

Rationale for defining problem space

Lot of scope for malicious intenders to disrupt personal life of individuals who perceives smart home as a enabler of joy and comfort. Hence, to provide an optimal solution from those malicious attacks and offer a great integration of human life with technology is the rationale behind this study.

Rich Picture

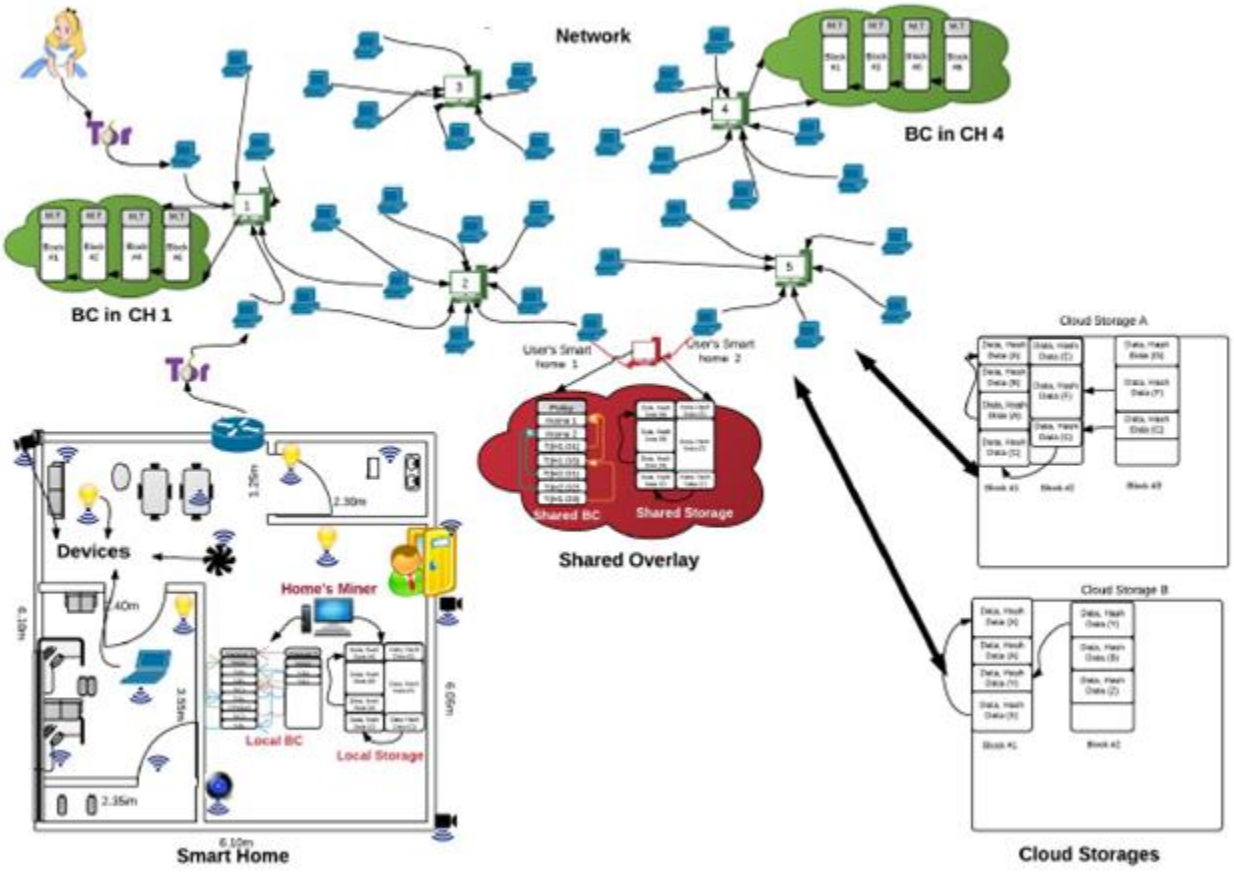


Figure 3: Rich Picture Defining Smart Based Block Chain Technology

Discussion on Block chain approaches for enabling data security in smart homes

In the following sections, three different approaches of block chain technology which can provide robust solutions to the problem space are discussed. The distributed ledgers which are online form store data decentralized manner is the prominent driving force beyond employing block chain technology. This distributed ledger eliminates the usage of centralized data storage or authority for various applications embedded in smart homes. As the data exchange in block

chain happens to be in a decentralized manner among peer-to-peer networks with standard encryption protocols, provide security requirements such as authentication, security and confidentiality for users. (Lee et al., 2020).

1. Smart home gateway network based on Block chain to avoid data forgery

Multiple heterogeneous collectively form a smart home which is controlled and communicated through a central gateway which can be called as smart home gateway. Through this gateway all of the data gets transacted, hence securing gateway in terms of confidentiality, integrity and authentication is highly important. This approach would secure smart home gateway through block chain inducement to provide all the three factors of security mentioned above.

The proposed system will deal the problem by fragmenting it into three layers namely (ref Fig.3): device layers, gateway layers and cloud layers. Each one of the layers is designed for dedicated action such as device layer collects and monitors data from all the interconnected heterogeneous devices enabled by IoT, gateway layers which stores data received from the devices finally cloud layer will be perform registration of ID's to each gateway and to the processed data at each gateway, then stores them in block chain. These blocks are shared across all users, to gain access of information irrespective of space and time.

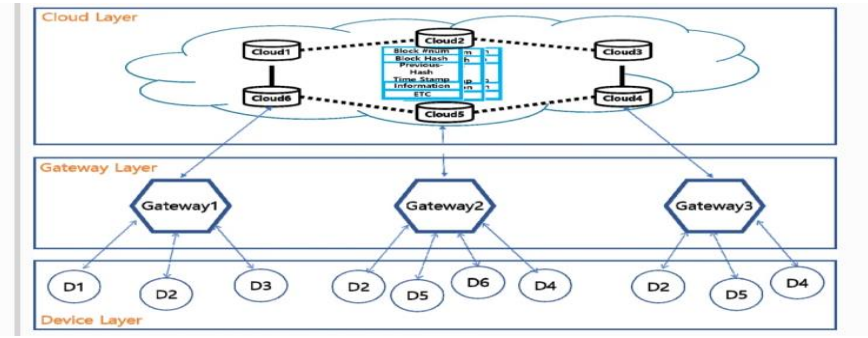


Figure 4: Layers Design for the Proposed Architecture

Note: 'D' represents Device.

Devices connected to the IoT will have each a gateway and Unique ID. And possess ability to work on encryption and decryption algorithms with SHA2 and PKI. Data collected from the gateways will undergo formatting and hash value processing, creates blocks and validates them periodically to ensure data integrity, by eliminating factor of data falsification. Identification of

gateway devices and process of collecting data can be done in series of tasks, which can be seen below:

Task 1: Device attempts to register with a gateway, and gateway in turn asks for device ID.

Task 2: Device gateways will encrypt information using a cryptographic algorithm and sends message to device, then devices decrypts the message with pre-shared keys.

Task 3: Encrypted information of gateway is decrypted and requests to another unencrypted gateway.

Task 4: Encryption of data which is device ID as well as SHA2 key is done and transferred through a gateway to enable continuous communication between routers and device.

Task 5 & Task 6: In which gateway decodes the transmitted information and verify for registration as normal devices.

Task 7: After completing above identification process, device ID is stored in the cloud. Communication between cloud and gateway over device ID list is performed.

Task 8: In the process of collecting information from device, a request message is created by gateway and sent to device.

Task 9: These data request messages are encrypted using SHA2 algorithm.

Task 10 & 11:Data transfer takes place in this the devices ask for a key for previously encrypted message used for decoding then encrypting the message .

Task 12: Message which is received is stored in gateway.

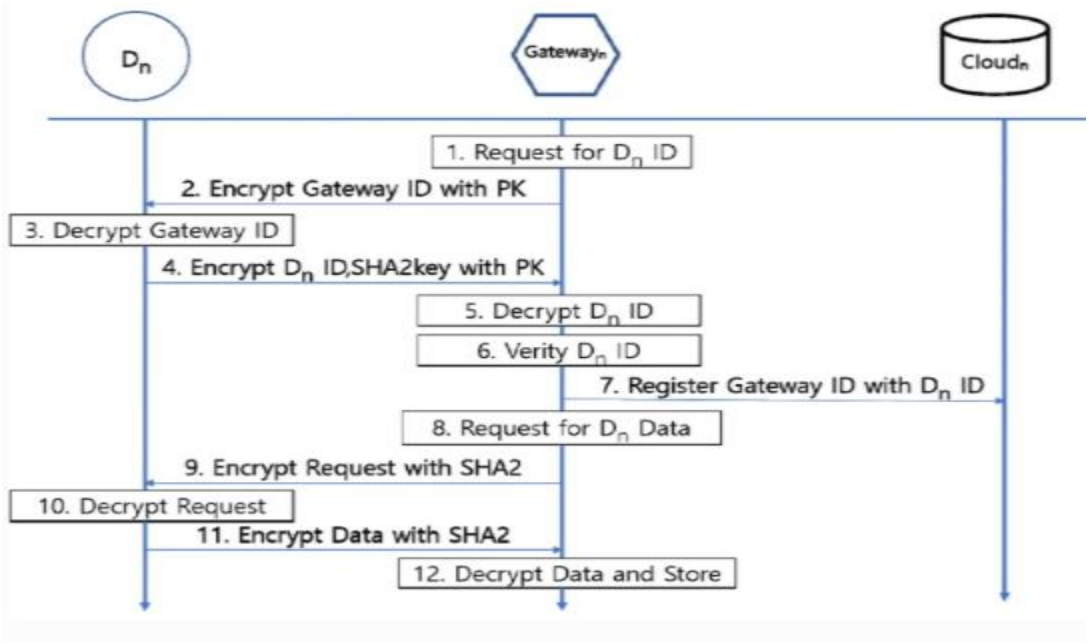


Figure 5: Data collection and Identification architecture

Data management b block chain based gateway is the crucial part, in this data is being produced from the last nodes of the network are stored through SHA3 algorithm in the data base, these blocks are verified in the block chain established in cloud in real-time to validate block, and detects blocks which are tampered . This whole process can be viewed from Fig 5.

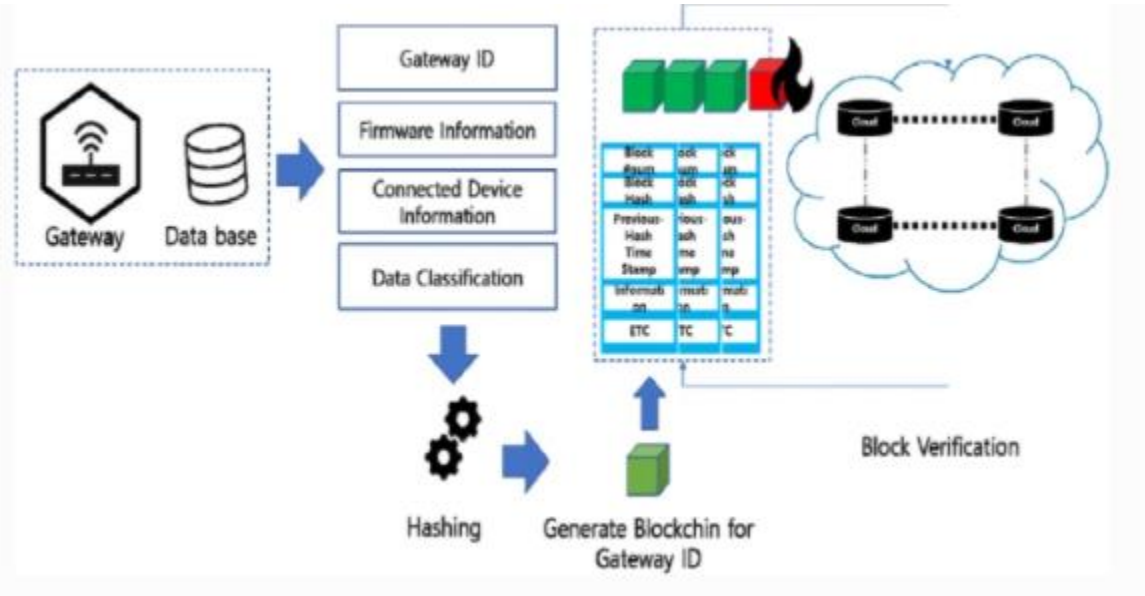


Figure 6: Data management of block chain based Gateway

2. Block chain-smart contracts for smart home security

A smart contract is defined as computerized transaction protocol that is defined and executed with terms of contract. (Zhou et al., 2018). This approach would employ three core elements: smart contracts, public Block chain and a unique private Block chain for each smart home.

The proposed solution will have below mentioned elements as core parts and processes of the architecture.

- The smart contracts will design patterns for devices behaviours during certain conditions.
- Every node in the IoT network will behave as private block chain with storage of locally distributed ledger.
- Each smart is employed with a 'local miner' in order to carry out transactions on both public and private Block chain.
- Local miner is responsible for storing device data, and enables adding new device to node or private block chain and embeds new smart contracts to devices.
- Local miners will be updated by private block chain periodically with period of 10 days.

Application procedure

Communication rules between devices are decided by the smart contracts in this model, and all the transactions among devices are designed through them. As said, once device triggers smart contract manners after satisfying certain condition, then it sends information to the proof of work based local miner to verify, once it is verified then necessary action is performed. Once, information is passed to local miner a new smart contract is developed to adjust with user behaviour and these new ones become another protocol between the devices. Local miner stores and secures private block chain and every device in the block chain will have same distributed ledger, and these devices can communicate among them only through the shared key developed by Dieffe-hellmen algorithm. This shared key is distributed among devices by local miner by examining the activity header of the block or by receiving permission from the owner. The block consists of both activity header and block header. Here, block header refers to previous block and activity header stores device information and transaction information. When it comes to

local miner, he will verify the transactions using light weight hash functions. Then the smart homes will be connected to the public block chain through local miners. Any of the transaction happens on public block chain, will be verified through local miner public key, once proof of work and transaction status gets completion then it will be uploaded to all the nodes in the public block chain.

This is the robust proposal with additional benefits such as low storage and compliments computational power drawbacks of IoT. During the process of sharing transaction internally, local miner will validate with private key and on public block chain validation will be done through public key, providing maximum data security along with high visibility, traceability and transparency.

3. Practical Byzantine Fault Tolerance based block chain for smart Homes data security

In this approach the consensus among nodes can be concluded using Practical Byzantine Fault tolerance protocol. Nodes share messages among themselves to commit a block into the block chain. The validity of block is done using this algorithm unlike other methods it is more easy in verifying blocks. In this proposed consensus method, the validation and addition of blocks is done once two-thirds of the nodes in the network agree or comes into consensus, this algorithm can tolerate faults or malicious behaviour till one third of all nodes perform maliciously. For example, four nodes are required for one malicious node is needed to gain consensus. (Salimitari & Chatterjee, 2019). In this model the proposed system will be divided in to four layers. Unlike proof of work or Proof of stake, Practical Byzantine Fault tolerance algorithm doesn't require any special miner but provides the same agreeability factor like POW & POS.

Design architecture

The design architecture or implementation process of block chain in IoT will be done in four layers IoT physical layer, Connectivity Layer, IoT block chain service layer, and an application layer. The primary advantage would be decoupling of layers, hence a developer can add or remove layers without disturbing the rest of system. As we know IoT physical layers contains various devices, which are capable for communication, computation and data storage. Connectivity layer is endorsed for routing management, because of devices lacks in global

internet protocols. Network management, message brokering and security management would be another prominent functions of this layer. The IoT block chain layer will enable system to have block chain technologies with conglomeration of all modules. These modules could be consensus (PBFT), Identity management as well as peer-to-peer network communication. The whole information shared across the block chain will be the consensus of distributed ledger, this allows all the participants of network to have same copy of ledger, more specifically nodes of the network. If any attacker or malicious intender tries to modify the data, then it is visible across all the nodes ledgers and predefined or any approved validator can validate the authenticity of information and add to the ledger once it gets validated.

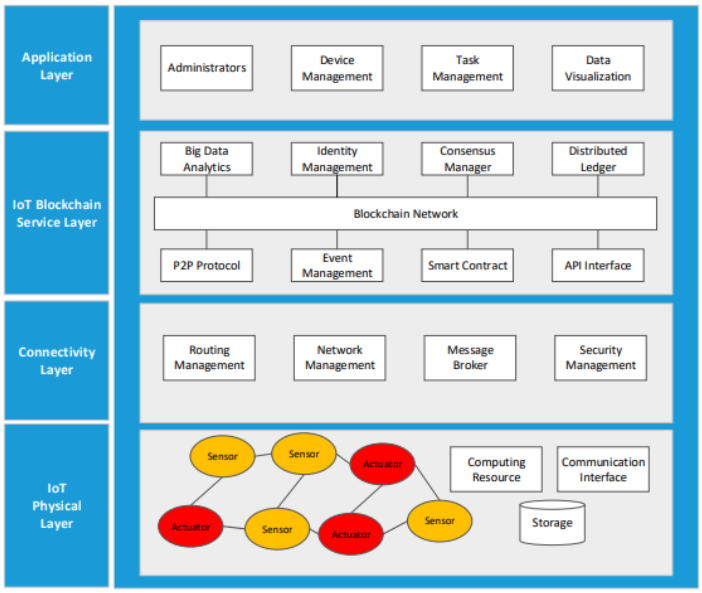


Figure 7: Layer's architecture for Proposed system

One of the primary differences in this approach is infusion of big data analytics, which enables Block chain to have efficient online data storage. Deploying big data will interpret and analyse large amount of data that is fed to the network from large number of IoT devices. (Almeid, 2017). These interpretations will reduce burden on data storage facilities, and compliments block chain application as it consumes more data storage. In a smart home due to communication between various devices, provides humongous data hence it analytics will become more helpful during this implementation.

Practical Byzantine Fault tolerance consensus algorithm will be more beneficial as it doesn't need hashing, (World, 2018) hence energy utilization will be effectively done. And this is proved to be beneficial for small group of consensus, another differential would be big data analytics, both these implementations unlike above two will provide same level of security, and leaves enough room for block chain to perform effectively.

Appraisal of block chain solutions to the problem space

All the three approaches were different in their internal mechanism, workflows and execution, but all together ends up in providing the same strength of data security for the smart home applications. After extensive research, it was found that block chain in any form can provide robust security, and the same can be witnessed through the above mentioned analysis. There were certain technical glitches corresponding to block chain integration with IoT in smart homes such as additional computation complexity, low processing speed, high storage etc., but the amount of security it can provide will rule out those issues. Though transaction speed, lack of talent, energy consumption, irrevocability , irreversibility, quantum computing will lead us into negotiation, but when block chain concerts with other technologies it will give maximum benefits in terms of efficiency in internal and external processes, provenance and transparency and build a better system on a whole. (Rijmenam, 2019).

Conclusion

Proliferation of smart homes in recent times across borders without any limitations had brought variety of benefits, in the same way, brining in diverse security challenges. Data security, privacy and confidentiality are the predominant issues. This study dealt with this problem and provided three block chain based solutions, in order to provide data security. These approaches are critically developed by considering various other loop holes of Block chain technology and provided optimal designs for data security that can be compatible with IoT based smart Home.

References

Almeid, F.L.F., 2017. Benefits, Challenges and Tools of Big Data Management. *Journal of System Integration*, 4, pp.12-19.

Hang, L. & Kim, D.-H., 2019. Design and Implementation of an Integrated IoT Blockchain Platform for Sensing Data Integrity. *Sensors*, 9, pp.1-26.

Lashuk, A., 2020. *Blockchain Knocks at your Door: What Solutions Can DLT Tools Bring to Smart Homes?* [Online] openledger Available at: https://openledger.info/insights/blockchain-in-smart-homes/ [Accessed 12 January 2021].

Lee, Y., Rathore, S., Park, J.H. & Park, J.H., 2020. A blockchain-based smart home gateway architecture for preventing data forgery. *Human-centric Computing and Information Sciences* , 9.

Maglaras, F.H.a.L., Theodoros Aivaliotis, L.X. & Kantzavelou, I., 2020. Smart Homes: Security Challenges and PrivacyConcerns. *Elsevier*.

Mohanta, B.K., Jena, D., Panda, S.S. & Sobhanayak, S., 2019. Blockchain technology: A survey on applications and security privacy Challenges. *Elsevier*, 8, pp.1-17.

Moniruzzaman, M., Khezr, S., Yassine, A. & Benlamri, R., 2020. Blockchain for smart homes: Review of current trends and research challenges. *Elsevier*, 83, pp.1-16.

Rijmenam, D.M.v., 2019. *7 Blockchain Challenges to be Solved before Large-Scale Deployment*. [Online] Dataseries Available at: https://medium.com/dataseries/7-blockchain-challenges-to-be-solved-before-large-scale-deployment-3e45b47eee6 [Accessed 12 Janaury 2021].

Salimitari, M. & Chatterjee, M., 2019. *A Survey on Consensus Protocols in Blockchain for IoT Networks*. Orlando: University of Central Florida.

World, L., 2018. *Practical Byzantine Fault Tolerance (PBFT) and How it Can Create a Social Impact*. [Online] Lala World Available at: https://medium.com/@MyLaLaWorld/practical-byzantine-fault-tolerance-pbft-and-how-it-can-create-a-social-impact-5c61d9749799 [Accessed 12 January 2021].

Zhou, Y. et al., 2018. Improving IoT services in smart-home using Block chain smart contracts. In IEEE, ed. *Confs on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing,Smart Data, Blockchain, Computer and Information Technology, Congress on Cybermatics*. China, 2018. IEEE.