International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT22811

Blockchain and IoT for Personal and Physical Security

Prof. Harshita Jain[1] , Dr. Ritu Shrivastava[2] , Dr. Rajiv Srivastava[3]

[1] Assistant Professor, Computer Science & Engineering, SIRT, Bhopal, Madhya Pradesh, India
[2] Professor and Head, Computer Science & Engineering, SIRT, Bhopal, Madhya Pradesh, India
[3] Professor and Director, Computer Science & Engineering, SIRT, Bhopal, Madhya Pradesh, India

Article Info
Volume 8, Issue 1
Page Number : 61-67

Publication Issue :
January-February-2022

Article History
Accepted : 02 Jan 2022
Published : 13 Jan 2022

ABSTRACT

The Internet of Things connects intelligent physical objects (things) and people. IoT enables every "Thing" to connect and interact, creating and transferring massive amounts of data. Because IoT de-vices handle so much data, it became necessary to incorporate Cloud Computing, Machine Learning, and Information Modelling. The significant rise in IoT is creating a surge in ICT business. By 2020, 95% of new goods will include IoT at their heart. As can be seen, IoT items will be more pre-sent, raising concerns about their visibility on the internet and legal access to resources. Innovating apps that improve a person's physical and personal life are enabled by IoT, but people's lack of security and susceptibility may lead to serious concerns like home security being penetrated and centralized organisations employing sensitive data being hacked. Blockchain technology is getting widespread interest and investigation because to its remarkable solutions to the challenges connected with the traditional centralized IoT architecture. Because there are so many IoT devices on the mar-ket for enhancing physical and mental health, and overall quality of life, a distributed trust platform that ensures scalability, privacy, and reliability is required. Integration of IoT and BC is a complex task. This research paper's goal is to create an IOT and Blockchain Application Environment that will improve a person's personal and physical existence. Thus, our main emphasis will be on developing a secure and safe Smart Home. Our suggested design uses a hierarchical and distributed blockchain platform to preserve security and privacy while meeting IoT needs. Thus, we have linked home automation with physical health, assuring safety, convenience, and health.

Keywords: Blockchain, Internet of Things, Smart Home, Smart contract, Protection, Highly automated

I. INTRODUCTION

As the Internet matures, new technologies rapidly empower old sectors. The Internet of Things (IoT) era has changed the Internet forever. This technology is rapidly evolving from a single smart device (centralised networking) to a dispersed network of linked physical devices (distributed networking). The Internet of Things has transformed the way we connect with critical equipment and has in-creased

their potential. Because IoT technology collects vast amounts of data, it may be leveraged to improve user experience. Because data collection and analysis are vital to IoT success, data security is critical. The Internet of Things (IoT) era has changed the Internet forever. Fast-growing IoT technology includes machinery, autonomous transportation, household gadgets, and Smart Homes. IoT is a network of "things" or embedded sensors linked through a private or public network. These gadgets may be remotely controlled to execute specified tasks for the users. The gadgets also share information through a network utilising common protocols.

Sensor chips were in every smart device, from wearables to industrial. IoT gathers crucial data to enhance user experience. Securing data generated by IoT devices is critical to its success. IoT data security is becoming more critical. Because IoT networks are so big and dispersed, security and privacy are crucial. Blockchain technology is gaining popularity due to its decentralised nature. It address-es many of the issues associated with the typical centralised IoT setup. Blockchain is a distributed ledger that maintains transaction integrity by sharing ledgers across Internet users. A distributed trust solution that assures scalability, privacy, and reliability is necessary due to the large number of IoT devices on the market. Block-chain (BC) technology has lately increased in popularity due to its inherent security. To automate machine-to-machine interactions, blockchain may be used for crypto-currency and trade. This is a rapidly expanding field. A lot has changed in blockchain technology, which now provides an intriguing answer for IoT security. Blockchain secures data, restricts IoT de-vice access, and shuts off compromised devices.

IoT is a world where things talk to one other. A wide range of smart gadgets may be created using this technology. It's one of Blockchain's most promising application cases. A Blockchain's data is un-changeable. New Blockchain features may be used to address difficult IoT issues [1]. Despite its mys-tique and scepticism, blockchain has fascinating IoT applications. Blockchain applications in IoT provide several benefits, from data security to automated data sales. Most IoT devices communicate over public networks, making them vulnerable to attacks. Blockchain provides everlasting indexed records [2].

II. CHALLENGES IN SECURING IOT

The combination of IoT and BC is complex. Many surveys are being done to examine these difficulties and build IOT and Blockchain applications. Gartner predicts that by 2017, over 20% of enterprises would use security solutions to secure IoT devices and services. Because IoT devices and services link and function online, they raise the danger of cyber-attacks on enterprises. To combat the rising number of internet security breaches, firms must widen and change their security approach. Security must now be tailored to the capabilities of the devices and assess the threats posed by the networks that link them. Because data collection and analysis are critical to IoT success, data security is critical. Security is critical not just during collection but throughout the data life cycle. Existing security measures assist mitigate IoT hazards, but they are insufficient to deliver data securely to the right location, at the right time, and in the appropriate format. Developing solutions for the Internet of Things requires unparalleled cooperation, coordination, and connection across all system components. The gadgets must communicate and interact smoothly with linked systems and infrastructures in a secure manner. It is conceivable, but it is costly, time consuming, and challenging until a new way of thinking and approaching IoT security emerges that is not centralised. Currently, IoT ecosystems employ centralised, brokered communication models (server/client). Cloud servers with massive storage and processing capacity identify, authenticate, and connect all devices. Even if devices are just a few feet away, they must be connected over the internet.

Because the IoT platform includes devices ranging from tiny embedded processors to huge high-end servers, it must handle security challenges at many levels. Following is a list of IoT security vulnerabilities. As shown below, we identify security concerns based on IoT deployment architecture.

- Basic security problems
- Middle-level security Problems
- High security Problems

The IoT security risks exploit multiple components such as applications/interfaces, network components, software, firmware, and physical devices. In an IoT paradigm, users interact with components through protocols, which pose a security risk. To achieve a certain degree of security, countermeasures target the interaction's weaknesses at multiple tiers. The many protocols used to deploy components add to the complexity.

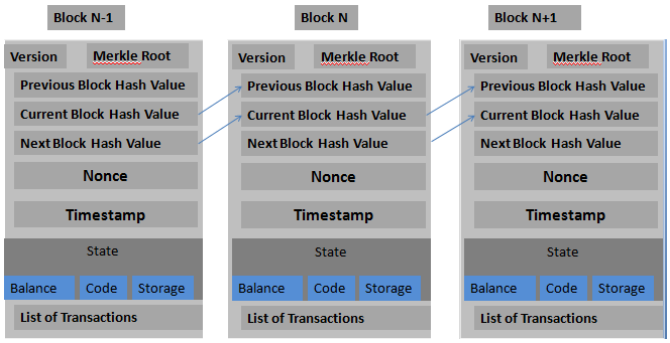

Fig. 1 A Blockchain internal working architecture block connected with other block using hash value.

This data structure organises and links transactions to preceding blocks. The header and trans-actions make up the structure. It may link a transaction to its source and destination. Identifiers for each block are stored in the header, which links them together. Partial collision is another property of the hash that demands complex computing expertise to discover. All subsequent blocks' hashes are recalculated since each block references its predecessor. Long descendent chains ensure the Blocks are unchangeable and hence secure. We use the Internet of Things (IoT) in many facets of our daily life [3]. Internet of Things (IoT) is crucial in making homes smart and cities smart. A vast volume of data is processed by the IoT, which before was not conceivable. When digitization occurs, this big volume helps create smart apps that improve people's lives. It is now possible to process data in real time using cloud computing, which has improved recently. It has opened up new avenues for data collection and sharing, for example. However, the general public lacks faith in this topic since they are unsure of how the data will be used. In this way, the blockchain may help the IoT with more secure data.

Blockchain can be considered as a tool for solving privacy, dependability and scalability issues with respect to IoT which has a centralized architecture. In centralised architecture, there are issues related to bottlenecks and central points of failure. Shifting to a peer to peer based architecture will solve this issue. Since the storage gets decentralised, smaller companies can also control the data and process them contrary to centralised architecture where large companies control the data. It also enables bet-ter fault tolerance and scalability in the system[5]. Identity of the connected devices are important since this leads to security and trust issues. By utilising a single blockchain system, all the connected devices can be identified in a unique manner. The identity is also necessary for identifying which data was provided by which device. In addition, the blockchain also provides authentication of the IoT devices. Due to the integration of Block chain various autonomous Smart devices with futuristic features and hardware can be devised. The smart devices will be able to interact with each other even in the absence of servers. This can be utilised by the IoT for Decoupled applications. The system developed is also reliable since there is no scope of loss of data through the blockchain. The users will be able to verify the data authenticity in order to make sure that the data

is still intact without any tampering. The system will also be able to trace and account the data.

III. METHODS AND MATERIAL

To maintain Blockchain Security and Privacy, the suggested Framework (Fig 2) would be hierarchical with dispersed trust. We will build a Smart Home framework that prioritises the user's physical and mental well-being as well as their comfort and convenience. Also, the data collected may serve as a person's medical record, storing crucial statistics. A cloud storage is required since the data collected by IoT devices and sensors is vast. A miner controls the Smart Home's gadgets. Users' phones and computers will be connected to an overlay network[4]. Overlay networks like Bitcoin offer a distributed aspect to our design. There is a Cluster Head for each cluster of nodes in the network (CH). Every Cluster Head has a public Blockchain with keylists. In this case, the overlay users are permitted to access data from the smart home devices linked to the network through the Requester key list the list of smart devices linked to the cluster that may be accessed by the requestee key list.

They use cloud storage to store and exchange data. Indirectly accessible devices provide design security. Different smart home transaction structures Symmetric encryption is used for smart home devices because it is lightweight and secure. The proposed model includes:

A. Transactions

Transactions are exchanges of data between smart devices or overlay nodes. Every Transaction has a purpose. Store transactions will store smart device data, access transactions will allow service providers to access cloud storage, and monitor transactions will allow the house owner to monitor device data. Transactions are also used to add and remove devices. All transactions are secured by a shared key. All smart home transactions are kept on a private Blockchain and Local Blockchain. Each Smart home has a local BC that keeps track of transactions and establishes a transaction policy[6]. Each transaction is connected together in a ledger that cannot be modified. Two headers per block, a block plus a policy header. The block header contains the preceding block's hash to prevent BC changes. Besides headers, BC stores transactions and parameters.

B. Home Miner

An entering and outgoing transaction policy is created by the local BC in each Smart home. A ledger is created by chaining all transactions together. Each block has a block and a policy header [7]. Anyone can't modify the BC as it's hashed. BC also stores transactions and settings.

C. Local storage

Local storage is any device that stores data created by devices, such as a backup drive[8]. This may be standalone or connected with the miner. Data is stored as a ledger linked to the device's beginning point using the FIFO approach.

D. Overlay Network

It's a telecommunications network constructed on top of another network's infrastructure. Encapsulating one packet within another decouples network services from the underlying infrastructure. After reaching the destination, the encapsulated packet is decapsulated[9]. Most overlay networks operate on top of the public Internet, which originated as an overlay research network on top of the PSTN's infrastructure (PSTN). Other overlay network deployments include VPNs, P2P networks, CDNs, VoIP services like Skype, and non-native software-defined networks. VXLAN, NVGRE, STT, GRE, and Network Virtualization Overlays 3 (NVO3).

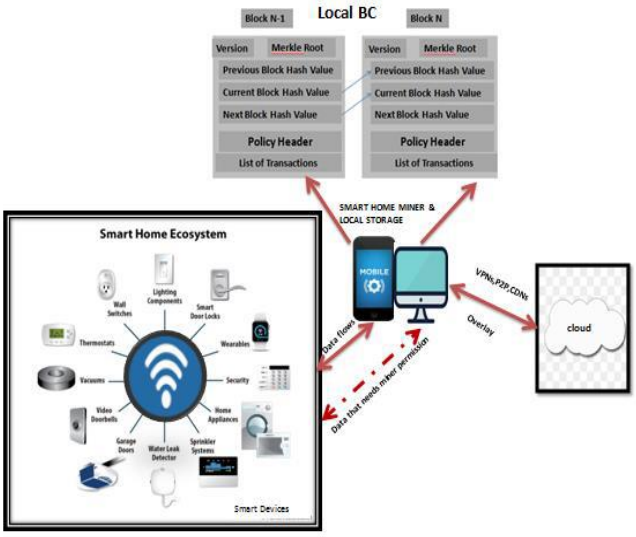

Fig 2. Proposed Framework in which mobile device connected with home appliances authenticated with blockchain local server and at the same time with cloud also.

The smart devices communicate directly with each other or with devices external to the smart home. Each device inside the home may request data from another internal device, and offer certain services, e.g., the light bulb requests data from the motion sensor in order to switch on the lights and A/C as someone enters the home. In order to allow user control a shared key is allocated to the devices by the miner. After receiving the key the devices can exchange data directly with one another as long as the key is valid. To deny this exchange the miner marks the distributed key as invalid and sends a message to the devices. The advantage of this method will be that the miner (owner) has a list of devices that share data and that the communication between the devices is controlled by the miner with the help of the shared key[10]. Since in the proposed model we are also focusing on the health and wellbeing of the residents therefore we have devices to monitor the personal parameters of the residents. This patient centric data handling can also be achieved with BC and IoT, where the owner (miner) gains ownership of their data. Once the person gets access it can manage its own data, which would be not possible without a BC.

The person's medical history may be broadcast with high security with an anonymous digital identity. When a person's medical history from various places is merged together the patient needs only one platform. This is also helpful if a critical patient requires regular surveillance. Hence the vital statistics of the person can be uploaded by the smart sensors and since, all is stored in the cloud, these parameters can be accessed even when the caregiver is away from home. Since, the complete history of the patient is available, in case of a medical emergency a message can be sent to the hospital for an ambulance and the complete history can be shared with the doctor (Fig 3).

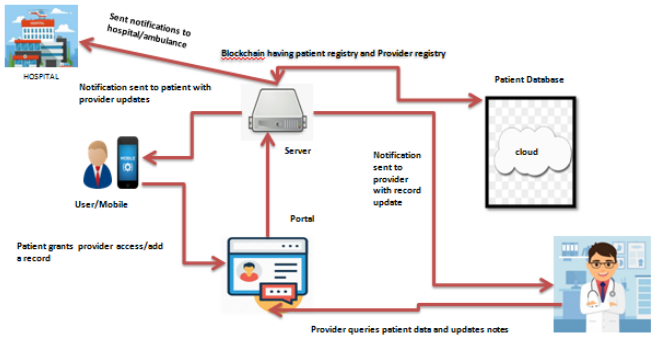

Fig 3. Proposed Framework in which a mobile device can use a portal which is associated with blockchain server through which doctor can have privilege to see the history of patient and can write prescription which is saved to cloud and notification can be sent to nearest hospital also.

Adding IoT to cloud technologies is considered as beneficial. Similarly, numerous potential exist for blockchain to reform IoT[11]. It may enhance the IoT by providing a trusted sharing service with readily identifiable data. The data source may be tracked at any moment, increasing security. This interface enables data sharing between users in applications where security is paramount. A data breach may lead to fraudulent operations or delayed security mechanisms, causing substantial harm or loss to the organisation. CIA stands for Confidentiality, Integrity, and Availability. Confidentiality guarantees only authorised users may see the message, Integrity

ensures the message is received intact, and Availability ensures the data or service is accessible when needed. With Hash functions, the BC secures data by generating a summary or data fingerprint. It creates a unique output for data integrity verification[12]. The hash output size is independent of the input size. SHA-256 and RIPEMD160 are common hash algorithms. We will employ Hash functions and Encryption. It is a combination of procedures that make sensitive data unintelligible to others. Here's how it works: A message and a key are ciphered and sent through unsecured channels without danger of unauthorised users understanding it. Using the same public/private key, decrypt the message.

IV. CONCLUSION AND FUTURE SCOPE

As a security mechanism, blockchain produces an unchangeable global index of all transactions that occur in a specific network, allowing them to be decentralised as security measures. It's a global ledger that's accessible to everyone. Without a third party, it builds trust and agreement between two people. Blockchain may be used for supply chain, smart contracts, digital identity management, and other applications. AI and blockchain may benefit from each other's abilities to analyse massive amounts of data faster. In fact, combining the two might result in a paradigm shift. By governing the chain using ML and AI, the chain may also be substantially safer. The decentralised structure of Blockchain, which encourages data sharing, also gives a chance to design better models.

V. REFERENCES

[1] N. Kshetri, "Can Blockchain Strengthen the Internet of Things?," IT Prof., vol. 19, no. 4, pp. 68–72, 2017.

[2] H. Orman, "Blockchain: the Emperors New PKI?," IEEE Internet Compute, vol. 22, no. 2, pp. 23–28, Mar. 2018.

[3] M. Conoscenti, A.Vetro, J.C.D.Martin, Blockchain for the Internet of Things: A systematic literature Review, in the 3rd International Symposium on Internet of Things: Systems, Management and Security, IOTSMS-2016

[4] Y.Zhang, J.Wen, An IoT elrctric business model based on the protocol of Bitcoin, in 2015 18th International Conference on Intelligence in Next Generation Networks, pp.184-191

[5] I. Friese, J. Heuer, N. Kong, 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), 2014,pp.1-4.

[6] Hany F. Atlama,b, Gary B. Willsa , Technical aspects of Blockchain and IOT, anarticle in Press.

[7] S. Notra, M. Siddiqi, H. H. Gharakheili, V. Sivaraman, and R. Boreli, "An experimental study of security and privacy risks with emerging household appliances," in Communications and Network Security (CNS), 2014 IEEE Conference on. IEEE, 2014, pp. 79–84.

[8] S. Notra, M. Siddiqi, H. H. Gharakheili, V. Sivaraman, and R. Boreli, "An experimental study of security and privacy risks with emerging household appliances," in Communications and Network Security (CNS), 2014 IEEE Conference on. IEEE, 2014, pp. 79–84.

[9] Sukhvir Notray, Muhammad Siddiqiy, Hassan Habibi Gharakheiliy, Vijay Sivaramany_, Roksana oreli_y,An Experimental Study of Security and Privacy Risks with Emerging Household Appliances, conference paper

[10] Dorri, A., Kanhere, S.S. and Jurdak, R., 2017, April. Towards an Optimized BlockChain for

IoT. In Proceed-ings of the Second International Conference on Internet of-Things Design and implementation (pp. 173-178). ACM.

[11] Stanciu, A., 2017, May. Blockchain Based Distributed Control System for Edge Computing. In Control Sys-tems and Computer Science (CSCS), 2017 21st International Conference on (pp. 667-671). IEEE.

[12] Emanuel Ferreira Jesus , Vanessa R. L. Chicarino, Célio V. N. de Albuquerque, and Antônio A. de A. Rocha, A Survey of How to Use Blockchain to Secure Internet of Things and the Stalker Attack, Wiley India.

Cite this article as :

Prof. Harshita Jain, Dr. Ritu Shrivastava , Dr. Rajiv Srivastava, "Blockchain and IoT for Personal and Physical Security", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 8 Issue 1, pp. 61-67, January-February 2022. Available at
doi: https://doi.org/10.32628/CSEIT22811
Journal URL : https://ijsrcseit.com/CSEIT22811