IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, July 2024

Advanced Survey of Blockchain for the Internet of Things Smart Home

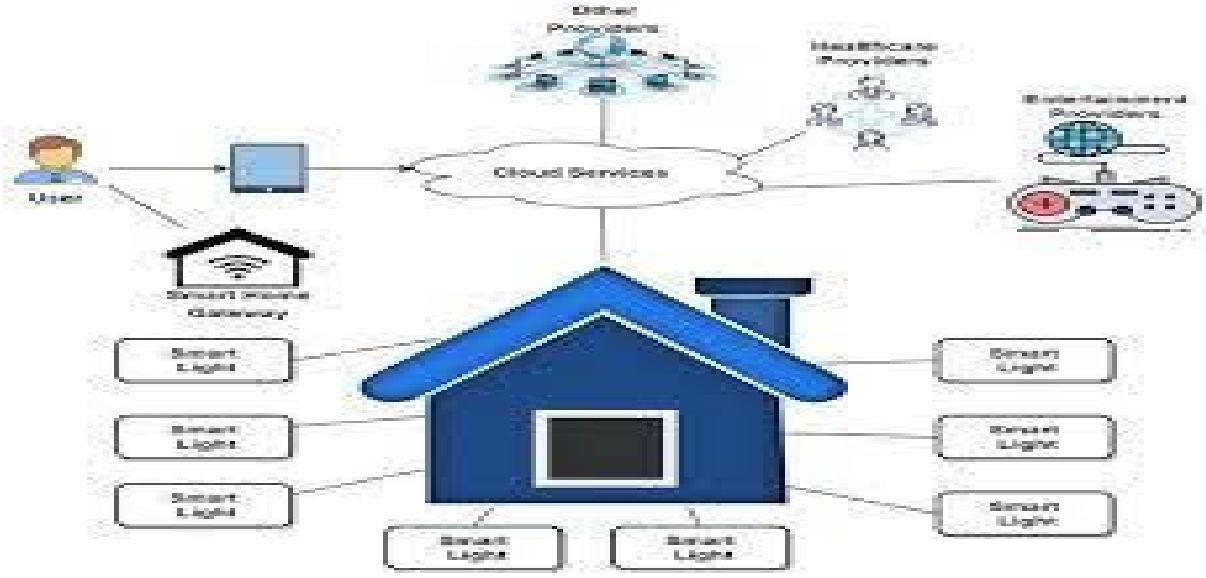
Pratheeksha Shetty, Prof. Jayanth Kumar Rathod, Sanika Gowda, Drushya Hegde, Niriksha Rai
Department of Computer Science and Design
Alva's Institute of Engineering and Technology, Mijar, Moodabidiri, India
Affiliated to Visvesvaraya Technological University, Belgaum, Approved by AICTE
pratheekshashetty830@gmail.com,sanikagowdaaaa19@gmail.com
drushyahegde99@gmail.com,niririai3344@gmail.com

Abstract: *"The Internet of Things (IoT) has many uses, like making homes smarter. But a big problem with IoT is that it relies too much on a central server, which can be risky. Blockchain, a new kind of system where everyone shares control, can fix this issue. Smart homes face lots of security problems, like hackers and privacy concerns. Blockchain is helpful here too, making sure data and transactions are safe. This paper talks about using Blockchain in smart homes, breaking it down into three main parts. It explains how Blockchain can protect data and transactions, and talks about the security of IoT smart homes.".*

Keywords: IoT, Smart Homes, Centralized Servers, Blockchain, Security, Privacy, Data Protection, Transactions, Decentralization

I. INTRODUCTION

We utilize a variety of items in our daily lives, including ovens, TVs, refrigerators, and lights. We refer to this phenomenon as the Internet of Things (IoT) when these items are networked and controlled via certain protocols. With IoT, we can remotely monitor and operate household appliances. The appliances themselves and appropriate communication equipment, as well as interfaces and modules to link these devices to the internet, are required for this to function.[1]J. Gabhane, S. Golait, and P. Gaikwad, 2015 International Conference on Computation of Power, Energy, Information and Communication (ICCPEIC) "A survey based on SmartHomes system using Internet-of-Things"



Important characteristics of blockchain technology include auditability, anonymity, permanence, and decentralization. It is capable of decentralized operation with the use of cryptography,Malware can target smart home devices like routers and webcams, leading to issues like DDoS attacks. To protect user privacy, current methods often filter out noisy or insufficient data, which can limit personalized services. This is why IoT needs a security system that is

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, July 2024

lightweight, distributed, and scalable. Blockchain technology, with its distributed, secure, and private nature, could be the answer to these security challenges in IoT. Roman-Belmonte, H. De la Corte-Rodriguez, and E. RodriguezMerchan, "How blockchain technology can change medicine," Postgraduate Medicine, 2017.

In this paper, we'll focus on using Blockchain for IoT in smart homes.We'll begin with a synopsis of IoT and Blockchain before delving further into the ways in which Blockchain can be used with IoT. We'll also talk about how blockchain technology might help with IoT security concerns. We'll wrap up by discussing our findings."[1]"A survey based on Smart Homes system using Internet-of-Things," P. Gaikwad, J. Gabhane, and S. Golait, International Conference on Computation of Power, Energy, Information and Communication (ICCPEIC), 2015). Self-learning capabilities are included into smart household appliances, enabling them to recognize schedules and change as necessary. Owners of smart homes equipped with lighting control can lower their electricity use and save money on energy-related expenses.While some home automation systems notify the homeowner if motion is detected while they are away, others have the ability to contact the fire or police departments in the event of an emergency.

Services like smart appliances, security systems, and doorbells are all included in the internet of things (IoT) technology, which is a network of physical items that can collect and exchange electronic data once linked. The Internet of Things, or IoT, encompasses internet-linked products, smart home automation, and connected gadgets.

II. LITERATURE REVIEW

"In a 2018 study, Madhugundu and associates outlined the primary security issues with IoT-based smart houses. Appliances can be remotely monitored and controlled with a smart home. These appliances are referred to as gateways, as is everything that acts as a service provider for the user. Authentication, confidentiality, authorization, availability, and integrity are among the security objectives, particularly when dealing with outside parties for services.[10] D. Madhugundu, F. Ahmed, and B. Roy, "A Survey on Security Issues and Challenges in IoT Based Smart Home," SSRN Electronic Journal,

There are two types of security attacks: passive and active. Gas leaks, water blockages, and fire detection are problems in the Internet of Things environment. Attacks can be made against sensitive data, including voice messages, videos, and pictures.

Blockchain (BC) was defined by Zheng and colleagues (2018) as a chain of blocks where each block is connected to the one before it. For transactions, each user has their own private and public keys. While the public key is used to verify transactions and is available to everyone on the network, the private key is used to sign transactions.[7]Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: a survey," International Journal of Web and Grid Services, 2018.

Blockchain has disadvantages including high bandwidth overhead and computational cost, even though it solves some security and privacy concerns in the Internet of Things. A decentralized public Blockchain at the level of higher-end devices and a centralized private Immutable Ledger (IL) at the local IoT network level comprised the lightweight

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, July 2024

Blockchain architecture for IoT that Dorri et al. (2017) proposed.[11] G. Ramachandran and B. Krishnamachari, "Blockchain for the IoT: Opportunities and Challenges," arXiv preprint arXiv.

When dealing with a large number of IoT devices, synchronization can be challenging. Huh et al. in 2017 suggested using Ethereum as a Blockchain platform due to its smart contract capabilities. They managed keys using RSA public key cryptosystems, storing public keys on Ethereum and private keys on individual devices[12] K Dorri, Ali, Salil S. Kanhere, and Raja Jurdak, "Towards an optimized blockchain for IoT." Proceedings of the Second International Conference on Internet-of-Things Design and Implementation. .

Although Blockchain has drawbacks like energy consumption and delays, it still offers decentralized security and privacy.[9] A. Dorri, S. S. Kanhere, R. Jurdak and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home,"IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Kona.Dorri et al. in 2017 also presented a lightweight version of Blockchain focusing on smart home components and functions. They introduced a high-resource device called a "miner" in each smart home to manage communication and add blocks to the Blockchain, enhancing efficiency by reducing time delays and energy consumption while increasing packet payload size".[13] S. Huh, S. Cho and S. Kim, "Managing IoT devices using blockchain platform," 19th International Conference on Advanced Communication Technology (ICACT), Bongpyeong.

"A Low Cost Design & Monitoring Of Automatic Irrigation System Based OnZigBee Technology" by-Dhawan S. Thakur , Aditi Sharma , Dileep KumarSharma- ACET, Eternal University Presented in - International Journal of Engineering Research and Technology(IJERT)www.ijert.org ISSN 2278 –0181Vol. 2 Issue 6, May -2013pages: ESRSA Publication © 2012, in this study researcher proposed a study of system which uses ZigBee network for automation of irrigation monitoring . Researcher has designed a Automatic Irrigation System which eliminate the complication of wiring and provide good operating range that ordinary system based on Bluetooth technology which can be flexibly customized as per individual requirements.

"Device Control Using Voice Recognition in Wireless Smart Home System", by- M.R.manikandan, A.Raghuram, D.Saravanan, S.Vignesh, R.Thenmozhi Selvan-Assistant Professor,Department of Electronics and Communication Engineering, Narasu's Sarathy Institute of Technology, Salem, Tamilnadu, India, presented in -International.

An ISO 3297: 2007 Certified Organization, the Journal of Innovative Research in Computer and Communication Engineering, ISSN (Online): 2320-9801, ISSN (Print): 2320-9798, Vol. 3, Special Issue 2, March 2015, describes an attempt to design a smart home system using HM2007 software, which recognizes voice, converts it to binary format, and uses a zigbee transceiver to transmit the data to the main control device. Voice commands are used to control the fan speed and light intensity of the device with the use of Laplace software.

III. IOT SMART HOME BLOCKCHAIN

"In 2017, [9]A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram conducted a research titled "Blockchain for IoT security and privacy: The case study of a smart home," which was presented at the IEEE International Conference on Pervasive Computing and Communications Workshops; Kona. From configuring IoT devices to managing transactions, Dorri and his group gave a thorough description of smart houses. Smart house, overlay, and cloud storage are the three primary layers into which they separated smart homes.

They began by outlining some important concepts and guidelines that are necessary to comprehend how the system functions. Home device communications are referred to as transactions. They may be divided into several categories, such as genesis and delete transactions, each of which has a distinct purpose. These transactions are tracked by a local private Blockchain (BC) in the smart home, which maintains security via immutable ledgers and policy headers.

The 'home miner,' a device that handles transactions to and from the house, is the brains of the system. It may be used as a stand-alone unit or in conjunction with the internet gateway in the house to verify, approve, and audit transactions. For data storage, local storage serves as a backup.

To initialize devices, the owner updates the latest blocks' policy header, which authorizes and controls device actions. The owner uses Diffie-Hellman to share keys, stored in the Genesis transaction, and sets up communication between devices using shared keys distributed by the miner. To enhance security and reduce overhead, the owner sets a threshold for periodic data transmission, terminating connections if exceeded.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, July 2024

For security analysis, the study focused on confidentiality, integrity, and availability, addressing issues like DDoS attacks and malware installation. Performance evaluation showed minimal impact on packet overhead, time overhead, and energy consumption. The study proposed a lightweight BC-based architecture for IoT, combining a centralized private Immutable Ledger (IL) for reduced network overhead and a decentralized public BC for increased trust and faster block processing[12] K Dorri, Ali, Salil S. Kanhere, and Raja Jurdak, "Towards an optimized blockchain for IoT." Proceedings of the Second International Conference on Internet-of-Things Design and Implementation.
In conclusion, the study used BC to address IoT difficulties, establishing a decentralized public BC and a centralized private IL to reduce processing time and network overhead."

IV. SECURITY REPORTING IN BLOCKCHAIN

Internet of Things (IoT)-connected smart homes [14] 2017; B. Botticelli. One of the biggest obstacles facing blockchain-enabled smart homes is security. The primary problems are included here, along with threats and attacks. We may divide dangers in smart homes into three categories to further our understanding of them:

1. Accessibility Threat: This makes data or services inaccessible to authorized users.
2. Threat to Authentication and Access Control: In this scenario, attackers attempt to authenticate themselves in an effort to access a user's data.
3. Danger to Anonymity: By examining transactions and publicly available data, adversaries try to determine a user's true identity.

Let's talk about the primary attacks now. Although there are three sorts of attacks—anonymity, authentication, and access control—each has unique characteristics. As an illustration:
- Accessibility assault: In this assault, a target node is overloaded with fictitious traffic from infected IoT devices bymeans of a distributed denial of service (DDOS).
- Anonymity Attack: This attack is comparable to the anonymity threat in that it links transactions and reveals the identity of the user by using the same public key.
- Authentication Attack: The attackers target the smart home's current gadgets.
Additionally, Minoli [15] In their paper "Blockchain mechanisms for Internet of Things security," D. Minoli and B. Occhiogrosso (2018) discussed the security needs, which include availability, confidentiality, and integrity.
Data encryption and virtual private networks (VPNs) preserve confidentiality; digital signatures preserve integrity; and i ntrusion detection systems preserve availability.
The user should define smart home devices beforehand, and local Blockchain mining should be done on them (BC).
By guaranteeing scalability and durability, utilizing shared resources from every device, and reducing superfluous traffi c flow, BC improves smart home security.Minoli [15] In their paper "Blockchain mechanisms for Internet of Things security," D. Minoli and B. Occhiogrosso (2018) discussed the security needs, which include availability, confidentiality, and integrity. Data encryption and virtual private networks (VPNs) preserve confidentiality; digital signatures preserve integrity; and intrusion detection systems preserve availability.
The user should define smart home devices beforehand, and local Blockchain mining should be done on them (BC). By guaranteeing scalability and durability, utilizing shared resources from every device, and reducing superfluous traffic flow, BC improves smart home security.
Additionally, BC establishes a secure network over untrusted parties and offers anonymity, protecting user identities.

V. SUMMARY

The security of the Internet of Things will be complicated since it runs on simple operating systems and processors that do not enable sophisticated security measures. The gadgets in the cloud were connected by cloudservers.
Internet of Things, or IoT, is characterized and validated by a cloud with enormous processing and storage capacities. Expensive IoT techniques result from the high infrastructure and maintenance costs of massive servers, centralized clouds, and network equipment. The cloud servers will continue to be a source of failure and bottleneck that could harm the entire network. The IoT can employ a decentralized strategy to address the issues raised above.Peer-to-peer processing of billions of transactions across devices reduces the expenses associated with setting up and managing

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, July 2024

centralized data centres, hence distributing computing and storage demands amongst these Internet of Things devices. The blockchain is a decentralized technology; no single master computer or centralized system controls the entire chain. It's safe as well; previous records cannot be altered and the database can only be enlarged. Because BC exists everywhere, it can be impervious to multiple attacks, even malevolent ones. Since there isn't a single channel of communication, there is also the man-in-the-middle assault. The finest or most ideal IoT solution is decentralized, made possible by blockchain technology, and it has the ability to maintain an unchangeable history of smart device usage. Despite all of BC's advantages, there are a few problems and difficulties:

A. Scalability: Centralization may result from it.

B. Processing speed and capacity: This problem arose when all items were encrypted.

C. Storage: As a result of the nodes' own cumulative storage within the ledger, the ledger will grow in size.

D. Skill deficiency: Not everyone is able to comprehend how the BC operates.

E. Legal and compliance: There is no legal or compliance code to adhere to in any of its new zones.

The devices must cooperate, coordinate, work together, and be integrated in order for IoT to function effectively. While it is feasible, putting this into practice will be costly, time-consuming, and challenging. Numerous validity checks, data verification, authentication, and encryption are required for all 61 of this. Every IoT device could become a target for one or more threats or assaults in the absence of a robust infrastructure. To address all of these problems, we therefore need a safe and secure solution for the Internet of Things system that will use blockchain technology.

VI. CONCLUSION

This article discusses IoT-enabled smart houses, emphasizing the primary security issue they face and how blockchain technology might help. It also describes security analysis for possible dangers and the used safeguards. Blockchain technology is distributed over numerous computers rather than being managed by a single one. Once data is added, it cannot be removed, making it secure. This renders it impervious to a wide range of attacks, including malevolent ones and man-in-the-middle attacks.

As previously noted, having a "miner" is the greatest approach for IoT security. All transactions to and from the smart home are managed by this miner, who also makes sure they are safe and secure. Additionally, it manages local data storage and key changes. In the end, it updates the Blockchain with every transaction.

Nevertheless, the miner cannot perform its duties effectively if it is assaulted. This can result in further issues and illegal access to data. Therefore, the miner's security should be the main emphasis of future work.

IoT can offer flexible home automation solutions that let users remotely control equipment and appliances in their homes to suit their needs.TheInternet of Things (IoT) can offer flexible solutions for energy and water supply monitoring, utility metering, leak detection, and resource conservation. In addition to watering the plants as needed, gardening sensors may measure light, humidity, temperature, wetness, and other essential gardening parameters.

Through this initiative, IoT can offer dynamic solutions for home appliance control and security monitoring straight from a smart phone. When it comes to atomizing and optimizing the concept of intelligent homes—that is, smart houses with smart rooms and smart appliances that monitor and control everything automatically—IoT can offer dynamic solutions for automations based on smart homes that take into account all the factors like power consumption, cost, monitoring, and security.

REFERENCES

[1] P. Gaikwad, J. Gabhane and S. Golait, "A survey based on Smart Homes system using Internet-of-Things," 2015 International Conference on Computation of Power, Energy, Information and Communication (ICCPEIC), Chennai, 2015, pp. 0330-0335.

[2] L. Carlozo. What is blockchain? Journal of Accountancy, 2017, 224(1)

[3] J. Roman-Belmonte, H. De la Corte-Rodriguez, and E. Rodriguez Merchan, “How blockchain technology can change medicine,” Postgraduate Medicine, 2017, 130(4), pp.420-427

[4] S. DAVIDSON, P. DE FILIPPI, and J. POTTS, “Blockchains and the economic institutions of capitalism,” Journal of Institutional Economics, 2018, 14(4), pp.639-658.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, July 2024

[5] Yu, B., Wright, J., Nepal, S., Zhu, L., Liu, J. and Ranjan, R, "IoTChain: Establishing Trust in the Internet of Things Ecosystem Using Blockchain," IEEE Cloud Computing, 2018, 5(4), pp.12-23.
[6] F. Wessling and V. Gruhn, "Engineering Software Architectures of Blockchain-Oriented Applications," IEEE International Conference on Software Architecture Companion (ICSA-C), Seattle, WA, 2018, pp. 45-46.
[7] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: a survey," International Journal of Web and Grid Services, 2018, 14(4), p.352.
[8] N. Kshetri, "Can Blockchain Strengthen the Internet of Things?" IT Professional, 2017, 19(4), pp.68-72.
[9] A. Dorri, S. S. Kanhere, R. Jurdak and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home, "IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Kona, HI, 2017, pp. 618-623.
[10] D. Madhugundu, F. Ahmed, and B. Roy, "A Survey on Security Issues and Challenges in IoT Based Smart Home," SSRN Electronic Journal, 2018.
[11] G. Ramachandran and B. Krishnamachari, "Blockchain for the IoT: Opportunities and Challenges," arXiv preprint arXiv:1805.02818, 2018.
[12] K Dorri, Ali, Salil S. Kanhere, and Raja Jurdak, "Towards an optimized blockchain for IoT." Proceedings of the Second International Conference on Internet-of-Things Design and Implementation. ACM, 2017.
[13] S. Huh, S. Cho and S. Kim, "Managing IoT devices using blockchain platform," 19th International Conference on Advanced Communication Technology (ICACT), Bongpyeong, 2017, pp. 464-467.
[14] B. Botticelli, (2017). Blockchain for IoT - Smart Home. [online] Slideshare.net. Available at: https://www.slideshare.net/BiagioBotticelli/blockchain-for-iotsmart-home [Accessed 5 Jan. 2019].
[15] D. Minoli, and B. Occhiogrosso, "Blockchain mechanisms for IoT security," Internet of Things, 2018, 1-2, pp.1-13.
[16] A. Reyna, C. Martín, J. Chen, E. Soler and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities", Future Generation Computer Systems, vol. 88, pp. 173-190, 2018. Available: 10.1016/j.future.2018.05.046.