IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

BLOCKCHAIN FOR INTERNET OF THINGS: FRAMEWORK, PROS AND CONS

S.R.Ajitha[1] , Dr.G.V.Ramesh Babu[2]

[1]Research Scholar, Dept of Computer Science, SV University, Tirupathi, A.P.

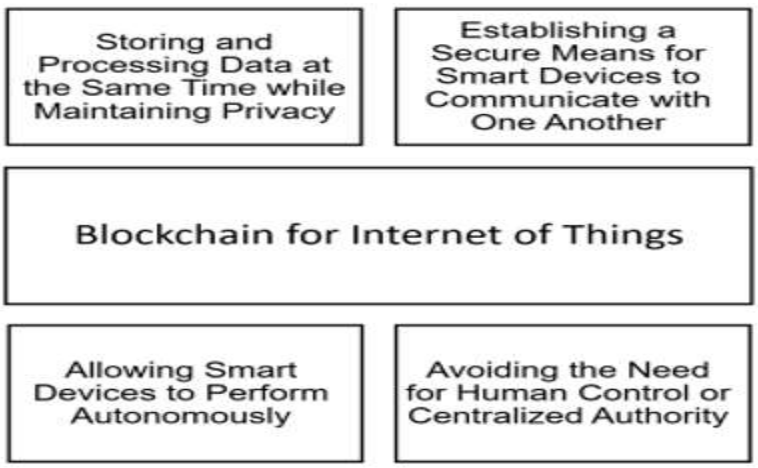
[2]Associate Professor, Dept of Computer Science, SV University, Tirupathi, A.P.

Abstract: The Internet of Things (IoT) is the linking of smart devices for data collection and intelligent decision making. Yet, IOT is open to privacy and security risks due to the absence of security measures. The centralized architecture of the Internet of Things is a significant challenge. Every node in a redIoT infrastructure is typically a potential point of weakness that could be used to start cyber attacks. Data confidentiality and authentication are other continuous and serious concerns. IoT data could be hacked and misused if data security is not provided properly for Data integrity is another issue for IoT. Decision making support systems are one of the most important IoT applications. So, protecting the system from injection attacks, which attempt to insert fake measures and, thus, impact decision making, is crucial. For automated systems, such as manufacturing sectors and vehicular networks, which handle real-time data, availability is crucial. The addition of a publicly verifiable audit trail that is not reliant on a trusted third party is necessary, as it addresses all of these issues.

Keywords: BlockChain, IOT, Security

I. Introduction

The future includes the Internet of Things (IoT). IoT can be summed up as a dynamic, world-wide network architecture with self-configuring features based on open, standardized communication protocols.



A variety of IoT conceptual designs and applications are shown, and they all concur that basic embedded sensor networking should develop into the essential standards and Internet-enabled infrastructure for communication between items.

IoT is made up of a vast number of linked things that, depending on the application context, serve a variety of purposes. Simple home sensors, medical equipment, nuclear reactors, and other objects are examples of objects.

The development of a strong and robust security framework is necessary to thwart hacking attempts given the IoT technology applications' rapid and widespread adoption.

II. Challenges in IOT

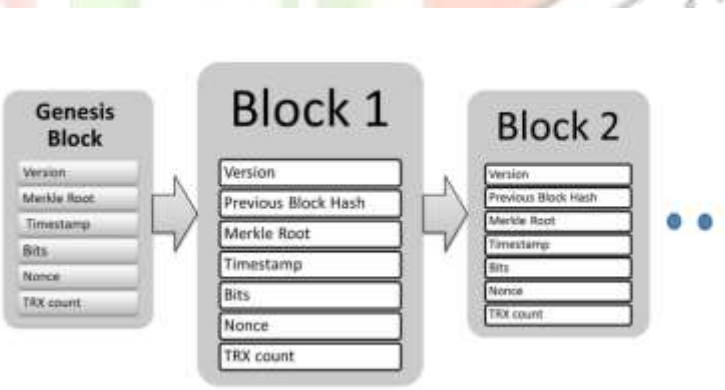
Establishing a secure framework there are numerous problems for IoT, which are summarized in the following points:

1) Scalability: IoT devices are growing quickly; by 2020, it's anticipated that they will outnumber people. Services and strategies for security must keep up with this exponential growth.

2) Heterogeneity and Resource Sufficiency: Because IoT devices and communication networks are diverse, standard and legacy security protocols, methodologies, and services are not appropriate for all devices. Additionally, a lack of resources prevents the application of strong security methods on top of IoT devices.

3) Transparency: A secure framework must be able to deploy silently and be as "plug and play" as possible while concealing intricate features from users.

A persistent time-stamped list of documents or transactions organized into blocks is known as a blockchain (BC). As seen in Figure, a block includes the number, version, hash of the preceding block, Merkle root, timestamp, nonce, transaction count, and signed transactions. The initial block of a blockchain is known as a genesis block. It is constantly hardcoded into the programs of the programs that make use of its BC. It can alternatively be classified as block number 0, however earlier versions counted it as block number 1. Given that it doesn't make reference to a preceding block, the genesis block is regarded as a "special" block. The BC peer-to-peer network is maintained by nodes, each of which has a copy of the complete blocks.



III. Properties

IoT and BC have a number of properties that can be classified as

- Technical and
- Non-Technical characteristics.

We provide brief descriptions of these characteristics below:

1) Technical

a) Heterogeneous: The Internet of Things (IoT) is made up of a variety of hardware capabilities and specifications-varying devices, even small ones-designed by various manufacturers.

b) Larger Scale: In order to serve public applications and include users from all over the world, both IoT and BC are typically deployed on a big scale.

c) General Domain Applicability: Similar to how IoT is used in a variety of fields, BC is widely used and is not just associated with cryptocurrencies.

d) The Need for Auto Deployment and Autonomous Peer-to-Peer Operations: The Internet of Things (IoT) calls for devices to interact with one another as little as possible through human involvement. Without centralized servers, BC operates purely, which adds latency and expense.

2) Non-Technical

a) Recent Technologies: Kevin Ashton first used the term "Internet of Things" in a presentation to Proctor & Gamble in 1999, but it has gained significant attention in the past ten years. A paper by Nakamoto that is regarded as the beginning of the BC technology was published in October 2008.

b) Research Work Trend: Current research directions have given both technologies significant attention. The study on IoT and BC that was done over the past ten years is depicted in Figure 2. It has been observed that the growth of research in both IoT and BC has been rapid. It's also important to note that beginning in 2017, the amount of research on IoT and BC is rapidly changing.

IV. Frameworks for BlockChain-Based Security

The Internet of Things (IoT) technology replaces centralized structures with a sophisticated network of decentralized smart gadgets. Because of the vast scale and heterogeneity of IoT devices, creating an effective security architecture is no longer an easy process. Many IoT challenges can be modeled using BlockChain. Table I lists the IoT problems that BC can solve. Not only does BlockChain aid in the resolution of important IoT issues, but it also has other advantages:

1) Data tampering proof.

2) Sturdy and dependable.

3) More personal information.

4) Documents historical events.

5) Absence of a single control authority.

6) Cost-cutting in the development of massive internet infrastructure.

V. Layers of Blockchain

The framework used BlockChain for smart house applications and introduced a four-tiered architecture:

1) Physical Layer: Many sensory devices in smart homes collect and convey data to the other levels. Many smart gadgets (for example, security cameras) are prone to security breaches due to a lack of access control mechanisms and encryption.

2) Communication Layer: In this layer, smart devices exchange data via various communication protocols (e.g., Bluetooth). The block chain protocol must be connected with the communication layer to offer security and privacy during data transmission. This integration is difficult because the requirements differ from one application to the next.

The intruders.QuillBot's paraphraser alters your sentences, allowing you to edit and republish your text.

3) Database Layer: A distributed ledger, often known as a block chain, is a sort of decentralized database that stores and records received data one after the other. Each ledger record includes a time constraint as well as a unique cryptographic signature. A user with permission can check the ledger's history. In practice, there are two sorts of distributed ledgers: permissionless and permissioned.

Because the public ledger is vulnerable to anonymous assaults, it is best to employ permissioned to assure real-time object security, scalability, and performance.

4) Interface Layer: This layer contains a number of devices that communicate and transfer data with one another. For example, using a mobile phone device to manage a refrigerator or view home security cameras. The main thing to remember is that the applications or devices must be appropriately integrated so that outsiders do not gain access.

VI. Conclusion

To summarize, the use of blockchain for IoT applications enables high levels of security, preventing unauthorized data access. However, scalability remains an unresolved subject because the blockchain's size might grow over time, making it impossible to acquire and save the ledger.

REFERENCES

[1] M. Zorzi, A. Gluhak, S. Lange, and A. Bassi, From Todays's INTRAnet of Things to a Future INTERnet of Things: A Wireless- and Mobility Related View, IEEE Wireless Commun., vol. 17, no. 6, pp. 44–51, 2010.

[2] Ali H.Ahmed, Nagwa M. Omar, Hosny M. Ibrahim, Modern IoT Architectures Review: A Security Perspective, International Conference on ICT: Big Data, Cloud and Security (ICTBDCS), 2017.

[3] Parul Datta and Bhisham Sharma, A survey on IoT architectures, protocols, security and smart city based applications, International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2017.

[4] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, academia.edu, 2009.

[5] IDC, Connecting the IoT, http://www.idc.com/infographics/IoT/ATTACHMENTS/IoT.pdf, accessed: 28/2/2019.

[6] Imane BouiJ-Pasquier, Anas Abou El Kalam and Abdellah Ait Ouahman and Mina De Montfort, A Security Framework for Internet of Things, Cryptology and Network Security, 2015.

[7] S.Sridhar and Dr. S,Smys, Intelligent Security Frmaework for IoT Devices, International Conference on Inventive Systems and Control (ICISC), 2017.

[8] Mahmoud Ammar, Giovanni Russello and Bruno Crispo, Internet of Things: A survey on the security of IoT frameworks, Journal of Information Security and Applications, vol. 38, pp. 8–27, 2017.

[9] Xiruo Liu, Meiyuan Zhao, Sugang Li, Feixiang Zhang and Wade Trappe, A security Framework for the Internet of Things in the Future Internet Architecture, Journal of Future internet, vol. 9, no. 3, pp. 1–28, 2017.

[10] Himanshu Gupta and Garima Varshny, A Security Framework for IoT Devices Against Wireless Threats, International Conference on Telecommunication and Networks (TEL-NET), 2017.

[11] Seyoung Huh, Sangrae Cho, and Soohyung Kim, Managing IoT Devices using Blockchain Platform, International Conference on Advanced Communication Technology (ICACT), 2017.

[12] Ethereum White Paper, https://github.com/ethereum/wiki/wiki/WhitePaper, accessed: 2019/2/28. [13] Ethereum, Writing a Contract, https://github.com/ethereum/goethereum/wiki, accessed: 28/2/2019.

[14] G. Wood, Ethereum: A Secure Decentralised Generalised Transaction Ledger, http://gavwood.com/paper.pdf, accessed: 28/2/2019.

[15] S. Sridhar and Dr. S. Smys, Intelligent Security Framework for IoT Devices, International Conference on Inventive Systems and Control (ICISC), 2017.

[16] Available online: https://www.ethereum.org/, accessed: 28/2/2019

[17] Available online: https://drive.google.com/open?id=1rzJXVtE8NbSHh SHI899mN2cs1iA-CJXf, accessed: 28/2/2019.

[18] Available online: https://remix.ethereum.org/, accessed: 28/2/2019.

[19] Available online: https://solidity.readthedocs.io/en/v0.5.3/types.html, accessed: 28/2/2019.

[20] Available online: https://store.arduino.cc/usa/arduino-mega-2560-rev3, accessed: 28/2/2019.

[21] Available online: https://www.microchip.com/wwwproducts/en/ATmega2 560, last accessed 28/2/2019.