International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT206628

IOT –Overview, Implementation and Upcoming Challenges

Sativilla Mohan Kumar[1], Advin Manhar[2]
[1]Research Scholar, Amity University Chhattisgarh, Raipur, Chhattisgarh, India
[2]Assistant Professor, Amity University Chhattisgarh, Raipur, Chhattisgarh, India

Article Info
Volume 6, Issue 6
Page Number: 215-218
Publication Issue :
November-December-2020

Article History
Accepted : 01 Dec 2020
Published : 05 Dec 2020

ABSTRACT

IoT is a chain of Physical Objects that are installed with sensors, software, and other technologies for the goal of connecting and transferring data with other devices and systems over the Internet. In many research, it has been found that the data and communication between the Internet of Things are insecure. Also, the data which is transferred from one end to the other end is accessible for a shorts distance. A discovered protocol for Data Integrity in IoT communication. A protocol for providing an environmental monitoring solution and a system that facilitates the practical experimentation of the IoT solutions. After the data is secured with the protocols and it has received an environment for the experiments, the message has to be sent over a long distance.

Keywords – IoT, Data Integrity, LoRa , High Density Sensors, Ethureum Blockchain

I. INTRODUCTION

In the View of the rising IoT Devices in the market and in our daily lives. The security of these devices is under great threat. Numerous videos and articles are available on open- source platforms on how to hack these IoT devices in minutes. And the reason for hacking is the lack of communication in these security devices. This security gap can be resolved through an Integrity First Communication Protocol Ethereum Blockchain Light Client. Blockchain is used because it provides a scalable, distributed ledger that requires consensus across all participating nodes. Though the communication of the IoT devices is secured by the first Communication Protocol. But deploying the devices at a wide range of distances around the globe becomes difficult. With the rise in IoT devices, several questions come up in the mind of various researchers and scientists. The questions are how the communication should be set up, where the IoT nodes should be placed. So the implementation of IoT and its evaluation in a real environment is required. Therefore Building the IoT testbed system would allow the realism of the testing environment. The testbed system was based on high levels of simplicity and scalability. The evaluation of the testbed system was conducted by a Technology Acceptance Model(TAM). The purpose of the testbed system is that it's ready to use and easy to control in order to save time.

For long-distance communication, we need a long scale sensor network. And efforts have been made to increase the performance of the Long Scale Sensor Network which means the battery should last for decades. After intensive research and integrating a huge number of sensors LoRaWAN Protocol is the best fine. This protocol provides large communication distance and it's based on LoRa(Long Range)modulation.

Over the most recent few years, progressions in Internet technologies, which empowered systems administration of regular articles, significantly expanded the fame of the Internet of Things (IoT). The IoT describes implanted gadgets with Web network, permitting them to associate with each other, administrations, and individuals on a worldwide scale to increment dependability, supportability, and efficiency by improved admittance to data [1]. Frameworks, which affect one another, can be interconnected like home and building robotization with ecological checking to permit data to be shared between these frameworks. With low controlled remote inserted gadgets, which require a little framework, similar to the mainstream Raspberry Pi (RPi), a modest completely fledged broadly useful. As opposed to those methodologies, which generally cover little application zones with very specific conditions and cloud network, the further advancement of Montreal centers more on being an overall sensor observing structure fitting more use cases by being effectively extensible and material. To empower a clear updatable, versatile, and reasonable system with fitting innovations on energy-efficient gadgets, SensIoT kept on utilizing lightweight holder virtualization.

Besides, got sensor information is still prepared locally without the need to transfer it to cloud administrations or costly frameworks and without the weight to overflow the center organization with superfluous information traffic. Therefore, there is at present no broad sensor monitoring structure like SensIoT accessible what's more Montreal none of them utilizes compartment virtualization to disentangle the general arrangement and support of their application.

II. RELATED WORKS

At present, there is no business standard for how IoT devices should communicate securely. Many popular communications protocols for IoT devices either badly address security, or are not scalable. Researchers have only recently begun studying Blockchain as a possible IoT communication protocol. However, most IoT Blockchain implementations are too large, too centralized, too expensive, or use hardware solutions.

A. Legacy Communication Protocols

One of the Originally proposed Communication mechanisms for IoT devices is Modbus. Modbus was originally made for the isolated systems and the integration of messages was not taken into consideration.

B. Modern IoT Communication Protocols

IoT devices with faulty resources are often regarded as stifled nodes. Currently, DTLS is the default security protocol used for application messages between constrained nodes.

C. IoT Blockchains

Blockchain has been shown to be extremely scalable but has not been applied to IoT devices nor examined as a source of integrity- first communication. The most well-known modification of blockchain particularly devised for IoT is the knot, which is guided by the IOTA coin.

D. IoT Chain

IoT chain utilizes a DAG structure alike to the tangle and also uses Simplified Payment Verification (SPV) to aid services on smaller devices. SPV provides devices to carry payment verification without keeping entire Blockchain information as lengthy as block headers are preserved.

E. IoTeX

IoTex similarly uses PBFT and SPV to ensure fast transaction times and limited storage space. The fundamental thought for IoTex is the notion of blockchains inside blockchains.

F. NeuroMesh

One blockchain that successfully provides secure communication for IoT devices, which is most similar to our design, is NeuroMesh.It functions as a "friendly" botnet to fight against other botnets and delivers security commands to IoT devices with the help of Bitcoin blockchain as the connection protocol.

III. CONCLUSION

The process of forming a light client expects to speak the obstacles with communication integrity for IoT devices. Civil blockchains such as Ethereum have given us the capacityto broadcast data in a scalable and distributed fashion. The forthcoming work on the light client will add further lessening its size and practicing optimal conditions for its function on smart city IoT devices. The aim to reveal a means that will represent data from the light client and execute instructions on the IoT endpoint. Creating an agent for thelight client will be the foundation for an integrity-driven approach to performing updates for IoT devices at scale.

IV. REFERENCES

[1]. Gregory Falco, Arun Viswanathan, Carlos Caldera, and Howard Shrobe. A master attack methodology for an ai-based automated attack planner for smart cities. IEEE Access, pages 48360–48373, August 28, 2018. Shodan, (accessed April, 2018). www.shodan.io/.

[2]. Jiyong Han, Minkeun Ha, and Daeyoung Kim. Practical security analysis for the constrained node networks: Focusing on the dtls protocol. 2015 5th International Conference on the Internet of Things (IOT), 2015.

[3]. Andrew Minteer. Analytics for the Internet of Things (IoT).

[4]. Iotchain: A blockchain security architecture for the internet of things. In Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC 2018), pages 1–6, April 2018.

[5]. Riccardo Bonetto, Nicola Bui, Vishwas Lakkundi, Alexis Olivereau, Alexandru Serbanati, and Michele Rossi. Secure communication for smart iot objects: Protocol stacks, use cases and practical examples. 2012 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2012.

[6]. David Easley, Maureen O'Hara, and Soumya Basu. From mining to markets: The evolution of bitcoin transaction fees. (May 1, 2018). https://ssrn.com/abstract=3055380.

[7]. Gregory Falco, Caleb Li, Pavel Fedorov, Carlos Caldera, Rahul Arora, and Kelly Jackson. Neuromesh: Iot security enabled by a blockchain powered botnet vaccine. ACM Proceedings: International Conference on Omni-Layer Intelligent Systems (COINS), 2019.

[8]. Gregory Falco, Arun Viswanathan, Carlos Caldera, and Howard Shrobe. A master attack methodology for an ai-based automated attack

planner for smart cities. IEEE Access, pages 48360–48373, August 28, 2018.

[9]. Igor Fovino, Andrea Carcano, Thibault Murel, and Alberto Trombetta. Modbus/dnp3 state-based intrusion detection system. 2010 24th IEEE International Conference on Advanced Information Networking and Applications, 2010.

[10]. Adam Gencer, Soumya Basul, Ittay Eyall, Robert van Renessel, and Emin Sirer. Decentralization in bitcoin and ethereum networks. arXiv preprint arXiv:1801.03998,2018.

[11]. Popov Sergui. The tangle. 2015. https://iota.org/ IOTAWhitepaper.pdf.

[12]. Zhengguo Sheng, Shusen Yang, Yifan Yu, Athanasios Vasilakos, Julie McCann, and Kin Leung. A survey on the ietf protocol suite for the internet of things: standards, challenges, and opportunities. IEEE Wireless Communications, pages 91–98, 2013.

[13]. Dinesh Thangavel, Xiaoping Ma, Alvin Valera, Hwee- Xian Tan, and Colin Tan. Performance evaluation of mqtt and coap via a common middleware. 2014 IEEE Ninth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), 2014.

[14]. Gavin Wood. Ethereum (eth) – whitepaper. 2015. http: //gavwood.com/paper.pdf.

[15]. Satoshi Nakamotoi. Bitcoin: A peer-to-peer electronic cash system. 2008. https://bitcoin.org/bitcoin.pdf.

[16]. Iotex: A decentralized network for internet of things. 2018. https://iotex.io/white-paper.

[17]. Our response to ‘a cryptocurrency without a blockchain has been built to outperform bitcoin. 2018

[18]. Ethereum Blockchain App Platform, (Accessed: 2019-02- 13). https://www.ethereum.org.

[19]. Assessment of Linguistics Web Technologies Based on Cyclic Sequential Access Structure, CIKITUSI JOURNAL FOR MULTIDISCIPLINARY RESEARCH, ISSN NO: 0975-6876, Advin Manhar, Mohammed Bakhtawar.

[20]. F. D. Davis, “Perceived usefulness, perceived ease of use, and user acceptance of information technology,” MIS Quarterly, vol. 13, no. 3, pp. 319–340, 1989.

Cite this article as :

Sativilla Mohan Kumar, Advin Manhar, "IOT - Overview, Implementation and Upcoming Challenges", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 6 Issue 6, pp. 215-218, November-December 2020. Available at doi : https://doi.org/10.32628/CSEIT206628
Journal URL : http://ijsrcseit.com/CSEIT206628