International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 09 | Sep 2020 www.irjet.net p-ISSN: 2395-0072

A BIRD EYE VIEW ON LSB (LIGHTWEIGHT SCALABLE BLOCKCHAIN) IN THE PLATFORM OF INTERNET OF THINGS

N.P.Roshan[1], N.Pavithra[2]

Abstract: -*Significant attention has been developed in the field of IoT (Internet of Things) in recent times. IoT is incorporated with huge intelligent communication via internet and allows the connected things with great and fresh abilities. Now a days, the security properties for privacy preservation is regarded as the most challenging task. IoT has been implemented in most of the products and large number of devices have been linked and communicated through the internet and hence, security becomes the predominant factors for the legitimate user for accessing the sensitive resources and informative data. A promising methodology named as blockchain has been implemented with built in security setup. This system comprises the features of immutability and could able to provide efficient security in the IoT environment with the use of various cryptographic methods. The transactions and sensitive information is stored in the form of blocks with the use of hash values. However, the transaction has to be constrained per second in the blockchain process followed by the exhibition of limited throughput. Huge computational complexity occurs because of the measures taken for security methods in the protection of IoT environment. Due to this mechanism, there is a chance of occurring scalability issues with high computational complexity that limits the suitability to IoT applications. This comprehensive survey deals with the solutions for the above stated problems and the risks associated with blockchain mechanism and IoT. So for reducing the complexity and improving the security, various lightweight methods have been investigated with the aim of preventing vulnerable attacks. The presented survey clearly emphasized on the Lightweight Scalable Blockchain mechanism LSB that ensures the security and end to end privacy against harmful attacks prevailing in the IoT platforms. The paper also addresses the challenges and potential solution regarding the prescribed issues.*

Keywords- IoT, LSB, security, privacy, attacks complexity, blockchain.

1. INTRODUCTION:

Intelligent physical objects referred as people and things on the basis of universal internet work is considered as IoT (Internet of Things). It allows anything. To converse and to interconnect via internet and thereby leads to huge information system in the perspective of physical world[1]. The information and communication systems greatly benefitted due to the advancement of IoT makes it to be an important part in our day to day life activities. It is implemented in various products and large number of devices were linked and communicated thereby increasing security as the predominant factors for the legitimate user for accessing the sensitive resources and informative data[2].

The innovative applications by universal nature have been originated on one hand but on the other hand security lacking end up in serious issues for end user. For example smart alarm hacking i.e. burglary[3]. Hence security is the must and it enhances the privacy. The security properties should be considered while connecting the millions of devices and hence the user cannot use data illegally and cracking the privacy. The IoT environments seeks new technologies and suggestions related to security, interoperability and privacy. A distributed trust technology assures privacy, reliability and scalability as keystone for securing growth. Hence to attain such goals, blockchain BC has implemented and it looks promising for the intrinsic security. Blockchain offers security and also prevents high security risks and possess additional capabilities like immutability, auditability, operational resilience, transparency and data encryption [4-6]. Blockchain techniques are also sometimes vulnerable despite providing robust approaches for secure IoT. The consensus process in blockchain allow the attackers to host which is based on miner's hashing power[7]. Hence effective mechanisms needed for transactions privacy and also to avoid attacks.

LSB-The Lightweight Scalable Blockchain regulated by high resource devices and ensured regarding the security and end-to-end privacy. The LSB regulates the organized overlay networks that has been formed into cluster heads with reduced overloads[8, 9].It combines several optimization algorithms for consent of lightweight, trust distribution and management of throughput. The LSB was strong against many security attacks discussed by qualitative argument. The packet overhead and delay reduced by LSB and in addition to that the scalability of blockchain BC increased compared to relevant methods. Hence it reduced the processing time compared to existing methods and it leads to no extra delay for the smart home services thereby offering attack free IoT applications

2. CHALLENGES:

- Maintenance of privacy and security in a greater level for IoT applications and operations.
- Scalability issue, limited throughput and high processing time because of large number of security properties in the discussed blockchain mechanism.

- High complexity and vulnerability occurs in some of the cases of blockchain mechanism.

This article signifies on the challenges in IoT and blockchain mechanism that has been investigated in the following.

A. Internet of things IoT security and its challenges:

[10] This survey described the importance and framework of IoT for its applications. With the use of IoT setup, huge IoT applications were developed that make simpler implementation process in accordance with standardized terms, protocols and guiding rules. The framework generally signified on the security measures and a total of eight frameworks were discussed for framing the architecture, third party development of smart app, hardware compatibility and security. The architecture comparison linked with security depicted the various approaches in the ease of providing security.

[11] The study investigated on the IoT application of the privacy preservation with the decentralized authentication network implementation. This study has been undertaken by the ad-hoc network of cutting edge method that results to achieve communications security, privacy guaranteed by assuring security. The nodes in decentralized system related with cyber physical organization and also preserving privacy. The efficiency done on this suggested system has not relayed on the centralized organisation and the data collection during the interaction of the data collector without the idea of secured factors. Hence the paper revealed the usage of privacy preservation with decentralization for efficient security.

[12] The paper describes the definition and applications of IoT and also it signified the engaged technologies, features, functions and framework associated with the future challenges. The paper described that IoT could be linked with any kind of network with the utilization of peculiar protocols and data sharing with smart recognitions were obtained. The article concluded that IoT has been regarded as the emerging methodology in the internet and composed of mixture of applications depicted in the figure 1 with various communications of the embedded techniques.

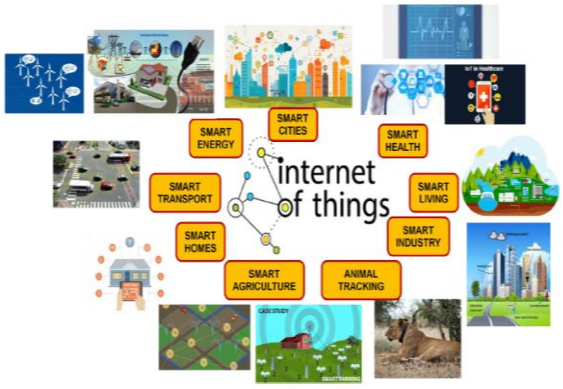


Figure 1- IoT applications

[13] The paper discussed briefly about the vulnerabilities of smart home securities associated with their modest measures. Because of the provision of services without the security by the smart phones and mobile network, defencelessness occurs. The innumerable measures comprise complex passwords and smart home services that provided awareness for information security. After reviewing and following security policy the suggested countermeasures have been utilized. So the smart applications with IoT secured against harmful threats.

[14] The paper analysed and introduced the distributed IoT applications, the authentication mechanism for WSN .The authentication mechanism has been categorized into mutual communication, authentication end-users and edge devices cryptographic credentials. Sensor nodes authenticates the end-users and they access sensitive data and services. The assessment of the suggested work depicted that the feasibility of authentication mechanism in WSN resource constrained devices. The security analysis of the suggested system effectively shows its performance when compared with the state of art methods.

[15] In this study, the multi-factor remote user authentication of lightweight biometric system for IoT services has been developed. Through gateway node the user has to register themselves initially. By using the smart devices to access any services the user then has to register to sensor nodes. Since lightweight concept used, the lesser expensive operations such as one-way hash, X-OR operations and hash functions have used and especially for IoT devices which is resource constrained it is appropriate. Using the AVISPA tool the proposed scheme evaluated. It has been secured against various attacks. The major drawback is the lesser memory.

B. Block chain mechanism in IoT:

[16] This research focused on the IoT security challenges and block chain BC implementation. For data collection the smart devices interconnected and related with IoT wise decisions should be taken. But IoT was vulnerable to

privacy and security due to the lacking of intrinsic security measure. By development the in-build security is required to solve this kind of issue and hence block chain BC introduced and IoT requirements has expected to be solved. [17] The BC showing the properties like auditability, transparency, immutability, data encryption and operational flexibility which helps in solving the IoT shortcomings. This study analysed the above mentioned part and BC approach and its approach towards IoT technologies are reviewed. In Fig.2 it clearly mentioned about the block chain working mechanism and for transactions by users' various blocks have used. Data management, various applications domains and usage patterns of manipulating device and solution level development have reported finally. The BC incorporation towards IoT and its challenges have analysed further.

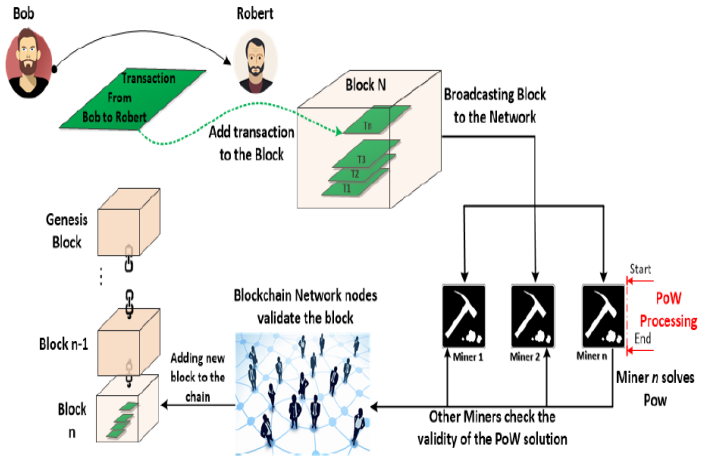
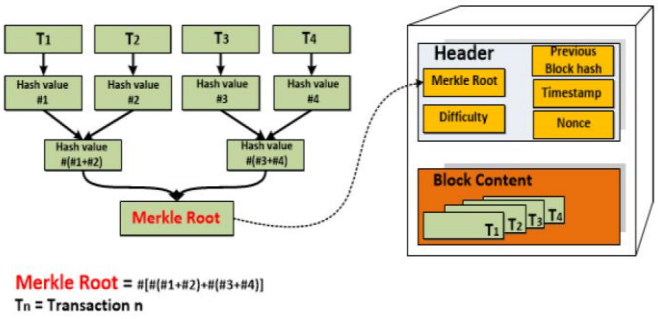


Figure [16] 2- Blockchain integration as blocks on IoT

Through hash function the approved transaction group are connected to previous block and resulted in immutable stamp, by merkle root the transactions in blocks are encoded and it clearly shown in Fig. 3 and ensure that the recorded data are not tampered.

Thus, BC decentralization scheme are proved to be distributed further and its highly secured and distributed which are proved and also the central entity is removed.



Figure[16] 3- Structure of blocks

[18] This study developed the bubbles of trust – decentralized system which provide assurance about strong identification and device authentication. The data availability and integrity are protected highly. Block chain mechanism and virtual zones exhibited security or bubbles generated in which identification of things and trust between them formed for ensure security measures taken by proposed system. Using the C++ language and Ethereum block chain this proposed study has been implemented. Low cost and efficiency have been obtained and also IoT requirement satisfied.

[1] The IoT scalability issues addressed in this study. By centralized access control system, increased load cannot be dealt. Further, this study considered about [19]fully decentralized based blockchain method to overcome many constrained IoT devices issues. This design has been proved b the Proof of Concept PoC. Scalability, generic and easy handling to manage the IoT access control system properties have been ensured in this study. High flexibility has seen through the management hub nodes which used several specific nodes integrated with many IoT devices to BC.

[20] This study analysed about the smart home settings which assures about privacy and security through blockchain. Three tiers developed in this framework like smart home, cloud storage and overlay. In ever smart home the miner has employed which refer as high resource device and it manages all internal and external communications based on home. For ensure privacy and security mainly for auditing and communication control the miner preserves BC. This proposed BC smart home context evaluated based on integrit, security, availability and confidentiality. The computational over heads have seen such as energy consumption and traffic, processing time. However, by compared with attained security and privacy this study considered the drawbacks as unimportant.

[4, 21] The security issues based on block chain technology have been addressed in the study. To many fields BC mechanism have been applied and in crypto-currency it has shown to the latest smart contract techniques. On block chain mechanism the security risks examined are Ethereum, Bitcoin etc. the vulnerabilities and real attacks reviewed and analysed. With extra improvised security techniques the block chain security can be improved further. The improvements have suggested as solution against various vulnerable threats.

A. Blockchain enhancement by LSB and other lightweight blockchain techniques:

[8] To enhance the privacy and security in IoT, this research focused on Lightweight scalable Blockchain LSB. The organized overlay networks managed by public blockchain BC and it designed into cluster heads which decreased the overheads also shown in figure 4. Many optimization algorithms have integrated by LSB for consent of trust distribution, lightweight and throughput management. Qualitative arguments suggested that the LSB was robust against various security attacks. The reduction in delay and packet overhead resulted from simulation results and moreover the blockchain BC scalability has increased related with similar techniques. For smart home devices this proposed system shows its efficiency. In high level IoT application and users, the LSB assures about security and privacy

[22] This research focused on the Sensor-Chain lightweight scalable blockchain framework for resource constrained IoT devices have been proposed. By following three stages the traditional block chain has been formed to lightweight. At first, in spatial domain small local block chain in disjoint manner are generated and required storage space seen but compared with traditional block chain it always smaller. In next stage, the temporal domain size has limited be the temporal constraint on local bock chain life span. And at the end of the stage, to retain one local block chain at a time in the memory, sensor nodes have required. The sensor chain was analysed based on scalability and long run performance. Compared with existing techniques it shows that it takes only little storage space. The sensor chain can be incorporated into smart contract considered as future work.

[23] Using leveraging lightweight blockchain the surveillance cameras data integrity addressed by this study. The video footage has considered as important footage in case of criminal investigations. The video evidence obtained through the trusted and untrusted surveillance system. However, the integrity and auditability with respect to information from the untrusted sources raises an issue. As an example, the airport ecosystem is used and video sources variety and several trusts involved in producing video surveillance information have been analysed in this research. The authorities issues not tampering video footage which assures about stored videos data integrity. The lightweight block chain technology used to validate the video integrity which are then save the video metadata as blockchain transactions. In this study, auditability and non-repudiation have ensured. Less latency seen in simulation results which are introduced by blockchain overhead.

[24] [25] For the industrial IoT, lightweight hash-based blockchain architecture has been proposed in the previous researches. Based on transaction rate, the hash function of block chain flexibly changed which further improve the block chain availability in network. In this proposed architecture, based on the terms of area, throughput and power consumption, three lightweight hash functions executed like QUARK, PHOTON and SPONGENT yields higher performance. It mainly implemented on resource constraint devices in smaller area and assures about cryptographic security. By flexible hash chain each data block was connected. Hence latency and computational complexity reduced. Some cells formed by the fields and cell nodes controlled it and hence scalability improved.

3. COMPARATIVE ANALYSIS:

The above reviews have been comparatively analysed and tabulated below:

S. No	Author	Advantages/Disadvantages	Description
1.	[12]	IoT –an emerging technology employed in mixed applications.	IoT definition, features, applications, functions and future scope discussed.

2.	[10]	Various security measures from various IoT frameworks known.	8 IoT framework for IoT applications implementation. Security mechanism.
3.	[11]	Better performance in terms of security.	IoT applications implemented privacy platform technique with decentralized system
4.	[13]	Ensure security against smart home threats.	IoT application in smart home, security vulnerabilities and the methods against them.
5.	[14]	Secure against many attacks. Feasible authentication mechanism. Need improvised security mechanism.	Authentication mechanism in WSN for distributed IoT applications.
6.	[15]	Secured against many attacks. Less-expensive operations used since lightweight concept followed. Memory requirement needs to be focused.	Lightweight biometric system depends multi factor remote authentication.
7.	[16, 17]	Blockchain in-build security measures analysed and the solutions against attacks found.	Blockchain BC integration and its decentralized features on IoT challenges related to security measures against vulnerable attacks.
8.	[18]	Security ensured and also efficiency and low cost.	Decentralized system namely bubbles of trust proposed using Ethereum block chain.
9.	[1] [19]	Ensures scalable, generic end and easy to manage IoT access control system features and acquires flexibility.	Decentralized access system in BC handled scalability and other issues in constrained IoT devices.
10.	[20]	Processing time, energy consumption and traffic in this proposed method have been unimportant when compared to the gains achieved in privacy and security.	Smart home setting to ensures block chain security and privacy. Three tiers consists of cloud storage, overlay and smart home presented.
11.	[4, 21]	Many of the blockchain systems in lack of security and it should be enhanced.	Blockchain security risks and the real attacks surveyed.
12.	[8]	Privacy and security enhanced to high level. Processing time reduced.	Lightweight scalable blockchain on IoT applications.
13.	[22]	In addition to privacy and security, little storage space used.	The Sensor-Chain lightweight scalable blockchain framework for resource constrained IoT devices.
14.	[23]	Non-repudiation and auditability. Less latency.	Data integrity in surveillance cameras using leveraging lightweight blockchain
15.	[24] [25]	Cryptographic security and scalability improved. Reduced latency and computational complexity.	For industrial IoT, lightweight hash-based blockchain architecture has been proposed. Three light weight hash functions chosen such as QUARK, PHOTON and SPONGENT implemented.

4. CONCLUSION:

This survey is mainly focused on challenges in IoT environments and its required security. The solution for the IoT requirements are further discussed and considered on the block chain technology and decentralization characteristics. The LSB overcame the challenges, lack of security and greater complexity and hence the light weight techniques are focused and discussed in this study. Thus, the LSB provides high level security in IoT environments have been identified in this review.

5. REFERENCES:

[1] O. Novo, "Blockchain meets IoT: An architecture for scalable access management in IoT," IEEE Internet of Things Journal, vol. 5, pp. 1184-1195, 2018.

[2] L. Atzori, A. Iera, and G. Morabito, "Understanding the Internet of Things: definition, potentials, and societal role of a fast evolving paradigm," Ad Hoc Networks, vol. 56, pp. 122-140, 2017.

[3] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," International Journal of Web and Grid Services, vol. 14, pp. 352-375, 2018.

[4] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," Future Generation Computer Systems, 2017.

[5] I.-C. Lin and T.-C. Liao, "A survey of blockchain security issues and challenges," IJ Network Security, vol. 19, pp. 653-659, 2017.

[6] V. Rakovic, J. Karamachoski, V. Atanasovski, and L. Gavrilovska, "Blockchain Paradigm and Internet of Things," Wireless Personal Communications, vol. 106, pp. 219-235, 2019.

[7] Y. Xu, G. Wang, J. Yang, J. Ren, Y. Zhang, and C. Zhang, "Towards secure network computing services for lightweight clients using blockchain," Wireless Communications and Mobile Computing, vol. 2018, 2018.

[8] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Lsb: A lightweight scalable blockchain for iot security and privacy," arXiv preprint arXiv:1712.02969, 2017.

[9] A. S. Sani, D. Yuan, W. Bao, P. L. Yeoh, Z. Y. Dong, B. Vucetic, et al., "Xyreum: A High-Performance and Scalable Blockchain for IIoT Security and Privacy," in 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS), 2019, pp. 1920-1930.

[10] M. Ammar, G. Russello, and B. Crispo, "Internet of Things: A survey on the security of IoT frameworks," Journal of Information Security and Applications, vol. 38, pp. 8-27, 2018.

[11] A. Alcaide, E. Palomar, J. Montero-Castillo, and A. Ribagorda, "Anonymous authentication for privacy-preserving IoT target-driven applications," Computers & Security, vol. 37, pp. 111-123, 2013.

[12] K. K. Patel and S. M. Patel, "Internet of things-IOT: definition, characteristics, architecture, enabling technologies, application & future challenges," International journal of engineering science and computing, vol. 6, 2016.

[13] S. Yoon, H. Park, and H. S. Yoo, "Security issues on smarthome in IoT environment," in Computer science and its applications, ed: Springer, 2015, pp. 691-696.

[14] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, and M. Ylianttila, "Two-phase authentication protocol for wireless sensor networks in distributed IoT applications," in 2014 IEEE Wireless Communications and Networking Conference (WCNC), 2014, pp. 2728-2733.

[15] P. K. Dhillon and S. Kalra, "A lightweight biometrics based remote user authentication scheme for IoT services," Journal of Information Security and Applications, vol. 34, pp. 255-270, 2017.

[16] A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito, "Blockchain and iot integration: A systematic survey," Sensors, vol. 18, p. 2575, 2018.

[17] X. Wang, X. Zha, W. Ni, R. P. Liu, Y. J. Guo, X. Niu, et al., "Survey on blockchain for Internet of Things," Computer Communications, vol. 136, pp. 10-29, 2019.

[18] M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, "Bubbles of Trust: A decentralized blockchain-based authentication system for IoT," Computers & Security, vol. 78, pp. 126-142, 2018.

[19] R. Xu, Y. Chen, E. Blasch, and G. Chen, "Blendcac: A blockchain-enabled decentralized capability-based access control for iots," in 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2018, pp. 1027-1034.

[20] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in 2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops), 2017, pp. 618-623.

[21] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," Future Generation Computer Systems, vol. 82, pp. 395-411, 2018.

[22] A. R. Shahid, N. Pissinou, C. Staier, and R. Kwan, "Sensor-Chain: A Lightweight Scalable Blockchain

Framework for Internet of Things," in 2019 International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2019, pp. 1154-1161.

[23] R. A. Michelin, N. Ahmed, S. S. Kanhere, A. Seneviratne, and S. Jha, "Leveraging lightweight blockchain to establish data integrity for surveillance cameras," arXiv preprint arXiv:1912.11044, 2019.

[24] B. Seok, J. Park, and J. H. Park, "A Lightweight Hash-Based Blockchain Architecture for Industrial IoT," Applied Sciences, vol. 9, p. 3740, 2019.

[25] Y. Liu, K. Wang, Y. Lin, and W. Xu, "$\mathsf {LightChain} $: A Lightweight Blockchain System for Industrial Internet of Things," IEEE Transactions on Industrial Informatics, vol. 15, pp. 3571-3581, 2019.