A Security Framework for A Sustainable Smart Ecosystem using Permissioned Blockchain: Performance Evaluation

George Gabriel Richard Roy, S. Britto Ramesh Kumar

Abstract**: *This world always revolves around technology. There is always some disruptive technology that topples down any technology that people normally consider as a de-facto standard or norm. The Internet was one of these disruptive technologies which turned the whole way of how people were communicating with each other. It has revolutionized computing and communication. After a few decades of disruption, today people have accustomed to make their jobs easier with automation, remote control over the Internet, unsupervised actuation etc., This is all feasible with the advent of Internet of Things (IoT). IoT is one of the disruptive technologies of this era. Consumers of IoT are of different sorts ranging from, normal home automation to space engineering. These consumers share important details in these IoT networks which are susceptible to attacks from intruders who abuse the flaws of the IoT network for their own benefit. IoT security is one of the major concerns among all the issues of implementing an IoT based solution. Blockchain another disruptive technology is amalgamated to form a robust secure Smart Home Ecosystem. An Ecosystem is designed to incorporate IoT and Blockchain seamlessly. Where services could be automated and operated in a secure manner. This paper proposes the performance results of a Security framework for a Sustainable Smart Ecosystem using permissioned Blockchain.***

Keywords: **Blockchain, IoT Security, Smart Ecosystem, Disruptive Technologies.**

I. INTRODUCTION

People have always sought the aid of technology in their everyday life. From the very dawn of life till now people are making use of tools to make their life easier, with the advent of digital technology, the way that tools get incorporated into a person's life is almost seamless. Although the lesser tech-savvy consumers are the ones who just prefer to get the job done and don't worry about the intricate details of the underlying technology. Especially with upcoming Disruptive Technologies (DT) like Internet of Things (IoT), Artificial Intelligence (AI) and Blockchain (BC) the intricate details are too complex for an end user to understand. IoT as a DT has infiltrated into everyday life thanks to its pervasive nature and its versatility to adapt to any scenario. IoT is used in almost all industries [1], ranging from Agriculture to Supply Chain Management, this versatility makes IoT the candidate for many automation implementations. IoT works on things which are normally living or non-living objects that could be uniquely identified over the Internet with an IP address. These things have sensors/actuators and perform specific functions according to what they are programmed to do. With IoT almost all the objects in an environment can be connected to each other for communication and transmission of information. IoT can connect many types of appliances, electronic devices, huge machines, small sensors and actuators the list is almost endless, all this to aid humans to bring better productivity. IoT devices that are capable to transfer and manipulate data, identify other devices are said to be Smart Devices. With Smart Devices in the IoT system, humans can use it to locate, track, identify, monitor and perform actions based on the input received [2]. These complexities of connecting and the communication between devices are not know to the end users and the network operations are also not known to them in the case of a Smart Home scenario. With the exponential rise in adapting IoT so does the risk for privacy of data and rise of vulnerabilities rises [3]. Security is lacking in these IoT implementations which poses a serious threat to the people using it. The attackers are getting smarter every day and they utilize tools to find loop holes, backdoors, and other vulnerabilities to compromise the system. Unauthorized access to the system, denial of service attacks, snooping and eavesdropping are some of the attacks performed on these networks. To protect the valuable data and to facilitate uninterrupted data and service availability the security for these networks are to be strengthened. Blockchain is another one of the DTs. It was popularized after Satoshi Nakamoto created a version of it for the cryptocurrency platform Bitcoin. Contrary to popular belief Bitcoin is not blockchain. Blockchain is an immutable decentralized ledger which store transactions which is done between two nodes on its linked list like structure with cryptographic hashes without the need of a third party to authenticate the transaction, thereby eliminating the need for a middleman. Initially blockchain was only used for cryptocurrency like Ethereum, Bitcoin etc., as the popularity grew many jumped on the bandwagon and started polluting them market with Initial Coin Offerings (ICOs) [2]. With all that pollution in the market there was disorder and confusion among the cryptocurrency providers which lead to the downfall.

Manuscript published on 30 August 2019.
*Correspondence Author(s)

George Gabriel Richard Roy, Department of Information Technology, St. Joseph's College, Trichy, India.
Dr. S. Britto Ramesh Kumar, (Research Supervisor), Department of Computer Science, St. Joseph's College, Trichy, India.

Although many has seen the potential of blockchain as a technology which could fit in various domains with little tweaks. Blockchain is based on peer to peer communication and it is generally distributed and decentralized in nature [10].

Considering the nature of IoT Security and the secure nature of blockchain it would be a seamless integrated security system to provide optimal results.

This paper is structured as follows, section II contains the related work pertaining to the proposed work, section III contains a brief gist of the proposed framework which this paper's results are based upon, section IV has the results and discussion of the proposed work and section V concludes this paper.

II. RELATED WORK

Pundir et al. Discussed in their work on how blockchain could be used to work along with IoT, they proposed that the data from the sensors, identification of the IoT devices, authentication all could be done on the blockchain. In this way the genuine data would not be corrupted by attackers with malicious intent, also providing a secure identification of the devices instead of relying on a middleman to establish trust. They also proceeded to mention that single source of failure could be eliminated if blockchain is used as a distributed ledger among many peers, whereas the operational cost and the response time could be reduced, including the deployment of the system could be economical. In their paper they have presented an idea of how IoT can work along with blockchain to facilitate digitization of supply chain management, they mentioned that the complementary combination of IoT and Blockchain has the potential to be a very powerful model which paves way to significant changes in the productivity of supply chain, Smart Contracts enables automated processes can could be a game changer in how business operates in the present [4]. Although they presented a theoretical model for the supply chain in general without exacting the model without explicit regard to security.

Sun et al., devised in their work about the optimal communication between Wireless Internet of Things and Blockchain based on the deployment of nodes, they established a model to analyze their system by considering spatiotemporal Poisson distribution. The main objective of their work was to determine the node deployment of their blockchain system to provide optimal results, maximizing the throughput and analyzing the security performance by exposing their system to typical attacks focusing on protecting the physical layer with their algorithm [5].

Tang et al., has described in their paper that cross-platform collaboration always yields in better user experience because of the needs of the user and the products that the vendors distribute are fragmented in time. They proceed to mention that centralized systems propose a challenge of establishing trust that drastically limits the scalability of the system and making it less diverse. They propose a decentralized trust framework called IoT Passport which facilitates the platforms to establish trust by proposing and adapting to rules which are pre-set for collaborations among the participating peers in the blockchain through smart contracts. All transactions are stored on the blockchain and the records are used to authenticate and authorize services and end users [6]. They have developed a multilayer architecture with reference to traditional IoT models.

Dorri et al. proposes a private and secure model of the combination of blockchain and IoT for Smart Homes, in this proposal they adapt a miner which is a high-end device that acts as the central node for the transactions and consensus. They propose to protect the Smart Home system from attacks that jeopardize the integrity, confidentiality and availability of data and services. They take the Bitcoin blockchain into contemplation and discussed various types of transactions and components associated with it, although using a blockchain designed for public usage will reduce the chances of a good scalable model [7]. However, depending on a miner for the tasks at hand poses a risk if that miner fails.

Just by using cryptographic hashes and distributed consensus does not mean that the data which is stored on a blockchain is secure, stated Dedeoglu et al. in their work on a trust architecture for blockchain in IoT. They state that blockchain in its normal state does not provide trustworthiness of the data from where it is originated so they have proposed a layered architecture to improve the end-to-end trust to be adapted by various IoT applications. The nodes are designed in such a way that they report to the gateways to calculate the trust and the reputation of the sensor. Data trust is been implemented on a custom private blockchain to achieve optimal performance analysis [8].

III. METHODOLOGY

Fig. 1. Denotes the previous work on which this paper is based upon, a Security Framework for A Sustainable Smart Home Ecosystem [9], where the concept of a multichain model is implemented. It is divided into three chains, the Ecosystem Home Chain (ESHC), the Ecosystem Core Chain (ESCC), and the Ecosystem Service Chain (ESSC). The ESCH is the home to all the sensors and the actuators, IoT Devices, Appliances, Gateways and Routers, it is responsible for all the sensing and automation that takes place in the Smart Home. The devices are connected to the gateways and the identity of the devices are managed by blockchain which is exclusive to the Smart Home. The Service requests originate from the ESHC and go through the service manager to the ESCC to invoke the smart contracts depending on the type of the request. The requests for services are then forwarded to the respective ESSCs with the help of the smart contracts and the responses are provided back to the requester if all the conditions are met.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

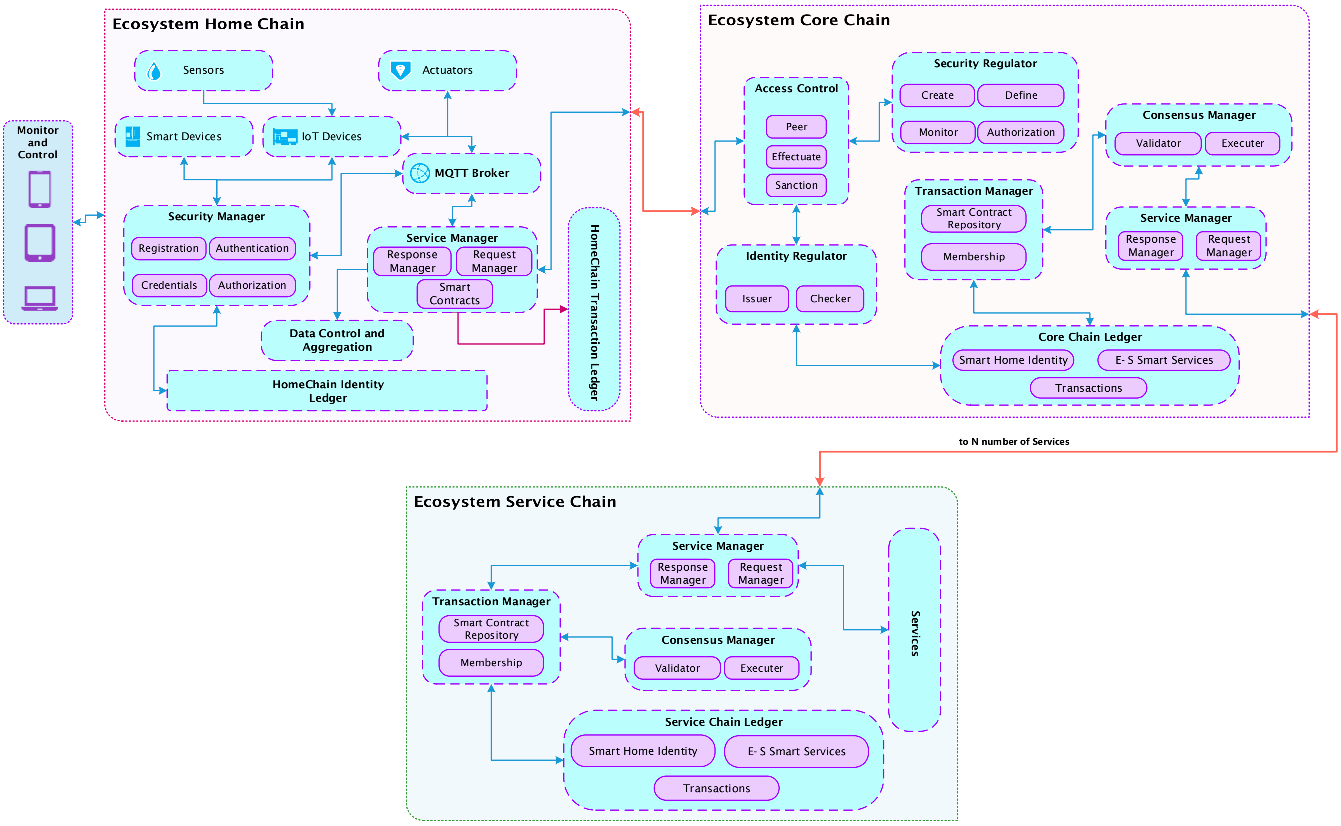

Fig. 1. A Security Framework For A Smart Ecosystem Using Permissioned Blockchain

IV. RESULTS AND DISCUSSION

The user interface and the blockchain of the proposed system is implemented in Python, HTML, CSS, JavaScript, PHP with MySQL and Hyperledger Fabric. JavaScript, Arduino C, Node Red and Python are used to code IoT devices and Gateways. The performance of the proposed system is tested using benchmarking tools Gauge and Caliper and the results are displayed in the form of charts. The results displayed below are retrieved by benchmarking the system.

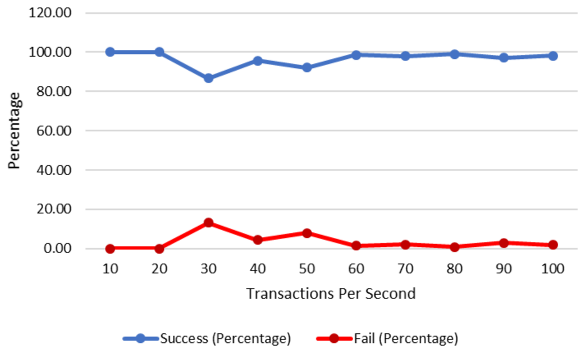

Fig. 2. Transaction Performance Analysis

Fig. 2. Represents the success rates of the number of transactions per second(tps) that have succeeded to find if the system is able to take on the load. It was found that in an average 96.59 % of transactions were successful.

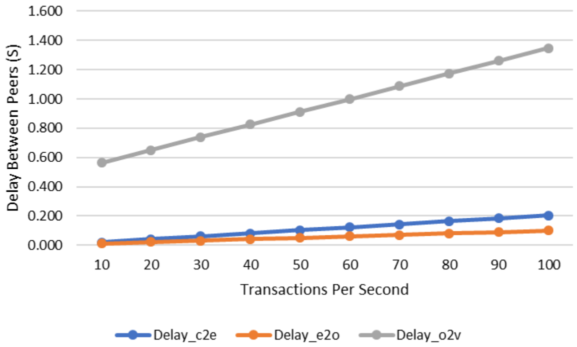

Fig. 3. Transaction Delay Between Peers

Fig 3. Shows the transaction delay between the peers, from committers to endorsers, endorsers to orderers and orderers to verifiers, it was found that the rate of delay is minimal and there is considerably slight increase in the delay as the tps increases.

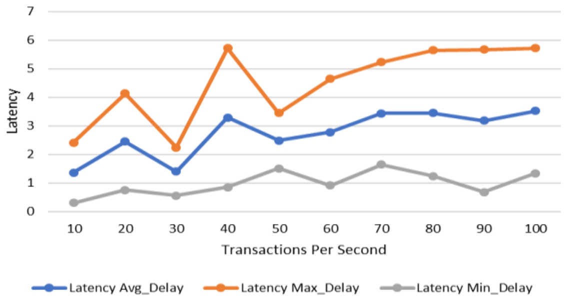

Fig. 4. Transaction Latency

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

Fig. 4. Shows the transaction latency with respect to the transactions per second, although there were random spikes at the initial stages the latency was high but further on the average latency was normalized.

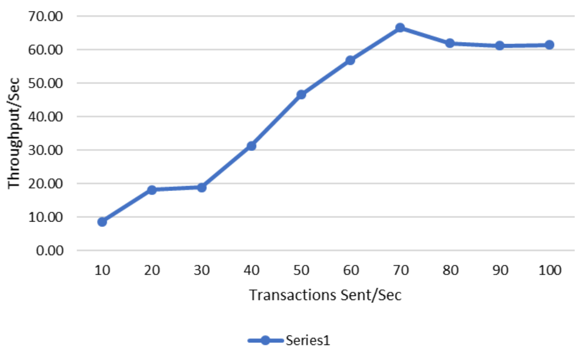

Fig. 5. Transaction Throughput

Fig. 5. Depicts the transaction throughput of the proposed system, the throughput is calculated by the total number of committed transactions divided by the total time in seconds at the node that it was committed on. Here the throughput is the rate where valid transactions are completed by the proposed system at the defined period.

V. CONCLUSION

Security in IoT networks is still considered to be a major concern especially in a home automation environment. Consumers are unaware of the threats they face on an insecure network and the amount of valuable data and resources they could lose. Thus, a security framework was proposed for a Sustainable Smart Home Ecosystem using permissioned Blockchain to mitigate those threats. Since IoT deals with resource constrained devices, the underlying technology should not be too demanding. Therefore, this paper shows the results of the system when implemented in a resource constrained environment and the benchmarks show that this system is scalable and would be effective and secure at the same time. The success rate of the proposed work was found to be 96.59%. The average latency is minimal so transactions will have a good response time. As future work the security analysis of this proposed framework could be performed and a mathematical model could be designed.

REFERENCES

1. M. Shyamala Devi, R. Suguna, Aparna Shashikant Joshi, and Rupali Amit Bagate, “Design of IoT Blockchain Based Smart Agriculture for Enlightening Safety and Security,” Springer Nature Singapore Pte Ltd ICETCE 2019, CCIS 985, pp. 7–19, 2019.
2. Qin Wang, Xinqi Zhu, Yiyang Ni, Li Gu, Hongbo Zhu, “Blockchain for the IoT and industrial IoT: A review,” Internet of Things, Elsevier, July 2019 (Accepted for Publication – In Press).
3. Ali Dorri, Salil S. Kanhere, and Raja Jurdak, “Blockchain in Internet of Things: Challenges and Solutions,” arxiv, 2016.
4. Kumar Pundir, Ashok & Devpriya, Jadhav & Chakraborty, Mrinmoy & Ganpathy, L, “Technology Integration for Improved Performance: A Case Study in Digitization of Supply Chain with Integration of Internet of Things and Blockchain Technology,” CCWC 2019, pp. 0170-0176, 2019.
5. Y. Sun, L. Zhang, G. Feng, B. Yang, B. Cao and M. A. Imran, "Blockchain-Enabled Wireless Internet of Things: Performance Analysis and Optimal Communication Node Deployment," in IEEE Internet of Things Journal, vol. 6, no. 3, pp. 5791-5802, June 2019.
6. Bo Tang, Hongjuan Kang, Jingwen Fan, Qi Li, and Ravi Sandhu, “IoT Passport: A Blockchain-Based Trust Framework for Collaborative Internet-of-Things,” In Proceedings of the 24th ACM Symposium on Access Control Models and Technologies (SACMAT '19), ACM, New York, USA, 83-92, 2019.
7. Dorri, Ali & Kanhere, Salil & Jurdak, Raja & Gauravaram, Praveen., “Blockchain for IoT Security and Privacy: The Case Study of a Smart Home,” 10.1109/PERCOMW.2017.7917634, 2017.
8. Volkan Dedeoglu, Raja Jurdak, Guntur D. Putra, Ali Dorri and Salil S. Kanhere, “A Trust Architecture for Blockchain in IoT,” arXiv:1906.11461v1 [cs.CR] 27 June 2019.
9. George Gabriel Richard Roy, Britto Ramesh Kumar. S, “A Security Framework for a Sustainable Smart Home Ecosystem using Permissioned Blockchain,” JETIR, Volume 6, Issue 3, pp 489-497, March 2019.
10. A. Baliga, N. Solanki, S. Verekar, A. Pednekar, P. Kamat and S. Chatterjee, "Performance Characterization of Hyperledger Fabric," 2018 Crypto Valley Conference on Blockchain Technology (CVCBT), Zug, 2018, pp. 65-74.

AUTHORS PROFILE

George Gabriel Richard Roy has completed his Masters in Computer Applications, Masters in Philosophy Computer Science, and is Currently pursuing his PhD in Computer Science in the Field of IoT Security. He currently serves as an Assistant Professor in the Department of Information Technology, St. Joseph’s College, Tiruchirappalli, Tamil Nadu, India.

Dr. S. Britto Ramesh Kumar is an Assistant Professor of Computer Science at St. Joseph’s College (Autonomous), Tiruchirappalli. His research interests include software architecture, wireless and mobile technologies, information security andWeb Services. He has published many journal articles and book chapters on the topics of Mobile payment and Data structure and algorithms. His work has been published in the International journals and conference proceedings, like JNIT, IJIPM, IEEE, ACM, Springer and Journal of Algorithms and Computational Technology, UK. He was awarded as the best researcher for the year 2008 in Bishop Heber College, Tiruchirappalli. He has completed a minor research project. He has visited countries like China, South Korea and Singapore.