Blockchain Technology using System Requirement Specification and IoT Devices

Greeshma PP[1], J S Rajashekar[2]

Student[1] , Professor[2], Department of Electronics and Instrumentation Engineering
Dayananda Sagar College of Engineering, Bangalore, India

---***---

Abstract - *The Internet of Things (IoT) is a network connected objects like sensors; actuators, electronics and software that are future requirements of any industry and modern society. These embedded systems are made to provide state-of-the-art facilities to exchange data over the internet. IoT technology can be efficiently used in various sectors like agriculture, healthcare, transportation, water and wastewater management, product manufacturing, power generation & distribution etc. Blockchain has emerged as a key technology is quickly rising to the top, especially considering its widespread use. The integration into workplace networks still faces some difficulties. IoT raises security and privacy issues because data authentication and exchange are handled solely through the central server. The main server model and blockchain technology is added while a component about IoT to label such certainty and problems. Three primary characteristics, namely, extensibility, inactivity, and network longevity, impact security measures without them, internal attack mitigation would be difficult. Using block chain can upgrade net conservation, efficiency and certainty. Recovery after events is fairly simple because the block chain stores the entire history of modifications to device configuration.*

Key Words**: Blockchain Technology, Internet of Things (IoT), Sensors, Embedded Systems, Data authentication**

1. INTRODUCTION

Data is gathered from multiple selector, sensors, and apparatus in a manufacturing setting the right to approach and command the data, is the data itself. It is being created by things that are allowing on the Internet, like Industrial IoT refers to such a circumstance (IIoT). The development of Industry 4.0 and the IIoT creates opportunities for connecting pre-programmed computer control schemes for remote observation and quick response to situations necessitating concurrent handling. Additionally, the use of sensors may result in a number of benefits over other industrial architectures. Blockchain, often known as a Distributed shared ledger, is a cryptographically protected, unchangeable store of information. Digital advantage can be traded and stored without the requirement for outside supervision. Devices that download configuration files from a centralized server must have confidence in that authority; otherwise, the device is susceptible. A blockchain eliminates the need for a centralized authority. Peer-to-peer is the direct exchange of strength between devices.

In Information technology, the term "Internet of Things" refers to the link between on-devices and the internet. The devices should be connected wirelessly, opening up new opportunities for system interactions as well as new possibilities for the management, succeeding, and initiation of improved service ability. IoT devices have performance and resource limitations by design when compared to network devices in enterprise contexts. When creating management and monitoring systems for IoT devices, this must be taken into account. IoT device heterogeneity employs multiple configurations and offers varied levels of monitoring for diverse reasons. Enterprise network settings similar device heterogeneity makes it possible to adapt current network monitoring and management tools for IoT implementation. As the backbone of communication within communities or businesses, undertaking networks and popular entrance networks are a commonly used presenting enabler globally. The entire enterprise sector is in constant need of stronger, more secure connection for all nodes. Networks are being developed systematically and are open to new ideas. The primary innovation need to be on the following crucial elements boosting network efficiency, boosting security, and decreasing using blockchain technology to save maintenance expenses.

The term "System Requirements Specification"(SRS) or "Requirements Specification" is used in the requirements engineering community to refer to a contract that details various practical issues of a structure, generally a firmware system and also sometimes a system that combines software and hardware. Throughout various phases of the forecast life cycle, an SRS is used to help the major stakeholders share the system's vision, as well as to streamline communication and the general project administration and system evolution processes. A better SRS offers a number of advantages, including establishing the foundation for accordance between the purchaser and the supplier providing a basis for approximate budget and programme, offering a control for confirmation and affirmation and serving is a foundation for future preservation activities. A SRS may further be included in contracts or request for proposals documents related to a project. A SRS typically attach to a predetermined arrangement that provides a specific document construction and additional useful suggestions. SRS templates must, by definition, be modified and tailored to the requirements of the company in question.

This stage involves determining the project's feasibility and presenting a business scheme that includes a very simple project outline and some cost evaluate. During system analysis, the feasibility of the suggested system must be studied. This will secure that the offered resolve won't put a tension on the company.

1.1. SYSTEM REQUIREMENT SPECIFICATION ON BLOCKCHAIN

A key document that establishes the framework for the process of product advancement is the System Requirement Specification (SRS). It includes a description of the structure's key feature in addition to its requirements. A SRS is simply an organization's assessment of a client's or potential client's operational needs and circumstances at a certain moment in time prior to any real outline or improvement work. It is a symbolic protection scheme that ensures especially at any specified time, the association and the customer are both aware of the requirements of exchange from that perspective. The inclusion of programming requirement information reduces effort required for advancement since careful review of the report can find oversights, false assumptions, and variability earlier in the improvement circle when they are secure to fix. Although the SRS may required to be modified, it does supply a substructure for moving forward with creation assessment. Simply said, determining the necessity of programming is the first step in every product improvement process. Decoding client thoughts and information into a formal archive is what the SRS refers to as the output of the prerequisite stage. Therefore, the stage's output is composed of formal requirements that are, ideally, complete and consistent, whereas the data lacks all of these characteristics.

Functional requirements specify how a software structure should work and counter to specific inputs or conditions. Computations, data clearing, and other limited functionality may be amidst them. One of the most crucial elements in terms of the overall mechanism of modules is the project's functional requirements. Fig 1 shows the entry details in the SRS software, Service providers can register, add device information, add privacy policies, and add device specifications. Transferred from the sensor to the server, the information is saved in the blockchain, the user has access to the sensor information, and the user can make payments. The framework must provide crucial security in addition to bug prevention and must prevent the entire process from collapsing. Security became a major worry for an association when innovation began to advance at a rapid pace. Giving security requires a significant investment of financial resources. Bug tracking ensures that unauthorized users can't access crucial issue data without permission while delivering the highest level of security currently possible. Multiple verified clients receive different mystery passwords from the bug-following framework, resulting in limited functionality for all clients.

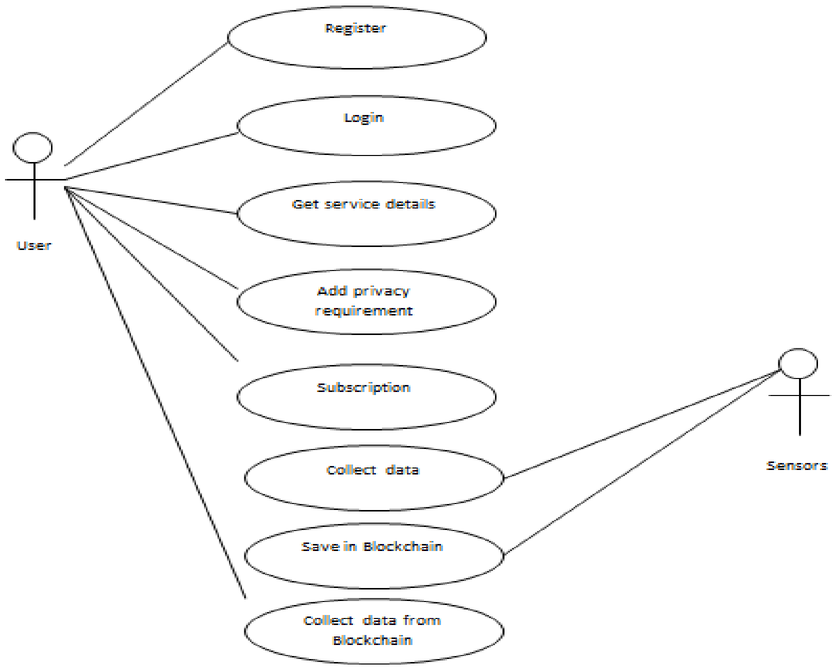

Fig 1: IoT devices registration on Blockchain.

The system will be used continuously by many factors. Performance becomes a significant consideration as the framework will be run on a unique web server and a single particular server that are both unseen. Although several customers are using the framework continuously, it shouldn't fail. All of its customers should be able to access it quickly. For instance, there shouldn't be any irregularity concurrently if two test specialists are simultaneously trying to notify the location of a bug.

1.2. IoT Blockchain

Focusing on the subsequent challenges, such as confirmation, exposure, and empirical of IoT or wireless sensors in the industrial platform, is necessary fully govern every smart device. We must make sure that the individuals tracking the product's manufacture or documentation are reputable and possess the appropriate credentials. Even though industry 4.0 uses smart devices to handle all data and activities, there are still some security concerns that could compromise sensors and IoT devices, hence exponentially slowing down corporate growth. Therefore, it is necessary to indexing each sensor that recognize data into the blockchain grid in order to give clarity and track whereabouts of each employee and product. Additionally, it is necessary to regularly gather and verify data from each registered IoT device. So that once the information or IoT/sensors are cast, nothing should be up to exchange, adjust, or path them. Blockchain technology, which allows for easy tracking of all device activities including data collection, product documentation, manufacturing, and shipment, can, however, resolve these concerns. The compromised sensor or device may enter the system fast or easily. As a result, before offering services, all IoT devices will schedule in the blockchain grid.

Prior to receiving assistance, IoT devices must schedule on the Blockchain grid. A contribution appeal must first sent to the grid, position will be checked by miner nodes. Additionally, miners use information-accessing devices to verify the authenticity or legality of each sensor. After successful confirmation or substantiation, miners will produce a split key that will aid in subsequent confirmation. Finally, utilising the shared key between squint junction and sensors, all sensors will assemble their allocate blink sensors. Each Internet of Things (IoT) device or user is connected to nearby or subscribing peer devices. Each organization or user must register on the blockchain grid in order to enjoy the services offered by the industry supplier. When a user requests a product from the industry, we have treated them as customers for the sake of our framework. Similar to this, we count an industry provider as a provider any time it ships the customer's order. Every time a user orders the shipment of a goods, they must register and construct their user profile on the blockchain. The user includes information about their identification, the product, payment details, etc. in that profile. The user can access or utilize the product once they have successfully registered. For product and service operations, security and privacy are crucial.

2. DISCUSSIONS AND RELATED WORKS

We can manage and keep track of any IoT device that is integrated into our blockchain infrastructure. If it require new arrangements or situations, a trusted customer adds them to the blockchain, where they are optionally or directly accessed by the IoT device. Middleware fetches fresh data and alerts users when a successful or a failed attempt. This implies that IoT network management can be decentralized. All configurations are known provenances, distributed, and immutable. The following traits are achieved by making use of blockchain technology. The succeeding challenges, such as confirmation, clarity, and empirical of IoT/wireless sensors in the production platform, need to be the emphasis of every smart device. We must make sure that the individuals tracking the product's manufacture or documentation are reputable and possess the appropriate credentials. Even though industry 4.0 uses smart devices to handle all data and activities, there are still some security concerns that could compromise sensors and IoT devices, hence exponentially slowing down corporate growth. The design that are communicated in the examine document and evolved in the outline phase are actually put into practice during the implementation phase. In order to provide the required final result, execution should be a flawless plot of the outline document in an appropriate programming language. Choosing the wrong programming language or using an inappropriate approach of programming frequently results in the product being damaged. It is ideal for the coding stage to be straight related to the outline phase in the sensation if the outline is in terms of object oriented phrase then execution should be ideally conveyed out in an object oriented approach.

Additionally, it is necessary to regularly gather and verify data from each registered IoT device. So that once the information or IoT/sensors are cast, nothing should be able to exchange, remake, or trace them. Blockchain technology, which allows for easy tracking of all device activities including data collection, product documentation, manufacturing, and shipment, can, however, resolve these concerns. Additionally, we must explain the necessary smart agreement just as we write the copy, rules, codes, and article between the organizations. Without any further interference, all sensor or IoT devices or junction can calculate their consensus outcomes. Using blockchain technology, each IoT device or user involved in the production or delivery of a product must first register or log in to the network in order to utilize or provide the services.

3. CONCLUSION

All sensor or IoT devices can compute their common results. Using blockchain technology, each IoT device or user involved in the production or delivery of a product must first register or log in to the network in order to utilize or provide the services. The IoT apparatus or sensors are gathered in the blockchain to track each sensor activity. In order to assure security and transparency among users in various locations, the blockchain project is typically utilized to forced details from sensors and to additionally conserve and extract it into blockchain. With the help of a blockchain mechanism and several security indicators, the suggested framework significantly increased the security of wireless sensors. The suggested framework is tested against the likelihood that an attack would succeed, the system's capacity to detect an assault, and a alteration attack. IoT could present a number of security and privacy concerns. These were found based on observations of the interactions between IoT components.

Only the alternatives for resolving the problems and difficulties in IoT is blockchain technology. The work describe the possibility for blockchain combination with IoT. The numerous IoT and blockchain technologies requisition were also discussed. This technology can be used for a variety of engineering services. But it is important to thoroughly research the precise consequences of each technology. Blockchain offers more freedom in how you can access the data.

REFERENCES

[1] Geetanjali Rathee, M. Balasaraswathi2, K. Prabhu Chandran3, Sharmi Dev Gupta4 C. S. Boopathi5. A secure IoT sensors communication in industry 4.0 using blockchain technology

[2] Kristián Koštál , Pavol Helebrandt, Matej Belluš , Michal Ries and Ivan Kotuliak. Management and Monitoring of IoT Devices Using Blockchain.

[3] Chanson, Andreas Bogner , Dominik Bilgeri , Elgar Fleisch , Felix Wortmann Leveraging, Blockchain Technology to Protect Sensor Data Mathieu. Privacy-Preserving Data Certification in the Internet of Things.

[4] Manoj Kumara ,Pradeep Kumar Mallickb.Blockchain technology for security issues and challenges in IoT Nallapaneni.

[5] Dr. D. Sivaganesan. A Data Driven Trust Mechanism Based on Blockchain in IoT Sensor Networks for Detection and Mitigation of Attacks

[6] Alberto Rodrigues da Silva , Jan Verelst , Herwig Mannaert , David Almeida Ferreira1 , Philip Huysmans. Effects Towards a System Requirements Specification Template that Minimizes Combinatorial.

[7] Sabah Suhail, Rasheed Hussain, Raja Jurda, Alma Oracevic, Khaled Salah, Raimundas Matulevičius, Choong Seon Hong, Blockchain-based Digital Twins: Research Trends, Issues, and Future Challenges.

[8] Suhail, Rasheed Hussain, Raja Jurdak, and Choong Seon Hong, Trustworthy Digital Twins in the Industrial Internet of Things with Blockchain,

[9] Günther Pernul and Marietheres Dietz. 2020. Unleashing the Digital Twin's Potential for ICS Security.

[10] Dimitris Geneiatakis, Ioannis Kounelis, Ricardo Neisse, Igor Nai-Fovino Gary Steri, and Gianmarco Baldini. Security and Privacy Issues for an IoT based Smart Home.

[11] Noria Foukia, David Billard & Eduardo Solana. PISCES: A Framework for Privacy by Design in IoT.

[12] Arijit Ukil, Soma Bandyopadhyay, Joel Joseph, Vijayanand Banahatti & Sachin Lodha. Negotiation-based Privacy Preservation Scheme in Internet of Things Platform.

[13] Jong-Hyouk Lee and Marc Pilkington. How the Blockchain Revolution Will Reshape the Consumer Electronics Industry.

[14] Christian Cachin. Architecture of the Hyperledger Blockchain Fabric.

[15] Nigel Davies, Nina Taft, Mahadev Satyanarayanan, Sarah Clinch, Brandon Amos. Privacy Mediators: Helping IoT Cross the Chasm.

[16]Fangyuan Sui, Fangfeng Cheng, Qinglin Qi, Meng Zhang, He Zhang, and Fei Tao. Big data-driven digital twin-driven product design, manufacturing, and service.

[17] Satoshi Nakamoto Bitcoin is a peer-to-peer electronic currency. Report on Technology. Manubot,2019. Journal of IoT in Social, Mobile, Analytics, and Cloud, June 2022, Volume 4, Issue 2 105

[18] Ibrahim Yitmen, Christopher Santi Götz, and Patrik Karlsson. 2020. The applicability, interoperability, and integrability of Blockchain-based digital twins for asset life cycle management are being investigated.

[19] Jiewu Leng, Guolei Ruan, Pingyu Jiang, Kailin Xu, Qiang Liu, Xueliang Zhou, and Chao Liu. 2020. A survey of blockchain-enabled sustainable manufacturing and product lifecycle management in Industry 4.0.

[20] Günther Pernul, Marietheres Dietz, and Benedikt Putz. 2019. A Distributed Ledger approach to Digital Twin data sharing security.

[21] Chao Zhang, Guanghui Zhou, Han Li, and Yan Cao, Manufacturing Blockchain of Things for the Configuration of a Data-and Knowledge Driven Digital Twin Manufacturing Cell, 2020.

[22] Günther Pernul, Benedikt Putz, Marietheres Dietz, Philip Empl, and Benedikt Putz. 2021. EtherTwin is a blockchain-based information management system for secure digital twins

[23] Andrea Urbinati, Claudio Mandolla, Antonio Messeni Petruzzelli, Gianluca Percoco, and Claudio Mandolla. A case study of the aerospace industry in creating a digital twin for additive manufacturing using blockchain technology.

[24] Xiongbing Fang, Sihan Huang, Guoxin Wang, Yan Yan, and Sihan Huang. 2020. For the digital twin of a product, blockchain-based data management is used.

[25] Haya R Hasan, Khaled Salah, Raja Jayaraman, Mohammed Omar, Ibrar Yaqoob, Saa Pesic, Todd Taylor, and Dragan Boscovic are among the members of the squad. 2020. A Blockchain-Based Approach to Digital Twin Creation.

[26] F. Shahid, C. Maple, A. Ahmad, and G. Jeon. A. Khan, F. Shahid, C. Maple, A. Ahmad, and G. Jeon. Spiral Digital Twin Framework and Twinchain for Smart Manufacturing Blockchain-based digital twins for the industrial internet of things

[27] Trond Kvamsdal, Adil Rasheed, and Omer San 2020. From a modelling standpoint, what are the benefits, constraints, and facilitators of a digital twin? [28] Chapter Thirteen - Empowering digital twins with blockchain. Pethuru Raj. 2021. Blockchain Technology for Secure and Smart Applications in a Variety of Industries

[29] J. S. Rajashekar , P. P. Greeshma. Blockchain-based Digital Twins for the Industrial Internet of Things

[30] Moily, Ashwini, Guru Prasanna, Keerthi S. Shetty, and Sanjay Singh. "Model checking message exchange in Location Based Services" , International Conference

[31] Shashank Kathar, Harsh Hardel, Zeeshan Alam, Shraddha Phansalkar, Rajani Sajjan. "Auction System for Agricultural Trade Using Blockchain Technology [32] J S Rajashekar, Greeshma P P .Blockchain for Industrial Internet of Things.

[33] Chao Wang, Wei Duan, Jianzhang Ma, Chenhui Wang. "The research of Android System architecture and application programming", Proceedings of International Conference on Computer Science and Network Technology.

[34] "Information Systems Design and Intelligent Applications", Springer Science and Business Media LLC, 2018

[35] Alberto Rodrigues da Silva. "Linguistic Patterns and Linguistic Styles for Requirements Specification (I)" , Proceedings of the 22nd European Conference on Pattern Languages of Programs - EuroPLoP '17, 2017.