BIIoT: Provenance of Industrial IoT Data with Blockchain Technology

J. Chandra Priya[1*], S. Puvaneswari[2], Shibani Raju[3]
[1, 2] Assistant Professor, Department of Computer Science and Engineering, Kings College of Engineering, Pudukkottai, India
[3]PG Scholar, Department of Computer Technology, Anna University MIT Campus, Chennai, India

Abstract **- The Internet of Things (IoT) is the collection of internets connected devices that are embedded with electronics, sensors, and hardware that can be observed and controlled. IoT appears to be a double-edged sword: it has a range of possibilities for ultra-low-power communications and makes such communication vulnerable to malicious attacks because all IoT devices are wireless. To improve security in IoT devices, blockchain technology is utilized here. Hybrid industrial architecture is used for various branches of an organization and is located in more than one country. Although IoT devices are used in several organizations, they reduce their product prices along with improving quality. Various threats can occur in IoT devices perpetrated by different intruders. Attackers compromise IoT devices by performing malicious activities. For example, a company's workers can steal some product. Blockchain technology is used to provide privacy and protect the control system in real-time conditions to prevent such problems. In this paper, the researcher has discussed using a Blockchain mechanism to extract data from IoT devices and keep the blockchain records to maintain transparency among different users located at different places.**

Keywords - Internet of Things, Industrial Internet of Things, Blockchain, Data Provenance

I. INTRODUCTION

An Internet of Things (IoT) network is formed with the networking of internet-connected devices that are embedded with electronics, sensor devices, and other hardware that can be remotely observed and controlled. Things on the Internet can be associated with an automobile with sensors imparted to notify the driver when tire pressure is reduced, or any natural or human-made item dispensed an IP can move information over a system. Differently, enterprises utilize IoT to work all the more productively, better comprehend clients to convey upgraded client assistance, improve essential leadership, and increment the business's estimation. IoT is not a Internet-associated buyer gadget. IoT is the innovation that manufactures frameworks fit for detected by its own and reacting to upgrades from this present reality without human intercession. To build up a strategy stream for a distinct structure over which an IoT arrangement is assembled.

Actuators are a thing regarding the Internet of Things, ought to be outfitted with sensors and actuators in this manner enabling to produce, acknowledge, and procedure signals**.** Data Acquisition Systems is the sensors' information begins in simple structure and changed over into computerized streams for further examination. Information procurement frameworks play out these information agglomeration and transformation techniques**.** Edge Analytics is the IoT information that has been digitalized, collected, and might require further handling before it enters the server farm. Cloud Analytics is the **i**nformation that needs extra top to bottom procedure gets sent to physical server farms or cloud-based frameworks.

II. RELATED WORKS

Yigit et al (2019) proposed a system the Internet of Things (IoT) contains a different gathering of sensors, actuators, and alternative Internet-connected devices communicating, processing information, and performing a different technique. Attack graphs give analytical support to stop multi-step network attacks by showing all potential sequences of vulnerabilities and their collaborations. Attack graphs generally consist of a vast number of nodes, and it is computationally challenging to analyze them for network hardening—greedy algorithm using compact attack graphs to search for a cost-effective solution to secure IoT frameworks. The algorithm scales almost linearly with the network size, and it tends to be applied to enormous-scale graphs with an incredibly massive number of IoT nodes. In addition to network-hardening, the proposal measures the network's security level in each progression to exhibit the framework's vulnerability grade.

Huh et al (2017) proposed a technique Blockchain technology emerged as the next revolutionary technology. IoT gadgets need to impart and synchronize with each other. The current model of server-client may have some limitations and issues while in synchronization. They were using blockchain to build IoT systems. Ethereum is our blockchain platform because using its smart contract, using Ethereum, blockchain computing platform. To save data coming from meter and smartphone. Using an Ethereum account, the meter continually sends power. Technology does not need to worry about synchronization and denial of service attacks while serving them productively and quickly.

Lundqvist et al (2017) proposed a system of thing-to-thing payments is a critical empowering influence in the Internet of Things (IoT) era, to ubiquitously allow for gadgets to pay each other for services with no human interaction. Blockchain technology is Bitcoin, with its decentralized structure and simplicity of record creation. A crucial drawback is the exchange expenses in the Bitcoin network when doing microtransactions. The proof-of-concept shows that trustless, self-ruling, and ubiquitous thing-to-thing micro-payments is no longer a future innovation. One severe

limitation the authors tend to establish was the high bitcoin transaction fee for micropayments. The work implemented a single-fee micro-payment protocol to reduce this cost, which aggregates multiple smaller transactions into one larger transaction, thus reducing value.

Puthal et al (2019) proposed a technique for the concept of proof of authentication (PoAh) for the light-weight implementation of blockchains in the Internet of Things (IoT). The IoT is on the vision to associate physical gadgets to the Internet and access remote information to control the distanced physical world. The building blocks of the IoT are objects or embedded devices that can be associated with the Internet. The IoT incorporates detecting, calculation, correspondence, recognizable proof, and semantics. PoAh removes the reverse hash function from PoW to light-weight the procedure. Accordingly, blockchains can efficiently integrate with resource-constrained networks such as the IoT and related applications. It also works proficiently in various leveled systems and mist computing scenarios.

J.Huang, et al (2019) proposed a modern system Internet of Things (IIoT) plays an indispensable role for Industry 4.0. IIoT systems are vulnerable to single points of failure and malicious attacks, which cannot provide stable administrations. Incorporating blockchain and the Internet of Things (IoT) increases extensive interest. The framework is constructed dependent on coordinated non-cyclic diagram organized blockchains, which is more efficient than the Satoshi-style blockchain in execution. The information authority management strategy can secure information protection without affecting the framework execution, which is also practical in the IIoT system. The outcome of extensive experiments and evaluation of the research work indicates that our system has a decent exhibition in IIoT. This work is critical to research in distributed IIoT systems by providing a practical DAG-structured blockchain-based agreement. The answer is suitable for smart factory and able to adapt to adjust to different IIoT situations.

J.Wan et al (2019) proposed a system, the Industrial Internet of Things (IIoT), a smart factory that has entered the booming period. However, as the number of nodes hikes, the network size becomes more extensive. The conventional IIoT architecture can no longer provide adequate support for such an enormous system. Therefore, the Blockchain architecture, which is an emerging scheme for constructing the distributed networks, to reshape the traditional IIoT architecture. First, the traditional IIoT architecture's serious issues are investigated, and the current enhancements are condensed. Second, the authors present a security and privacy model to help design the blockchain-based architecture. On this premise, the work disintegrates and reorganizes the original IIoT architecture to form a new multicenter halfway decentralized design. At that point, the researchers acquaint some relative security advances to improve and optimize the new architecture. After that, the researchers design the information cooperation process and the algorithms of the architecture. At long last, the researchers utilize a programmed generation stage to examine the particular usage.

M.Mohammadi et al (2015) proposed a system, the Internet of Things (IoT), emphasizing empowering innovations, conventions, and application issues. The IoT is empowered by the most recent improvements in RFID, smart sensors, correspondence innovations, and Internet conventions. The IoT environment is expected to smoothly switch diverse technologies to enable new applications by interfacing physical articles together on the side of smart, necessary leadership. The goal is to provide a more thorough summary of the most significant conventions and application issues to permit the researchers and application developers to quickly speed how the various conventions fit together to deliver desired functionalities. An outline for this idea, its enabling technologies, conventions, applications, and the recent research addresses various IoT parts. To improve the quality of life by connecting many smart devices, technologies, and applications.

Christidis et al (2016) proposed a technique Blockchains have recently attracted the interest of stakeholders over a wide range of enterprises: from finance, and healthcare, to utilities, real estate, and the administration division. The convergence of blockchains and IoT contexts can be truly incredible. Blockchains give us vital, truly distributed peer-to-peer networks and the capacity to associate with peers in a trustless, auditable manner. Smart contracts allows to automate complex multi-step processes. The devices in the IoT biological system are the points of contact with the physical world. The endnote is that the blockchain-IoT merging is vibrant and can cause significant transformations across several industries, paving the way for new business-case models and novel, decentralized applications.

Fernandez-Carames et al (2018) proposed a system that the IoT paradigm of the Internet of Things (IoT) is paves the way for a world where many of our everyday items are interconnected. A vision requires, in addition to other things, seamless authentication, information protection, security, power against assaults, and self-support. The most relevant BIoT applications are portrayed to accentuate how blockchain can affect conventional cloud-focused IoT applications. This work aimed to evaluate the practical limitations and identify areas—BIoT design, like its architecture, the required cryptographic algorithms, or the consensus mechanisms. The present difficulties and potential advancements are point by point concerning numerous angles that influence the plan, improvement, and arrangement of a BIoT application. The point of directing future BIoT specialists and designers on a portion of the issues that should be handled before sending the up and coming of BIoT applications.

Frustaci et al (2018) proposed a system Internet of Things (IoT) fuses with social networks to allow people and devices to interact and facilitating information sharing. Security and protection issues are an excellent test for IoT, yet they are likewise empowering components to make a "trust biological system." The IoT security panorama providing a taxonomic analysis from the perspective of the three main key layers of the IoT system model: 1) perception, 2) transportation; and 3) application levels. The IoT framework model's most powerless degree is the observation layer because of IoT gadgets' physical presentation to their compelled assets and their mechanical heterogeneity. Because of the examination,

the most fundamental issues with the point of controlling future research headings.

Y.Liu et al (2019) proposed a system the intersection of blockchain and the Industrial Internet of Things (IIoT) has received significant research interest research. The contention between the high asset prerequisites of blockchain and the, for the most part, short presentation of IIoT gadgets has not been all around handled. On the one hand, due to the presentations of numerical ideas, including Public Key Infrastructure (PKI), Merkle tree, and Proof of Work (PoW), deploying blockchain demands enormous computational resources. Conversely, full nodes should synchronize massive block information and manage various exchanges in distributed systems, whose control of capacity limit and data transfer capacity makes IIoT gadgets hard to bear. This paper proposed a light-weight blockchain system called LightChain, which is resource-proficient and suitable for power-constrained IIoT scenarios. A green consensus model known as Synergistic Multiple Proof stimulates IIoT devices' cooperation and a light-weight data structure called Light Block to streamline broadcast content. Block Offloading Filter to keep away from the boundless development of record without influencing blockchain's recognizability.

Kshetri et al (2017) proposed a technique blockchain is a data structure that enables a creation of a tamper-proof digital ledger of transactions and share them. This innovation uses public-key cryptography to sign transactions among parties. The ledger consists of cryptographically connected blocks of transactions, which form a blockchain. It is impossible or challenging to change or remove blocks of data—blockchain's role in improving by and extensive security in supply chain networks. With blockchain, it is possible to access changeless records for various transactions involving a product to understand critical vulnerabilities in the upstream production network. This innovation can likewise reinforce downstream production network accomplices' and gadget proprietors' preparatory and guarded cybersecurity measures recorded on the blockchain record.

Lee et al (2015) proposed a system Digital Physical Systems (CPS) is characterized as transformative advances for overseeing interconnected frameworks between its physical resources and computational abilities. Advanced information analytics, networked machines have the option to perform all the more productively, cooperatively, and versatilely. CPS can be additionally created for overseeing Big Data and utilizing machines' interconnectivity to arrive at the objective of intelligent, healthy, and self-versatile machines. A 5C design for Cyber-Physical Systems in Industry 4.0 assembling frameworks. It gives a suitable and pragmatic rule for assembling industry. To execute CPS for better item quality and framework dependability with increasingly canny and flexible assembling hardware.

Li et al (2015) proposed a system IoT is considered separate from the Internet of the future and comprises billions of intelligent communicating 'things. The Internet of Things (IoT) enables the associated things with new capabilities. The definitions, architecture, fundamental innovations, and applications of IoT are systematically investigated. The improvement of IoT includes numerous issues, for example, foundation, correspondences, interfaces, conventions, and models. Various activities have been produced for security and protection insurance, a dependable security assurance system for IoT is still sought after for information secrecy, security, and trust. Existing IoT uses have been grouped into business, interpersonal organizations, social insurance, foundation, security, and observation.

Zhang et al (2016) proposed a pervasive social network (PSN)-based healthcare system. Healthcare blockchain is used for the nodes to share health data with others. The central issue is how a PSN node can safely impart well-being information to different network nodes to understand the idea. A secure system for PSN-based healthcare. Two protocols are designed for the system. The first one is an improved version of the IEEE802.15.6 display authenticated association. The second protocol uses the blockchain technique to share health data among PSN nodes. Human body channels are proposed for PSN node in some utilization cases. The proposed framework outlines a potential technique for utilizing blockchain for PSN-based applications. The proposed technique can be stretched out to other PSN-based applications, including condition screen and transport. It improves the nature of individuals' life.

Zhao et al (2018) proposed a system Healthcare is a significant application scenario of blockchain, and utilized in medicinal services are called well-being blockchain. Blockchain blocks are open, and the transactions in them are public. If some security information is involved in these transactions, it is leaked. As the healthcare system involving a great deal of privacy data, specific security mechanisms must be built to protect these privacy data in health blockchain. The BSN and the health blockchain use the BSN's biosensor nodes to propose a light-weight reinforcement and effective recuperation conspire for keys of health blockchain. The core of security mechanisms is the key administration schemes, and the appropriate key administration schemes should be designed before blockchains can be used in the healthcare system. The core issue is designing an effective key administration scheme. A distinguished key can encrypt the blockchain with lower storage cost and high performance, and it significantly improves the security of physiological protection information on the health blockchain.

Lu et al (2017) proposed a system of IoT, Cyber-Physical System (CPS), Information and Communications Technologies (ICT), Enterprise Architecture (EA), and Enterprise Integration (EI). Regardless of the dynamic idea of the exploration of Industry 4.0. A comprehensive review of Industry 4.0 presents an outline of the substance, extension, and discoveries of Industry 4.0 by looking at the current written works in the majority of the databases inside the Web of Science. The improvement of industry is an incorporated procedure of multifaceted nature and nimbleness among humans and machines. Industry 4.0 expands the digitization

of assembling with CPS, wherein people and robots' associated systems connect and cooperate with data shared and dissected, upheld by enormous information and distributed computing along whole mechanical worth chains. Industry 4.0 expands cost-and time-proficiency and improves item quality related to empowering advancements, techniques, and instruments. The primary issue of the interoperability of Industry 4.0 proposes an applied edge work of interoperability for Industry 4.0.

Yang, et al (2017) proposed a system that develops centralized management systems. Risks in cyberspace, including personal data phishing, malicious code infection, hacking, and DDoS attack, are becoming significant issues in the real world. Blockchain, being a rapidly growing technology, promotes transaction records integrity and reliability by admitting for all network participants to combinedly own and verify data, which was previously done by a central server. The technology can cut down the brokerage fees and construction costs and guarantees high integrity and data security. The research applies blockchain innovation for safe information the executives. There are two types of nodes. The category includes representative nodes and participating nodes. A representative node can replace a proxy server of Fog Computing. Participating nodes can replace devices in Fog Computing. For easy search of identifiers, NDN based system is arranged. It proposes a framework highlighting expanded well-being utilizing square chain innovation as a technique to part and reestablish identifiers. Sensitive identifier scans be safely saved and managed through such an identifier split management system.

Fraga-Lamas et al (2019) Proposed a system the automotive industry has arguably transformed society, being one of the most unpredictable, refined, and mechanically propelled ventures, with advancements running from the crossover, electric, and self-driving vehicles. To the improvement of IoT-connected cars. Industry 4.0 technologies, like robotics, advanced manufacturing systems, cyber-physical systems, or augmented reality. The automotive industry is blockchain, enhancing its data security, privacy, anonymity, traceability, accountability, integrity, robustness, transparency, trustworthiness, and authentication and provide long-term sustainability and a higher operational efficiency to the whole industry. The most pertinent use cases, since the expansive selection of blockchain, opens a vast region of short-and medium-term promising car applications. The utilization of blockchain can give to the car business a stage ready to circulate trusted and digital versatile data that oppose current non-shared authoritative structures.

Zheng, et al (2019) proposed a technique Blockchain, the foundation of Bitcoin, has recently received extensive attention. Blockchain serves as an immutable ledger that allows transactions to take place in a decentralized manner. Blockchain has indicated its potential for changing the conventional industry with its essential qualities: decentralization, persistency, obscurity, and auditability. It introduces a thorough outline of blockchain innovation. An overview of blockchain architecture firstly and compare some typical consensus algorithms used in different blockchains. Blockchain-based applications are springing up, and we plan to conduct depth investigations on blockchain-based applications.

III. BLOCKCHAIN TECHNOLOGY

A blockchain is a continuous growing list of digital records in packages (called blocks) linked and secured using cryptography. These digitally recorded blocks of information are stored in a Sequence chain. Each blockchain block contains data (e.g., bitcoin transaction), is cryptographically hashed, and time-stamped. The blocks of hashed data tie upon the previous block in the chain. All data are ensured in the overall blockchain has not been tampered with and altered.

A. DECENTRALIZATION

Decentralization refers to any sort of innovation that has no overseeing authority by any associations. This is debatably the fundamental feature of crypto-innovation and blockchain innovation. The thing that builds cryptocurrencies like Bitcoin popular is that there is no administering authority over them and can be utilized for exchanges anyplace in the world between the clients. Since decentralization doesn't include any sort of focal hub and abandons a system of free, single clients, the idea of blockchain is this accumulation of clients itself.

B. SECURITY

The most significant concern for each individual who includes in cryptocurrency is its security. Security generally denotes both safety and privacy. If the so-called cryptocurrencies are not verifying enough, no one risks such insecure platforms for security. Various ways guarantee that the individuals have secure access to their contributed assets. One such strategy is utilizing crypto wallets, which have their digital address and can be a part of online assistance stages that interface you to a particular blockchain and enable you to purchase and sell.

C. SCALABILITY

Scalability defines the capacity to build its ability simultaneously to keep up smooth activities. It means to eliminate slow processing times, system bloating, lags. The Bitcoin blockchain generally gets expanded due to its immense popularity and on-demand. This system must be capable of handling multiple transactions every second. Nearly about millions of transactions per second. Therefore, to manage these loads of real-time transactional information, better equipment assets and infrastructure must be implemented.

IV. THE PROPOSED APPROACH

A web-based framework is bestowed to produce a higher understanding of the communication between a sender and receiver. Within the execution of the face network, that's the Blockchain system, and there are joined along as a system of peer nodes. In this, the joined that are a part of blockchain among some are thought-about as miners and are accountable for validating or adding a brand-new user within the network. Every dealings of each user is placed within the block that joins to create a Blockchain—a hybrid industrial design wherever different branches of a corporation are settled in additional than one country. Though IoT devices are utilized in several organizations and help reduce their production prices alongside rising quality, many threats occur in IoT devices initiated by varied intruders.

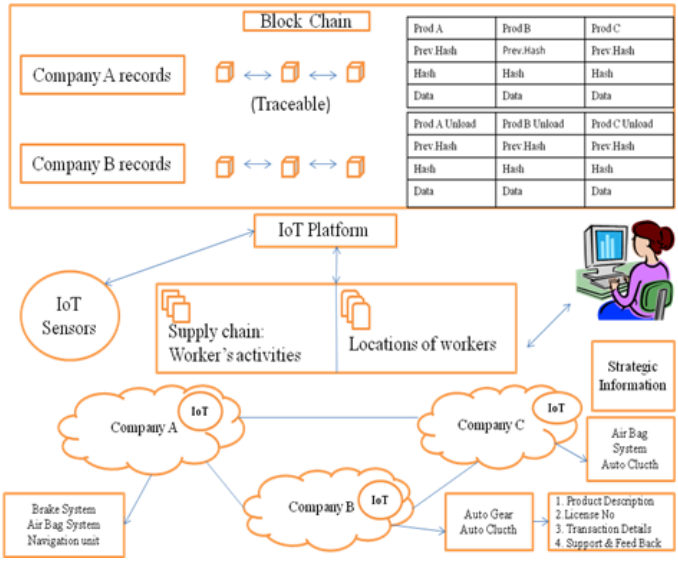

FIG.1. BIIoT: System Architecture

V. DETAILED DESIGN

A hybrid industrial architecture is situated at three different locations, where each entity is equipped with its internet technologies or IoT devices. If the company's headquarter is located on Main, it has all the rights to overlook, keep records, or examine all branches' activities in different locations. IIoT is advantageous because it monitors or controls all legal or illegal activities happening at any place from a single location. Devices with Internet Protocol (IP) connectivity are linked to the Internet to provide better usability in day-to-day activities. The industry principle is to collect, analyze, and record data and control entities' activities by automating real-time with reduced production costs and improved quality.

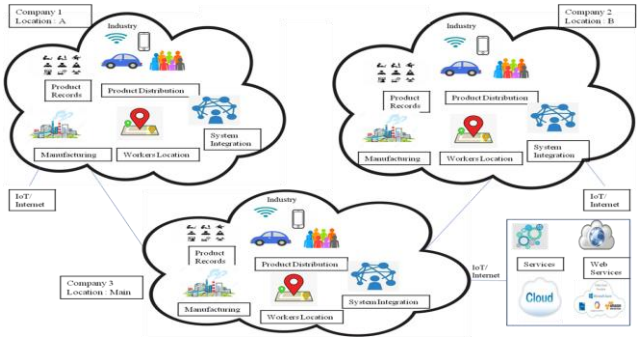

FIG.2. BIIoT: Detailed Design

Algorithm steps for consensus

Input: Block
Output: Validity of the block

1. Consensus(u)
2. Initialization:
3. Neighbour_nodes, new_chain
4. Max length,
5. For(node : 1 to n)
6. if(length(u)> max length)
7. Then
8. Max_length := length
9. new_chain := chain
10. assign new_chain := u
11. return True
12. Else
13. return False

VI. EXPERIMENTAL RESULTS

Bevywise simulator has been used to simulate the IIoT network from which the data has been acquired. It uses the MQTT protocol for data transfer between the devices and nodes of the IIoT network.

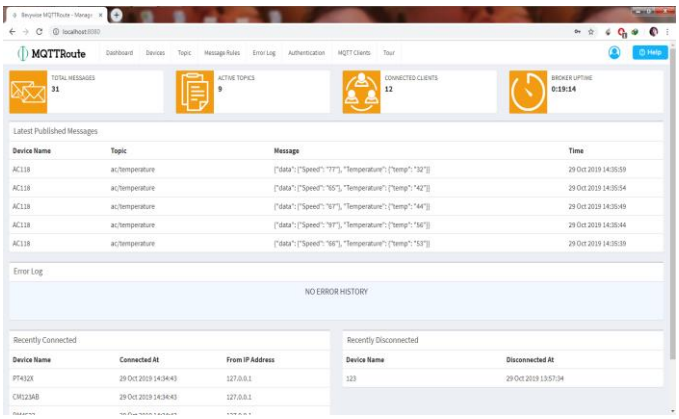

FIG.3. IIoT: Simulated Networking Environment

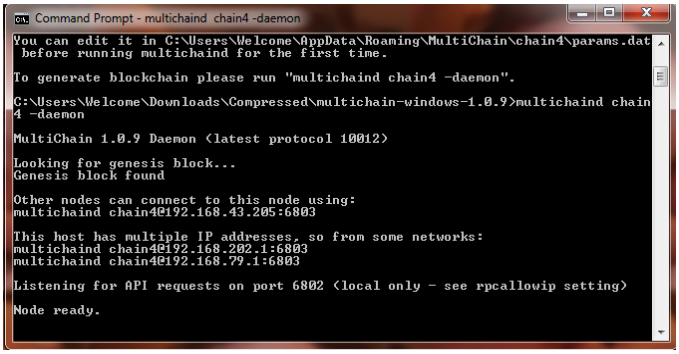

FIG.4. BIIoT: Simulated MultiChain Environment

The procedure of hand-shaking in a MultiChain environment occurs when the nodes in a blockchain connect. The identity of every node characterizes itself with an IP address with a list of permissions. Therefore the each node which it denotes sends a message to the other users. The peer-to-peer connection aborts if they do not receive any critical messages from the hand-shaking process.

FIG.5. BIIoT: MultiChain Transactional Environment

VII. CONCLUDING REMARKS

The automobile dataset to globalize the information agglomeration in IIot with the help of bevywise simulator, simulate the dataset used in the blockchain, store the data and any third party cannot influence it. The future work is to be extended with scalability for the integration of IPFS with blockchain and secure data management. Additionally, back traceability is achieved by using the supply chain.

REFERENCES

[1] Yiğit, B., Gür, G., Alagöz, F. and Tellenbach, B., (2019). 'Cost-aware securing of IoT systems using attack graphs'. Ad Hoc Networks, 86, pp.23-35.
[2] Huh, S., Cho, S. and Kim, S., (2017) February. 'Managing IoT devices using blockchain platform. In Advanced Communication Technology (ICACT)', 19th International Conference on (pp. 464-467).
[3] Lundqvist, T., de Blanche, A. and Andersson, H.R.H., (2017) June. Thing-to-thing electricity micro payments using blockchain technology. In Global Internet of Things Summit (GIoTS), 2017 (pp. 1-6).
[4] Puthal, D. and Mohanty, S.P., 2019. Proof of Authentication: IoT-Friendly Blockchains. IEEE Potentials, 38(1), pp.26-29.
[5] J. Huang , L. Kong , G.Chen, Min-You Wu,X. Liu, and P.Zeng: Towards Secure Industrial IoT: Blockchain System With Credit-Based Consensus Mechanism IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, VOL. 15, NO. 6, JUNE 2019.
[6] J. Wan , J. Li, M.Imran , Di Li, and Fazal-e-Amin: A Blockchain-Based Solution for Enhancing Security and Privacy in Smart Factory, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, VOL. 15, NO. 6, JUNE 2019.
[7] M., Mohammadi, M., Aledhari, M. and Ayyash, M., 2015. Internet of things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys & Tutorials, 17(4), pp.2347-2376.
[8] Christidis, K. and Devetsikiotis, M., 2016. Blockchains and smart contracts for the Internet of things. IEEE Access, 4, pp.2292-2303
[9] Fernandez-Carames, T.M. and Fraga-Lamas, P., 2018. A Review on the Use of Blockchain for the Internet of Things. IEEE Access.
[10] Frustaci, M., Pace, P., Aloi, G. and Fortino, G., 2018. Evaluating critical security issues of the IoT world: Present and Future challenges. IEEE Internet of Things Journal, 5(4), pp.2483-2495.
[11] Y.Liu, K. Wang , Y. Lin , and W. Xu , LightChain: A Lightweight Blockchain System for Industrial Internet of Things, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, VOL. 15, NO. 6, JUNE 2019.
[12] Kshetri, N., 2017. Can blockchain strengthen the Internet of things?. IT Professional, 19(4), pp.68-72.
[13] Lee, J., Bagheri, B. and Kao, H.A., 2015. A cyber-physical systems architecture for industry 4.0-based manufacturing systems. Manufacturing Letters, 3, pp.18-23.
[14] Li, S., Da Xu, L. and Zhao, S., 2015. The Internet of things: a survey. Information Systems Frontiers, 17(2), pp.243-259.
[15] Zhang, J., Xue, N. and Huang, X., 2016. A secure system for pervasive social network-based healthcare. IEEE Access,4, pp.9239-9250.
[16] Zhao, H., Bai, P., Peng, Y. and Xu, R., 2018. Efficient key management scheme for healthblockchain. CAAI Transactions on Intelligence Technology, 3(2), pp.114-118.
[17] Lu, Y., 2017. Industry 4.0: A survey on technologies, applications and open research issues. Journal of Industrial Information Integration, 6, pp.1-10.
[18] Yang, H.K., Cha, H.J. and Song, YJ, 2019. Secure identifier management based on blockchain technology in NDN environment. IEEE Access, 7, pp.6262-6268.
[19] Fraga-Lamas, P. and Fernández-Caramés, T.M., 2019. A Review on Blockchain Technologies for an Advanced and Cyber-Resilient Automotive Industry. IEEE Access, 7, pp.17578-17598.
[20] Zheng, Z., Xie, S., Dai, H., Chen, X. and Wang, H., 2017, June. An overview of blockchain technology: Architecture, consensus, and future trends. In Big Data (BigData Congress), 2017 IEEE International Congress on (pp. 557-564).