Blockchain and Edge computing for Industrial Internet of Things (IIoT) Applications.

Ankit Singh
School of Engineering and Technology,
CSE, Sharda University
Gr. Noida, U.P, India
2019004929.ankit@ug.sharda.ac.in

Shekhar Raghav
School of Engineering and Technology,
CSE, Sharda University
Gr. Noida, U.P, India
2020531085.shekhar@ug.sharda.ac.in

Prashant Kumar Senger
School of Engineering and Technology,
CSE, Sharda University
Gr. Noida, U.P, India
2019004893.prashant@ug.sharda.ac.in

Ashish Kumar
School of Engineering and Technology,
CSE, Sharda University
Gr. Noida, U.P, India
2019004894.ashish@ug.sharda.ac.in

Abstract-**Today IIoT is widely used in a wide range of Internet applications for items outside the consumer space and the iot business market, such as the umbrella name for applications and case applications in many industrial sectors. The goal of this paper is to highlight the ease of application of iiot(Industrial Internet Of Things) using Blockchain and Edge computing it also highlight various challenges of blockchain for iiot and with respect to that their approachable solutions. It also gives a detailed study of Deployment of edge computing in iiot sector.**

Keywords : IIoT, Blockchain, CIA

I. Introduction

Industry 4.0 points to a new phase in the Industrial Revolution that focuses more on communication, automation, machine learning, and real-time data. Industry 4.0, also sometimes called IIoT or smart production, combines physical production and digital technology, machine learning, and big data to build a comprehensive and better connected ecosystem for companies that specialize in asset management [4]. While every company and organization operating today is different, they all face the same challenge - the need to connect and achieve real-time understanding of processes, partners, products and people[1].

Emerging blockchain technology demonstrates a promising ability to develop industrial and Internet system logistics (IoT) by providing applications for demolition, unrepentant preservation, and crucifixion[5]. A few years ago, many more applications in industrial IoT (IIoT) have emerged and blockchain technology has attracted large number of attention from industrial and academic researchers[2].

The features and functionality of edge computing are what bring the various benefits associated with it and make it attractive to organizations. Understanding the automated and security benefits they offer, the deployment of an IIoT camera within the store creates an excellent environment for descriptive purposes[3]. An IoT camera installed inside the warehouse to capture staff behavior pattern will capture data about employee movement patterns, store traffic, and delay points. The IoT camera processor can also analyze store traffic and traffic patterns with the aim of saving only the contact data extracted from employees while discarding sensitive employee and physical data. Analytical links can be sent to a centralized system to drive new content management policies that eliminate traffic congestion and improve productivity.

In summary, the major contribution of our work is as follows-

- This work will give you a brief description of IIot, its background and its different technology categories for industry 4.0.
- This work will give an explanation about Security requirements in IIoT, its CIA Traids, Authentication, Access control, Data security and data sharing And network security.
- This work will describe about the blockchain based solutions for application of IIoT and about its hardware and software.
- Finally its will allow you to understand the role of Edge computing for IIoT, its deployment, reference architectures.

The remainder of paper is organized in 4 more sections in which Section 2 contains description of IIot, its background and its different technology categories for industry 4.0. Section 3 contains Security requirements in IIoT, its CIA Traids, Authentication, Access control, Data security and data sharing And network security. Section 4 contains blockchain based solutions for application of IIoT and about its hardware and software. And finally section 5 contains the role of Edge computing for IIoT, its deployment, reference architectures. And, At the end the conclusion of the paper.

II. Background of IIoT

A. Overview

IIoT is advanced version of Iot (Internet Of Things) dealing with synchronization of huge data making industrial work efficient. Iot is focused On small scale application like indoor localization, health-monitoring, smart home etc. [7] while IIoT works on large scale application like remote maintenance, smart logistics, intelligent factories etc.[8], and it is mainly production oriented. The fundamental structure of IoT is supposed to be designed from very basics on the other hand fundamentals of IIot are more focused on traditional industrial infrastructure. The devices in IIoT are fixed, generate large data, have negligible tolerance rate and large number of sensors with high precision are installed on the other hand in IoT devices are mobile, movable, have finite tolerance rate, no of sensors are less and they also have low precision.

The roots of IIot are spread around the widely known concepts like CPS, IOT, INDUSTRY4.0 and INDUSTRIAL INTERNET highlighting the deep bond of integration of many computer science driven technologies like sensing technology, hardware and software technology and embedded technology. IIot in business is very often used for optimization of production and to increase efficiency[10]. And for achieving this factories, companies and many big industries are trying to fetch and analyze data driven from production work and machines. This enhancement in industries from technology is widely known as sensor driven business [9]. Despite having advantages of IIot over old industry model there are some disadvantages which cannot be denied like security issues, trust and of tampering. And these cons are creating a big problem in the fourth industrial revolution[6]. In the modern setting, security is tended to by the CIA group of three (Confidentiality, Integrity, Authentication) [11] and by the requirement of correspondence channels and capacity. Then again, upholding security by bringing together the 115 control and the board of the framework could prompt trust gives that emerge when information is constrained by a solitary specialist among a few ones having a place with a similar consortium or market [12].

B. *Technology Categories for Industry 4.0*

In this section, we provide descriptions of the new categories of Industry 4.0. Indeed, these new classes were produced while leading the current experiment. Accordingly, we describe the new Industry 4.0 classes as follows.

Cyber Physical Systems deals with systems where physical and software objects are tightly integrated, enabling improved communication (i.e., data exchange) between different components in a number of ways.

The Internet of Things speaks of a network that provides communication between "objects" (i.e., objects or gadgets) through the sensors through data and the basis of communication technology, which brings constant discovery and stimulation of energy.

Big Data Analytics refers to training to find data that is integrated into large data sets (e.g., big data sets), collected on a variety of gadgets, using advanced comprehension techniques (e.g. data mining, statistical analysis, and forecasting analytics), which provides on-going power.

Cloud computing deals with computer management which is the master of capturing information sharing, sharing and configuration using visible and flexible assets on the Internet.

Fog and Edge Computing address for power consumption, preparation and use that takes place on the edge of an organization. This management acts as a conduit between end customers and cloud server farms, effectively reducing the distance information should flow through the organization and creating unnecessary delays.

Augmented Reality and Virtual Reality focuses on the development of information that provides seamless integration by creating virtual space-based virtual reality (VR) and enables understanding of real-time (AR) PC-based images, which provides human connectivity in a virtual environment.

Robots represent a framework that uses modern robots and additional machine gadgets, which are self-sufficient, adaptable, and adaptable, so that modern Robotization can create creative assignments without a doubt with minimal human input. Cyber Security addresses "the arrangement of innovations and cycles intended to ensure PCs, networks, programs, and information from attack, unapproved access, change, or annihilation".

Semantic Web Technologies, like the current web extension, represents a collaborative movement and a set of levels at which information is provided in a well-defined definition, enabling computers and individuals to work collaboratively.

Additive Execution refers to the cycle of manufacturing by joining a layer of building materials (rather than inventing new removable items) by looking at computer data, enabling three-dimensional objects to be delivered on request.

III. SECURITY REQUIREMENTS IN IIOT

A. *The CIA triad*

The Confidentiality, Integrity, Availability (CIA) triad is a remarkable data security model.

Confidentiality is about obtaining complete data from its properties. This includes encryption, access control, network closure, but additional security angles.

Integrity is related to consistency, precision, accuracy, and most importantly the general honesty of things.

Availability affects framework performance certificates. As such it ensures that the operation will be done within the critical cutting times.

In general, the CIA is for data security but may be appropriate for a real digital framework.

In industrial situations, demand is more likely to be available than honesty and ultimately secrecy.

This compares with the structures associated with Inter.

These three angles are generally excellent to be remembered for the safety purposes of the framework but are not essential to reduce the need to return to parts[13]. of the CIA triad.

B. *Authentication -*

Verification of remote objects is an important problem for certain types of IoT connections. Another concern is verification and data validity.

There are a number of topics related to authentication -

1) *Key Distribution*

Key distribution is a critical requirement for some systems in IoT and in some parts of IIoT. General Public Infrastructure (PKI) is no longer operational[14]. Managing dynamic situations, few arrangements that he can manage the deletion of node additions, such as rethinking or a little more transfers by requiring a single one-person relay message confirmation of direction or no authorized authority, but the Hash Distributed Hash (DHT) Table relating to the spread of personality and inquiries.

2) *Affiliate Verification*

Authentication of both is classified as one of the requirements for any validation system. It is important, as large quantities of it are introduced in foreign lands. Customer framework / secret phrases are not easy to understand either flexible enough. Point out that full proof of criminal integrity is necessary[15]. There is some new applications that aim to address this use hidden ones in categories such as Abstract Physical Activity or Reliance on Biometrics with known evidence and by determining the characters by examining the patterns of behaviour.

3) *Non-objection*

Not discarded ensures that the message maker cannot discard the origin of this message in time. This is in line with other ideas besides messages.

Non-disposal can be considered a need for security and basic assets. The benefit of proposing a WSN certification system on the grounds that is a part of the heavy computers can be transferred to outsiders, the computational requirements for the sensors nodes themselves can remain low[16].

4) *Anonymity and Confidentiality*

Anonymous verification confirms the authenticity of an object without revealing the nature of the object. This is important in some cases where one needs to protect customer protection. The need to protect clients from visibility when the enemy approaches authenticity management[17].

A community-based authentication tool is being proposed, turning customer anonymity into a strict requirement or not in terms of a blockchain, however in the work to provide a calculation guide. Both of these proposed systems use Attribute-Based Signatures (ABS).

C. *Access Control -*

Accessibility Control (AC) is important in a variety of contexts, where the device considers two modes of communication, one for standard customer behaviour and one for the framework guides to transmit refreshments, the type of access control is required. In addition, the lack of adequate allocation of rights has been identified as a possible overdose of existing frameworks, such as the Supervisory Control And Data Acquisition (SCADA) protocol. Difficulty in access control is identified by the use of resources, but more accessibility. In specially selected cases, it should not happen that AC policies are unattainable due to the frustration of the association[18].

That means limiting the use of power on simple devices, the signature format of the allowance, as the AC framework for WSNs, is suggested.

A blockchain based authentication protocol was further developed that contains an AC framework and addresses access to one of the most frustrating challenges using blockchain, and DHT containing AC policies[19].

The Ring mark used to create a lightweight AC framework has also been suggested. This framework clearly identifies WSNs and access customer blurring by collecting clients with comparative rights, ensuring that AC professionals are not able to distinguish between marks from clients in the same circle.

A blockchain framework, which separates the requirement for dynamic access control and stream management has also been proposed. They use ingenuity contracts and uses non-disclosure and respect within the blockchain framework to propose a resource management framework, with a well-adjusted AC in which it operates[20].

D. *Data security and data sharing -*

These days, data security is fundamental to almost any digital environment, and IIoT is no exception. Many of the functions tested in this review break the division into data as a security requirement for another building.

A few different ways to keep data separated are -

1) *Data Transfe*

MQTT Protocol is widely used for data sharing between modern systems, but without anyone else supporting client / password verification only, and does not provide security steps in the organization or application layer. This is detrimental to the placement of IIoT. In line with these lines, to treat this, it is suggested to use TLS as a safe layer where MQTT can work. This method puts the top up on the edge devices[21].

2) *External Parties*

The separation of data when it is still very active or on the way, is always approved by cryptographic methods. Difficulty finding the appropriate codes for the IIoT integrated environment. The main difficulty seems to be related to the strength and other needs of the asset. Independent of the code used, the more creators see the key allocation and the board problem. Reliable volume, ease of use, efficient pursuit, and reliable data clearing are some of the key issues in Cloud and Fog situations.

3) *Data Flow Control:*

With data flow control, data access arrangements can be authorized at a much higher level than encryption strategies, providing a way to address security and privacy requirements that determine data processing as it goes by framework[22]. Schütte and Brost pointed out that data flow authorization is necessary in some cases, and they proposed a data-flow control framework that is ready to view messages between both mathematical and start-up objects.

4) *Data Privacy:*

Data confidentiality and ownership is an important issue for some organizations and governments, and for the new prominence of cloud storage management.

With the on-going establishment in the European Union (General Data Protection Regulation (GDPR)) that effectively seeks the private success of all systems, data confidentiality must be properly managed by producers.

Privacy does not only care about data integration and cloud storage, but also requires confusion or metadata[23].

E. *Network Security -*

Making adequate network security involves many things, including authentication, secure transportation, a reliable and secure route, and more.

As industry networks become increasingly unpredictable due to the many connected gadgets, we are facing problems similar to those that occur during the rapid expansion of the World Wide Web.

Many configurations, traffic controls, and security systems rely on limited systems that make integration into common management structures unthinkable[24].

At the same time, they point out that network infrastructure is needed in order to be flexible, to handle dynamic environments. To cope with this trial, two relevant models point to the separation of setups and controls from real-time data acquisition: SDN and Network Function Virtualization (NFV).

SDN is concerned with setup and management, while NFV is concerned with virtual network deployments and security in a layer that is cut off from the gadgets in which it operates[25].

The focus, in which SDNs can improve frame security, is

1) Delays and time:

Adding access and disconnection between endpoints is a network safety requirement, although this can be defined as security measures without the assistance of a third party.

2) Availability:

Delay is not the only problem. From a reliable point of view, one count of disappointment should be removed. Besides, with the current Cloud infrastructure, network planning is always proposed by cloud providers that bind clients to that particular cloud management provision[26].

3) Wireless:

Many smart gadgets use wireless data transmission methods. These wireless communication standards operate at a lower level than the data transmission progress tested in section V-F1.

IV. BLOCKCHAIN FOR IIOT

A. Challenges

1) Interoperability

Mechanical device space is amazing. The PLCs were 190 key computational units in the longest creative lines: fitted with edge jewelry, uniquely unique projects, they could not be easily extended to help significant customization or replacement. Delivery systems that use open machines, Real-Time Operating System (RTOS), or Linux-specific assignments are frequently used as imports in 195 tuation environments. Locations are included with IoT login methods when the data is finalized and distributed to cloud management or organizational staff. According to the point of contact center, these days, the range of fixed vehicles (AGV) and fixed arms are used to produce plants and cells. These automated systems typically use the new ROS system, a 200 GNU / Linux OS designed for applications[27].

2) Portability

In Industrial Content, each device and gear must be devoted to the presentation of explicit assignments. It is not enough to demand a change in hardware systems to allow these components to make Blockchain a force. In addition, Blockchain and trading activities may require explicit meetings while successfully registering, blocking and tedious.

Therefore, it is important to set up a simple framework that is expected to clear Blockchain-related approaches to hardware and capabilities. In this unique scenario, job flexibility is defined as the framework of the framework associated with any gadget or Industrial gadget (and has a compressive power) that allows the display of Blockchain-related skills using direct and indirect fire orders[28].

3) Scalabiity

Diversity is reflected in the ability of the framework to adequately address the work being done, to keep the level of productivity in line with expanded resources. For business, to manage the increase in volume orders without falling or cutting demands on customers. In this unique situation, the power of separation is not

It is recommended as a machine tool, but as a standard plant preparation tool to add Blockchain volume to its creative line. In this context, distribution is considered to be a source of IoT performance component that can be added to normal compatible interactions while ensuring future development capabilities without the need for major assistance .It is important to note As Blockchain applications have been introduced in the Industrial IoT world, having a flexible response to agreeing to enter into strong agreements granted to Blockchain clauses ensures that having the option to resist the one that speaks to huge profits[29].

4) Security

A reliable framework will not address the security of compatible gadgets. Transactions can be sent without encryption but are allowed to ensure reliability and validity, the same as in the case of Ethereum informal community. Some Blockchain categories, especially those that offer the freedom to use legitimate meeting conditions, also look at the basis of independent channels for secured trading (e.g. 250 Hyperledger Fabric).

No matter, the secret key is required to sign the exchange and the final development must be taken to find and combat its looting. In these lines, a strong cryptographic stack is required for performing security tasks.

Two developmental standards can be obtained: to secure private keys in any event that maintains Industrial Io security standards: provide a reliable stack under the cryptographic basis[30]. A clickable mind map that gives an overview of the categories (categories) and specific topics (subscriptions) discussed in this section is constructed in fig 1.

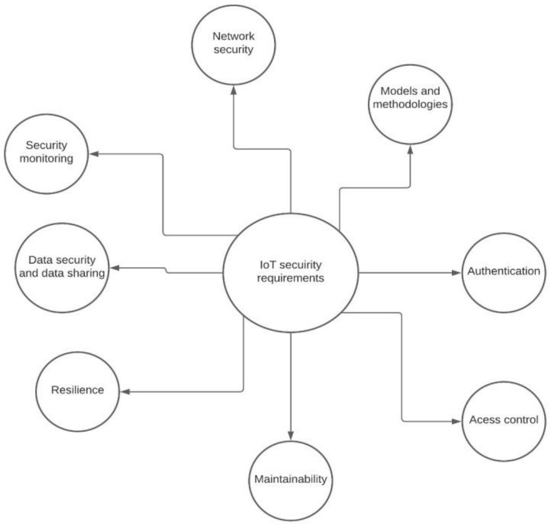

Fig. 1. A clickable mind map that gives an overview of the categories.

B. Blockchain based solutions

1) Hardware

Points for point control around the creators of the external system configuration that is expected to ensure the complete disposal of the useful Blockchain from modern techniques and exercises. Eventually, in the current PC-controlled machines, to use the undamaged system that should be introduced using modern application techniques. However, it would not be possible to guarantee that the frustration and crash of system-focused interventions would not affect the overall strength of the framework. In addition, the recognized system will use the equipment of the host machine that violates the DR3: Decrease. Alternatively, seam binding machines will require guidelines on a modern machine while recovering normal response. The current situation requires the upgrading of the commonsense, usable, productive, robust and amazing connector for IBT. Dedicated equipment should also have the option to address the understanding required on the board, ensure a redesign with a variety of equipment and settings while also ensuring an increase in the number of stored and blockchains.

2) Software

a) SDK (Software Development Kit)

The development phase began with the selection of the SDK to plan for IBT. The official 4ZeroBox SDK is Zerynth [31], a platform that allows editing on Python MCUs for IoT applications. Zerynth is a Python Virtual Machines (VM) that generates a bytecode integrated with Python with an external toolbar (Zerynth Studio). Zerynth VM runs on real-time operating system that supports multi-threaded programs.

b) Hayes Command Set Extended

With the order line construction, the order rule is displayed and applied. A popular order set, used for quite a long time in social media and network work, the Hayes conference, otherwise called the AT order set. Introduced and widely used by modems, modulator / demodulator gadgets in the sense of the old style, capturing computer data and balancing it with various channels, and getting high quality data removed from an external channel (simple channels). Throughout the long run, the modem concept has gained full acceptance, even with special gadgets used to integrate PCs into PCs or various organizations. In this broad sense, IBT can be considered as a type of Blockchain modem. A modem that creates a relationship between a modern device and a Blockchain user that creates a leading twin of resources using Blockchain token technology[31].

c) Blockchain Platform and Interface

In order to use the demo case, various Blockchain categories (IOTA, Hyperledger and Ethereum) have been tested. Particle is a digital currency that emerged in 2015 to address perhaps the most critical issue: development. Blockchain branding like Bitcoin is not rapidly developing and they will not face rapid exchanges. Particle handles these problems in a new way called Tangle. A knot is an uncommon source of information where members need to look at different exchanges for opportunities that they need to do. With this figure, IOTA can manage an unlimited exchange rate and increase its organization limit if more members join.

d) Smart contract

A smart standard contract was developed using Solidity, the official language of editing Ethereum. The contract serves as a storage for receivables data also enables the creation of digital twins by generating a Blockchain token (limits on this option are discussed in 6). The contract contains built-in rules that can be applied depending on the industry conditions to renew the value of shipping or to produce production warnings and alarms based on data and tracking history.

e) User Interface and Dashboard

Also available is a backend for generating a user interface to report data published in Blockchain by IBT. The interface is built using the Web to call intelligent contracting methods from JavaScript, React and Leaflet with Open StreetMap in the construction of UI elements including a tracking map where a case of use is required[30].

V. EDGE COMPUTING FOR IIOT

A. Deployment of edge computing

The IIoT framework has a very large number of invisible harp gadgets, compatible with highly connected networks and cables and connectors. A wide range of organizations includes sensory organizations, remote Wi-Fi organizations, 3G / 4G / LTE / 5G textbook associations and dedicated field delivery [63]. The sheer number of offline gadgets that keep the organization afloat, collecting the latest information on an ongoing basis and transferring it to a PC cloud and controller. With the IIoT head, the size of such organizations is improving, and conventional information network networks are making progress in continuous realization, achieving the ms level of preparatory information. It seeks to reduce overall bandwidth infiltration, reduce network transfer interest rates, and improve the performance of a large framework.

Ensuring Data Security and Privacy: Cloud-based expert organizations provide clients with organized information security arrangements. However, in the event that only one data is stored, it will create adverse effects. Edge processing in the IIoT allows organizations to deploy very useful arrangements nearby, minimizing the risk of data loss during the flow of information and the amount of information placed on the cloud platform, reducing security and security risks.

- *Reduce operating costs:* When information is delivered directly to the cloud component, data transfer, optimal data transfer capabilities and retrospective features require significant operating costs. Edge processing in IIoT can reduce data transfer volume, thereby reducing data transfer volume, transmission power consumption and inefficiency, and reducing operating costs.

B. Reference Architecture of Edge Computing in IIoT

1) Device layer

Gadget cover includes various sensors, compact terminals, metals and meters, sharp gadgets, fine cars, robots and various gadgets or hardware. For various types of remote organizations (Fieldbus, Industrial Ethernet, Industrial Optical Fiber, etc.) or remote organizations (Wi-Fi, Bluetooth, RFID, NB-IoT, LoRa , 5G, etc.), These gadgets or gadgets combine many details of various sensor parameters, go to Edge Layer and strictly wait for control orders from Edge Layer, separate information distribution and control development between Device Design and Edge Layer.

2) Edge layer

Edge Layer is an important layer of new design in IIoT. Edge Layer is responsible for obtaining, modifying and transmitting information streams from the Layer of the device, providing critical time management, for example, border warranty and security insurance, to Edge Layer: Near-Edge Layer, Mid-Edge Layer, and Far Edge Layout.

Far-Edge Layer: Far-Edge Layer contains edge controls that collect information from Device Layer, perform Startup judgments or filter data, and then move the control stream down to Device Layer from Edge Layer or Cloud Application Layer.

Because of the diversity of sensors and gadgets in the gadget layer, the edge controllers in the Far-Edge Layer should have the option to use different sessions that go down and access different sensors or gadgets, in order to have the option to collect data continuously from critical IIoT organizations. After the data has been collected from IIoT, it should be processed to judge or filter the data. After that, the Far-Edge Layer controllers need to install an accounting library based on climate planning in order to continuously improve system performance. In the meantime, Far-Edge Layer edge controllers need to move the control stream to the Layer of the device via a PLC control or function control module after getting the option in the Far Edge Layer or higher layers[32].

Mid-Edge Layer: Mid-Edge Layer essentially comprises of certain edge doors and is liable for gathering information from Far-Edge Layer through remote organizations (Fieldbus, Industrial Ethernet, Industrial Optical Fiber, and so forth) Or remote organizations (Wi-Fi, Bluetooth, RFID, NB-IoT, LoRa, 5G, and so on), store information gathered and give a lot bigger PC. Meanwhile, the entryway edge in the center edge is additionally answerable for moving control stream from the upper layers to the Far-Edge Layer, dealing with gear in the Mid-Edge Layer or the Far Edge Layer. Not at all like the Far-Edge Layer just makes it simple to pass judgment or channel information, Mid-Edge Layer has numerous assets for putting away and utilizing a PC to handle information gathered in IIoT.

Near-Edge Layer: Near-Edge Layer consists of potential end users and responds by performing complex and sensitive data management and managing robust selections based on information collected from Mid-Edge Borders by dedicated organizations. In the meantime, employees working on the fringes of Near-Edge Layer should have business applications from managers and organize board powers. Edge-edge Near-Edge Layer operators are integrated into a small PC component, with PC storage devices and more efficient than Far-Edge Layer and Mid-Edge Layer machines. In this way, Near Edge Layer is used to measure and deal with more information, to advise and train more accurate models to find the best organizational structure to plan the edges. Currently, Near-Edge Layer works with a variety of assets throughout the Edge Layer, requiring the Near-Edge Layer to operate and operate efficiently on stage, just as sending and editing a field-tested strategy management uses it as a next thought. , to ensure the appointment of competent assets and to complete proper delivery and management[33].

3) Cloud application layer

The cloud-based system is very flexible in the number of expected mines from public information and the potential portion of goods to a business, region, or country across the country. In this way, the cloud application layer receives information from Edge Layer about the organization that interacts with others, supports the compilation system, for example, object or aggregation, business financing, deal management and post-transaction management, and provide inputs. model and neglected help in Edge Layer. In addition, the framework of the cloud application can separate data about cloud organizations between circles for a variety of reasons such as masters, corporate organizations, creators, and customers, achieving the most important and deepest mines. Selection times are usually calculated at the level of the day[34].

VI. CONCLUSION

Current practice in terms of various developments promising technology provides a solid foundation in relation to achieve the vision of Industry 4.0. In this context, this paper combines two emerging technologies (i.e. blockchain and edge computing) we elaborate these two technology and their frameworks for the IIoT betterment. The purpose through this paper is to study the blockchain and computing technology and then setting a co-relation with IIoT and achieve its full potential with above technologies.

REFERENCES

[1] T. M. Fernández-Caramés and P. Fraga-Lamas, "A Review on the Application of Blockchain to the Next Generation of Cybersecure Industry 4.0 Smart Factories," in IEEE Access, vol. 7, pp. 45201-45218, 2019, doi: 10.1109/ACCESS.2019.2908780.

[2] Y. Qu, S. R. Pokhrel, S. Garg, L. Gao and Y. Xiang, "A Blockchained Federated Learning Framework for Cognitive Computing in Industry 4.0 Networks," in IEEE Transactions on Industrial Informatics, vol. 17, no. 4, pp. 2964-2973, April 2021, doi: 10.1109/TII.2020.3007817.

[3] L. Chen, S. Zhou and J. Xu, "Computation Peer Offloading for Energy-Constrained Mobile Edge Computing in Small-Cell Networks," in IEEE/ACM Transactions on Networking, vol. 26, no. 4, pp. 1619-1632, Aug. 2018, doi: 10.1109/TNET.2018.2841758.

[4] H. Qi, J. Wang, W. Li, Y. Wang and T. Qiu, "A Blockchain-Driven IIoT Traffic Classification Service for Edge Computing," in IEEE Internet of Things Journal, vol. 8, no. 4, pp. 2124-2134, 15 Feb.15, 2021, doi: 10.1109/JIOT.2020.3035431.

[5] S. Zhao, S. Li and Y. Yao, "Blockchain Enabled Industrial Internet of Things Technology," in IEEE Transactions on Computational Social Systems, vol. 6, no. 6, pp. 1442-1453, Dec. 2019, doi: 10.1109/TCSS.2019.2924054.

[6] C. Mbohwa and A. Kumar Sahu, "Performance Assessment of Companies Under IIoT Architectures: Application of Grey Relational Analysis Technique," 2018 International Conference on Inventive Research in Computing Applications (ICIRCA), 2018, pp. 1350-1354, doi: 10.1109/ICIRCA.2018.8597285.

[7] P. P. Gaikwad, J. P. Gabhane, and S. S. Golait, "A survey based on smart homes system using internet-of-things," in 2015 International Conference on Computation of Power, Energy, Information and Com munication (ICCPEIC), 2015, pp. 0330–0335

[8] L. Xu, W. He, and S. Li, "Internet of things in industries: A survey," IEEE Transactions on Industrial Informatics, vol. 10, no. 4, pp. 2233–2243, 2014.

[9] D. Mourtzis, E. Vlachou, N. Milas, Industrial big data as a result of iot adoption in manufacturing, Procedia Cirp 55 (2016) 290–295.

[10] C. Perera, C. H. Liu, S. Jayawardena, The emerging internet of things 930 marketplace from an industrial perspective: A survey, IEEE

Transactions on Emerging Topics in Computing 3 (4) (2015) 585–598.

[11] D. B. Parker, Information security in a nutshell, Information Systems Se curity 6 (1) (1997) 14–19.

[12] R. von Solms, J. van Niekerk, From information security to cyber security, Computers & Security 38 (2013) 97 – 102, cybercrime in the Digital 940 Economy. doi:https://doi.org/10.1016/j.cose.2013.04.004. URL http://www.sciencedirect.com/science/article/pii/S0167404813000801

[13] Z. Birnbaum, A. Dolgikh, V. Skormin, E. O'Brien, and D. Muller, "Unmanned aerial vehicle security using recursive parameter estima tion," in Proc. Int. Conf. Unmanned Aircraft Syst. (ICUAS), 2014, pp. 692–702.

[14] V. Sharma, G. Choudhary, Y. Ko, and I. You, "Behavior and vulnerabil ity assessment of drones-enabled industrial Internet of Things (IIoT)," IEEE Access, vol. 6, pp. 43368–43383, 2018.

[15] A. Bicaku et al., "Towards trustworthy end-to-end communication in industry 4.0," in Proc. IEEE 15th Int. Conf. Ind. Informat. (INDIN), 2017, pp. 889–896.

[16] M. H. Eldefrawy, N. Pereira, and M. Gidlund, "Key distribution proto col for industrial Internet of Things without implicit certificates," IEEE Internet Things J., vol. 6, no. 1, pp. 906–917, Feb. 2019.

[17] V. Sklyar and V. Kharchenko, "Challenges in assurance case application for industrial IoT," in Proc. 9th IEEE Int. Conf. Intell. Data Acq. Adv. Comput. Syst. Technol. Appl. (IDAACS), vol. 2, 2017, pp. 736–739.

[18] E. Weippl and P. Kieseberg, "Security in cyber-physical production systems: A roadmap to improving it-security in the production system lifecycle," in Proc. AEIT Int. Annu. Conf., 2017, pp. 1–6.

[19] S. R. Chhetri, N. Rashid, S. Faezi, and M. A. A. Faruque, "Security trends and advances in manufacturing systems in the era of industry 4.0," in Proc. 36th Int. Conf. Comput.-Aided Design (ICCAD), 2017, pp. 1039–1046.

[20] A. Hassanzadeh, S. Modi, and S. Mulchandani, "Towards effective security control assignment in the industrial Internet of Things," in Proc. IEEE 2nd World Forum Internet Things (WF-IoT), 2015, pp. 795–800.

[21] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, and M. Gidlund, "Industrial Internet of Things: Challenges, opportunities, and direc tions," IEEE Trans. Ind. Informat., vol. 14, no. 11, pp. 4724–4734,

[22] A. Sadeghi, C. Wachsmann, and M. Waidner, "Security and privacy challenges in industrial Internet of Things," in Proc. 52nd Annu. Design Autom. Conf. (DAC), 2015, pp. 1–6.

[23] T. Pereira, L. Barreto, and A. Amaral, "Network and information secu rity challenges within industry 4.0 paradigm," Procedia Manuf., vol. 13, pp. 1253–1260, Jun. 2017.

[24] U. Hunkeler, H. L. Truong, and A. Stanford-Clark, "MQTT-S—A pub lish/subscribe protocol for wireless sensor networks," in Proc. 3rd Int. Conf. Commun. Syst. Softw. Middleware Workshops (COMSWARE), 2008, pp. 791–798.

[25] S. Katsikeas et al., "Lightweight & secure industrial IoT communica tions via the MQ telemetry transport protocol," in Proc. IEEE Symp. Comput. Commun. (ISCC), 2017, pp. 1193–1200.

[26] M. A. Ferrag, L. A. Maglaras, H. Janicke, J. Jiang, and L. Shu, "Authentication protocols for Internet of Things: A comprehensive survey," Security Commun. Netw., vol. 2017, Nov. 2017, Art. no. 6562953.

[27] "2018 OWASP IoT top 10," OWASP, Rockville, MD, USA, Rep., Dec. 2018. [Online]. Available: https://www.accenture.com/t00010101T000000Z__w__/it-it/_acnmedia/PDF-5/Accenture-Industri al-Internet-of-Things-Positioning-Paper-Report-2015.pdf

O. Bergmann, S. Gerdes, and C. Bormann, "Simple keys for sim ple smart objects," in Proc. Workshop Smart Object Security, 2012, pp. 172–182.

[28] S. Raza, D. Trabalza, and T. Voigt, "6LoWPAN compressed DTLS for CoAP," in Proc. IEEE 8th Int. Conf. Distrib. Comput. Sensor Syst., 2012, pp. 287–289.

[29] V. Buterin, et al., Ethereum white paper: a next generation smart contract & decentralized application platform, First version.

[30] D. Mazzei, G. Baldi, G. Montelisciani, G. Fantoni, A full stack for quick prototyping of iot solutions, Annals of Telecommunications 73 (7-8) (2018) 439–449.

[31] D. Mazzei, G. Montelisciani, G. Baldi, A. Ba`u, M. Cipriani, G. Fantoni, Improving the efficiency of industrial processes with a plug and play iot data acquisition platform, Enterprise Interoperability: Smart Services and 1005 Business Impact of Enterprise Interoperability (2018) 315–321.

[32] C. Weber, J. Koenigsberger, L. Kassner, and B. Mitschang, "M2ddm-a maturity model for data-driven manufacturing," Manufacturing Systems 4.0, vol. 63, pp. 173–178, 2017.

[33] J. Wang, J. Liu, and N. Kato, "Networking and communications in autonomous driving: A survey," IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1243–1274, Secondquarter 2019.

[34] P. G. V. Naranjo, M. Shojafar, A. Abraham, and E. Baccarelli, "A new stable election-based routing algorithm to preserve aliveness and energy in fog-supported wireless sensor networks," in 2016 IEEE International Conference on Systems, Man, and Cybernetics (SMC), 2016, pp. 002 413–002 418.