Integration of Next Generation IIoT with Blockchain for the Development of Smart Industries

Aamir Iqbal [a], Mohammad Amir [b*], Vinod Kumar [c], Aftab Alam [b], Mohammad Umair [d]

[a] *Department of Mechanical Engineering, Amity University, Noida, (Uttar Pradesh), 201313 India*

[b] *Department of Electrical Engineering, Jamia Millia Islamia (Central University), New Delhi, (Delhi), 110025 India*

[c] *Department of Mathematics, PGDAV Collage, University of Delhi, New Delhi, (Delhi), 110065 India*

[d] *Department of Computer Science & Engineering, Galgotias University, Greater Noida, (Uttar Pradesh), 226001 India*

Abstract

In modern era, a wide range of smart industries is being focus on automation-based applications. Various technologies are rapidly implementing in Industrial Internet of Things (IIoT) for manufacturing sectors that helping to achieve advanced schedule production framework and on time delivery of products. The integration of IIoT platforms with the blockchain are challenging service in manufacturing system. The primary objective of this article is to characterize various issues and challenges that are implementing IIoT and blockchain in industries. The proposed work is an integration of IIoT and blockchain in industrial processes for solving the security issues in real-time. Also, identifying various enablers of blockchain and issues of IIoT from smart industries manufacturing using a survey tool is formed in the form of questionnaire. Based on these responses Decision Making Trial and Evaluation Laboratory (DEMATEL) technique has been implemented for categorizing these challenges into cause and effect. In this paper, we introduce the general layout with their key issues and challenges of IIoT and blockchain that signifies the safety requirements to design the IIoT and blockchain. Further, we describe how IIoT can be integrated to the blockchain for smart Industrial applications. Finally, various recommendations are the proposed to upcoming IIoT and blockchain developments. The proposed work will be highly beneficial for the smart industries to develop a next generation IIoT and blockchain based framework.

1- Introduction

In recent developments, upgradation of technologies is highly dependent on automation based on internet, still in manufacturing sectors industrial automation is quite lacking behind as compared to developed countries like Japan and China [1]. The industrial revolution was initially started depending on water, steam power, labor, electrical energy and lastly idea of industry 4.0 came into existence. Nowadays, the concept of Internet of thing (IoT) is becoming too popular and widely used in every aspect of day to day life. The term IoT developed in 19th century [2], it has been used for connecting gadget or machine in the field of commercial, corporate and industrial sector [3]. Every component, things, parts are connected with sensors through which data are automatically being shared and parts respond accordingly [4]. The industrial IoT is applying the concept of IoT in the field of industries. Industrial Internet of thing (IIoT) is the application in Industrial using IoT. The IoT can be defined as a group of infrastructures connecting sensors, actuators providing their management, data mining and accessing them [5]. The IoT is the extension of internet connectivity and computing facilities which facilitates minimum human efforts to analyze, generate, exchange and data controlling [6]. In this study the main aim is to tackle out the main issue or factor affecting the implementation

---

of IIoT in the autonomous industries, the factors have been identified from the literature review and questionnaire for IIoT and blockchain separately.

1-1- Industrial Internet of Things

The idea of Internet in Industries was started by General Electric [7], as the Industrial Internet is connection of machines sensors and actuators to the Internet for wide area network (WAN) or it may be defined as the combination of physical and digital technology. Various researchers defined IIoT as the combination of Internet of thing (IoT), machines, people, computers, doing various manufacturing operation using advance data analyzing techniques for converting traditional business approach to full automation and redefining all concept [8]. The IIoT facilitate companies to use sensors, software's and other technology to collect data from various physical source and use them to manage the operation and provide value services [9]. Various definitions of IIoT areas: The use of IoT engineering which includes smart objects in the cyber Field for the benefits of industries. It may also be defined as the use of IoT in the field of manufacturing [10].The field of IoT does not limit to only smart keys, smart home appliances, smart kettles, and smartphones but it is a wide areas which aims is to connect industries assets such as power grid, engines part and Internal sensors to cloud via web [11]. The functions of IIoT devices are to examine, accumulate, interchange and record data so that it can be interchange information without human intervention.

The Fast-Moving Consumer Goods (FMCG) companies which one very high productivity-based industry where demand from the consumer is driving manufacturing unit to it and this is the place where data is more important for these people. In this case, productivity is one of the aspects, but we have overall equipment effectiveness (OEE), a major factor in profitability. In the FMCG manufacturing type industry, the line type production, where we have different machines on different shop floor before IIoT manufacturers use to do that they individually move to different shop floor and record data i.e., number of hours machine run, efficiency of machine, downtime hours and then comes to center and feed the data. The data was handwritten and prone to various error in this system. But, now with IIoT based manufacturing unit every data was recorded automatically in real time with no error and then put into analysis and automatically detect productivity of each machine. Individual analysis of every machine about no of hours machine runs if any errors come like if machine has to run for 12 hours but it ran for only 8 hours then what is the issue whether it is run time error, breakdown errors, lack of raw material, unavailability of operators all the parameters were identified and send automatically and loss and energy issue can be easily identified and OEE can be easily be calculated and Overall Line Effectiveness (OLE) can be determined and which improves company productivity.

1-2- Advancement in Blockchain Technologies

In modern era, blockchain is vital technology that would lead to a huge change in the upcoming ten years for communication networking. Now, it is very emerging concept for the industries. In 2008, the concept of blockchain has presented [12]. This technology will have a great impact on providing business opportunities, improve efficiency and would provide transparency and visibility in the work. The blockchain is vaunted technology that facilitates strong cyber security and high standard of privacy of data. The blockchain is a digitally based account that stores information in the form of blocks. Every information is being compiled in the form of coding in sequential form. Blockchain consist of a series of blocks which are cryptographically attached to the preceding blocks. This technology has totally modified the system for transferring without third-party intervention. The blockchain uses bitcoin concept for strengthening cybersecurity and protecting privacy. Nowadays data are being kept in cyber cloud storage for the IoT. The blockchain facilitates us in privacy and data security and covers every aspect of industrial. The blockchain facility is quite better than the IoT concept as it focuses on the decentralized network which results in low susceptibility to manipulation of data and illegal copying by venomous participants as compared to IIoT. The data are stored in the interconnected and interlocked contended devices. According to Kestenbaum, if in any system of blockchain data are altered then, the system rejects the process [13].

Blockchain provides high security in the form of multi-signature to operate and multi-keys are required to finalize the process or transaction. If the hacker tries to enter into the system or tries to steal information and if it is hacked, then also there are lots of other back-ups it could be easily retrieved [14]. Which means data are kept in the interconnected computer. Even then, if they have to hack then they have to hack more than 55% of the computers simultaneously which is impossible at this time. For example, if they hacked the system by knowing the key, then also they could not access because they could not match the specific multi-signature [15, 16]. The blockchain keeps data in the form of small blocks where each block stores a bitcoin transaction. Blocks are group together with reference to previous blocks. The main features of the blockchain are as below:

(a) Decentralized Network

In this type of system facilitates having:

- Avoids using a single and centralized network to take all its decision.

- There is no single authority.
- Communication becomes fastened.
- It lowers the cost.

(b) Distributed Network

In these types of network contains:

- Everyone is accessible to every node.
- Transparency of data is there.
- Tampering of data is impossible.
- The culprit is easily identified.

(c) Immutable Features

It contains as following:

- Data once cannot be altered or change, for this we need to add a new block.
- Results cannot be easily changed.

(d) Various Components of the Block

- It consists of hash, data, and hash of the previous block. The hash is nothing but works same as fingerprints. Any variation in the block of data will lead to change in hash.

1-3- Correlation between Blockchain and IIoT

- All the manufacturers in the industries have to regularly update their work continuously and for that, they have to publish manuals for repairing and maintenance. These manuals publications are required by every technician, so with the help of blockchain, they could easily access.
- Various confidential design and document like the design if fighter plane, guns, arms can be easily shared via blockchain technology as its impossible to hack. The data are sent to exactly the same person to whom we need to send as it requires multiple keys to operate.
- Parts that are manufactured and send can be easily traced, with the technology of blockchain miss- matching and misplacing of parts can be identified.
- In the blockchain, every data and transaction are crystal clear and transparent.

1-4- Integration of IIoT and Blockchain

Recently, IoT in industries is transforming every manual work to automation due to the highly competitive market. The knowledge of automation in this field leads to the development of a management system. Through the digitization life quality of people is upgrading day by day. Implementation of cloud computing upgradation, the platform of IoT facilitates to provide process information in a systematic way and converting them into real-time actions and information [17]. Cloud storage plays a vital role in IoT but there is a threat of data security, transparency and privacy. Therefore, to overcome this issue we need to integrate blockchain and It in the industrial sector. Blockchain can provide trusted sharing service where we get reliable information and data. Data can be even easily traceable, and it is immutable and thus enhances its security. Data are shared in the form of chain and leakage of information leads to unauthorized way of food traceability. Integrating blockchain and IoT in the food industries would increase food safety and saves the lives of many people due to contaminated food infection caused by eating the same food, we can easily trace them. Various changes due to the integration of blockchain and IoT are below:

- **Redistributed/decentralization:** Every company individually take a decision and single big companies cannot have the authority to keep all data. Improvement in the fault tolerance and system scalability of IIoT [18].
- **Trustworthy:** Through the blockchain data and information are immutable. Every individual has the facility to verify data authenticity and they could certify at each step that they are not being tampered.
- **Security aspects:** As discussed in the above section that security in the IIoT is improved by the integration of blockchain.

● **The market of services:** The blockchain can facilitate the best environment for data exchange and better IoT ecosystem. Moreover, we do not need now third-party authority to transfer between peers [19, 20, 21].
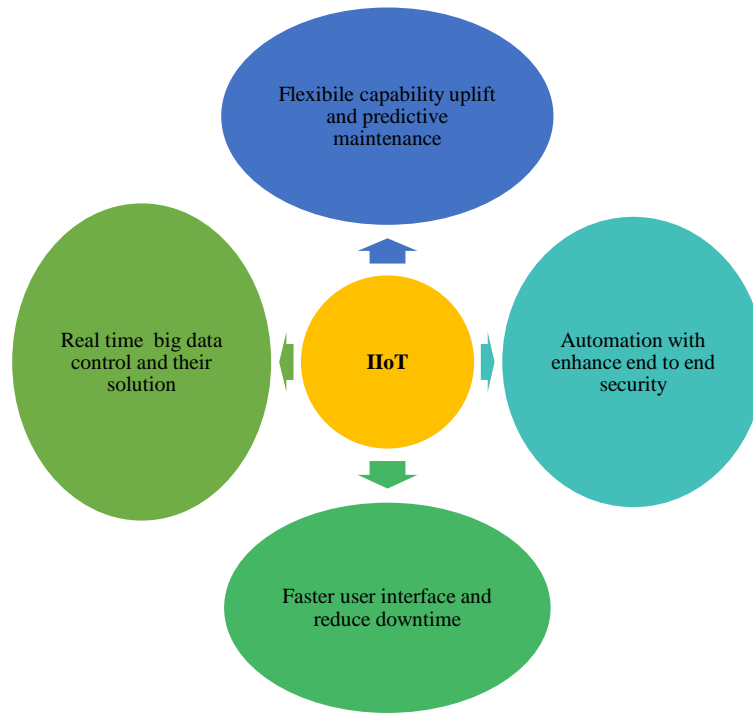
Figure 1. Key benefits of IIoT in Industrial sector.

IIoT is now a fast-booming technology that requires implementing in every sector for fast growth rate and efficient production. Several benefits of IIoT as shown in Figure1. Even in the field of quality control, automation and IoT can automatically detect number of hours machine run, efficiency of machine, downtime hours and run time error, breakdown errors, lack of raw material, unavailability of operators all the parameters were identified and proceed automatically. Loss and energy issues can be easily identified and OLE can be easily be calculated thus OLE can also be determined, and which improves company productivity. But there is a various issue of IIoT which needs to tackle by integrating with blockchain as it facilitates a better environment for data exchange and does not require third-party authority. in the paper we will solve the various major issue.

Although blockchain is itself a complex chain and it has its own demerits like loss of their operating key would lead to huge loss of data like recently according to report; gerald cotton, founder, and chief executive officer of crypto exchange quadrigacx has to lead to loss of cad $190 million. even though every coin has two faces it is having a large benefit with some drawbacks also.

2- Challenges towards the Integration of IIoT and Blockchain

In this section dealing with the major challenges that we face while integrating them. Firstly, blockchain was invented for internet setting and requires large computers and IoT does not require all these advance high-level computers. Blockchain operations are operated digitally and require high operational keys and require effective internet facility while combining them leads to slow work.

2-1- Enablers of Blockchain

The enablers of blockchains are below as:

(a) **Multi-node storage of data:** Blockchain is a decentralized network hence it required large storage capacity for storing data in the form of nodes and it stores information in the multiple nodes and so it cannot be traceable and hacked because millions of nodes are interconnected in such a way that hacking or misusing of any nods data would lead to overall failure [22, 23].

(b) **Enhance cyber Security:** Blockchain is more advanced than IIoT in security concern even though various virus attacks like finney attack, Denial of Service, Man in the Middle/Sybil lead to dis functioning of network operating blockchain [24, 25, 26].

(c) Efficient and prompt processing: Time required for encryption and decryption of codes and it facilitates complex processing of data in a very easy manner and also it delivers information at the exact time [27, 28].

(d) Enhance transparency of data: Although blockchain enhances total transparency of work and it always show exact data and value but sometimes this could have beneficial to hackers [29, 30].

(e) Reducing scalability issue: due to the large nodes available and each node are interconnected, facilitates scalability issue which means now the problem of securing complex data can be cured easily [23-27].

(f) Infrastructure design and setup cost: As we all know to implement this advance blockchain technology requires a huge investment in both infrastructure and capital investment securing data of large industries require huge setup of infrastructure and design which blockchain can facilitate [31, 32].

(g) Password security: It enhances higher security with multiple passwords at each node and data can only be accessed with particular operational keys [31-39].

(h) Issue of global acceptance: The trusting record of blockchain that since blockchain is a new concept hence it is not globally accepted even though it is accepted everywhere and plays a greater role in crypto currency [31-33].

(i) Lack of skills/knowledge: Implementing blockchain require high skilled and knowledgeable employees which facilitates their best output and using their skills for the resolving of IIoT issue [27-31].

(j) Hardware compatibility issues: Data are mostly captured through sensors, PLCs and connected through the cloud so the machines need to be compatible and updated [36].

2-2- Issues and Open Challenges of IIoT

There are following issues and challenges of IIoT:

(a) Data security: Data security is major issues as leakage of personal data, hacking of important information and trapping of data by unauthorized user which are being stored in the cloud memory .therefore to implement IIoT we need a better security platform for storing our data so that no one can access it [34, 35].

(b) Data connectivity and power: To implement IIoT we have better internet connectivity and quick access to data. Moreover, we must have better power supply as power loss at any moment could lead to huge capital loss [36, 37].

(c) Storage capacity: Various IIoT requires high storage and memory capacity for efficient performance. As all data are to be stored in the memory; hence, due to lack of efficient high storage capacity implementing causes a problem [38, 39].

(d) Lack of standardization: There is no specific and standard protocol for how to implement IIoT [40, 41].

(e) Higher investment/committed resources: For implementing IIoT requires high capital investment and high resource in any industries [36-42].

(f) The requirement of advanced software: For implementing IIoT in industries we need high technology software and supercomputer. Lack of all these leads to failure [43, 44].

(g) The difference in technology adoption between customer and suppliers: Every industry before implementing IIoT must aware of customers' demands and need because misunderstanding between them leads to loss [36-45].

(h) Hardware compatibility issues: The people faced losses in the production and setting up IIoT because we don't have better software and the software that we are using are not updated [36-46].

(i) Complicated processes: Many times, design and procedure that we use are not to mark and various complex steps are made [47, 48].

(j) Unemployment: As we know that implementing IIoT will lead to unemployment to various unskilled labors [49, 50].

(k) Appropriate infrastructure requirement: Implementing some better technology requires better infrastructure for efficient performance [43-51].

(l) Top management commitment/policy: It is an important factor as if we don't have better support from higher and top management than any new methodology will not be implemented [43-47].

Table 1. Enablers of blockchain.

S. No.	Enablers	Descriptions
1	Multi-node storage of data	As block-chain is a decentralized network and every data has to be stored in the form of nodes and the sensors and smart devices do not have enough storage capacity [22, 23].
2	Enhance cyber security	Various attacks like Finney attack, Denial of Service, Man in the Middle and Reply attacks to lead to malfunctioning of the network [24-26].
3	Efficient and prompt processing	Requires time for Encryption and Decryption [27, 28].
4	Enhance transparency of data	In the blockchain, every transaction can be examined, inspect and scan publicly [29, 30].
5	Reducing scalability issue	Concern about the limit of the transaction, speed of the transaction [23-27].
6	Infrastructure design and setup cost	Implementing bitcoin requires high setup cost and proper infrastructure [31, 32].
7	Password security	Specific keys are provided to operate with coins if lost it will be unoperated [29-31].
8	Issue of global acceptance	Modern concept and not even legally used by government, so various business companies feel insecure to adopt it [31, 33].
9	Lack of skills/ knowledge	Lack of knowledge and proper education of how to implement blockchain in industries, they think it for financial transaction [27, 31].
10	Hardware compatibility issues	Data are mostly captured through sensors, PLCs and connected through the cloud so the machines need to be compatible and updated [36-52].

Table 2. Issues and challenges of IIoT.

S. No.	Enablers	Descriptions
1	Security of data	Data security is one of the major issues as leakage of personal data, hacking of important information and trapping of data by the unauthorized user which are being stored in the cloud [34, 35].
2	Data connectivity and power	Various machines even depend on PLCs, telemetry system and RTU to generate data [36, 37].
3	Storage capacity	Various IIoT implementation requires high memory and storage capacity for efficient performance [38, 39].
4	Lack of standardization	There is no standard protocol for implanting IIoT [40, 41].
5	Lack of resources and infrastructure	Lack of resources for investment in implementing IoT [36-42].
6	The requirement of advanced software	Lack of high-tech software and supercomputers are the main issues in the implementation of IIoT [43, 44].
7	Customer and supplier relationship management	Every IIoT must understand the need and demand of customer and provide value to them. They should provide customer satisfaction [36-45].
8	Complicated processes	Many times, designing is made poorly, and various protocols make the configuration complex [46, 47].
9	Unemployment	Implementing IIoT will lead to the omission of various labors and employees and would lead to raising the level of their skills [48, 49]
10	Top management commitment/policy	It is one of the crucial factors as if there would not be a change in the thinking of managers towards IIoT, then it could not be implemented [50].

3- Proposed Methodology

We have adopted the procedure for implementation of IIoT and blockchain in the industries using DEMATEL technique is graphically shown as below in Figure 2.
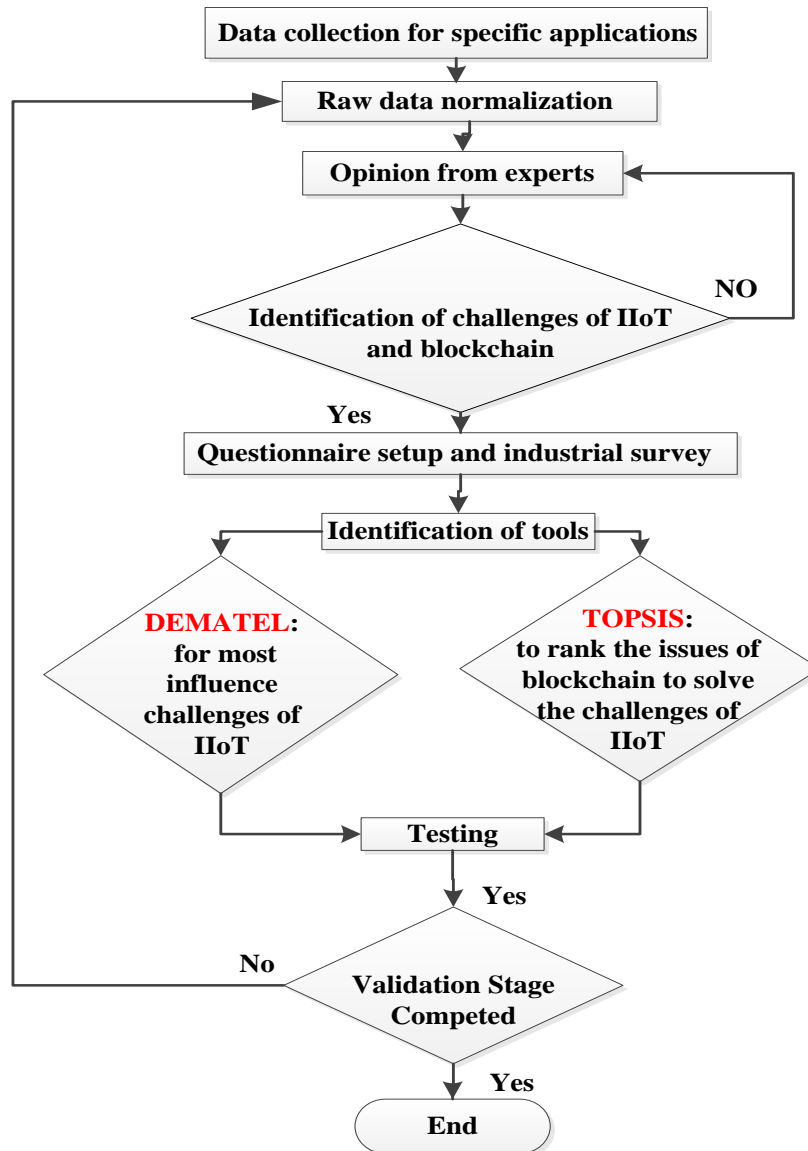
Figure 2. Flowchart for the integration of IIoT and Blockchain.

3-1- Decision Making Trial and Evaluation Laboratory (DEMATEL) Technique

The DEMATEL approach is being used in the paper to analyses the most influential issue and challenges in implementing IIoT in industries. It is normally used to determine the influence of many factors with the given set of factors. This method is used to resolve the complex multi-criteria decision making (MCDM) industrial problem [52]. This method is suitable for allocating specific values to a powerful factor based on the given condition. It gives the relationship through matrixes and diagraph [53] i.e., it helps in indicating the relationship between various factors .this technique uses a set of components i.e. F= {F1, F2 … Fn} which varies with other components and have a specific relationship with different factors which can be evaluated easily. It is mainly used for estimating complex type problems with a large number of variable as it helps in focusing the most influential factor in the case. The process of DEMATEL technique is listed as follows:

- **Step 1:** Fill the relationship matrix by the experts of that field:

In this method, the matrix is being filled by the experts according to their knowledge and experience. The matrix is filled to evaluate the influence of one factor on the rest all factor. This is measured by rating the factor in a scale of 0 to 4 whereas 0 shows the least significance and 4 significance max influence. The scale that is used as the DEMATEL scale, the matrix which we obtained the relationship matrix.

- **Step 2:** Estimating the mean matrix:

After obtaining a relationship matrix the sum is calculated and divided by each element to obtain the average matrix table.

$$N_{avg} = \begin{pmatrix} N_{1i} & N_{1n} \\ N_1 & N_{nn} \end{pmatrix} \tag{1}$$

- **Step 3:** The matrix is being normalized:

In this step after obtaining the average matrix, normalizing of the matrix is done by ranking each element of the matrix between 0 and 1. In this type of matrix, each diagonal element of the normalized matrix is made zero also known as 'Fuzzy cognitive method'. The symbol is being used to denote the matrix which is denoted by $Y=[Y_{ij}]_{n*n}$. The Y shows the influence of the matrix in between these elements.

- **Step 4:** Estimating the full direct/indirect influence matrix:

After obtaining initial influence matrix in the above step now we calculate the full direct/indirect influence matrix with the help of Equations 2 and 3 shown below. Symbol N_{ij} is used in this Equation 3. Where i, j represents elements of the matrix.

$$X = p \times n \tag{2}$$

$$\text{Where, } p = \min\left\{\frac{1}{\max 1 \le i \le \sum_{1 \le i \le n,\ j=1}^{n} N_{ij}}\right\} \tag{3}$$

$$\lim_{h \to 0} X^h[0]\ n \times n,\ 0 \le x_{ij} \le 1 \tag{4}$$

- **Step 5:** Calculating total influence matrix:

It is calculated by Equation 4, where I represent the identity matrix.

$$T_0 = Y(I - Y)^{-1} \tag{5}$$

- **Step 6:** Obtaining prominence factors with their causes and effects value:

In the relationship matrix, the sum of each ith row element gives the value of D_i. In the same, by adding the value of each column we can get the value of R_j. The notation D+R reveals how much important the criteria have, degree of importance or relation of that criteria with other criteria. The row which is having more value of D+R shows more relationship with other criteria and less value shows less relationship with other criteria, and D-R shows kind of relation between the criteria. The positive value of D-R gives cause group which means that these criteria influence other criteria. Negative value of D-R shows the effect group indicating receiver i.e. it gets affected by other criteria.

3-2- Data Capturing Technique

In the data capturing procedure, firstly questionnaire is made with experts and is send to companies via hardcopy and mailed to their email and LinkedIn and responses are recorded and analyzed. On the basis of the response came for the questionnaire the factors are categorized and ranked according to their influence, after obtaining the data, the further calculation is done via DEMATEL.

3-3- DEMATEL Calculation Process

The calculation which is done for the ranking of factors has been divided into two basic categories:

- **Step1:** Firstly, the mean value of all influence matrix is calculated after filling of all initial influence matrix filled by the learned experts in their prospective field. The table.3 showing the filled data of the influence matrix of IIoT. The value ranges from 0 to 4 are being filled by the experts and literature review which shows the most influence issue and challenge factors with respect to other factors.

- **Step 2:** After calculating the mean value of all influence matrix normalizing of a matrix are done with the help of formula $Y=[Y_{ij}]_{n*n}$ for IIoT and then further calculation is done according to the step mentioned in Figure 2.

Table 3. Enablers of blockchain.

	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10
C1	0	2	1	3	1	2	1	1	1	4
C2	2	0	3	3	1	4	4	2	2	3
C3	3	3	0	3	3	4	1	2	1	2
C4	4	3	2	0	2	3	0	0	2	0
C5	3	4	2	3	0	3	3	2	4	3
C6	4	3	3	3	2	0	3	3	1	3

C7	2	1	0	3	3	1	0	4	4	3
C8	4	3	3	4	1	2	4	0	2	3
C9	1	1	0	1	1	3	2	1	0	4
C10	2	2	1	2	2	1	0	4	3	0

Table 4. Average of all influence matrices for IIoT.

	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10
C1	0	0.07407	0.037037	0.111111	0.037037	0.074074	0.037037	0.037037	0.037037	0.148148
C2	0.074074	0	0.111111	0.111111	0.037037	0.148148	0.148148	0.074074	0.074074	0.111111
C3	0.111111	0.111111	0	0.111111	0.111111	0.148148	0.037037	0.074074	0.037037	0.074074
C4	0.148148	0.111111	0.074074	0	0.074074	0.111111	0	0	0.074074	0
C5	0.111111	0.148148	0.074074	0.111111	0	0.111111	0.111111	0.074074	0.148148	0.111111
C6	0.148148	0.111111	0.111111	0.111111	0.074074	0	0.111111	0.111111	0.037037	0.111111
C7	0.074074	0.037037	0	0.111111	0.111111	0.037037	0	0.148148	0.148148	0.111111
C8	0.148148	0.111111	0.111111	0.148148	0.037037	0.074074	0.148148	0	0.074074	0.111111
C9	0.037037	0.037037	0	0.037037	0.037037	0.111111	0.074074	0.037037	0	0.148148
C10	0.074074	0.074074	0.037037	0.074074	0.074074	0.037037	0	0.148148	0.111111	0

Table 5. Total influence matrix for IIoT.

	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	D
C1	0.238	0.269	0.18	0.323	0.183	0.273	0.19	0.211	0.216	0.352	2.425
C2	0.412	0.297	0.313	0.438	0.262	0.439	0.372	0.335	0.339	0.435	3.642
C3	0.43	0.391	0.21	0.423	0.309	0.43	0.268	0.313	0.289	0.386	3.449
C4	0.366	0.308	0.219	0.231	0.217	0.321	0.171	0.174	0.244	0.239	2.49
C5	0.471	0.457	0.301	0.468	0.24	0.443	0.368	0.355	0.431	0.474	4.008
C6	0.489	0.414	0.325	0.456	0.299	0.322	0.35	0.372	0.317	0.45	3.794
C7	0.36	0.293	0.183	0.387	0.286	0.299	0.208	0.354	0.373	0.393	3.136
C8	0.49	0.412	0.322	0.487	0.27	0.393	0.379	0.272	0.352	0.451	3.828
C9	0.238	0.212	0.128	0.235	0.168	0.277	0.21	0.201	0.165	0.336	2.17
C10	0.316	0.287	0.194	0.313	0.222	0.263	0.184	0.316	0.295	0.246	2.636
R	3.8	3.34	2.375	3.761	2.456	3.46	2.7	2.903	3.021	3.762	

Table 6. Cause and effect correlation for IIoT.

Criteria	Notation	D	R	D+R	D-R
Security of data	C1	2.425	3.8	6.225	-1.375
Data Connectivity and power	C2	3.642	3.34	6.982	0.302
Storage capacity	C3	3.449	2.375	5.824	1.074
Lack of standardization.	C4	2.49	3.761	6.251	-1.271
Lack of resources and infrastructure	C5	4.008	2.456	6.464	1.552
the requirement of advanced software	C6	3.794	3.46	7.254	0.334
customer and supplier relationship management	C7	3.136	2.7	5.836	0.436
Complicated processes	C8	3.828	2.903	6.731	0.925
Unemployment	C9	2.17	3.021	5.191	-0.851
Top management commitment/policy	C10	2.636	3.762	6.398	-1.126

3-4- Entropy Technique for Decision Making

The entropy approach is being used for the evaluation of weightage of the criteria. Entropy comes from the concept of thermodynamics. This approach is very helpful in estimating the significance of each criterion or factor which would be helpful in in decision making. It is quite simple than other MCDM and is error free.

Table 7. Data collection.

Criteria	Favourable			Non favourable		
Factors	C1	C2	C3	C4	C5	C6
B1	4	4	1	4	3	5
B2	4	4	4	3	5	1
B3	5	5	5	1	1	4
B4	3	1	2	5	1	3
B5	5	4	3	1	1	4
B6	3	4	2	2	5	4
B7	1	2	1	1	1	2
B8	1	1	2	1	1	1
B9	1	1	1	1	4	4
B10	2	3	4	3	2	5

In Table.7; C1: Data Connectivity and power, C2: Storage capacity, C3: requirement of advanced software, C4: customer and supplier relationship management, C5: lack of resources and C6: Complicated processes.

- **Step 1: Normalizing of a matrix**

Where, $K_{ij} = 1,2,3...n$ using Equation 2, normalized data of Table 1 is calculated and shown in Table 8.

Table 8. Criteria weight calculation using entropy approach.

	Normalized matrix					
	C1	C2	C3	C4	C5	C6
B1	0.137931034	0.137931	0.04	0.181818	0.125	0.15152
B2	0.137931034	0.137931	0.16	0.136364	0.2083333	0.0303
B3	0.172413793	0.172414	0.2	0.045455	0.0416667	0.12121
B4	0.103448276	0.034483	0.08	0.227273	0.0416667	0.09091
B5	0.172413793	0.137931	0.12	0.045455	0.0714286	0.12121
B6	0.103448276	0.137931	0.08	0.090909	0.2083333	0.12121
B7	0.034482759	0.068966	0.04	0.045455	0.0416667	0.06061
B8	0.034482759	0.034483	0.08	0.045455	0.0416667	0.0303
B9	0.034482759	0.034483	0.04	0.045455	0.1666667	0.12121
B10	0.068965517	0.103448	0.16	0.136364	0.0833333	0.15152

- **Step 2: Calculation of N_j value for each criterion Equation (6) for G_j value:**

$$G_j = -k\sum_{i=1}^{n} X_{ij} \times \ln(X_{ij}) \quad , j = 1,2 \ldots \ldots . . m \qquad (6)$$

$$k = \frac{1}{\ln(n)} \qquad (7)$$

Table 9 shows calculated Gj value using Equation 7.

- **Step 3: Weight for each criterion**

Calculation of weight for 'j' criteria using Equation 8 is shown in Table 9.

$$W_j = \frac{1-G_j}{\sum_{j=1}^{n}(1-G_j)} \quad , (\text{where, } j = 1,2\ldots n) \qquad (8)$$

Table 9. Showing the value of *Gj* and W_j.

	C1	C2	C3	C4	C5	C6
Gj	0.873874014	0.931806	0.888906	0.807311	0.91250714	0.899673
1-Gj	0.126125986	0.068194	0.111094	0.192689	0.08749286	0.100327
Wj	0.183878064	0.099419	0.161962	0.280919	0.127555139	0.146266

3-5- Technique for Order Preference by Similarity to Ideal Solution (TOPSIS) Method

This method is use for the definitive analysis of data that are received by the survey; hence a mathematical tool is used for best and authentic results.
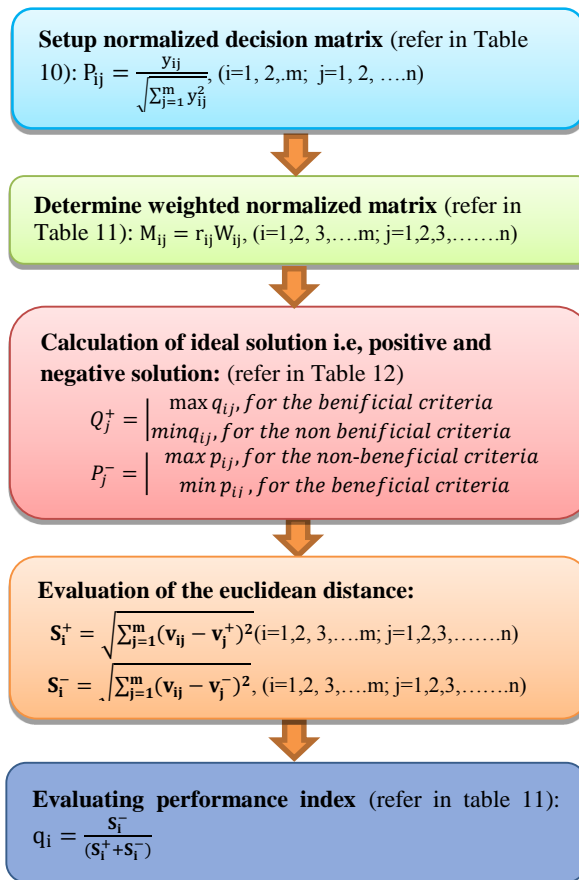
Setup normalized decision matrix (refer in Table 10): $P_{ij} = \dfrac{y_{ij}}{\sqrt{\sum_{j=1}^{m} y_{ij}^2}}$, (i=1, 2,.m; j=1, 2, ….n)

Determine weighted normalized matrix (refer in Table 11): $M_{ij} = r_{ij}W_{ij}$, (i=1,2, 3,….m; j=1,2,3,…….n)

Calculation of ideal solution i.e, positive and negative solution: (refer in Table 12)

$$Q_j^+ = \begin{vmatrix} \max q_{ij}, \text{for the benificial criteria} \\ \min q_{ij}, \text{for the non benificial criteria} \end{vmatrix}$$

$$P_j^- = \begin{vmatrix} \max p_{ij}, \text{for the non-beneficial criteria} \\ \min p_{ij}, \text{for the beneficial criteria} \end{vmatrix}$$

Evaluation of the euclidean distance:

$$S_i^+ = \sqrt{\sum_{j=1}^{m}(v_{ij} - v_j^+)^2}\,(i=1,2, 3,….m; j=1,2,3,…….n)$$

$$S_i^- = \sqrt{\sum_{j=1}^{m}(v_{ij} - v_j^-)^2},\,(i=1,2, 3,….m; j=1,2,3,…….n)$$

Evaluating performance index (refer in table 11): $q_i = \dfrac{S_i^-}{(S_i^+ + S_i^-)}$

Figure 3. Proposed methodology for TOPSIS approach.

Table 10. Setup normalization decision matrix.

	C1	C2	C3	C4	C5	C6
B1	0.386695	0.39036	0.111111	0.48507125	0.327327	0.440225
B2	0.386695	0.39036	0.444444	0.363803438	0.545545	0.088045
B3	0.483368	0.48795	0.555556	0.121267813	0.109109	0.35218
B4	0.290021	0.09759	0.222222	0.606339063	0.109109	0.264135
B5	0.483368	0.39036	0.333333	0.121267813	0.109109	0.35218
B6	0.295599	0.39036	0.222222	0.242535625	0.545545	0.35218
B7	0.096674	0.19518	0.111111	0.121267813	0.109109	0.17609
B8	0.096674	0.09759	0.222222	0.121267813	0.109109	0.088045
B9	0.096674	0.09759	0.111111	0.121267813	0.436436	0.35218
B10	0.193347	0.29277	0.444444	0.363803438	0.218218	0.440225

Table 11. Weighted normalized matrix.

	C1	C2	C3	C4	C5	C6
B1	0.071105	0.038809	0.017996	0.136266	0.041752	0.06439
B2	0.071105	0.038809	0.071983	0.102199	0.069587	0.012878
B3	0.088881	0.048511	0.089979	0.034066	0.013917	0.051512
B4	0.053328	0.009702	0.035992	0.170332	0.013917	0.038634
B5	0.088881	0.038809	0.053987	0.034066	0.013917	0.051512
B6	0.054354	0.038809	0.035992	0.068133	0.069587	0.051512

B7	0.017776	0.019405	0.017996	0.034066	0.013917	0.025756
B8	0.017776	0.009702	0.035992	0.034066	0.013917	0.012878
B9	0.017776	0.009702	0.017996	0.034066	0.05567	0.051512
B10	0.035552	0.029107	0.071983	0.102199	0.027835	0.06439
q+	0.088881	0.048511	0.089979	0.170332	0.013917	0.012878
q-	0.017776	0.009702	0.017996	0.034066	0.069587	0.06439

Table 12. Showing the value of Euclidean distances (Si+ and Si-).

	Si+	Si-
B1	0.100899	0.122109
B2	0.092061	0.117904
B3	0.141637	0.122509
B4	0.079675	0.154657
B5	0.14646	0.102291
B6	0.138699	0.06193
B7	0.172682	0.068453
B8	0.167467	0.077952
B9	0.183161	0.018961
B10	0.271323	0.099963

TOPSIS favors the longest distance from negative ideal solution maximizing cost criteria and minimizing favorable criteria and shortest distance from the positive ideal solution for maximizing the favorable criteria and minimizing cost criteria.

4- Results Analysis

The DEMATEL method examined the inter relationship between the factors has the following result as shown in Table 14. This method basically divides the group into causes and effects group. With the help of this methodology, we could find the value of D+R and D-R easily which provides logical consequences of the assumed data.

Table 13. Cause and effect analysis.

Causes	D-R	Rank
Lack of resources and infrastructure (C5)	1.552	1
Storage capacity (C3)	1.074	2
The complicated process at adoption level (C8)	0.925	3
The difference in technology adoption between Customer & suppliers (C7)	0.436	4
The requirement of advanced software(C6)	0.334	5
Effect group	**D-R**	**Rank**
Security of data (C1)	-1.375	1
Lack of standardization (C4)	-1.271	2
Top management commitment/policy (C10)	-1.126	3
Unemployment(C9)	-0.851	4

The value of D+R and D-R are the most important factor in determining the criteria of the value of D_i, R_j, D+R, and D-R for the above-calculated matrix have the following significance as the D-R value provides us the knowledge of classifying our challenges into cause and effect group. As the result obtained from the matrix above, we can conclude that the negative value of D-R represents effect challenges and a positive value represents the cause challenges. We compared the both positive and negative value for the degree of cause and effect group. In Table 11, lack of resources and infrastructure (C5) is ranked first in the cause group which means it will highly influence other factor together with other factors are dependent on this factor as if there is no proper resources and infrastructure available then implementing IIoT will be an issue. Second higher influence factor is (C3) as storage is one the crucial factor which influences every factor because without having proper storage capacity complex security program cannot be implemented. The third most important factor is the Complicated process at adoption level (C8) which means

implementing of IIoT have to the issue of adoption at higher level i.e. higher managerial and industrialist is not showing interest and they feel insecure to invest in it.

Similarly for the Effect group have negative value of D-R as they are receiver group, these factors are dependent on other factor and first among them are Security of data (C1) as security is the major concern as it depends on every other factor for its proper and efficient functioning i.e. without proper implementation of others factors security cannot be achieved. The second most dependent factor is the lack of standardization as proper standardization and format must be there for efficient functioning without having proper guidelines and format it cannot be implemented. Top management commitment/policy (C10) is ranked third most dependent issue as top commitment and support are highly demanding without their proper guidance and support it cannot be implemented.

Alternatively, D+R shows the higher degree of the relation of one factor on another factor. The result shows that C6 (requirement of advanced software) for the IIoT is having the highest value for D+R value. Data connectivity and power (C2) is the second most and Lack of resources and infrastructure (C5) is ranked third in the list having a higher degree of relation with another factor.
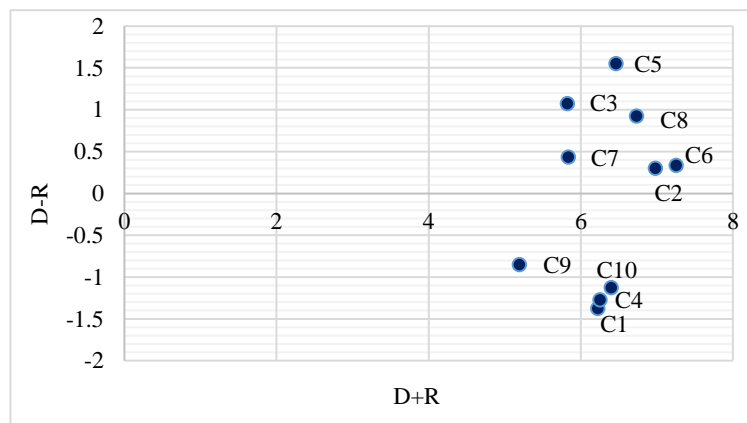

Figure 4. Causal diagram.

Table 14. The values of performance index and rank.

Notation	Enablers of blockchain	Pi	Rank
B1	Multi-node storage of data	0.547556	3
B2	Enhance cyber security	0.561542	2
B3	Efficient and prompt processing	0.463794	4
B4	Enhance transparency of data	0.65999	1
B5	Reducing scalability issue	0.411218	5
B6	Infrastructure design and setup cost	0.308681	6
B7	Password security	0.283879	8
B8	Issue of global acceptance	0.317628	7
B9	Lack of skills/knowledge	0.093812	10
B10	Hardware compatibility issues	0.269234	9

(a) **Enhance transparency of data:** This factor is having the highest performance index of 0.659 which highly influence the issue and challenges of IIoT. The blockchain provide the transparency of data i.e. it shows exact value and information which helps IIoT, as now problems of IIoT can easily be traceable and notified with the help of blockchain transparency as it can track exact problems at each step.

(b) **Enhance cyber security:** This is the second most influential factor having performance index of 0.561 which helps us in tackling the issue of IIoT. Cyber security is the major threat to every sector so as for the industrial IoT, now with the help of blockchain which facilitates higher level of security as compared to IoT. The blockchain has advance security setup which helps to solve the issue of IIoT.

(c) **Multi-node storage of data:** It has the performance index of 0.547 as ranked as the third most influential factor which affects the issues of IIoT. Blockchain have multiple nodes which means it stores information in the multiple nodes and so it cannot be traceable and hacked because millions of nodes are interconnected in such a way that

hacking or misusing of any nods data would lead to overall failure. As data are not directly being stored at one exact location.

(d) Efficient and prompt processing: These having the performance index of 0.463 and ranked fourth most influencing enablers of blockchain. This enabler helps in improving the issue of IIoT as it facilitates complex processing of data in a very easy manner and also it delivers information at the exact time.

(e) Reducing scalability issue: It is ranked fifth among all factor and have performance index of 0.4112 and it helps in tackle out the issue of IIoT as it facilitates scalability issue which means now the problem of securing complex data can be cured easily.

(f) Infrastructure design and setup cost: It is ranked the six in the rank table. It helps in solving the issue of IIoT because securing data of large industries require huge setup of infrastructure and design which the blockchain can facilitate.

(g) Issue of global acceptance: Even though the blockchain is not globally accepted everywhere but plays a greater role in crypto currency.

(h) Password security: Blockchain can help in improving the security of IIoT as it enhances higher security with multiple passwords at each node and data can only be accessed with particular operational keys. These having the performance index of 0.283.

(i) Hardware compatibility issues: These factors having the performance index of 0.269 as hardware issue of tackling heavy machine can be easily be resolved by using blockchain.

(j) Lack of skills/knowledge: Implementing blockchain require high skilled and knowledgeable employees which facilitates their best output and using their skills for the resolving of IIoT issue is quite easy for them. This enabler having the performance index of 0.093.

This ranking is then ranked into two groups, the first group having performance index greater than 0.4 i.e. enhance Transparency of data, enhance cyber security, multi-node storage of data, efficient and prompt processing, and reducing scalability issue. On the other hand, second group having performance index less than 0.4 have factors like infrastructure design and setup cost, issue of global acceptance, password security, hardware compatibility issues, lack of skills/knowledge.
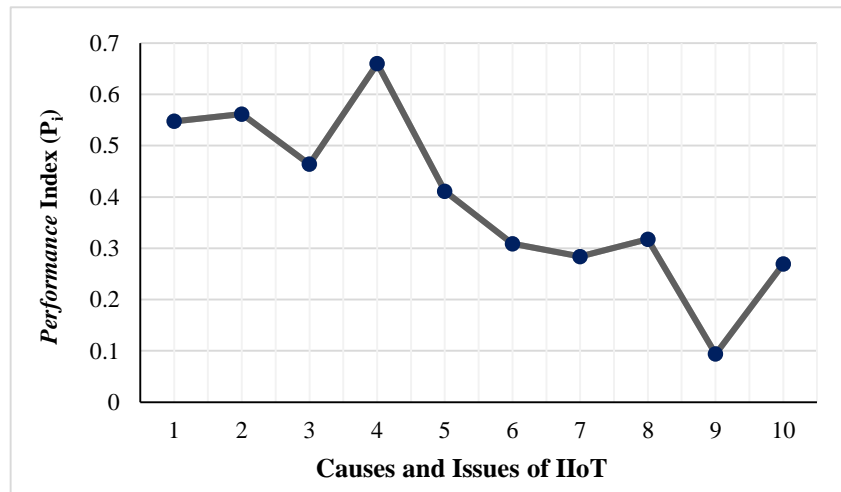

Figure 5. Resulted plot of TOPSIS analysis.

TOPSIS is applied to determine the most influential enablers of blockchain that can resolve the major six issue of IIoT.

5- Conclusion and Future Scopes

From the DEMATEL approach we have calculated the top challenges of IIoT for implementation in the industries, these factors are not favorable factors and in causal diagram these have value above the origin and their plot is above x axis. Data connectivity and power as for high level of security there is always a need of higher level of software and advance power setup which is lacking in the several industries. So, can be resolved by blockchain factors infrastructure design and setup cost (B6) as it provides huge setup of infrastructure and design. The second major issue

is storage capacity which can be resolved by the blockchain factor hardware compatibility issues (B10) as; hardware issue of tackling heavy machine and storage issue can be easily be resolved. Lack of resources and infrastructure is also a major concern which is resolved by the infrastructure design and setup cost (B6). The other important issue is customer and supplier relationship management as implementing IIoT requires better understanding between customers and producers, the top management system must take care of all needs and demands of customers and the proper survey should be made.

Furthermore, entropy approach was made for determining the weight of each factor in which customer and supplier management is having the value of 0.28091 then followed by connectivity and power having the value of 0.18387. Then, TOPSIS is applied to determine the most influential enablers of blockchain which could resolve the major six issue of IIoT; which are as follows enhance transparency of data (B4) having pi value of 0.6599, enhance cyber security (B2) having a pi value of 0.5615, multi-node storage of data (B1) having value 0.547, efficient and prompt processing (B3) of p_i value 0.4637 and so on. This research work shall be a beneficial scope for all the industries running on automation.

In this paper emphasis is done to track out the most important factor and issue that hinders for the successful implementation of IIoT in manufacturing industries and government and other policies should take care of these factors in future before implementing them.

6- Conflict of Interest

The author declares that there is no conflict of interests regarding the publication of this manuscript. In addition, the ethical issues, including plagiarism, informed consent, misconduct, data fabrication and/or falsification, double publication and/or submission, and redundancies have been completely observed by the authors.

7- References

[1] Goel, Abhinav and Alhosani, Ali, "India: A Macro Level Analysis of World's Fastest Growing Economy" (May 3, 2007). doi:10.2139/ssrn.1271007.

[2] Khodadadi, F., A.V. Dastjerdi, and R. Buyya. "Internet of Things: An Overview." Internet of Things (2016): 3–27. doi:10.1016/b978-0-12-805395-9.00001-0.

[3] Al-Fuqaha, Ala, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari, and Moussa Ayyash. "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications." IEEE Communications Surveys & Tutorials 17, no. 4 (2015): 2347–2376. doi:10.1109/comst.2015.2444095.

[4] Faccioni Filho, Mauro, Designing 'Things' for the Internet of Things (October 6, 2016). doi:10.2139/ssrn.2847674.

[5] hodadadi, F., A.V. Dastjerdi, and R. Buyya. "Internet of Things: An Overview." Internet of Things (2016): 3–27. doi:10.1016/b978-0-12-805395-9.00001-0.

[6] Aitzhan, Nurzhan Zhumabekuly, and Davor Svetinovic. "Security and Privacy in Decentralized Energy Trading Through Multi-Signatures, Blockchain and Anonymous Messaging Streams." IEEE Transactions on Dependable and Secure Computing 15, no. 5 (September 1, 2018): 840–852. doi:10.1109/tdsc.2016.2616861.

[7] British Standards Document (BS ISO 22153) "Electric Actuators for Industrial Valves General Requirements" (January 2020). doi:10.3403/30364159u.

[8] Neises, Jurgen, George Moldovan, Thomas Walloschke, and Bianca Popovici. "Trustworthiness in Supply Chains : A Modular Extensible Approach Applied to Industrial IoT." 2020 Global Internet of Things Summit (GIoTS) (June 2020). doi:10.1109/giots49054.2020.9119580.

[9] Jung, Jieun, Byunghun Song, Kym Watson, and Thomas Usländer. "Design of Smart Factory Web Services Based on the Industrial Internet of Things." Proceedings of the 50th Hawaii International Conference on System Sciences (2017). doi:10.24251/hicss.2017.716.

[10] Monshizadeh, Mehrnoosh, and Vikramajeet Khatri. "IoT Security." A Comprehensive Guide to 5G Security (January 5, 2018): 245–266. doi:10.1002/9781119293071.ch11.

[11] Liao, Yongxin, Eduardo de Freitas Rocha Loures, and Fernando Deschamps. "Industrial Internet of Things: A Systematic Literature Review and Insights." IEEE Internet of Things Journal 5, no. 6 (December 2018): 4515–4525. doi:10.1109/jiot.2018.2834151.

[12] Fernandez-Carames, Tiago M., and Paula Fraga-Lamas. "A Review on the Application of Blockchain to the Next Generation of Cybersecure Industry 4.0 Smart Factories." IEEE Access 7 (2019): 45201–45218. doi:10.1109/access.2019.2908780.

[13] Epiphaniou, Gregory, Herbert Daly, and Haider Al-Khateeb. "Blockchain and Healthcare." Advanced Sciences and Technologies for Security Applications (2019): 1–29. doi:10.1007/978-3-030-11289-9_1.

[14] He, Jiahao, Guangyuan ZHANG, Jiheng Zhang, and Rachel Zhang. "An Economic Model of Blockchain: The Interplay Between Transaction Fees and Security." SSRN Electronic Journal (2020). doi:10.2139/ssrn.3616869.

[15] Wang, Xunhua, Brett Tjaden, and M. Hossain Heydari. "Bitcoin for E-Commerce." Encyclopedia of E-Commerce Development, Implementation, and Management (2016): 1013–1030. doi:10.4018/978-1-4666-9787-4.ch072.

[16] "Towords Secure Data Management Using Blockchain in Iot Enabled Environment." Regular Issue 9, no. 1 (November 10, 019): 1759–1763. doi:10.35940/ijitee.l2666.119119.

[17] Díaz, Manuel, Cristian Martín, and Bartolomé Rubio. "State -of-the-Art, Challenges, and Open Issues in the Integration of Internet of Things and Cloud Computing." Journal of Network and Computer Applications 67 (May 2016): 99–117. doi:10.1016/j.jnca.2016.01.010.

[18] Cui, Laizhong, Shu Yang, Ziteng Chen, Yi Pan, Zhong Ming, and Mingwei Xu. "A Decentralized and Trusted Edge Computing Platform for Internet of Things." IEEE Internet of Things Journal 7, no. 5 (May 2020): 3910–3922. doi:10.1109/jiot.2019.2951619.

[19] Zhao, Shanshan, Shancang Li, and Yufeng Yao. "Blockchain Enabled Industrial Internet of Things Technology." IEEE Transactions on Computational Social Systems 6, no. 6 (December 2019): 1442–1453. doi:10.1109/tcss.2019.2924054.

[20] Roy, Chandana, Sudip Misra, and Saswati Pal. "Blockchain-Enabled Safety-as-a-Service for Industrial IoT Applications." IEEE Internet of Things Magazine 3, no. 2 (June 2020): 19–23. doi:10.1109/iotm.0001.1900080.

[21] Ram Kumar, R, Sreerag Menon, and Nima S Nair. "Blockchain Solutions for Security Threats in Smart Industries." 2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC) (March 2020). doi:10.1109/iccmc48092.2020.iccmc-000141.

[22] Cao, Jiangdong, and Wei Cao. "Bitcoin Mining, the Way to Process Transaction Information or the Way to Make Money?" INSIST 4, no. 1 (April 1, 2019): 191. doi:10.23960/ins.v4i1.191.

[23] Zorgui, Marwen, and Zhiying Wang. "Centralized Multi-Node Repair Regenerating Codes." IEEE Transactions on Information Theory 65, no. 7 (July 2019): 4180–4206. doi:10.1109/tit.2019.2898660.

[24] Li, Xiaoqi, Peng Jiang, Ting Chen, Xiapu Luo, and Qiaoyan Wen. "A Survey on the Security of Blockchain Systems." Future Generation Computer Systems 107 (June 2020): 841–853. doi:10.1016/j.future.2017.08.020.

[25] Eyal, Ittay, and Emin Gün Sirer. "Majority Is Not Enough: Bitcoin Mining Is Vulnerable." Lecture Notes in Computer Science (2014): 436–454. doi:10.1007/978-3-662-45472-5_28.

[26] Apostolaki, Maria, Gian Marti, Jan Muller, and Laurent Vanbever. "SABRE: Protecting Bitcoin Against Routing Attacks." Proceedings 2019 Network and Distributed System Security Symposium (2019). doi:10.14722/ndss.2019.23252.

[27] Fernandez-Carames, Tiago M., and Paula Fraga-Lamas. "A Review on the Use of Blockchain for the Internet of Things." IEEE Access 6 (2018): 32979–33001. doi:10.1109/access.2018.2842685.

[28] Beck, Roman, Michel Avital, Matti Rossi, and Jason Bennett Thatcher. "Blockchain Technology in Business and Information Systems Research." Business & Information Systems Engineering 59, no. 6 (November 15, 2017): 381–384. doi:10.1007/s12599-017-0505-1.

[29] Reyna, Ana, Cristian Martín, Jaime Chen, Enrique Soler, and Manuel Díaz. "On Blockchain and Its Integration with IoT. Challenges and Opportunities." Future Generation Computer Systems 88 (November 2018): 173–190. doi:10.1016/j.future.2018.05.046.

[30] Zyskind, Guy, Oz Nathan, and Alex "Sandy" Pentland. "Decentralizing Privacy: Using Blockchain to Protect Personal Data." 2015 IEEE Security and Privacy Workshops (May 2015). doi:10.1109/spw.2015.27.

[31] Nawaz, Samsudeen Sabraz, and Mohamed Hussain Thowfeek. "Blockchain Technology Adoption by Chain Professionals." International Journal of Psychosocial Rehabilitation 24, no. 1 (January 31, 2020): 121–137. doi:10.37200/ijpr/v24i1/pr200113.

[32] Rimba, Paul, An Binh Tran, Ingo Weber, Mark Staples, Alexander Ponomarev, and Xiwei Xu. "Comparing Blockchain and Cloud Services for Business Process Execution." 2017 IEEE International Conference on Software Architecture (ICSA) (April 2017): 257-260. doi:10.1109/icsa.2017.44.

[33] Lemieux, Victoria Louise. "Trusting Records: Is Blockchain Technology the Answer?" Records Management Journal 26, no. 2 (July 18, 2016): 110–139. doi:10.1108/rmj-12-2015-0042.

[34] Forsstrom, Stefan, Ismail Butun, Mohamed Eldefrawy, Ulf Jennehag, and Mikael Gidlund. "Challenges of Securing the Industrial Internet of Things Value Chain." 2018 Workshop on Metrology for Industry 4.0 and IoT (April 2018): 218-223. doi:10.1109/metroi4.2018.8428344.

[35] Sadeghi, Ahmad-Reza, Christian Wachsmann, and Michael Waidner. "Security and Privacy Challenges in Industrial Internet of Things." Proceedings of the 52nd Annual Design Automation Conference on - DAC '15 (2015): 1-6. doi:10.1145/2744769.2747942.

[36] Mahmoud, Rwan, Tasneem Yousuf, Fadi Aloul, and Imran Zualkernan. "Internet of Things (IoT) Security: Current Status, Challenges and Prospective Measures." 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST) (December 2015): 336-341. doi:10.1109/icitst.2015.7412116.

[37] Mumtaz, Shahid, Ahmed Alsohaily, Zhibo Pang, Ammar Rayes, Kim Fung Tsang, and Jonathan Rodriguez. "Massive Internet of Things for Industrial Applications: Addressing Wireless IIoT Connectivity Challenges and Ecosystem Fragmentation." IEEE Industrial Electronics Magazine 11, no. 1 (March 2017): 28–33. doi:10.1109/mie.2016.2618724.

[38] Zheng, Pai, Zuoxu Wang, and Chun-Hsien Chen. "Industrial Smart Product-Service Systems Solution Design via Hybrid Concerns." Procedia CIRP 83 (2019): 187–192. doi:10.1016/j.procir.2019.02.129.

[39] Jiang, Hai, Feng Shen, Su Chen, Kuan-Ching Li, and Young-Sik Jeong. "A Secure and Scalable Storage System for Aggregate Data in IoT." Future Generation Computer Systems 49 (August 2015): 133–141. doi:10.1016/j.future.2014.11.009.

[40] Sisinni, Emiliano, Abusayeed Saifullah, Song Han, Ulf Jennehag, and Mikael Gidlund. "Industrial Internet of Things: Challenges, Opportunities, and Directions." IEEE Transactions on Industrial Informatics 14, no. 11 (November 2018): 4724–4734. doi:10.1109/tii.2018.2852491.

[41] Al-Qaseemi, Sarah A., Hajer A. Almulhim, Maria F. Almulhim, and Saqib Rasool Chaudhry. "IoT Architecture Challenges and Issues: Lack of Standardization." 2016 Future Technologies Conference (FTC) (December 2016). doi:10.1109/ftc.2016.7821686.

[42] Miroshnik, Victoria W. "Study C: Organizational Culture and Organizational Commitment in the Indian Subsidiary." Organizational Culture and Commitment (2013): 169–198. doi:10.1057/9781137361639_8.

[43] Gierej, Sylwia. "The Framework of Business Model in the Context of Industrial Internet of Things." Procedia Engineering 182 (2017): 206–212. doi:10.1016/j.proeng.2017.03.166.

[44] Wan, Jiafu, Shenglong Tang, Zhaogang Shu, Di Li, Shiyong Wang, Muhammad Imran, and Athanasios Vasilakos. "Software-Defined Industrial Internet of Things in the Context of Industry 4.0." IEEE Sensors Journal (2016): 1–1. doi:10.1109/jsen.2016.2565621.

[45] YU, Jie, Nachiappan Subramanian, Kun Ning, and David Edwards. "Product Delivery Service Provider Selection and Customer Satisfaction in the Era of Internet of Things: A Chinese e-Retailers' Perspective." International Journal of Production Economics 159 (January 2015): 104–116. doi:10.1016/j.ijpe.2014.09.031.

[46] Chen, Baotong, Jiafu Wan, Lei Shu, Peng Li, Mithun Mukherjee, and Boxing Yin. "Smart Factory of Industry 4.0: Key Technologies, Application Case, and Challenges." IEEE Access 6 (2018): 6505–6519. doi:10.1109/access.2017.2783682.

[47] Biswas, Abdur Rahim, and Raffaele Giaffreda. "IoT and Cloud Convergence: Opportunities and Challenges." 2014 IEEE World Forum on Internet of Things (WF-IoT) (March 2014). doi:10.1109/wf-iot.2014.6803194.

[48] Vermeulen, Ben, Jan Kesselhut, Andreas Pyka, and Pier Saviotti. "The Impact of Automation on Employment: Just the Usual Structural Change?" Sustainability 10, no. 5 (May 21, 2018): 1661. doi:10.3390/su10051661.

[49] K., Jekishan, and Ankit Desai. "IoT: Networking Technologies and Research Challenges." International Journal of Computer Applications 154, no. 7 (November 17, 2016): 1–6. doi:10.5120/ijca2016912181.

[50] Lin, Ru-Jen. "Using Fuzzy DEMATEL to Evaluate the Green Supply Chain Management Practices." Journal of Cleaner Production 40 (February 2013): 32–39. doi:10.1016/j.jclepro.2011.06.010.

[51] Zhu, Qinghua, Joseph Sarkis, and Yong Geng. "Barriers to Environmentally-Friendly Clothing Production Among Chinese Apparel Companies." Asian Business & Management 10, no. 3 (June 8, 2011): 425–452. doi:10.1057/abm.2011.15.

[52] Boyes, Hugh, Bil Hallaq, Joe Cunningham, and Tim Watson. "The Industrial Internet of Things (IIoT): An Analysis Framework." Computers in Industry 101 (October 2018): 1–12. doi:10.1016/j.compind.2018.04.015.