Protected Industrial Iot: Blockchain Process Using Credit-Based Consensus Process

Buriki Eknath[1], D. SASIKALA[2]
[1,2]Scholar, MTech CNIS,Department of CSE, Nalla Malla Reddy Engineering College, Hyderabad

Email: [1]8eknath8@gmail.com,[2]godnnature@gmail.com

ABSTRACT: In the active scheme Industrial Internet of Things (IIoT) carries out essential concern in lieu of Industry 4.0, individuals remain steadfast in realizing a universal, extensible and protected IIoT structure embraced in a number of businesses. In established methods, by the advent of blockchain(BC), conception of merging BC plus IoT maintains achieved extensive involvement by way of an access control arrangement set up at the BC technology to get along IoT devices. Yet, it is not wholly put upon the disseminated mode for the reason of handling of the key controlling axis. The minute it's seized up or ruined, IoT devices attached to it befits inaccessible. In purported scheme that shield reliable data concealment, a data authority justified order is structured to standardize the right to use the sensor data. Investigation outcomes concluded that credit-centered proof-of-work (PoW) besides data compliance control have a reliable attainment in IoT devices.

Keywords: Sensor Data, IIoT, BC system, credit-centered PoW, Directed Acyclic Graph (DAG) structured BC.

1. INTRODUCTION

At this time the BC subsists, the hint of fusing BC and IoT has put on noteworthy introspection [3]–[5]. By inducing aspects of tamper-proof then distributed concord practice in BC resolving safety concerns in IIoT processes. Presently, numerous persistent research practices are fulfilled on this theme. IIoT eases as well as expurgated by flaws, moderate budgets, progresses proficiency and boost protection in industrial and engineering practices that are loaded with possibilities to turn into manufacturing arena an advanced plane of veracity, readiness and expandability. Still, safety outbreaks and crashes may well root abundant hitch intruding the worldwide IoT set-up [1] that prevails over every of these gains. Instead, the vital stockpile is at risk to SPOF besides vindictive attacks as DDoS, Sybil outbreak [2] that can't assure amenities obtainability.

The three fold core confronts are briefed as below: 1) The dealing including proficiency plus protection 2) Synchronicity of clarity and concealment 3) Engagements concerning excessive multiple reckonings and little output in a production process. Further, the type consent happenings at the same time in chain-shaped BCs can't oblige best usage of maximum rate of facts relocation within a set path inside IIoT processes. Thus toward progress extent of BC and sustaining the requisites of persistent operations in IIoT processes fit to be the third barrier. To present with these technical sabotages, a BC process with credit-centered consent process is held out for IIoT. To decline the power-depletion in consent methodology a self-adaptive PoW logic is agreed for energy confined IoT appliances amending the effort of PoW built upon intersections' actions that cut the barrier instead of honest connections but rising in favor of malign nodules. Similarly a log on checking practice centered at the precise identical cryptology form is executed around the apparent BC structure that is liable for a malleable data authority directing routine for users. This process frame is put up centered by the DAG structured BC that perk up the process productivity by inducing this consent archetype not match up in time.

2. LITERATURE SURVEY

Review paper [1] scientifically analyses IoT cybersecurity with the significant concerns as security and union of unrelated smart gadgets plus information communication technologies (ICT). Research work [2] brings about the innovative SybilLimit modus operandi that influences the identical instinct according to SybilGuard then submits intensely enriched besides proximate-optimal assurances. Manuscript [3] confirms that the suggested BC-based smart home edifice is defended by precisely studying its protection relevant to the eventual defense intents of privacy, veracity, and accessibility. Document [4] recommends a different scheme on behalf of defining duties and approvals within IoT remaining as a wholly disseminated log on controller process. In research work [5] a decentralized trust management scheme was set forth in VANETs centered upon BC methods. Here, vehicles authorize inward notes after close vehicles by Bayesian Interpretation Archetype. With using the services of the shared PoW and proof-of-stake consent process, the furthest aggregate rate of equalizers (stake) exists within the chunk, the simpler RSU spot the special occurrence for the hash function. In work [6][11] a credit-centered compensation scheme follows on preparing out to upkeep swift and regular energy handling. An ultimate rating strategy by Stackelberg sport aimed at credit-centered finances stays consistently forestalled. Manuscript [7] first introduces a unique conception of edge computing for mobile BC then presenting a fiscal approach for its resource organization. Research [8] presents Vegvisir, a split-indulgent BC for deployment inside energy-confined IoT atmospheres using restricted web linkage[9]. This exists as a favored, DAG-structured BC that is applied towards constructing pooled, loss resilient facts depot that retains trajectory of facts attribution [12].

3. EXISTING SYSTEM

IIoT structures are liable to SPOF and vindictive attacks unaccountable for persistent amenities. Exceptional toward the buoyancy plus security prospective of BC, the indication of inclusion of BC with IoT increases significantly[13]. But, BC is energy-congregated and less-productivity and non-exist that is apt in lieu of energy-confined IoT gadgets. Towards holding these encounters, a BC structure using credit-centered consent process is stated for IIoT. **Disadvantage**: These systems cannot provide stable services.

4. PROPOSED SYSTEM

Credit-centered PoW process is intended in lieu of IoT gadgets that is assuring process protection plus operation competence concurrently. For defending delicate facts concealment, a facts expert directing scheme exists regarded ordering the access to sensor data[14]. Besides, this process is constructed centered on DAG-shaped BCs that remains further proficient than the satoshi-style BC in enactments. Implementation of this system is done upon Raspberry Pi, carrying out Case studies aimed at the smart factory[15]. Credit-centered PoW process plus facts log on controller are protected in addition proficient in IIoT. **Advantages of Proposed System:** 1. This protects the sensitive data confidentiality. 2. It provides system security and transaction efficiency.

UML Diagrams:

Class Diagram For Industrial Manager:

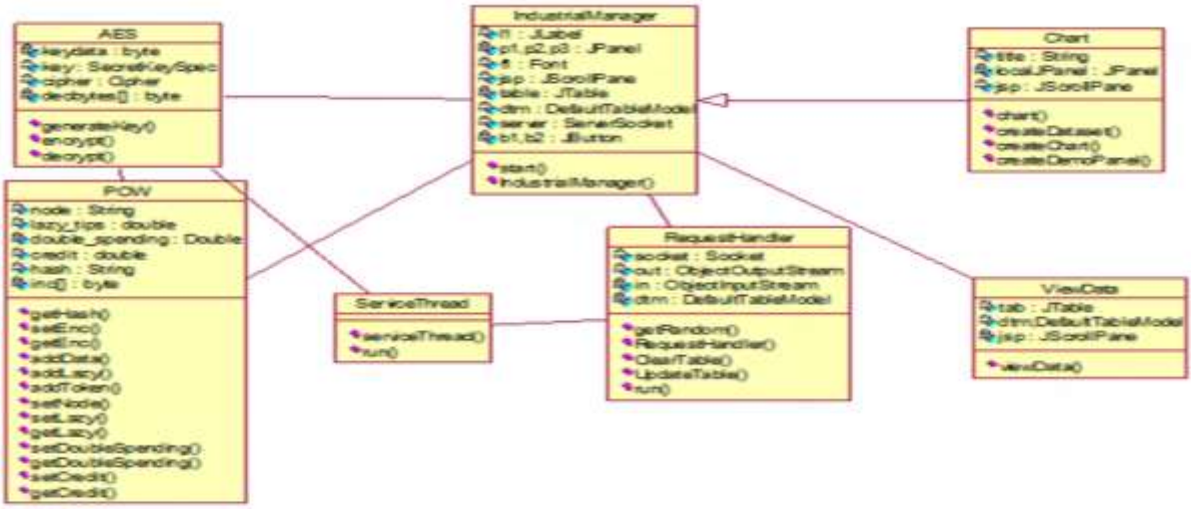


Fig 1. Class diagram for Industrial Manager

The classes signify mutually the core entities, alliances within the usage then the classes en route for programming.

Class Diagram For Wireless Sensor:

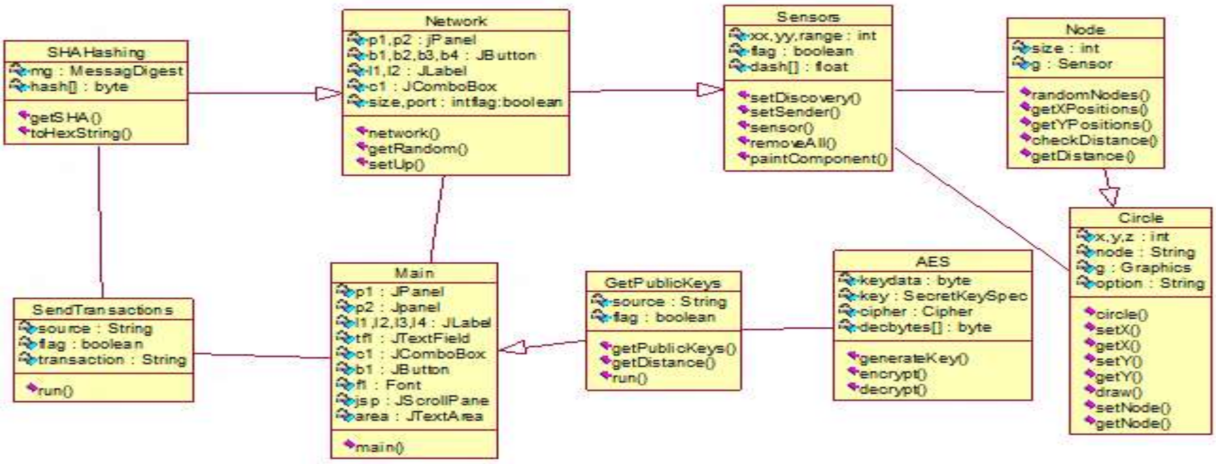


Fig 2. Class Diagram for Wireless Sensor

Use-case diagram:

A use-case drawing reveals the diverse categories of manipulators of a process then their numerous means that those collaborate using it.

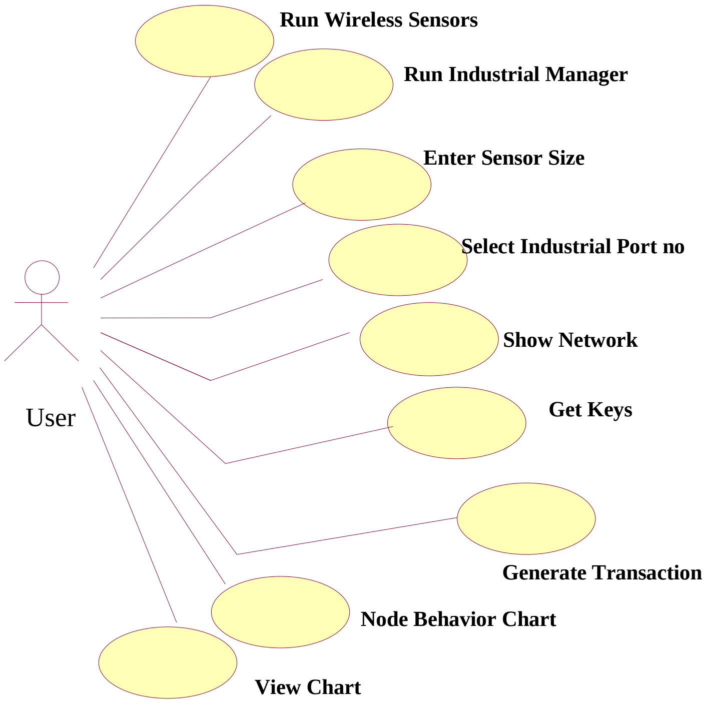


Fig 3. Use-case diagram

Sequence Diagram:

A sequence diagram in Fig 4. indicates entity interfaces set up in time series[16]. Collaboration diagram in Fig 5. imply a blend of data procured as class, system, and use-case charts outlining equally the inert configuration and vibrant depiction of a scheme. Component Diagram in Fig 6. are drawn to elucidate the configuration of fairly multifaceted schemes. Deployment diagram in Fig 7. mockups the real deployment of items on nodes. A single node in a deployment diagram may theoretically denote numerous tangible nodes, for instance a gathering of database servers.

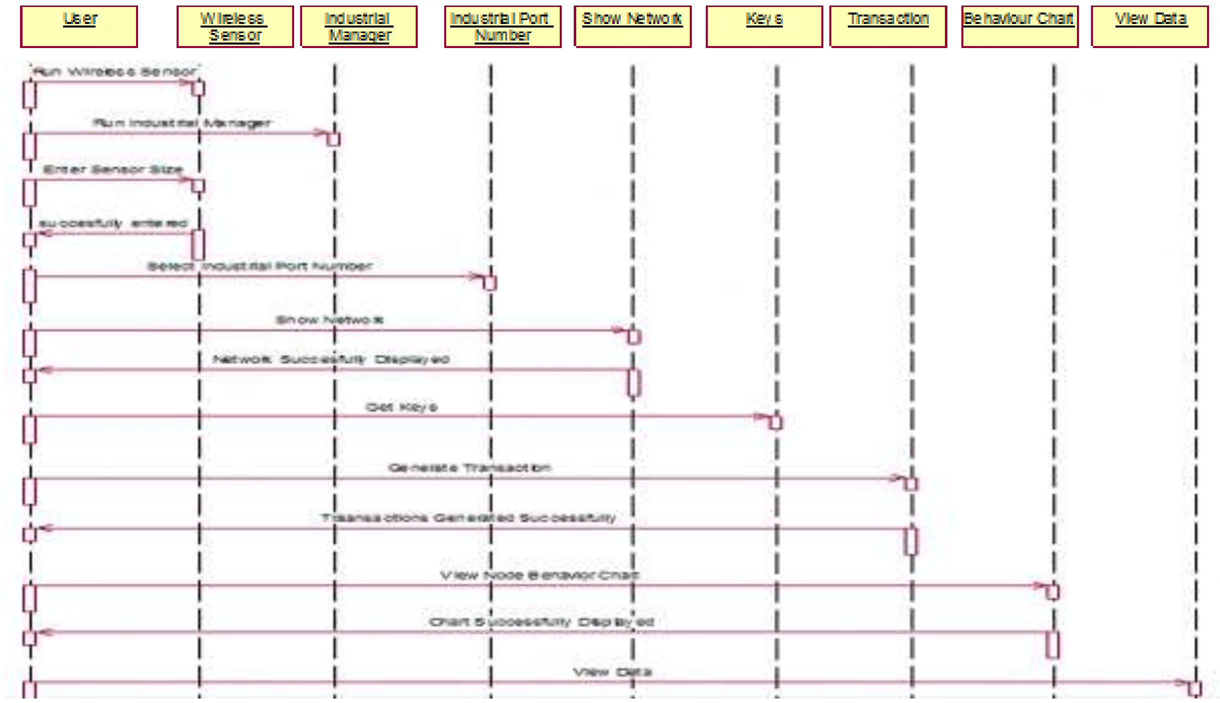


Fig 4. Sequence Diagram

Collaboration Diagram

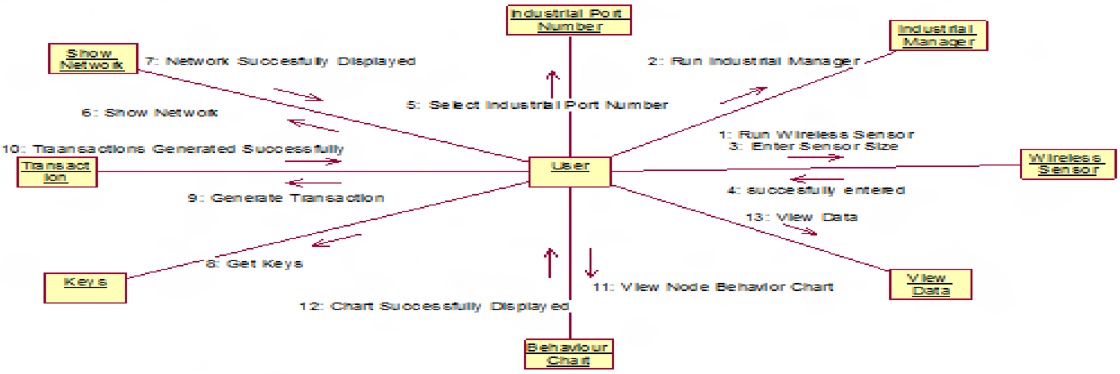
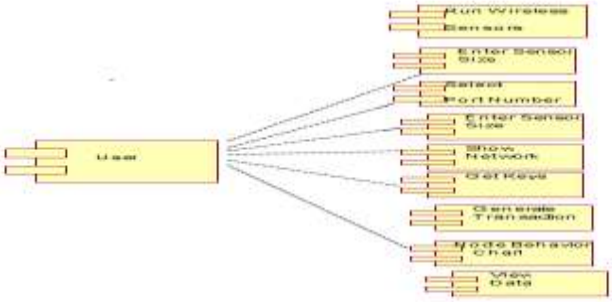


Fig 5. Collaboration Diagram

Component Diagram and Deployment Diagram



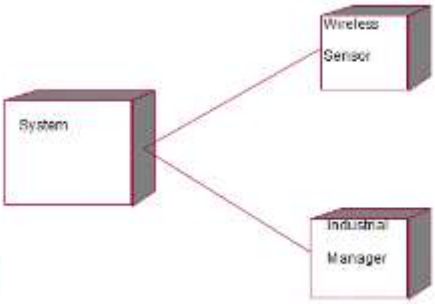


Fig 6. Component Diagram

Fig 7. Deployment Diagram

Activity diagram in Fig 8. is mainly a flowchart to express the steps forward starting from one interpretation of an activity to an advanced activity. This headway can be successive, bifurcated or simultaneous.

Activity diagram:

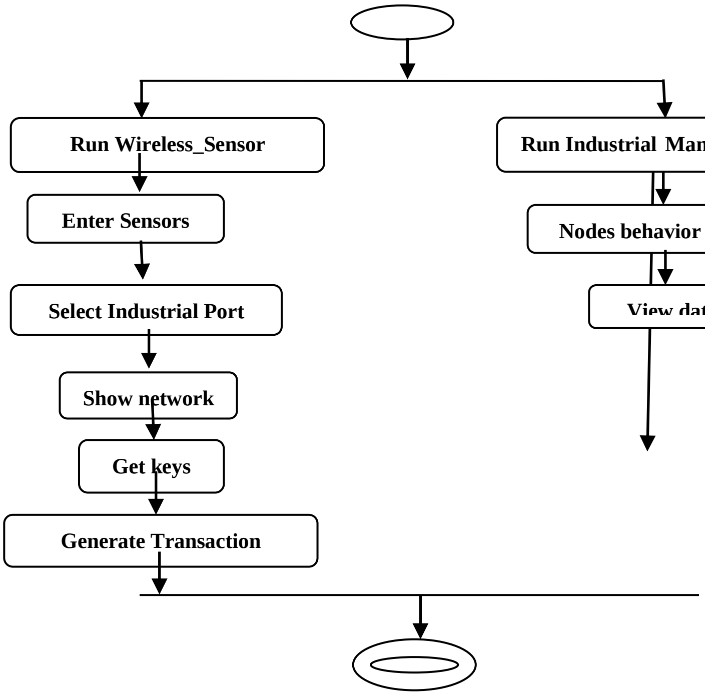


Fig 8. Activity diagram

Data Flow Diagram: It is a model that expounds the opening of data in a practice.

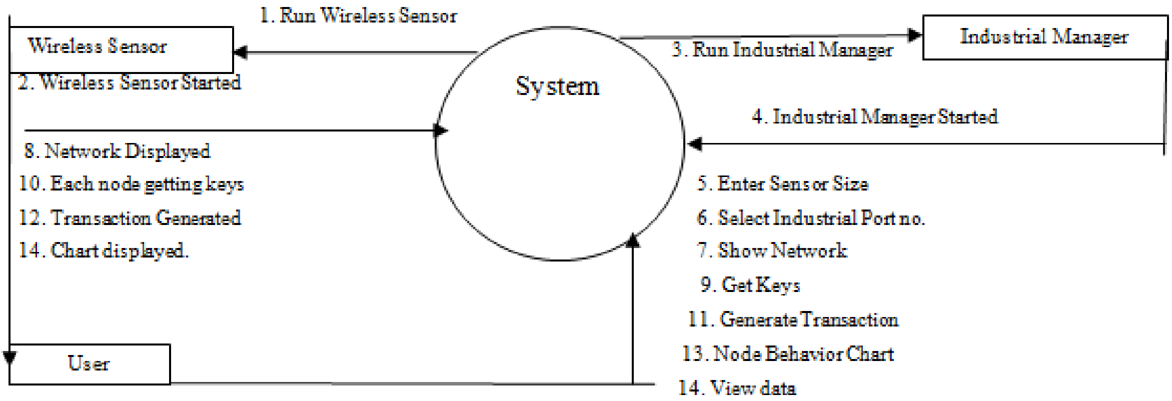


Fig 9. Data Flow Diagram

External Interface Prerequisites: User Interface - An easy accessible Java GUI**.**
Hardware - Collaboration concerning user besides the cabinet realized over Java resources**.**
Software - JAVA1.6**. Operating Environments -** Windows XP, Linux**.**
Hardware Prerequisites: Pentium –IV processor with Ghz 1.1 as speed , 256 MB (min) RAM, 20 GB HDD, Regular Windows Keyboard, 2 /3 Button Mouse and SVGA Monitor**.**
Software Prerequisites: Windows XP - Operating System, Java Programming Language and MySQL Database**.**

5. IMPLEMENTATION

Using Java, Applications and applets, AWT and Swings: GUIs, Components, Containers and types of it: Basic GUI Logic, Creating a Frame.
Method1: Here, it intends in constructing frame through run on Frame class that results stated within java.awt package. Three techniques are used here: **setTitle**, **SetVisible** and **SetSize.**
Method 2: Here, prefer producing the Frame class case aimed at constructing frame window.
Types of Components: 1) Labels 2) Buttons 3) CheckBox 4) Radio Button 5) Choice 6) List 7) TextField 8) TextArea.
Layout Managers: Java has a number of predefined **LayoutManager** classes that are beneficial and is puts in the use that are availed namely, **FlowLayout, BorderLayout**, **GridLayout.**
Swings: Swing utilizes Java instructions using a GUI with components that ensues integral Swing toolkit: such as labels, buttons, list, tree and table controllers. Every AWT malleable sections are structured using the Java Swing that moreover comprises the elementary user interfaces, for example drag & drop, event handling, customizable painting etc.
Attributes in Java Foundation Classes (JFC) craft programs are accessible with diverse language styles, capacity towards enhancing valuable graphics, serviceability, and so on. Appropriate abundant constituents confined within Swing toolkit, for instance, buttons, check boxes, text, tables and so on. Specific extremely rudimentary constituents too are responsible for cutting-edge functionality. As an illustration, text fields formulate aligned text entry key in or cipher field performance. Additionally, the file browsers and dialogues are applied permitting to one's prerequisite and are also custom-built. The components in AWT are **JTabbedPane class : JMenuBar, JMenu, JMenuItem**

6. TESTING:

Table 1. Sample Cases (SC)

SC ID	SC Name	SC Description	SC Steps			SC Status	SC Priority
			Step	**Expected**	**Actual**		
01	Run wireless sensor and industrial Manager	Verify the wireless sensor and industrial Manager started or not	Without wireless sensor and industrial Manager	Users cannot do further operations	Wireless sensor and industrial Manager are started	**High**	**High**
02	Enter sensor size	Verify sensor size is enter or not	Without entering the sensor size	It cannot display the sensor size	It can display the sensor size	**High**	**High**

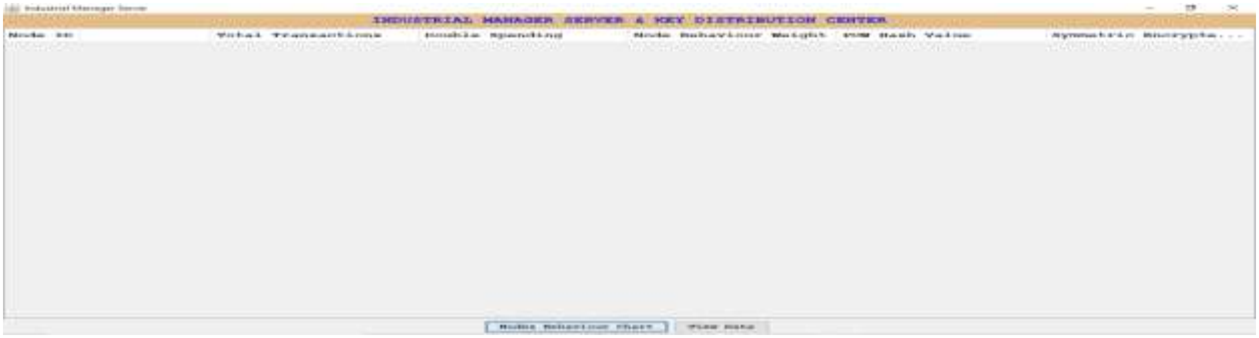
03	Show Network	Verify the network is displayed or not	Without selecting the industrial port number and sensor size	Network cannot be generated	Network can be generated	**High**	**High**
04	Get keys	Verify keys are getting or not	Without allowing sensors to obtain keys	Nodes are not getting keys	Each node is getting key from Gateway	**High**	**High**
05	Generate transaction	Verify the transactions are generating or not	Without selecting random nodes	Random transaction data cannot send to gateway	Random transaction data can send to gateway successfully	**High**	**High**
06	Node behavior Chart	Verify the node behavior chart is displayed or not	Without saving the abnormal weight of the sensors	The Node behavior Chart is not displayed	The Node behavior Chart is displayed successfully	**High**	**High**
07	View Data	Verify data is displays or not	Without entering any sensor name	The data cannot be displayed	The data is displayed	**High**	**High**

7. OUTPUT DISPLAY SCREENS

To begin with double-click on ‘run.bat’ file starting with ‘IndustrialManager’ to develop the following display and authorize it to process.

In the screen of Fig 10, each transaction details can be seen from each node and then monitor node to detect its ‘normal’ or ‘abnormal behaviour’. At present double-click on ‘run.bat’ file as of ‘Wireless_Sensors’ folder to acquire the display revealed below in the Fig 11 and in its screen enter number of sensors and then click on ‘Show Network’ screen to get the Fig 12 screen. In the screen of Fig 12. click on ‘Get Keys’ button to allow all sensors to obtain keys from gateways.

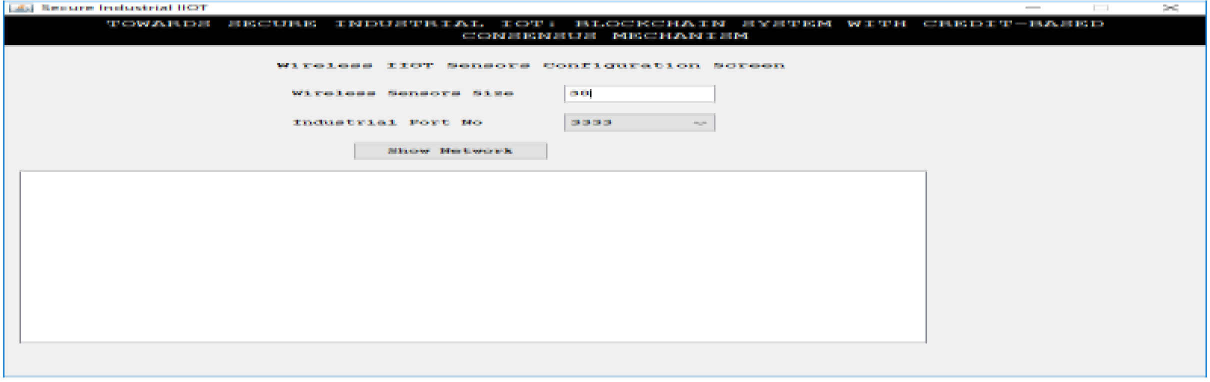
In the screen of Fig 13. each node getting keys from gateway can be seen and these key details can be seen at ‘manager screen’ as well.



INDUSTRIAL MANAGER SERVER & KEY DISTRIBUTION CENTER

Node ID	Total Transactions	Double Spending	Node Behaviour Weight	PoW Hash Value	Symmetric Encrypte...

Fig 10. Screenshot of Transaction Details



TOWARDS SECURE INDUSTRIAL IOT: BLOCKCHAIN SYSTEM WITH CREDIT-BASED CONSENSUS MECHANISM

Wireless IIOT Sensors Configuration Screen

Wireless Sensors Size: 30

Industrial Port No: 3333

Fig 11. Wireless IIOT Sensors Configuration Screen

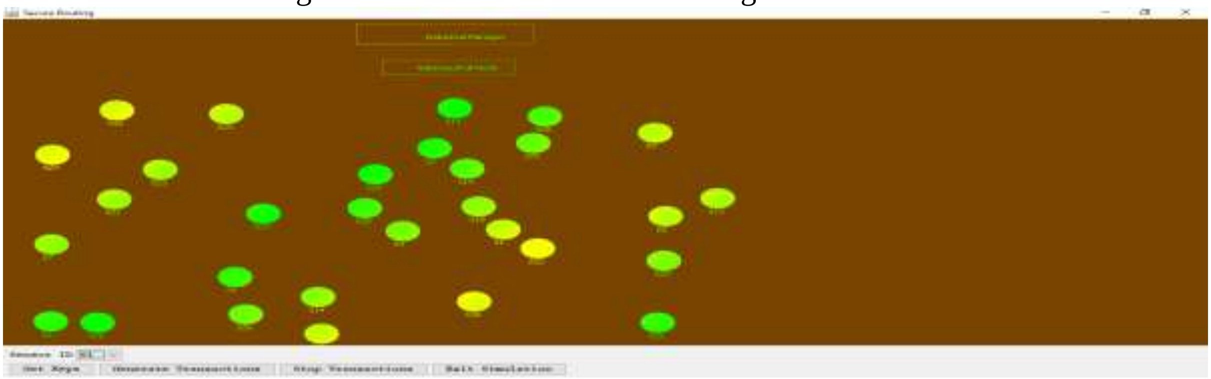


Fig 12. Secure Routing Screen One

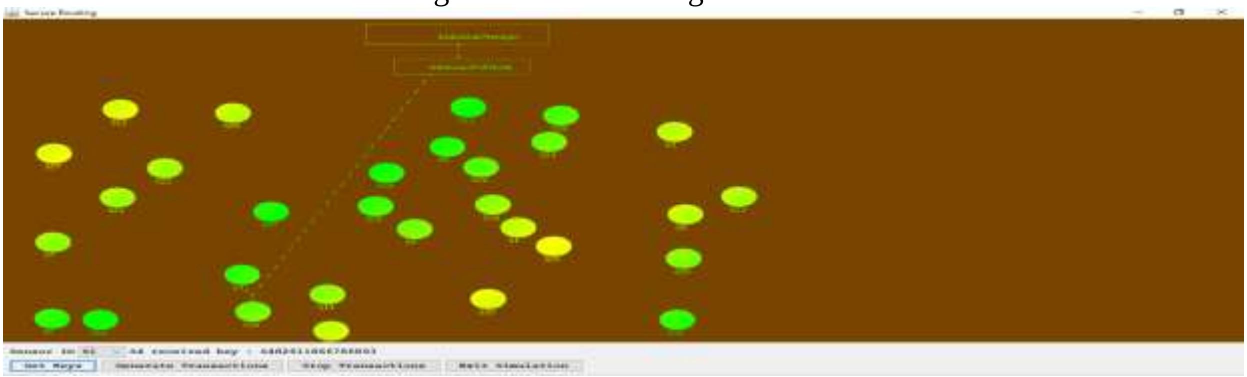
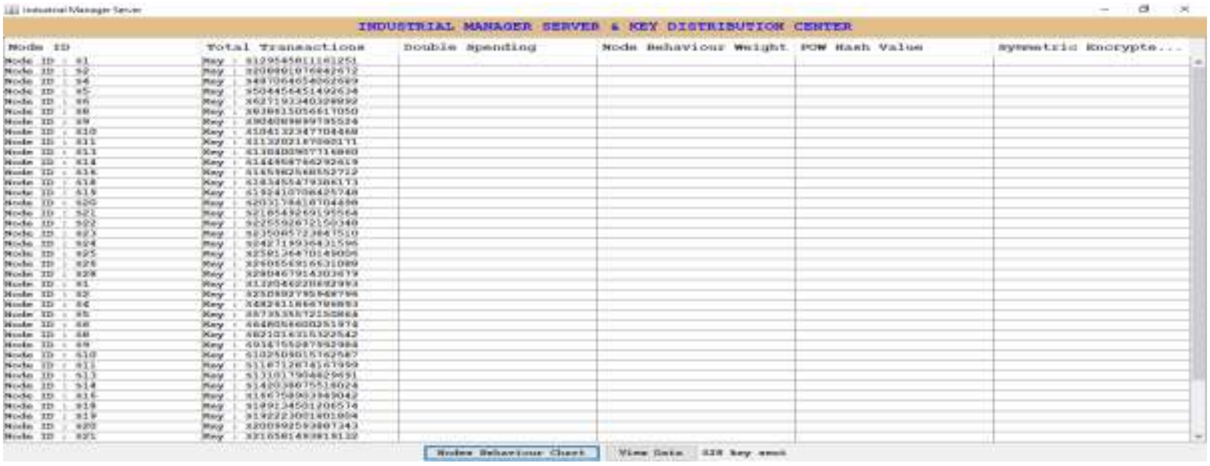


Fig 13. Secure Routing Detailed Screen Two

Now in the Fig 13. go to simulation screens and click on 'Generate Transactions' button to select random nodes and to send random transaction data to gateway. Due to random data sometime nodes will report same transaction then PoW detects it as abnormal transaction. This random data and continuous data sending concept just using to make some node to report same data and PoW can record it and after sometime click on ‘Stop Transaction’ to stop it.


Industrial Manager Server

INDUSTRIAL MANAGER SERVER & KEY DISTRIBUTION CENTER

Node ID	Total Transactions	Double Spending	Node Behaviour Weight	POW Hash Value	Symmetric Encrypte...
Node ID : S1	Key : [illegible]				
Node ID : S2	Key : [illegible]				
Node ID : S4	Key : [illegible]				
Node ID : S5	Key : [illegible]				
Node ID : S6	Key : [illegible]				
Node ID : S8	Key : [illegible]				
Node ID : S9	Key : [illegible]				
Node ID : S10	Key : [illegible]				
Node ID : S11	Key : [illegible]				
Node ID : S13	Key : [illegible]				
Node ID : S14	Key : [illegible]				
Node ID : S16	Key : [illegible]				
Node ID : S18	Key : [illegible]				
Node ID : S19	Key : [illegible]				
Node ID : S20	Key : [illegible]				
Node ID : S21	Key : [illegible]				
Node ID : S22	Key : [illegible]				
Node ID : S23	Key : [illegible]				
Node ID : S24	Key : [illegible]				
Node ID : S25	Key : [illegible]				
Node ID : S26	Key : [illegible]				
Node ID : S28	Key : [illegible]				
Node ID : S1	Key : [illegible]				
Node ID : S2	Key : [illegible]				
Node ID : S4	Key : [illegible]				
Node ID : S5	Key : [illegible]				
Node ID : S6	Key : [illegible]				
Node ID : S8	Key : [illegible]				
Node ID : S9	Key : [illegible]				
Node ID : S10	Key : [illegible]				
Node ID : S11	Key : [illegible]				
Node ID : S13	Key : [illegible]				
Node ID : S14	Key : [illegible]				
Node ID : S16	Key : [illegible]				
Node ID : S18	Key : [illegible]				
Node ID : S19	Key : [illegible]				
Node ID : S20	Key : [illegible]				
Node ID : S21	Key : [illegible]				

Figure 14. Industrial Manager Server Screen

In the screen of Fig 15. transaction sending to gateway for processing can be seen. Now each transaction processes status can be seen below manager screen.

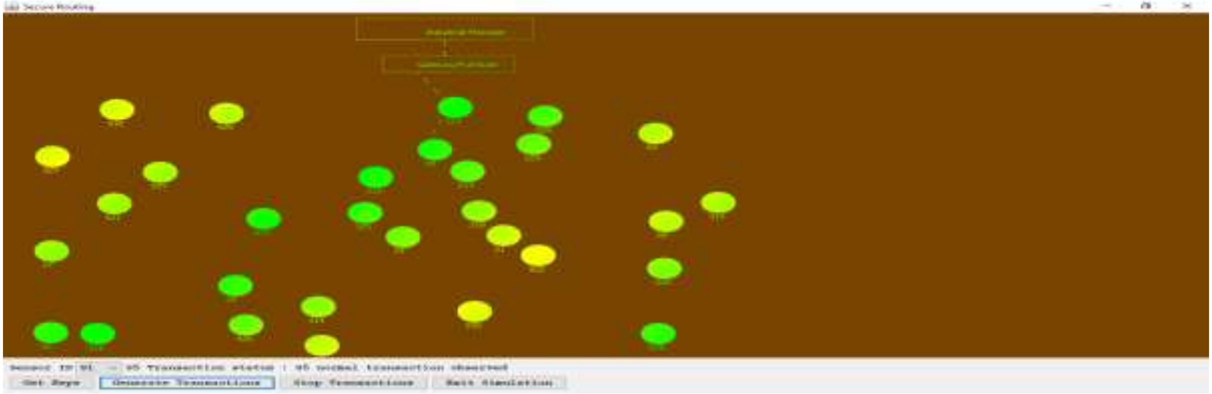
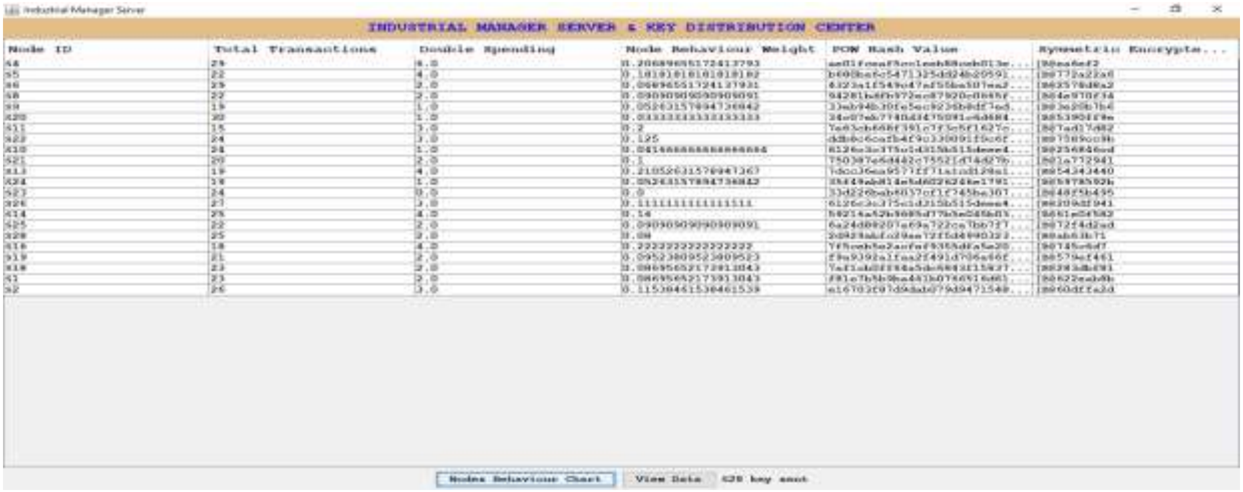

Sensor ID S1 -- S5 Transaction status : S5 normal transaction observed

Figure 15. Transaction Process Status Screen

In the screen of Fig 16. each node data report is recording and their hash values checking to collect their behavior, if they send old transaction data hash value then it will be considered as ‘abnormal behavior’. In above screen it is showing all nodes sending abnormal attack data and in real time this will not happen. Just to show the concept of old hash values random continuous request are sent and all nodes send repeated data and becomes in abnormal behavior.

From the screen of Fig 16. first nodes can be seen that sent total 29 transaction and out of that 6 transaction report old hash values then it will detect as abnormal behavior. If it reports 1 or 2 times then it can be managed and considered to be normal behavior. Now in the above screen click on ‘Node Behavior Chart’ button to see which nodes report same old hash value more no. of times.

In the screen of Fig 17. only 2 nodes report old hash values more number of times and be consider as abnormal nodes. S4 and S23 are the two nodes whose Double Spending Weight is 17 and other are not up to that. In above graph x-axis represents node id and y-axis represent Double Spending Weight. In screen of Fig 18. also normal or abnormal behavior can be observed.



Industrial Manager Server
INDUSTRIAL MANAGER SERVER & KEY DISTRIBUTION CENTER
Nodes Behaviour Chart
View Data
S28 key sent

Node ID	Total Transactions	Double Spending	Node Behaviour Weight	POW Hash Value	Symmetric Encrypte...
S4	29	6.0	0.20689655172413793	ae01feaaf5ec1eeb88ceb013e...	[B@ea6ef2
S5	22	4.0	0.18181818181818182	b6f0bafc5471325dd24b20591...	[B@772a22a6
S6	29	2.0	0.06896551724137931	4323a1f549c47af55ba501ea2...	[B@3578d8a2
S8	22	2.0	0.09090909090909091	94281b6f0972ec87920c0845f...	[B@4e970f34
S9	19	1.0	0.05263157894736842	33eb94b30fe5ec9236b8df7ed...	[B@3e20b7b4
S20	30	1.0	0.03333333333333333	34e07eb7740d475091c4d484...	[B@5390ff9e
S11	15	3.0	0.2	7a63cb66bf391c7f3c5f1627c...	[B@7ad17d82
S22	24	3.0	0.125	ddbdc6cafb4f9c330091f5c6f...	[B@7589cc9b
S10	24	1.0	0.041666666666666664	6126c3c375c1d315b515deee4...	[B@2568f46ed
S21	20	2.0	0.1	750387e6d442c75521d14d27b...	[B@1a772941
S13	19	4.0	0.21052631578947367	1dcc36ea9577ff71atcd129e1...	[B@54343440
S24	19	1.0	0.05263157894736842	3f449ab814e5d6026246e1791...	[B@5978592b
S23	24	0.0	0.0	33d226bab6037cf1f745ba307...	[B@48f5b495
S26	27	3.0	0.1111111111111111	6126c3c375c1d215b515deee4...	[B@209df941
S14	25	4.0	0.16	58214a52b9685d77b3e0458d5...	[B@61e04582
S25	22	2.0	0.09090909090909091	6a24d00207a69a722ca7bb727...	[B@72f4d2ad
S28	25	2.0	0.08	2d928abfc29ee72f5d490322...	[B@ab63b71
S16	18	4.0	0.2222222222222222	7f5ceb5e2acfef9355dfa5e20...	[B@745c6d7
S19	21	2.0	0.09523809523809523	f9a9392a1faa2f491d706a66f...	[B@579ef461
S18	23	2.0	0.08695652173913043	7af1ab0ff84a5de8483f15827...	[B@283db891
S1	23	2.0	0.08695652173913043	f81a7b5b9ba4431b076651666...	[B@622eab8b
S2	26	3.0	0.11538461538461539	e16703f07d9dab079d9471540...	[B@60dffa2d

Fig 16. Node Behavior Status Screen

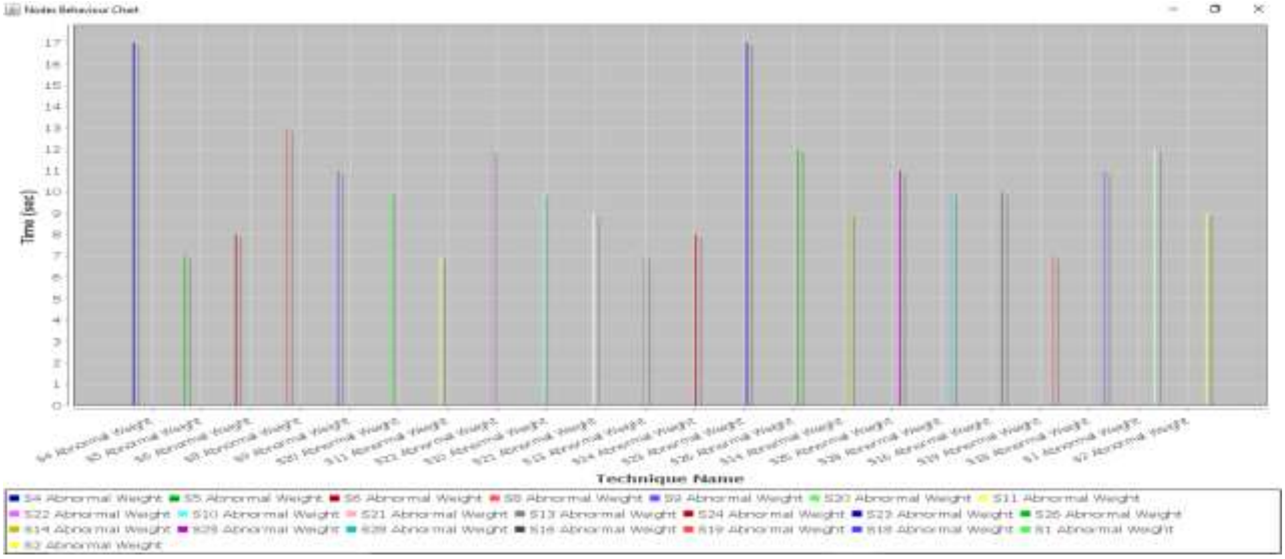
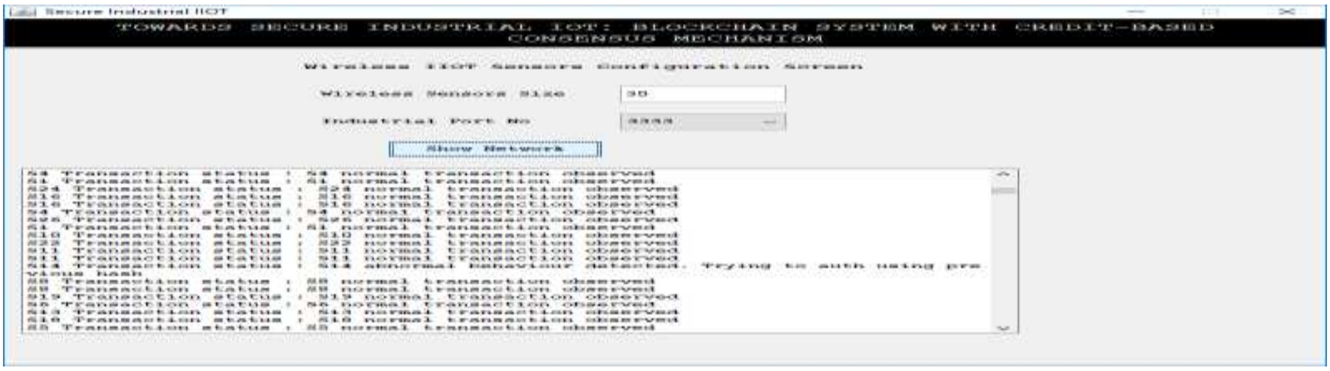


Fig 17. Node Behavior Chart Screen



Secure Industrial IIOT
TOWARDS SECURE INDUSTRIAL IOT: BLOCKCHAIN SYSTEM WITH CREDIT-BASED CONSENSUS MECHANISM
Wireless IIOT Sensors Configuration Screen
Show Network

Wireless Sensors Size: 30

Industrial Port No: 8888

```
S4 Transaction status : S4 normal transaction observed
S1 Transaction status : S1 normal transaction observed
S24 Transaction status : S24 normal transaction observed
S16 Transaction status : S16 normal transaction observed
S16 Transaction status : S16 normal transaction observed
S4 Transaction status : S4 normal transaction observed
S26 Transaction status : S26 normal transaction observed
S1 Transaction status : S1 normal transaction observed
S10 Transaction status : S10 normal transaction observed
S22 Transaction status : S22 normal transaction observed
S11 Transaction status : S11 normal transaction observed
S11 Transaction status : S11 normal transaction observed
S14 Transaction status : S14 abnormal behaviour detected. Trying to auth using pre
vious hash
S8 Transaction status : S8 normal transaction observed
S9 Transaction status : S9 normal transaction observed
S19 Transaction status : S19 normal transaction observed
S6 Transaction status : S6 normal transaction observed
S13 Transaction status : S13 normal transaction observed
S18 Transaction status : S18 normal transaction observed
S5 Transaction status : S5 normal transaction observed
```

Fig 18. Wireless IIOT Sensors Configuration Result Screen

8. CONCLUSION AND FUTURE WORK

In this research, a BC-centered IIoT process within the realistic states of smart industrial unit was set up toward attending the aforesaid disputes for IIoT. This beset credit-based PoW process cuts power intake aimed at honest nodules while escalating work out intricacies for vindictive nodes, facilitates in causing the DAG shaped BC further fit representing IIoT processes. Furthermore, the facts expert directing routine looks after the data privacy except for influence on the process performance that is similarly factual in IIoT process. The effects of broad investigations and assessments confirmed that this process has an effective execution in IIoT. This function will be of high significance in research and promoted stretched out as future prospects within disseminated IIoT processes with endowing an applied DAG shaped BC centered resolution that is not only apt for smart factory besides manipulating numerous IIoT scenarios. Yet, in imminent ends hardly any further inadequacies of this process, for instance sensor data quality control, storing constrictions must to be studied in detector gage facts attribute direction edifices contained by BC-centered processes then specific ways towards saving massive quantities of data requests are to be attained.

9. REFERENCES

[1] Y. Lu and L. D. Xu, “Internet of things (iot) cybersecurity research: A review of current research topics,” IEEE Internet of Things Journal, pp. 1–1, 2018.

[2] H. Yu, P. B. Gibbons, M. Kaminsky, and F. Xiao, “Sybillimit: A near-optimal social network defense against sybil attacks,” in IEEE Symposium on Security and Privacy (S&P), May 2008, pp. 3–17.

[3] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, “Blockchain for iot security and privacy: The case study of a smart home,” in IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), March 2017, pp. 618–623.

[4] O. Novo, “Blockchain meets iot: An architecture for scalable access management in iot,” IEEE Internet of Things Journal, vol. 5, no. 2, pp. 1184–1195, April 2018.

[5] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. M. Leung, “Blockchain based decentralized trust management in vehicular networks,” IEEE Internet of Things Journal, pp. 1–1, 2018.

[6] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang, “Consortium blockchain for secure energy trading in industrial internet of things,” IEEE Transactions on Industrial Informatics, vol. 14, no. 8, pp. 3690– 3700, Aug 2018.

[7] Z. Xiong, Y. Zhang, D. Niyato, P. Wang, and Z. Han, “When mobile blockchain meets edge computing,” IEEE Communications Magazine, vol. 56, no. 8, pp. 33–39, August 2018.

[8] M. Swan, Blockchain: Blueprint for a new economy. ” O’Reilly Media, Inc.”, 2015.

[9] K. Karlsson, W. Jiang, S. Wicker, D. Adams, E. Ma, R. van Renesse, and H. Weatherspoon, “Vegvisir: A partition-tolerant blockchain for the internet-of-things,” in IEEE 38th International Conference on Distribut- ed Computing Systems (ICDCS), July 2018, pp. 1150–1158.

[10] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, “An overview of blockchain technology: Architecture, consensus, and future trends,” in Big Data (BigData Congress), 2017 IEEE International Congress on. IEEE, 2017, pp. 557–564.

[11] S. Popov, “The tangle,” cit. on, p. 131, 2016.

[12] R. Bohme, N. Christin, B. Edelman, and T. Moore, “Bitcoin: Economics, technology, and governance,” Journal of Economic Perspectives, vol. 29, no. 2, pp. 213–38, May 2015.

[13] A. Churyumov, “Byteball: A decentralized system for storage and transfer of value,” URL https://byteball. org/Byteball. pdf, 2016.

[14] X. Wang, X. Zha, W. Ni, R. P. Liu, Y. J. Guo, X. Niu, and K. Zheng, “Survey on blockchain for internet of things,” Computer Communicatios, 2019.

[15] Sujatha krishnamoorthy Automatic epilepsy detection using hybrid decomposition with multi class support vector method,Multimedia Tools and Applications An International Journal.

[16] Ponmagal, R.S., Karthick, S., Dhiyanesh, B. et al. Optimized virtual network function provisioning technique for mobile edge cloud computing. J Ambient Intell Human Comput (2020).

Eknath Buriki is pursuing MTech Computer Networks and Information Security, Department of CSE, Nalla Malla Reddy Engineering College, Hyderabad. His areas of interests are IoT, Block Chain Technology, Computer Networks, Information Security and Cloud Computing.

D.Sasikala is presently working as Professor, Department of CSE, Nalla Malla Reddy Engineering College, Hyderabad. She received B.E.(CSE) from Coimbatore Institute of Technology, Coimbatore, M.E. (CSE) from Manonmaniam Sundaranar University, Tirunelveli. Phd (CSE) from Anna University, Chennai. This teaching faculty is with 20 years of experience and supervised numerous UG and PG projects. Being a life member of ISTE, her interest is on Data Science and Data Analytics, Deep Learning and Artificial Intelligence, DBMS, System Software, Software Engineering, Operating Systems and Digital Image Processing.