IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Improve the performance by a derived criteria using credit-based Proof of Work mechanism

[1]Taruvu Sree Sai Pooja, [2]G. Praveen Babu

[1]Students, [2]Associate Professor
[1]Software Engineering,
[1]School of Information Technology-JNTUH, Hyderabad, India

Abstract: In the Internet of Things (IoT) perspective, conventional machines perform self determined and smart. Its solutions hold an improving demand for its devices that are connected and offered services. However, inherent features raise many challenges like poor interoperability,decentralization and challenges to address in the security domain . Now blockchain is given a attention that it is capable of providing solutions to IoT problems. Its use can be suitable in any financial situations also, blockchain gives guarantee for its work to be secured and resistant from privacy issues.Nonetheless, blockchains are power intensive and they provide low throughput, these are not suitable for power constrained IoT devices. To overcome these difficulties, blockchain is integrated with Industrial IoT, IoT 4.0 version, with credit based Proof of work mechanism. Repeated examination and results show that this system can provide data access control and proved to provide secure and effective IIoT services.To ensure confidentiality , data authority the board technique is intended to manage the accessibility to sensor information. Trust incorporation in distributed environments without the requirement for authorities is a major advancement that can technically develop change in numerous enterprises, IoT within them. The Objective here is to give a complete idea about the structure and activity of block chain and to examine how this innovation provides security and protection in IoT. This project work centers around this relationship, researches difficulties in blockchain IoT applications, and studies the most significant works to examine how blockchain might improve the IoT. In the early stages the result obtained is record processing, where the data is processed from resources together with its statistics and then the data is reported in the records with their hash values and their behavior is checked by checking their hash values. Hash value gets updated after the record gets updated, if old transactions hash value is displayed in the output then it is considered as “Abnormal behavior”, if the new hash value is displayed then it is considered as normal behavior. Symmetric exception values are recorded that are used for the security feature.

***Index Terms* - Industrial IoT, blockchain, credit-based, proof-of-work,security, efficiency, privacy**

I.INTRODUCTION

The incorporation of IoT with industry provides great advancement in automation and robotisation of the industry. Industrial Internet of Things(IIoT) assists to remove errors, move high costs, make the process more efficient and upgrade security in manufacturing and other industrial procedures, that have an good opportunity to make the industry oriented field with significant level of integrity, range of availability and scalability. Attacks over security and failures arising because of it are the major problem in IoT network all over the world.[1] this may not let the real benefits exceed.If we consider the data central data center to not be available to single point of failure and malicious attacks, in the same way, DDoS, Sybil attack [2], this can not guarantee the access to authorised administrators.This may lead to danger of data security. In the same way the attempt of data interpretation may happen while communicating among IoT devices, which can't guarantee the credibilities of gathered information.At some situations the incorporation of blockchain with IoT has gained much interest [3]-[5]. as it can provide features such as decentralized consensus mechanism and tamper-proof blockchain,it chas great chance to ensure the security in IIoT systems. it has high chances of determining security related to blockchain issues in IIoT systems. There are some evaluated points which justify this point,O. Novo [4] controls the access framework based on the management of the devices concept in IoT.At some points management hub faces situation cursing failure Z. Li et al. [6] explained the measures blockchain can provide.However, they don't ponder protection issues, for example, the delicate information exposure, and so it can't guarantee information confidentiality.Furthermore, there are few unique difficulties that are likewise provided now during the dispatch of new plan of blockchain into Industrial IoT frameworks. The three fold fundamental difficulties are summarized as below:1.) The trade-off amongst the process of being efficient and secure: It is noticed that consensus algorithms in blockchain can help to protect from malicious attacks, and PoW is the majorly used consensus algorithm, this provokes the nodes to work with high complexity while transactions are verified. But it affects the power consumed by IoT devices. If PoW mechanism is removed then efficiency of transactions can be improved yet causes security issues. this is noted as the major challenge.2.) The transparency and privacy coexistence : Transparency feature is the main field that affects this financially . For some Industrial IoT devices this may be a drawback as it may lose confidentiality of sensitive data. 3) The high concurrency comparison with low through-put: Providing high concurrency results in data availability continuously. And complex cryptographic based security mechanisms results in low throughput of blockchain. So the question arises to elevate the throughput of blockchain to satisfy the need of very frequent transactions to settle down the third challenge. Major things provided by this project are explained as following:

• Three major challenges caused because of integrating blockchain with IIoT are provided with three solutions.

• Industrial IoT designed such that its cost effective and access controlled system that are power compelled and where the blockchain is provided with a security, scalability and generalisation to IIoT. Also this is different from all the previous works where in here by using DAG structured blockchain higher throughput is achieved.

• The proposed systems are smart factory systems design and implementation.Experiments gives results which prove good performance of IoT devices are assured with credit based PoW mechanism and management method of data authority.

Objective of the Project: Industrial IoT plays a crucial role that could make IIot systems secured, generalised and scalable. In the existing system, the neat explanation of blockchain the process of combining both iot and blockchain gained huge enthusiasm . Access control system allows blockchain to integrate with IIoT devices. Because of usage of the central management hub the system is not fully made on distributed architecture. The coupling gets inappropriate when the management hub fails or gets attacked. To protect all the confidential sensitive data, a data authority management is created to protect the data and avail the data to authorised user. Experiments ensure that the PoW mechanism which is credit-based provides great performance by using data authority management.

1.1. Existing System

Industrial IoT devices are generally accessible to single point of failure and malicious attacks that could not provide constant services. Because of the security constraints of block chain and resilience, the plan of collaboration of block chain with IOT improves much interest. Anyhow, block chains are power-intensive and low-throughput, that are not good for IoT machines that are power-constrained. To handle these challenges, propose a block chain system for Industrial IoT with consensus mechanism that are credit-based.

Disadvantages of Existing System:

1. Stable services are not available.

1.2. Proposed System

This Project is a credit-based system that is built dependent on Directed Acyclic Graph (DAG) structured block chains, that is advantageous more than the satoshi-style block chain in performance. Raspberry Pi is implemented on a system , and a project for a smart factory conducted. Immense validation including analysing the outcomes exhibit that credit-based Proof of Work mechanism and data access control are secured and efficient in Industrial IoT.

Advantages of Proposed System:

1. This protects the sensitive data confidentiality.
2. It provides system security and transaction efficiency.

II. System Requirements

2.1 Hardware Requirements

- Processor : Core – i4
- RAM : 4GB
- Hard Disk :1TB

2.2 Software Requirements

- Coding Language : Java
- IDE : Eclipse
- Operating System : Windows 10

III. RELATED WORK

Internet of things cyber security research: A review of current research topics [1]

As a newest technology, the IoT transform the worldwide network including the smart devices, data, people, intelligent objects and data. IoT blooming is yet in its infant stage and plenty of affairs has to be decoded. IoT may be a united details of embedding all things. IoT incorporates good opportunity in making the planet a better standard of confidentiality, integrity, accessibility, scalability,interoperability and availability. Yet, challenging task is protecting IoT. Base for the development of IoT is System security. that text detailedly overviews IoT cybersecurity. The main regards are information communication technologies (ICT) and incorporation of heterogeneous smart machines and also the protection. This review gives very useful data and insights to practitioners and researchers curious about cybersecurity of IoT, which include this module of IoT cybersecurity, IoT its taxonomy and architecture, key process enabling strategies and counter measures, key applications in finding latest trends, industries and challenges.

Blockchain meets iot: An architecture for scalable access management in iot [2]

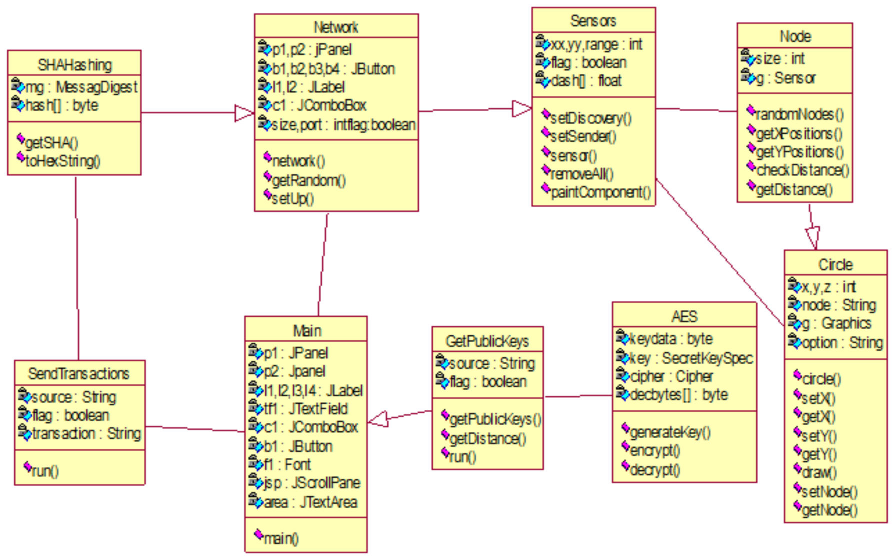
The IoT has getting off of infancy to show itself as a portion of coming future network with full maturity. The capability that could manage having many numbers of its devices installed all over he world in them is one of many technical challenges. In spite the fact that technologies the access of the management coexist in IoT, they came with a new variation of technical limitations to move them globally which are based on centralized models. In this, the process suggest a novel planning for negotiating kind of roles and its tolerance in IoT. The nowel architecture is a full-fledged that contains distributed access that could control structure for IoT that rely on technology of blockchain. The backed framework is "a proof of work" employment and solved in realistical IoT scenario, and the solution shows that blockchain technologies could be utilised in specific scalable Internet of Things scenarios as technology of access management.

When mobile blockchain meets edge computing [3]

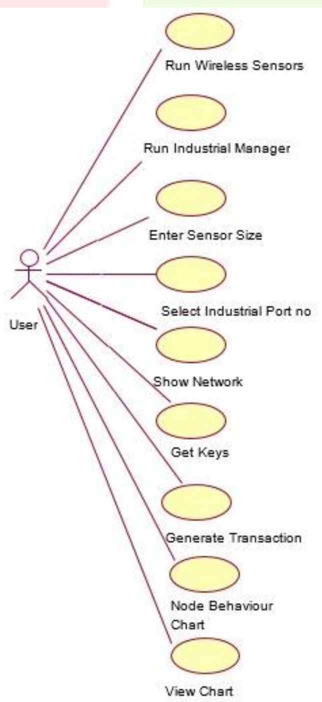
Blockchain, being the backbone of technologies of the ongoing famous digital currency called Bitcoin, it has been a trustable framework management that is data decentralized. In spite blockchain being implementable in various applications widely (like., logistics, finance and healthcare), its applications in portable service is yet limited. That could due to the existing fact that blockchains users needs to resolve the puzzles of the present proof-of-work which to add new data (i.e., block) within the blockchain. Proving the POW, anyhow, occupies substantial resources such as that of CPU's energy and time that couldn't be suited for resource-limited mobile mode devices.For Easing blockchain application in coming days mobile IoT system, access mobile edge computing viewed to be an output to resolve the proof-of-work gamblers for users who work under mobility. Firstly here new concept is introduced called edge computing for the mobile blockchain.

IV. PRODUCT DESIGN: UML DESIGN

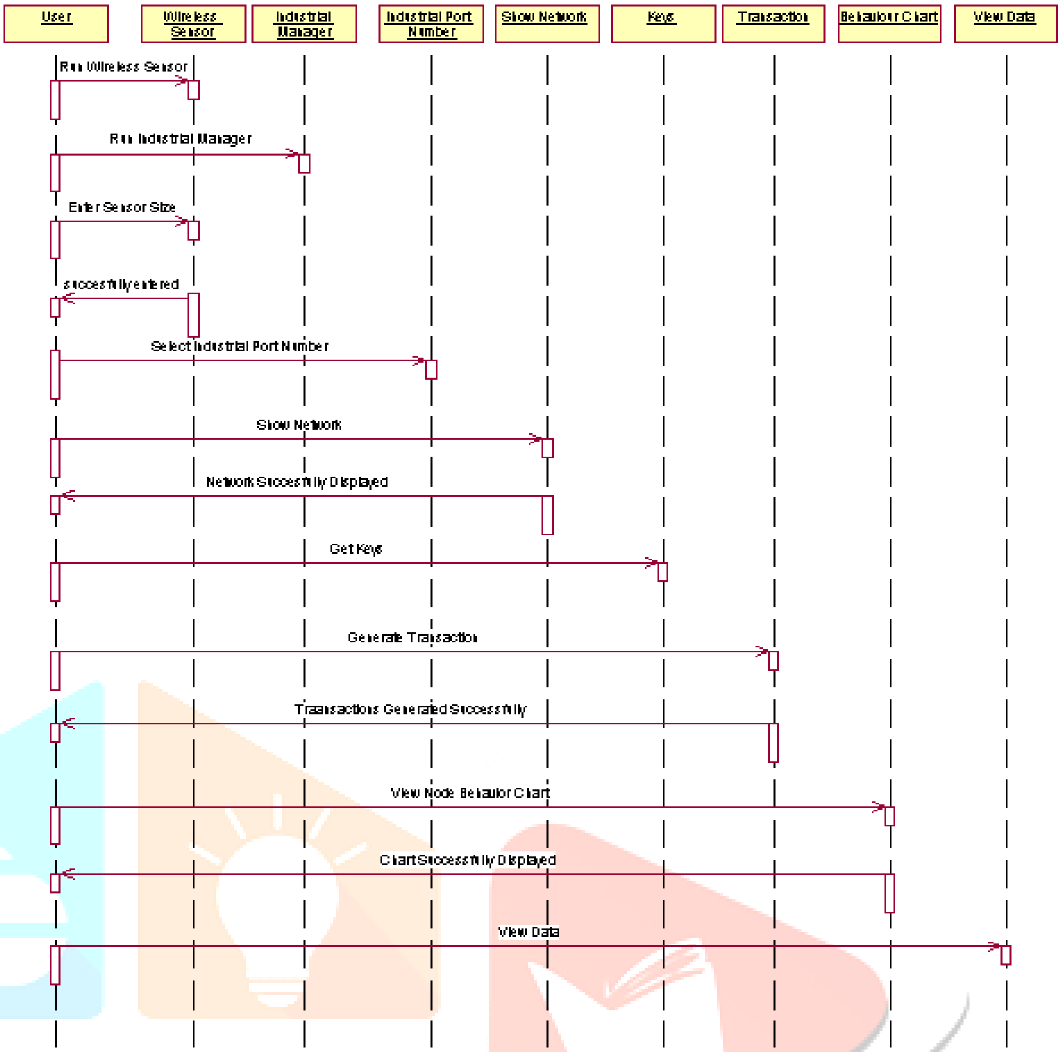
CLASS DIAGRAM FOR INDUSTRIAL MANAGER:



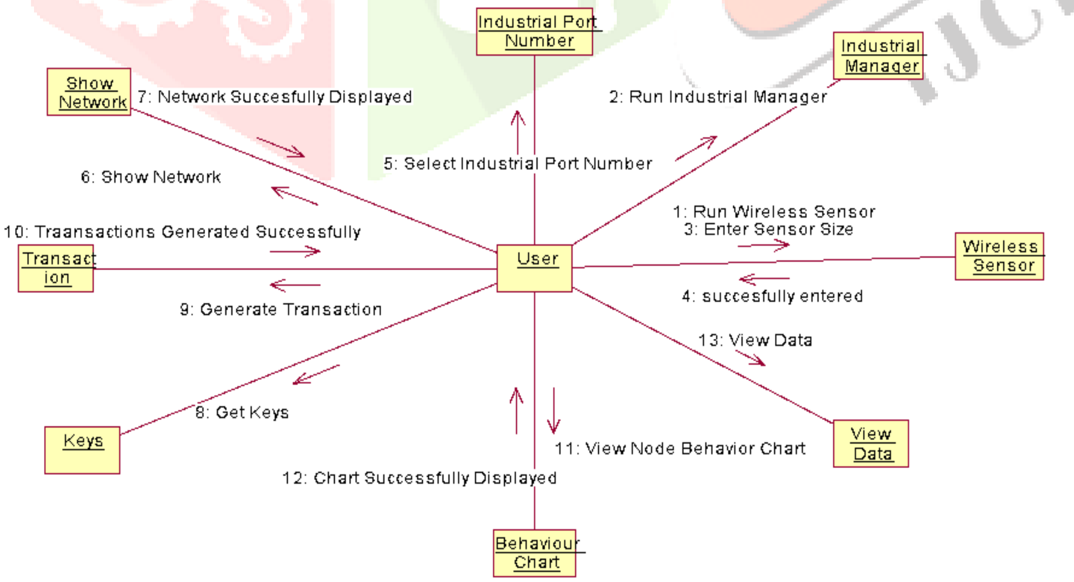
Use case diagram:



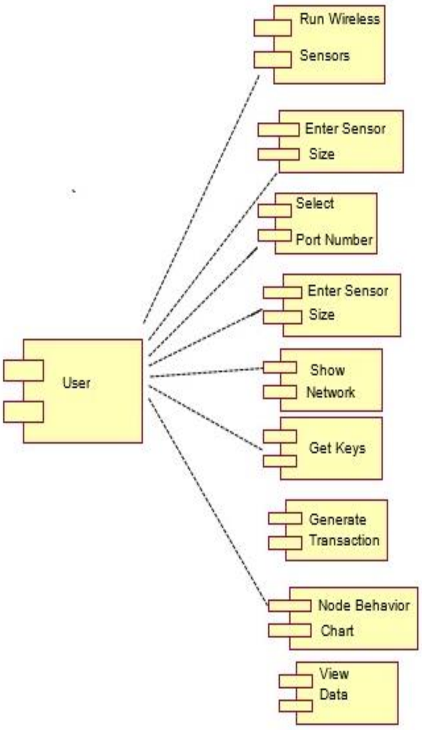
Sequence Diagram:



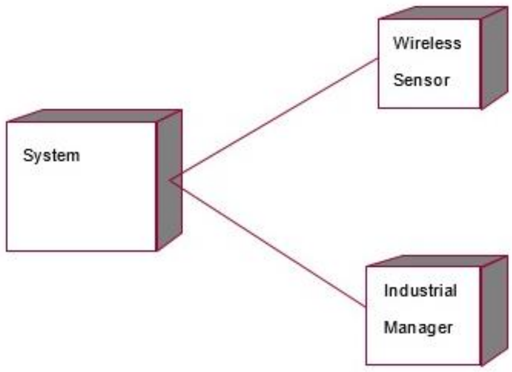
Collaboration diagram:



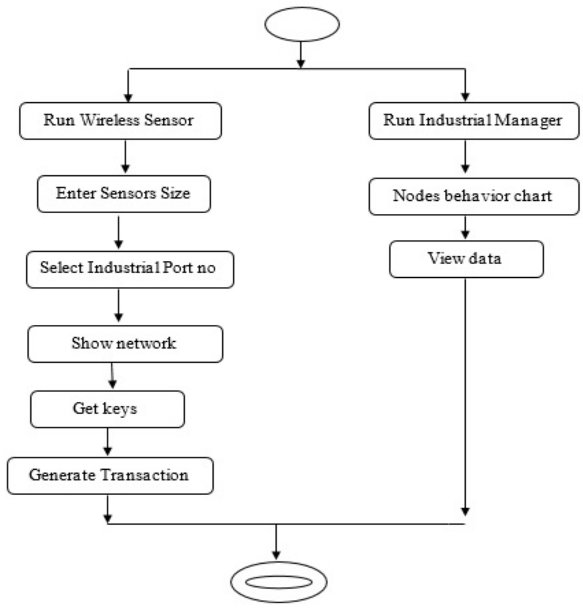
Component Diagram



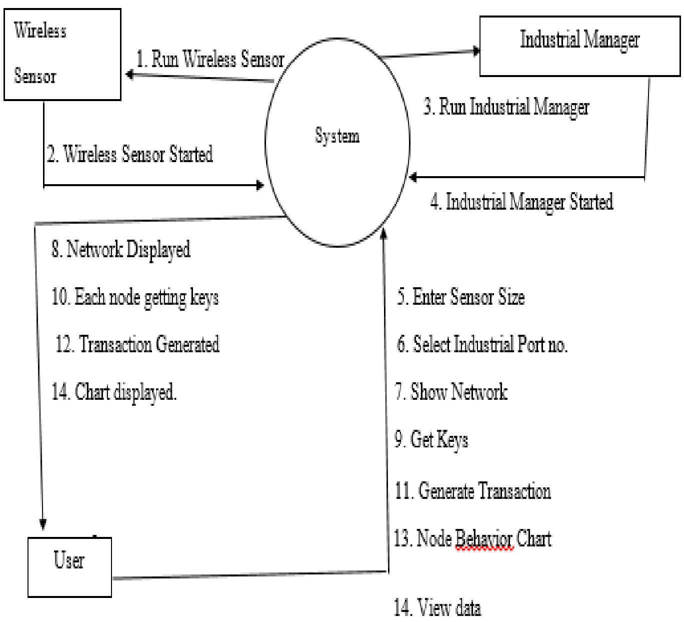
Deployment Diagram



Activity diagram:



Data Flow Diagram:



V. IMPLEMENTATION

Implementation is the most important process in the project, in this phase the proposed techniques and methods are implemented. All industries like banking, hospitals are using Industrial IoT devices based algorithms such as POW (proof of work) and credit consensus. Entire Blockchain technique cannot be implement as this devices are small and run on battery so POW and Credit Consensus concepts are used from Blockchain technique. The problems that are faced causing the utilization of POW and credit consensus concept from entire block chain technique are:

a) Efficiency and Security: All transactions are safe under blockchain Credit Consensus and if the entire Blockchain is used then efficiency problem will raise in devices (sensors) to run entire Blockchain technique. Hence Credit Consensus is used.

b)Transparency and Privacy: All transaction done in Credit Consensus are available publicly and there is no privacy for data. So to provide security to data author is using symmetric encryption technique to hide data from public and can only be decrypted by industrial manager. When sensors or devices setup then industrial manager share public keys with sensors via GATEWAYS. All

sensors encrypt data using public key and send to GATEWAY and GATEWAY will store at industrial server where manager can decrypt all data using keys.
c)High concurrency and low throughput: As sensors report huge data to servers so concurrent requests will arrive from all sensors and then server can produce low throughput or output. To increase throughput by using DAG (directed acyclic graph architecture) concept. In DAG each transaction referred as node instead of maintaining multiple blocks. Running transaction as nodes take less time compare to blocks generation.In this application the following three types of devices:
1. Sensors: This are small devices which interact with GATEWAYS to send/ receive data and KEYS also are collected from GATEWAYS. Sensor will encrypt data and then generate hash code on transaction and then send to gateway. Gateway/industrial server will authenticate hash and check all transactions contains unique hash value, if hash value unique then sensor credit will increase and this hash values will be used as Proof Of work for transactions. While sending transactions sensors can report two types of attacks called 'Lazy Tips and Double Spending' and this two attacks can be easily detected with Credit Consensus Algorithm.

A. Lazy Tips: In this malicious sensor report same hash values for all transactions and Credit Consensus POW look for new hash values. If same hash value detected for all transaction then Lazy Tips attack or abnormal behaviour detected.
B. Double Spending: In this technique sensors report success hash values of previous transactions and if POW Consensus detect old hash value then this abnormal behaviour will detected.

By using above two values credit positive and negative value will be calculated. Sensors also called as light node
2. Gateways: Also called as Full Node because it will have high energy compare to normal sensors. Gateways receive request from manager authorized sensors and then send to credit consensus POW algorithm to check sensor behaviour and then send response data to manager.
3. Manager: Manager will generate public and secret keys and store it in gateways to exchange public keys with sensors. All sensors data can be access by this manager by using secret keys. Sensors will send data to gateways and gateways store received/processed data at manager server.
To implement above concept SHA256 for hashing and AES for data encryption are used to provide privacy.
To implement this project work two applications are designed called 'IndustrialManager and Wireless_Sensors'.
IndustrialManager: This application responsible to generate keys for sensors and then run Credit Consensus POW algorithm to process/check each transaction send by sensors.
Wireless_Sensors: This is a simulation based application which request gateways to receive keys and then send encrypted transaction to gateways for processing.In the early stages the result obtained is record processing, where the data is processed from resources together with its statistics and then the data is reported in the records with their hash values and their behavior is checked by checking their hash values. Hash value gets updated after the record gets updated, if old transactions hash value is displayed in the output then it is considered as "Abnormal behavior", if the new hash value is displayed then it is considered as normal behavior. Symmetric exception values are recorded that are used for the security feature.

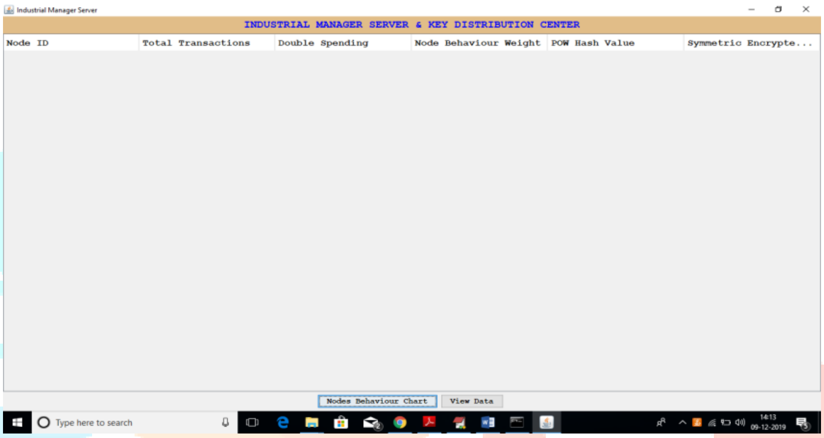
VI. Testing and Results

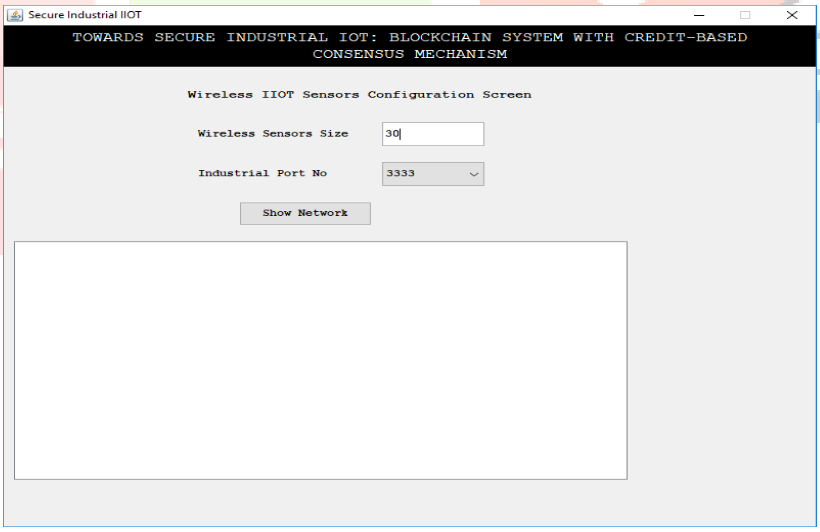
Testing is performed after the user finally satisfies with the accuracy of the solution to the problem. This confirms that the system can now be assigned to original goals and objectives without any waste of time, money. It is final step where the project is accepted and ready for the performance of its operation.

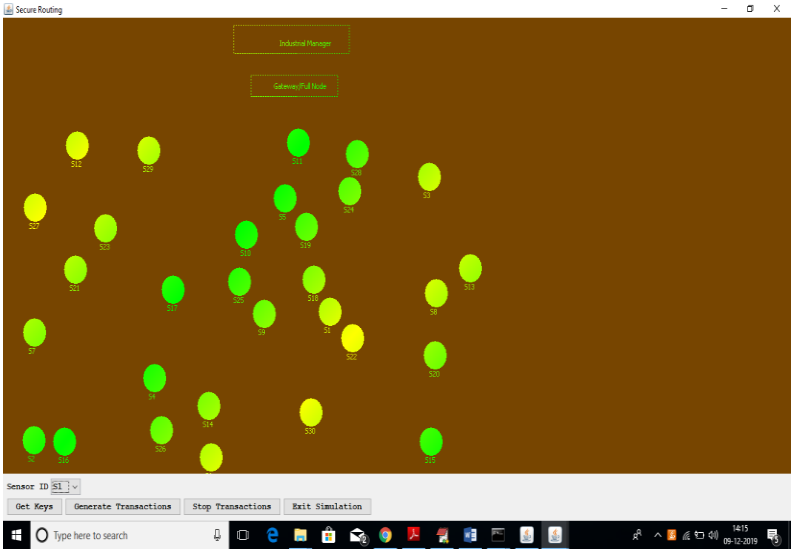
TEST CASE ID	NAME OF TEST CASE	TEST CASE DESC.	TEST STEPS			STATUS OF TEST CASES	Test Priority
			STEP	EXPECTED	Actual		
01	Run wireless sensor and industrial Manager	Verify the wireless sensor and industrial Manager started or not	Without wireless sensor and industrial Manager	Users cannot do further 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	cannot generate network	can generate network	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		

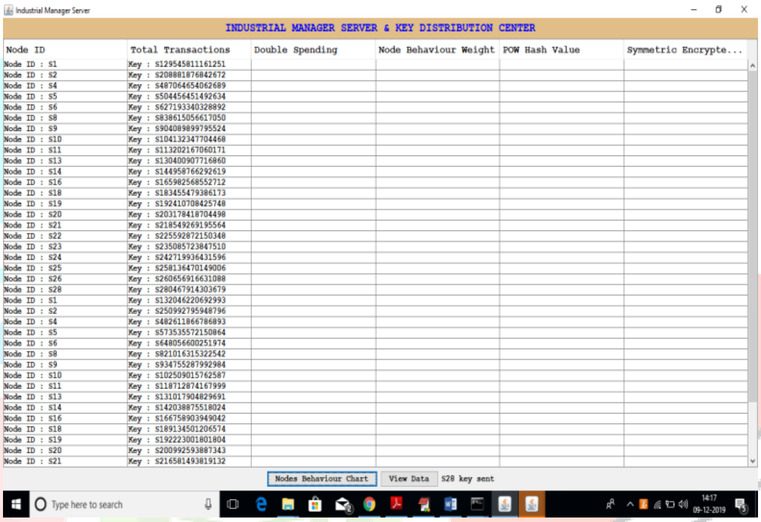
RESULT



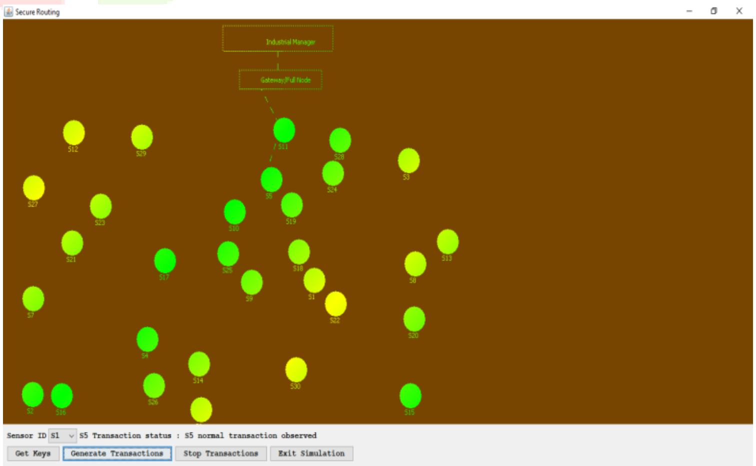




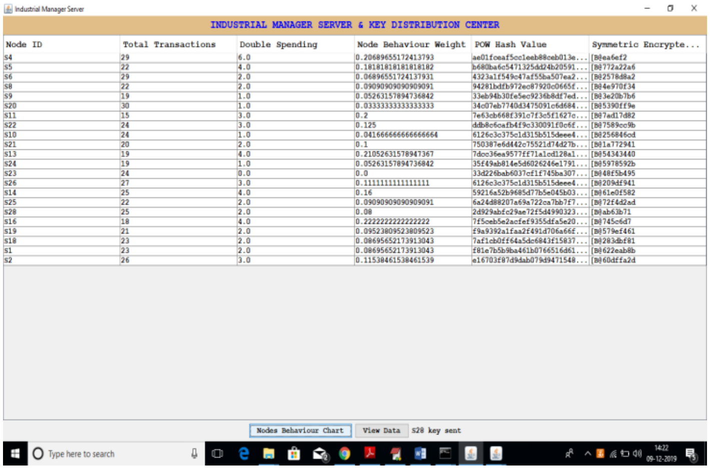
In above screen click on ‘Get Keys’ button to allow all sensors to obtain keys from gateways
In above screen can see each node is getting keys from gateway and this keys details can see at ‘manager screen’ also.



Now go to simulation screen 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 dissertation same transaction then POW detect it as abnormal transaction. This random data and continuous data sending concept just use to make some node to dissertation same data and POW can record it. After some time you can tap on ‘Stop Transaction’ to stop it.



In above screen can see transaction sending to gateway for processing. Now can see each transaction process status at below manager screen



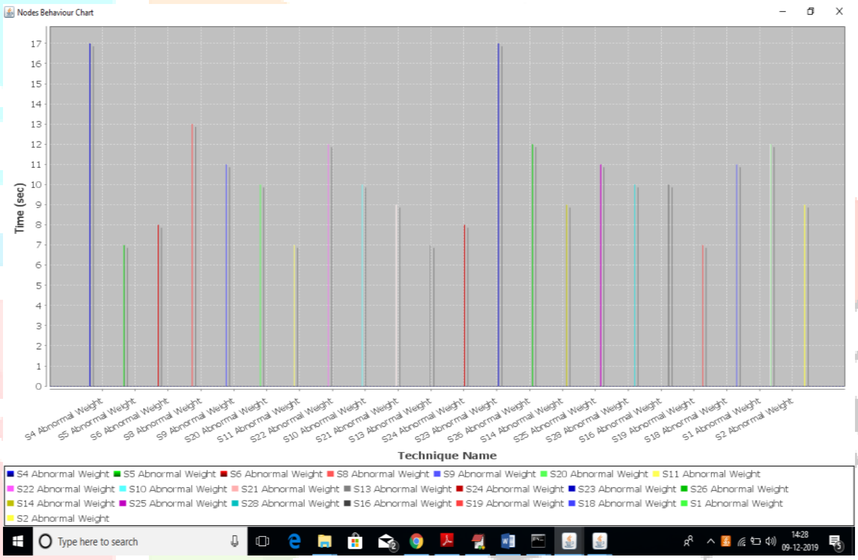
Industrial Manager Server

INDUSTRIAL MANAGER SERVER & KEY DISTRIBUTION CENTER

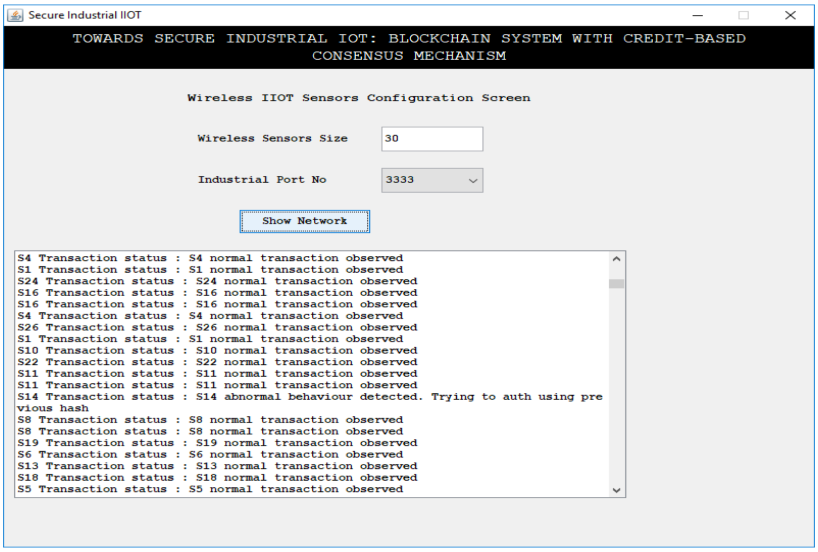
Node ID	Total Transactions	Double Spending	Node Behaviour Weight	POW Hash Value	Symmetric Encrypte...
S4	29	6.0	0.20689655172413793	ae01fceaf5cc1eeb88ceb013e...	[B@ea6ef2
S5	22	4.0	0.18181818181818182	b680ba6c5471325dd24b20591...	[B@772a22a6
S6	29	2.0	0.06896551724137931	4323a1f549c47af55ba507ea2...	[B@2578d8a2
S8	22	2.0	0.09090909090909091	94281bdfb972ec87920c0665f...	[B@4e970f34
S9	19	1.0	0.05263157894736842	33eb94b30fe5ec9236b8df7ed...	[B@3e20b7b6
S20	30	1.0	0.03333333333333333	34c07eb7740d3475091c6d684...	[B@5390ff9e
S11	15	3.0	0.2	7e63cb668f391c7f3c5f1627c...	[B@7ad17d82
S22	24	3.0	0.125	ddb8c6cafb4f9c330091f0c6f...	[B@7589cc9b
S10	24	1.0	0.041666666666666664	6126c3c375c1d315b515deee4...	[B@256846cd
S21	20	2.0	0.1	750387e6d442c75521d74d27b...	[B@1a772941
S13	19	4.0	0.21052631578947367	7dcc36ea9577ff71a1cd128a1...	[B@54343440
S24	19	1.0	0.05263157894736842	35f49ab814e5d6026246e1791...	[B@5978592b
S23	24	0.0	0.0	33d226bab6037cf1f745ba307...	[B@48f5b495
S26	27	3.0	0.1111111111111111	6126c3c375c1d315b515deee4...	[B@209df941
S14	25	4.0	0.16	59216a52b9685d77b5e045b03...	[B@61e0f582
S25	22	2.0	0.09090909090909091	6a24d88207a69a722ca7bb7f7...	[B@72f4d2ad
S28	25	2.0	0.08	2d929abfc29ae72f5d4990323...	[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	7af1cb0ff64a5dc6843f15837...	[B@283dbf81
S1	23	2.0	0.08695652173913043	f81e7b5b9ba461b0766516d61...	[B@622eab8b
S2	26	3.0	0.11538461538461539	e16703f87d9dab079d9471548...	[B@60dffa2d

Nodes Behaviour Chart View Data S28 key sent

In above screen each node data dissertation is recording and their hash values checking to collect their behaviour, if they send old transaction data hash value then it will be consider as 'abnormal behaviour'. In above screen are showing all nodes sending abnormal attack data and in real time this will not happen. Just to show the concept of old hash values sent random continuous request and all nodes send repeated data and becomes in abnormal behaviour. From above screen can see first nodes sent total 29 transaction and out of that 6 transaction dissertation old hash values then it will detect as abnormal behaviour. If it dissertations 1 or 2 times then it can be manage and consider as normal behaviour. Now in above screen click on 'Node Behaviour Chart' button to see which nodes dissertation same old hash value more no of times.



In above screen only 2 nodes dissertation old hash values more number of time and be considered 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 represents Double Spending Weight.



In above screen also can see normal or abnormal behavior.

VII. CONCLUSION

In this project work, the blockchain-based IIoT system implies impact of smarter factory to showcase previously mentioned challenges for Industrial IoT. By implementing the credit based PoW mechanism the power that is consumed for the real honest nodes is decreased where as its complexity keeps increasing in malicious nodes, this is the strategy that makes DAG structured blockchain look suitable for Industrial IoT systems. The data authority management helps in keeping the accessibility secured by attaining data privacy which helps protection of data from data piracy. By the results of extensive experiments it can be confirmed that this system has a good performance in Industrial IoT. Its major importance is attained in industrial IoT systems by offering a solution that is DAG structured blockchain oriented. The final solution is suitable not just for the smarter factories, but also able to accomodate to kinds of Industrial IoT scenarios.

VIII. FUTURE SCOPE

The present project is very major for the research in industrial IoT systems that are distributed by supplying actual results based on DAG structured blockchain. But, there exist some limits in the systems, as storage limitations, sensor data quality control. Further ways, in blockchain- based systems could search schemes of sensor data quality control and few methods that store data of large quantities. E.g, all the datas that are computed over the system could be stored for further computation.

BIBLIOGRAPHY

[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.