Smart Contract Based Industrial Data Preservation on Block Chain

Dr.D.Sivaganesan
Professor, Department of Computer Engineering
PSG Institute of Technology and Applied Research
Coimbatore, India
Email: sivaganesan@psgitech.ac.in

Abstract: The ground work for establishing the industrial 4.0 age involves the tiered architectures that are made up of multiple planes encompassed with the physical things that are embedded with internet capabilities. This infrastructure enables an incorporation of the various functions that are necessary in a manufacturing industry to enhance the efficiency of the industry, and contrivance a highly supple and a self-organizing industry that is smart. On the other hand it becomes essential to preserve the information's safely as many internet enabled devices are utilized and more networks are formed for the proper incorporation of the various activities taking place. Since the conventional methods are inadequate the block chain method was most preferred due to its transparency and highly reliable and expedient services. To further structure a tamper proof network the blockchain is built with the smart contract laid on the system providing the impermeable authenticity on the industrial data transferred by securing the information's against the authentication that is anonymous. The performance of the system is validated to on the basis of security provided on the transactions made, and the cost spent on the proposed design.

Keywords: Industry 4.0, Block Chain, Data Preservation, Smart Contract, Proof of Authenticity.

1. Introduction

The industries take a vital part in the economy as they produce more and more goods and material that are technologically advanced and automatized. "Continually from the time when the beginning of the industrialization, the technology progresses leading to paradigm shifts, that was named previously as the industrial revolution." The revolutions in the industry that started with the usage of more advanced technologies in its first phase followed by revolution against the severe utilization of the energy in the second phase and advancement towards the wide spread digitization in the third phase, still strives to improves itself with the employment of the highly innovative digitalization, and the integration of the technologies that are yet to come along with internet skills and the utilization of the smart objects to further cause a new level of basic up gradation in the industries.

The envisage to have a industry or factory facilitated with the flexible and competent system to manufacture with the capability of regulating its own production procedures necessitates the integration of the various

Ubiquitous Computing
Communication Technologies

components in the factory and making them to communicate without human intervention over the internet. "This is thought to comprehend the production of the single product, in a batch size of one while retaining the economic status of the mass production." Desirous about the anticipations over the development of the industry in the future, the term coined as the "Industry 4.0 that was a recollection of software versioning" was introduced as a fourth phase of revolution in the industry.

This offered enormous, chances for comprehending the sustainable procedures in manufacturing, in turn to elude the issues endured due to the globalization i.e. "the challenges to meet the constantly progressing worldwide demand for the capital and the consumer goods by simultaneously ensuring a bearable evolvement of human existence in its social environment and economic dimension."

The "industry 4.0" was initially started in the Germany as the fourth phase of revolution and was very prominent among the current researches as it was exactly associated with the "internet of things, enterprise architecture, information and communications technologies, and the enterprise integration". It includes the further developments in the industries to attain an manufacturing process that are very intelligent and reliable by following a vertical, horizontal and peer to peer integration and formulating systems with proper adjustment and the competent super vision.

The "industry 4.0" makes conceivable the collection and the examination of the data among the machineries, allowing the speedy, supple and proficient procedures to generate goods materials at lower cost and improved quality, thus increasing the production of the unit , improvising the organizations effectiveness.

Despites the competencies of the "industry 4.0" the security and the protection against the data emitted from the equipment and tools in the industrial operations are questionable. Since the conventional methods are incompatible with the peer to peer network (Block Chain) was preferred in protecting the data generated by the machineries as well as the confidential information's maintained.

The Block chain (Blk-Chn) is fundamentally a "distributed ledger", it is a "peer to peer connecting technology" working on the principle laid upon the consensus that is dispersed, retaining its secrecy. The block chain is the chain of blocks which is usually a ledgers digital page storing the information's visibly once the node has initiated its approval. It assures its clients with complete protection on the enormous of data produced with insights. It is inculcated with authority for distribution, regulating the heavy traffic flow, paving way for the value dispersion. It is capable of functioning offline delivering an immutability, notarization and the time stamp. The smart contracts are mechanisms that allow automatic movements of digital assets based on the rules that are pre-specified arbitrarily. This encodes the random state transactions

Ubiquitous Computing
Communication Technologies

and enables to develop mechanisms that are founded on laws that previously specified. So the smart contract remains as a security that stops the Blk-Chn holding the unfit blocks

So the paper structures a tamper proof network the blockchian is built with the smart contract laid on the system providing the impermeable authenticity on the industrial data transferred by securing the information's against the authentication that is anonymous. The performance of the system is validated to on the basis of security provided on the transactions made, and the cost spent on the proposed design.

The Blk-Chn designed incorporated with the smart contract is explained clearly with the 2 detailing the literature survey, the 3 explaining the mechanism developed, 4. Experimenting the security provisions of the system put forth and 5. Presenting the summary and the future scope.

2. Literature Survey

Jazdi, Nasser et al [1] introduces the "Cyber physical systems in the context of Industry 4.0." Lee et al [2] proffers the "Service innovation and smart analytics for industry 4.0 and big data environment." Lasi, et al [3] discusses the details on the "Industry 4.0." as the fourth revolution in the industry. Zhou et al [4], discusses the future aspects, issues and the benefits of utilizing the "industry 4.0". Lee, et al [5] details the "A cyber-physical systems architecture for industry 4.0-based manufacturing systems."

Stock et al [6] elaborates the "Opportunities of sustainable manufacturing in industry 4.0." and Gilchrist et al [7] discusses the "Industry 4.0: the industrial internet of things" Lu et al [8] elaborates the. "Industry 4.0: A survey on technologies, applications and open research issues." Ahram et al [9] conducts the "Blockchain technology innovations." Ananthi, J. Vijitha et al [10] explores the "A Peer to Peer Overlay Approach for Topology Maintenance in Wireless Networks."

Fernández-Caramés et al [11] discusses the "A review on the application of blockchain to the next generation of cybersecure industry 4.0 smart factories." Suma, V et al [12] performs the "Security and Privacy Mechanism Using Blockchain." Mohamed et al [13] discusses the ways to enhance the security in industry by. "Applying blockchain in industry 4.0 applications."

Sathesh, A et al [14] discusses the. "Enhanced Soft Computing Approaches for Intrusion Detection Schemes In Social Media Networks." Onik, et al [15] performs the "Blockchain in the Era of Industry 4.0." Bhalaji, N et al [16] conducts the "Qos and Defense Enhancement Using Block Chain for Fly Wireless Networks."

Ubiquitous Computing
Communication Technologies

3. Proposed Work

The Methodology is developed to provide a secure, and distributed, industrial data preservation using the block chain, consider a manufacturing unit functioning in different states of the country, the information's of all the units are regularly updated to the head of all the manufacturing unit over internet and stored in the cloud for is any time access. The information update include the valuable data generated from the machineries, the particulars of the workers and the confidential details of each unit. To elude the security breaches in the network formed by clubbing the all the devices and the functions. The paper develops the a novel algorithm of accordance as the "authentication Proof". The Blk-Chn devised in the paper preserves the data produced from all the units, so there is chance information getting leaked so the paper utilizes the Smart contract laid on the "proof authentication" to preserves the information's.

Each manufacturing unit is identified using an ID $M = \{M_1, M_2, \ldots M_n\}$ with and the data generated being represented as $M_d = \{M_{d1}, M_{d2}, \ldots M_{dn}\}$, every unit information are protected with the common and a secret key, the information's each unit are gathered in the JSON format and transformed into to encrypted form utilizing the "SHA 256" using the "asymmetric-cryptography" method the results obtained from encryption is represented as $\{E_{M_d} = E_{M_{d1}}, E_{M_{d2}} \ldots \ldots E_{M_{dn}}\}$, the data is protected with the public key so that it can be accessed only by the authorities of the particular unit and further converted into hexadecimal form and then into a perfect data form including the "publisher", who is the head of all the units. The head of all the unit and the head of the particular unit id identified with the identification key (ID_KEY) and the number (ID_NUM) that is unique respectively. The figure.1 below shows the structure of the blocks in the Blk-Chn used in the system.
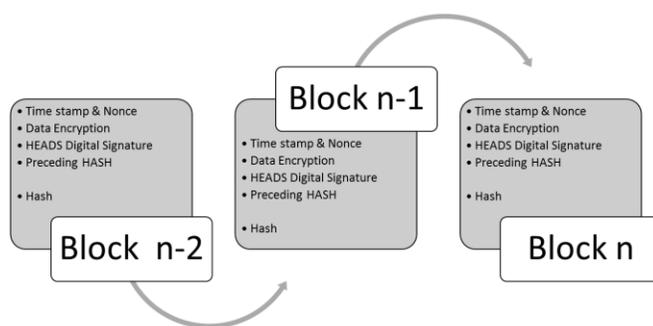

Figure.1 Block Structure

Information stored on the Blk-Chn is can be fetched by the any unit head entering the ID_NUM of the unit but could be accessed or completely read only if Head and the unit head delivers the permission, to access. The further blocks are appended to the Blk-Chn only after defining the accordance and if accepted by more than 50 %of the evaluators who are the unit heads. The flow of data from each manufacturing unit is represented as shown in the figure.2 below
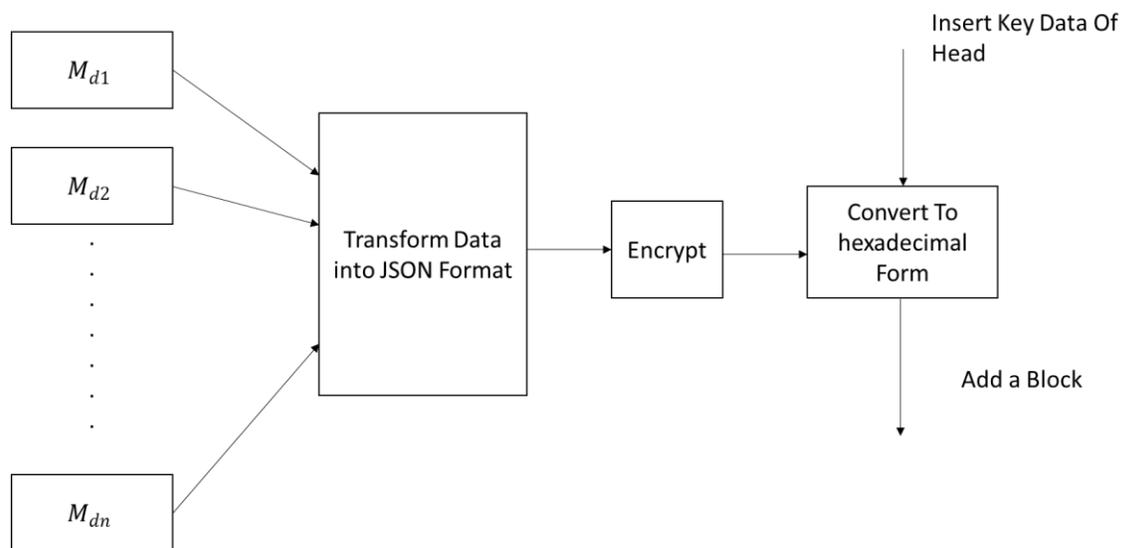

Figure.2 Data Flow from Manufacturing Unit

As shown the information's that are encrypted holds the original particulars of each manufacturing unit, the data's are digitally signed by the authority who heads all the units, to further used to monitor the authentication of the blocks on the execution of the algorithm that is based on accordance. The blocks integrity are defined by the HASH (SHA-256) of the blocks that are preceding. At the end the blocks are delivered with the hash for each blocks that are very helpful in identifying the tampering of the blocks. The synchronization of the time stamp with the universal time was accomplished using the Linux Epoch. The algorithm below in figure. 3 states the process of "authentication proof"

Input: $M_d, Time_{Stamp}, Nonce$
1 M <- receive public key of each unit $(M_d. ID\_NUM)$;
2 E_{M_d} <- encrypt(M_d, M);
3 $Pre_\#$ <- Preceding Hash ();
4 D_S <- $Digital_{Signature}(M_d, ID\_KEY)$;
5 $Data_{structure}$ <- dictionary $(Time_{Stamp}, Nonce, M_d, D_S, Pre_\#)$;
6 $Data_{structure}$ <- encrypt $(Data_{structure}, M)$;
7 obtain $(HEX (Data_{structure}))$
8 $hash < - SHA256(Data_{structure})$;
9 wait $(Nonce)$;
10 $Distribute (Data_{structure}, hash, M_d. ID\_KEY)$

Figure.3 Proof of Authentication

4. Results Evaluation

The Blk-Chn with "proof of authentication" is designed and implemented in Java-Script and was validated in MATLAB, on the basis of the security level provided and the cost spent , when compared to the conventional security measures to preserve the stored information's. Before examining the security level and the expenditure. The time taken by the "proof of authentication" and the CPU cycle utilized were examined and compared with the "proof of work" and "proof of stake" for number of industrial units involved.
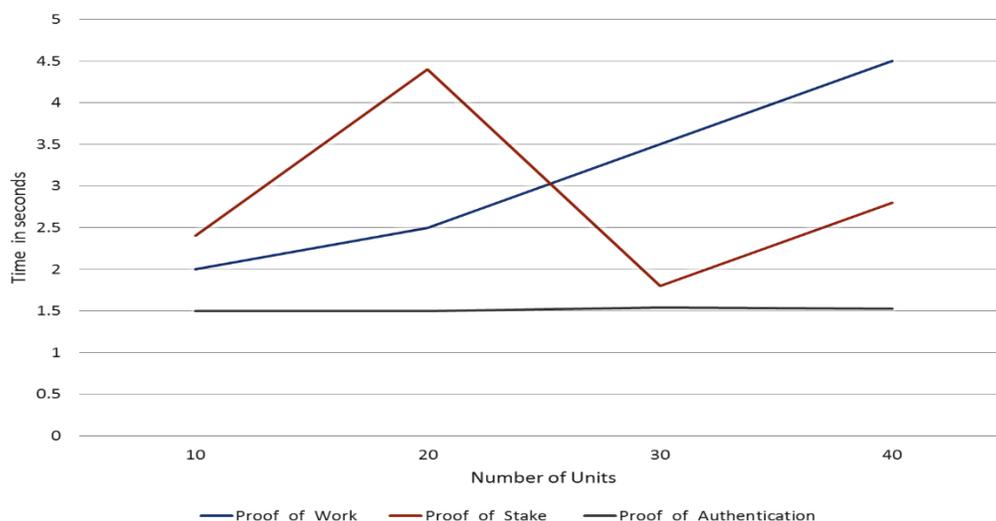

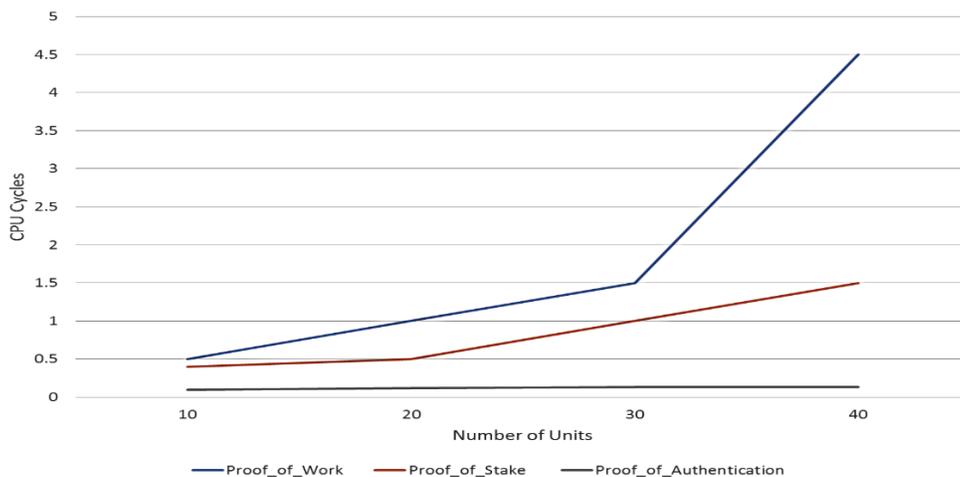Figure. 4 (a) Time Taken and Figure

Figure. 4 (b) CPU Cycles

The figure 4 (a) and 4 (b) shows that the proposed way of preserving in the Blk-Chn Consumed less time and CPU cycles Compared to the and more over found to be stable. When compared with the "proof of work" and "proof of stake".
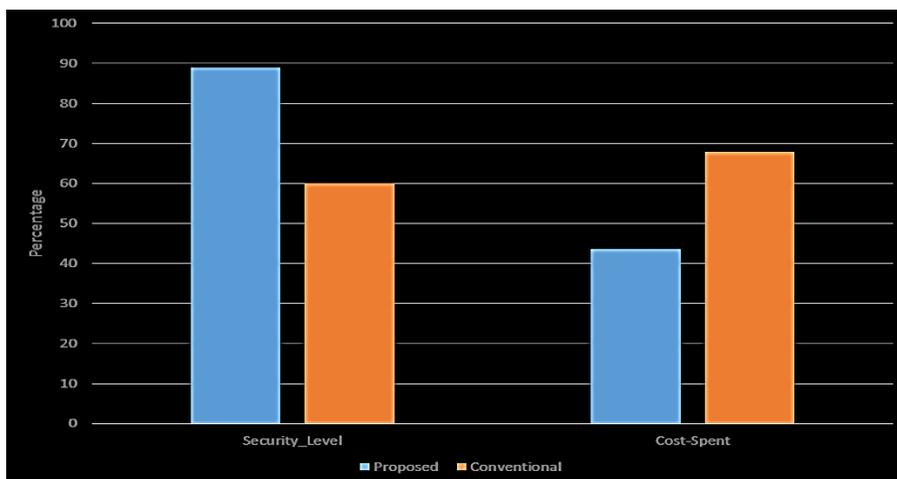

Figure. 4 (C) Cost and Security Level Comparison among the Blk-Chn Put Forth and the Conventional Security

The figure. 4 (C) presents the Cost and Security Level Comparison among the Blk-Chn put forth and the Conventional Security measures used in protecting the preserved information'. The proposed method outperforms the conventional security measures in terms of the security level provided against the attacks and as well as the expenditure.

5. Conclusion

The method to elude the security breaches in the network formed in the smart industries by connecting all the devices and the functions happening in the industries, the paper devised a block chain, supported by smart contract laid on proof of accordance to preserve the information's and provide it only to the authenticated persons, the method was designed using JAVA_Script and the evaluated in MATLAB , the evaluation of the time and the CPU cycles consumed by the proof of accordance was very much lesser and as well as consistent compared to the proof of stake and work. The proposed method further outperforms the conventional security measures in terms of the security level provided against the attacks and as well as the expenditure.

References

[1]   Jazdi, Nasser. "Cyber physical systems in the context of Industry 4.0." In *2014 IEEE international conference on automation, quality and testing, robotics*, pp. 1-4. IEEE, 2014.

[2]   Lee, Jay, Hung-An Kao, and Shanhu Yang. "Service innovation and smart analytics for industry 4.0 and big data environment." *Procedia Cirp* 16, no. 1 (2014): 3-8.

[3]   Lasi, Heiner, Peter Fettke, Hans-Georg Kemper, Thomas Feld, and Michael Hoffmann. "Industry 4.0." *Business & information systems engineering* 6, no. 4 (2014): 239-242.

[4]   Zhou, Keliang, Taigang Liu, and Lifeng Zhou. "Industry 4.0: Towards future industrial opportunities and challenges." In *2015 12th International conference on fuzzy systems and knowledge discovery (FSKD)*, pp. 2147-2152. IEEE, 2015.

[5]   Lee, Jay, Behrad Bagheri, and Hung-An Kao. "A cyber-physical systems architecture for industry 4.0-based manufacturing systems." *Manufacturing letters* 3 (2015): 18-23

[6]   Stock, Tim, and Günther Seliger. "Opportunities of sustainable manufacturing in industry 4.0." *Procedia Cirp* 40 (2016): 536-541.

[7]   Gilchrist, Alasdair. *Industry 4.0: the industrial internet of things*. Apress, 2016.

[8]   Lu, Yang. "Industry 4.0: A survey on technologies, applications and open research issues." *Journal of Industrial Information Integration* 6 (2017): 1-10.

[9]   Ahram, Tareq, Arman Sargolzaei, Saman Sargolzaei, Jeff Daniels, and Ben Amaba. "Blockchain technology innovations." In *2017 IEEE Technology & Engineering Management Conference (TEMSCON)*, pp. 137-141. IEEE, 2017.

Ubiquitous Computing
Communication Technologies

[10]   Ananthi, J. Vijitha, and Jennifer S. Raj. "A Peer to Peer Overlay Approach for Topology Maintenance in Wireless Networks."

[11]   Fernández-Caramés, 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.

[12]   Suma, V. "Security and Privacy Mechanism Using Blockchain." *Journal of Ubiquitous Computing and Communication Technologies (UCCT)* 1, no. 01 (2019): 45-54.

[13]   Mohamed, Nader, and Jameela Al-Jaroodi. "Applying blockchain in industry 4.0 applications." In *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, pp. 0852-0858. IEEE, 2019.

[14]   Sathesh, A. "Enhanced Soft Computing Approaches for Intrusion Detection Schemes In Social Media Networks." *Journal of Soft Computing Paradigm (JSCP)* 1, no. 02 (2019): 69-79.

[15]   Onik, Md Mehedi Hassan, Mohiuddin Ahmed, and A. K. Pathan. "Blockchain in the Era of Industry 4.0." *Data Analytics: Concepts, Techniques, and Applications* (2018): 259-298.

[16]   Bhalaji, N. "Qos and Defense Enhancement Using Block Chain for Fly Wireless Networks." *Journal of trends in Computer Science and Smart technology (TCSST)* 1, no. 01 (2019): 1-13.

Ubiquitous Computing
Communication Technologies