INTERNATIONAL JOURNAL OF RESEARCH CULTURE SOCIETY ISSN(O): 2456-6683
Monthly Peer-Reviewed, Refereed, Indexed Journal [Impact Factor: 6.834]
Volume - 7, Issue - 10, October - 2023 Publication Date: 25/10/2023

DOIs:10.2017/IJRCS/202310007 --:-- Research Paper / Article / Review

Credit-Based Consensus Mechanism Using Blockchain System for Providing Secure Industrial Internet of Things

Venkata Ramana Kaneti
Assistant Professor, Department of CSE
VNR Vignana Jyothi Institute of Engineering and Technology, Hyderabad, Telangana, India – 500090.
kvramana_2001@yahoo.com

Abstract: *The integration of the Internet of Things (IoT) with industry represents a pivotal strategy to drive automation and informatization within the industrial landscape. The Industrial Internet of Things (IIoT) holds the potential to significantly reduce errors, minimize costs, enhance operational efficiency, and bolster safety across manufacturing and industrial processes. This convergence offers the prospect of elevating the industry to new levels of integrity, availability, and scalability. However, existing IIoT systems are plagued by vulnerabilities such as single points of failure and malicious attacks, hampering their ability to provide stable services. Recognizing the resiliency and security advantages inherent in blockchain technology, there is growing interest in amalgamating blockchain and IoT. In the current state-of-the-art system, Scalable Access Management in IoT was implemented to facilitate access control between IoT devices and blockchain technology. However, this system has limitations due to its reliance on a central management hub. In the event of a failure or attack on this central hub, IoT devices connected to it become inaccessible. Additionally, the system employs chain-structured blockchains in IoT, which can be resource-intensive for power-constrained IoT devices. The architecture presents three primary challenges: 1) Balancing Efficiency and Security in Computing, 2) Navigating the Duality of Transparency and Privacy, and 3) Addressing the Conflict between High Concurrency and Low Throughput. To address these challenges, this paper proposes a novel blockchain system designed to support IIoT with a credit-based consensus mechanism. In a bid to reduce power consumption within the consensus mechanism, a self-adaptive Proof-of-Work (PoW) algorithm is implemented, tailored to power-constrained IoT devices. This innovative mechanism enables honest nodes to consume fewer resources while raising the cost of attacks for malicious nodes. Furthermore, an access control scheme is introduced, based on symmetric cryptography, within the blockchain system. This scheme offers a flexible approach to data authority management for users. The infrastructure of this system is founded on a directed acyclic graph (DAG)-structured blockchain, leveraging an asynchronous consensus model to enhance system throughput.*

Keywords: *Index Terms—Internet of Things, blockchain, credit-based, proof-of-work, directed acyclic graph, security.*

1. INTRODUCTION :

The Internet of Things (IoT) is a network of interconnected computing devices, mechanical and digital machines, objects, and people, each assigned unique identifiers (UIDs) and endowed with the ability to transmit data across a network without necessitating human-to-human or computer interaction. IoT empowers individuals to lead smarter lives and gain better control over their daily activities. Its relevance extends beyond the realm of smart home automation, playing a crucial role in various industries. IoT equips companies with real-time insights into the functionality of their enterprise systems, offering a window into aspects ranging from machine performance to supply chain and logistics operations. By streamlining processes and reducing labor costs, IoT facilitates waste reduction and enhances service quality, resulting in cost-effective production and consistent consumer transactions. Its influence extends to diverse sectors, encompassing health, banking, retail, and manufacturing. Smart cities harness IoT technologies to minimize waste and energy consumption, while in agriculture, connected sensors aid in monitoring crop and cattle yields, facilitating growth trend forecasts.

However, the IoT's significance transcends digital voice assistants and wearable devices. IoT applications are reshaping the way businesses operate behind the scenes in the industrial landscape. The Industrial Internet of Things (IIoT), also referred to as Industry 4.0 when applied to the manufacturing sector, represents the integration of intelligent manufacturing equipment, AI-driven automation, and advanced analytics aimed at enhancing worker productivity and overall factory efficiency. The convergence of IoT and business processes is a vital driver for market automation and digitization. IIoT is instrumental in defect reduction, cost control, performance improvement, and safety enhancement within manufacturing and industrial operations. Nevertheless, the promising landscape of IIoT is accompanied by looming security threats and vulnerabilities that could potentially outweigh its advantages.

The IIoT has the potential to revolutionize manufacturing by enabling the rapid and efficient collection of significantly larger volumes of data than ever before. Many manufacturers have already embarked on the implementation of IIoT devices and processes,

leveraging intelligent wired devices within their factories, warehouses, and workshops. While the specific application of this technology may vary from one company to another, the common objective remains consistent: to enhance operational efficiency through analytics, automation, and connectivity. Interconnected sensors and actuators empower businesses to promptly identify inefficiencies and issues, resulting in time and cost savings, while also supporting business intelligence (BI) efforts. In the manufacturing domain, IIoT holds substantial promise for quality assurance, sustainability, supply chain transparency, and overall supply chain performance. IIoT plays an indispensable role in industrial processes, encompassing predictive maintenance (PdM), improved field support, energy management, and asset monitoring.

1.1 How IIoT works

IIoT is a network of smart devices linked to forming networks that track, store, share, and analyze data.

- Intelligent tools that can perceive, interact, and store knowledge about themselves.
- Public and/or private data processing systems
- Analytics and applications extracting business information from raw data; and People.

1.2 IIoT versus IoT

The Internet of Things (IoT) and the Industrial Internet of Things (IIoT) share numerous common technologies, including cloud networks, sensors, networking, machine-to-machine communications, and data analytics. However, they serve distinct purposes.

IoT applications interconnect devices across various verticals, encompassing agriculture, healthcare, consumer products, utilities, government, and cities. Typical IoT devices comprise smart appliances, exercise bands, and other applications that typically do not lead to emergency situations when issues arise.

Conversely, IIoT applications connect machines and devices within critical industries such as oil and gas, utilities, and manufacturing. In IIoT deployments, system failures and downtime can result in high-risk or even life-threatening situations. In contrast to the user-centered design of IoT applications, IIoT applications are primarily concerned with enhancing performance, health, and safety.

1.3 Benefits of IIoT

The digital Internet of Things offers companies a range of top-class advantages, with predictive maintenance being a prominent one. This involves organizations harnessing real-time data generated by IIoT systems to predict machine failures, allowing them to take proactive steps to rectify issues before a component fails or a computer breaks down.

Increased field service is another common benefit of IIoT technologies. They empower field service technicians to identify potential problems in customer equipment before they escalate into major issues, enabling technicians to resolve these concerns before they inconvenience customers.

Asset tracking is another valuable perk of IIoT. Suppliers, producers, and customers can utilize asset management systems to monitor product location, status, and condition throughout the supply chain. Instant alerts are sent to stakeholders if goods are damaged or at risk, giving them the opportunity to take immediate preventive action to rectify the situation.

IIoT also contributes to improved customer loyalty. As products become linked to the Internet of Things, manufacturers can collect and analyze data on how consumers use their products. This data allows manufacturers and product designers to tailor IoT devices to meet customer needs, resulting in more customer-centric product roadmaps.

Furthermore, IIoT enhances service maintenance. Given that manufacturing equipment is subject to wear and tear, as well as various environmental conditions within a facility, sensors can monitor vibrations, temperature, and other factors that might lead to less-than-ideal operating conditions. IIoT is fundamentally reshaping industries, driving unprecedented levels of productivity, efficiency, and performance, enabling manufacturers to reap substantial financial and operational transformation benefits.

Following are the advantages that make IIoT a vital and effective resource in the digital future for manufacturing companies that want to expand and prosper. In recent years, with the advent of the blockchain, the concept has arisen. Combining blockchain and IoT has gained considerable momentum interests, [1]-[5].

a. Optimum Energy Efficiency

The electricity bill stands as one of the most significant expenses for industrial organizations. IIoT is poised to motivate manufacturing leaders to pinpoint resource wastage within their operations and take corrective actions. Real-time data provides valuable insights, including off-hour usage and other energy-saving prospects, enabling managers to identify operational inefficiencies and areas of waste.

b. Just in Time Manufacturing (JIT)

The Just in Time (JIT) approach is designed to minimize cycle times within the production and manufacturing network, reduce reaction times between suppliers and consumers, and enhance mutual cooperation throughout the supply chain. Through IIoT, basic metrics like performance, uptime, and failure rates are continuously monitored, among other factors. The analysis of this data enables

ongoing enhancements in manufacturing processes and staff performance. Real-time data obtained from IIoT sensors and devices encompasses information about distribution schedules, production capacity, staff availability for goods receipt and loading, and notifications regarding material availability.

c. Predictive Maintenance (PdM)

The primary objective of Predictive Maintenance (PdM) is twofold: to forecast when machine or equipment failure is likely to happen and subsequently prevent such occurrences through timely maintenance. PdM strives to keep maintenance efforts at a minimum, ideally at an optimal level, and prevent unplanned reactive maintenance, thus enabling a more efficient maintenance schedule. It offers numerous cost-related advantages, including the reduction of manufacturing hours lost to repairs, decreased expenses on replacement parts and materials, and a reduction in the time needed to service machines and equipment.

d. Machine Repeatability

High-frequency sensor data recording enables the tracking of parameters such as vibration, speed, and temperature during system operation, with data collected in milliseconds. Repeatability, in this context, pertains to the ability to reproduce a specified set of conditions or circumstances within a limited range or tolerance. Through IIoT, data analytics manufacturers can achieve a quicker return on investment (ROI) at a reduced cost.

e. Fast and Informed Decision Making

In IIoT operations, administrators are no longer left uninformed about machine or equipment outcomes and issues. Similar to Predictive Maintenance (PdM), this shifts a manager's approach from a reactive one to a proactive one, resulting in waste reduction and improved overall visibility. The key lies in the quality of the data they possess and their readiness to take action based on the insights derived from the data. The future factory aspires to be more efficient, run more profitably, and enhance customer satisfaction.

In current research on this subject, O. Novo [3] introduces a blockchain-based access control framework for IoT app management. However, due to its reliance on a central management core, the system lacks complete reliance on a distributed architecture. In the event of control hub failure or an attack, IoT devices connected to it become inaccessible. Z. Li et al. [4] utilize consortium blockchain technology to establish a stable energy trading network. Nevertheless, they do not adequately address privacy concerns, such as the risk of unauthorized data disclosure, and therefore cannot guarantee the confidentiality of sensitive data. In the context of IoT applications, the aforementioned solutions all implement chain-structured blockchains, which can be burdensome for power-constrained IoT devices. Z. Xiong et al. [6] present an innovative approach by implementing edge computing for mobile blockchain applications. They introduce an effective edge resource management Stackelberg game model for mobile blockchains. Through the utilization of edge computing, they successfully reduce the computational demands on mobile devices.

When introducing a novel blockchain architecture into IIoT systems, three major challenges come to the forefront:

1. Balancing Efficiency and Security in Transactions: Blockchain consensus algorithms, while effective in safeguarding against malicious attacks, often employ resource-intensive mechanisms. The most prevalent of these is the Proof-of-Work (PoW) algorithm, which compels nodes to execute complex hash algorithms to verify transactions. However, this approach is overly demanding for power-constrained IoT devices. The dilemma faced in this study is finding the right trade-off between ensuring security and optimizing efficiency within the consensus processes.
2. Navigating the Coexistence of Transparency and Privacy: Blockchain is renowned for its transparency, a key financial feature. However, this transparency can pose limitations in certain IIoT systems, particularly when handling sensitive data that necessitates confidentiality, accessible only to authorized parties. Therefore, a critical consideration is designing an access control system that can function within the framework of a transparent blockchain.
3. Resolving Conflicts between High Competitiveness and Low Performance: In IIoT systems, IoT devices continuously generate and record data, leading to high levels of competitiveness. Regrettably, the intricate cryptographic security measures deployed within blockchains often hamper throughput. Furthermore, the synchronous consensus model of chain-structured blockchains employed in IIoT systems does not fully exploit available bandwidth. Consequently, the third challenge entails the enhancement of blockchain throughput to meet the demands for routine transactions in IIoT systems.

These challenges underscore the intricacies of harmonizing security, transparency, and performance in the context of integrating blockchain technology with IIoT systems.

1.4 Block Chain Technology

Blockchains serve as distributed ledgers or databases, underpinned by intricate cryptographic technologies and a consensus model [9]. They facilitate parties with varying levels of trust to establish and maintain consensus on shared facts' existence, status, and evolution. The principles of blockchain technology have garnered significant interest and adoption in both industry and academia. Blockchain is set to play a pivotal role in enabling IoT, while also providing defense mechanisms against hacking attempts. Given its inherent design for centralized control, a protective framework built around it should be sufficiently scalable to accommodate the rapid expansion of IoT. Furthermore, blockchain's robust defense against data theft can prevent a rogue computer

from disseminating false information that could harm homes, factories, or transportation networks. Two main types of blockchains exist based on structural differences: chain-structured blockchains and DAG-structured blockchains.

a. Chain-Structured Blockchain

Most existing blockchain implementations, such as Bitcoin, Ethereum, and Hyperledger, are based on chain-structured blockchains. In Figure 1, white squares represent valid blocks, while gray squares represent invalid blocks. A chain-structured blockchain designates the longest chain as the primary chain within the system. Blocks connected to the main chain are recognized as legitimate transactions. When two blocks are generated a few seconds apart, bifurcations may occur, and the most recent block within the longest chain is always selected. Consequently, other blocks in shorter chains are considered invalid. However, the power-intensive nature of chain-structured blockchain, owing to its complex cryptographic security mechanisms [9], makes it less suitable for power-constrained IoT devices. Furthermore, synchronous consensus mechanisms limit system throughput, as transactions can only be verified one by one, which may not meet the requirements of regular IoT system requests.

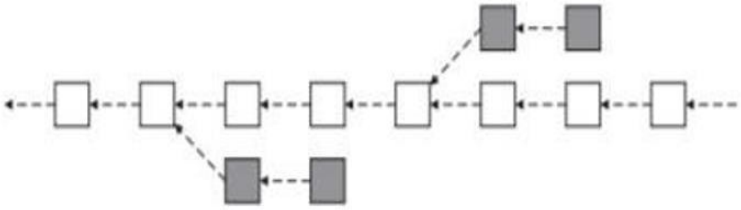

Figure 1. Chain-structured blockchain

b. DAG-Structured Blockchain

In an endeavor to make blockchain technology more practical, especially in power-constrained applications, innovators have introduced a novel blockchain framework based on a directed acyclic graph architecture known as "tangle." Unlike the traditional block-based approach, tangle dispenses with blocks, and each transaction operates as an individual node interconnected in the distributed ledger.

Within the tangle, transactions verify two prior transactions that are attached but not yet confirmed in the tangle – these are referred to as "tips." Only after these verifications are complete, a new transaction is issued. Subsequently, the new transaction becomes linked to these two preceding transactions through the PoW (Proof of Work) algorithm.

The new transaction is then broadcast to the tangle network, and over time, numerous older transactions will validate each new transaction. For each transaction, a metric known as "weight" is assigned, which is proportional to the transaction's number of validations. In the context of Bitcoin, this concept is akin to the notion of "six-block security" [2], where a higher weight value indicates increased resistance to tampering.

In a chain-structured blockchain, new transactions must undergo synchronous consensus, i.e., they require verification before being incorporated into the main chain. In contrast, tangle employs an asynchronous consensus model, which proves to be more effective in enhancing system throughput.

As depicted in Figure 2, white squares represent verified transactions, while grey squares denote tips. DAG-structured blockchain operates without the perpetual constraints of a single main chain and potential forks. The relationships between transactions resemble a complex web. This innovative architecture and consensus mechanism hold the promise of significantly improving network performance and system response times. Notable examples of DAG-structured blockchains include IOTA, Byteball [11], and NANO.

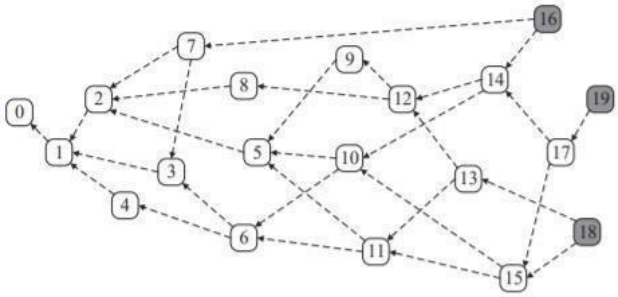

Figure 2. Directed acyclic graph (DAG)-structured blockchain

1.5 How does blockchain Works?

Whenever anyone decides to connect a transaction to the chain, it must be checked by all participants in the network. It they do by applying a transaction algorithm to check its validity. How exactly "true" means is determined by the blockchain framework, and can differ between systems. It is then up to a majority of the participants to agree on the transaction being legitimate. A collection

of accepted transactions is then bundled into a block, which is sent to all of the network nodes. In turn they validate the new block. Increasing successive block contains a hash of the previous block which is a unique fingerprint. Following are the two types of Blockchains:

a. Public Blockchain

In a public blockchain, anyone can read or write data. Some public blockchains allow unrestricted access to both reading and writing, while others may restrict write access. For example, Bitcoin follows an open model where anyone can participate in reading and writing transactions.

b. Private Blockchain

Private blockchains are designed for a closed network comprising identified and trusted participants. Access is limited to known entities, making it well-suited for scenarios involving multiple companies belonging to the same legal entity or similar use cases. Private blockchains prioritize privacy and control over openness.

1.6 The Blockchain and IoT

Blockchain technology is the missing link in the Internet of Things to address questions about scalability, safety and reliability. Perhaps blockchain technology may be the magic bullet the IoT industry requires. Blockchain technology can be used to monitor trillions of connected devices, enable transaction processing and system coordination; allow substantial savings for manufacturers in the IoT industry. This decentralized approach would remove single failure points, creating a more robust environment to operate on devices. Blockchains' cryptographic algorithms would make user data more secure.

Blockchain ledger is tamper-proof and can't be exploited by malicious actors since it doesn't exist in any particular place, so man-in-the-middle attacks can't be orchestrated because there's no single email line to intercept. Blockchain has already proven its value in the field of financial services by cryptocurrencies such as Bitcoin [10], offering secure peer-to-peer payment transactions without the need for third-party brokers. The blockchain's decentralized, autonomous, and trustless capabilities make it an ideal component for being an integral element of IoT solutions. It's no wonder that enterprise IoT solutions have rapidly become one of blockchain solutions' early adopters. The blockchain will hold an unchanging record of the history of smart devices within an IoT network. This feature allows the smart devices to operate autonomously without the need for centralized authority. As a result, the blockchain opens the door to a number of IoT scenarios that without it would been incredibly difficult, or even impossible to introduce.

Using the blockchain will allow real, autonomous smart devices that can exchange data, or even execute financial transactions, without a centralized broker being required. This form of autonomy is possible because the nodes in the blockchain network are going to check the transaction's validity without relying on a central authority.

2. LITERATURE SURVEY :

Blockchain for IOT security and privacy: The case study of a smart home (A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram) [1]: Security and privacy on the Internet of Things (IoT) remain a major challenge, primarily due to the pervasive and dispersed existence of IoT networks. Blockchain-based solutions provide decentralized protection and privacy but require considerable overhead resources, delay, and computing expenses that are not sufficient for most resource-constrained IoT applications. A lightweight instantiation of a blockchain is introduced in earlier research to remove the Proof of Work (POW) and the definition of coins. In a smart home environment, this approach has been exemplified and consists of three main sections: cloud storage, overlay, and smart home. In this paper specific core components and smart home tier roles are outlined. Every smart home is equipped with a high-resource, always online computer, known as the "miner," which is responsible for handling all communication inside and outside the home. The miner also maintains a private and safe BC, used for communications control and auditing. The proposed smart home system based on blockchain is protected by carefully evaluating its protection with respect to the basic safety goals of confidentiality, honesty, and availability. Finally, simulation results to illustrate that the overheads imposed by this method (in terms of traffic, processing time, and energy consumption) are negligible in comparison to its gains in protection and privacy.

An overview of blockchain technology: Architecture, consensus, and future trends (Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang) [9]: With a specially built data storage system, Bitcoin network transactions may take place without any third party and the key technology for creating Bitcoin is blockchain, first introduced in 2008 and implemented in 2009. Blockchain may be called a public ledger, and all transactions committed are stored in a block list. This chain grows as new blocks are continually appended to it. For user safety and accuracy of the ledger, asymmetric cryptography and distributed consensus algorithms were introduced. In general, blockchain technology has core features of decentralization, durability, transparency, and audibility. Blockchain is immutable. When bundled into the ledger, the transaction cannot be tampered with. Businesses that require a high degree of reliability and integrity can use blockchain to attract clients. In addition, blockchain is distributed and the single point of fault situation can be avoided. As with smart contracts, once the contract is placed on the blockchain, the contract will be executed automatically by the miners.

PoW (work proof) is a consensus technique used in the network Bitcoin. Somebody has to be chosen for tracking the transactions in a decentralized network. Random collection is the best way to do so. Nevertheless, selection at random is vulnerable to attacks.

So if a node tries to publish a transaction block, there is a lot of work to be done to show that the node is not going to attack the network. The job usually requires calculations for the machine. In PoW, a hash value of the block header is determined by each network node. The block header includes a nonce, and the miners would frequently change the nonce to get different hash values. The consensus requires the calculated value to be equal to, or less than, a given value. Once one node hits the target value, the block will be transmitted to other nodes and all other nodes will confirm the correctness of the hash value to one another. Many miners can add this new block to their own blockchains if the block is validated. Nodes calculating the hash values are called miners, and in Bitcoin, the PoW process is called mining. Possible blockchain future directions are blockchain testing, stopping the tendency to centralization, big data analytics, and blockchain application

Blockchain-based decentralized trust management in vehicular networks (Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. M. Leung) [5]: Vehicle networks allow vehicles to produce and transmit messages to improve the safety and efficiency of the traffic. Nevertheless, it is difficult for automobiles to determine the authenticity of obtained texts, due to the untrusted environments. In this paper, we suggest a decentralized trust management system based on blockchain technologies in-vehicle networks. In this method, vehicles may use the Bayesian Inference Model to validate the obtained messages from neighboring vehicles. The vehicle will produce a ranking for each message source vehicle, based on the outcome of the validation. With the ratings uploaded from vehicles, roadside units (RSUs) measure the trust value offsets of the vehicles involved and bundle these data into a "box." Instead, each RSU will attempt to link their "blocks" to the confidence blockchain that all RSUs hold. The more the total value of offsets (stake) is in the block, the easier the RSU can find the nonce for the hash function (PoW), by using the Joint Proof-of-Work (PoW) and proof-of-stake consensus mechanism. In this way, all RSUs work together to maintain a modified, secure, and consistent blockchain of trust. Results of the simulation show that the device proposed is efficient and feasible in capturing, measuring, and storing trust values in-vehicle networks.

Consortium blockchain for secure energy trading in the industrial Internet of Things (Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang,) [4]: In industrial Internet of Things (IIoT), peer-to-peer (P2P) energy trading takes place Omni presently in various contexts, such as microgrids, energy storage networks, and vehicle-to-grid networks. Within such cases, however, there are growing protection and privacy problems posed by untrustworthy and untransparent energy markets. The consortium blockchain technology is used to address security issues by introducing a stable energy exchange network called energy blockchains. This energy blockchain can be commonly used in general P2P energy trading scenarios to get rid of a trusted middleman. In addition, a credit-based payment system is proposed to enable fast and regular energy trading to reduce the transaction limitation arising from transaction confirmation delays on the energy blockchain. It also proposes an optimal pricing strategy for credit-based loans using the Stackelberg game. Security analysis and numerical tests based on an actual dataset show that in IIoT the proposed energy blockchain and credit-based payment scheme is safe and efficient.

Blockchain meets IoT: An architecture for scalable access management in IoT (O. Novo) [3]: The Internet of Things (IoT) is reaching full maturity from its infancy and developing itself as a cornerstone of the future Internet. The ability to control them is one of the technological challenges of getting trillions of devices deployed worldwide. Although access management systems exist in IoT, they are based on centralized frameworks that create a new variety of technological limitations for globally managing them. It proposes a new framework to arbitrate functions and permissions in IoT. The new architecture is a fully distributed, blockchain-based IoT access control scheme. Supported by proof-of-concept implementation, the design is tested in practical IoT scenarios. The findings demonstrate that, in particular scalable IoT applications, the blockchain system may be used as an access control system.

Sybillimit: A near-optimal social network defense against sybil attacks (H. Yu, P. B. Gibbons, M. Kaminsky, and F. Xiao) [14]: Decentralized distributed networks such as peer-to-peer networks are especially vulnerable to Sybil attacks, in which a malicious user pretends to have several identities (called Sybil nodes). Without a trustworthy central authority, it's very difficult to protect against Sybil attacks. Our latest SybilGuard protocol [H] is amongst the limited number of decentralized approaches. Yu et al., 2006] leverage a key insight into social networks to connect the number of agreed Sybil nodes. Although its path is promising, SybilGuard will allow for the acceptance of a large number of Sybil nodes. Additionally, SybilGuard believes social networks are quickly merging, which has never been proven in the real world. This paper introduces the novel protocol SybilLimit, which leverages the same expertise as SybilGuard but provides significantly enhanced and near-optimal safeguards. In our experiments for a million-node network, the number of sybil nodes approved is decreased by an ominous factor (radian), or around 200 times. This further shows that the guarantee of SybilLimit, when considering solutions based on fast-mixing social networks, is at most a log n factor away from the optimum. Finally, we have the first proof based on three large-scale real-world social networks that real-world social networks are indeed quickly mixing up. Which validates the fundamental assumption behind the approach taken by SybilLimit and SybilGuard.

When mobile blockchain meets edge computing (Z. Xiong, Y. Zhang, D. Niyato, P. Wang, and Z. Han) [6]: Blockchain has become a revolutionary decentralized data-management platform as the core technology of the massively common Bitcoin digital currency. While blockchain has been widely adopted in many applications (e.g., finance, healthcare, and logistics), its use is still limited in mobile services. This is because blockchain users have to solve predetermined proof-of-work puzzles in order to add new data (i.e., a block) to the blockchain. Nevertheless, solving the work proof requires considerable CPU time and energy resources which are not ideal for resource- limited mobile devices. Multiple access mobile edge computing seems to be an auspicious solution for solving the proof-of-work puzzles for smartphone devices in order to promote blockchain applications in future smartphone Internet of Things systems. We're introducing a novel edge computing concept for mobile blockchain first. We would then

incorporate an economic approach to edge management of computing capital. In addition, a prototype of blockchain-enabled mobile edge computing systems is presented with experimental findings to support the proposed design.

3. THEORETICAL ANALYSIS

3.1 Existing System

A decentralized access regulation framework based on blockchain technology was proposed for managing IoT devices as shown in he Figure 3. However, the system is not entirely built on a distributed architecture due to its reliance on a central management center. In the event of a control hub failure or a targeted attack, IoT devices connected to it may become inaccessible. Furthermore, this framework fails to address privacy concerns, such as the risk of unauthorized data disclosure, and thus cannot ensure the confidentiality of sensitive data. In IoT systems, this architecture relies on chain-structured blockchains, which can be overly burdensome for power-constrained IoT devices.

The following are the disadvantages of the existing system:

- The use by nodes of high-complexity hash algorithms to validate transactions.
- The downside is that a central management system is used.
- The use of complex cryptographic-based safety mechanisms decreases blockchain throughput.
- The architecture is unable to provide reliable services.

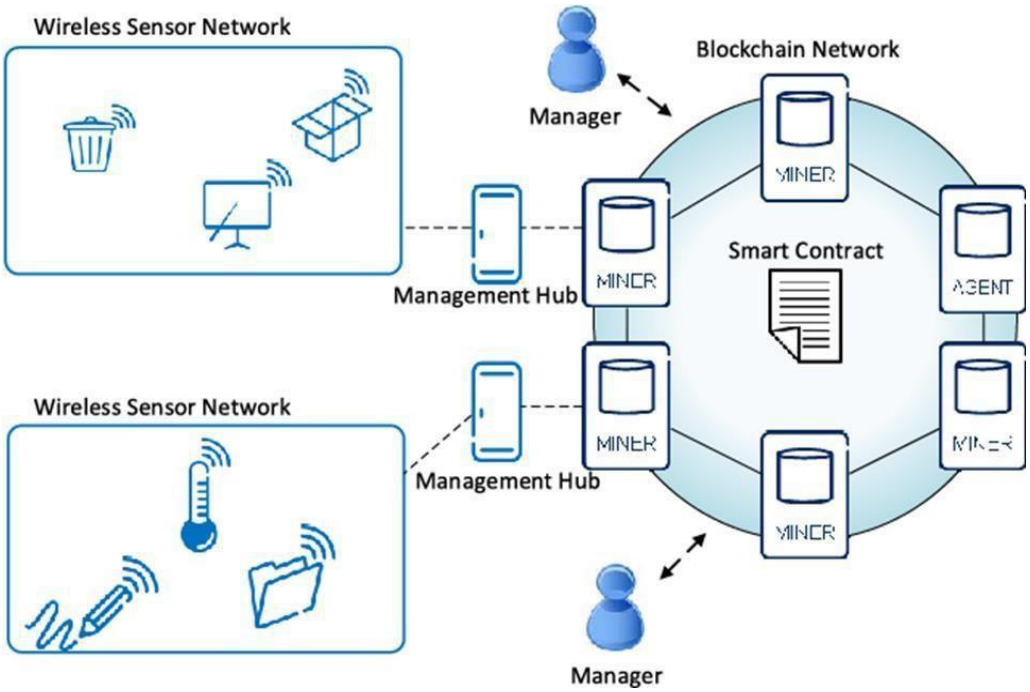

Figure 3. Decentralized Access Control System

3.2 Proposed System

A blockchain network with a credit-based consensus mechanism for IIoT is conceived in the proposed framework as shown in the Figure 4. For power-constrained IoT computers, a self-adaptive Proof-of-Work (PoW) algorithm is implemented to decrease the power consumption in the consensus mechanism. This mechanism would allow honest nodes to consume fewer resources as malicious nodes are forced to increase the cost of attacks. In the blockchain framework, an access control scheme based on symmetric cryptography is implemented which provides users with a flexible method of managing data authority. This network architecture is built on a standardized blockchain based on the guided acyclic graph (DAG), which enhances the network throughput by leveraging its asynchronous consensus model.

The following are the advantages of the proposed system:

- The architecture ensures the confidentiality of sensitive data.
- Provides machine protection and the quality of transactions.
- Reduces power consumption.

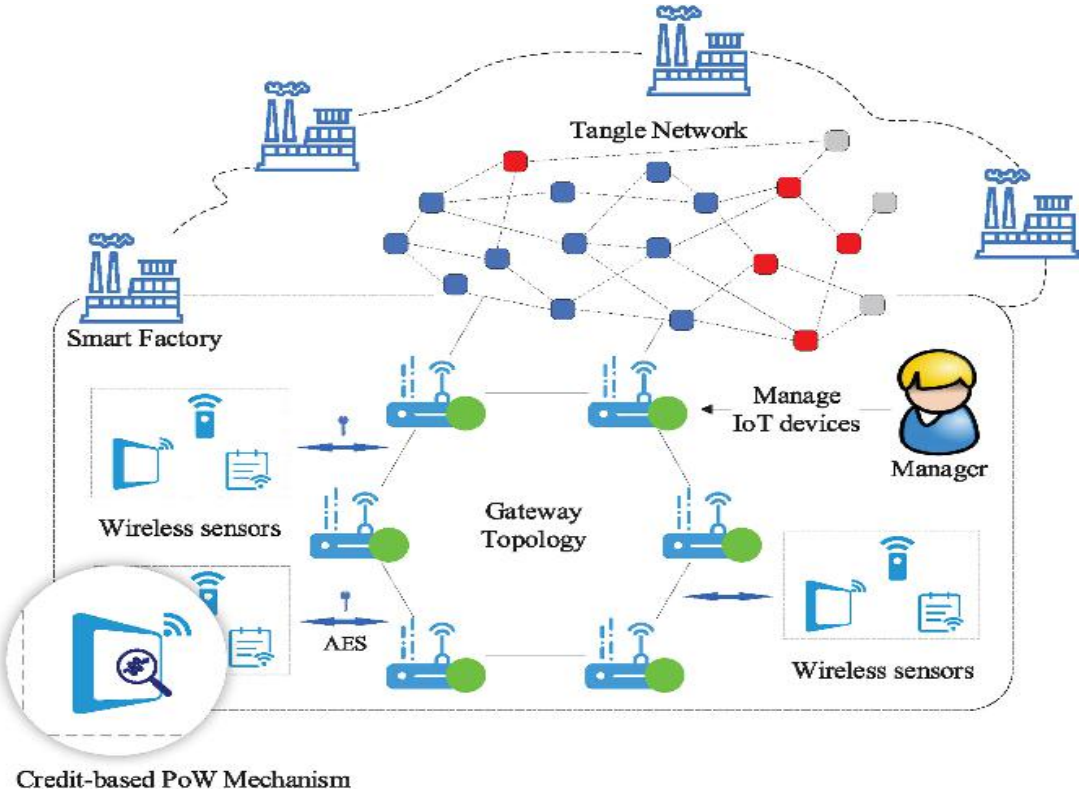

Figure 4. The architecture of blockchain-based IIoT system for smart factory

4. METHODOLOGY :

This section outlines the methodology for the proposed blockchain-based Industrial Internet of Things (IIoT) framework, encompassing system architecture, the credit-based Proof-of-Work (PoW) process, and data authority management.

a. Architecture Design for Smart Factory

The network architecture is founded on a Directed Acyclic Graph (DAG)-structured blockchain, with each entity functioning as a node within the IIoT system based on blockchains. This can be categorized into two groups for functional differentiation: light nodes and full nodes. Light nodes pertain to power-constrained devices, including IoT devices, which, due to their resource limitations, do not store blockchain information. Light nodes are responsible for tasks such as testing tips, executing PoW consensus algorithms, and forwarding new transactions to full nodes. Full nodes, on the other hand, encompass more capable devices, such as gateways or servers, primarily tasked with managing the entire blockchain network or tangle. They accept transaction requests from light nodes and propagate them across the blockchain network.

b. Credit-Based PoW Mechanism

In this section, we introduce the credit-based PoW mechanism designed to strike a balance between efficiency and security within the consensus process. Each node, denoted as 'I,' possesses a credit value denoted as Cri. The credit value dynamically adjusts based on the actions of the node. Normal activities, such as adhering to program rules when submitting transactions, result in a gradual increase in the credit value over time. Conversely, nodes engaged in irregular activities may experience a decrease in their credit value. The complexity of the PoW mechanism is self-adaptive and is contingent on the credit value of each node. Lower credit values necessitate a longer time to execute the PoW algorithm. This mechanism incentivizes honest nodes to consume fewer resources while imposing a higher cost on malicious nodes engaging in attacks.

We address two potential abnormal behaviors within the system through the design of the credit-based PoW mechanism:

1. Lazy Tips: A 'lazy' node perpetually verifies a fixed pair of very old transactions while failing to contribute to the validation of more recent transactions. For instance, a malicious entity can artificially inflate the number of tips by creating numerous transactions that validate a fixed pair of transactions. This enables the selection of these tips with a high probability for future transactions, effectively sidelining the tips belonging to honest nodes.
2. Double-Spending: A malicious node attempts to spend the same token multiple times by generating several transactions before the previous one undergoes validation. While such behavior is detected and annulled by the asynchronous consensus mechanism, it hampers system efficiency as other related transactions also require revalidation.

c. Data Authority Management Method

Due to the inherent transparency of blockchain, sensor data stored in the blockchain is accessible to the public. To address this, a data authority management method is proposed to control access to sensor data within the network. For open systems, data security is ensured through encryption. There are two primary encryption algorithms: symmetric key encryption and public key encryption. Considering encryption efficiency, symmetric key encryption significantly outpaces public key encryption (roughly 100-1000 times faster), making it suitable for power-constrained devices. Given the substantial volume of sensor data in smart factories, the use of slower public key encryption is impractical. To circumvent this, a symmetric key encryption is employed, distinct from public key encryption, for secure secret key transmission. This entails a decentralized key distribution scheme, eliminating the need for a central trusted party, resulting in a versatile data authority management system. Each node possesses a unique identifier in the form of a public/secret key (PK, SK), as per the earlier architectural design, and employs public key encryption for symmetric key distribution.

5. ALGORITHMS AND IMPLEMENTATION :

In this section, we delineate the methodology for the practical implementation, which is bifurcated into two modules: the "Industrial Manager" and "Wireless Sensors."

a. Industrial Manager:

The Industrial Manager module encompasses the following wireless sensor components:

Set of Sensors: The wireless sensors deployed within a smart factory fall within the category of light nodes. Upon initialization, each sensor generates a unique blockchain account, comprising a public/secret key pair (PK, SK) that serves as its distinct identifier within the system. These key pairs are not only utilized for transaction signing but also for secure key exchange. These compact sensor devices facilitate data communication with GATEWAYS. Sensors encrypt the data, generate transaction hash codes, and subsequently transmit them to the gateway. During transaction transmission, sensors can detect and report two types of potential attacks: "Lazy Tips" and "Double Spending."

Gateways: Gateways assume the role of full nodes and are dedicated to the maintenance of the tangle network. Gateways swiftly receive transaction requests from various sensors and broadcast these transactions within the tangle. Importantly, gateways exclusively process transactions originating from authorized sensors, as approved by the manager.

Manager: The Manager functions as a specific full node within a smart factory, responsible for overseeing IoT devices. The manager's public key is hardcoded into the gateway software, conferring exclusive authority to the manager for publishing the device authorization list. The manager is empowered to manage IoT devices, including their addition or removal, by initiating transactions that document the public keys of registered IoT devices. The application is also responsible for generating sensor keys and executing the Credit Consensus Proof-of-Work (PoW) algorithm to process and validate sensor transactions.

Tangle Network: The tangle network utilized in our system functions as a public blockchain network, accessible by any concerned party. Gateways, serving as full nodes, ensure the integrity and security of the network by transmitting transactions and maintaining copies of the blockchain. Furthermore, secure data sharing is facilitated between different factory entities. For sensitive data, a data authority management method is employed to safeguard the privacy of sensor data.

b. Wireless_Sensors:

This segment represents a simulation-based program that entails gateways receiving keys and subsequently transmitting encrypted transactions to processing gateways.

Full Nodes: There are two pivotal roles for full nodes, encompassing the manager and gateway. A full node operates within the tangle network, serving as both a transaction relay and a network information provider. It furnishes a straightforward RESTful HTTP interface to enable light nodes to post transactions through this interface to full nodes. Additionally, the credit-based PoW system incorporates features related to symmetric key generation and distribution into full nodes. The SHA-256 algorithm is employed for secret key distribution, while sensor data encryption utilizes the AES block cipher algorithm.

Light Nodes: Light nodes represent IoT devices linked to full nodes, facilitating interactions within the tangle network. These nodes are built on the IOTA Python API Library, PyOTA3. Notably, PyOTA3 does not provide a native PoW interface, necessitating the implementation of a Java-written extension package to extend PyOTA's capabilities for PoW. The kit specifications align with the credit-based PoW system design outlined previously. Light node control is established through data authority and the AES-based encryption of collected sensor data.

ALGORITHMS

Proof-of-work **[13],** or PoW, is the initial consensus algorithm in a network of blockchains. This algorithm is used in Blockchain to validate transactions and to add new blocks to the chain. WithPoW, miners compete with each other to complete network transactions and get rewarded.

In a network, users send digital tokens to each other. A shared ledger puts all the transactions together into blocks. However, the transactions should be checked and blocks organized with care.Special nodes called miners share this burden and a method is called mining. The core guiding principles are a complex mathematical puzzle, and an ability to prove the solution easily.

ISSN(O): 2456-6683
[Impact Factor: 6.834]
Publication Date: 25/10/2023

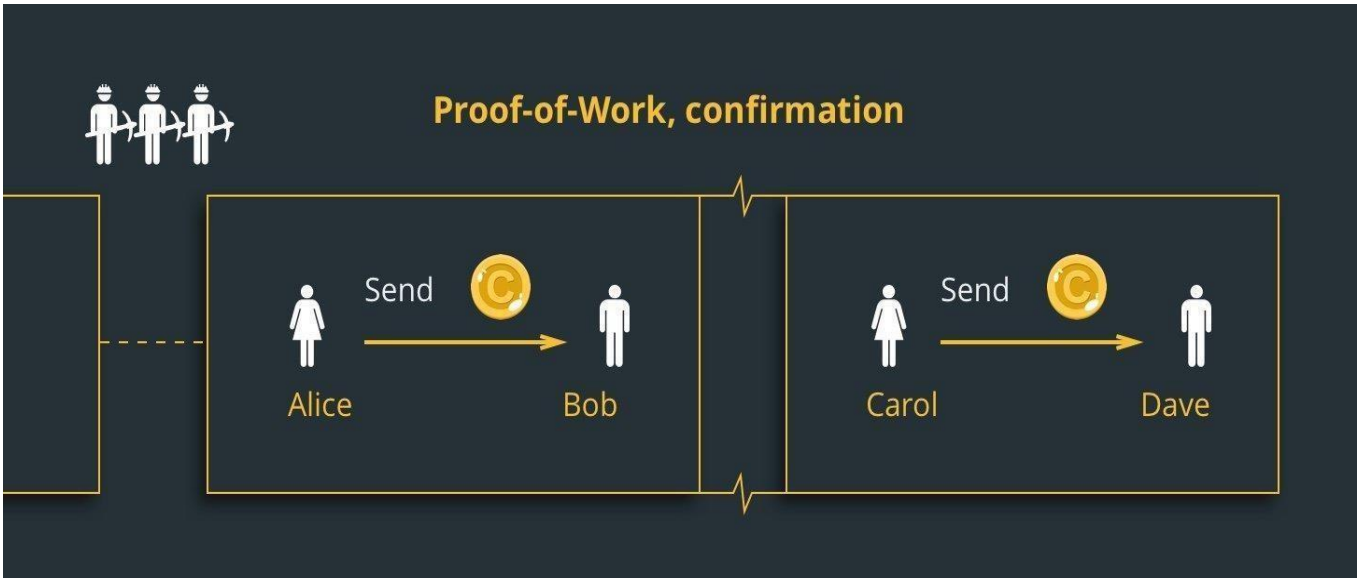

Figure 5. Proof-of-work, confirmation

A mathematical puzzle is a problem that often requires a significant amount of computational power to solve. For example, there are various types of mathematical puzzles:

a. Hash Function Puzzle: This involves finding the input that produces a specific output in a hash function.

b. Summation Puzzle: This puzzle is about interpreting a number as the sum of two other numbers.

c. Guided Tour Protocol Puzzle: In cases where a server suspects a Distributed Denial of Service (DoS) attack, it might require performing a series of hash function calculations in a specific order among nodes. This puzzle relates to finding a sequence of hash function values.

The solution to the Proof of Work (PoW) problem is often referred to as a "hash" or a "mathematical equation." The functionality and speed of a precise blockchain system depend on the PoW, which should strike a balance. If the PoW is too difficult, it can significantly slow down block production, causing transactions to become stuck, and leading to workflow interruptions. If the PoW problem cannot be solved within a reasonable time frame, it may become nearly impossible to generate new blocks. On the other hand, if the PoW is too simple, it can expose the system to vulnerabilities, such as bugs, DoS attacks, and spam.

Ideally, the solution to the PoW problem should strike a balance between being challenging enough to ensure security and not overly burdensome to allow efficient block generation. The solution should also be easily verifiable to maintain transparency within the blockchain. If the PoW requires highly specialized and resource-intensive computations, not all nodes in the network may be able to verify it, which contradicts one of the fundamental principles of blockchain - transparency.

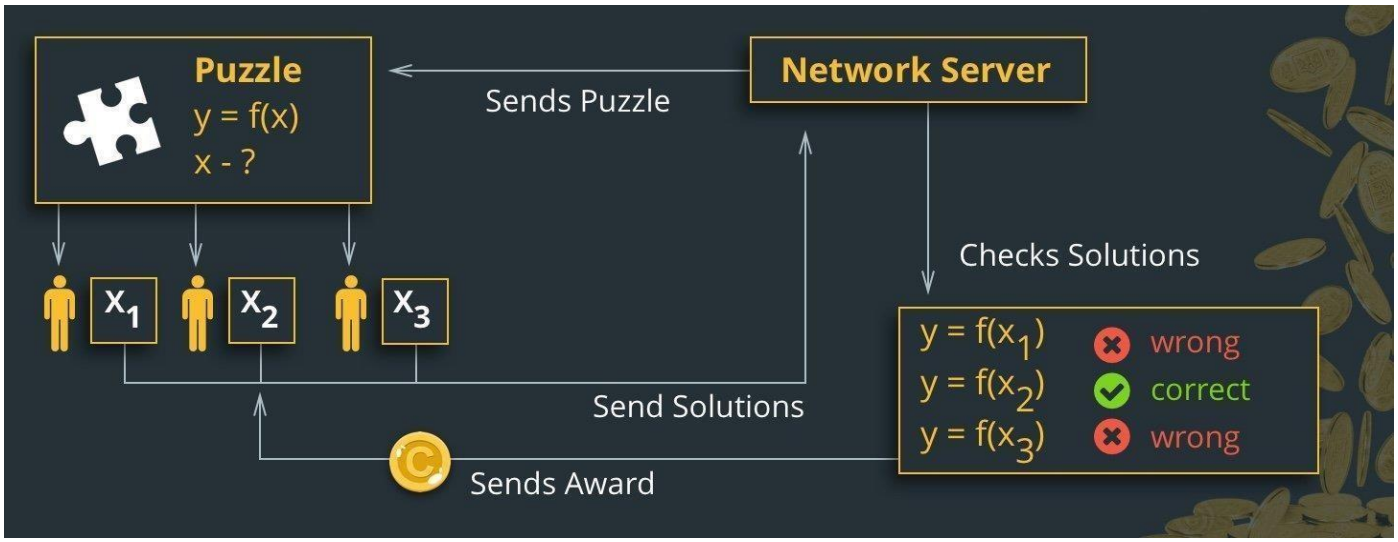

Figure 6. Proof-of-work in blockchain

Miners play a crucial role in the blockchain network by solving puzzles, creating new blocks, and verifying transactions. The complexity of these puzzles depends on factors such as the number of users, the current network capacity, and the network's

transaction fees. Each block's hash includes the hash of the previous block, enhancing security and preventing any tampering with the blockchain. When a miner successfully solves the puzzle, a new block is created, and the transactions within that block are considered verified.

The key advantages of this process include protection against Distributed Denial of Service (DoS) attacks and ensuring that stakeholders with varying amounts of stakes have an equal opportunity to participate in mining.

Regarding DoS security, Proof of Work (PoW) imposes restrictions on network behavior. Attackers would need significant computational resources and time to carry out an effective attack due to the substantial amount of work required. Such an attack is technically feasible but not practical, as the associated costs would be prohibitively high.

In terms of mining prospects, it's not the size of one's financial holdings that matters, but rather the possession of substantial computational resources for solving puzzles and creating new blocks. This means that individuals with significant financial resources do not have exclusive decision-making power over the entire network.

SHA-256 Algorithm:

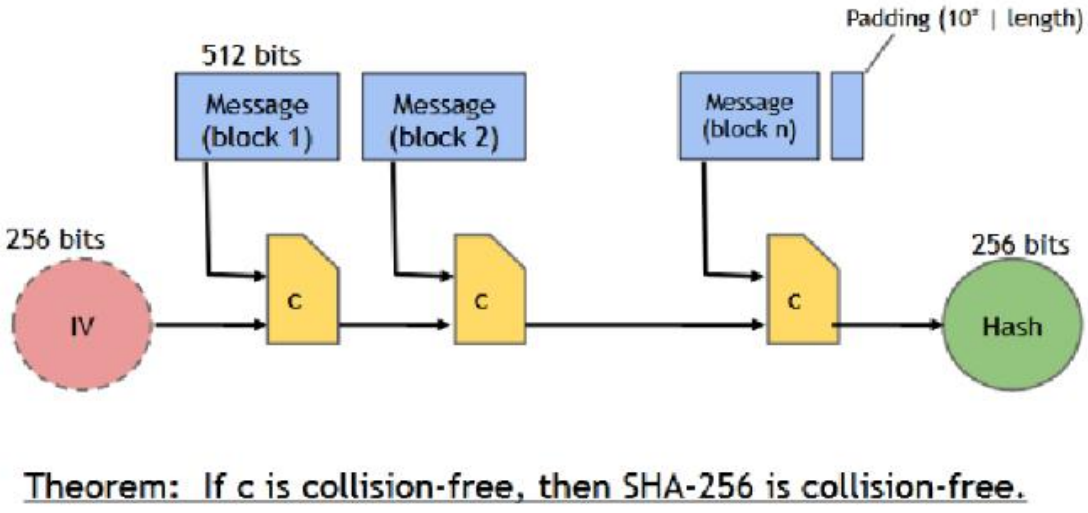

Figure 7. SHA-256 Algorithm

In blockchain technology, the SHA-256 algorithm is employed to consistently produce a 256-bit hash. This algorithm is also integral to computer encryption. SHA-256 is a cryptographic encryption algorithm, representing an enhancement over SHA-1, and it stands as one of the most robust hash functions available. To date, it remains unbroken. It generates a unique 256-bit hash code, often referred to as a signature for text or data files. Data integrity can be verified by comparing the calculated 'hash value' to an expected and known hash value.

In Figure 7, you can observe the algorithm's prototype. It involves an initial 256-bit data set called IV. The resulting feedback is expected to grow significantly. Consequently, the 512-bit data is divided into chunks. Since the input isn't always a perfect multiple of 512 bits, some part of the input remains unprocessed. To address this, left padding is applied to the input by appending 10 * bits to it. This transforms the output into a complete multiple of 512 bits, allowing the process to proceed.

The 512-bit input is then processed to yield a total of 768 bits, including the 256-bit IV. These 768 bits undergo compression via the 'c' compression function to produce a 256-bit output. This 256-bit output is subsequently combined with the 512-bit input from block B2. Once more, the combined data undergoes compression to yield a 256-bit output. This iterative process continues until the final block (block n). Once again, a compression function is initiated, culminating in the ultimate 256-bit output, which is what we refer to as the input hash.

Advanced Encryption Standard (AES):

AES is one of the commonly known algorithms for encryption. AES has its own special, encryption and decryption framework as shown in the Figure 8. AES can handle three different key sizes including AES 128, 192 and 256 bit and each of these ciphers has a block size of 128 bit. The number of rounds is dependent on key length. The key size determines how many rounds AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys.

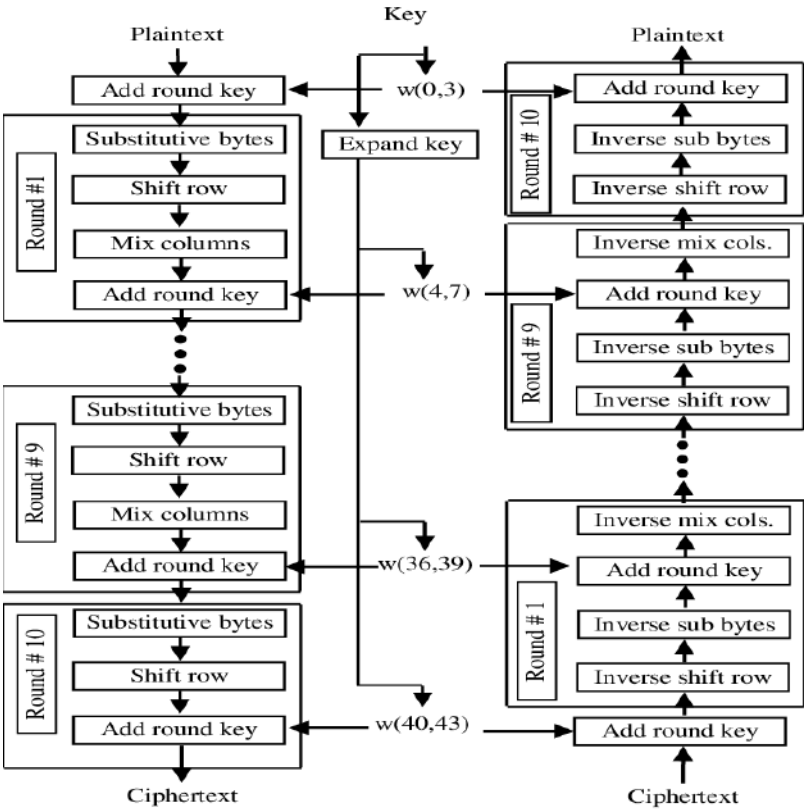

Figure 8. AES Encryption and Decryption

The AES encryption algorithm is more mathematically effective and elegant than the DES encryption algorithm, and exponentially stronger. Blockchain technology definition and encryption algorithm to secure the data file from a server to a client. Firstly, the data in the text file requested is encrypted using the AES encryption algorithm. Second, the encrypted data file is sent to the hash function that implements the hash algorithm SHA 256 and gives a hash code. The encrypted data file is then forwarded to the device. The encrypted file is received on the server side, and the server checks the hash code to verify its authenticity. If the hash code matches then it is known that no intruders or hackers change or access the data file. Upon verification of authentication, the client decrypts the data file using the same key used for encryption.

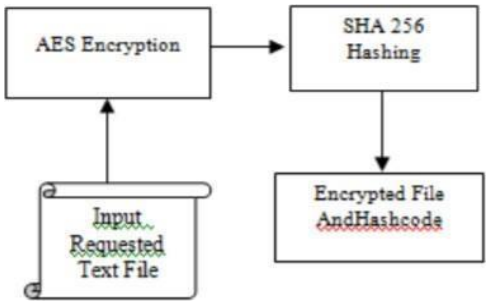

Figure 9. Block diagram of server-side

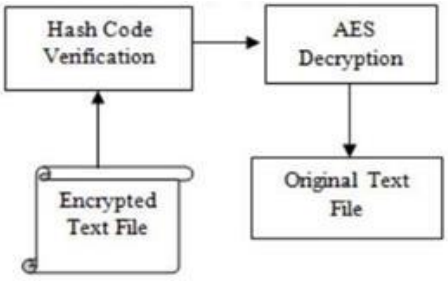

Figure 10. Block diagram of client-side

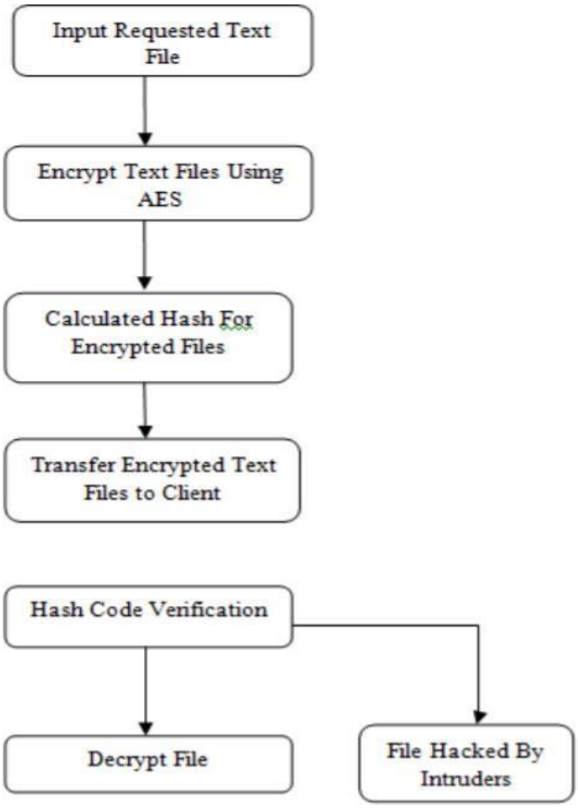

Figure 11. Process Flow

- Client requests to server for a text file.
- For encryption, the requested text files are sent to the server side as input.
- Text files are encrypted using the 'file processor' feature in fileread.java, using AES encryption.
- In StringUtil.java the hash code for the encrypted text file is determined using the function 'applySha256'
- Using Socket, the encrypted text file is sent out to the server client. Step 6: The client receives the encrypted file, and the hash codes are verified.
- The client side hash code is computed and compared with the server side hash codes.
- If the hash codes match, then the file is no problem, the client will decrypt it using the symmetric secret key.
- If the hash codes do not fit then the file will change and the hacker will have modified the original data. The cycle is stopped in this situation.

6. CONCLUSION:

We've introduced a new architecture for blockchain-based Industrial Internet of Things (IIoT) systems, designed to improve transaction efficiency and system security. Our approach employs a credit-based Proof-of-Work (PoW) mechanism to enhance defense against attacks and reduce power consumption for IoT devices. By leveraging the DAG-structured blockchain model, we boost transaction performance through asynchronous consensus. This architecture ensures the integrity of data stored in nodes and maintains data privacy through a robust data authority management method. We've also implemented an access control system using symmetric cryptography for flexible data authority management within a transparent blockchain framework. This architecture is not only suitable for smart factories but can also be applied to various IIoT scenarios. Our future work involves exploring sensor data quality control and addressing storage constraints for handling large data volumes.

REFERENCES :

1. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, “Blockchain for IoT security and privacy: The case study of a smart home,” in Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops, 2017, pp. 618–623
2. Y. Lu and L. D. Xu, “Internet of things (iot) cybersecurity research: A review of current research topics,” IEEE Internet Things J.

3. O. Novo, "Blockchain meets IoT: An architecture for scalable access management in IoT," IEEE Internet Things J., vol. 5, no. 2, pp. 1184– 1195, Apr. 2018.
4. 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 Trans. Ind. Inform., vol. 14, no. 8, Aug. 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 Things J.,
6. Z. Xiong, Y. Zhang, D. Niyato, P. Wang, and Z. Han, "When mobile blockchain meets edge computing," IEEE Commun. Mag., vol. 56, no. 8, pp. 33–39, Aug. 2018.
7. M. Swan, Blockchain: Blueprint for a New Economy. Sebastopol, CA, USA: O'Reilly Media, Inc., 2015.
8. K. Karlsson et al., "Vegvisir: A partition-tolerant blockchain for the internet- of- things," in Proc. IEEE 38th Int. Conf. Distrib. Comput. Syst., 2018,
9. Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in Proc. IEEE Int. Congr. Big Data, 2017, pp. 557–564. [11] S. Popov, "The tangle," Cit. on, p. 131, 2016.
10. R. Bohme, N. Christin, B. Edelman, and T. Moore, "Bitcoin: Economics, ¨ technology, and governance," J. Econ. Perspectives, vol. 29, no. 2, pp. 213– 38, May 2015.
11. Churyumov, "Byteball: A decentralized system for storage and transfer of value," URL https://byteball. org/Byteball. pdf, 2016.
12. X. Wang et al., "Survey on blockchain for internet of things," Comput. Commun., vol. 136, pp. 10–29, 2019.
13. M. Vukolic, "The quest for scalable blockchain fabric: Proof-of-work vs. ´ bft replication," in Open Problems in Network Security. Cham, Switzerland: Springer, 2016, pp. 112–125.
14. 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.