DOI: https://doi.org/10.33103/uot.ijccce.23.3.3

Decentralized IoT System Based on Blockchain and Homomorphic Technologies

Mohanad A. Mohammed[1], Hala B. Abdul Wahab[2]
[1, 2]*Computer Sciences Department, University of Technology, Baghdad, Iraq*
[1]*Mohanad_ali1986@yahoo.com,* [2]*110005@uotechnology.edu.iq*

Abstract*— decentralization within IoT eliminates the need to use distributed networks within IoT to communicate only with servers that may face difficulties related to the internet, vulnerabilities, DDOS, or hijacks, merging blockchain with IoT converted the IoT system into a decentralized with many benefits and outcomes from this conversion. An encryption scheme homomorphic technique (HE) is a method that encrypts the cipher data without the need to decrypt it,paillier encryption method is used. This paper aims to propose a system that integrates Paillier cryptosystem homomorphic technology with IoT and lightweight blockchain technology to provide decentralization to the IoT environment and improve security. The proposed system results in improving the IoT device's work environment by solving the main challenges of security using blockchain, privacy using homomorphism, and data volume using blockchain. The data set used to implement and evaluate the proposed system is industrial internet of things data* The dataset used in this paper is generated via machine industry 4.0 Storage System status which represents the system failure and work status. *this system is evaluated using standard metrics used to evaluate the blockchain effectiveness and time, resources consumed and shows better results in time and power consumption.*

Index Terms*— internet of things, homomorphic, blockchain, IoT decentralization, IioT.*

I. INTRODUCTION

The development of Internet technology was very rapid and as a result of this revolution in internet technology techniques the world is currently within the fourth generation of the industrial decade or which is called industry 4, this led to the conclusion that everything will be connected to the internet world and interacting with the cyber network. Many technologies showed up as a result of the huge impact of the fourth revolution within the industry such as artificial intelligence, 5th generation, cloud computing, big data, cryptocurrency, and blockchain.[1].

The IoT has many advantages and disadvantages related to its main characteristics and disadvantages and needs to be handled very carefully. Since the internet of things network generates data with a huge which may lead to many problems related to privacy and security and since there are no standards related to devices designs it cannot be guaranteed the security of data generated by each device and even applications deals with the data generated by IoT devices need to be fully protected to keep the data privacy of each user within the system.[2].

Difficulties reference to the IoT architecture faces some challenges such as security, privacy, and data volume which can be solved by integrating some technologies such as blockchain and homomorphic encryption where the characteristics of blockchain technology such as transparency, privacy, public verifiability, securiaudibilitylity, and data immutability can be employed to solve the security since it verifies the data sent by all devices and ensure data consistency and data volume by accepting the high amount of data for the scalable blockchain where user can verify and retrieve historically saved data, and homomorphic encryption where data privacy met since no one rather than authorized can reach data and read it.

Received 29/October/2022; Accepted 23/December/2022
 ISSN (Print) 1811-9212 *ISSN (Online) 2617-3352*

DOI: https://doi.org/10.33103/uot.ijccce.23.3.3

II. INTERNET OF THINGS (IoT)

The Internet of Things (IoT) has a huge impact on all human life fields and provides exhilarating services to a lot of industries, including healthcare, smart cities, social media applications, smart homes, and the revolutionary intelligent transportation system (RITS).

Internet of things (IoT) devices defines as small heterogeneous devices will low computations capabilities as well as memory and very limited battery life which are connected via the internet to each other, mainly application of IoT is within the internet of military things, the internet of vehicles, and, internet of drones and so on and since there is no limit to smart things connected within the IoT network general name can contain the IoT main idea which is the internet of everything.[3].

The main architecture of the IoT network connects it to a centralized system and the data transfer between devices using the client-server mode, within this type of system every protection provided to the client and server will not be enough since the centralized server can be hijacked or acting maliciously which may lead to fraud related to the user personal and private data.

And solving this issue requires converting such a system from a centralized environment to a decentralized environment of IoT system this may provide full control to users above their private data. [4].

A decentralized IoT system will ensure that users' private data will not be handled and processed by a centralized server and provide a shared resource that may provide better performance to the IoT devices. This is done by using a schema based on peer-to-peer architecture such as blockchain, which provides decentralized environments and a high level of security. Hence the heterogeneous devices and elements connected within the internet are called the Internet of Things (IoT) which provide a level of intelligence and are connected via IP and can work automatically with no interference or control from humans. [5].

Many available technologies are used to transfer data between IoT networks such as narrow band-IoT, zig bee, and Bluetooth[6], and many artificial intelligence technologies can be used to improve the network activity and effectiveness [7].

A. industrial internet of things (IIoT)

Using of actuators and sensors generated data that connect machines, sensors, and tools for monitoring the process for the manufacturing lines by a specialist as well as engineers which turns the production steps visualized to all, and the maintenance process for reading the internal machines' data a this can be done via employee IIoT technology in many fields usually it is hard for a human to monitor and maintain such as wind power, solar power, supply chain robotics, and construction vehicles. [8].

III. TIMPORTANCEAIN (BC)

Blockchain technology is a decentralized peer-to-peer computing paradigm that is mainly used to provide security and privacy and consider the backbone of the cryptocurrencies such as Bitcoin and Ethereum [9].

The blockchain mainly provides security and privacy within the trustless network, using blockchain within this environment eliminates the need for centralized servers, and trust and verifications are done via the peer nodes within the network.

Mutual databases which are usually referred to as ledgers used within the blockchain are secured using consensus algorithms that verify each peer within the network and prove eligibility to add blocks to the chain via a consensus algorithm such as a proof of work mechanism, the unique distributed ledger shares via the network to all peers nodes and this exact copy of ledger used to provide the anonymity and security of blockchain.[10].

Received 29/October/2022; Accepted 23/December/2022
 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.23.3.3

The popularity of blockchain grew side by side with cryptocurrency which happened quickly and fast and later researchers applied blockchain technology in many fields rather than the financial field such as industry, healthcare, real estate, and so on, blockchain is one of the technologies that is used within the metaverse world security[11].

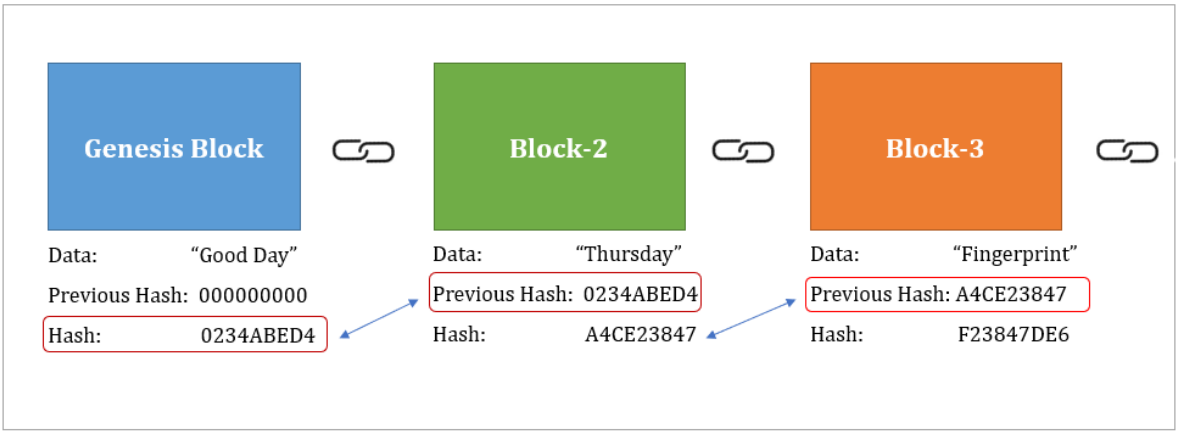

FIG. 1. BLOCKCHAIN HASHING MECHANISM[10].

For every peer node to add to the blockchain the need to win against other nodes that would like to add a block at the same time this is done via algorithm proof of work (PoW) which is a complicated math puzzle that is hard to solve and require many computations to solve which consider the main reason why the blockchain consider resource consuming technology and it is counter known types of attack such as double spending attack, reaching the correct nonce within the blockchain means the node can add the block to the chain and earn a reward (in cryptocurrencies) this is the main method for block verification within the blockchain.[12], *Fig. 1* shows the blockchain hashing mechanism.

Using a consensus algorithm such as PoW guaranteed the prevention of faking and tampering which is required huge computation power to change all hashes within the blockchain and the successor blocks which is considered theoretically impossible.

IV. THE HOMOMORPHIC ENCRYPTION (HE)

Homomorphic Encryption (HE) is an encryption method that can improve and increase privacy and security by solving problems related to them by allowing the third party to operate and perform a specific operation on user-encrypted data without decrypting it this may help to maintain privacy levels of user data.

Mainly homomorphic encryption is applied within the cloud environment where the user data need to be protected and not be revealed from cloud servers for any reason.

Homomorphic encryption has four main operations to be implemented where an additional operation to the encrypted data is provided by 3rd party without decrypting the data itself which helps to maintain user data privacy as shown in *Fig. 2*.[13].

Received 29/October/2022; Accepted 23/December/2022

ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.23.3.3

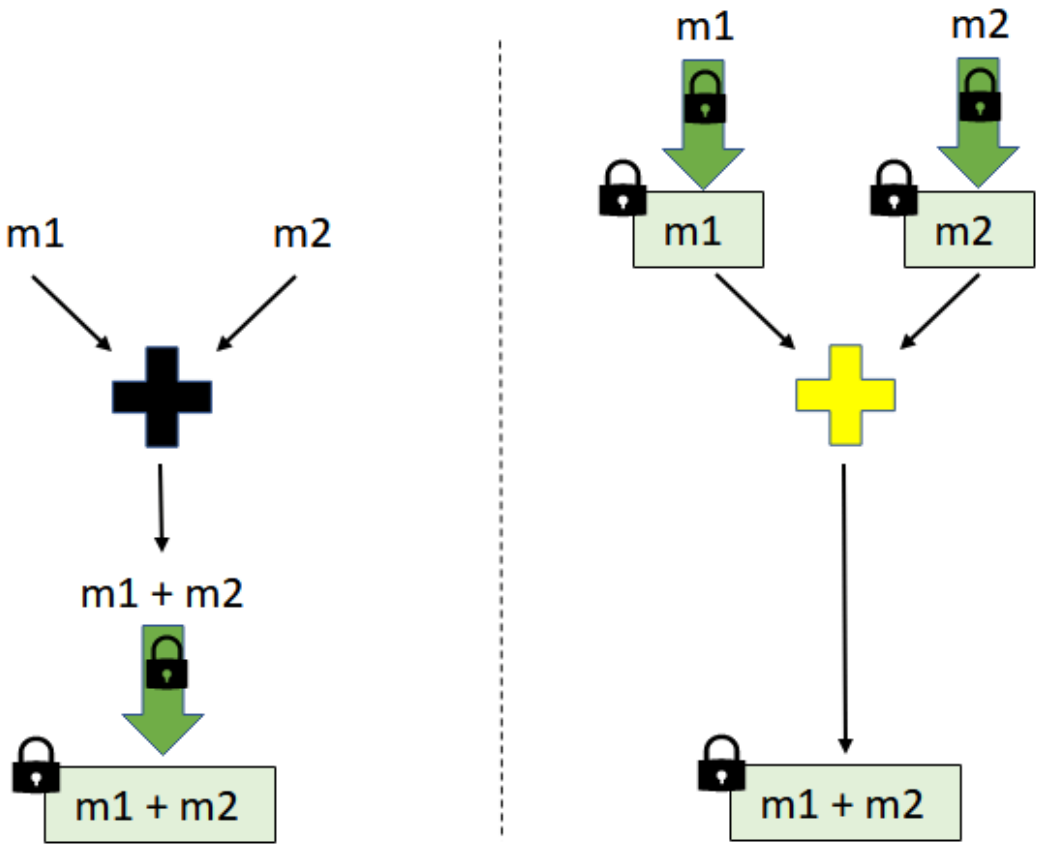

FIG. 2. HOMOMORPHIC ENCRYPTION[13].

Homomorphic encryption is used to secure the data send from the sensors stations to the base station and the centralized server and since no server is used with the decentralized environment of blockchain this data is received from one of the nodes and saved as encrypted data in the blockchain in a distributed ledger can be accessed and retrieved from any node and verified easily.

A proper key distribution method should be used to distribute the keys to all peer-to-peer network node members.

A. Paillier cryptosystem

This partially homomorphic encryption algorithm was presented in 1999 by Paillier which allows the addition operation related to homomorphic characteristics, this algorithm considers more complicated than other homomorphic encryption methods such as ElGamal. [13].

Algorithm 1 shows the steps required to generate public and private key pairs where the user must choose two large numbers p and q which should be relatively prime to each other and calculate n, and then use the least common devisor to find λ, g is randomly selected and u calculated the final keys should be the public key pair is (n,g) and the private key pair is (λ,u).

Algorithm 1 Paillier key generation
Input:p,q
Output: public and private pairs
start
Step1: choose 2 large prime numbers p, q where gcd (P*Q,(P − 1)(Q − 1)) = 1
Step2: find n where n=p*q

Received 29/October/2022; Accepted 23/December/2022

ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.23.3.3

Step3: find λ where λ = lcm(p − 1,q − 1)
Step4: randomly select g as an integer belonging to Z, g∈Z*n2
step5: define L where L(x) = $\frac{x-1}{n}$
step6: find u = (L(gλ mod n2))− 1 mod n
step7: the public key pair is (n,g) and the private key pair is (λ,u)
end

Algorithm 2 represents the step required to encrypt a message using Paillier starting by randomly choosing the r value which should be r∈Z*n2 and the encryption is done via an encryption equation, the encryption is done using the public key generated in algorithm 1 [13].

Algorithm 2 Paillier encryption
Input: plaintext
Output: ciphertext
start
Step1: the select random value of r where r∈Z*n2
Step2: encrypt the message m, using the following equation
c = gm × rn mod n2
end

The cipher text obtained from the encryption process should be c∈Z*n2 and the decryption is done via a decryption equation the decryption is done using the private key generated in algorithm 1 [13].

Algorithm 3 Paillier decryption
Input: ciphertext
Output: plaintext
start
Step1: c cipher text should be c∈Z*n^2
Step2: decrypt the ciphertext c, using the following equation
m = L(cλ mod n2) × u mod n
end

V. RELATED WORK

IoT can be integrated easily with homomorphic and blockchain technology, and the latest research reference to this integration is highlighted below

A. Integration of blockchain in IoT

O. Novo[14] proposes a new scalable scheme that is employed for IoT access control which reduces the time required for data access using blockchain where which eliminated the need for a traditional centralized access management system, using smart contract reduce the number of times required for communications between nodes and some nodes elected as managing nodes to implement and monitor the access policy, the consensus algorithm used within this research is proof of concept.

Y. Rahulamathavan et al.[15] proposed a system that monitors and resolves data preserving and privacy-preserving using Attribute-based Encryption (ABE) within this scheme the IoT data exchanged between IoT devices preserving and privacy-preserving can be controlled and ensures data confidentiality using single encryption and their system eliminates the need for centralized management using multiple management nodes that are distributed using blockchain and this may in total reduce the computation overhead.

O. Alphand, et al [16] proposed an integrated system of blockchain and IoT which they refer to as IoTchain architecture, within this architecture permissioned blockchain was used and end-to-end

Received 29/October/2022; Accepted 23/December/2022
 ISSN (Print) 1811-9212 *ISSN (Online) 2617-3352*

DOI: https://doi.org/10.33103/uot.ijccce.23.3.3

security and privacy service provided the blockchain technology used within this work are built over the top of Ethereum technology, the proposed architecture shown high protection to the data and privacy of the user.

L. Seitz et al. [17]authors proposed an authentication mechanism based on blockchain technology that is employed within the Wireless Sensor Network (WSN) nodes since these devices suffer from a low level of energy, computation, and storage and reference to this constraint authors use a smart contract that builds on the top of Ethereum to hold the transaction within the network and only limited number of trusted nodes has access to the blockchain and authorized for adding a new block to the chain which was employed to provide a type of authentication (decentralized authentication) within the scope of the blockchain technology. However, the authors didn't discuss the problems that are related to the size of the network and the no. of authorized peer nodes where it can be increased rapidly which is generally called scalability.

B. Integration of homomorphic encryption in IoT

J. Song et al.[18] proposed a homomorphic system that can be used to provide security to data generated by vehicles' such as locations and distances and apply privacy preservation within the collected data where data can be analyzed without revealing the original data, retrieving the distances without revealing the real data to a third party and analysis it this may help to provide a type of security against vehicles attackers and provide preservation to the privacy.

W. Jiang et al.[19] proposed a new and novel protocol that is used for authentication called (RAU stands for Randomized Authentication) which may be used to preserve the privacy of sensitive data, which are built using the partial homomorphic encryption algorithm Parlier's scheme which is suitable to work under VANET and MANET environments, the proposed scheme allows the user himself to generate many of authentication identification (IDs) using the concept of zero-knowledge proof (ZKP) this scheme consider lightweight and it is considered usable for small IoT devices that own small and limited resources.

Y. Song, et al[18] proposed a linear homomorphic encryption scheme for controlling drones (drones ground controllers) for their work to be safe and secure as well as autonomous flights, it is secure against outside attacks except when the attacker reveals the secret key ground controller then he/she can control the drone, this system provides logically fast encryption decryption for real-time data which provide mainly security and preserve the privacy.

M. Ali, et al [20] propose a new consensus algorithm for the blockchain environment by using the Shamir secret sharing called proof of secret sharing (PoSS) to solve computations power problem low power devices, this algorithm reduces the time needed for the verification and validation of block and provides consensus for the authorized network node, authors test the algorithm using standard evaluation metrics to improve the effectiveness of the algorithm.

The dataset used in this paper is generated via machine industry 4.0 Storage System –Stats which represents the failure–work status in [21], this data set consists of 20 columns and 19k rows this updated dataset refers to specific sections such as timestamp, voltage machine-generated power and so on, only specific sensitive data in specific field voltage machine manufacturing power which represent the machine ability to accomplish missions were chosen to use and saved in the blockchain and any other field can be chosen reference to user needs and its importance.

Many technologies can be merged with the homomorphic algorithm to reach higher security such

Received 29/October/2022; Accepted 23/December/2022
 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.23.3.3

as using 4G networks [22] and modifying its security by adding PPL algorithms [23] which can be employed in medical images [24] and can be used in a blockchain for different security purposes [25].

VI. PROPOSED IMPROVEMENT TO THE IOT ARCHITECTURE

IoT Centralized servers could be hijacked or data could be tampered with using blockchain. IoT ensures that the result obtained can provide both authentication and verification which ensure that the result is obtained for a verified device and authorized.

The data in the blockchain is saved as plaintext so people can read the data contained within each node connected and have the authorization to access the blockchain data, Data security and privacy are obtained from Homomorphic encryption.

Designing a system that integrates blockchain, the internet of things (IoT), and Homomorphic encryption require splitting this system into two main phases rather than the existing phase of the IoT system as shown in *Fig. 3*:

Phase 1: existing IoT frame:

Every IoT system consists of sensors and getaway to connect IoT devices to the network and data generated from IoT devices, this means when losing the IoT server due to different factors such as natural catastrophes (earth shake, volcano, etc.) or since IoT is vulnerable to modification and loss, an attack such as DDOS All the data will be lost and cannot retrieve easily which may reflect the need to turn centralized IoT system into the decentralized using blockchain.

This phase assumes that the data generated from sensor stations will be encrypted using a paillier homomorphic encryption algorithm the encryption is done in the sensor and sometimes in the base station (management node), further hardware design is needed to decide which data to be encrypted.

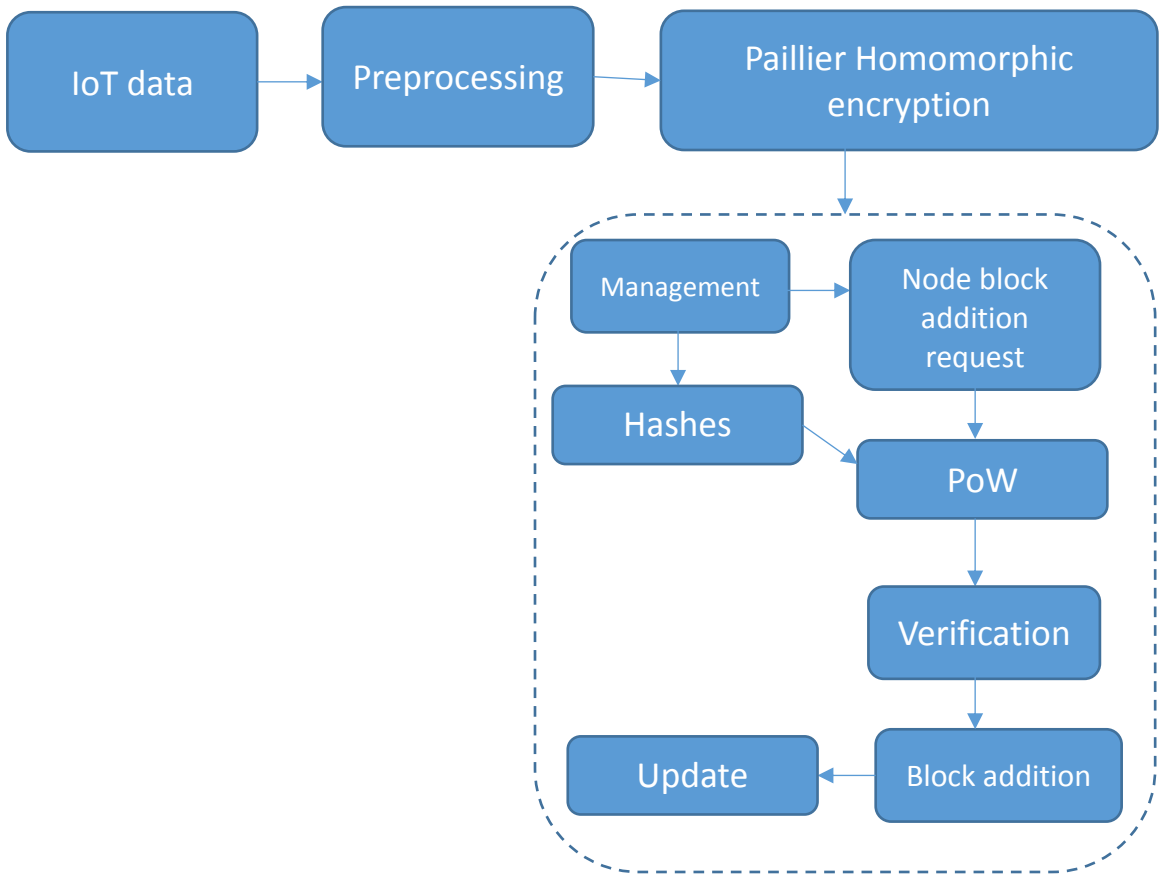

FIG. 3. PROPOSED SYSTEM PHASES.

Received 29/October/2022; Accepted 23/December/2022

ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.23.3.3

Phase2: homomorphic encryption:

Saving data within the blockchain will turn the centralized IoT into decentralized and since this help to improve the security of the system and will ensure the immutability of IoT data using the technology built into the blockchain it is still a problem related to the privacy factor where every authorized user can access and read the content of the blockchain which reflect problem-related to the privacy and may cause problem to the IIoT from the competitive manufactures, in this phase the numerical data only since it represent the most important part and reduces encryption time and computation resources required paillier homomorphic (partially homomorphic encryption method) used to encrypt data, each data within the system encrypted with the secret number and the result will be moved to phase3.

After the generation of the data and preparation for encryption, the data need to be encrypted using the public keys distributed using a proper key distribution method or key distribution center (KDC) and the output of this method will be saved within the blockchain in a distributed manner.

Phase3: blockchain technology:

Devices connected to the IoT networks are known to have low computation capability so they cannot perform complicated or heavy computations, internet of things computations will be performed within the nodes connected to the distributed network of blockchain.

Within this phase, the device which represents the blockchain-added block node is first verified using proof of secret sharing consensus algorithm where the shares of the secret is generated and distributed to the nodes using a key distribution center and each node participating in the verification of the block added to the chain and authentication of the nodes within the peer-to-peer network and if the majority approve the block then authentication is done and the block can be attached to the chain which is represented by distributed ledger this ledger is represented as a distributed text file that have blocks hashes and previous hashes, as well as the encrypted data and time stamp part of the verification process, check the distributed text file if it is identical and if hashes are identical to guarantee no modification is done to this file and if any modification done then the majority file of all nodes is considered correct, Researchers consider the blockchain itself as a secure database to save data in a secure manner with immutability, consistency, and security features many researchers use different types of databases such as oracle, SQL, and text files to save the blockchain ledger within this work text file adopted to reduce the total amount of data required to save the ledger, make the scalability easier, and hold space of huge data generated by the sensor stations. with proper authentication and verification, it can be updated to all nodes within the peer-to-peer network, and another device can operate to add a new block to the chain every block is retrieved easily and needs to decrypt the content of the block to reach the original data.

Since the chain used within this system is a permission blockchain (private) then no need for the nodes to race each other to add a block to the chain and the mining processes are replaced with secret sharing proofing of node identity and this may reduce the computations costs required for mining.

Phase three steps include:

1. Management node: this node represent the base station node and its uses to manage the process of node verification and coordinate with the key distribution center the keys needed by each node, some times this node needs to encrypt data itself using homomorphic encryption. If the sensor station would like to send data to the chain this is done by coordination with the management node using the peer-to-peer network.
2. Node block addition request: for every sensor node needs to add data to the chain a request must be made via the management node to the blockchain nodes to start the proof of secret sharing (modification to the proof of work) verification and authentication and compare the distributed text file used.

Received 29/October/2022; Accepted 23/December/2022
 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.23.3.3

3. Hashes: the standard version of the SHA-256 algorithm used to compute the digest of the block data and previous data and this ensures no one can modify the blockchain content.
4. Proof of work: a modified version of proof of secret sharing is used where each node would like to add data to the chain supplied with a shared secret that is generated from the original security generated by the system administrator and distributed via proper key distribution method.
5. Verification: every node participating in the decision of block validation will be authenticated via re-compute the secret using random N nodes and all selected nodes' text ledger files are checked and evaluated.
6. Block addition: when the data is validated and nodes verified the block is added to the chain with the hash of the previous block and the hash of the current block plus the encrypted data added.
7. Ledger updated: all the updates are sent to all nodes to reach the consistency of ledger files.

All the sensor stations and base stations will have the latest copy of the distributed ledger.

Algorithm 4 summarizes the main steps of the proposed system.

Algorithm 4 proposed a Decentralized IoT system

Input: keys, data

Output: distributed ledger

start

Step 1: Read the IIoT data from the IoT device, sensor station, or base station and send data to the homomorphic algorithm.

Step2: sensitive data is only encrypted using Paillier encryption (algorithm 1,2,3) and the output data can be added to the chain after the verification – authentication done

Step3: verify network peer nodes using proof of secret shares where selected nodes provide their shares to the management node to recompute the secret and if the secret is regenerated correctly then it is verified

Step4: authenticate nodes via used verified nodes to authenticate nodes (by letting the adding block node participate in the secret recomputing) and validate the distributed ledger data

Step5: if all nodes verified and authenticate the adding block nodes PoSS approves the addition of a block to the chain

Step6: add the block to the chain

Step7:update the ledger

end

VII. IMPLEMENTATION

This system can handle any data generated by internet of things devices, and keys with other related information calculated using algorithm 1, and encryption is done concerning algorithm 2, Table I shows the data which is generated from IoT devices and each value represents special coding this data encrypted by paillier homomorphic and the resulting encrypted value added to the chain and hash calculated as well as the nonce (no. related to complexity related to PoW) which is considered the main computation cost for the blockchain and need to be improved to reduce the execution time and complexity) and finally, the average time required to apply this within the blockchain without calculating the time of homomorphic.

The IoT data is turned into secure encrypted data that is saved in the blockchain that ensures data is consistent and immutability.

Received 29/October/2022; Accepted 23/December/2022
 ISSN (Print) 1811-9212 *ISSN (Online) 2617-3352*

DOI: https://doi.org/10.33103/uot.ijccce.23.3.3

TABLE I. PROPOSED SYSTEM IMPLEMENTATION

Data	Paillier Homomorphic data	Data hash	Nonce	Average time
1986	293919090340434416 37177963887	0000022af35078be6575a4b1096243cb93 df4772f48973518aab0936e9086b95	-	-
1561	419589854359730785 13869913344	000001fdb86a249e9ecb38b90a295d11467 efc9411525fa39b6235c78249bdaa	213387	09.17 ms
2022	259744684697273339 67275315012	00000eb70ca4e3901923afdf282f98c0cf71 1f928fa74c0afb590c8ab09e5256	4121	04.03 ms
3022017	208319036323032097 0465280717	000006b369a01c820f38992cef0707bf7b9 74535219156b80c0f815c5462d4e5	423571	04.46 ms

TABLE II. EVALUATION METRICS FOR STANDARD BLOCKCHAIN AND LIGHTWEIGHT BLOCKCHAIN WITH POSS

Evaluation metrics	Lightweight Blockchain with PoSS	Standard blockchain	Distributed ledger type
block size	0.3046875 kilo-byte	0.3046875 kilo-byte	Text file
Average CPU usage	3.8	14.2	Text file
Average Cpu user time	53582.03125	53868.93749999999	Text file
Average Cpu system time	38640.4375	38787.609375	Text file
Average Idle time	1890245.7031249998	1897998.1249999998	Text file
Average Interrupt time	2373.40625	2382.5	Text file
Average RAM %	50.8/100	46.8/100	Text file
Average block creation time	0.0037845999999994717	2.504000399999999	Text file
Average Transaction per second	0.000063	0.04173334	Text file
Average Verification time	1.0013759000000064	5.452229600000003	Text file

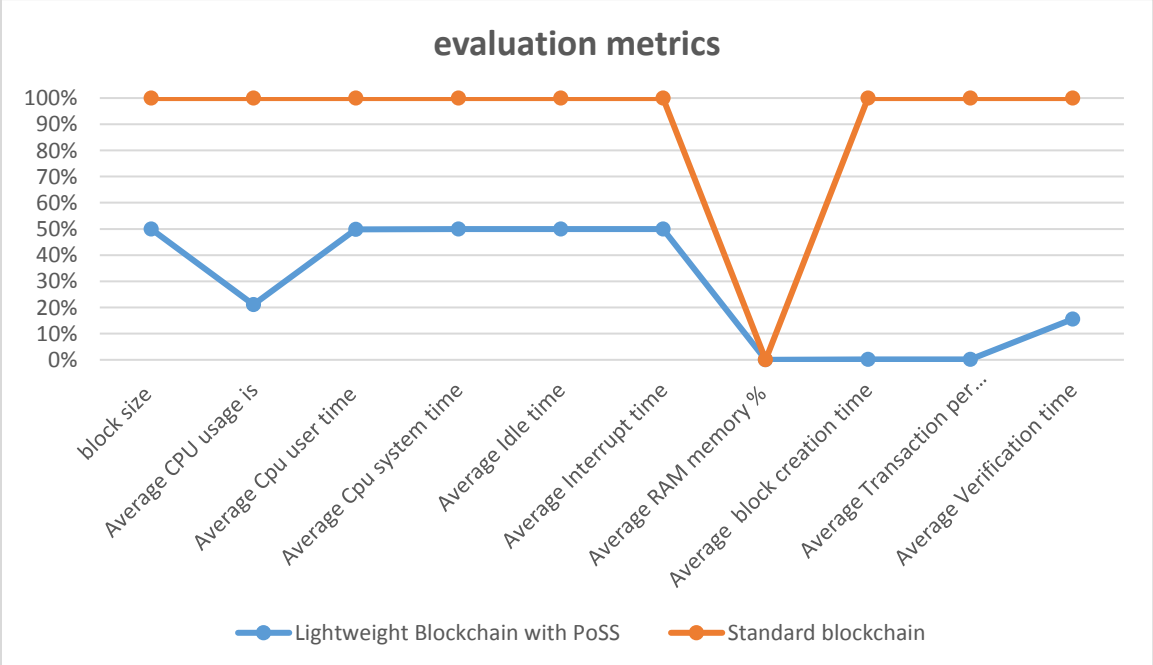

FIG. 4. EVALUATION METRICS FOR STANDARD BLOCKCHAIN AND LIGHTWEIGHT BLOCKCHAIN WITH POSS.

Received 29/October/2022; Accepted 23/December/2022

ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.23.3.3

Table II and *Fig. 4* show the evaluation metrics for standard blockchain and Lightweight Blockchain with PoSS which prove that the Lightweight blockchain needs less time and computation resources and is more suitable to use in an IoT environment.

- block size: represent the memory size needed by the block, it is reduced to the minimum level using a text file for the distributed ledger to reduce the size and retrieve time, lower block size results in lower resources needed to save the blockchain distributed ledger text file used to reduce the secondary storage needed.
- Average CPU usage: the average usage needed for the execution of the addition of data generated by the sensor station to the blockchain, reducing the time needed for implementing the system preferred when using IoT devices, Average CPU usage for Lightweight Blockchain with PoSS is 3.8 whereas 14.2 is for standard blockchain.
- Average Cpu user time: the time that is needed by the user code for the addition of data generated by the sensor station to the blockchain, Average CPU user time for Lightweight Blockchain with PoSS is 53582.03125 whereas 53868.93749999999 is for standard blockchain.
- Average Cpu system time: the time that is needed by the system for the addition of data generated by the sensor station to the blockchain, Average CPU system time for Lightweight Blockchain with PoSS is 38640.4375 whereas 38787.609375 is for standard blockchain.
- Average Idle time: average idle time of the system
- Average Interrupt time: average Interrupt time of the system
- Average RAM: the random access memory needed for the system
- Average block creation time: the time needed for the creation of a block within the blockchain as a part of the system throughput, Average block creation time for Lightweight Blockchain with PoSS is 0.0037845999999994717 whereas 2.504000399999999 is for standard blockchain.
- Average Transaction per second: the time needed for the creation of a block within the blockchain in seconds, Average Transaction per second for Lightweight Blockchain with PoSS is 0.000063 / second whereas 0.04173334 / second is for standard blockchain.
- Average Verification time: the time required to verify a node to add a block to the chain, Average Verification time for Lightweight Blockchain with PoSS is 1.0013759000000064 whereas 5.452229600000003 is for standard blockchain.

VIII. CONCLUSIONS

Integrating the IoT architecture within the blockchain shall turn the centralized system into a decentralized one which helps to face disasters (natural and human-made) by saving the data generated by devices into a distributed ledger and improving the security using the internal characteristics of the blockchain and that's two of main challenges against using the IoT, and secure the data saved within the chain by encrypting them using one of the homomorphic encryption algorithms which allow to mathematical operation on the encrypted data using paillier homomorphic encryption algorithm which provide privacy (which consider one of the main challenges against using the IoT) to the data.

Using Paillier cryptosystem HE to encrypt the data of the IoT device to save this data securely within the server, to obtain the verification and authorization of the data where no one can reach the data directly from the server in case, it is compromised.

Using a standard proof of work consensus algorithm affects the system since such an algorithm is a too heavy reference to the computations cost and other algorithms or modifications to this algorithm shall be used.

Received 29/October/2022; Accepted 23/December/2022
 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.23.3.3

A modified version of proof of work, proof of secret sharing algorithm within the blockchain technology modified to lightweight blockchain and use special file type of distributed ledger and remove the competition between nodes to reduce the time and space needed, to be used within the sensor station of the internet of things, an implementation shows that the modified version of the blockchain reference to time, space and computations costs improve the needs for time and resources and provide security and privacy to the data generated of the IoT device using the homomorphic encryption.

REFERENCES

[1] S. S. Gill et al., "Transformative effects of IoT, Blockchain and Artificial Intelligence on cloud computing: Evolution, vision, trends and open challenges," Internet of Things, vol. 8, pp. 100118, 2019.

[2] J. Li, M. S. Herdem, J. Nathwani, and J. Z. Wen, "Methods and Applications for Artificial Intelligence, Big Data, Internet-of-Things, and Blockchain in Smart Energy Management," Energy and AI, pp. 100208, 2022.

[3] S. Li, L. D. Xu, and S. Zhao, "The internet of things: a survey," Information systems frontiers, vol. 17, no. 2, pp. 243-259, 2015.

[4] A. A. Laghari, K. Wu, R. A. Laghari, M. Ali, and A. A. Khan, "A review and state of art of Internet of Things (IoT)," Archives of Computational Methods in Engineering, pp. 1-19, 2021.

[5] J. Mocnej et al., "Quality-enabled decentralized IoT architecture with efficient resources utilization," Robotics and Computer-Integrated Manufacturing, vol. 67, pp. 102001, 2021.

[6] T. A. Jaber and M. A. Hussein, "Study on known models of NB-IoT Applications in Iraqi environments," in IOP Conference Series: Materials Science and Engineering, 2019, vol. 518, no. 5: IOP Publishing, pp. 052013.

[7] T. A. Jaber, "Artificial intelligence in computer networks," Periodicals of Engineering and Natural Sciences (PEN), vol. 10, no. 1, pp. 309-322, 2022.

[8] S. R. Shakya and S. Jha, "Challenges in Industrial Internet of Things (IIoT)," in Industrial Internet of Things: CRC Press, 2022, pp. 19-39.

[9] M. Javaid, A. Haleem, R. P. Singh, S. Khan, and R. Suman, "Blockchain technology applications for Industry 4.0: A literature-based review," Blockchain: Research and Applications, pp. 100027, 2021.

[10] A. Upadhyay, S. Mukhuty, V. Kumar, and Y. Kazancoglu, "Blockchain technology and the circular economy: Implications for sustainability and social responsibility," Journal of Cleaner Production, vol. 293, pp. 126130, 2021.

[11] T. A. Jaber, "Security Risks of the Metaverse World," International Journal of Interactive Mobile Technologies, vol. 16, no. 13, 2022.

[12] C. Schinckus, "Proof-of-work based blockchain technology and Anthropocene: An undermined situation?," Renewable and Sustainable Energy Reviews, vol. 152, pp. 111682, 2021.

[13] C. Fontaine and F. Galand, "A survey of homomorphic encryption for nonspecialists," EURASIP Journal on Information Security, vol. 2007, pp. 1-10, 2007.

[14] 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, 2018.

[15] Y. Rahulamathavan, R. C.-W. Phan, M. Rajarajan, S. Misra, and A. Kondoz, "Privacy-preserving blockchain based IoT ecosystem using attribute-based encryption," in 2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), 2017: IEEE, pp. 1-6.

[16] O. Alphand et al., "IoTChain: A blockchain security architecture for the Internet of Things," in 2018 IEEE wireless communications and networking conference (WCNC), 2018: IEEE, pp. 1-6.

[17] A. Seitz, D. Henze, D. Miehle, B. Bruegge, J. Nickles, and M. Sauer, "Fog computing aan s enabler for blockchain-based IIoT app marketplaces-A case study," in 2018 Fifth international conference on internet of things: systems, management, and security, 2018: IEEE, pp. 182-188.

[18] W.-T. Song, B. Hu, and X.-F. Zhao, "Privacy protection of IoT based on fully homomorphic encryption," Wireless Communications and Mobile Computing, vol. 2018, 2018.

[19] L. Jiang, L. Chen, T. Giannetsos, B. Luo, K. Liang, and J. Han, "Toward practical privacy-preserving processing over encrypted data in IoT: an assistive healthcare use case," IEEE Internet of Things Journal, vol. 6, no. 6, pp. 10177-10190, 2019.

[20] M. A. Mohammed and H. B. Abdul Wahab, "Proposed New Blockchain Consensus Algorithm," International Journal of Interactive Mobile Technologies (iJIM), vol. 16, no. 20, pp. 162-176, 2022. doi: 10.3991/ijim.v16i20.35549.

[21] H. Hussain, Z. Zeeshan, A. Akhunzada, J. Iqbal, I. Bibi, and A. Gani, "Secure IIoT-enabled industry 4.0," Sustainability, vol. 13, no. 22, pp. 12384, 2021.

[22] R. M. Zaki and H. B. Abdul Wahab, "4G Network Security Algorithms: Overview," International Journal of Interactive Mobile Technologies, vol. 15, no. 16, pp. 109-124, 2021.

Received 29/October/2022; Accepted 23/December/2022
 ISSN (Print) 1811-9212 *ISSN (Online) 2617-3352*

DOI: https://doi.org/10.33103/uot.ijccce.23.3.3

[23] R. M. Zaki, "SNOW3G Modified by using PLL Algorithms in Magic Cube," Iraqi Journal of Computers, Communications, Control and Systems Engineering, vol. 22, no. 3, 2022.

[24] R. M. Zaki and H. B. Abdul Wahab, "A Novel SNOW3G-M Algorithm and Medical," in International Journal of Online & Biomedical Engineering, vol. 18, no. 3, 2022.

[25] R. F. Ghani, A. A. Salman, A. B. Khudhair, and L. Aljobouri, "Blockchain-based student certificate management and system sharing using hyperledger fabric platform," Periodicals of Engineering and Natural Sciences, vol. 10, no. 2, pp. 207-218, 2022.

Received 29/October/2022; Accepted 23/December/2022
 ISSN (Print) 1811-9212 *ISSN (Online) 2617-3352*