Securing IoT Data in the Cloud with Blockchain Technology

Manishankar S
Department of Computer Science,
Amrita School of Arts and Sciences,
Amrita Vishwa Vidyapeetham, Mysuru Campus,
Karnataka, India.
s_manishankar@my.amrita.edu

Dechamma TS
Department of Computer Science,
Amrita School of Arts and Sciences,
Amrita Vishwa Vidyapeetham, Mysuru Campus,
Karnataka, India.
dechammats49@gmail.com

Anoop A
Department of Computer Science,
Amrita School of Arts and Sciences,
Amrita Vishwa Vidyapeetham, Mysuru Campus,
Karnataka, India.
anoop_a@my.amrita.edu

Abstract- **Preserving privacy and integrity is one of the important needs of any internet based platform especially if it is based on cloud. Block chain has been a recent technology key player in securing cloud based platforms. In the proposed work, we have used Blockchain technologies to provide encryption for cloud IoT results. Blockchain has recently become a promising software for cloud cluster integration and enhancement of cloud transaction protection and access to data and application codes. The main objective is to use blockchain technology to encrypt heterogeneous and enormous data. Authorizing the data obtained from different sources. Furthermore, more stable and better hash functions, such as SHA-256, SHA-384, and MD5 are now available, a future attacker would require more time to produce all available SHA512 hashes to brute force a hashed password from your database from a security standpoint. As a result, we consider SHA512 to be more robust and reliable in terms of the time it takes to compute a single hash when opposed to all other hash functions. As a result, we have introduced modified SHA512 in the proposed work for added reliability**

Keywords—Blockchain, Heterogeneous IoT Data, SHA-512.

I. Introduction

Cloud users ask Cloud Service Providers for the services (CSP). CSPs are third parties that provide their customers with cloud storage services. Third-party auditors (TPA) and Attribute Authority (AA) are several other third-party service providers that are expected to have cloud protection functionality [1]. As we are aware, protection and trust are the most important and vital issues that support cloud-based organizations and institutions. Cloud users do not even know who they are communicating with or sharing information with. Transparency is also serious since cloud users do not have any details about their data users and how the data flows inside the cloud. Blockchain is an evolving and novel technology that cloud users can use to improve trust and maximize the efficiency of decentralized blockchain and to provide data protection when outsourcing and obtaining cloud services [2][3]. Compared to centralized database security, Blockchain can provide advanced security. Blockchain keeps track of the documents that are linked to and secured by the previous block that used a cryptographic hash function. A blockchain is a distributed ledger that may be used to track transactions and prevent manipulation. Blockchain is often run via peer-to-peer networks and is designed to prevent arbitrary manipulation. With data storage in the central database, Blockchain may protect at the same level. From management aspects, it is possible to escape data storage losses and attacks. The use of Blockchain has an openness feature when applied to an environment involving data disclosure, It can include data integrity. It can be used and its applications are projected to develop in several areas, including the financial sector and the IoT climate, due to these strengths. Cloud protection and safety issues have since been discussed in terms of major security dimensions. Blockchain-as-a-service (Baas) refers to cloud storage and administration for businesses that build and operate blockchain software by third parties [4]. Baas works like a web host, handling the back-end activities of a blockchain-based app.

Blockchain is a data management system that makes it very difficult, if not impossible, to modify, hack, or scam the system. A blockchain is essentially a decrypted and mirrored digital data processing ledger that is distributed through a computer network [5].

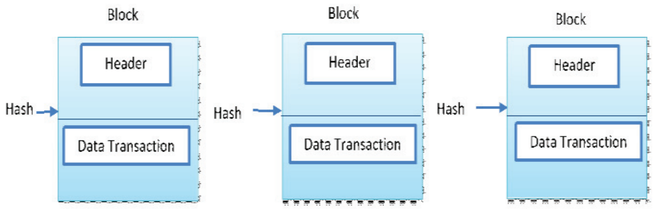

Fig. 1. Data transfer in Blockchain

A hash function is a vector that may be used to translate arbitrary-size data to fixed-size values. Hash numbers, hash codes, digests, or simply hashes are the outputs of a hash algorithm. The values are often used to index a hash table, which is a fixed-size table. Hashing or scatter storage addressing is the use of a hash function to index a hash table. Figure 1 shows that the information is stored in the form of blocks that use hashes to be chained together. "Therefore, it is named as "block-chain".

In this paper, further things included are part B literature survey which explains our view on the papers which we have reviewed, and part C methodology - which explains the methods and tools, and also the system architecture which our proposed system carried out to build a blockchain application. And in part D implementation - we have explained the detailed process or steps of our implementation and also the proposed algorithms that have been used in developing our blockchain application. In part E conclusion, we have concluded our paper, about implementation and methods that are being used. And at the last, in reference we have mentioned all the articles we have reviewed.

2021 Asian Conference on Innovation in Technology (ASIANCON) | 978-1-7281-8402-9/21/$31.00 ©2021 IEEE | DOI: 10.1109/ASIANCON51346.2021.9544613

Authorized licensed use limited to: Dayananda Sagar University. Downloaded on September 24,2024 at 10:58:56 UTC from IEEE Xplore. Restrictions apply.

II. LITERATURE SURVEY

Scholars have conducted an extensive study into the use of blockchain technology to secure heterogeneous IoT data in the cloud:

The works of Rehman, M et al., addressed the nature of Blockchain, its features, and the security standards of Cloud Computing. They concluded that Blockchain could be a viable and effective platform for protecting the Cloud Computing world based on their research.[1]

On the works based on Uchibeke, U. U et al., in heterogeneous VCS networks, proposed a novel security model for key transfer among SMs. Their scheme uses a complex transaction compilation cycle to implement the blockchain principle and maximize efficiency. Under the decentralized SM network, the proposed blockchain framework allows for safe key transfer.[2]

Research done by Lei, et al., proposed a novel continuous restorative record sharing and protection strategy based on disseminated figuring, knowledge grouping, and Blockchain technology. Their emphasis in this project is on developing a stable access management system regulated by a single smart contract to handle customer access and ensure efficient and safe medical data sharing.[3]

A significant amount of research by Muthanna, A et al., proposed a mechanism for IoT devices to provide safe services. They take into account computational innovations like cloud computing and edge transparent computing in their proposed system. The service codes issued by edge servers are also compared and checked using smart contracts.[4]

The works of Chen, Y et al., introduced a concept for health records in a cloud computing environment using a blockchain-based framework. The paper provides an overview of the system, its internal operations, and protocols for dealing with heterogeneous health records.[5]

Research done by Kaur, H et al., proposed a Rural Sustainable Development Using a Smart Rural Governance Platform Based on Blockchain Technology to improve rural governance topic building, unite rural governance consensus, innovate rural governance process, build the rural business, and realize rural governance mode innovation.[6]

In the research conducted by Barenji, A et al., as an upgrade to an IoT-Cloud method, a decentralized architecture for resource control permission and delegation roles is developed. The initiative uses blockchain as a technical foundation for the system, with smart contracts serving as the primary engine for trustless decentralization and autonomous auditing.[7]

Research done by Wang, S et al., using Ethereum blockchain technologies, a new safe cloud computing system with access control has been proposed. Ethereum blockchain technology is used with ciphertext-policy associate encryption in the new method.[8]

The works of Murthy, C. V. B et al., proposed alternatives to the cloud's major problems, including combining it with blockchain technologies. To show their superiority, they typically perform a short survey of previous studies that concentrated on blockchain interacting with the cloud. They have built an architecture that integrates blockchain to the cloud, exposing the connectivity among blockchain and cloud, as part of this survey.[9]

On the research conducted by Yang, C et al., proposed AuthPrivacyChain, a cloud-based access management system with privacy security. The user posts all authorization-related transfers to the blockchain. This paper introduces a system model focused on the EOS blockchain, which considers access authorization and other details to be additional descriptions of blockchain transactions.[10]

In the works of Tapas, N et al., Cybersecurity was proposed as a shared peer-to-peer network for various cloud manufacturing platforms. They would concentrate on the encapsulation of the service into the framework and then on the introduction of the new structure in the future.[11]

The research work of Bojamma, M. A et al., proposed Encryption based on Cipher-text-Policy Attributes for managing access to and protecting encrypted data in the cloud. The approach provides scalable results while reducing the search time.[12]

On the work done by Gupta, A et al. created a data offloading method that assigns user's perspectives to distinct data sets and computation functions to Open Flow switches depending on their current workload. The proposed algorithm is tested in a testbed and also in simulation. The proposed architecture produces good resource consumption efficiency, according to experimental findings.[13]

The research findings of Xia, Q et al., introduced a blockchain-based mechanism for facilitating access to a pool of shared data between users. In comparison to the Bitcoin blockchain network, they built a robust and lightweight blockchain to show the efficacy of our architecture, which allows for safe data exchange whilst protecting data privacy.[14]

The study conducted by Wang, H et al., proposed a bilinear mapping and data integrity checking method based on blockchain. They introduced a new method for verifying data security. They have included provable updating processes in the scheme to cope with the complex nature of IoT results. They proposed a prototype device that would process IoT data using edge computing.[15]

The work done by Li, et al., proposed a behavior auditing system based on a blockchain system that stores file metadata and also user behavior data on the blockchain. The platform performs activities such as file integrity auditing and user activity auditing. They discovered that as the file size becomes larger, the average time spent packing documents into the block steadily reduces.[16]

The work by Wang, H et al., recommended that IoT, Blockchain, and Cloud technology be incorporated into the medical system to provide healthcare and telemedicine medical supplies. It makes for secure tracking of a patient's vital signs in a smart hospital or specific area.[17]

The research conducted by Guo, J et al., proposed a novel way to govern cloud data access using blockchain. Their method distributes the authentication, authorization, even auditing services to nodes in a network, close to bitcoin. They also use the Shamir password exchange system to keep track of the encryption key for cloud users.[18]

The research work of Sindhushree, B et al., proposed an AWS cloud EC2 instance and associated it with a unique

Authorized licensed use limited to: Dayananda Sagar University. Downloaded on September 24,2024 at 10:58:56 UTC from IEEE Xplore. Restrictions apply.

instance-id. EC2 remote workspace has been released and R studio has been installed. Their findings indicate that SVM has the highest time efficiency.[19]

The works of Kaur, H et al., T introduced a concept for health records in a cloud computing system using a blockchain-based framework. The paper provides an overview of the system, its internal operations, and protocols for dealing with heterogeneous health data.[20]

A significant amount of research by Roy, S et al., introduced how to integrate Blockchain into IoT environments to achieve protection and privacy. Blockchain has received much interest since it was first used in bitcoin because of the many software possibilities it offers.[21]

The research conducted by Dorri, et al., proposed a new BC that retains the protection and privacy advantages of the classic BC while eliminating the workload. This employs a layered paradigm that includes a centralized private Immutable Ledger at the regional IoT network layer to save workload and a decentralized public BC on top-end devices for increased confidence.[22]

In the method proposed by A. Anoop et al., A library book recommendation system that facilitates the efficient completion of the library's daily tasks. In this website, the administrator creates a mechanism for storing and retrieving books from a database. In this cloud-based library recommendation system, which employs a distributed filtering algorithm, the admin adds books based on categories and also proposes the top-rated books.[23]

The works of Tselios C et al., gave an overview of typical SDN security problems when connected to IoT clouds, the design concepts of the newly adopted Blockchain paradigm were outlined, and it was stated that Blockchain is now a data privacy driver for SDN and IoT solutions.[24]

The research conducted by Dwivedi A. D et al. proposed a novel hybrid solution that uses private keys, public keys, blockchain, and a variety of other compact cryptographic methods to provide a secure and private patient-centric access control scheme for electronic health data.[25]

The research work of Shafagh, H et al., proposed the basic principle of a distributed protected storage of data aimed only at the IoT. Their process allows for great access control and the processing of information from period detectors from IoT Devices.[26]

On the work by Liu, B et al., for Data Integrity Support, proposed a blockchain-based platform. Without depending on some Third-Party Auditor, a more accurate data integrity check is given by both Data Owners and Data Consumers within such a system (TPA).[27]

The research work of Manzoor, A et al., helped in developing a blockchain-based trading network with a complimentary free ultra-system to protect sensor data delivery to consumers. They also validated the proof-of-work model on a private Ethereum testbed.[28]

The research findings of Zhiqing Huang et al. introduced a secure blockchain-based IoT data management and security scheme. On small IoT computers, edge computing is used to handle data storage and computations.[29]

The research conducted by Huang, Z et al., proposed a decentralized approach for IoT data confidence sharing built on the blockchain. In this article, the underlying concepts of blockchain and associated core innovations within the investigation of three major stable criteria in IoT data exchange highlighted the situation in great detail. [30]

In the research conducted by Rathee, G et al., Blockchain technology has been proposed as a secure healthcare framework. Each activity captured by IoT devices is stored inside the Blockchain to provide secrecy and transparency among the patients, intermediates, and to trace the activity of the intermediates.[31]

A significant amount of research by Murugan, et al., introduced a Blockchain-enabled Healthcare Information Exchange framework that would address issues such as data accuracy and integration. Blockchain integration in HIE would provide access to historical and accurate healthcare data.[32]

The works of Yano, I. H et al., demonstrated how blockchain can be used to store and monitor the knowledge of sugarcane production lots in sugar and alcohol production, only in the mill environment. Since industrial processing is at the center of a sugarcane supply chain, the plan is primarily focused on it.[33]

The work by Maroufi, M et al., assesses most of the key obstacles they experienced in incorporating Blockchain as well as IoT technology and proposes perspectives and elevated ideas that could theoretically fix its limitations and drawbacks from both techniques.[34]

The research findings of Al Breiki et al., introduced blockchain and trustworthy oracles to create a decentralized management system for IoT info. Smart contracts were used in the proposed solution to achieve decentralized access control, allowing people to browse IoT data stored remotely. To provide integration between organizations hosting IoT data or the blockchain network, as gateways, trustworthy oracles were utilized.[35]

The work by Yangang, Z et al., saw blockchain as a storage supply chain that could be checked, accountable, and eternal. Because of these intrinsic features, it may be a viable option for healthcare data networks that are concerned with both patient safety and data sharing. As a result, this research proposes a database scheme and utility system built on the blockchain for saving, exchanging, and using medical data.[36]

The research work of Nisarga, B. L et al., proposed an advanced hybrid hazard prevention framework with a reconnaissance framework, which reduces the large bulk of human communications through the use of IoT technology. Because microcontrollers and low-cost sensors are used, this is a cost-effective option. Future work will be coupled with an analytical system that can predict hazards far ahead of time.[37]

The research work of Fan, L et al., helped in developing a model that offers a private Blockchain platform for distributed IoT applications, which can duplicate system data and verify device transactions using smart contracts. they proposed a model that Smart city strategies using IoT devices and investigated in what way Blockchain technologies can help with IoT data processing.[38]

Authorized licensed use limited to: Dayananda Sagar University. Downloaded on September 24,2024 at 10:58:56 UTC from IEEE Xplore. Restrictions apply.

The research findings of Kumar, R. R et al., introduced blockchain technologies applied in an industrial setting as a defense against security threats that guarantee privacy, availability, and confidentiality.[39]

Research done by andana, R et al., with minimal effort, increased security by using the SHA and RSA algorithms. To authenticate texts, they proposed a tweaked RSA algorithm that generates a pair key and digital signature. They concentrated on ensuring secrecy between the cloud and its customers as well as stopping attackers from accessing it.[40]

III. METHODOLOGY

The study on existing techniques and literature survey gives a clear view that most of the effort has been carried out for securing and improving to encrypt heterogeneous and enormous data. Yet, servers cannot be trusted and privacy concerns still exist. In this section for data confidentiality, we have used Blockchain technologies to provide encryption for cloud IoT data with an improved SHA-512 hashing algorithm because SHA512 is more robust and reliable in terms of the time it takes to compute a single hash when opposed to all other hash functions.

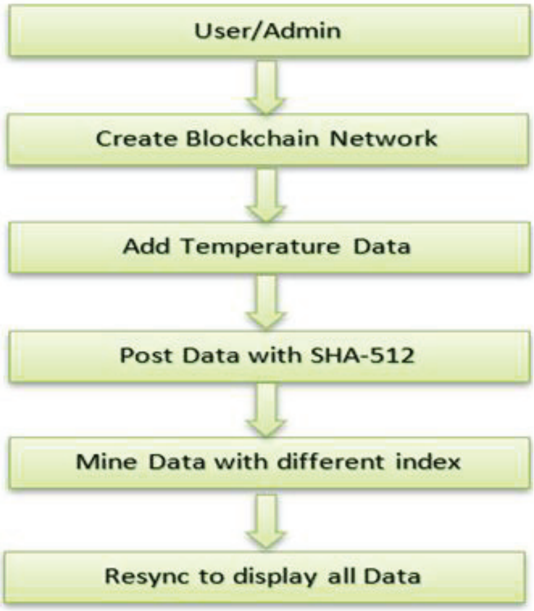
User/Admin
Create Blockchain Network
Add Temperature Data
Post Data with SHA-512
Mine Data with different index
Resync to display all Data

Fig. 2. The architecture of the System

Figure 2 is the built environment of our Blockchain network application where the user or admin first creates the blockchain network and adds or inserts the temperature data which is generated by the IoT device to the blockchain system and posts the data with SHA-512 hashing function where data is converted to a hash value. Later the data is represented as a block and the block is mined with the different index values. We have used Resync to display the history data post with user name and time.

This proposed solution uses blockchain technologies to protect heterogeneous and large data on the cloud. As opposed to storing all data in a single database, blockchain will have better security. Harm from database attacks is avoided in terms of data storage and maintenance. For this reason, the user interface was developed utilizing JavaScript and HTML in a web-based frontend platform.

In terms of encryption, a future attacker would require more time to produce all available SHA512 hashes to brute force a hashed password from the database since the Hash algorithm is more robust and generates random strings to prevent replication of data stored in the database. As a result, compared to all hash functions we can consider SHA512 to be more stable and secure because of the amount of time it takes to compute a specific hash [6]. So, for more stability, we have implemented modified SHA512 in our project. Despite its slower performance, SHA-512 is more trustworthy than MD5 for a variety of reasons. For example, instead of 128 bits, it creates a 160-bit digest, making brute-force attacks a much harder block.SHA-256, like SHA-1, uses a 512-bit stack, while SHA-384 and SHA-512 use 1024-bit blocks.SHA-512 has been implemented because the performance of SHA-512 is 512 bits in length. Collision resistance implies there aren't any, that finding 2 separate inputs to a hash function that produce the same outcome is impossible (hash digest).

To improve the appearance of web pages, we applied Jinja2 templating and CSS, when developing our application's user interface. Until the transaction is connected to the collection of unconfirmed transactions by submitting a POST request to a linked node, our framework collects user details using an HTML type. We have used Python as a programming language because it's simple and straightforward.

A Blockchain protocol works on-demand over the Internet, on such a peer-to-peer network of machines that all execute the protocol and have an identical copy of the transaction ledger, enabling peer-to-peer being that without the need for an intermediary credit to system agreement. The data is connected and encrypted using a cryptographic hash function SHA-512, which is constantly monitored by the blockchain. In the Cloud Computing environment, Blockchain is both an appropriate and strong technology for security purposes. The thing we do this is to add some constraints to Rather than accepting some hash for the stack, we added a limit which should begin with two key ways zeroes in our hash.

We also know that the hash would change if the block's contents are altered. we have added a 'nonce' field to our block. A nonce seems to be a series of numbers that we may change until we find a hash that meets our requirements. The number of significant zeros determines the "difficulty" of our Proof of Work method. We have also observed that our Proof of Work is complex to compute but easy to verify if the nonce is known.

TABLE I. DATASET GENERATED FOR TEMPERATURE SENSOR IOT DEVICE

id	room_id	date	temp	outside/inside
temp.data_ex09we3091	Admin	10-12-2019 09:30	27	inside
temp.data_ex09we3092	Admin	10-12-2019 09:30	27	inside
temp.data_ex09we3093	Admin	10-12-2019 09:27	38	outside
temp.data_ex09we3094	Admin	10-12-2019 09:27	38	outside
temp.data_ex09we3095	Admin	10-12-2019 09:27	38	outside
temp.data_ex09we3096	Admin	10-12-2019 09:27	38	outside

Authorized licensed use limited to: Dayananda Sagar University. Downloaded on September 24,2024 at 10:58:56 UTC from IEEE Xplore. Restrictions apply.

temp.data_ex09we3097	Admin	10-12-2019 09:28	27	inside
temp.data_ex09we3098	Admin	10-12-2019 09:28	27	inside
temp.data_ex09we3099	Admin	10-12-2019 09:26	27	inside
temp.data_ex09we3100	Admin	10-12-2019 09:26	27	inside

The data gathered by the Temperature sensor IoT device which is stored in a cloud store is shown in Table 1.sensor data is an output of an IoT device that detects and responds to some type of input from the physical environment. Heterogeneous data are being considered wherein 97607 datasets are generated. With the combinations harnessed it is stored into an excel sheet and further for data transfer purposes it is extracted from an excel sheet.

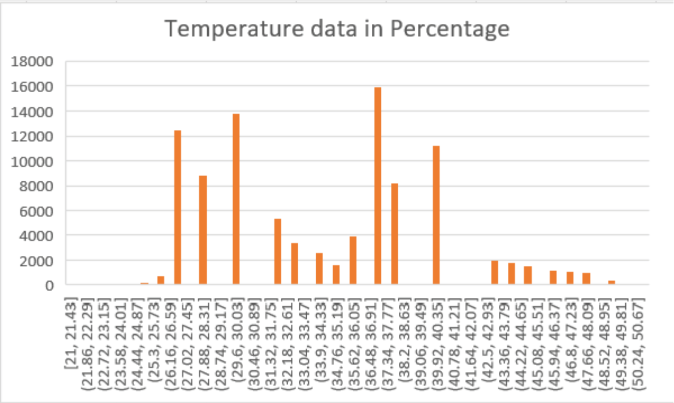

Fig. 3.

In the above Figure, 4 represents the sensor data of the Temperature sensor IOT device in Bar chart format where it consists of temperature data in percentage value.

IV. IMPLEMENTATION

The decentralized application we're trying to create can make things more interesting. We aim to create a blockchain application that allows us to share information or thoughts about it. It is immutable and irreversible, as the content would be stored on the blockchain [7]. A bottom-up strategy is adopted to execute items. This information is added and processed in the blockchain yields some pretty valuable features:

- Context integrity
- Un-hackability of the device
- The data consistency
- No single failure stages

The structure of data in our application will be identified by these things:

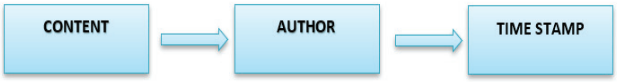

Fig. 4. Figure 3 Structure of Data

1.Content: Some Data that has been transferred to the blockchain system.

2.Author: Name of the author who posts the data.

3.Time Stamp: It displays the time at which the data has been created and transferred.

To prevent ambiguity and to ensure consistency, we will refer to the post data as "transaction" in the post. Transactions are bundled into blocks. So, one or more transactions may be contained in a block. On the blockchain, blocks containing activities are continually produced and preserved. Because there may be numerous blocks, each one has its id. We want the data stored within the block to detect some kind of tampering. A hash function on the blockchain is used to accomplish this.

The hash function is defined as taking some size of data and generating data of a specific size from it, usually to classify the input. We choose SHA512 in our research since it is among the most possibly the best reliable cryptographic hash methods.

Algorithm Steps - SHA-512

1. The input
2. Initialization of the hash buffer
3. Processing of Messages
4. Result

1. The input: SHA-512 is limited in its ability to hash messages for any dimension, i.e., it has a maximum input size. The original message, padding bits, and original message size make up the entirety of the formatted message. And the total size of all of this should be a multiple of 1024 bits.

Padding Bits: Padding bits are added to the input message to make it the required length. The padding bits are ‘0' bits with a leading ‘1'.The algorithm still includes padding, even though it is just with one bit. As a result, only one padding bit will be a ‘1'. The overall size should be 128 bits smaller than a multiple of 1024 bits since the formatted message size is a multiple of 1024 bits. (N x 1024)

msg + pad

Padding Size: The original message's size must be given in 128 bits, and as the largest number that can be measured in 128 bits is (2^{128}-1), the message's size can only be (2^{128}-1) bits; and since the one padding bit is required, the original message's average capacity is (2^{128}-2)

msg + pad +size

2. Initialization of the hash buffer: The methods work by utilizing the output of the preceding block to process each 1024-bit block of the message. It causes a situation for the first 1024-bit block, as it is unable to use the results of subsequent processing. This issue can be fixed by giving the first block a default value, which will start the process. Each intermediate result is always kept for later use since it must be utilized in the processing of the following block.

3. Processing of Messages: A most important part of the data processing step is the Rounds. Each round requires three items: one Word, the previous Round's performance, and an SHA-512 constant. Round one uses the total output of the previous data forwarding round for the previous block with 1024 bits because no previous round's output is available.

Authorized licensed use limited to: Dayananda Sagar University. Downloaded on September 24,2024 at 10:58:56 UTC from IEEE Xplore. Restrictions apply.

4.Result: We receive the final 512-bit Hash value of our plaintext after any block of 1024 bits travels through the request processor stage, i.e. the last iterations for the phases.

Modified SHA512

Plaintext
Modified SHA512
Hash value

Fig. 5. .Structure of SHA 512 Block Diagram

It is similar to SHA512 action and it will take some time but it is more efficient because SHA512 will take 80 rounds of iteration to convert a message, in new SHA512 it will take 80 + iterations like :

Iteration = 80 iterations + num of msg blocks in plaintext

where SHA512 consists of 80 round iterations with several message blocks in plaintext, it means more iterations are possible using this modified SHA512. More of the iterations-more secure and efficient application can be. Here, iterations are done block by block.

A sequence of blocks is required to make up the blockchain. The python list will include all of the blocks. In our current implementation, it's not difficult to create a new block with updated transactions, generate a hash, and merge it with an earlier block. The blocks' immutability and order should be maintained. It will ensure that any changes to previous blocks will invalidate the entire chain. To link the blocks, one method is to utilize the hash. Chaining is the process of using the previous block's hash in the current block. Consequently, If the content of a previous block varies, the hash of that block will also update, causing a discrepancy using the previous hash field of the next block. The "Genesis Block" is the first of the blocks, generated either manually or using a specific logic. The previous hash field has been added to the Block class, and our Blockchain class's initial structure has been introduced.

Proof of Work:

There was a draw: when we change the block header, we can conveniently recompute the hashes of all subsequent blocks, generating a new valid blockchain. To avoid this, we can make calculating the hash complicated and unpredictable. We accomplished this by adding a restriction to the block instead of accepting any hash for it. We added the requirement that our hash begins with two leading zeros. We all know that until the parameters of the block are changed, the hash will remain unchanged. As a result, we'll have a "nonce" zone in our block. A nonce is a number that will be modified before we find a hash that meets our restriction. The "difficulty" of our Proof of Work method is determined by the number of leading zeroes. [6]. It's tough to calculate Proof of Work, but it's easy to prove once we know the nonce. It's just a matter of trial and error at this stage.

Blocks to be added to the chain:

Before adding the block to the chain, we double-checked that the Proof of Work is valid and that the previous hash field of the block to be added points to the hash of the most recent block in our chain. The algorithm for adding the chain's links is as follows:

```
Add a new block ():
        If the previous hash! =block. previous
        Return false
        If not blockchain valid is true:
        Return false
        Block hash=proof
        Append(block)
```

Mining:

The transactions aren't immediately sent to the blockchain. They're saved in a pool of unconfirmed transactions at first. Block mining is the process of placing unconfirmed transactions in a block and computing Proof of Work. We conclude that a block has been mined and applied to the blockchain before the nonce that meets our restrictions has been discovered. Many cryptocurrencies reward miners with cryptocurrency in exchange for using their computer capacity to calculate Proof of Work (including Bitcoin). Our mining function would look like this:

```
Mining ():
        If not self-unconfirmed transaction:
        Return False
        Last block=self-last block
        Proof=new block
        Self-add block (new block)
        Self-unconfirmed transaction= []
        Return true
```

Interacting with the network:

Our node's interfaces will be built for interaction with other peers as well as the application we will be building. To communicate with our node, we used Flask to build a REST-API.

```
App=flask(name)
Blockchain=blockchain ()
```

A postman is a tool used for mining. Postman is a basic GUI for sending and browsing HTTP requests and replies. We don't need to write an HTTP client network code while using Postman for research. Instead, we build collections of tests and let Postman interact with the API. As a consequence, work is more productive and less boring.

Consensus and decentralization:

A consensus algorithm is a way for all peers in a Blockchain network to agree on the status of the public ledger. In a distributed computing environment, consensus algorithms achieve network stability and build trust between unspecified peers in this way. The code we have written so far is designed to run on a single machine. We can't trust a single entity even though we are connecting blocks with hashes. To keep our blockchain running, we will need multiple nodes. So, we have built an endpoint that informs a node about other peers in the network. We also provided a protocol for every node to notify the rest of the network that this has mined a block, allowing us to upgrade our blockchain and move on to mining new transactions. Nodes simply need to verify the proof of work and add it to one's chains. The announced new block method is named after the node that mines each block for peers to attach it to their chains.

Authorized licensed use limited to: Dayananda Sagar University. Downloaded on September 24,2024 at 10:58:56 UTC from IEEE Xplore. Restrictions apply.

V. Result

We proposed a blockchain decentralized application to store and secure heterogeneous IOT data i.e., temperature data generated from IoT sensor devices. To prevent ambiguity and to ensure consistency, Blocks are made up of transactions. On the blockchain, blocks containing transactions are continually produced and preserved. Because there may be numerous blocks, each one has its id. We want the data stored within the block to detect some kind of tampering. This is achieved using an efficient hash function SHA-512 with 80+interactions with several message blockchain plaintexts in the blockchain.

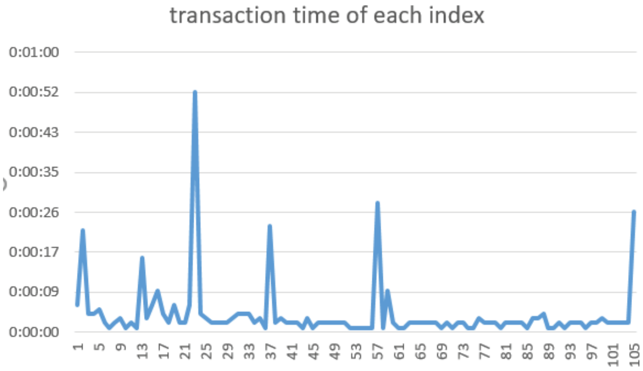

Fig. 6. Transaction Time of each index

In the above, Figure 6 represents the transaction time per second of each index where the x-axis consists of the number of transactions and the y axis consists of each transaction time in seconds. Here in this data transaction, 97607 datasets are carried out. This graph shows that each transaction time is differentiated according to the type and size of data and speed of the transaction. The accuracy of our application is based on the time taken for each transaction. The average time is taken for a transaction is 0.0 4sec.

VI. Conclusion

This paper introduced a blockchain network and secured IoT data on the cloud using Blockchain technology. We have proposed a blockchain decentralized application to store and secure heterogeneous IOT data i.e., temperature data generated from IoT sensor devices with 90607 combinations. More stable and better hash functions, such as SHA-256, SHA-384, and MD5 are now available. A future attacker would require more time to produce all available SHA512 hashes to brute force a hashed password from the database from a security standpoint. As a result, in terms of the time it takes to compute a single hash, SHA512 can be considered more robust and reliable than all other hash functions. So, for more stability, we have implemented improved SHA512 in our project, and it consists of 80+ iterations with several message blocks in plaintext. More number of the iterations-more secure and efficient application it can be. Here, iterations are done block by block. In the future, we have planned to update our blockchain decentralized application with modified cryptographic hashing algorithm and to make it more stable and efficient than the proposed system on cloud.

References

[1] Rehman, M., Javaid, N., Awais, M., Imran, M., & Naseer, N. (2019, December). Cloud-based secure service providing for IoTs using blockchain. In 2019 IEEE Global Communications Conference (GLOBECOM) (pp. 1-7). IEEE.

[2] Uchibeke, U. U., Schneider, K. A., Kassani, S. H., & Deters, R. (2018, July). Blockchain access control Ecosystem for Big Data security. In 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) (pp. 1373-1378). IEEE.

[3] Lei, A., Cruickshank, H., Cao, Y., Asuquo, P., Ogah, C. P. A., & Sun, Z. (2017). Blockchain-based dynamic key management for heterogeneous intelligent transportation systems. IEEE Internet of Things Journal, 4(6), 1832-1843.

[4] Muthanna, A., A Ateya, A., Khakimov, A., Gudkova, I., Abuarqoub, A., Samouylov, K., & Koucheryavy, A. (2019). Secure and reliable IoT networks using fog computing with software-defined networking and blockchain. Journal of Sensor and Actuator Networks, 8(1), 15.

[5] Chen, Y., Ding, S., Xu, Z., Zheng, H., & Yang, S. (2019). Blockchain-based medical records secure storage and medical service framework. Journal of medical systems, 43(1), 1-9.

[6] Kaur, H., Alam, M. A., Jameel, R., Mourya, A. K., & Chang, V. (2018). A proposed solution and future direction for blockchain-based heterogeneous medicare data in the cloud environment. Journal of medical systems, 42(8), 1-11.

[7] Barenji, A. V., Guo, H., Tian, Z., Li, Z., Wang, W. M., & Huang, G. Q. (2019). Blockchain-based cloud manufacturing: Decentralization. arXiv preprint arXiv:1901.10403.

[8] Wang, S., Wang, X., & Zhang, Y. (2019). A secure cloud storage framework with access control based on blockchain. IEEE Access, 7, 112713-112725.

[9] Murthy, C. V. B., Shri, M. L., Kadry, S., & Lim, S. (2020). Blockchain-Based Cloud Computing: Architecture and Research Challenges. IEEE Access, 8, 205190-205205.

[10] Yang, C., Tan, L., Shi, N., Xu, B., Cao, Y., & Yu, K. (2020). AuthPrivacyChain: A blockchain-based access control framework with privacy protection in the cloud. IEEE Access, 8, 70604-70615.

[11] Tapas, N., Merlino, G., & Longo, F. (2018, June). Blockchain-based IoT-cloud authorization and delegation. In 2018 IEEE International Conference on Smart Computing (SMARTCOMP) (pp. 411-416). IEEE.

[12] Bojamma, M. A., & Pushpa, B. R. An approach towards efficient search-based information retrieval over encrypted cloud data.

[13] Gupta, A., Siddiqui, S. T., Alam, S., & Shuaib, M. (2019). Cloud computing security using blockchain. J. Emerging Technol. Innovative Res, 6(6).

[14] Xia, Q., Sifah, E. B., Smahi, A., Amofa, S., & Zhang, X. (2017). BBDS: Blockchain-based data sharing for electronic medical records in cloud environments. Information, 8(2), 44.

[15] Wang, H., & Zhang, J. (2019). Blockchain-based data integrity verification for large-scale IoT data. IEEE Access, 7, 164996-165006.

[16] Li, C., Hu, J., Zhou, K., Wang, Y., & Deng, H. (2018, June). Using blockchain for data auditing in cloud storage. In International Conference on Cloud Computing and Security (pp. 335-345). Springer, Cham.

[17] Wang, H. (2020). IoT-based Clinical Sensor Data Management and Transfer using Blockchain Technology. Journal of ISMAC, 2(03), 154-159.

[18] Guo, J., Yang, W., Lam, K. Y., & Yi, X. (2018, December). Using blockchain to control access to cloud data. In International Conference on Information Security and Cryptology (pp. 274-288). Springer, Cham.

[19] Sindhushree, B., Manishankar, S., & Dhanushya, B. P. (2019). Cloud-Based Healthcare Framework for Criticality Level Analysis. International Journal of Recent Technology and Engineering (IJRT E), ISSN, 2277-3878.

[20] Kaur, H., Alam, M. A., Jameel, R., Mourya, A. K., & Chang, V. (2018). A proposed solution and future direction for blockchain-based heterogeneous medicare data in the cloud environment. Journal of medical systems, 42(8), 1-11.

[21] Roy, S., Ashaduzzaman, M., Hassan, M., & Chowdhury, A. R. (2018, December). Blockchain for IoT security and management: Current prospects, challenges, and future directions. In 2018 5th International Conference on Networking, Systems, and Security (NSysS) (pp. 1-9). IEEE.

Authorized licensed use limited to: Dayananda Sagar University. Downloaded on September 24,2024 at 10:58:56 UTC from IEEE Xplore. Restrictions apply.

[22] Dorri, A., Kanhere, S. S., & Jurdak, R. (2017, April). Towards an optimized blockchain for IoT. In 2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI) (pp. 173-178). IEEE.0

[23] A. Anoop and N. A. Ubale, "Cloud-Based Collaborative Filtering Algorithm for Library Book Recommendation System," 2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT), 2020, pp. 695-703, DOI: 10.1109/ICSSIT48917.2020.9214243.

[24] Tselios, C., Politis, I., & Kotsopoulos, S. (2017, November). Enhancing SDN security for IoT-related deployments through blockchain. In 2017 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN) (pp. 303-308). IEEE.

[25] Dwivedi, A. D., Srivastava, G., Dhar, S., & Singh, R. (2019). A decentralized privacy-preserving healthcare blockchain for IoT. Sensors, 19(2), 326.

[26] Shafagh, H., Burkhalter, L., Hithnawi, A., & Duquennoy, S. (2017, November). Towards blockchain-based auditable storage and sharing of IoT data. In Proceedings of 2017 on Cloud Computing Security Workshop (pp. 45-50).

[27] Liu, B., Yu, X. L., Chen, S., Xu, X., & Zhu, L. (2017, June). Blockchain-based data integrity service framework for IoT data. In 2017 IEEE International Conference on Web Services (ICWS) (pp. 468-475). IEEE.

[28] Manzoor, A., Liyanage, M., Braeke, A., Kanhere, S. S., & Ylianttila, M. (2019, May). Blockchain-based proxy re-encryption scheme for secure IoT data sharing. In 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC) (pp. 99-103). IEEE.

[29] Zhiqing Huang, Xiongye Su, Yanxin Zhang, Changxue Shi, Hanchen Zhang, Luyang Xie- A Decentralized Solution for IoT Data Trusted Exchange Based-on Blockchain, 978-1-5090-6352-9/17/$31.00 ©2017 IEEE.

[30] Huang, Z., Su, X., Zhang, Y., Shi, C., Zhang, H., & Xie, L. (2017, December). A decentralized solution for IoT data trusted exchange based on blockchain. In 2017 3rd IEEE International Conference on Computer and Communications (ICCC) (pp. 1180-1184). IEEE.

[31] Rathee, G., Sharma, A., Saini, H., Kumar, R., & Iqbal, R. (2019). A hybrid framework for multimedia data processing in IoT-healthcare using blockchain technology. Multimedia Tools and Applications, 1-23.

[32] Murugan, A., Chechare, T., Muruganantham, B., & Kumar, S. G. (2020).Healthcare information exchange using blockchain technology. International Journal of Electrical and Computer Engineering, 10(1), 421.

[33] Yano, I. H., CASTRO, A. D., CANÇADO, G. D. A., da SILVA, F. C. (2020). Storing data of sugarcane industry processes using blockchain technology. In Embrapa Informática Agropecuária-Artigo em anais de congresso (ALICE). In: ENCONTRO NACIONAL DE ENGENHARIA DE PRODUÇÃO, 40., 2020, Foz do Iguaçu. Contribuições da engenharia de produção para a gestão de operações energéticas sustentáveis: anais. Rio de Janeiro: ABEPRO, 2020.

[34] Maroufi, M., Abdolee, R., & Tazekand, B. M. (2019). On the convergence of blockchain and the internet…. of things (IoT) technologies. arXiv preprint arXiv:1904.01936.

[35] Al Breiki, H., Al Qassem, L., Salah, K., Rehman, M. H. U., & Svetinovic, D. (2019, November). Decentralized access control for IoT data using blockchain and trusted oracles. In 2019 IEEE International Conference on Industrial Internet (ICII) (pp. 248-257). IEEE.

[36] Yangang, Z., & Zhiyi, D. (2020). Research on the Application of Smart Rural Governance Platform Based on Blockchain Technology in Rural Sustainable Development. *Revista Argentina de Clínica Psicológica*, 29(5), 1339-1349.

[37] Nisarga, B. L., Manishankar, S., Sinha, S., & Shekar, S. (2020, July). Hybrid IoT-based Hazard Detection System for Buildings. In 2020 International Conference on Electronics and Sustainable Communication Systems (ICESC) (pp. 889-895). IEEE.

[38] Fan, L., Gil-Garcia, J. R., Werthmuller, D., Burke, G. B., & Hong, X. (2018, May). Investigating blockchain as a data management tool for IoT devices in smart city initiatives. In Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age (pp. 1-2).

[39] Kumar, R. R., Menon, S., & Nair, N. S. (2020, March). Blockchain Solutions for Security Threats in Smart Industries. In 2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC) (pp. 756-763). IEEE.

[40] Vandana, R., Raj, L. B., & Kumar, B. J. (2020). Information Integrity and Authentication over Cloud Using Cryptographic Techniques. European Journal of Molecular & Clinical Medicine, 7(2), 5227-5235.

Authorized licensed use limited to: Dayananda Sagar University. Downloaded on September 24,2024 at 10:58:56 UTC from IEEE Xplore. Restrictions apply.