ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 8, Issue 3, 2019

An Integrated Blockchain Method for Developing Model for a Secure IoT-Based Systems

U. Harita,

Assistant Professor, Koneru Lakshmaiah Education Foundation, Vaddeswaram Guntur

uharita@gmail.com

Abstract:

Automation technologies have undergone significant change thanks to the Internet of Things (IoT). By adding some sensors or actuators, ordinary objects or things can be transformed into "smart objects." These gadgets can communicate with one another over the internet. User-friendliness is increased in IoT systems through lightweight protocols. But ensuring data security for IoT applications is one of the most important tasks facing any IoT designer. Despite the fact that "things" are networked, there is a significant risk of data manipulation or theft. IoT application scalability, dependability, and data security can all be guaranteed with block chain technology. To ensure data security, we suggest an IoT architecture built on a secure blockchain. Millions of connected components are tracked and coordinated with the help of blockchain technology. Blockchain creates a stable, interoperable, secure system by using a decentralized approach that can prevent single points of failure. Sensor data can be secured using cryptographic algorithms. Thus, our model improves end-user privacy concerns in addition to security.

INTRODUCTION:

In essence, the Internet of Things consists of a collection of physically embedded software-enabled devices that are interconnected. Both a microprocessor and a microcontroller could be part of the physical system. Examples of similar boards are the Raspberry PI, Arduino, and Intel Galileo. Various types of sensors are utilized to gather data in real time. These retrieved data are sent to the central coordinator device, which uses the linked actuators to process the data appropriately and start the appropriate action [2].IoT makes use of both software and hardware. It makes use of a class of software architectural patterns in addition to hardware architectures. For Internet of Things applications, standardized software architectural patterns

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 8, Issue 3, 2019

include Peer-to-Peer, Publish-Subscribe, REST, and Client-server. Heterogeneity and security are the primary factors considered when selecting patterns for various Internet of Things applications [3].

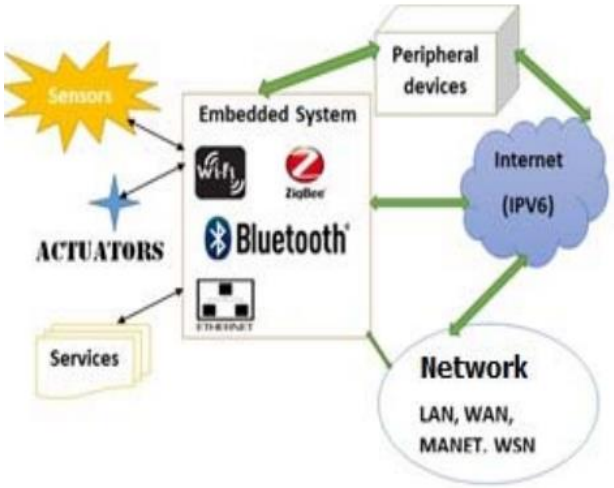

Fig.1 Architecture of Internet of Things [16]

In the digital age, where people prefer to control everything remotely, the Internet of Things is very relevant. Despite the heterogeneous nature of the devices, modeling an IoT system for a specific domain is a monumental task for the designer. Data security and privacy assurance are two major issues with IoT-based systems. Numerous Internet of Things applications, such as weather forecasting, manufacturing, power plants, patient health monitoring, and structure health monitoring (buildings, dams, etc.), deal with extremely sensitive data. Assuring the security and privacy of the gathered data is a dangerous task for IoT developers. Blockchain has a lot to offer in this situation.An intriguing technology that provides a safe way to conduct digital transactions is blockchain. It functions as a "distributed ledger," securely, auditably, effectively, and transparently logging every transaction. This is a novel idea with a wide range of applications and significance in the business world.

All that blockchain is is a distributed database system with an ever-expanding collection of data records. To ensure authenticity, each transaction is digitally validated and signed. The entire chain is not held by a master server. Every computer (node) involved in the transaction has a copy of the transaction chain.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 8, Issue 3, 2019

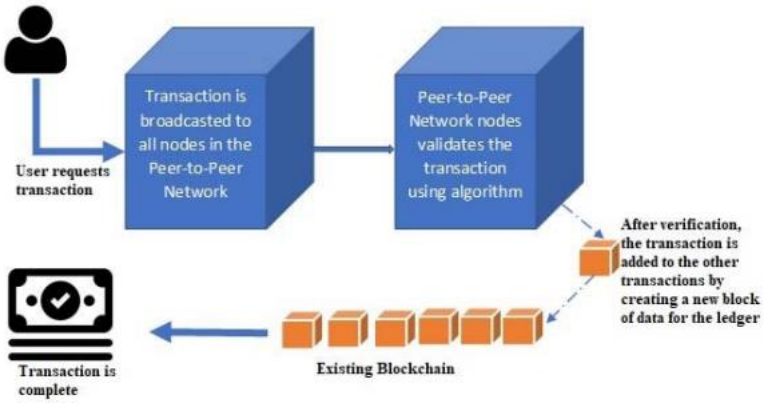

Fig 2. Working of a Block Chain Technology

Working of a Block chain Technology

A blockchain is made up of two components:

• Transactions: All of the activities that members of the distributed system carry out.

• Blocks: This component makes sure that no transaction has been tampered with by recording all of the transactions in a sequential order. Every transaction is time-stamped when and where it is added to the chain, ensuring this.

The majority of the nodes taking part in the blockchain implementation run algorithms to confirm and assess the history of each block chain block that is taken into consideration when a transaction edit request or a new transaction enters the blockchain. The new transaction block is approved into the distributed ledger and a new block is created if the majority of the involved nodes believe the history and digital signature to be legitimate. Reject and discard change or addition requests if the majority of participating nodes do not accept the digital signature as authentic. Blockchain can therefore function as a distributed ledger without the need for a centralized authority to verify the records or transactions thanks to the distributed consensus model. The three main characteristics of blockchain technology are transparency, immutability, and decentralization.

The feature of a block chain called immutability makes sure that once data is added to the system, it cannot be altered. Among the advantages that set blockchain apart from other comparable methods, such as centralized systems and Bitcoin, is this. Blockchain immutability is accomplished through the use of a cryptographic hash function. Blockchain can be compared to a linked list that contains a hash pointer and data. A chain of blocks is created since the hash

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 8, Issue 3, 2019

pointer points to the block before it. Similar to a pointer in a linked list, a hash pointer also stores the hash of the data contained in the previous block that is still in the chain, rather than just the address of the previous block. All that is involved in the blockchain network is a group of interconnected nodes. Peer-to-peer network architecture is used to maintain the blockchain. A single centralized server does not exist in the peer-peer model. Each system that is a part of the network has the same priority. All systems are able to speak with one another. The same system can function in different contexts as both a client and a server. As a result, several dispersed and decentralized servers will exist. Despite the Peer-Peer model employed by the system, there won't be a single point of failure. Blockchain integration with IoT will raise the bar for IoT-based product security.

INTEGRATION OF BLOCK CHAIN AND IoT

The Internet of Things, or IoT, is revolutionizing and effectively streamlining manual processes in order to obtain massive amounts of data gathered from multiple real-time systems. The necessary information is extracted from these collected data after they have been processed appropriately to draw conclusions. Weather forecasting, stock market forecasting, smart farming, patient health monitoring, and other applications use this model. The idea of cloud computing gives Internet of Things systems access to a number of functionalities, including data processing and analysis. There are now new ways to access and share information thanks to this extraordinary IoT development. However, end users lack the confidence to share sensitive information through IoT systems because of their transparency. In most Internet of Things applications, where network participants lack a clear understanding of the shared data via the network, centralized architecture is employed. Users may not know the legitimacy or source of the shared data, and it may appear to be a black box. The next section discusses the need for blockchain in the Internet of Things.

Due to the distributed nature of Internet of Things network, each node could potentially be a point of failure that hackers could take advantage of (distributed denial of service attack, for example). System collapse may result from an integrated class of nodes that have several infected devices operating at the same time.

The existence of a central cloud service provider in an IoT environment is another major worry. Vulnerability could result from any failure of this central node, so it should be fixed.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 8, Issue 3, 2019

Data confidentiality and authentication are two of the most important issues. Inadequate data security in Internet of Things devices can be misused and exploited. Data security is now necessary because of the involvement of contemporary business models, where the system can share or exchange data/resources autonomously. The security of data is vital.

Data integrity is a significant IoT challenge that has some applications in the field of decision support systems (DSS). Timely instructions or decisions can be generated by utilizing the sensor data that has been collected. Therefore, it is essential to defend the system against injection attacks, in which attackers introduce erroneous measurements or values that could materially impair the ability to make accurate decisions.

For application domains where real-time data is continuously monitored, such as manufacturing plants, automated vehicle networks, and smart grids, availability is essential. A single data loss event could lead to the system failing as a whole. It will be advantageous for these kinds of situations to incorporate a security measure that makes the audit trail publicly verifiable.

Since it guarantees both performance and security, the integration of multiple technologies, including Blockchain, IoT, and cloud computing, into a single system has shown to be unmatched [13]. The idea of integrating blockchain technology into Internet of Things systems is revolutionary since it offers dependable and traceable data sharing services [14]. The data is unchangeable while also allowing for the tracking of its source at any point in time.

Reliable data must be shared in order to add new nodes, or participants, to the system and improve services in areas like AI-powered smart cars and smart cities.

As a result, the use of blockchain technology can improve security and reliability for Internet of Things (IoT) based applications. Even though blockchain can help with IoT functionality, there are still a lot of problems and limitations in research that need to be worked out.

PROPOSED MODEL:

We integrate blockchain concepts to propose a secure Internet of Things system. Figure 3 shows an illustration of the suggested model. The four layers of the suggested Secure IoT model are the following: sensor, communication, data processing, and data storage.

A variety of sensors placed in real-time environments make up the sensor layer. Throughout nature, the sensors might be dispersed. Firewall gateways supply the central coordinator module with the data collected by the various sensors. Using TCP/IP connection management

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 8, Issue 3, 2019

policies, the firewall gateway guarantees end-to-end connectivity between the sensors and the central coordinator. In addition to supporting network address translation, firewall gateways negotiate different firewall hops. The Twofish algorithm is then used to encrypt the data that the central coordinator has collected. A block ciphering system with a single key up to 256 bits in length is used by the Twofish algorithm.

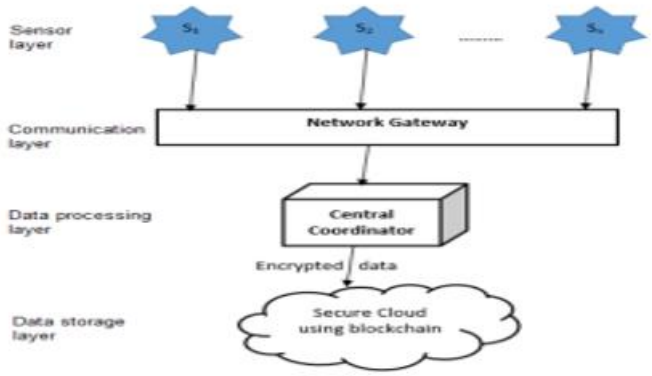

Fig 3. Proposed system Architecture-Diagram

This encryption standard works well and is compatible with Internet of Things devices. Together with its gateway ID, this encrypted data from multiple gateways is kept in the cloud as a blockchain. Because these blocks are shared, users can access them at any time and from any location. Below is a discussion of the transaction chain's new block creation algorithm.

A. Sensor data storage algorithm as a new block

1. As a Transaction (Ti), read the sensor input.
2. Ti is sent out to every node (N1, N2,... n).
3. Each node compiles fresh transactions into a block and runs the block's consensus algorithm.
4. The node broadcasts the block after processing the consensus algorithm, and the processing outcomes are mapped into blocks according to trust value.
5. Only when every transaction in the block is legitimate will Node Ni accept it.
6. A hash function is used to create the following block in the chain if acceptance is successful.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 8, Issue 3, 2019

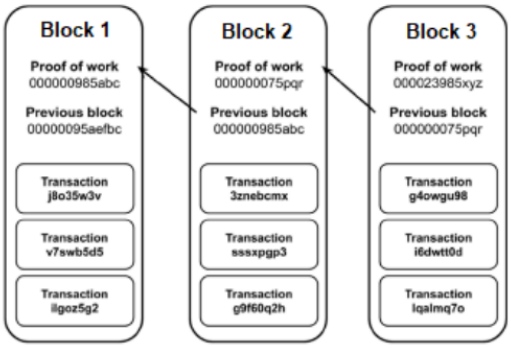

Fig 4. Hierarchy of related blocks

The blocks are connected so that, as seen in Fig. 4, the hash of the parent block is kept in the header field of the child's block. Each updated sensor value is kept in a transactional database. All transactions are stored and hashed correctly. To create the next hash, the hashes of two transactions are fetched and combined. This process is repeated until all of the transactions stored in a block are combined into a single hash. Transaction Merkle root hash is the hashing algorithm employed in this instance [15].

Because of the way the blockchain system is designed, any attempt to modify data will result in an objection. It is impossible to alter data once it has been entered into the distributed ledger as a block on the chain without also altering all blocks that come after it. Our suggested model makes use of this fascinating aspect of blockchain technology to improve data security in Internet of Things systems. Ethereum is a popular decentralized ledger that employs SHA256 for all hashing operations.

By employing the Internet of Things to create a smart farming system, we have verified our suggested model [16]. The lightweight architecture of the smart farming system is why we selected it as our experimental domain. It is made up of different modules, each of which needs security and trust at every stage of data storage. Three modules make up the suggested smart farming system: a central coordinator module, sensors module, and Android app module. The agricultural field is equipped with sensors to detect the necessary parameters. The central coordinator, which is run by an Android application, received the data from the sensors. A cloud database receives this data. When a parameter crosses a threshold limit, the farmer receives an alert from the mobile app that analyzes the cloud data.

Based on the cloud-stored data that the sensors have retrieved, the automated watering procedure is started. The generation of a Transaction (Ti) occurs each time the moisture

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 8, Issue 3, 2019

retrieves the value. Based on the trust value produced by the consensus algorithm, it is hashed. The value is processed by the consensus algorithm and then added as a new block to the cloud. As a result, this system can guarantee the integrity of the data. The Android module processes the information to start the required processes, like watering, after decrypting the stored data. Mobius IoT server platform is used in our system. it can share sensor data between devices and applications and later uploads to the block chain server. Ethereum is used for implementing the smart contract in our system. In this system, the authentication method followed is discussed as follows. The 'sensor id', 'device id' and password are used as the password for blockchain to register in the Mobius server. The Mobius server initiates a request to generate a new account in the block chain with the sender password and receives the account address as the response. All these information (sensor id, device id and account address) is sent to the client application of the database.

Sensor data is saved in the appropriate account address in the server system when the agricultural field is being monitored by the central coordinator device. All of these sensor data are combined by the smart contract, which then uses data analytics to start the required transactions (such as watering or notifying farmers, among other things). Following the block's creation, the central coordinator uses the Mobius server to send a request to the sensor ID to obtain the most recent data. These retrieved data are uploaded to the block using the block chain address and the database's corresponding sensor ID. The Android application shows all of the data that has been gathered.

Our system's blockchain module makes sure that the farmers can trust us. So, IoT applications can be secured using our model.

Conclusion

Nearly every aspect of human life makes use of the Internet of Things (IoT). The necessary data is collected by the sensors and kept in a cloud database. These data are processed by the central coordinator in order to start the required actions. Even though stored data is used to trigger the actuators, it is important to guarantee the accuracy of this data. This stored data can be accessed by any unauthorized person, which could cause the automation process to malfunction. Thus, data manipulation could cause the entire Internet of Things system to fail. We suggested a blockchain integrated secure IoT model as a solution to this. Every time the sensor retrieves data, a transaction is started, the new block is added, and the hash function is

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 8, Issue 3, 2019

estimated using the prior data. and only after the transaction has been verified is the new block added.

As a result, we can prevent data manipulation by restricting unwanted access to IoT data. By using our model in a smart farming system that automatically waters and fertilizes an agricultural field, we have validated it.

The outcomes of our experiments demonstrate that our model can be applied to lightweight IoT models to guarantee data security and reliability.

REFERENCES

[1] V. M. Arshdeep Bahga, Internet of Things: A hands on approach, Universities Press, First edition, 2015.

[2] P. M. Jacob and P. Mani, "A Reference Model for Testing Internet of Things based Applications," Journal of Engineering, Science and Technology (JESTEC, vol. 13, no. 8, pp. 2504-2519, 2018.

[3] P. M. Jacob and P. Mani, "Software Architecture Pattern Selection Model for In ternet of Things based systems," IET Software, vol. 12, no. 5, pp. 390-396, October 2018.

[4] May 2019. [Online]. Available: https://blockgeeks.com/guides/whatis-blockchain-technology/.

[5] P. Jacob, M. Ilyas, J. Jose and Josna, "An Analytical approach on DFD to UML model transformation techniques," in Proceedings - 2016 International Conference on Information Science, ICIS 2016, Kochi, 2016.

[6] M. Singh, A. Singh and S. Kim, "Blockchain: A game changer for securing IoT data," in 2018 IEEE 4th World Forum on Internet of Things (WF-IoT), Singapore, 2018.

[7] Mutijarsa and D. Fakhri, "Secure IoT Communication using Blockchain Technology," in 2018 International Symposium on Electronics and Smart Devices (ISESD), Bandung, 2018.

[8] O. Novo, "Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT," IEEE Internet of Things Journal, vol. 5, no. 2, pp. 1184-1195, April 2018.

[9] P. Lv, L. Wang, H. Zhu, W. Deng and L. Gu, "An IOT-Oriented Privacy-Preserving Publish/Subscribe Model Over Blockchains," IEEE Access, vol. 7, pp. 41309-41314, 2019.

[10] W. Viriyasitavat, L. D. Xu, Z. Bi and A. Sapsomboon, "New Blockchain-Based Architecture for Service Interoperations in Internet of Things," IEEE Transactions on Computational Social Systems, vol. 6, no. 4, pp. 739-748, Aug 2019.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 8, Issue 3, 2019

[11] R. Doku, D. B. Rawat, M. Garuba and L. Njilla, "LightChain: On the Lightweight Blockchain for the Internet-of-Things," in 2019 IEEE International Conference on Smart Computing (SMARTCOMP), Washington, DC, USA, 2019.

[12] J. Pan, J. Wang, A. Hester, I. Alqerm, Y. Liu and Y. Zhao, "EdgeChain: An Edge-IoT Framework and Prototype Based on Blockchain and Smart Contracts," IEEE Internet of Things Journal, vol. 6, no. 3, pp. 4719-4732, June 2019.

[13] Y. Lee, Rathore, P. S. and J. al., "A blockchain-based smart home gateway architecture for preventing data forgery," Hum. Cent. Comput. Inf. Sci., vol. 10, no. 9, 2020.

[14] C. AnaReyna, "On blockchain and its integration with IoT. Challenges and opportunities," Future Generation Computer Systems, vol. 88, pp. 173-190, November 2018.

[15] N. Tapas, F. Longo, G. Merlino and A. Puliafito, "Experimenting with smart contracts for access control and delegation in IoT," Future Generation Computer Systems, vol. 111, pp. 324-338, 2000.