International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 01 | January - 2024 SJIF Rating: 8.176 ISSN: 2582-3930

Implementing Security in IOT Systems Via Blockchain

Dhanush C.C: *Research Scholar, Department of Electronics and Telecommunication, Bangalore Institute of Technology, Bangalore, India.*

Guide : Dr. M Rajeshwari, *Head of Department, Department of Electronics and Telecommunication, Bangalore Institute of Technology, Bangalore, India*

Abstract: With today's day and age rapidly going digital, the emergence of Internet of Things has become prominent and IoT systems are now being applied to almost every field. IoT systems can be seen being applied to fields such as healthcare, agriculture, manufacturing and many more. As IoT systems encompass numerous devices, each of these devices becomes a target for attacks and exploitation; thus, IoT systems have long been associated with issues related to security. Hence, making IoT systems secure and safe is of paramount importance. While Internet of Things has become a technology that is extremely widespread today due to the wide range of advantages it provides including scalability, dependence, and ease of access; the shortcomings and possible loopholes should also be accounted for.

Currently a client/server model or a centralized model of networking in employed in IoT devices.These devices also use a single gateway to transfer data between them and connect through a cloudserver. This model has lots of shortcomings like high cost of centralized cloud maintenance and network equipment and the cost will continue to rise with the increase in the number of devices and the volume of data. Single gateway is not very secure as it allows gaining access to a whole IoT network by compromising a single device.

To tackle the issue of security, we propose the inclusion of blockchain technology. A Blockchainis a distributed ledger where data is stored across various nodes all over the world, this eliminatesthe single point of failure. This project proposes the plethora of benefits that blockchain technologyoffers and aimsto tackle the security aspect of IoT systems.

Keywords: Blockchain, Internet of Things, Security

1 Introduction

The Internet of Things (IoT) is an arrangement of interrelated and internet associated objectsthatare used to gather and transfer the data over a wireless network without any humancontact. Currently Internet of Things (IoT) uses client/server model. The devices use a single gateway to transfer the data between them and then connect them through a cloud server. The model used herehas been utilized over the last decades and is now no longer suitable for theincreasing number ofIoT devices and the volume of data that is being shared. The majorshortcomings are the high cost of centralized cloud maintenance and the networking equipment. This will continue to rise with proliferation of the connected devices. The restriction on data exchange with other centralized infrastructures causes interoperability. The data collected by these devices is very sensitive and therefore a single gateway is not trustworthy, as it allows gaining access to the whole IoT networkby compromising only a single device. There is a dire need of improving security in these devices. IoT devices are so popular that convenience is always prioritized over security.

Most of the consumers know about the issues andyet are willing to sacrifice their security for convenience. One of the examples being Amazon Echo. Although the employees of the company have admitted to listening to users' conversationsfor the purpose of improving the product, this has barely impacted the sales figures of these devices. As the prospect of the devices in the infrastructure growing exponentially, it is becominga big challenge to identify, secure and authenticate the devices. The current centralized security model will be exceedingly difficult and expensive to maintain, scale and manage. It will be an easytarget for

DDoS attack and also introduces a single point of failure.

This type of infrastructure willbe extremely difficult to implement in an industrial setup where the edge nodes are widespread geographically. Blockchain can be used to improve the security issues in IoT devices. A Blockchain is a distributed ledger where data is stored acrossvarious nodes all over the world which eliminates the single point of failure. In blockchain ledger, data is stored on all the variousnodes all over the world which eliminates the single point of failure. Before we add any data to the network, all nodes must approve and verify it. Therefore, no change will be allowed without a common agreement from all of the participants.

This is named as peer-to-peer communication andis used to protect blockchain transactions from attackers. Since there is no single server, there willbe no chance of a man in the middle attack, where

hackers can grab the information sent betweena server and a device. Blockchain is public which makes it accessible to everyone in the network.All the participants can see the common history of all the stored blocks and transactions, but theyneed a private key to see the content. This gives it complete transparency to all the operations andkeeps the data safe at the same time. Therefore, once a piece of information is stored in a blockchain, it willbe impossible to change it.

2 Related works

Benedict Occhiogrosso and Daniel Minoli in their Research paper talks about IoT and its different types of applications. For unpleasant situations we have smart grid, intelligent transportation system, video surveillance-health and they can also be used for business- oriented applications like banking, logistics and insurance. While deploying these internets of things, we provide room for attack which requires attention. This is because the data taken from these devices like managerial surveillance, decision making, and analytics is clearly an area which gives many options for intrusion. The lack of security standard in the industry adopted internet of thing architectures also increases chance of stealing of data. We need a comprehensive support of security in the IoT, so that we can use these applications. Till now many security techniques and approaches have been tried and tested but none of them are upto the mark. We need a solution which follows the CIA triad. Here C stands for confidentiality, which is making sure that the data packets are not examined. 'I' denotes Integrity which is making sure that the data packets received and stored have not been altered. A here stands for availability which is making sure these devices are not prevented from doing their functions properly. Blockchain can play an important role in securing many IoT applications by becoming part of a security. Here a blockchain is a database that will store all the processed transactions, data in a sequential order, which will be tamperproof to adversaries. All these transactions will be then shared by all the users. The information is kept as a public ledger that is impossible to modify. Every user in the system will retain the same ledger as all other users in the network. Blockchain which was just associated with digital currency now has many potentials uses which can help us integrate security in IoT systems. Still blockchains must be combined with other security mechanisms like NTRU cryptosystem, firewalling. The biggest advantage of blockchains is that they will work at the

lower layer of the communications models and application layer.

Mubashir Husain Rehmani and Jinjun Chen in their Research paper talks about how as the internet of things systems are getting more revolutionized, all the objects in our everyday life are getting interconnected. These systems can link and communicate with each other and their surroundings for

performing their tasks. The interconnection between these system requires security, robustness and proper authentication and finally easy maintenance services. To provide all these facilities we will need blockchain. The decentralized nature can resolve many security, authentication issues and maintenance problems we face in our current IoT systems. However, the IoT network is public, transactional details and encrypted keys are visible for everyone in the network. Thus, any problem can leak critical information. For this we need to implement privacy preservation techniques to make blockchain more secure. We need to use blockchain because it has transparent log, secure transaction, no third-party interference, easy backtracking, and digital ledger to keep updated records. To make it more secure, we can use public and private keys to preserve and identity and privacy which will help in encryption. For private contract between nodes, we will only allow programmable contract between concerning nodes containing transactional details. We can also combine and merge transactions to hide original identity. We also need to add data perturbation to make data indistinguishable. These strategies can improve the security of blockchain based IoT systems.

Muhammad Azahar Mushtaq and Abid Sultan in their Review paper talk about how Internet of thing has gained a lot of popularity and is being used in the banking sector, medical centres and even in healthcare. Sadly, these IoT network devices operate on very less computing power, low storage capacity and limited network bandwidth. This makes them more vulnerable than other end point devices such as a smartphone. Moreover, as it becomes more popular the computing infrastructure of these devices is getting complicated. This can give a rise in cyber-attacks. In recent times blockchain has come forward as it has many characteristics to solve different issues which are faced by IoT network devices. Blockchain maintains a distributed database of records. It has proof of all the work done between the network nodes. These transactions are immutable. The nodes will communicate with the blockchain network with combinations of public and private keys. The user will use its own private key to digitally sign all their transactions and then will be able to access the network with their public key. All the transactions are then verified by all the nodes which are in the blockchain network except the node which initiated the transaction. In this process invalid transactions are removed. By using blockchain technology, it makes the device capable of doing everything without third party, therefore making it risk free from a third party. Many IoT issues are solved by blockchain characteristics like data privacy issue can be solved by decartelization, anonymity, and smart contract.

Rahul Agarwal, Pratik Verma, Umang Goel in their Research paper talk about the Internet of things infrastructures like smart cities and smart buildings which are having two major disadvantages which are lack of trust between the entities of the system and that a single point of failure which will be a vulnerability can destroy the whole system. We need blockchain based IoT security solution so that the trust can be established through the decentralized and immutable nature of blockchain. The distributed

nature will make the system more immune to single point of failure. All the user interaction in the IoT will be stored in blockchain as a transaction and the sequence of all the transactions will represent the users trail in IoT. Along with the normal encryption system, every interaction will be mediated with a crypto token which can only be used by authorized user. The generation of these tokens will depend on the user's current state and all the possible actions. The tokens

will not be generated if there is a case of suspicious action. Using prediction models, we will pre generate crypto tokens. This will enhance the security of the system without troubling the user as the tokens will be already pre-generated.

Zhang, Zibin Zheng and Hong-Ning Dai in their survey talk about how internet of things is advancing and creating smart cities with data driven decision applications, these features are resulting in more challenges like decentralization, bad interoperability, and security vulnerabilities. Blockchain technology can help us with these problems. There is a big issue in complexity of networks. This is because there are a huge number of network protocols coexisting in IoT. These include Bluetooth, Sigfox and NFC, all of them offer different network services. As stated, the poor interoperability in both hardware and software to properly make use of information and collaborate with each other. Due to the heterogeneity of IoT systems we face a huge challenge to exchange the data between different sectors. Also, these IoT devices such as sensors, RFID tags and actuators suffer from resource constraints which include battery power, and storage resource. Blockchain can help us with these challenges due to its characteristics. With blockchain, transaction between two peers is validated without the need of authentication therefore reducing the service cost. They also consist of a large, linked chain of blocks where each link is an inverse hash point of the previous block. Therefore, any modification on the previous block disapproves all the consequently generated blocks. During this, root hash of the Merkle tree stores the hash of all the committed transactions. Any change on any of the transactions will generate a new Merkle root. With this any type of security issue can be detected. It will also help in the interoperability issue by storing the IoT data into blockchains.

Eman M, Abou Nassar and Abdullah M Iliyasu in their paper talk about the blockchain based trust models for healthcare IoT systems. One of the applications of IoT is healthcare systems. Here, different devices are synchronized in a way to create an IoT network specially for the healthcare assessment. These systems collect information from different sensing devices and for efficient handling of the heterogeneity, it will require interoperability and trust issues support. This is a key challenge in achieving integration between all the systems. To provide a trustworthy information, we use distributed

service which makes sure that the information stays immutable. All of these requirements get fulfilled by Blockchain. With blockchain, it will ensure data reliability and would permit institutions to share and safely move the data. It will provide a paradigm shift in securing ways we share information. This will help in improving decentralized storage, distributed ledger, authentication, interoperability and to facilitate secure interactions between nodes like patients, healthcare providers and suppliers. Moreover, whenever a new transaction is added to the chain, everyone in the network must validate it. This will happen by applying an algorithm that verifies the transaction but the term "valid" is always defined by the system and differs from other systems. Therefore, to confirm the validity of a transaction is done by majority of the people.

Lei Hang and Do-Hyeun Kim talk about how IoT based technologies are opening new opportunities in various aspect of our lives. With the help of network technology and embedded computing hardware we can make large scale autonomous IoT systems. IoT works in unattended environment and these wireless sensor networks are the most vulnerable. Most of the IoT systems depend on the centralized architecture by connecting to cloud servers. Though this solution helps in computation and data management, it still has security issues. One of the biggest disadvantages is that it has single point of failure which compromises the entire data center. That's why it will be important to implement a secured environment. Using blockchain we get many advantages like transparency, enhanced security, improved traceability, low costing and has no third-party intervention. For proving their proposed concept, they implemented their approach using Raspberry pi and other devices. After evaluation it had a steady level and effective transaction execution. They also compared with other existing designed systems which showed the significance of the new proposed system. Michael P Anderson and John Kolb in their paper talk about the importance of authorization. It is a very crucial security component of many systems. They propose a fully decentralized authorization system which will operate at a global scale providing fine grained permissions, proofs of permission that are efficiently verified by using smart contacts on a blockchain it will be resistant to DoS attacks without relying on a central trusted party. They have presented a mechanism for protecting out of band channels. They implemented their proposed system; WAVE and it has shown positive response and can support city-scale federation with many participants and infrastructures. The final evaluation done shows that WAVE is efficient enough for all the applications.

Dinan Fakhri and Kusprasapta Mutijarsa in their paper talk about the secure IoT communication using the technology of blockchain. As the development of IoT is growing, it is also increasing security problems because of the many violation of the security policies. Blockchain can solve all the security issues of IoT. One of the ways is to make a secure communication between all the devices. To show the importance of Blockchain they created 2 IoT system, one with blockchain and one without blockchain

and compared it. The communication protocol used are MQTT and Ethereum. They have analysed both systems by simulating attacks and observing the outcome. After carrying various test, it was proven by them that the IoT system using blockchain technology was better and was able to solve security problems.

Bandar Alotaibi, in this paper, has surveyed and highlighted recent advancements in security to overcome IoT limitations using blockchain. The author has demonstrated how the blockchain attempts to overcome IoT limitations with regards to Cyber Security. They can be thus divided into 4 types: end-to-end traceability; data privacy and anonymity; identity verification and authentication; and confidentiality, data integrity, and availability (CIA). This paper also explores systematic processes for future purpose. Successful IoT applications and methods (those related to cyber security) are investigated to show how the integration of advanced technologies like blockchain along with IoT can indeed be extremely beneficial. Finally, the potential challenges that might thwart the integration of IoT and blockchain are summarized.

Steve Huckle, Rituparna Bhattacharya, Martin White and Natalia Beloff have discussed regarding importance of internet of things and blockchain technology in shared economy applications. The paper is focused on creating decentralized and shared economy applications via blockchain to secure things. They have introduced an IOT design fiction called ExpressIT taking into various use case scenarios. Moreover, they also have explored regarding the Sussex's Shared things team's research relationship with IOT. With the collaboration of their industrial partner, they are focusing on application scenarios and implementation of Dapps. It also explores how IOT, and distributed ledger technologies can provide great chance to develop distributed applications for the shared economy.

S. Sicari, A. Rizzardi, L.A. Grieco, Coen-PorisiniIn have presented the main research challenges and the existing solutions in the field of IoT security. They also have identified open issues and suggested some solutions for future purpose. The paper analyses and presents the existing approaches which includes confidentiality and access control in IOT, privacy and trust issues, and about policies enforcement in IOT applications. As this paper investigates and highlights many open issues, there is a need to further research the IoT

security field. The research and survey conducted by authors through this paper demonstrated that appropriate solutions must be developed and designed which will therefore provide guarantee regarding the confidentiality, access control and trustworthiness.

Konstantinos Christidis and Michael Devetsikiotis has reviewed the mechanism of blockchain and

smart contracts in IOT. They have demonstrated the detailed view regarding how blockchain network basically works and operates, and how interactions between transacting parties in the network takes place. Authors also have demonstrated regarding the how blockchain-IOT combination can facilitate the sharing of services which could then lead to the creation of marketplace of services between devices. They also have addressed regarding the issues and concerns which an IOT developer might need to keep in consideration while deploying the IOT on the blockchain applications. This will then allow and enable the reader to identify potentially new use cases; and thereby allow them to make well-informed and educated decisions regarding integration of a blockchain in their project. Rodrigo Roman, Jianying Zhou, Javier Lopez in this paper, aim to supply a particular analysis of the features and security challenges of the distributed approach of the IoT, so as to understand what's its place within the Future Internet. There are numerous challenges that has got to be solved, like assuring interoperability, reaching a business model, and managing the authentication and authorization of entities. Still, there are multiple benefits as well. Since intelligence is not targeting a limited set of centralized application platforms – although these platforms also can exist to supply additional support – scalability is improved. Data is managed by the distributed entities; thus, it is possible not only to push/pull data only needed, but also to implement specific privacy policies. Nevertheless, both added trust and fault tolerance mechanisms can be especially devised and implemented here. These and other benefits show that this approach is useful and applicable to the important world. To conclude, the authors discuss the possibility of the coexistence of both centralized and distributed
approaches. This provides the foundations of a full-fledged Internet of Things.

Muhammad Salek Ali, Koustabh Dolui, Fabio Antonelliin in this paper aim to propose a decentralized access model for IoT data. For this, they will use a network architecture that they call a modular consortium architecture for IoT and blockchains. The proposed architecture in this paper enables and allows IoT communications over a software stack of blockchains and peer-to- peer data storage mechanisms. The principal aim here is to have in-built privacy and adaptable for multiple IoT use cases. Further, to account for feasibility and deployment of this proposed architecture, the authors consider two blockchain platforms- Ethereum and Monax; and carry out a performance analysis.

Xueping Liang, Juan Zhao, Sachin Shetty, Danyi Li present the thought of securing drone data collection and communication together with a public blockchain for provisioning data integrity and cloud auditing. The assessment of the framework as proposed by the authors shows that it is/can a secure, reliable, and distributed system for drone data assurance. Further, it is resilient and robust with reasonable overhead which can also support scalability. The drone has the potential to be widely adopted and leveraged in future IoT applications with its capability to sense and deliver in a less limited range of locations. In this paper, they propose a general architecture for drone data collection and control using

blockchain, making it a step closer to such a vision that drone-based applications can collect sensor data and be controlled in a trusted and dependable way while reducing potential attacks and data losses. This system can provide reliability and accountability, as well as data assurance for real-time data collection and drone control. Yu

Zhang, Jiangtao Wen propose an IoT E-business model, which is exclusively designed for the IoT E-business. The authors also redesign many aspects of the traditional E-business

models. Lastly, the authors realize the transaction of smart property and paid data on the IoT with the assistance of P2P trade supported the Blockchain and smart contract. They have proposed a business model for IoT. They start with the introduction of DACs and introduce it into the IoT E- business model. they also discuss details of the IoT E-business model from entity, commodity, and transaction process, in which they study on the 4 stages of the traditional E-business (i.e., they are Pre-transaction preparation stage, Negotiation stage, Contract signing stage and Contract fulfilment stage.) and redivide them according to the feature of IoT E-business model. To achieve the complete decentration of the IoT E-business model, they propose a P2P transaction mode on the IoT based on the Blockchain.

Mandrita Banerjee, JungeeLee, Kim-Kwang, and Raymond Choo make a plethora of observations in this paper. This includes the shortage and lack of publicly available IoT datasets that can be used by individuals or research communities/ organizations. The authors believe that due to the volatile and rather sensitive nature of datasets, it is imperative that a mechanism be devised that allows sharing IoT datasets among the researchers, stakeholders, and all relevant organizations. Thus, the authors explain the potential for blockchain technology and how this can help in in facilitating secure sharing of IoT datasets and securing IoT systems, before presenting two conceptual blockchain-based approaches.

Antonio Vetro, Juan Carlos De Martin in this paper found 18 use cases of blockchain in the literature. Among these, four are exclusively designed for Internet of Things. They also found some use cases that are designed for a private-by-design data management. They also found several issues in the anonymity, integrity, and adaptability. With regards to anonymity, the authors there exist guarantee of only pseudonymity in the blockchain. Regarding adaptability and integrity, they found that the integrity of the blockchain largely depends on the high difficulty of the Proof-of- Work and on the massive number of honest miners, but at an equivalent time a difficult Proof-of- Work limits the adaptability. They documented and categorized the present uses of the blockchain and provided a couple of recommendations for future work to deal with the above-mentioned issues. They conducted a Systematic Literature Review to investigate which are the uses cases of the blockchain in the literature and which factors affect integrity, anonymity, and adaptability of this technology. The goal of our research is to leverage the blockchain and P2P approaches for a private-by design IoT where data produced by devices are not entrusted to centralized companies.

In this paper, Ali Dorri, Salil S. Kanhere, Raja Jurdak and Praveen Gauravaram deliver an outline the various core components and functions of the smart home tier. The authors explain how every single smart home is equipped with a miner. This miner is constantly online and is a high resource device. It is this miner that is responsible for handling all internal and external communication. The miner holds and preserves a private, safe, and secure blockchain. This is used to audit and control all the communication. The authors illustrate the security of this propose Blockchain-based smart-home system by deep analysis of its security. This is done by accounting for the CIA triad-confidentiality, integrity, and availability. Lastly, the authors present results of the simulation to highlight that the overhead that has been introduced by this approach is negligible in comparison to the security and privacy gains.

In this paper, Ana Reyna, Cristian Martín, Jaime Chen, Enrique Soler, Manuel Díaz present challenges of IoT and blockchain and therefore the potential advantages of their combined use are going to be analysed. Disruptive applications during this area are getting to be highlighted additionally to a review of the available blockchain platforms to affect these challenges. the most contributions of the paper survey on blockchain technology, analysing its unique features and open challenges, Identification, and analysis of the varied ways of

Implementing security in iot systems via blockchain *9*

integrating IoT and blockchain, study of challenges, potential benefits, and open problems with the mixing of blockchain and IoT, study of existing blockchain–IoT platforms and applications, Evaluation, and comparison of the performance of various blockchains in an IoT device. This paper investigates this relationship, challenges that are present in blockchain IoT applications, and lastly, sheds light on how the real- time application of blockchain in IoT systems can in fact be incredibly beneficial.

In this paper, Tiago M. Fernández-Caramés and Paula Fraga-Lamas are objectifying a meticulous review on how to adapt blockchain to the specific needs of IoT to develop Blockchain- based IoT (BIoT) applications. After objectifying the basics of blockchain, the most relevant BIoT applications are described with the objective of emphasising how blockchain can knock traditional cloud- centred IoT applications. Further, the current challenges present followed by the possible optimisations are discussed with regards to multiple factors that include effect on design, development, and deployment of a BIoT application. Finally, some recommendations are specified with the aim of guiding future BIoT researchers and developers on some of the issues that will have to be tackled before deploying the next generation of BIoT applications.

In this paper, Nir Kshetri, Rick Kuhn and Tim Weil express their idea of if and how Blockchain strengthen the Internet of Things. First, they discuss what Blockchain is and how it functions. Nir Kshetri

tells that blockchain which is a kind of ledger tech which has been stated in the popular press as one of the next big things. He answers different kinds of questions in this paper such as why Blockchain and how it can help in improving Internet of Things. Later in the paper he tells different ways to incorporate blockchain in Internet of Things security. The paper further shows a tabular representation of the challenges faced in Internet of things their explanation and certain potential blockchain solutions as remedies to these challenges. He tells that blockchain based identity and access management systems can be leveraged such as to strengthen the Internet of Things. This paper concludes with statements supporting promising future for Blockchain in strengthening Internet of Things in the coming time.

In this paper, Madhusudan Singh, Abhiraj Singh and Shiho Kim first a summary of the blockchain technology and its implementation has been explained. Then we have discussed the infrastructure of IoT which is predicated on Blockchain network and eventually a model has been provided for the safety of internet of things using blockchain. The purpose of this research paper is to supply guidance for the utilization of blockchain technology, through cases to form a safer and trustable IoT model. It has the power to revolutionize and optimize the worldwide infrastructure of the technologies connected with one another through internet. It consists of majorly two fields which are influenced by it. This is done through the creation of a decentralized system and this entirely eliminates the involvement of central servers and facilitates peer-to-peer communication and interaction. It can create a totally transparent and hospitable all database, which could bring transparency to the governance and elections. Blockchain technology consists of 4 major pillars. The first among these is Consensus, which provides the proof of work (PoW) mechanism and verifies the action within the networks. The second is Ledger, which provides the entire details of transaction within networks. Third, Cryptography, it makes sure that each one data in ledger and networks gets encrypted and only authorized user can decrypt the knowledge and fourth is sensible contract, which in the verification and validation of the participants of the network.

In this paper, Arshdeep Bahga, Vijay K. Madisetti propose a decentralized, peer-to-peer platform called BPIIoT for Industrial IoT; this is based on Blockchain which is popularly known as the technology that powers Bitcoin. This platform will play a major role as a key-

enabler for a wide range of tasks. These include cloud-based manufacturing, enhancement of the functionality of existing CBM platforms. While Cloud-Based Manufacturing allows on-demand access to manufacturing resources, a trusted and reliable “middle-man” or entity in the middle is needed. This enables transactions between users who want to make use of manufacturing services. Therefore, with the inclusion of this advanced technology blockchain technology, the BPIIoT provides a decentralized network which facilitates peer-to-peer communication.

3 Methodology

3.1 Methodology Description

Present day IoT systems are cloud-based infrastructures are not completely secure. The following section illustrates a plausible scenario that can occur in an IoT system which can thereby compromise the security of the system.

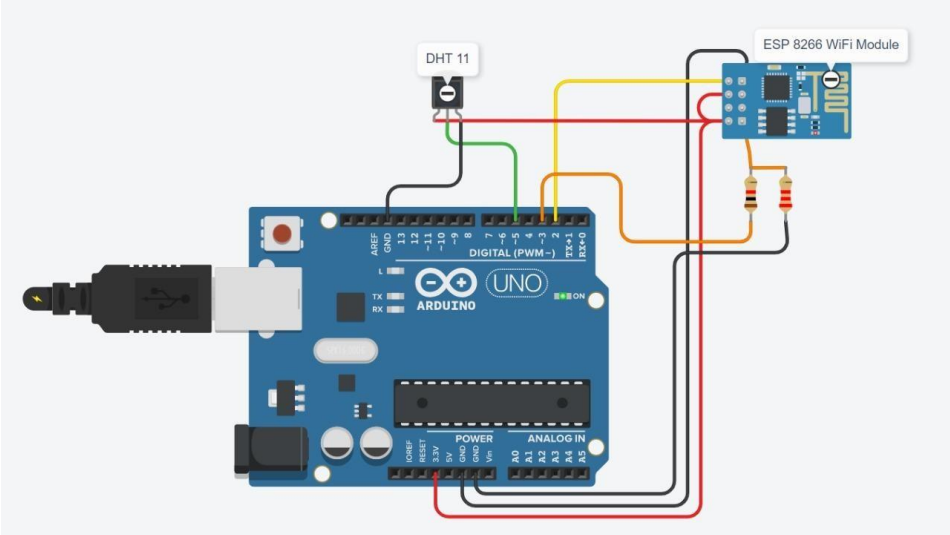

Figure. 3.1.1 IoT set-up for weather monitoring system

In developing the project, we are using ARDUINO UNO which is the heart of the project as shown in Fig3.1.1. There are various other sensors and devices which are interfaced to Arduino UNO which includes ESP 8266 WiFi module and DHT 11. Arduino is an open- source electronics platform based on easy-to-use hardware and software which able to read inputs - light on a sensor, a finger on a button and turn it into an output. The DHT11 is a basic, ultra-low-cost digital temperature and humidity sensor. The ESP8266 WiFi Module is a self-contained SOC with integrated TCP/IP protocol stack that can give any microcontroller access to your WiFi network. ESP 8266 and DTH 11 is calibrated to the Arduino. DTH11 being as an input sensor is used to read the temperature of the surrounding and ESP 8266 is used to connect to the internet. Once entire connection is made DTH reads the temperature of the surrounding and sends it to the Arduino. The Arduino sends the temperature value to the cloud using WiFi module ESP 8266 as it is used to connect to the internet.

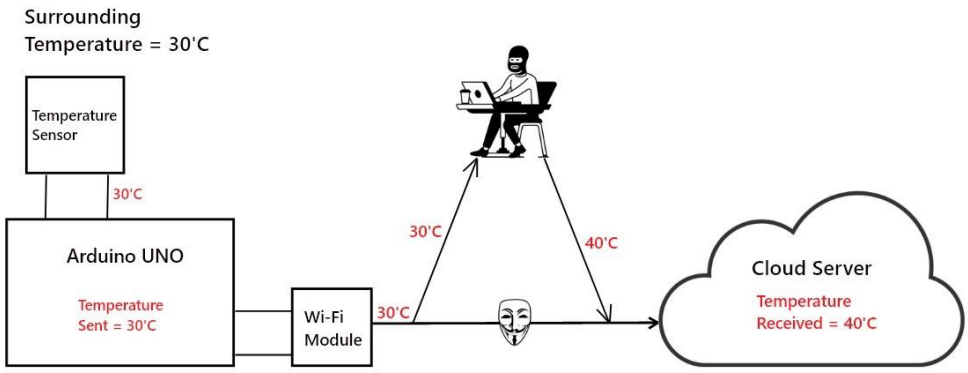

Figure 3.1.2 Attack scenario in IoT infrastructure

Fig. 3.1.2 depicts that if any attack such as man-in-the-middle attack takes place then the temperature that was read by the DTH 11 and was send to Arduino will be intercepted by an attacker causing itself to interject in the process and manipulating the data being sent from the Arduino to the cloud via WiFi Module. For example, as shown above DTH 11 reads temperature as 30 degree Celsius from the surrounding and sends it to the Arduino. Arduino passes the temperature value as 30 to the cloud via WiFi Module. However, if the attack takes place in between then it manipulates the data and sends the false data as 40 degree Celsius to the cloud. This is how the attack can take place while passing over the data to the cloud. We propose a functional blockchain that is coded using C++ programming language. This model blockchain as proposed by us demonstrates the processes with regards to security nodes in a blockchain network. In this implementation of a blockchain, we include objects that are IoT components like sensors. The blockchain tests the possibility of data tampering dur to an attacker and the same is explained further in section

3.2 Algorithms used

Blockchain technology works on hashing as opposed to encryption. Due to this, it is extremely difficult to break, and the hashing algorithm used is SHA256.

3.2.1 SHA256 Hashing Algorithm

Blockchains use the SHA-256 hashing algorithm as their hash function. A cryptographic hash is a 'signature' type of text or data file. The SHA-256 hashing produces a signature that differs from the 256-

bit (32-byte) text provided. The hash is not 'encrypted' - it cannot be encrypted back to the original text (it is a cryptographic function of 'one-way', and it is the default size of any source text size).

This makes it appropriate to compare 'quick' versions of texts, as opposed to encrypting text to get the original version. Such applications include hash tables, integrity verification, challenge handshake challenge, digital signatures, etc.

- A 'handshake challenge' (or a 'hash proof authentication challenge') avoid transferring lost passwords 'clearly' a client can send a hash password online to be verified by the server without the risk of the original password being intercepted.
- The anti-tamper link message hash is real, and the recipient can reply to the message and compare it with the given hash: if it is the same, the message has not been changed; this can be used to ensure that there is no data loss in the transfer
- Digital signatures are very involved, but in reality, you can sign the document hash by encrypting it with your private key, producing a digital document signature.

Anyone else can check if you have verified the text by removing the encryption with your public key to get the actual hash again, and then compare it with their text hash.

SHA-256 is one of the following hash functions in SHA-1 (collectively called SHA-2) and is one of the most powerful hash functions available. SHA-256 is not much more complicated to install than SHA-1, and it has not been disturbed in any way. The 256-bit key makes it a great work for AES partners. Described in the NIST (National Institute of Standards and Technology) standard 'FIPS 180-4'. NIST also provides multiple test vectors to ensure implementation accuracy.

4 Modelling Design

This paper proposes a method and design that a decentralized one, whereas the existing nature of IoT systems is centralized. With this introduction of a decentralized nature as opposed to a centralized one, the aspect of security is dealt with. Further, a single point failure cannot take place as there are several other nodes present on the network. For the case of data manipulation, in case of a centralized system, it is possible for an attacker to tamper with data and not get noticed. Whereas in a decentralized system, due to the presence of multiple nodes, if the same scenario were to occur, the blockchain would compare the data of the other nodes and maintain the correct data by correcting itself. Blockchains work on the concept of hashing and not on encryption, thus, there is no possibility of decrypting the data. The hashes generated for every transaction are unique and even the most minute change or tampering of the data being transacted will result in a new hash being generated.

This property of blockchain technology renders it highly secure.

Another aspect that is integral to blockchains is that even if a new hash is generated in a node, the blockchain will then correct that node based on the presence and validation of the data of majority of the nodes on the block.

For the purpose of this paper, we will be considering a weather monitoring system for our proposed methodology and data manipulations. Accordingly, components such as temperature and humidity sensing via dht11 sensor are considered.

Implementing security in iot systems via blockchain *13*

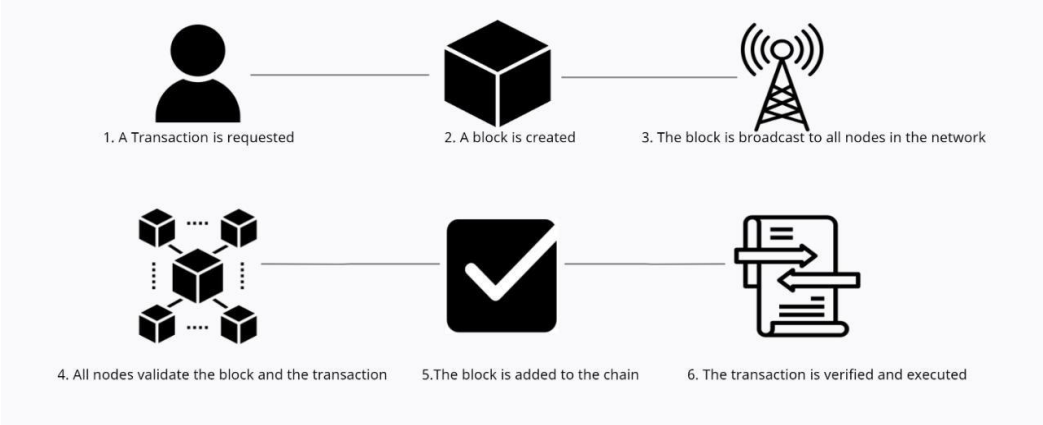

Figure. 4.1 Blockchain transaction

Fig. 4.1 depicts the working of the blockchain technology. First, a transaction is requested; this is the initial step. Once a transaction has been requested. A block is then created that holds data (along with other fields such as timestamp, hash, and previous hash vales). Now this block is sent to all the nodes present in the network for validation. Once validated, the block is successfully added to the chain; and all nodes on the network are now updated with the latest block. This completes the transaction. Due to three essential features- hashing, proof-of-work, and distributed nature of the blockchain which allows for peer-to-peercommunication; the blockchain has immense security and is extremely difficult to break.

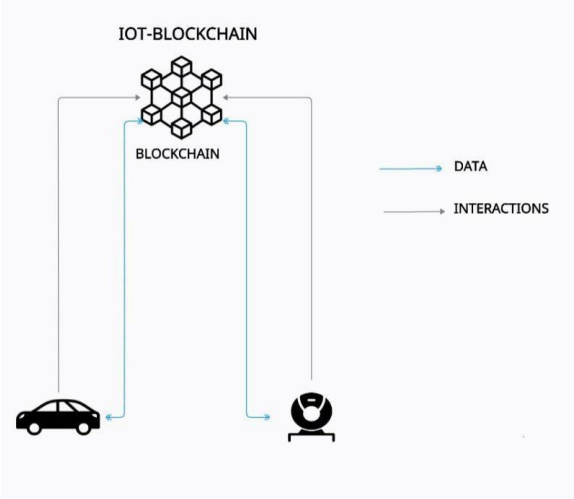

Figure 4.2 Overview of blockchain in IoT system

With the addition blockchain technology, the central cloud server in the above-mentioned system is eliminated and in place of it, a blockchain system is introduced as shown in Fig.
4.2. All the data and interactions will pass through this blockchain and get stored on it.

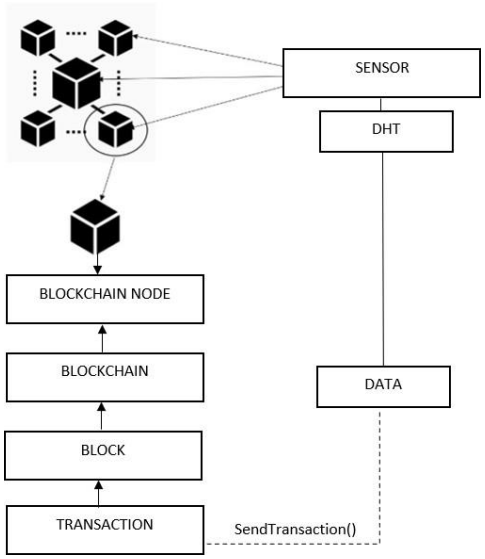

Figure 4.3 Working of our code

Fig 4.3 shows how different aspects in our code fit together. The DHT11 sensor entity sends the temperature and humidity data via a transaction. This the moves into a block when then is a part of a blockchain. This is contained with a Blockchain node. The sensed data is sent to the three closest nodes. The other two remaining nodes do not receive the transactions but due to the process of synchronization, the other nodes also get updated eventually after all the validation is done. The blocks are all individual classes.

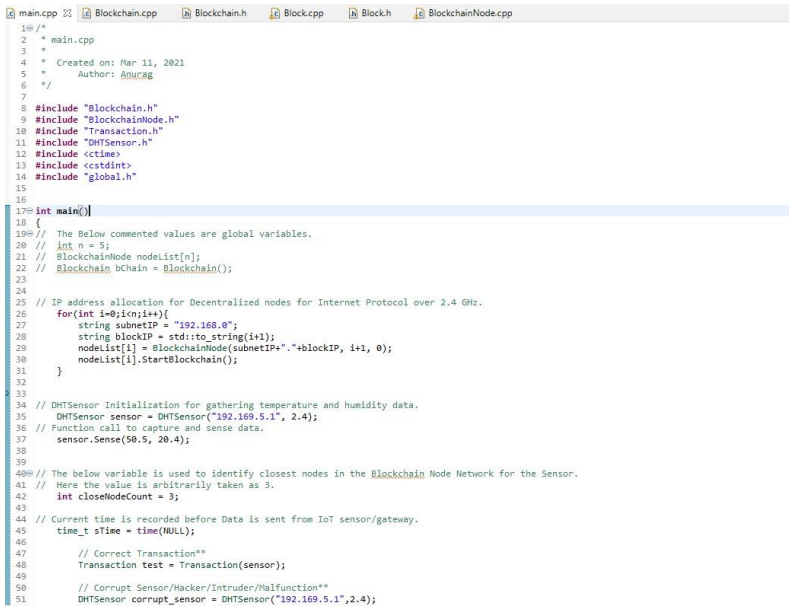

Figure. 4.4 Main initializations

Implementing security in iot systems via blockchain *15*

This paper presents the working of a model blockchain that consists of 5 nodes and the transactions are being sent to the three closest nodes. As the scenario of weather monitoring system is considered, the code consists of corresponding class of DHT11 sensor that will send readings of temperature and humidity. These readings are then encapsulated into a “transaction” that are then sent over to the nodes of the blockchain. Here, the three closest nodes have been selected to receive the transactions. Fig. 4.4 shows the main initializations set. The Sensor constructor is set to transmit the sensor readings. The whole blockchain is set as a list and the hashes with their counters are key-value pairs in a mapping. As the nodes, sensors are part of a network, they have IP addressed that are set as shown in Fig. 4.4. The sensor is a separate entity that only sends the data over a transaction to the blockchain.

```
void BlockchainNode::sendTransaction(Transaction t, time_t sTime,int cnc){

    nodeCount++;
    // Validating the transaction with Majority and Proof of Work will be executed when the Block is being created.

    // Majority
    // finding existing top count
    map<string,int>::iterator i;
    if(!temp_transmap.empty()){
        for(i = temp_transmap.begin();i != temp_transmap.end(); ++i){
            if(i->second > maxCount){
                maxCount = i->second;
                maxLeader = t;
            }
        }
    }else{
        maxCount = 1;
        maxLeader = t;
    }
    if(t.GetHash()!=" " && temp_transmap.empty()){
        temp_transmap.insert(pair<string,int>(t.GetHash(),1));
    } else if(temp_transmap.find(t.GetHash())==temp_transmap.end()){
        temp_transmap.insert(pair<string,int>(t.GetHash(),1));
```

Figure. 4.5 Majority algorithm

```
} else {
    maxCount++;
    maxLeader = t;
    temp_transmap.at(t.GetHash())++;
}
cout<<"The current received Transaction Hashes with their count: ";
for(i = temp_transmap.begin();i != temp_transmap.end(); ++i){
    cout<< endl<< i->first<<"---"<<i->second<< endl;
}
cout<<endl;
cout <<"Majority number of Hashes: "<< maxCount <<endl<<"The current Leading Majority Hash: "<< maxLeader.GetHash()
      <<endl<<"-------------------------------------------------"<<endl;

// find by value from map
std::vector<std::string> vec;
bool bResult = false;
auto it = temp_transmap.begin();
// Iterate through the map
while(it != temp_transmap.end()){
    // Check if value of this entry matches with given value
    if(it->second == maxCount)
    {
        // Yes found
        bResult = true;
        // Push the key in given map
        vec.push_back(it->first);
    }
    // Go to next entry in map
    it++;
}
if(bResult && vec.size() > 1){
    for(auto elem : vec)
    {
        cout<<"equal count : Forking....for hash: ";
        cout<<elem<<endl<<endl;
    }
}
cout << "*****************************Transaction End*********************************"<<endl;
if(nodeCount == cnc){
    cout <<endl<< "\t Synchronizing Blockchain"<<endl<<"************************************"<<endl;
    cout << "Node number : "<<nodeCount<<" Transmiting correct transaction after Majority...";
    for(int i=0;i<n;i++){
        nodeList[i].updateTransactionandAddBlock(sTime);
    }
    cout<<"Closest Nodes Synchronized! Synchronizing Blockchain Network..."<<endl;
}
```

Figure. 4.6 Majority algorithm

```
void BlockchainNode::updateTransactionandAddBlock(time_t sTime){
    _blockCount++;
    maxLeader._destAddr = _ipAddr;
    cout<<"Adding Block with transaction from sensor with time: "<< sTime <<endl;
    bChain.AddBlock(Block(_blockCount,maxLeader,sTime));
    cout<<endl<<"The transaction has of block is : "<<bChain._GetLastBlock().GetTransaction().GetHash()<<endl<<endl;
}
```

Figure. 4.7 Majority algorithm

Fig. 4.5, 4.6 and 4.7 elucidate the majority algorithm. It is due to this that any tampering of data carried out by an attacker can be disregarded. As an attacker will have to follow proof of work mechanism it is seemingly not possible for an attacker to tamper with more than halfthe transactions at once. Thus, we take into account the majority of transactions with the same hash value and validate this to be the actual data. Section 5 delves more deeply into this concept.

```
void Block::MineBlock(uint32_t nDifficulty){
    char cstr[nDifficulty + 1];
    for(uint32_t i=0;i<nDifficulty;++i){
        cstr[i] = '0';
    }
    cstr[nDifficulty] = '\0';

    string str(cstr);

    do{
        _nNonce++;
        _sHash = _CalculateHash();
        //cout<<"Hash with nonce "<<_nNonce<<" : "<< _sHash<<endl;
    }while(_sHash.substr(0,nDifficulty) != str);

    cout<<"Block mined: " << _sHash <<endl;
    cout<<"Time taken: "<< time(NULL)-_tTime<<" seconds"<<endl;
    cout <<"Transaction address data: "<< _sData.GetSAddr()<<"-->"<<_sData.GetDAddr();
}

inline string Block::_CalculateHash() {
    stringstream ss;
    string transHash = _sData.GetHash();
    ss << _nIndex << _tTime << transHash << _nNonce << sPrevHash;

    return sha256(ss.str());
}
```

Figure. 4.8 Proof of Work

A blockchain has multiple nodes and all the nodes have the same stake of the blockchain. While adding a new block in the blockchain, to differentiate between a proper and malicious node, proof of work is used. Proof of work is a consensus algorithm. Here, all the nodes which are competing with each other to add the new block to the blockchain have to do some computing work. All of them are given the generated hash by SHA-256.For example if our difficulty is 4, they will try to iterate and calculate more hashes with the same hash and nonce which is an iterating number. They keep on iterating until they get a randomly generated hash with all the values which they are passing in and this randomly generated should have its first four digits to be zero, since our difficulty level is 4. If these passes, then they are successfully validated and now can add the block. This is useful in detecting the malicious node as if there are 3 blocks competing to add the block, blockchain will only select the block which did the most computational work and will disregard others because they have done it in less computational work therefore concluding them to be the malicious block. The more computational work tells the blockchain how secure the block is.

Highlighting the security aspect of the blockchain, the situation where tampering of data or corruption can happen has been considered and illustrated in Section 5 of this paper.

Implementing security in iot systems via blockchain *17*

5 Experiments, Results and Discussion

This section delves into three possible scenarios that can occur when corrupted data (by a hacker) is sent in a transaction to particular nodes.

5.1 Case 1: Node 3 is corrupted

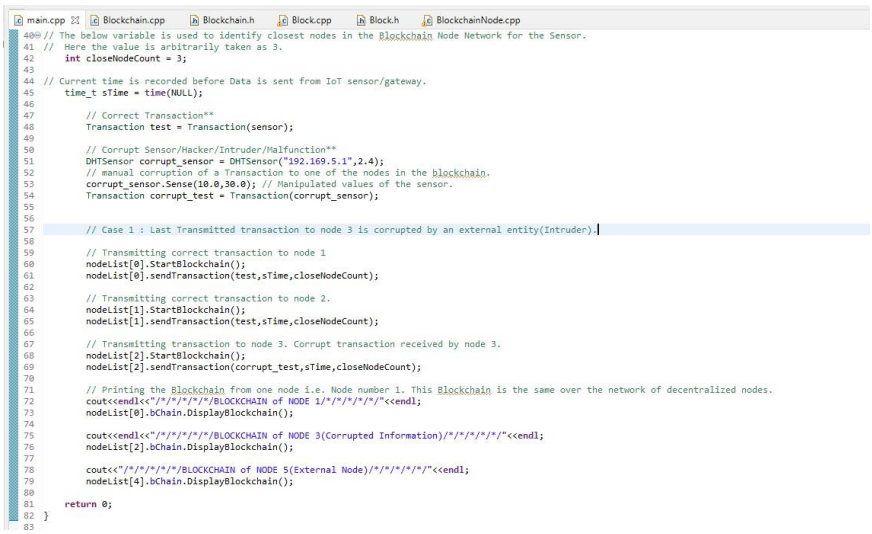

Figure. 5.1.1 Main initializations with node 3 corrupted

Here, the transaction is sent to three closest nodes 1, 2, and 3. While the transactions are being sent to nodes 1, 2 and 3; nodes 4 and 5 do not receive a transaction as it relatively farther away. Now, here, all three nodes receive the transaction at the same time, but the correct data is sent to nodes 1 and 2 while node 3 is receiving corrupted data that may have been altered by a hacker. This is set here by the attacker spoofing as the sensor to the blockchain.

Figure. 5 1.2 Output 1

Fig. 5.1.2 shows the output of this case scenario. There is a mapping in place that keeps track of the hashes as keys and the corresponding count of each hash as a value. Upon all three nodes receiving the transactions, it can be seen that nodes 1 and 2 receive the same hash, i.e., the same correct reading from the sensors and thus the count of that hash value becomes 2. Whereas the hash received by node 3 does not match. Due to majority, the hash value sent to nodes 1 and 2 are accepted, validated, and included in the blockchain and the one sent to node 3 is disregarded.

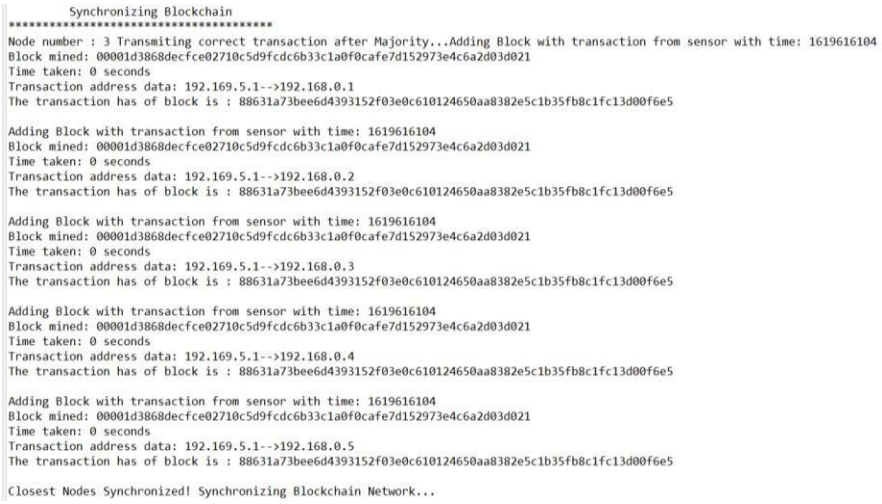

Figure. 5.1.3 Output 2

In continuation of the output, Fig. 5.1.3 shows the synchronization of the blockchain. While the transactions were sent to only 3 nodes, our blockchain contains 5 nodes and all these need to be updated with the latest transactions. For this, due to majority, first node 3 is updated with the correct hash. Following this, all the nodes in the blockchain are synchronized to hold the same validated data as shown in Fig. 5.1.3.

Figure. 5 1.4 Output 3

Lastly, Fig. 5.1.4 shows the blockchains of nodes 1,3 and 5. It can be seen that the blockchains of these nodes are now identical following the synchronization. Even though node 5 never received the transaction, upon synchronization it has been updated. The hold the same sensordata and hash values for that transaction.

5.2 Case 2: Node 2 is corrupted

```
// Case 2 : Second Transmitted transaction to node 2 is corrupted by an external entity(Intruder).

// Transmitting correct transaction to node 1.
nodeList[0].StartBlockchain();
nodeList[0].sendTransaction(test,sTime,closeNodeCount);

// Transmitting transaction to node 2. Corrupt transaction received by node 2.
nodeList[1].StartBlockchain();
nodeList[1].sendTransaction(corrupt_test,sTime,closeNodeCount);

// Transmitting correct transaction to node 3.
nodeList[2].StartBlockchain();
nodeList[2].sendTransaction(test,sTime,closeNodeCount);

// Printing the Blockchain from one node i.e. Node number 1, 2, 5. This Blockchain is the same over the network of decentralized nodes due to the Synchronization.
// Synchronization takes the majority transaction and updates the Blockchain Network.
cout<<endl<<"/*/*/*/*/*/BLOCKCHAIN of NODE 1/*/*/*/*/*/"<<endl;
nodeList[0].bChain.DisplayBlockchain();

cout<<endl<<"/*/*/*/*/*/BLOCKCHAIN of NODE 2(Corrupted Information)/*/*/*/*/*/"<<endl;
nodeList[1].bChain.DisplayBlockchain();

cout<<"/*/*/*/*/*/BLOCKCHAIN of NODE 5(External Node)/*/*/*/*/*/"<<endl;
nodeList[4].bChain.DisplayBlockchain();
```

Figure. 5.2.1 Main initializations with node 2 corrupted

In this scenario, all nodes 1, 2 and 3 receive the transaction at the same time, but the correct data is sent to nodes 1 and 3 while node 2 is receiving corrupted data that may have been altered by a hacker as depicted in Fig. 5.2.1.

```
The current received Transaction Hashes with their count:
88631a73bee6d4393152f03e0c610124650aa8382e5c1b35fb8c1fc13d00f6e5---1

Majority number of Hashes: 1
The current Leading Majority Hash: 88631a73bee6d4393152f03e0c610124650aa8382e5c1b35fb8c1fc13d00f6e5
------------------------------------------------
*******************************Transaction End**********************************
The current received Transaction Hashes with their count:
88631a73bee6d4393152f03e0c610124650aa8382e5c1b35fb8c1fc13d00f6e5---1

9ea0a17ae2cd7b511ece9af56abab20838ef9fed2843ef106c2410fd237bdd50---1

Majority number of Hashes: 1
The current Leading Majority Hash: 88631a73bee6d4393152f03e0c610124650aa8382e5c1b35fb8c1fc13d00f6e5
------------------------------------------------
equal count : Forking....for hash: 88631a73bee6d4393152f03e0c610124650aa8382e5c1b35fb8c1fc13d00f6e5

equal count : Forking....for hash: 9ea0a17ae2cd7b511ece9af56abab20838ef9fed2843ef106c2410fd237bdd50

*******************************Transaction End**********************************
The current received Transaction Hashes with their count:
88631a73bee6d4393152f03e0c610124650aa8382e5c1b35fb8c1fc13d00f6e5---2

9ea0a17ae2cd7b511ece9af56abab20838ef9fed2843ef106c2410fd237bdd50---1

Majority number of Hashes: 2
The current Leading Majority Hash: 88631a73bee6d4393152f03e0c610124650aa8382e5c1b35fb8c1fc13d00f6e5
------------------------------------------------
*******************************Transaction End**********************************
```

Figure. 5.2.2 Output 1

Fig. 5.2.2 shows the output of case 2. Here, as the nodes receive the transactions, the first node receives a hash and the counter for that hash is increased. The hash received by node 2 is not the same as the one received by node 1, thus the counter is increased for this new hash as well. Now, a forking situation arises and based on the hash value received by node 3 via the transaction, the corresponding transaction will be accepted. Here, the hash of node 3 matches that of node 1 and so this transaction is validated and accepted.

```
        Synchronizing Blockchain
****************************************
Node number : 3 Transmiting correct transaction after Majority...Adding Block with transaction from sensor with time: 1619617991
Block mined: 0000d42127c51cabacdcff5e0c2511a39c17c96cd919e6a8331428e2154cd4dc
Time taken: 0 seconds
Transaction address data: 192.169.5.1-->192.168.0.1
The transaction has of block is : 88631a73bee6d4393152f03e0c610124650aa8382e5c1b35fb8c1fc13d00f6e5

Adding Block with transaction from sensor with time: 1619617991
Block mined: 0000d42127c51cabacdcff5e0c2511a39c17c96cd919e6a8331428e2154cd4dc
Time taken: 0 seconds
Transaction address data: 192.169.5.1-->192.168.0.2
The transaction has of block is : 88631a73bee6d4393152f03e0c610124650aa8382e5c1b35fb8c1fc13d00f6e5

Adding Block with transaction from sensor with time: 1619617991
Block mined: 0000d42127c51cabacdcff5e0c2511a39c17c96cd919e6a8331428e2154cd4dc
Time taken: 1 seconds
Transaction address data: 192.169.5.1-->192.168.0.3
The transaction has of block is : 88631a73bee6d4393152f03e0c610124650aa8382e5c1b35fb8c1fc13d00f6e5

Adding Block with transaction from sensor with time: 1619617991
Block mined: 0000d42127c51cabacdcff5e0c2511a39c17c96cd919e6a8331428e2154cd4dc
Time taken: 1 seconds
Transaction address data: 192.169.5.1-->192.168.0.4
The transaction has of block is : 88631a73bee6d4393152f03e0c610124650aa8382e5c1b35fb8c1fc13d00f6e5

Adding Block with transaction from sensor with time: 1619617991
Block mined: 0000d42127c51cabacdcff5e0c2511a39c17c96cd919e6a8331428e2154cd4dc
Time taken: 1 seconds
Transaction address data: 192.169.5.1-->192.168.0.5
The transaction has of block is : 88631a73bee6d4393152f03e0c610124650aa8382e5c1b35fb8c1fc13d00f6e5

Closest Nodes Synchronized! Synchronizing Blockchain Network...
```

Figure. 5 2.3 Output 2

Following this, Fig. 5.2.3 shows the synchronization of the blockchain. First based on majority, the hash value of node 2 is updated to the correct one and then the all the nodes onthe blockchain are updated.

```
/*/*/*/*/*/BLOCKCHAIN of NODE 1/*/*/*/*/*/

//////////////BLOCK///////////////
Block number: 0
Block creation time: 1619617991
Block hash: GENESIS BLOCK HASH

//////////////BLOCK///////////////
Block number: 1
Block Previous Hash: GENESIS BLOCK HASH
Block creation time: 1619617991
Block hash: 0000d42127c51cabacdcff5e0c2511a39c17c96cd919e6a8331428e2154cd4dc
***Block Transaction Details:
Transaction Hash: 88631a73bee6d4393152f03e0c610124650aa8382e5c1b35fb8c1fc13d00f6e5
Transaction Sensor Data: 50.5 + 20.4
////////////////////////////////

/*/*/*/*/*/BLOCKCHAIN of NODE 2(Corrupted Information)/*/*/*/*/*/

//////////////BLOCK///////////////
Block number: 0
Block creation time: 1619617991
Block hash: GENESIS BLOCK HASH

//////////////BLOCK///////////////
Block number: 1
Block Previous Hash: GENESIS BLOCK HASH
Block creation time: 1619617991
Block hash: 0000d42127c51cabacdcff5e0c2511a39c17c96cd919e6a8331428e2154cd4dc
***Block Transaction Details:
Transaction Hash: 88631a73bee6d4393152f03e0c610124650aa8382e5c1b35fb8c1fc13d00f6e5
Transaction Sensor Data: 50.5 + 20.4
////////////////////////////////
/*/*/*/*/*/BLOCKCHAIN of NODE 5(External Node)/*/*/*/*/*/

//////////////BLOCK///////////////
Block number: 0
Block creation time: 1619617991
Block hash: GENESIS BLOCK HASH

//////////////BLOCK///////////////
Block number: 1
Block Previous Hash: GENESIS BLOCK HASH
Block creation time: 1619617991
Block hash: 0000d42127c51cabacdcff5e0c2511a39c17c96cd919e6a8331428e2154cd4dc
***Block Transaction Details:
Transaction Hash: 88631a73bee6d4393152f03e0c610124650aa8382e5c1b35fb8c1fc13d00f6e5
Transaction Sensor Data: 50.5 + 20.4
////////////////////////////////
```

Figure. 5 2.4 Output 3

Fig. 5.2.4 shows the blockchains of nodes 1,2 and 5. It can be seen that the blockchains of these nodes are now identical following the synchronization. In spite of receiving tampered or corrupted data, node 2 now contains the actual data. Also, even though node 5 never received the transaction, upon synchronization it has been updated. The hold the same sensordata and hash values for that transaction.

5.3 Case 3: Node 1 is corrupted

```
// Case 3 : First Transmitted transaction to node 1 is corrupted by an external entity(Intruder).

// Transmitting transaction to node 1. Corrupt transaction received by node 1.
nodeList[0].StartBlockchain();
nodeList[0].sendTransaction(corrupt_test,sTime,closeNodeCount);

// Transmitting correct transaction to node 2.
nodeList[1].StartBlockchain();
nodeList[1].sendTransaction(test,sTime,closeNodeCount);

// Transmitting correct transaction to node 3.
nodeList[2].StartBlockchain();
nodeList[2].sendTransaction(test,sTime,closeNodeCount);

// Printing the Blockchain from one node i.e. Node number 1, 3, 5. This Blockchain is the same over the network of decentralized nodes due to the Synchronization.
// Synchronization takes the majority transaction and updates the Blockchain Network.
cout<<endl<<"/*/*/*/*/*/BLOCKCHAIN of NODE 1(Corrupted Information)/*/*/*/*/*/"<<endl;
nodeList[0].bChain.DisplayBlockchain();

cout<<endl<<"/*/*/*/*/*/BLOCKCHAIN of NODE 3/*/*/*/*/*/"<<endl;
nodeList[2].bChain.DisplayBlockchain();

cout<<"/*/*/*/*/*/BLOCKCHAIN of NODE 5(External Node)/*/*/*/*/*/"<<endl;
nodeList[4].bChain.DisplayBlockchain();
```

Figure. 5.3.1 Main initializations with node 1 corrupted

In this scenario, all nodes 1, 2 and 3 receive the transaction at the same time, but the correct data is sent to nodes 2 and 3 while node 1 is receiving corrupted data that may have been altered by a hacker as depicted in Fig. 5.3.1.

```
The current received Transaction Hashes with their count:
9ea0a17ae2cd7b511ece9af56abab20838ef9fed2843ef106c2410fd237bdd50---1

Majority number of Hashes: 1
The current Leading Majority Hash: 9ea0a17ae2cd7b511ece9af56abab20838ef9fed2843ef106c2410fd237bdd50
------------------------------------------------
*****************************Transaction End*********************************
The current received Transaction Hashes with their count:
88631a73bee6d4393152f03e0c610124650aa8382e5c1b35fb8c1fc13d00f6e5---1

9ea0a17ae2cd7b511ece9af56abab20838ef9fed2843ef106c2410fd237bdd50---1

Majority number of Hashes: 1
The current Leading Majority Hash: 9ea0a17ae2cd7b511ece9af56abab20838ef9fed2843ef106c2410fd237bdd50
------------------------------------------------
equal count : Forking....for hash: 88631a73bee6d4393152f03e0c610124650aa8382e5c1b35fb8c1fc13d00f6e5

equal count : Forking....for hash: 9ea0a17ae2cd7b511ece9af56abab20838ef9fed2843ef106c2410fd237bdd50

*****************************Transaction End*********************************
The current received Transaction Hashes with their count:
88631a73bee6d4393152f03e0c610124650aa8382e5c1b35fb8c1fc13d00f6e5---2

9ea0a17ae2cd7b511ece9af56abab20838ef9fed2843ef106c2410fd237bdd50---1

Majority number of Hashes: 2
The current Leading Majority Hash: 88631a73bee6d4393152f03e0c610124650aa8382e5c1b35fb8c1fc13d00f6e5
------------------------------------------------
*****************************Transaction End*********************************
```

Figure. 5.3.2 Output 1

Fig. 5.3.1 shows that even though node 1 has received a transaction with a particular hash

value, it is not automatically validated. The concept of majority is always considered. Thus, when nodes 2 and 3 are observed and as they have the transaction with the same hash value, the count for this hash value is increased.

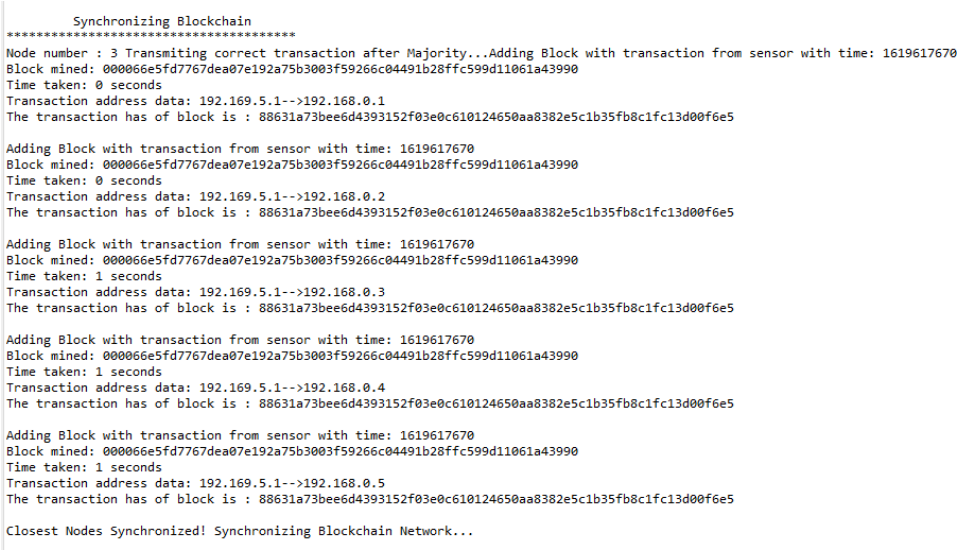

Figure. 5 3.3 Output 2

Here, again based on majority, the transaction as received by nodes 2 and 3 are accepted, the same is updated on node 1. Next, all the nodes in the blockchain are updated with the newly validated transaction as shown in Fig.5.3.3.

```
/*/*/*/*/*/BLOCKCHAIN of NODE 1(Corrupted Information)/*/*/*/*/*/

//////////////BLOCK///////////////
Block number: 0
Block creation time: 1619617670
Block hash: GENESIS BLOCK HASH

//////////////BLOCK///////////////
Block number: 1
Block Previous Hash: GENESIS BLOCK HASH
Block creation time: 1619617670
Block hash: 000066e5fd7767dea07e192a75b3003f59266c04491b28ffc599d11061a43990
***Block Transaction Details:
Transaction Hash: 88631a73bee6d4393152f03e0c610124650aa8382e5c1b35fb8c1fc13d00f6e5
Transaction Sensor Data: 50.5 + 20.4
////////////////////////////////

/*/*/*/*/*/BLOCKCHAIN of NODE 3/*/*/*/*/*/

//////////////BLOCK///////////////
Block number: 0
Block creation time: 1619617670
Block hash: GENESIS BLOCK HASH

//////////////BLOCK///////////////
Block number: 1
Block Previous Hash: GENESIS BLOCK HASH
Block creation time: 1619617670
Block hash: 000066e5fd7767dea07e192a75b3003f59266c04491b28ffc599d11061a43990
***Block Transaction Details:
Transaction Hash: 88631a73bee6d4393152f03e0c610124650aa8382e5c1b35fb8c1fc13d00f6e5
Transaction Sensor Data: 50.5 + 20.4
////////////////////////////////
/*/*/*/*/*/BLOCKCHAIN of NODE 5(External Node)/*/*/*/*/*/

//////////////BLOCK///////////////
Block number: 0
Block creation time: 1619617670
Block hash: GENESIS BLOCK HASH

//////////////BLOCK///////////////
Block number: 1
Block Previous Hash: GENESIS BLOCK HASH
Block creation time: 1619617670
Block hash: 000066e5fd7767dea07e192a75b3003f59266c04491b28ffc599d11061a43990
***Block Transaction Details:
Transaction Hash: 88631a73bee6d4393152f03e0c610124650aa8382e5c1b35fb8c1fc13d00f6e5
Transaction Sensor Data: 50.5 + 20.4
////////////////////////////////
```

Figure. 5.3.4 Output 3

Fig. 5.3.4 shows the blockchains of nodes 1,3 and 5. It can be seen that the blockchains of these nodes are now identical following the synchronization. In spite of receiving tampered or corrupted data, node 1 now contains the actual data. Also, even though node 5 never received the transaction, upon synchronization it has been updated. The hold the same sensordata and hash values for that transaction.

From the above experiments carried out, it can be inferred that the blockchain mechanism is robust, and due to hashing, proof of work and majority algorithm, the blockchain is reliable and secure. From the multiple cases shown, the possibility of an attacker trying to tamper and send altered data is also eliminated.

6 Conclusion

Blockchain and Internet of things are two of the most talked about technologies right now. IoT system right now uses client/server model or a centralized model of networking. They all use a single gateway to transfer data. This has been utilized for a long time, but is not suitable for our current needs. It has high-cost maintenance and the cost will increase as we increase the number of connected devices. The

single gateway used is not trustworthy, as it

allows gaining access to the whole network by compromising a single device. It has become a big challenge to identify, authenticate and secure these devices. The current model is expensive to scale and manage. In this paper we have proposed blockchain mechanism which is more robust and due to hashing, proof of work and majority algorithm, it is more reliable and secure than the traditional model. Therefore, from the above experiments carried out, it can be inferred that the proposed method is more reliable and secure than the traditional model. From the multiple cases shown, we can conclude that the possibility of an attacker trying to tamper and send altered data is also eliminated. Blockchain technology can become the future for IoT systems making it very secure and can be used in applications like smart cities.

References

Minoli, D. and Occhiogrosso, B., 2018. Blockchain mechanisms for IoT security. Internet of Things, 1, pp.1-13.

Hassan, M.U., Rehmani, M.H. and Chen, J., 2019. Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions. Future Generation Computer Systems, 97, pp.512-529.

Sultan, A., Mushtaq, M.A. and Abubakar, M., 2019, March. IOT security issues via blockchain: a review paper. In Proceedings of the 2019 International Conference on Blockchain Technology (pp. 60-65).

Agrawal, R., Verma, P., Sonanis, R., Goel, U., De, A., Kondaveeti, S.A. and Shekhar, S., 2018, April. Continuous security in IoT using blockchain. In 2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) (pp. 6423-6427). IEEE.

Dai, H.N., Zheng, Z. and Zhang, Y., 2019. Blockchain for Internet of Things: A survey. IEEE Internet of Things Journal, 6(5), pp.8076-8094.

Abou-Nassar, E.M., Iliyasu, A.M., El-Kafrawy, P.M., Song, O.Y., Bashir, A.K. and Abd El- Latif, A.A., 2020. DITrust chain: towards blockchain-based trust models for sustainable healthcare IoT systems. IEEE Access, 8, pp.111223-111238.

Hang, L. and Kim, D.H., 2019. Design and implementation of an integrated iot blockchain platform for sensing data integrity. Sensors, 19(10), p.2228.

Andersen, M.P., Kolb, J., Chen, K., Fierro, G., Culler, D.E. and Popa, R.A., 2017. Wave: A decentralized authorization system for iot via blockchain smart contracts. University of California at Berkeley, Tech. Rep.

Fakhri, D. and Mutijarsa, K., 2018, October. Secure IoT communication using blockchain technology. In 2018 International Symposium on Electronics and Smart Devices (ISESD) (pp. 1-6). IEEE.

Alotaibi, B., 2019. Utilizing blockchain to overcome cyber security concerns in the internet of things: A review. IEEE Sensors Journal, 19(23), pp.10953-10971.

Huckle, S., Bhattacharya, R., White, M. and Beloff, N., 2016. Internet of things, blockchain and shared economy applications. Procedia computer science, 98, pp.461-466.

Sicari, S., Rizzardi, A., Grieco, L.A. and Coen-Porisini, A., 2015. Security, privacy and trust in Internet of Things: The road ahead. Computer networks, 76, pp.146-164.

Christidis, K. and Devetsikiotis, M., 2016. Blockchains and smart contracts for the internet of things. Ieee Access, 4, pp.2292-2303.

Roman, R., Zhou, J. and Lopez, J., 2013. On the features and challenges of security and privacy in distributed internet of things. Computer Networks, 57(10), pp.2266-2279.

Ali, M.S., Dolui, K. and Antonelli, F., 2017, October. IoT data privacy via blockchains and IPFS. In Proceedings of the seventh international conference on the internet of things (pp. 1- 7).