# Improving Data Integrity of IoT data using IOTA

[1]Mirza Furqaanbeg, [2]Gayatri Pandi
[1]Student, [2]Head of Department(CE)
[1]ME(IT)
LJIET, Ahmedabad, India

**Abstract:** Internet of Things (IoT) is growing rapidly in different platforms and generates large number of data from each device. It is a challenging task to ensure the security of data as the IoT applications are dynamic in nature. We cannot rely on the third party (can be cloud severs) to ensure the security of the data. There can be different attack performed on the cloud or the third party can do any malicious activity to misuse the data of the owner. To overcome this, we can use blockchain-based technology named IOTA to ensure the data is secured and stored in the database and in the Tangle. The IOTA removes the third-party interaction from the transmission of data between the two parties. By using IOTA both the parties directly interact with each other. It also ensures that data is securely stored in the Tangle as it uses the SHA-256 to encrypt the data. It generates the hash of data which is stored, and once data stored, it can't be changed as Tangle is immutable. Thus, by using blockchain-based technology with the IoT we can ensure data integrity, confidentiality and availability.

**Keywords**: IOTA, IoT, Tangle, Integrity.

## I. Introduction

The internet of things is simply an interconnection of various devices which might be merged in everyday items, allows them to do communication through the internet[9].The Internet of Things (IoT) has strong connectivity from "anyplace" to "anyone" at "anytime" for "anything[9].The growth of Internet of things(IoT) is at fast pace, and some report predicts that the growth of IoT devices will reach to 30 billion by 2020, which are 30 time more devices deployed in 2009[4].As the growth of IoT devices increases the security issues for the data of these devices will also be boosted. The problem to maintain data integrity, confidentiality and availability of the data is an issue for all the owner of the IoT device. Securing data on Internet of Things (IoT) is a difficult task faced by the industries. The global expenditure on IoT security is about to rise at an annual rate of 25%, embracing up to 900 million USD in 2020[5]. IoT deployment raises many security issues related to the characteristics of IoT devices, such as the need for lightweight cryptographic algorithms in terms of processing and memory capabilities, and the use of standard protocols, as per the necessity to minimize the size of data exchanged between nodes[2] There can also an another issue can occur for the securing data when the third party can go down or do any malicious activity which in turn can cause loss of private data for the owner which is critical. To secure data of the IoT devices and to remove the third party from the communication, we can use the technology named IOTA[1].

IOTA is a public distributed ledger that have ability to do microtransactions for the Internet of Things (IoT) devices [6] without any fees. It comes in market in 2015, it solves the core issues of network scalability and charges in traditional distributed ledgers. The market cap of circulating IOTA tokens amounts to nearly $3 billion as of March 2019 and it is among the top 15 cryptocurrencies by market cap [7]. One of the major changes in IOTA from current distributed ledgers is the validation structure namely, the Tangle [6], which is based on a Directed Acyclic Graph (DAG) not a blockchain. The protocol removes the concept of miners from the network. Instead, all the participants in the network are equally responsible for the network validation. Each time there is a transaction is happening, they validate two previous transactions [6]. This simple yet scalable approach increases the rate of validation on the network as the number of contributors grows in the network which will yield more approved transactions. The ultimate goal of IOTA is to enable the machine economy for smart devices. The smart connected devices around the globe will drastically increase to 75.44 billion by 2025 [8] and the distributed integrity layer of the tangle can replace by centralized storages for the data these devices will produce. However, with the nature of the tangle the value can also be exchanged, and digital currency can be securely tracked in a tamperproof way. IOTA tokens are stored at addresses which are encrypted public identities and generated from a random seed of 81 trytes. Transactions associated with these public identities stay anonymous if addresses cannot be linked to their holders. This paper is organized as section-II will give brief idea about related work, section-III explains about IOTA, section- IV will give brief idea of IOTA using a use case, section- V shows how the proposed system is implemented and paper will be concluded in conclusion section.

## II. Related work

In [10], the Caciano and Augusto proposed that the architecture can be split in three parts named as IoT, Fog and Cloud. It divides the tasks in three layers as IoT layer sense and actuate the data and send it to the gateway which is in next layer. The second layer is of fog make the replication of data, also generate log of data. It also stores data in the smart contract with the help of slice manager. And at the last layer the data is stored in two different places, in cloud storage and in the Ethereum blockchain. As it uses the Ethereum blockchain to store the data from Cyber Physical System(CPS) which can't match the speed of the system as the validation time of 1 Ethereum is 10 min which can't be suitable for the CPS as it is way faster than Ethereum. In [11], Bin and others has proposed a framework for checking the data integrity as a service in the network of data owner and data consumer.

There are different algorithms to check the integrity of the data for both the parties. In this also the author has used the Ethereum which needs the miners to mine the block but nowadays there are some miners that are making the network as a centralized by doing mining of maximum transactions and sending it to the blockchain network to validate it. If miner does not have computation power enough to compete with other miners than only few miners will rule the blockchain network making it centralized. In [12], Vidya Ramani and others have proposed the model for registering the data of the patient in the blockchain network using smart contract. The doctor can append the data when any new prescription has to be given to the patient. Here the smart contract is being used to append or to update the data in the network. It can be costly to update the data as the smart contract are written in the Ethereum and gas price has to be paid for the transaction each time. It can be costly for the poor patients to pay every time they visit to the doctor. In [13], Zijian Bao and others has proposed the three-tier architecture to secure the IoT data using the blockchain network. The layer of the architecture named as certification layer, Application layer and Blockchain layer. There are several protocols named as registration and cancellation transaction, Update release and query transactions, device storage transaction, permission release and request transactions and local interactive transactions are the core protocols in the architecture. In [14], Mohamad Badra and Rouba Borghol stated that using Public key Infrastructure(PKI) in the era of quantum computing is not enough to preserve the data integrity and non-repudiation of the data. So, for the storage of the data Merkle tree is used as per the proposed model. This solution offers a continuous proof of existence of the content. In [17], Manisha and Dr. Jasvinder Kaur stated that they are enhancing the data integrity of transactions in the blockchain. They are using an integrated approach of MD5 and multiplicative inverse to secure the transaction details. Also, they have used IP address for the verification along with the integrated MD5 and multiplicative inverse. In [18], Igor Zikratov, Alexander Kuzmin, Vladislav Akimenko, vicktor Niculichev, Lucas Yalansky stated that there are wide areas for digital assets and stocks. Thay are investigating blockchain activity in terms of how they are retrieved and shared in files in a decentralized network. They are ensuring that the security of the files stored in the datebase and it is achieved by well formed transactions, audit which is being provided by the blockchain. In [19], Jun Hak Park, Jun Young Park, Eui Nam Huh, stated that with the increase of cloud services, security threats are also increasing and also attacks methods are also becoming more diverse. To overcome these problems the blockchain is being used in the paper to make integrity management and logging of data for cloud forensics. In this paper the proposed system guarantees the data integrity while processing more transactions than existing permission-less blockchain. Above all paper are using the Blockchain either permissioned or permission-less but the limitation or can say drawback of blockchain is that to mine the transaction, it uses the long-chain rule and it can be a tedious task and currently the validation of a block takes up to a day to mine, which can't be feasible in the IoT network.

## III. IOTA

IOTA is a public distributed ledger designed especially for the Internet of Things economy. IoT devices are now much more popular and they play crucial part of the world economy [6]. It is estimated that the market of IoT growth goes up to the worth $475 billion by 2020 [7]. The devices generate data in very high frequency that non-related companies can make use of this data. At present, there is no way for these companies to buy this data. IOTA is designed to make a way for dealing with this problem by creating a fee-less cryptocurrency that operate on any of the IoT devices. The blockchain technology is not a best fit for the Internet of Things devices. Bitcoin and other blockchain-based cryptocurrencies are having the scalability problems and the charges are required to do a transaction means that sending a micropayment (say $0.01) is not imaginable. In order to find a solution that can fit for the IoT, IOTA has to make ensure that it has scalable network, and it can do transactions quickly and also Microtransactions payments without any fees. To do this activity , IOTA looked away from the blockchain and they opted to use a different technology named as a DAG called the Tangle [6].

In the traditional Blockchain network multiple transactions are stored in a single blocks of size 1 megabyte and the blocks are chained sequentially to each block. A tangle is a data structure based on DAG. Here, Each square show only one transaction. Each of the transaction always validates two previous non-validated transactions[16].

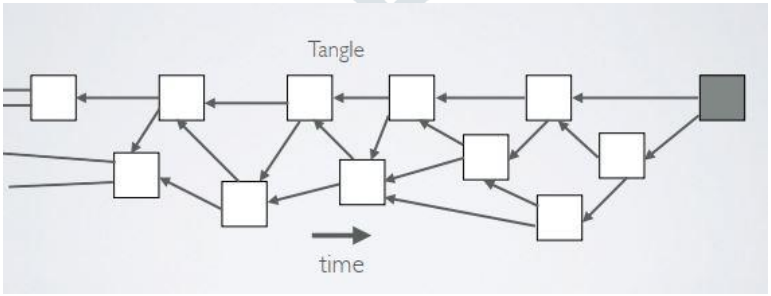


Fig-1 Structure of Tangle

## III. Proposed Work

Here we have taken a use case of supply chain which distributes the medicines from its source to the destination. The medicine taken here as an example to supply to the retailer or consumer must be kept at temperature of 8°-15°C. At Starting of journey, the shipment is registered with the IOTA and all other participants are also registered with IOTA as to keep track of the shipment. The different sensors have been attached to the shipment like location, temperature, humidity, air pressure, RFID, etc. as needed. We have considered the temperature sensor of the shipment for the data integrity verification.

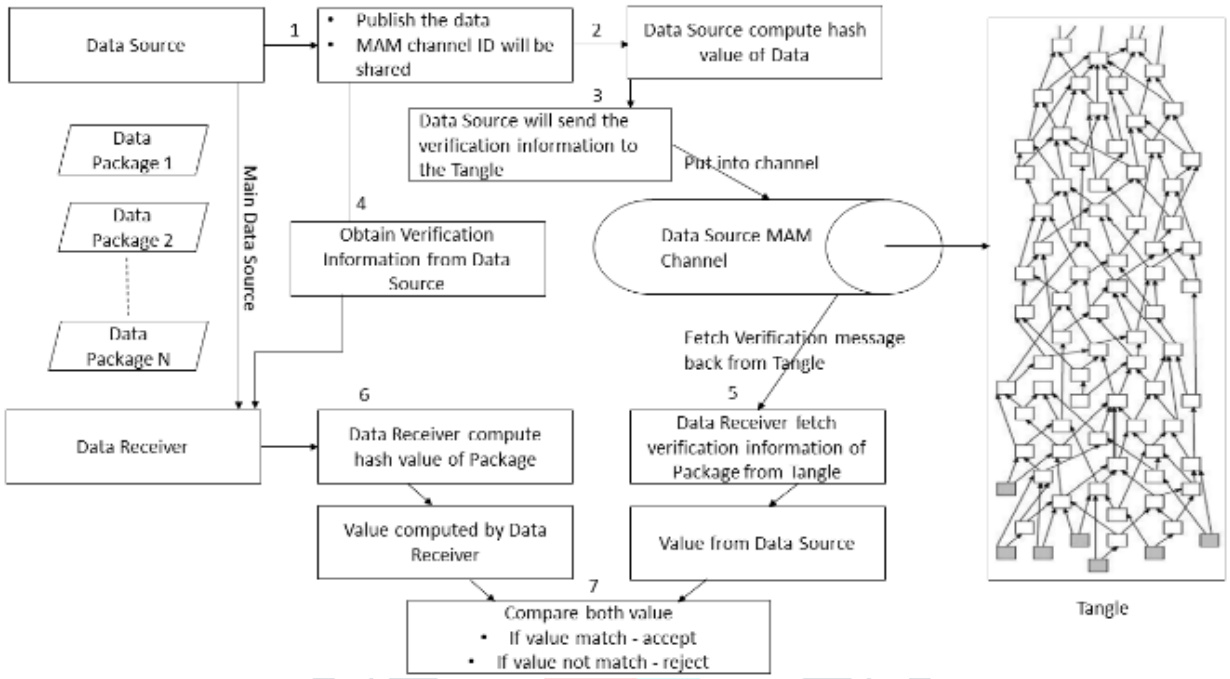


Fig-2 Proposed model to check the data integrity

**Taking the data of sensor and storing it in the Tangle**

Step-1: The temperature sensor node can measure temperature and humidity will send the data to the gateway which will receive the data.

Step-2: The gateway is connected to the internet and it will send the data to the server.

Step-3: The server which is running the Masked Authenticated Message (MAM) script which in turn send the sensor data to the Tangle.

**Verifying the integrity of the data stored in the Tangle**

To verify the integrity of the data below steps must be followed:

Step-1: Data source will publish the data and MAM channel ID is shared with the Data receiver.

Step-2: Data source computes the hash value of the data.

Step-3: Data source send the verification information to the Tangle and put it to the channel. The channel will store the data in the Tangle. Only hash value of the data will be stored in the Tangle.

Step-4: Data receiver will obtain the verification information from the data source to verify the integrity of the data.

Step-5: Data receiver will fetch the verification information package from the tangle based on the root address.

Step-6 Data receiver will compute the hash value by using same hash function.

Step-7 Data receiver will compare both the hash value, if the hash value matches then accept the data and print it. If the hash value is not matched, then reject the data package.

## IV. Use-Case

Here, we have taken a use case where we can integrate the sensors and also apply the IOTA in the system. We have taken the use case of the supply chain which supplies the medicines of the pharmaceutical company from its origin to the desired destination. The supply chain using IOTA can make the data secure and the transactions of the data from one point to all other point is fast.

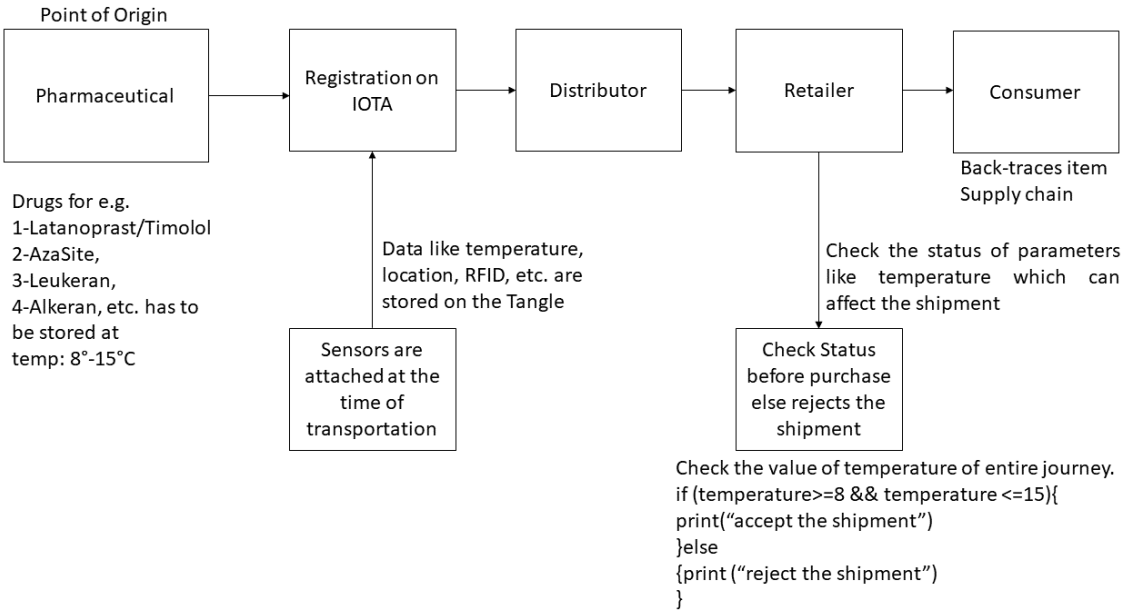


Fig-3 Use case supply chain using IOTA

Now the company wants to send some medicine to the retailer as it has been ordered by the retailer and the required medicine must be kept at a freezing temperature of 8°-15°C. The temperature sensor and other required sensors are attached to the vehicle and all the parties involved in the transportation of shipment are registered in the IOTA network. All the participants can know the status of the shipment and trace throughout its journey from origin to the end. At the destination, the retailer can check the integrity of the data from its source to all location it has been gone through. The decision to accept the shipment can be taken on the basis of this data, whether to accept the shipment or to reject the shipment.

## V. Implementation

The proposed system has been developed to check the feasibility of the IOTA network to work faster than the traditional blockchain network. The IoT data is dynamic in nature and it wants the network to behave fast and respond fast. The IOTA stores the data of the IoT sensors in different blocks or nodes and transaction validity is much faster than the traditional Blockchain. Our system is developed using Arduino Uno and a DHT11 sensor to sense the temperature data and send it to the IOTA network which will be stored in a Tangle. We have implemented our system on a single node for the testing purpose. We have written code using the JavaScript and we have used test network of IOTA to check whether the transaction is happening or not. This figure shows the temperature data is generated from the sensor and it is been stored on the IOTA network having delay of fifteen seconds. After every fifteen seconds the data is generated, and it has been sent to the IOTA network. This network is much faster than the traditional Blockchain network. This figure shows that by taking the root parameter we can check the integrity of the data. By running the script to check the integrity of data also giving the value of the root parameter as required to check the integrity.

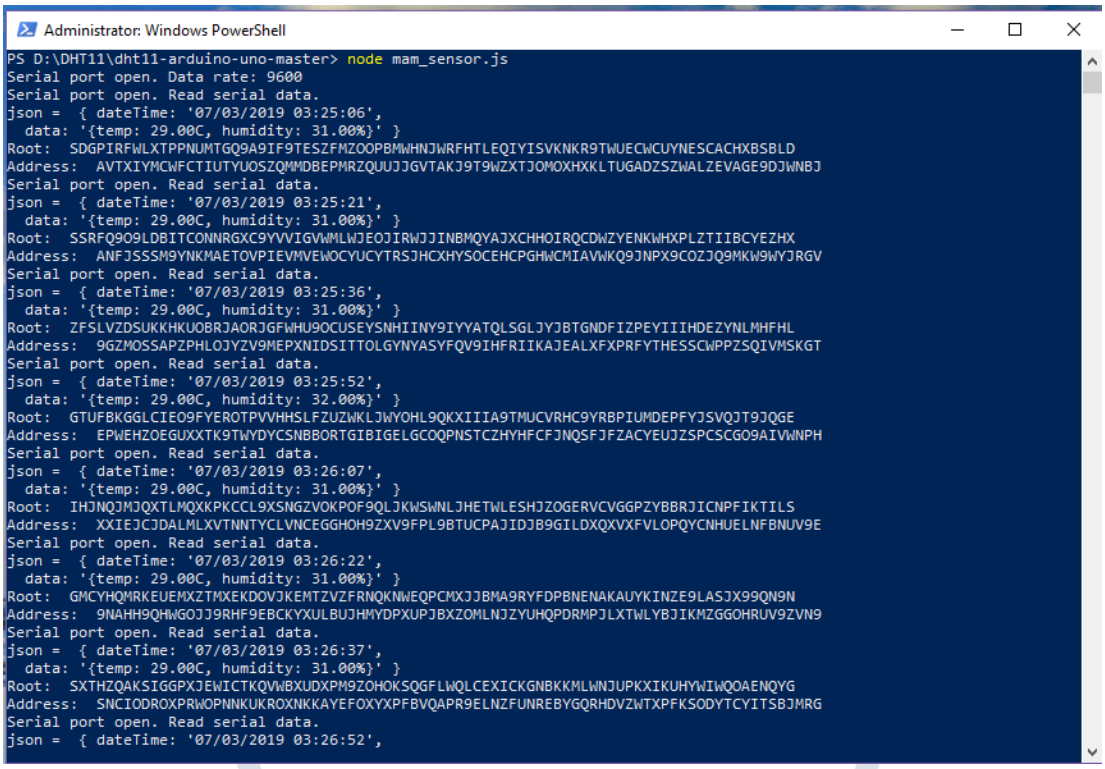


Fig-4 sending the sensor data to the network

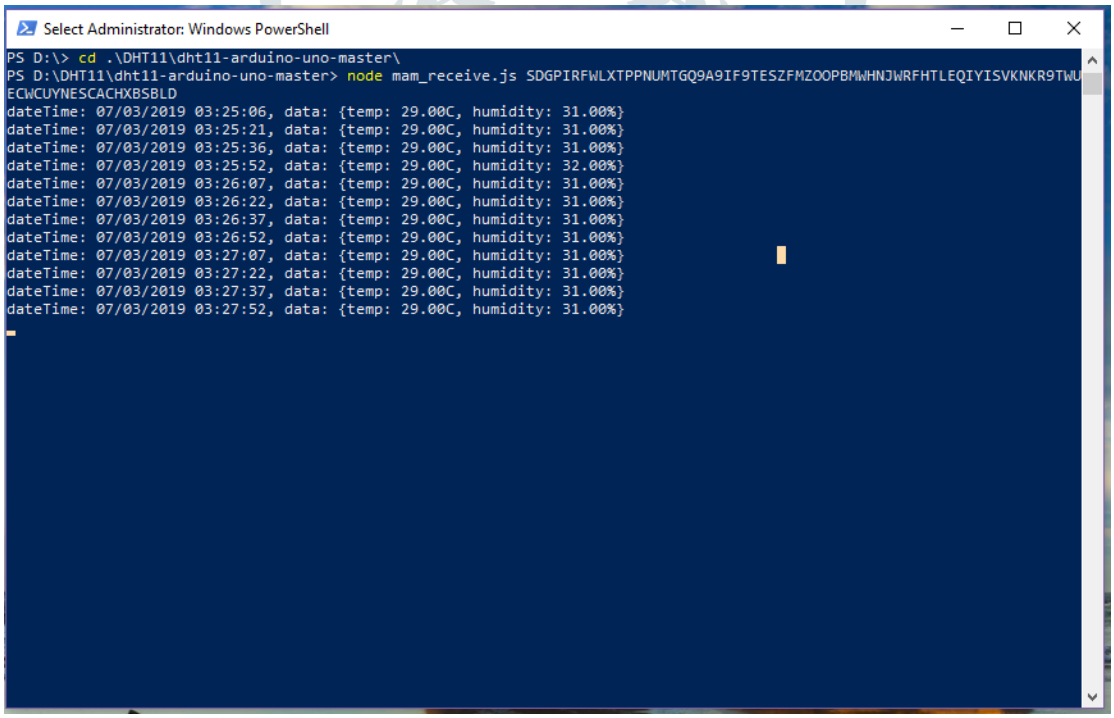


Fig-5 fetching the sensor data from network using the root parameter

## VI. Performance Calculation

In this section, we are calculating and comparing the transactions per second(tps) with different cryptocurrency mechanism with our proposed system. In each of the blockchain mechanism the mining must be done either it is permission-less or permissioned cryptocurrency. As the blockchain uses long chain rule for validating the transactions, the transactions per second are very less in these mechanisms. The tps formula for cryptocurrency from [19] is shown as follows:

$$tps = Blocksize/(Blocktime * size\ of\ transaction) \quad (1)$$

As shown in the table 1 there are different cryptocurrency mechanism which shows their ability to make transactions per second. As taken an example of bitcoin it does 6.41tps, for Ethereum 15.65tps and for Hyperledger around 167tps. These figures are shown in the Table 1.

Table-1 Comparison of different types of blockchain as per TPS

| | Blocksize(MB) | Blocktime(sec) | Transaction size(byte) | tps |
|---|---|---|---|---|
| Bitcoin [19] | 1 | 600 | 260 | 6.41 |
| Ethereum[19] | 4.7 | 14.3 | 21000 | 15.65 |
| Hyperledger[19] | 3.2 | 600 | 32 | 166.67 |
| IOTA | 10 | 120 | 1650 | 505.05 |

The proposed system here is implemented on the permission-less IOTA which is the third generation of blockchain. Here we are making an assumption that to validate the 10MB of data, approx. 120 seconds of time is taken by the network to validate the transaction. In our proposed system the seed are used which are quantum immune and also the combination of seeds is created using the trytes and trits. It is like bytes and bits in which three values are considered for one character each. So, the complexity level in the proposed system increased much higher than other blockchain mechanism. Therefore, it is assumed that 10MB size of transaction block in proposed system can make around 506 tps which is far more than the other blockchain mechanism. The graph is plotted which shows TPS of each cryptocurrency mechanism in Figure 6.

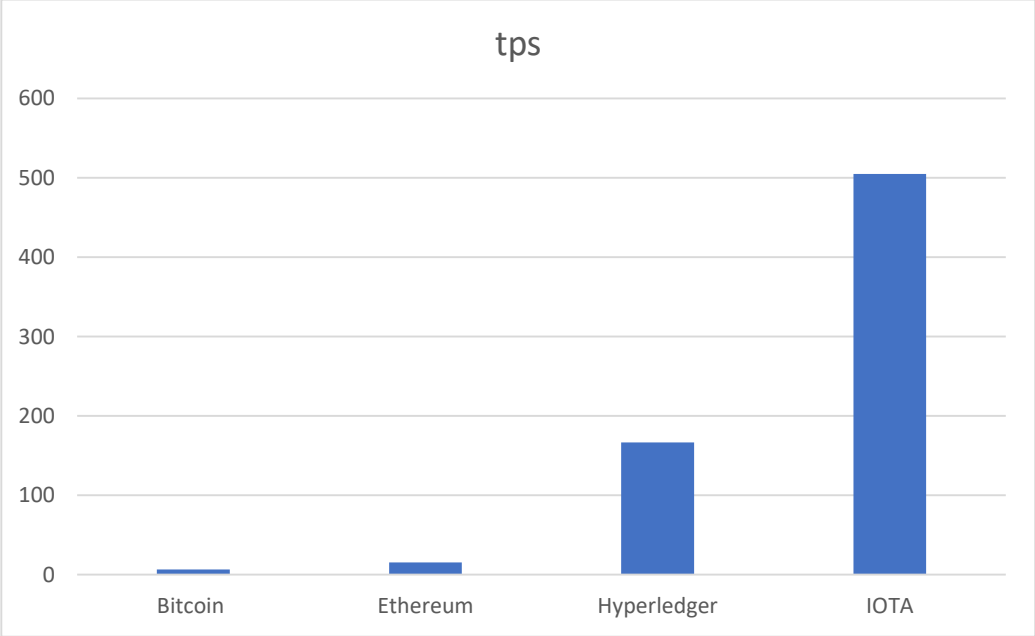


Fig-6 Comparison of each cryptocurrency transaction per second

## VII. Conclusion

The IOTA ensures that the integrity of the data is preserved. This technique is providing the security to the data from the source without intervention of the adverse entity. It also provides the transparency between the two peers who are connected to each other. The main purpose of IOTA is to provide the security to the data stored on the cloud and local storage which can be compromised by any attacker. The IOTA transactions are much faster than the other blockchain technology. The scalability of the network far better than the Blockchain.

## References


[1] Mirza Furqaanbeg, Gayatri Pandi, IOT-BLOCKCHAIN- REVIEW, SECURITY REQUIREMENT AND CHALLENGES, journal of Emerging Technologies and Innovative Research (JETIR), November-2018, volume-5, Issue-11,Page no: 604-613, http://doi.one/10.1729/Journal.18858

[2] Göran Pulkkis, Jonny Karlsson, and Magnus Westerlu. (2018). Blockchain-Based Security Solutions for IoT Systems. *Internet of Things A to Z: Technologies and Applications*, 255-273.

[3] Pradip Kumar Sharma, Jong Hyuk Park. (2018). Blockchain based hybrid network architecture for the smart city. doi:https://doi.org/10.1016/j.future.2018.04.060

[4] TIAGO M. FERN`NDEZ-CARAMÉS, & PAULA FRAGA-LAMAS. (2018). A Review on the Use of Blockchain for the Internet of Things. *6*, 32979-33001.

[5] Yash Gupta, & Rajeev Shorey, Devadatta Kulkarni and Jeffrey Tew. (n.d.). The Applicability of Blockchain in the Internet of Things. 561-564.

[6] S. Popov, IOTA: the tangle (2018). https://assets.ctfassets.net/r1dr6vzfxhev/2t4uxvsIqk0EUau6g2sw0g/45eae33637ca92f85dd9f4a3a218e1ec/iota1_4_3.pdf

[7] Crypto currency market capitalizations, 2018, https://coinmarketcap.com/

[8] Statistic Portal 2019, https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

[9] Ashwini , k., & sonali , b. (2018). SURVEY ON INTERNET OF THINGS (IOT) SECURITY ISSUES & SOLUTIONS. *Proceedings of the Second International Conference on Inventive Systems and Control (ICISC 2018)*, 307-312.

[10] Caciano Machado, Antonio Augusto Frohlich. IoT Data Integrity Verification for Cyber-Physical System using blockchain. 2018 IEEE 21st International Symposium on Real-Time Distributed Computing, DOI**:**10.1109/ISORC.2018.00019, pages 83-90.

[11] Bin Liu, Xiao Liang Yu, Shiping Chen, Xiwei Xu, Liming Zhu. Blockchain based Data Integrity Service Framework for IoT data. 2017 IEEE 24th International Conference on Web Services, DOI**:** 10.1109/ICWS.2017.54, pages 468-475.

[12] Vidhya Ramani, Tanesh Kumar, An Braeken, Madhusanka Liyanage, Mika Ylianttila. Secure and Efficient Data Accessibility in Blockchain based Healthcare Systems. ResearchGate.2018.

[13] Zijian Bao, Wenbo Shi, Debiao He, Kim-Kwang Raymond Choo. IoTChain: A Three-Tier Blockchain-based IoT Security Architecture, arxiv.org/abs/1806.02008v2.2018.pages 1-24

[14] Mohamad Badra, Rouba Borghol. Long-term integrity and non-repudiation protocol for multiple entities. Sustainable Cities and Society.2018 elsevier. https://doi.org/10.1016/j.scs.2017.11.023,pages 189-193.

[15] IOTA, https://commodity.com/cryptocurrency/iota/

[16] IOTA, https://www.mobilefish.com/download/iota/what_is_iota_part1.pdf

[17] Manisha, Dr.Jasvinder Kaur, Improving Data Integrity Using Blockchain Technology, International Journal of Electronics Engineering, volume-10, Issue-1, pg-315-320, 2018.

[18] Igor Zikratov, Alexander Kuzmin, Vladislav Akimenko, vicktor Niculichev, Lucas Yalansky, Ensuring Data Integrity Using Blockchain Technology, PROCEEDING OF THE 20TH CONFERENCE OF FRUCT ASSOCIATION, pg-534-539.

[19] Jun Hak Park, Jun Young Park, Eui Nam Huh, Blockchain Based Data Logging and Integrity Management System for Cloud Forensic, ICCSEA, WiMoA, SPPR, GridCom, CSIA, pg-149-159, 2017.