A Blockchain Solution based on Directed Acyclic Graph for IoT Data Security using IoTA Tangle

Mohan Bhandary
Department of Electronics and Telecommunication Engineering
Bharatiya Vidya Bhavan's
Sardar Patel Institute of Technology
Andheri (W), Mumbai, India
mohan.bhandary@spit.ac.in

Manish Parmar
Department of Electronics and Telecommunication Engineering
Bharatiya Vidya Bhavan's
Sardar Patel Institute of Technology
Andheri (W), Mumbai, India
manparmar@yahoo.in

Dayanand Ambawade
Department of Electronics and Telecommunication Engineering
Bharatiya Vidya Bhavan's
Sardar Patel Institute of Technology
Andheri (W), Mumbai, India
dd_ambawade@spit.ac.in

Abstract—**The growth of the Internet of Things (IoT) has recently seen an exponentially rise with the number of IoT devices been connected increasing in billions, but with such rapid demand and growth, IoT still faces few issues like data security, privacy, data integrity, authentication. The Distributed Ledger Technology like Blockchain also opens a wide range of opportunities, and it proves to be one solution for overcoming multiple issues. This paper highlights the use of Blockchain technology in the field of Internet of Things (IoT) and its practical limitations. The paper focuses on a new distributed ledger technology based on Directed Acyclic Graph(DAG) approach called IOTA, its working and features are discussed in detail. IOTA technology can overcome the practical limitations of classical Blockchain, and the implementation of IOTA for secure transferring of IoT sensor data is alsodiscussed.**

Index Terms—**Internet Of Things (IoT), Distributed Ledger Technology (DLT), Blockchain, IOTA, Tangle, Masked Authenticated Messaging (MAM), Directed Acyclic Graph (DAG).**

I. Introduction

The Internet of Things (IoT) being one of the most significant technologies of the Industry 4.0 revolution. There are various predictions that the number of IoT devices connected will grow above 25 billion by 2020, which is way more than the number of the device which was deployed in the year 2009 [7]. This exponential growth of the IoT devices opens a path to a wide range of applications ranging from automation, asset tracking, defense applications, supply chain, wearable technology, medical applications and other. Internet of Things has made our life a lot easier with the various smart application including healthcare, agricultural applications, smart cities and others. Internet of Things consists of a network of various connected devices, mostly controlled by a central node, which collects data or interacts with the external environment and communicates the collected data with each other.

As the number of IoT devices been deployed are increasing exponentially, there are few issues of this system that needs to be solved; The device mentioned above are mostly small sensors which normally are resource constraint devices with low power consumption, limited memory and limited computational power, thus for carrying out tasks with heavier computational requirements, some additional node is required. For this purpose, most of the IoT systems use another central device which is capable of performing the required extra computation which also controls many devices in the IoT network.

Considering the continuously increasing number of IoT device being deployed, security aspects and management of these devices are becoming a challenge. As these are resource constraint devices most of its processing ability and power is used while performing the primary functions for which it is been implemented, thus making security and privacy aspects challenging to implement. [4], [5] Also use of any heavy cryptography approaches are hard to implement becauseof the limited resource of these devices. Also, there exist other issues like the tracking of the device , device security, maintenance along-with the security and privacy issues of the data been transmitted and developing a resilient and more robust ecosystem for the device to work.

Another most significant and disruptive technology of the Industry 4.0 Revolution is the Blockchain Technology (BCT), been the technology behind the cryptocurrency named Bitcoin, continues gaining popularity since 2008, when Satoshi Nakamoto published the white paper of Bitcoin [3]. The Blockchain Technology has gained popularity as a disruptive technology because of it unique properties not only in the domain of cryptocurrency but across various domains including healthcare, finance, supply chain management, security services, IoT and many other. Also it is noteworthy that the number of research on Blockchain Technology has greatly increased involving individuals like researchers, developers,

978-1-7281-5371-1/20/$31.00 ©2020 IEEE

experts and many companies for further exploring the potentials of this disruptive technology and its possible use in various domains. A Blockchain is a distributed ledger technology which provides a tamper-proof, secured, shared and distributed ledger or database which is capable of tracking resources without any need of a trusted centralized party or a third party. The Blockchain provides communication among two parties in a peer-to-peer network (P2P) for exchanging resource, but the major decision is taken by all the distributed peer-to-peer nodes rather than by a single central entity. The Blockchain is categorized into two types: Permissionless Blockchain and Permissioned Blockchain. A Permissionless Blockchain (e.g., Ethereum, Bitcoin), as the named suggest it has no permission requirements for joining the blockchain network, it is open to public where participants can remain anonymous and the decision of validation is done by all or majority of the participating entities. Whereas a Permissioned Blockchain allows only the authenticated/authorized user to join the blockchain network, normally the participants know all or most of the other participants in the network. [6] The Blockchain Technology been decentralized in nature provides features like security, privacy, monitoring / tracking, immutability, transparency which ensures the integrity, confidentiality, privacy, and authentication in a application. It is this decentralized nature and the set of properties of the Blockchain Technology which has attracted many researchers to further explore its potential in solving the existing issues or limitations of the current IOT systems, as highlighted previously, to integrate IOT and Blockchain. But still some researches based on the objective of integrating IOT and Blockchain focuses more on the conceptual part but only few works based on this topic are at an initial phase of the integration.

In this paper, a Blockchain Technology solution for Internet Of Things (IoT) system is presented with an aim of overcoming the above mentioned limitation or issues of existing IOT systems. As mentioned previously about the features of the Blockchain technology mentioning few like decentralization, immutability, availability, tracing and tracking, integrity, smart contracts has made it emerge as an disruptive technology and suitable for IOT applications. The following section discusses few research papers which analyzes the use of blockchain in the domain of IOT and shows how blockchain could be used to overcome the limitations of the existing IOT systems. In this paper, mainly focus on using IOTA Technology for IOT systems, which is a new distributed ledger technology based on directed acyclic graph (DAG) approach, also known as a DAG based Blockchain Technology. In its following sections, the details of the IOTA technology and the implementation of IOTA for ensuring security and privacy while transfer of IoT sensor data is discussed.

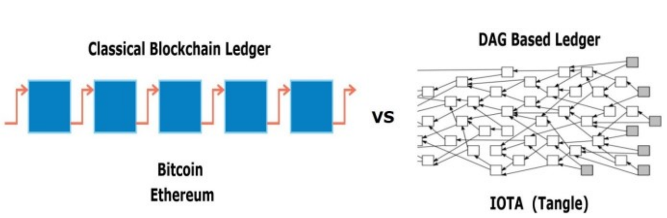


Fig. 1. Classical Blockchain vs DAG Based Ledger Technology

II. LITERATURE SURVEY

The research papers briefed in this sections gives a glimpse of the Blockchain Technology and also focuses on possible use of Blockchain Technology in the domain of Internet of Things (IOT) applications. However, most of the researches paper discussions are still as the theoretical or initial level and less number of papers presented from the implementation point of view.

[1], [2] represents an overall detail of the Blockchain technology, its features & potentials, while also briefly discussing various areas Blockchain has made an impact, like Banking, Supply chain management, Insurance industry, Government, Voting, Healthcare, Energy Management, and others, also highlighting few major concerns of the blockchain technology. [4], [5] presents a systematic literature review, analyzing the use of Blockchain technology for IOT applications, also highlighting the issues of the existing IOT system and the area which needs to be researched. These papers highlights point like privacy, security, energy efficiency, throughput and latency, computational expense and bandwidth overhead of Blockchain and many other, which are main concern areas for IOT systems. Also suggested using a directed acyclic graph (DAG) approach of Blockchain for IOT applications. [8] The author in this research presents how blockchain along with smart contracts can be used in an IOT applications and also a framework with the example of pharmaceutical sector application is presented ensuring transparency and security. [9] The paper focuses on the security and privacy aspects of blockchain and also shows the implementation of a digital signature based on RSA (Rivest, Shamir, and Adelman) for blockchain which can ensure authentication and confidentiality while transferring data. [10] The author in this paper explains the blockchain as a layered model and explains it various functions and applications and different consensus algorithms. [11], [12], [13], [14] In these papers, authors explain how IOT can be benefited from Blockchain Technology and described the infrastructure for blockchain based IOT systems and highlights how IOT security can be strengthened with the use of Blockchain technology. These research papers mainly focuses on how the security and privacy of an IOT system can be improves by Blockchain technology. The authors in [14] has described a framework for the improved security of IOT systems which is built upon blockchain concept such that the data is protected at every level of the system.

[15] This research paper presents the importance of consensus mechanism in blockchain and also compares two popular mechanism called proof of work (PoW) and proof of stake (PoS) and higlights the limitations they face while been used for IOT scenarios like computation power requirement, transaction fee, throughput limitation, confirmation delay. The

paper also discusses DAG based Blockchain technologies named IOTA and Hashgraph and their comparison. [15], [17], [18], [20] These research papers explains that a DAG based Blockchains are much more better fit for IOT application than the classical Blockchains. The papers also presents different DAG based Blockchain, like IOTA, DagCoin, and others, and highlighting the difference between them. Most of these paper presents IOTA as a the best fit for IOT system as it offers free data transfer, ensures integrity and also provides protection from classical blockchain attacks like double spending, quantum attacks above all it overcomes most of the limitation that hinders classical blockchain to be used for IOT system.

By analyzing the above research papers, understood that for IOT systems which normally consists of resource constraint devices and there exists a huge amount of data transfer between the devices, the Classical Blockchain approach wont be feasible because of its limitations, mostly in the way it works, like mining process, presence of transaction fees, transaction approval rate, no provision for transferring micro transactions or very small amount of currency and other, which hinders Classical Blockchain Technology to be used for IOT system. Whereas a Directed Acyclic Graph (DAG) based Blockchain seems to be a feasible solution as these approaches wont face the same problems as that of the Classical Blockchains. Few papers above discussed various DAG based Blockchains, out of which IOTA Technology is focused mainly because of the advantages that it provides like there are no fees for transferring data from source to destination and also scalability is not an issue in IOTA, which are explained in the following section.

III. IOTA Technology

IOTA is an open source distributed ledger technology, which is based on Directed Acyclic Graph (DAG) approach for storing every transaction, officially launched around 2018. The IOTA technology [19] provides the service of securely transferring data / currency between any connected devices / parties with no need of transaction fees i.e. can send x amount of currency and receive exactly the x amount of currency with no extra fee been paid. The IOTA is a cryptocurrency mainly focused for the Internet of Thing(IOT) economy and machine to machine communication. Its the drawbacks of the Bitcoin or more precisely the Blockchain which has led to the foundation of IOTA, which a DAG based Blockchain Technology.

IOTA, meaning infinitesimally small in Greek, it is what exactly it provides i.e. the possibility of performing micro-transactions. As IOTA's underlying architecture is the Directed Acyclic Graph (DAG) structure which is called as Tangle [21] by the IOTA foundation, and there are no concepts of block or chain, instead the individual transactions are interconnected with each other forming a DAG structure. As new transactions keep adding, got a continuous streamline of individual transaction which are interlinked with one another. The IOTA works on trinary logic system which has three states -1,0,1 instead of two sates 0 and 1 as that of the binary system followed by various cryptocurrencies like Bitcoin or Ethereum. IOTA system units are measured in trytes and trits analogous to bytes and bits in a binary system. Also considering blockchain which has the mining process for adding the valid block to the network but in IOTA for validation of transaction happen in a different way i.e a new transaction has to validate previous two transactions for it to be added to the DAG structure. It is due to this reason that there is no need of miners and so there exists no transaction fees. And yet IOTA provides the same fundamental functions as that of the blockchain technology which are: being a distributed ledger/ database, a P2P network,depends on a consensus and validation mechanism.The Tangle is a DAG structure, consisting of: nodes:- entities that performs issuing and validation of transactions; genesis transaction:- At the beginning, it is the first transaction which has all the IOTA token; transactions:- contains IOTA tokens or data to be exchanged.

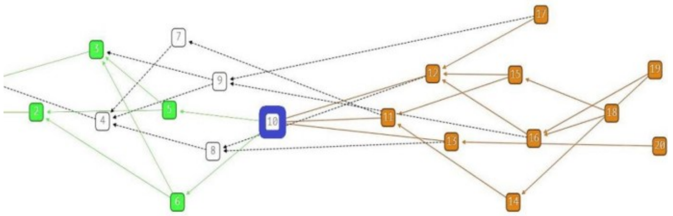


Fig. 2. Representation of IOTA Tangle

The underlying DAG structure of the IOTA Tangle consists of transactions at the vertices , while the edges functions like the reference link between the transactions(Refer Fig.2). The graph begins with the Genesis transaction which is approved directly or indirectly by all the incoming transactions. The new incoming transactions, are called as Tip, which are the unconfirmed transaction has not been yet approved by any other transactions.

Fig. 2 represents a Tangle graph. Here tips, which are the unconfirmed transactions at the right most side. Considering the highlighted blue coloured transaction, the green coloured transaction are approved directly or indirectly by the highlighted transaction where as the orange coloured transactions are the transactions which directly or indirectly approve the highlighted transaction.

The working of IOTA tangle: while adding or issuing any new transactions to the tangle the user has to approve previous two transactions, this provides some additional security to the network. When a transaction has more amount of approval then that transactions can be added to the tangle without any uncertainty. The nodes randomly selects unconfirmed tip for attaching the new incoming transaction, which follows a tip selection algorithm called as Markov Chain Monte Carlo (MCMC). The idea behind MCMC is to deploy some random walkers deep into the Tangle, and let these random walker randomly traverses through transactions in the Tangle towards the tips of the Tangle [19]. At the end, the tip on which the walkers stopped are used for attaching the new incoming transaction. This tip selection algorithm makes sure that most of the unconfirmed transactions are selected for attaching new transactions rather than the previously confirmed transactions, thus ensuring that unconfirmed transactions gets confirmed with time. Also the nodes check for any conflicting transaction, while approving a transaction and if any conflicting transaction exists then that transaction is not approved, which prevents the double spending transactions.

The features of the IOTA Technology are as follows:-

- Highly Scalable :- As the number of transaction increase, there will be more transaction available for approving the previous transaction, thus transaction approving rate increasing.
- Zero-fee transactions :- As there are no miners in IOTA, there exists no transaction fees, which enables us to perform micro-transaction, i.e. transaction of 1 cent is possible.
- Quantum Immune :- For preventing attackers from stealing the users IOTA tokens, IOTA make use of a quantum robust signature scheme, named Winternitz one time signature scheme [22].
- Secure data transfer :- Every data transferred using IOTA is encoded due to which the data storage , data transfer or reference are secured.
- Low resource requirements :- As IOTA is designed primarily for IOT device which are resource constraint devices, thus it would require low resources.

A. MASKED AUTHENTICATED MESSAGING (MAM)

The Masked Authenticated Messaging (MAM) is an outstanding feature and an important step focusing on securing the transfer of the data stored on the IOTA Tangle Technology.The research team of the IOTA foundation continues to improve this module and its still reviewed for enhancing its functionality. This module derives its name from its basic functions that it provides :

- "Masked" : the message been transferred is encrypted;
- "Authenticated" : the message is verified and confirmed to be coming from authorized node;
- "Messaging" : the node publishes data as a continuous stream of messages over the Tangle.

The Masked Authenticated Messaging (MAM) is a protocol provisions secure transferring and accessing of encrypted or masked data stream, which consists of messages transferred by zero value transactions, on the Tangle. [24], [25], [28] Using the MAM module, the nodes or devices connected to the IOTA Tangle can broadcast their messages, in an encrypted form, into a "Channel". The nodes interested in a message should subscribe to the channel with an appropriate authentication keys for accessing the channel and receiving the message. This process can be real time if the subscriber is listening to the channel, as they may receive the message as soon as the sender publishes the message. When a sender publishes a new message a corresponding Merkle tree is generated for every single message. The Merkle tree is used to create the MAM channels and the messages of this channel are signed with the private keys of the Merkle tree leaves.

The Channel acts as a stream of messages, which is normally a zero value transaction, and all messages are signed with Merkle tree signature scheme and its root becomes the Channel ID of the MAM channel. [27] Every message in the channel has a reference to the next message in the channel such that when one access a message in the channel, they can also find the next subsequent messages in the channel. This allows messages stream flow to be in a single direction providing an additional kind of forward secrecy as user does not have any information of previous messages but only of the future messages.

After the subscriber receives a MAM stream messages, its signature is checked for its validity and checked whether this signature matches any one of the signature of the Merkle Tree leaf and then the message is decrypted. Where as if the received message signature is invalid, then the message is not decrypted or is considered invalid.

The Masked Authenticated Messaging (MAM) provide three different mod:- Public mode, Private mode, Restricted mode, and with these different modes a sender has more control of the data accessibility in the MAM channel. The three MAM modes are explained below in briefly :-

- Public MAM Mode:- This Mode uses the address of transaction which is same as the root of the Merkle Tree. Here, if the address is there then can access and decrypt the message sent through the MAM channel as the address and root of the Merkle tree is identical.
- Private MAM Mode:- In this Mode, the addresses used by the transactions are obtained by hashing the root of the Merkle Tree. Thus, only if the root of the Merkle Tree is known, the address can be calculated and the message can be accessed.
- Restricted MAM Mode:- In this Mode, the addresses used by the transaction are obtained by the hash of the root of the Merkle tree and an authentication factor (called as side key). The side_ key adds an additional factor of security. That means for accessing the message both the key and the root is required, as the messages are encrypted with key. Thus, with a exact same side_ key, the message can be decrypted.

IV. SYSTEM IMPLEMENTATION

The work proposed in this paper focuses on the use of the MAM feature of IOTA Tangle for securing the transmission of IOT sensor data and which ensures the authenticity and confidentiality of the data been transferred. As the IOT systems are used in various applications, thus depending on the application and also on what kind of data is transferred between parties, there is need of ensuring data privacy and security i.e. integrity and confidentiality also authentication need to be maintained so that any attacker cannot tamper or eavesdrop the data. The idea of this proposed work is to provide a single solution for ensuring confidentiality, integrity

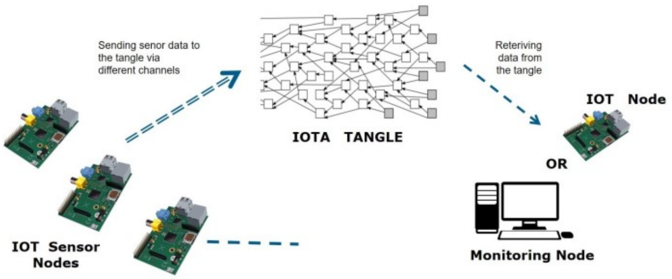
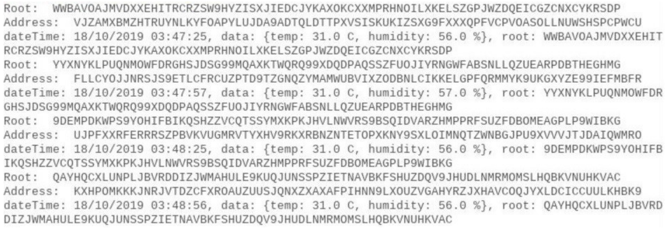

Sending senor data to the tangle via different channels
IOTA TANGLE
Reteriving data from the tangle
IOT Node
OR
Monitoring Node
IOT Sensor Nodes

Fig. 3. Implementation Architecture

and authentication of the data been transferred. Particularly, in application like Healthcare, Government and other where data privacy and security are main concerns, the IOT data collected by the sensors need to secured, thus for this purpose the IOTA Tangle can be used.

The IOTA Reference Implementation(IRI) [23], maintained by the IOTA Foundation, is an open source software module developed using Java for experimenting and implementing IOTA protocols for secure transferring of data or tokens between the network participants or nodes. The IRI software helps machines to connect to the IOTA network and act as a node, which has functions such as to validate the transactions, store these validated transactions on to the Tangle and also retrieve the transaction back from the Tangle whenever needed.

The [25] Masked authenticated messaging(MAM) feature of IOTA which allows only the authenticated entities to exchange data in the form of encrypted messages thorough which the integrity, confidentiality and authenticity of the data transfer can be maintained. In this demonstration, (Refer Fig. 3) used raspberry pi,with internet connectivity, to act as IOT node for sending & receiving the messages and collected data from the sensor, all the code were written in javascript and the details of the IOTA network address, MAM mode and side__key and other details were hard coded in the implementation codes. The work was carried out on an open source runtime environment Node.js, running on the raspberry pi, initially the node will connect to the IOTA network, normally the dev.net is used for testing and development purposes instead of the main-net, where the actual solutions are deployed for different application. After connecting to the IOTA development network, the node collects the sensor data and the publishes the sensor data to Tangle and the receiver with the root and the appropriate side_key can receive this data for further processing. Later for monitoring purpose or for processing those data, any change or modification in sensor data can cause problem in the actuation process. In this implementation, the Restricted MAM mode is used , so the sending node must share the root and the side_key with the receiving node for it to get the sent message. In this implementation, the proposed idea of securing the IOT data transfer was successfully implemented and obtained the published data after the retrieving it from the Tangle.



```
Root:  WWBAVOAJMVDXXEHITRCRZSW9HYZISXJIEDCJYKAXOKCXXMPRHNOILXKELSZGPJWZDQEICGZCNXCYKRSDP
Address:  VJZAMXBMZHTRUYNLKYFOAPYLUJDA9ADTQLDTTPXVSISKUKIZSXG9FXXXQPFVCPVOASOLLNUWSHSPCPWCU
dateTime: 18/10/2019 03:47:25, data: {temp: 31.0 C, humidity: 56.0 %}, root: WWBAVOAJMVDXXEHIT
RCRZSW9HYZISXJIEDCJYKAXOKCXXMPRHNOILXKELSZGPJWZDQEICGZCNXCYKRSDP
Root:  YYXNYKLPUQNMOWFDRGHSJDSG99MQAXKTWQRQ99XDQDPAQSSZFUOJIYRNGWFABSNLLQZUEARPDBTHEGHMG
Address:  FLLCYOJJNRSJS9ETLCFRCUZPTD9TZGNQZYMAMWUBVIXZODBNLCIKKELGPFQRMMYK9UKGXYZE99IEFMBFR
dateTime: 18/10/2019 03:47:57, data: {temp: 31.0 C, humidity: 57.0 %}, root: YYXNYKLPUQNMOWFDR
GHSJDSG99MQAXKTWQRQ99XDQDPAQSSZFUOJIYRNGWFABSNLLQZUEARPDBTHEGHMG
Root:  9DEMPDKWPS9YOHIFBIKQSHZZVCQTSSYMXKPKJHVLNWVRS9BSQIDVARZHMPPRFSUZFDBOMEAGPLP9WIBKG
Address:  UJPFXXRFERRRSZPBVKVUGMRVTYXHV9RKXRBNZNTETOPXKNY9SXLOIMNQTZWNBGJPU9XVVVJTJDAIQWMRO
dateTime: 18/10/2019 03:48:25, data: {temp: 31.0 C, humidity: 56.0 %}, root: 9DEMPDKWPS9YOHIFB
IKQSHZZVCQTSSYMXKPKJHVLNWVRS9BSQIDVARZHMPPRFSUZFDBOMEAGPLP9WIBKG
Root:  QAYHQCXLUNPLJBVRDDIZJWMAHULE9KUQJUNSSPZIETNAVBKFSHUZDQV9JHUDLNMRMOMSLHQBKVNUHKVAC
Address:  KXHPOMKKKJNRJVTDZCFXROAUZUUSJQNXZXAXAFPIHNN9LXOUZVGAHYRZJXHAVCOQJYXLDCICCUULKHBK9
dateTime: 18/10/2019 03:48:56, data: {temp: 31.0 C, humidity: 56.0 %}, root: QAYHQCXLUNPLJBVRD
DIZJWMAHULE9KUQJUNSSPZIETNAVBKFSHUZDQV9JHUDLNMRMOMSLHQBKVNUHKVAC
```

Fig. 4. Terminal output while Publishing the Sensor Data to the Tangle

V. RESULTS AND DISCUSSION

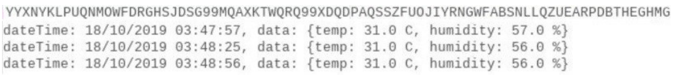
- Step I :- Collecting sensor data and Publishing the data to the Tangle

Here, used a Raspberry Pi, to act as an send- ing/publishing node. After the node gets connected to the IOTA network and collects the sensor data at regular pre- defined intervals, it then publishes this collected sensor data to the IOTA Tangle using the MAM feature. After the node collects the sensor data, it is accurately time-stamped and, then an encrypted message is created utilizing the root and side_key. This encrypted message is then published to the Tangle.

For verification purpose, the root of the Merkle tree and the address obtained along-with the data published is displayed on the terminal of the raspberry pi, after the data was published and attached to the tangle successfully.(Refer fig.4) It was observed on the Raspberry pi terminal, that the every data was sent with a different root indicating that every single data is processed as a new message in the MAM channel and corresponding Merkle tree is created whose root is used for encryption using the side_key; also each message has a reference to the next message which has the next sensor data.

- Step II:- Retrieving the Published Data from the Tangle

For receiving the published message, the node connected to the IOTA network must have the Merkle tree root and the side_ key used while publishing the message and used another Raspberry Pi, to act as a receiving node, which is also connected to the IOTA network using the IRI. The MAM mode used and the side_key used are hard coded in the receiver implementation codes. When a single MAM message is retrieved from the Tangle using the Merkle tree root and the side_key, got the next subsequent messages as every message has a reference to the next message in the MAM channel but no reference to the previous messages. This continues till the sender keeps publishing the sensor data to the Tangle. (Refer fig. 5) It was observed on the receiving Raspberry Pi terminal, that when a appropriate root was provided, the corresponding messages were received continuously from the Tangle in the same order in which



```
YYXNYKLPUQNMOWFDRGHSJDSG99MQAXKTWQRQ99XDQDPAQSSZFUOJIYRNGWFABSNLLQZUEARPDBTHEGHMG
dateTime: 18/10/2019 03:47:57, data: {temp: 31.0 C, humidity: 57.0 %}
dateTime: 18/10/2019 03:48:25, data: {temp: 31.0 C, humidity: 56.0 %}
dateTime: 18/10/2019 03:48:56, data: {temp: 31.0 C, humidity: 56.0 %}
```

Fig. 5. Terminal output while Receiving the Sensor Data from the Tangle

they were published. Also it was observed that any previous data were not retrieved from the Tangle as mentioned earlier. Alternatively instead of a receiving node, a monitoring system can also be setup which can receive the tamper-proof data in the MAM messages for monitoring purposes, without any doubt about its integrity and authenticity.

Considering the security and privacy aspects of the implementation, as the IOTA technology uses Winternitz one time signature scheme [22] which is quite robust to even quantum computers. Generally, quantum computers are considered as a threat to most of the cryptocurrencies and also to several cryptography algorithms, due to their computing ability. Also for hashing the data, IOTA uses Kerl hash functions which is a modified version of the Keccak SHA3-384 hash function. Considering the transferring of data using the Masked authenticated messaging(MAM) [27] of IOTA, which employs Merkle Tree based signature scheme for encrypting the messages which is generally used along-with the IOTA security aspects which were mentioned above, thus providing both security and the privacy characteristics. It should also be noted that the use of Blockchain in IOT system is not the solution for all IOT application but is only suitable for few specific applications which has higher security and privacy requirement like Healthcare, Government applications and other.

VI. CONCLUSION

Though Blockchain has impacted various domain with its disruptive features in few domains like IoT and M2M communication, there arise few noteworthy limitations. The DAG-based Distributed Ledger Technology IOTA serves the purpose of providing security and privacy along-with few additional features to an IoT system while solving the existing issues of the IoT systems. This paper discussed IOTA Technology and its working in detail. Also, successfully demonstrated tamper-proof and secure transferring of IoT sensor data using the Masked Authenticated Messaging (MAM) of IOTA which ensures data confidentiality and data authentication. The use of IOTA technology in the IoT systems ensures the the system is reliable highly scalable and is resilient to quantum computer attacks. Considering IOTA Technology, further research work is needed in the direction for enhancing the transaction rate, to handle the high rate IOT data more smoothly and also the development of different robust consensus mechanism is needed.

VII. ACKNOWLEDGMENT

I would like to express my respect and gratitude to the Management and all the faculties and supporting staffs of the Department of Electronics Telecommunication Engineering, S.P.I.T., Andheri(W), Mumbai for providing me with the opportunity to work in the domain of Distributed Ledger Technology and Internet Of Things and alongside providing the required encouragement, technical guidance and support throughout the research work timeline. I would also like to heartily thanks my parents, friends and colleagues for their encouragement and support.

REFERENCES

[1] Q. K. Nguyen and Q. V. Dang, ”Blockchain Technology for the Advancement of the Future,” *4th International Conference on Green Technology and Sustainable Development*, Ho Chi Minh City, pp. 483-486, 2018.

[2] Q. E. Abbas and J. Sung-Bong, ”A Survey of Blockchain and Its Applications,” *International Conference on Artificial Intelligence in Information and Communication* , Okinawa, Japan, 2019, pp. 001-003.

[3] S. Nakamoto. ,”Bitcoin: A Peer-to-Peer Electronic Cash System”, 2008.

[4] S. K. Lo et al., ”Analysis of Blockchain Solutions for IoT: A Systematic Literature Review,” in *IEEE Access*, vol. 7, pp. 58822-58835, 2019.

[5] T. M. Fernandez-Carames and P. Fraga-Lamas, ”A Review on the Use of Blockchain for the Internet of Things,” in *IEEE Access*, vol. 6, pp. 32979-33001, 2018.

[6] A. Banafa, ”Secure and smart Internet of Things (IoT)”, *River Publishers*, pp. 69-92, 2018.

[7] ”MARKET PULSE REPORT, INTERNET OF THINGS (IoT)”, *Growthenabler.com*, 2017.

[8] Sivaganesan D.,”BLOCKCHAIN ENABLED INTERNET OF THINGS”, *Journal of Information Technology*, 1(01), 1-8, 2019.

[9] Suma, V. (2019). SECURITY AND PRIVACY MECHANISM USING BLOCKCHAIN”, *Journal of Ubiquitous Computing and Communication Technologies (UCCT)*, 1(01), 45-54, 2019.

[10] A. F. Zorzo, H. C. Nunes, R. C. Lunardi, R. A. Michelin and S. S. Kanhere, ”Dependable IoT Using Blockchain-Based Technology,” *Eighth Latin-American Symposium on Dependable Computing* , Foz do IguaA˜ §u, Brazil, pp. 1-9, 2018.

[11] M. Singh, A. Singh and S. Kim, ”Blockchain: A game changer for securing IoT data,” *IEEE 4th World Forum on Internet of Things* , Singapore, pp. 51-55, 2018.

[12] S. Roy, M. Ashaduzzaman, M. Hassan and A. R. Chowdhury, ”Blockchain for IoT Security and Management: Current Prospects, Challenges and Future Directions,”*5th International Conference on Networking, Systems and Security* , Dhaka, Bangladesh, 2018, pp. 1-9.

[13] B. H. AlDoaies and D. H. Almagwashi, ”Exploitation of the Promising Technology: Using Blockchain to Enhance the Security of IoT.,” *21st Saudi Computer Society National Computer Conference*, Riyadh, pp. 1-6, 2018.

[14] K. N. Krishnan, R. Jenu, T. Joseph and M. L. Silpa, ”Blockchain Based Security Framework for IoT Implementations,” *International CET Conference on Control, Communication, and Computing (IC4)*, Thiruvananthapuram, pp. 425-429, 2018.

[15] B. Cao et al., ”When Internet of Things Meets Blockchain: Challenges in Distributed Consensus,” in *IEEE Network*,2018.

[16] H. Pervez, M. Muneeb, M. U. Irfan and I. U. Haq, ”A Comparative Analysis of DAG Based Blockchain Architectures,” 12th *International Conference on Open Source Systems and Technologies*, Lahore, Pakistan, pp. 27-34, 2018.

[17] A. Ahi and A. V. Singh, ”Role of Distributed Ledger Technology (DLT) to Enhance Resiliency in Internet of Things (IoT) Ecosystem,” *Amity International Conference on Artificial Intelligence*, Dubai, United Arab Emirates, pp. 782-786, 2019.

[18] B. Shabandri and P. Maheshwari, ”Enhancing IoT Security and Privacy Using Distributed Ledgers with IOTA and the Tangle,” 2019 *6th International Conference on Signal Processing and Integrated Networks*, Noida, India, pp. 1069-1075, 2019.

[19] S. Popov.,”The Tangle”, Version 1.4.3,April 30, 2018.

[20] H. Anwar , ”The Ultimate Comparison of Different Types of Distributed Ledgers:Blockchain vs Hashgraph vs Dag”, 101 Blockchains, 2019.

[21] A. Gal, ”The Tangle: an Illustrated Introduction”, *Medium*, 2019.

[22] Buchmann, Johannes Dahmen, Erik Ereth, Sarah Hulsing, Andreas & Ruckert, Markus, ”On the Security of the Winternitz One-Time Signature Scheme”,*International Journal of Applied Cryptography*, 3.363-378, 2018.

[23] IOTA Foundation, “IOTA Reference Implementation (IRI)”, iotaledger/iri,*GitHub*.

[24] A.B. mushi, ”IOTA: MAM Eloquently Explained”, *IOTA News*, 17-Jun-2019.

[25] ”Overview — Introduction — MAM — Client Libraries — IOTA Documentation”,*Docs.iota.org*, 2020.

[26] C.Aldave, ”Deciphering Masked Authentication Message (MAM),”*IOTA News*, 23-May-2019.

[27] M. A. Lindvall, ”How is authenthicity and confidentiality maintained for MAM channels on the IOTA Tangle?”,2018.

[28] P. Handy, ”Introducing Masked Authenticated Messaging,”, *Medium*, 09-Apr-2018.