A Secure Framework for Communication in Internet of Things Application using Hyperledger based Blockchain

Conference Paper · July 2019

DOI: 10.1109/ICCCNT45670.2019.8944811

CITATIONS
28

READS
966

5 authors, including:

Utkalika Satapathy
International Institute of Information Technology, Bhubaneswar
19 PUBLICATIONS **524** CITATIONS
SEE PROFILE

Bhabendu Kumar Mohanta
K L University
71 PUBLICATIONS **1,917** CITATIONS
SEE PROFILE

Soumyashree S Panda
International Institute of Information Technology, Bhubaneswar
25 PUBLICATIONS **1,115** CITATIONS
SEE PROFILE

Srichandan Sobhanayak
International Institute of Information Technology, Bhubaneswar
25 PUBLICATIONS **713** CITATIONS
SEE PROFILE

A Secure Framework for Communication in Internet of Things Application using Hyperledger based Blockchain

Utkalika Satapathy
Department of CSE
IIIT Bhubaneswar
Odisha, India, 751003
A117010@iiit-bh.ac.in

Bhabendu Ku. Mohanta
Department of CSE
IIIT Bhubaneswar
Odisha, India, 751003
C116004@iiit-bh.ac.in

Soumyashree S Panda
Department of CSE
IIIT Bhubaneswar
Odisha, India, 751003
C117011@iiit-bh.ac.in

Srichandan Sobhanayak
Department of CSE
IIIT Bhubaneswar
Odisha, India, 751003
srichandan@iiit-bh.ac.in

Debashis Jena
Department of CSE
IIIT Bhubaneswar
Odisha, India, 751003
debasish@iiit-bh.ac.in

***Abstract*—In the era of the Internet of Things(IoT) smart devices are connected with wire or wireless way. The IoT devices are capable of sensing the environment and has the ability to transmit that information to the next level. The application area of IoT is Smart city, Smart transportation, Healthcare sector, Agriculture, Monitoring environment. Each of these applications, lots of information are share or transmit among different devices. In the information sharing system among devices, lots of security and privacy challenges exist like data leakage, data modification, device identity. In this paper, authors firstly identify the communication protocols used in IoT application and given their working principle. Secondly, challenges exist in IoT and corresponding Blockchain solution approach are explained, Lastly, the authors proposed a secure architecture based on open Blockchain which can solve some of the challenges in IoT applications.**

***Index Terms*—Communication, Internet of Things, Blockchain,Hyperledger, Security.**

I. Introduction

The IoT devices are growing exponentially and the amount of data getting transmitted is enormous. Hence the major responsibility is to provide security, privacy and protection to the data and communication. Blockchain Technology has been anticipated to make extensive changes in various field like research, industry and also in IoT application. It will play a significant role to manage, control and secure IoT devices. In this paper we proposed a secure architecture based on Hyperledger to solve some of security issues persist in IoT application. The rest of the paper is organised as follows. In Section 2 we have briefly described about blockchain Technology. Several IoT communication protocols has been identified and described briefly in Section 3. This section also outlines the security challenges while doing secure communication in IoT application. Section 4 addressed the challenges by blockchain based solution. The secure architecture using blockchain is proposed in Section 5. At the end the final remarks are given in Section 6.

II. Background

A blockchain system is basically a decentralised, distributed, digital public ledger system. This incorporates a novel distributed consensus schemes, allowing transactions and data to be stored securely to the blockchain network after a verification/validation without intervention of any centralized or third-party authority. When we say, the blockchain is decentralised it means, the services are ruled without any centralised, governing authority. It has been found that one common reason for the major data breach in last few decades is due to storing all the data at one place i.e. at one server which makes easier for a malicious actor to steal the data at once. So, to secure the system, blockchains are made distributed by placing every data in every node making it difficult to modify the data by malicious actor in all the places simultaneously. The blockchain networks keeps the records, also known as blocks submitted by others in temporal order of their creation. The verification of this temporal order are performed by miners which are also the nodes of the same blockchain network by taking the help of timestamp. In order to make the blocks tamper-proof, to ensure data authenticity and integrity, elliptic curve cryptography (ECC) and SHA-256 hashing has been used. A blockhash is created after hashing the list of transactions in a ledger. That blockhash is treated as the unique identifier for that block. When a malicious actor tries to change the history of the transaction of a certain block then the output blockhash will be modified completely making it visible that some tampering has been done with it. When someone wants to add a new block to the blockchain network then, that digital ledger has to be verified by a majority consensus of miner nodes. In the network there are many miner nodes which compete with each other to add the block into the network by doing some computation like solving a complex mathematical puzzle. On winning the competition the node can add the block to the blockchain as a result he/she will receive some reward like digital coins. There are few techniques to know that the list of transactions are truthful such as Proof of stack(PoS) and Proof of Work (PoW) etc. In a bitcoin network [1] , the validation of the block is done by the miners which computes a hash with leading zero to match up the difficulty

[1]https://bitcoin.org/en/how-it-works.

target. After the transactions has been verified the blockdata are immutable i.e. the transactions can never be modified or deleted. Refer to Fig. 1. As blockchain manages and verifies data online hence enabling us to track billions of devices on Internet of Things.

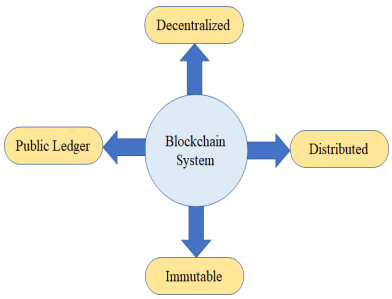

Fig. 1. Characteristics of Blockchain

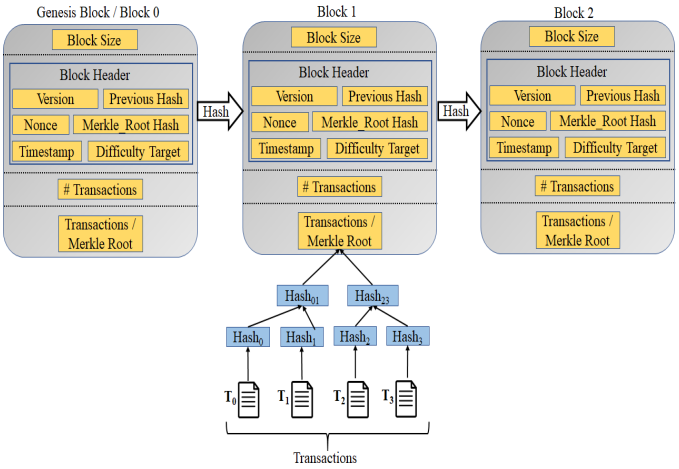

Fig. 2. Design Structure of Blockchain

Table. I shows the type of Blockchain which can be built [1]. Permissionless blockchain also known as public or decentralised blockchain is 100% transparent i.e. one can read everything. In Permissionless algorithm monetary incentives are given to miner and due to the nature of the Proof of Work consensus algorithm , a massive amount of energy is being used. In Permissioned Blockchain which is also known as private blockchain the degree of decentralization and transparency varies depending upon the application it is being used in. That means it can be Fully centralized or Partially decentralized. No crypto economic or monetary incentives are given to running node as no miners required for this. The consensus algorithm is computationally less expensive in permissioned blockchain allowing it to perform and scale better. Both the type of blockchain are secure, distributed databases each having distinct characteristics and adaptability.

The structure of a Block in Blockchain is described in Fig. 2. The basic block is consist of 4 sections. First section contains the block size which is the size of block in bytes. Next is the block header section which store several other information like version which is a number to track the software protocols upgrades, the Previous Blockhash which the hash of the previous entire block, the Merkle Root is the hash of root of Merkle tree. Merkle tree is nothing but the tree formed by all the transaction mentioned in the last section of the block. If any modification or deletion is done to the transactions then the hash of the merkle root will be changed hence it is used for data verification. The Block Header also contains the timestamp, a Difficulty Target which is a Proof of Work (PoW) algorithm and a Nonce which a random variable for the PoW algorithm [2], [3]. The blocktime for Bitcoin [2] and Ethereum [3] is 10 mins and 17.5 s respectively [4]. It is achieved by adjusting the number of leading zeros periodically in the difficulty target with the variation of computation power of hardware over time. The block time is an average time, set for mining a block i.e. making a block valid by the miners, by finding the appropriate value for nonce field.

Bitcoin is the foremost decentralised digital currency based on the blockchain architecture [5]. Its uses cryptographic tools such as cryptographic hash function e.g. SHA256 and RIPEMD160, Merkle Trees and Elliptic Curve Digital Signature Algorithm(ECDSA). Table. II shows the basic block header of the Bitcoin.

In the past few years, many research were focused on services of Bitcoin as a digital cyptocurrency but totally leave unnoticed the hidden potential within Bitcoin, the Blockchain which is the underlying key-enabling technology behind it. Currently there are more than 500 alternate blockchain offering alternative digital crypto currencies are available. Ethereum blockchain was launched by Vitalik Buterin in 2015 and made public. Nevertheless with the developement of Ethereum Blockchain, the prospective use space of blockchain has become countless. To build the distributed consensus Ethereum is a permissionless networks and uses Proof-of-Work (PoW) technology. It runs on smart contracts which are basically a computerised transaction protocol written as simple programming scripts using the Solidity language ,to be uploaded and run on its blockchain. Solidity,a JavaScript like language, is very simple and easy to understand unlike the scripts used in Bitcoin. This is one of the main reason why Ethereum provide a decentralised platform to build Smart application and democratic autonomous organizations (DAOs). The smart contracts can be scheduled to run at a particular time or based on a condition with zero possibility of downtime, fraud, third-party interference and censorship.[4] Eventually, similar smart-contract blockchain platforms have lately emerged. Some of them are Hyperledger[5], Eris [6], Stellar [7], Ripple [8], and Tendermint [9]. Hyperledger Fabric is a private and permissioned

[2]https://en.bitcoin.it/wiki/Block
[3]https://etherscan.io/chart/blocktime
[4]https://www.ethereum.org/
[5]https: //www.hyperledger.org/
[6]https://monax.io/2016/ 04/03/wtf-is-eris/
[7]https://www.stellar.org/develo pers/guides/get-started/
[8]https://ripple.com/network
[9]https://tendermint.com/intro

TABLE I
TYPES OF BLOCKCHAIN

Type	Details	Example of Usage	Characteristics
Permissionless Blockchain (Public or Decentralised Blockchain)	Allows any user to create and access data, Allows any user to publish smart contract, Anyone can run a node.	Bitcoin , Ethereum	Full Transparency, High level of Anonymity, Slow Performance, A major challenge is scaling, Crypto economic incentives are given to miners, Energy inefficient
Permissioned (Private Blockchain)	Not all users are freely allowed to join the network, see the recorded history or issue transactions of their own, A closed ecosystem with the predefined participant, Only pre-approved entities can run nodes	Preferred by Centralized Organizations, Hyperledger	Varying degree of Decentralization and Transparency, No Anonymity, Mining is not required, No need for crypto economic incentive, Consensus algorithms are computationally inexpensive, Increased Performance, Increased Scaling

TABLE II
BITCOIN BLOCK HEADER FORMAT

Field	Description	Size
Version	Block Version number	4 Bytes
Previous Hash	Hash of the previous block Header	32 Bytes
Merkle Root Hash	Transaction Merkel Root Hash	32 Bytes
Timestamp	Unix Timetstamp	4 Bytes
Difficulty Target	Current difficulty of the network	4 Bytes
Nonce	Random Variable to solve PoW	4 Bytes

network used in a specific enterprise environment allowing only previleged node to communicate with each other. To gain access, permission should be granted from a trusted Membership Service Provider (MSP), which provides and validates the certificates and also manages user authentication.

A. Motivation

Internet of Things technology is widely used by different applications. In an IoT application, different sensors are connected to the next layer in either wired or wirelessly. When information is passed from the physical layer to the network layer for processing and performing computation there are lots of security issues exist. The users privacy need to maintain so that trust can be built between users. In the case of the smart healthcare sector, patient privacy needs to be preserved. Similarly in the case of smart city IoT based application citizen personal information needs to be secure. so in this paper, we have proposed a framework based on Blockchain concept which can be addressed the security and privacy issues.

III. INTERNET OF THINGS COMMUNICATION PROTOCOLS

IoT communication is IP-based and it is based on the protocols above the network layer such as HTTP, CoAP, WebSockets, MQTT, XMPP, DDS, AMQP etc., shown in Fig. 3.

A. Application Communication Protocol

- MQTT

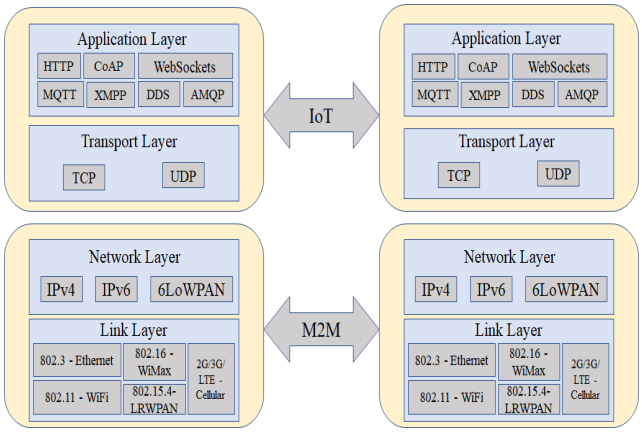

Fig. 3. Protocol Stack of IoT

MQTT (Message Queue Telemetry Transport) is a lightweight publisher/subscriber model based protocol present in application layer. It uses a client-server architecture where IoT device is treated as the client which connects to a proxy server (also known as MQTT Broker) and publishes messages to topics on the server as shown in Fig. 4. The broker publishes the messages to the subscriber of that topic. An environment with limited resources, processing and low network bandwidth, MQTT is well-to-do. MQTT is supported by TCP trasport protocol which is unsecured by default [6]. Hence it uses TSL/SSL for data encryption making the system robust. The drawback of this protocol can be limitation in scalability because of the additional overhead for device connected to a centralised broker.And also the redundant TCP handshaking before every communication set up affects more battery consumption.

- CoAP
  CoAP (Constrained Application Protocol) is one of the latest application layer communication protocol used for M2M (machine-to-machine) application and mainly

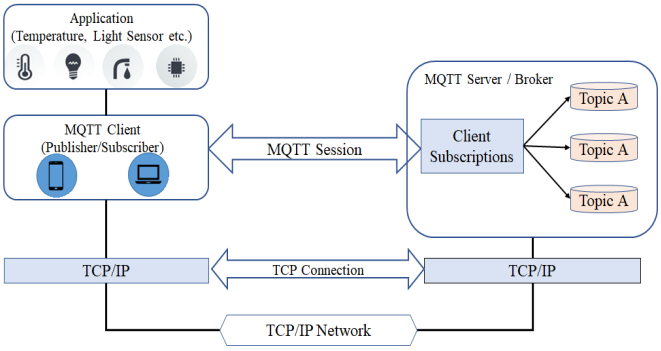

Fig. 4. MQTT Architecture

designed to interface with HTTP protocol easily. It's underlying transport layer protocol is UDP and it follows a Request-Response framework for communication. Basically it is secure because of the use of Datagram Transport Layer Security (DTLS). But it has been found that hundreds of thousands of MQTT and CoAP hosts combined are reachable through public-facing IP addresses. Hence providing attackers with millions of exposed records [7]. CoAP is suspetible to IP Spoofing and DDoS Attack [10].

- XMPP
  In context of IoT, XMPP (Extensible Messaging and Presense Protocol) is a free and open real-time communication protocol used for streaming XML data in small chunks between IoT devices in a network. Client-Server framework is used by this decentralized protocol. XMPP has built-in channel encyption feature using SASL and TLS [8], [9]. [11]

B. Routing Protocol

- 6LoWPAN
  6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks) shown in Fig. 5 which fits the IPv6 packet transmission in low power and lossy network with node have limited processing capabilites [10]. The operating bandwidth is 2.4GHz and data transmission rate is 250Kbps. IPv6 offers around 5 * 1028 addresses for each individual in the world however with the growing rate of IoT devices soon these address space is going to be exhausted. The vulnerability surface of 6LoWPAN protocol includes bootstrapping and key distribution, Dos due to constrained resources and etc. IPv6 Network Security, IPsec is used to protect the network layer [11]. One of the general problem area of 6LoWPAN is security including set up and maintainance. From different security objective of this protocol the obvious one are data integrity which require some form of authorization, confidentiality, availability by dealing with DoS attack and authorization and authentication of devices which wants to communicate.[12]

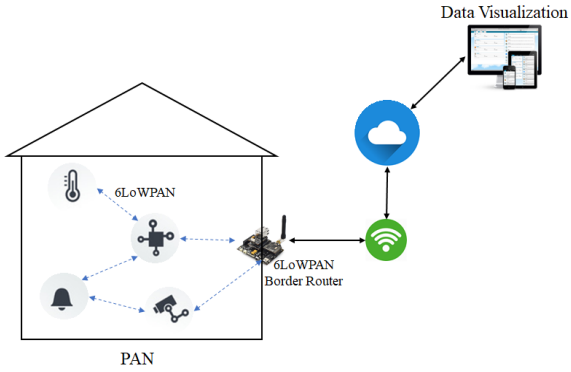

Fig. 5. 6LoWPAN Architecture

C. Security Protocol

- DTLS
  DTLS is a security protocol used to provide privacy in communication implemented above UDP based communication protocols. To intercept tampering, eavesdropping or message forgery in a client/server application this protocol is used. It is based on the TLS protocol and guarantees equal level of security.
- TLS
  In IoT devices the TLS is used in two ways: First, for encryption while data transmission. It makes more difficult for malicious actor to reverse engineer the communication used by device. This preserves data privacy. Second, to mitigate the impersonation attack so that an attacker can not fake a device, the device store the TLS certificate of the client used for the authentication between the device and application. Some issues with TLS implementation are discussed below. TLS is not lightweight and makes the IoT traffic slow due to the extra overhead taken for the initial handshake before the set up of every session. As the IoT devices have limited storage, it is a problem to store the certificate in device when the certificate size is too large. Finally third issue is that some of the protocols that are being developed for IoTs are plaintext by default.

D. Secure Communications

Internet of Things (IoT) is all about connecting the things to the internet. However, communication should be secure and encrypted otherwise all the data, passwords or user names will be exposed to everyone. Basically IoT application faces several security vulnerabilities:

- Data getting stored in an insecure IoT network faces issues with confidentiality and privacy of data.
- To communicate among various types of devices within a heterogeneous network a common standard communication protocol is not available.

[10]https://www.trendmicro.com/vinfo/hk-en/security/news/internet-of-things/mqtt-and-coap-security-and-privacy-issues-in-iot-and-iiot-communication-protocols

[11]https://xmpp.org/about/technology-overview

[12]http://6lowpan.tzi.org/SecurityObjectives

- Inadequate authorization or not enough authentication techniques for IoT devices in the network.

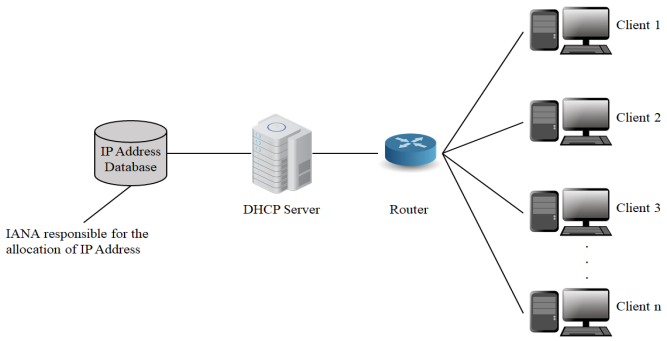

Fig. 6. IP Address Assignment by a central system

The communication protocols in IoT application such as MQTT, CoAP, HTTP and XMPP and the routing protocols such as 6LoWPAN and RPL are not secured by default. To make the communication secure in the application, on the top of these protocols another layer of security protocol has to be implemented such as TLS or DTLS. Likewise, to secure the transport layer routing protocols secure, IPSec is used.DTLS, TLS and IPSec are not lightweight due to the large certificate file that is stored on the resource constrained devices and makes the IoT traffic slow due to the extra overhead taken for the initial handshake before the set up of every session. Another major issue with these security protocols is that the key management and distribution by using the popular protocol of PKI is centralized

IV. IoT Challenges address by the Blockchain

IoT follows a client/server paradigm. For controlling the entire network a single web server and interface is required. IoT devices forwards the data to be stored in a central database which can be manipulated in security attack.

IoT devices are not smart enough for detecting the genuinity of the received data hence easy targets for security attacks. Blockchain can help to resolve this issue [12]. In this scenario it can help devices within the Blockchain network to reach at a decision whether the received data is genuine or not. They can spot the malicious actors and prevent IoT devices to interact with them further. In Blockchain because of the encryption while data transmission between IoT devices will remain safe from interception. Hence eliminating any third party or middle-men or broker for data exchange between IoT devices. Using blockchain in IoT application an unmodificable record of IoT device is maintained due to the imutable ledger technology.

IPv6 follows 128-bit addressing however blockchain follows 160-bit addressing. [13]. Hence blockchain can produce $1.46 * 10^{48}$ unique addresses offline and allocate them to IoT devices. It increases the probability of clashing of two addresses by 10^{48} which is quite large number. So it is considered as a secure method to allocate a Global Unique Identifier (GUID) to IoT device, without any registration or verification of uniqueness after assigning it. Refer the Fig. 8.Hence eliminating the central organization Internet Assigned Numbers Authority (IANA) responsible to assign IP (IPv6, IPv4) addresses as shown in the Fig. 6. Moreover blockchain generates $4.3 * 10^9$ addresses in excess of IPv6. Therefore in comparison to IPv6, blockchain is more scalable solution. To end IoT devices are constrained entities with limited memory and computational capacity making IPv6 stack unsuitable to run on them.

IoT defence is more asymmetric than the internet defence as the defender here are resource constrained opposite to the attackers. In IoT context, smart contracts based Blockchain is anticipated to play a significant role to manage, control and also secure IoT devices. This section discusses and summarize few inherent features of blockchain that can be exceptionally useful to IoT application, in particular IoT security. The centralized key management and distribution are completely eradicated with blockchain because every IoT device owns an asymmetric key pair and its own GUID once installed and joined to the blockchain network. This further leads to major simplification of security protocols such as DTLS (no need of handshaking before start of each communication). Consequently, a light-weight security protocols would fit the requirements for the computational and memory resources of IoT devices.

V. Proposed secure Architecture using Open Blockchain

Our proposed secure communication architecture of IoT application uses Open Blockchain also known as Hyperledger, which is a permissioned blockchain network as shown in the Fig. 7. In our proposed architecture the end users or IoT devices will go through a registration process that will authorize them to send and execute data. Like smart contracts in Ethereum, chaincodes in Hyperledger has to be deployed and registered within the network. Chaincodes are any arbitrary logic to be accommodated in its transactions and can be written in any conventional programming language. Fig. 7 depicts the entities present in our architecture.

- Membership management or Permission Issuer:
  This entity is responsible to identity an IoT device using device id, register it and issue necessary credentials for creating transaction successfully. This also helps in deploying chaincodes through Hyperledger.
- Nodes:
  There are 2 types of nodes: validators and non-validators. Validators's responsibility is to check the validity of the user-data (transaction) submitted to the network, execute it and add to the blockchain. Nonvalidators's responsibility is to receive user-data, perform validity checks and forward the data to their adjacent validating nodes. Every node keeps an up to date copy of the blockchain.
- End User and Client:
  These are the users and IoT devices registered to the membership management entity.

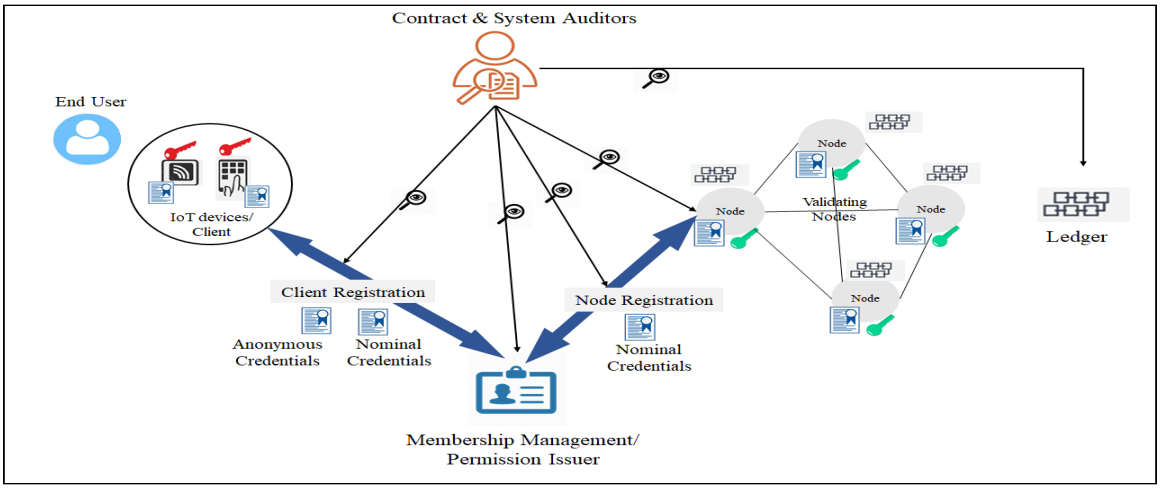

Fig. 7. Proposed Architecture

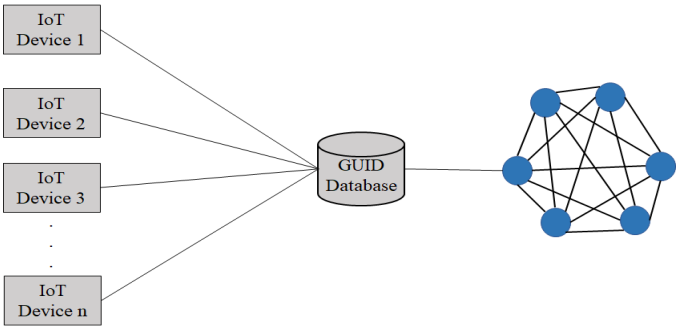

Fig. 8. GUID Database in Blockchain

2 key-pairs created for user during enrollment and both are created at the client side. One is an ECDSA key pair that is used for long-term user identity authentication and the second one is an ECDH (Elliptic curve Diffie Hellman) key pair for establishing a secret communication channel for user within the Hyperledger network. The secret signing and decryption keys are maintained in user side and never shared with membership management entity. And the public signature verification and encryption keys are generated during the user enrollment and mentioned in user's enrollment certificate.

Users use their certificate to authenticate themselves as valid users of the system. Hyperledger guarantees the below security properties:

- Nonrepudiation
  Users having a certificate to send data cannot deny having generated the data.
- Privacy
  In Hyperledger the membership Management or Permission Issuer encrypt the identity of each client (IoT devices in our case) and the transactions made by the client (sensor data in our case). The encrypted data can decrypted only by the required nodes at run-time, hence resolving the privacy issue.
- Scalability
  As Hyperledger network is a permissioned blockchain network, the number of nodes participating in the network can be controlled. Hence the controlled number of node will increase the scalability of the hyperledger.

Detecting Malicious actor is easy in Hyperledger network as every node knows about all other nodes and can revoke their access if needed.

VI. CONCLUSION

It is anticipated that Blockchain will make far-reaching changes in IoT applications in near future. We have addressed the vulnerabilities occur in secure communication in an IoT application by integrating it with Blockchain. In this paper, we proposed an architecture to communicate securely in IoT Applications using Hyderledger based Blockchain. In IoT application the data sent by various devices stored in a centralized database making it vulnerable for security breaches. Also the authenticity of the sender could not be verified properly making it open for security threats. In this paper we have proposed a secure architecture based on open Blockchain (Hyperledger) for IoT applications. Malicious actor detection will be easy as every node aware of all other node in the Hyperledger network. Concluding it guarantees the security measures for non-repudiation, privacy and scalablity in an IoT application.

As explained in this paper integration of Blockchain technology with IoT makes the communication secure. Each sender and receiver identity are verifiable by the network nodes Using the digital signature concept. The limitation, in this case, is that Blockchain is also having some security and computation problem. In the future, we would implement the proposed approach using any smart IoT based system in Hyperledger platform to test the framework with computational efficiency.

REFERENCES

[1] M. Vukolić, "Rethinking permissioned blockchains," in *Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts*. ACM, 2017, pp. 3–7.

[2] A. E. Gencer, S. Basu, I. Eyal, R. Van Renesse, and E. G. Sirer, "Decentralization in bitcoin and ethereum networks," *arXiv preprint arXiv:1801.03998*, 2018.

[3] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Capkun, "On the security and performance of proof of work blockchains," in *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*. ACM, 2016, pp. 3–16.

[4] S. Akira, "Ethereum-the next generation of cryptocurrency: A guide to the world of ethereum," 2018.

[5] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with iot. challenges and opportunities," *Future generation computer systems*, vol. 88, pp. 173–190, 2018.

[6] S. Hernández Ramos, M. T. Villalba, and R. Lacuesta, "Mqtt security: A novel fuzzing approach," *Wireless Communications and Mobile Computing*, vol. 2018, 2018.

[7] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, "Evaluating critical security issues of the iot world: present and future challenges," *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2483–2495, 2018.

[8] M. I. Malik, I. N. McAteer, P. Hannay, S. N. Firdous, and Z. Baig, "Xmpp architecture and security challenges in an iot ecosystem," in *Proceedings of the 16th Australian Information Security Management Conference*, 2018, p. 62.

[9] I. N. McAteer, M. I. Malik, Z. Baig, and P. Hannay, "Security vulnerabilities and cyber threat analysis of the amqp protocol for the internet of things," 2017.

[10] C. P. P. Schumacher, N. Kushalnagar, and G. Montenegro, "Ipv6 over low-power wireless personal area networks (6lowpans): overview, assumptions, problem statement, and goals," 2007.

[11] C. Hennebert and J. D. Santos, "Security protocols and privacy issues into 6lowpan stack: A synthesis," *IEEE Internet of Things Journal*, vol. 1, pp. 384–398, 2014.

[12] M. A. Khan and K. Salah, "Iot security: Review, blockchain solutions, and open challenges," *Future Generation Computer Systems*, vol. 82, pp. 395–411, 2018.

[13] A. M. Antonopoulos, *Mastering Bitcoin: unlocking digital cryptocurrencies*. " O'Reilly Media, Inc.", 2014.