Blockchain Technology For Security And Privacy Issues In Internet Of Things

Anuska Gupta, Bhumika Gupta, Kamal Kumar Gola

Abstract: Blockchain technology is a secure way of holding the record of data. It supports distributed public ledger. Blockchain supports data storage, real estate, asset manager other financial transaction. If we are talking about Blockchain in India Telangana is the first state of India which supports this technology for huge incubator and a world-class facility for promoting research. This paper presents the use of blockchain technology in internet of technology in terms of security and privacy.

Index Terms: IoT, security threats and challenges, application layer, MQTT, smart device, next generation networks, cryptography, bitcoin, blockchain technology, application of blockchain.

1 INTRODUCTION

IoT is collection of various independent and dependent device which is helpful in the transmission of data. IoT is made up of various layers which has specific task to perform [1-5]. Perception layer, Network layer, Application layer, Physical layer. This paper is all about these layers and specification as well as for the security of devices in each and every layers. IoT is made up of mainly four layers. There are various security principles which is helpful for proper working of these layers available in IOT. Each layer has specific application.

- Application layer
- Perception layer
- Network layer
- Physical layer

Massive amount of device are connecting with the network communication device and IOT devices day by day.

Security issues in IOT layers

A. Application Layer

The data integrity, data confidentiality, and data authenticity is guaranteed by this layer. The application layer protocol define application interface with lower layer protocol to send the data over network [6-8]. If some issues will be in this layer app can shut down and compromised easily. Some of the application layer protocol are given below-

This layer protocol enables process-to-process connection using ports.
- HTTP
- CoAP- (Constrained Application Protocol)

RFC 7252 Constrained Application Protocol is web transfer protocol which work along with constrained node and constrained network in IOT.

It is Machine-to-machine protocol (M2M). Application of CoAP protocol is smart energy and building automation. This protocol is dedicated to work specially with HTTP (hypertext transfer protocol).

Web socket
- MQTT- (Message Queue Telemetry Transport)

MQTT is widely used protocol based on Publish Subscribe Model. It is light weight protocol. This works as centralized data collection. This is suitable for specific network which having lower bandwidth and limited memory. MQTT protocol is very useful for making real time application for instant response.

- a) Facebook messenger app
- b) Open source application
- c) IECC signaling control system
- d) Amazon web services
- e) Open geospatial consortium sensor
- f) Various mobile application uses MQTT library for transmission

- XMPP-(Extensible Messaging and Presence Protocol)

This protocol is based on Client Server Architecture and Server-server communication path. It works on decentralized data collection.

This protocol has various application like

- a) Messaging
- b) Gaming
- c) Multiparty chatting
- d) Video calling
- e) Voice calling
- f) Data syndication

- DDS-(Data Distribution Service)

It mainly used for M-2-M and device to device communication. This support Pubic-Subscribe model.

- AMQP- (Advance Message Queuing Protocol)

This support Publish-subscribe model. It is an open standard application layer protocol for middleware messaging protocol. This protocol can do message orientation, queuing, switching, reliability, and security.
B. Perception Layer
The function of perception layer is to collect data and information from various real time resources, using sensors and actuators. The main target is node which is made up of sensors. This layer is also known as a sensor.

C. Network Layer
This layer acts like central nervous system (CNS) or backbone of the whole network. This is mainly the third layer in OSI model. This layer provides data routing paths for network communication. Transmission of data is being possible through IoT hubs and router. Data is transferred in whole path in form of packet. This layer responds to requests from transport layer and issues requests to the layer below it data link layer.

D. Physical Layer
This is the lowermost layer of OSI model. Mostly physical connection held in this layer. Bit by bit transmission of data held in physical layer this layer based on baseband and broadband transmission. Mesh, star, ring, bus topology are used for connecting device in this layer. Transmission mode of this layer is being in the simplex, half duplex, and full duplex.

This layer provide following service:
- Bit-by-bit delivery
- Line coding
- Bit synchronization
- Auto-negotiation
- Transmission mode control
- Signal equalization
- Forward error correction
- Collision detection etc.

### Major Security Risk

<table>
<thead>
<tr>
<th>MAJOR SECURITY RISK</th>
</tr>
</thead>
<tbody>
<tr>
<td>Poor physical security</td>
</tr>
<tr>
<td>Insufficient security configuration</td>
</tr>
<tr>
<td>Insecure mobile/cloud/network/software interface</td>
</tr>
<tr>
<td>Insufficient authorization/authentication</td>
</tr>
<tr>
<td>Fulfilling the need for security analytic capabilities</td>
</tr>
<tr>
<td>Understanding the complexity of vulnerabilities</td>
</tr>
<tr>
<td>Internet of things vulnerabilities management</td>
</tr>
<tr>
<td>Disrupting and DOS attacks</td>
</tr>
<tr>
<td>Insecure web interface</td>
</tr>
<tr>
<td>Module hardware and software components</td>
</tr>
</tbody>
</table>

**Fig. 2. Major Security risk [33]**

### Generation of IoT Security

2 GENERATION OF IOT SECURITY
Recent trends and concern related to IoT security

**Fig. 4. Generation of IoT [6][12][13]**

3 SECURITY REQUIREMENT AND SPECIFICATION
Security certification is necessary for the IoT as well as various network device, so that it will easily measure the security parameter of devices.
4 IMPORTANCE OF CYBER SECURITY IN IOT

Current internet security protocol is based cryptographic algorithm. 6 out of 10 devices that provide user interface were vulnerabilities to a range of issues such as persistent XSS and weak credentials. Here we are listed some them.

5 SECURITY IS A JOURNEY NOT A DESTINATION

Security of any device is a continuous and complex method. Security is getting tougher day by day as IoT devices are increasing in multiple manner. Now a day there are millions are devices which is being connected to the network for the transmission of data throughout the world.[6][21][25][29]

6 SECURITY INFO PROTOCOL

Protocol defines the blueprint of methods, properties that suit a particular task. Some of the protocol are [33][34]

- OpenIOC
- Cybox
- IODEF

7 SECURITY TECHNOLOGY

Some of the security technology is mentioned below [33][34]

- URL block listing
- Vulnerability assessment
- Device detection
- Exploits prevention
- Anomaly detection

8 ECOSYSTEM OF IOT

The Ecosystem of IoT is complete description of IoT. It defines each and every aspects of the system. Some of the aspects of them are identification, communication, actuators, storage, localization and tracking etc.

---

**Fig. 5. Security certification [34]**

**Fig. 6. Importance of cyber security [6][31][32]**

**Fig. 7. Security overview [31][32]**

**Fig. 8. Ecosystem of IoT [10][14]**
9 BLOCKCHAIN SOLUTION OF PRIVACY IN IOT
There are various privacy concern which is available in IOT security field, but one of the most trusted and efficient technology which is being used in security of IoT devices are Blockchain.

Blockchain was originated technology which was initially used to making financial transaction with full security and secretly. Blockchain is a decentralized digital currency, digital asset (having value) [22] [23]. Blockchain is like an internet database which support strong consistency. BC node makes a local copy of global data sheet, and local copy of data is being updated time to time with every new transaction, this is called Public Ledger. Every historical information is being used to utilize for future computation and every old transaction is used for validation of new transaction. Public ledger has various properties like security, consensus, protocol for commitment and privacy and authenticity. "A blockchain is can open distributed ledger that can record transaction between two parties efficiently and in a verifiable and permanent way". We know that blockchain is a decentralized (multiple point of coordination) platform which is full of specification, while centralized system has various problem like:

- Server crash
- Insufficient bandwidth
- Single point of coordination is not safe

Blockchain is based on Ledger - based tamper proof technology. Financial transaction like Bitcoin and other cryptocurrencies. This technology is enhanced the security of these IOT devices and sensors. Blockchain works like a database which continuously maintained and controlled the collected transaction dataset.

**Working of Blockchain**

Blockchain works mainly on two parts are transaction (participant created) and recorder block (of transaction). The main function of recorder block is to maintain check and maintain the correct sequence of transaction. If the sequence of transaction is correct, then there will be no any data tampering. Chain approach is being used to maintain the recorded data in sequential order. Each and every transaction is being shared with the participated nodes of network. Using this the central server concept it will be removed by recognizing the specific node which is involved in transaction sharing. In this cryptography (a secret method) is used. Cryptography allow us the authentication security throughout the transaction. With the increasing no of IOT device and sensors it will more and more try to interact with the internet for the communication but in such a large scale of these devices the centralized server is not an effective method. Most of the IOT devices are rely on centralized server concept. There is need for increasing the internet infrastructure power for the processing of IOT system. Peer-to-Peer Networking (PPN), Distributed File Sharing (DFS), and Autonomous Device Coordination (ADC) function are capable with decentralized and distributed network. Whether Blockchain can contain any of these function to make the track of connected device. Blockchain’s secure structure helps in elimination of Single Thread Communication (STC), which make the system more reliable, secure and robust.

There are various advantages in blockchain technology

- Security
- Decentralized network
- Elimination of intermediaries
- Immutability
- User control funds
- Legal and compliance
- Processing power and supply
- Peers might crash
- No notion of global time
- Peers might turns malicious
- Voting does not work

10 USE OF BLOCKCHAIN

Bitcoin is a famous crypto-currency and it also used as electronic cash. It was initially release in 9 Jan 2009. [33][34] Its domain is “bitcoin.org”. Bitcoin works on Gossip protocol. Bitcoin is also being used as an investment.

Bitcoin are created through mining. It si secured through Public Key Cryptography, using Elliptic Curve Digital Signature Algorithm (ECDSA) Current block reward is 25 coins per 10 minutes, it will half approximately every four years. As soon as we will reach 21 million coins by approximately 2140 bitcoin is increasingly divisible in measurement.

**How Bitcoins are Bought/Sold**
- Via Bitcoin exchange
- Online transaction
- India’s popular app: Zebpay

**How Bitcoins are generated**
- Via Bitcoin mining
- By solving math puzzles
- Limited circulation

**How Bitcoins are transferred**
- Mobile app
- Digital transfer
- Peer-to-Peer transaction
- Stored in digital wallets

**How Bitcoins are Black-Marketed**
- Bought via hard cash
- Touts organize transfers
- confidential transaction
- Offline resale in cash
Disadvantage of Bitcoin:
Every coin has two faces, if bitcoin provides us various facilities then it has some disadvantage too, here are some of them listed below:
- The exchanges are not regulated or supervised by a government agency
- Large price swings and “flash crashes”
- Market manipulation hence volatile in price
- Theft and hacking can be happen in Bitcoin
- Self-dealing by the exchanges may lack customer protection and system safeguard
- People are still unaware of digital currencies and bitcoin
- People are not much aware about bitcoin to apply it to their lives
- Networking is a must to spread the word on bitcoin.
- High transaction cost and time.
- Not easy to use for pay
- Not valid in every country
- According to latest gov order it will not be a legal tender in India.

Bitcoin value proposition:
Bitcoin is used as cross-country, untraceable currency, which is free from any rules regulation of country. The bitcoin blockchain size as of Dec 2017 is app 149GB
Current BTC price
1BTC=$8069.00

Various crypto-currencies
Till now crypto-currencies is being discover till now. Here are list of some of crypto-currencies mentioned below them.
- Bitcoin
- Ethereum
- Ripple
- Zcash
- Algorand

Value of Bitcoin in India:
Hence the value of bitcoin is very volatile, however we compare the value of bitcoin in India we have some comparative data which are mentioned below:

1 Bitcoin = Over 10lack
1 Bitcoin = 1 Honda city car
10 Bitcoin = 1 BHK in Mumbai suburb
40 Bitcoin = 1 Rolls Royce Phnatom

How to invest:
If we want to invest our money in bitcoin, we have various online Cryptocurrency Exchange Service available in which we can change rupee in bitcoin.

ZEBPAY- largest exchange service in INDIA

COINBASE- largest exchange service in all over World.

Bitcoin transaction life cycle:
Transaction of bitcoin is considered to be very safe and secure. It can be fully reliable and secure. The transaction life cycle of bitcoin are method in the block below.

Working of Bitcoin:
Bitcoin is fully secured and complex transaction method for the online transaction. It is the explanation of how the bitcoin exchange the transaction.

Blockchain in Artificial intelligence:
Blockchain and Artificial intelligence are two disruptive technologies. [31][32] Blockchain connect data storage and data usage AI-analytic over data Block chain can provide a strong backbone to development of AI algorithm.
Blockchain in Food Safety:
Consumer scan or input the tracing code printed on the package.

Fig.13. Food safety chain [30] [31] [32]

Food safety and traceability enables by blockchain. Foreign Supplier Verification Program (FSVP) - a component of FSMA requiring importers to asset and monitor health risk factors including:
- Formulation
- Transport
- Packaging
- Storage

Blockchain in Health care:
Blockchain is making very big impact in the field of the health-care.

Fig.14 Health-care overview [30] [31] [32]

Blockchain in Artificial Government:
Government needs to maintains documents either in paper or in digital form
- Daily operation and activities
- Record of people
- Business transaction
- Government assets (land record, building etc.)
- Details of people, organization, and institution
- Digital identity

12 CONCLUSION AND FUTURE USE OF BLOCKCHAIN
Blockchain is emerging technology which will be more efficient and accurate in future. Except bitcoin, blockchain has various application, but future will be more exited in this field. Here we are listed some of those use cases: - [29]
- Cross border payment
- Widespread Distributed Data Models
- DLT-Based Government Systems
- Standardization and Collaboration
- A Potential Ecosystem of Specialized Chains
- Government Crypto

13 REFERENCES


[22] Research Directions for the Internet of Things,John A. Stankovic, Life Fellow, IEEE


[27] Shahid Raza, Hossein Shafagh, Kasun Hewage, Ren Hummen, Thiemo Voigt, Lithe:Lightweight


“Security in Internet of Things :Challenges, Solution and Future Direction”Satish Alampalayam Harshit Srivastava 1530-1605/16©2016 IEE

[29] XVIII. Web links

[30] https://nptel.ac.in/courses/106105184/

[31] https://onlinecourses.nptel.ac.in/noc18_cs47/preview

[32] https://nptel.ac.in/noc/individual_course.php?id=noc18_cs47

[33] www.owasp.org intel proprietary