

A Study of Blockchain Technology In Internet of Things

E. Padma

Assistant Professor, Department of CSE, SCSVMV University, Enathur, Tamil Nadu, India

ABSTRACT

In the modern world data are exchanged and transformed without any protection in the digital world. Nowadays, more businesses are committed through online system. The digitization of data can be carried through the centralization and decentralization process with higher protection. All the data can be stored through blocks with transaction history as BlockChain. In a BlockChain the transaction can be simplified with peer-peer network that excludes the involvement of third party. As a new way of communication technology through sensors and actuation object, IoT has been taken its tremendous way of exchanging the information. Security and Privacy policies are to be maintained in their operational feature. The trusted party can be integrated with a chain of link for accessing the information. With the advent of security for high speed networks, smart homes, smart healthcare, the IoT has gained wide acceptance and popularity as the main standard. IoT deployment contains heterogeneous devices with embedded sensors interconnected through network. In this paper, a survey of IoT with Blockchain technology can be implemented for decentralization with high transparency. The security issues are categorized as low-level and high-level for decentralized data. Blockchain technology has been foreseen by research community and plays a major role in controlling and securing IoT devices. Blockchain technology can be worked out for permissible and non-permissible key users. The centralized users can use public Blockchain. The important underlying technology is bitcoin and as a survey in this paper, how the performance feature of Blockchain technology can be worked out for Bitcoin can be discussed. The IoT security and challenges may provide proper solution for the outcoming problems. The Blockchain can be timestamped and validated with a constraint. The main contribution involved in the paper can be summarized as analysis of security threats for decentralized users, IoT security issues with low-level and high-level, how to overcome with Blockchain security attacks. The security threats in IoT exploit Vulnerabilities of different components as software based applications, physical devices. In a distributed system, the decentralized data can be exchanged between each user by using separate key values. The generation of keys can be designed with certification. The keys are stored in a transaction history using blocks. A global security mechanism for various IoT protocols can be implemented interoperably.

Keywords : Security, Bitcoin, IoT, Blockchain, Protection of Data

I. INTRODUCTION

In the recent days of businesses, all consumers are exchanging their information through Information and Communication Technology. ICT provides all basic information about the knowledge of securing

data. Many services are launched for the usage of the consumers like SOA, SOAP etc., The innovation of business practice deals with protecting and securing the data. The integrated legal systems are effectively protected for personal data and information is paramount for digital world. Authenticated user is at

the core of many e-commerce services and elevates privacy and security risks. Nowadays, many businesses deal with the transaction through e-payment gateway. The security protection for the payment gateway is lagging in providing services to the consumers. Businesses must be strict in maintaining the reviews about their products. Businesses must ensure about the advertisement and services to the consumers. Innovative business must account to the knowledge of global nature with its own effective implementation and procedures which allow consumers to adapt for the environment of e-commerce to receive unsolicited commercial messages. To overcome present digital world business environment, all the Business and social resources are connected. The real world and the cyber world are connected. Then social values are brought to the real world by the IoT systems. Internet of Things (IoT) technology is being implemented broadly for information technology and industry applications. The industry initiative in IoT research would expect a realization of commercial product that instantly impact humans life. IoT is generally characterized by real world and small things with limited storage and processing capacity, and consequential issues regarding reliability, performance, security, and privacy. IoT becomes the future generation platform for advancement in computing. The main idea is to integrate each single physical entity with internet technologies for real time production oriented data.

IoT Service applications for innovative businesses are need to grow gradually to match with the market demands of digital world. IoT has multiple elements such as identification parameters which are enclosed with naming and addressing. Secure device and Secure Communications are the important principle for IoT security.

II. LITERAURE REVIEW

P.Mahalle et al in their paper [1] Requirement for identity is not adequately met in networks, especially

given the emergence of ubiquitous computing devices that are mobile and use wireless communications. Addressing identity problem requires changes to the architecture for naming, addressing, and discovery. Challenges include resource discovery; ways to expose relevant privacy distinctions to users, naming and addressing that restricts precise knowledge of identity to authorized parties

J.Gubbia et al in their paper [5] sensors and actuators blend seamlessly with the environment around us, and the information is shared across platforms in order to develop a common operating picture (COP). Fuelled by the recent adaptation of a variety of enabling device technologies such as RFID tags and readers, near field communication (NFC) devices and embedded sensor and actuator nodes, the IoT has stepped out of its infancy and is the the next revolutionary technology in transforming the Internet into a fully integrated Future Internet. As we move from www (static pages web) to web2 (social networking web) to web3 (ubiquitous computing web), the need for data-on-demand using sophisticated intuitive queries increases significantly.

D.Yang et al [6] Things are active participants in business, information and social processes where they are enabled to interact and communicate among themselves and with the environment by exchanging data and Informations are sensed about the environment, while reacting autonomously to the real/physical world events and influencing it by running processes that trigger actions and create services with or without direct human intervention

S.Khan et al [7] in their paper The Internet is continuously changing and evolving. The main communication form of present Internet is human-human. IoT provides connectivity for everyone and everything. The IoT embeds some intelligence in Internet-connected objects to communicate, exchange information, take decisions, invoke actions

and provide amazing services. This paper addresses the existing development trends, the generic architecture of IoT, its distinguishing features and possible future applications. The IoT is getting increasing popularity for academia, industry as well as government that has the potential to bring significant personal, professional and economic benefits.

Alessio Botta et al [9] in their paper IoT is generally characterized by real world small things, widely distributed, with limited storage and processing capacity, which involve concerns regarding reliability, performance, security, and privacy. The key feature in IoT is, without doubt, its impact on everyday life of potential users [5]. IoT has remarkable effects both in work and home scenarios, where it can play a leading role in the next future

Thomas Hardjono et al[10] in their paper address the issue of retaining user anonymity within a permissioned blockchain. We present the ChainAnchor architecture that adds an identity and privacy-preserving layer above the blockchain, either the private blockchain or the public Blockchain. ChainAnchor builds upon and makes use of the zero knowledge proof mechanisms of the EPID scheme, which has the advantage of an optional cryptographic binding to a TPM tamper-resistant hardware. The use of tamper-resistant hardware provides a significant increase in security

III. MEASURES OF BLOCKCHAIN TECHNOLOGY

Security is maintained using the technology of Blockchain for the decentralized users in the way of authenticated with permissible blockchain. The measures of technology can be proved with the reference key. The identity of the user can be identified with their own keys.

- ✓ Anonymity of users: Users achieve the same degree of anonymity as is currently achieved in the Blockchain.
- ✓ Anonymous permission verifiability: Verification of a User or Miner leaves them in the same degree of anonymity in the Blockchain.
- ✓ Permissions Enforcement: Only anonymous Users who have obtained permission will have their transactions processed. Similarly, only Miners who have obtained permission will have their work remunerated.
- ✓ Revocation of transaction keys: A verified anonymous User whose private-key has been lost or stolen can anonymously request his/her private-key from the available list.

The IoT will place different demands on communication infrastructures and services. Underlying these developments will be policies that promote the availability, quality and use of such infrastructures and services. In this regard, international governance and norms may need to be reviewed to ensure the performance and security of communication networks and services and thus contribute to building trust in the IoT. Replication Attacks, Connectivity issues and non updated systems are the major challenges in the IoT Business environment. More security can be provided for securing authenticated user by providing necessary Secured boot and access, Data encryption, Password authentication and Fighting cyber attacks. Consumer's data are highly protected to avoid theft and malicious attackers to steal the information. The authenticated password must highly protect the consumer's data. Only the authenticated user can have access about the business information. The innovation business deals with various devices security feature. Secured device must handle all the original data of the consumers. As a third party authentication, the devices are to be secured with highly protected passwords. The encryption techniques are to be strictly followed and must secure

with Message Authentication Code for all the user data.

IV. PROPOSED METHODOLOGY

The proposed method for the security issues are categorized as low-level and high-level for decentralized data. Blockchain technology has been foreseen by research community and plays a major role in controlling and securing IoT devices. Blockchain technology can be worked out for permissible and non-permissible key users. The centralized users can use public Blockchain. The important underlying technology is bitcoin and as a survey in this paper, how the performance feature of Blockchain technology can be worked out for Bitcoin can be discussed. The IoT security and challenges may provide proper solution for the outcoming problems. The Blockchain can be timestamped and validated with a constraint. The authentication of data plays a vital role in security measures. The enhanced feature of third party authentication can be done for accessing and storing each and every data of the consumer in the information storage area. In order to protect authenticated user while transformation of data using e-payment gateway, data authenticity policy to be maintained. Nowadays, as an innovative business transaction mode, IoT devices are managed with available security features. The storage of information can be connected via mobile device for the transaction of business. Information and Communication Technology provides more knowledge about stored information to the consumer. The consumer can protect the data via encrypted method.

In the Permisisoned Chain the user can follow the steps as the originator and the recipient of the transactions are from same permissioned-group.

Permisisoned-Block: Only the permissioned block of user can access the blocks with the permissible group of members.

Authenticated User	Key Reference
Access Secured Data	Retrieve the permissible key value as reference key
Provide Security policy	Check for authenticity and Access through IoT Device

A.Security Policies

To provide security for the authenticated user, certain policies are to be carried out in order to protect the information. Third Party authentication must be provided as a security feature. Every consumer must get register with the individual username and password from the authenticated server to access their data. The authenticated user must be highly protected with public key cryptographic algorithm. For each secured data hash code can be generated. In addition with the original information the generated hash code must be sent with encrypted format. The data can be stored in the server with unscrambled text. Trust of service is activated for better securing of data. In the modern world, the transaction of innovative business can be carried through e-payment gateway. The gateway must also be protected from unauthorized accessing. The authorized user of the machine can only access the relevant information.

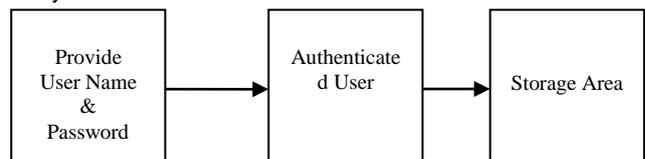


Figure 1. Trused Authenticated User in the Block

B.Accessing users information Through IoT Devices

IoT Device like Mobile can be used for accessing the stored information of authenticated users. The secret information can be accessed through the registered devices. A chip like small devices can also be embedded as a IoT devices. The functionality of the device can be identified using the registered information. The performance and reliability feature

for providing security using IoT devices plays a vital role in the digitized world. Through the sensors and actuators the relevant information of the consumer can be retrieved. The authenticated user must be able to gather their stored information by providing necessary username and password along with their reference key. The authenticity for accessing the stored data can be checked for each and every time with the available server. All the authenticated username and password can be checked with blockchain reference value. The device must be authorized only with the permissible block of value available in the chain.



Figure 2. Access information of Authenticated User

V Work Analysis of Protecting and Securing Authenticated user in the permissioned chain

The work flow analysis includes performance of the IoT devices for accessing the secured and protected user authentication with the group of permissible blocks of chain. The User in ChainAnchor has the same function as the originator/recipient of a transaction. User obtains permission to transact on the permissioned blockchain by requesting membership to the permissioned group that implements the permissioned blockchain. User validates the Membership Verification Public Key: Prior to using the parameters and verify the authenticity. The User can have any number of self-issued transaction public-key pairs. The data analysis fetches the information of the highly protected user data. The trusted user will get registered with IoT, the device connected to the server will respond to the authenticated user only. The unauthorized party wants to access the device, it will get locked. The speed rate of accessing with trustness to be included in the performance criteria. The difference in the speed up ratio of time rate leads to delayed accessing time for authenticated user. The trust as a service

phenomenon has to be enhanced in order to promote the speed up time.

$$s = pb/pt$$

The flow of speed up time must be compared with accessed data. The highly protected authenticated user information must be extracted using decentralized ledger. The user should know about the services provided by the server for accessing their data.

V. CONCLUSION

The protection and security of authenticated user can be purely identified with the Blockchain reference key. Many users are not aware of the storage of their data. The security has been given to their data are also not known to their knowledge. As a wholesome, the trusted party is the only authorized party. The registered IoT device will work according to their fetching of information. The device grants permission for the trusted user only. IoT services are typically provided as isolated vertical solutions, in which all system components are tightly coupled to the specific application context. The security threats in IoT exploit Vulnerabilities of different components as software based applications, physical devices. In a distributed system, the decentralized data can be exchanged between each user by using separate key values. The generation of keys can be designed with certification. The keys are stored in a transaction history using blocks. IoT device performance needs more speed up ratio for accessing authenticated user. This condition has to be taken as a future challenge. The security gateway of storing large volume of user data must be protected with secured user name and password. Thus Authenticated user are given more protection and highly secured performance feature with the public key cryptographic algorithm.

VI. REFERENCES

[1]. P. Mahalle, S. Babar, N. R. Prasad and R. Prasad, "Identity management framework towards internet of things (IoT): Roadmap and key

- challenges," In Recent Trends in Network Security and Applications, Vol.89, pp.430-439, Chennai, India, July 2010.
- [2]. <http://www.nec.com/en/global/solutions/iot/concept/index.html>
- [3]. <https://internetofbusiness.com/can-speed-iot-innovation/>
- [4]. <http://www.goodworklabs.com/how-to-implement-security-measures-for-internet-of-things/>
- [5]. J. Gubbia, R. Buyyab, S. Marusica and M. Palaniswamia, "Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions," *Future Generation Computer Systems*, Vol.29, No.7, pp.1645-1660, September 2013.
- [6]. D.Yang, F.Liu and Y.Liang, "A Survey of the Internet of Things," in *Proc. 1st ICEBI 2010*, pp 358-366
- [7]. R.Khan, S.U. Khan, R.Zaheer and S.Khan, "Future Internet: The Internet of Things architecture, possible applications and key challenges," in *Proc.10th Int. Conf.FIT,2012*,pp.257-260
- [8]. GSR14 Best Practice Guidelines on consumer protection in a digital world – A Survey Paper
- [9]. Alessio Botta , Walter de Donato, Valerio Persico, Antonio Pescapé, "Integration of Cloud computing and Internet of Things: A survey" in *Future Generation Computer Systems* 56 (2016) 684–700
- [10]. Thomas Hardjono, Ned Smith, Alex (Sandy) Pentland, "Anonymous Identities for Permissioned Blockchains" A survey paper 2016
- [11]. Ali Dorri, Salil S. Kanhere, and Raja Jurdak, "Blockchain in Internet of Things: Challenges and Solutions" - proceedings