Security of IoT System using Blockchain

Sujatha Kumari B A, Sadaf Farheen

Abstract: ***There is exponential growth in the in the research industry of Internet of Things (IoT), but it is still vulnerable to privacy and security. Devices in the IoT having resource-constraints and decentralized topology are not capable of conventional privacy and security approaches. The paper predominantly focuses on the survey in the IoT system. Where we can see the various issues in IoT. To overcome these issues researchers, use blockchain mechanism. Due to blockchain's popularity and success this technology is incorporated into many other industries. Blockchain is a technology that is booming since a decade. Despite various advancements in blockchain there are issues that are still present in IoT that needs to undergo improvisation. Before going to design and implement a model based on blockchain it is essential to understand the issues and challenges met by earlier research works. The paper presents study on the previous challenges and the solutions which are presented to get rid of the problems. Some of the existing problems are as follows- When the data is collected from the IoT devices and stored using blockchain still the data is under constant threat due to lack of security mechanisms relating to authentication and data privacy. Hence, providing security to blockchain becomes of utmost importance.***

The goal of this paper is presenting a detailed survey of security mechanisms for IoT systems. Also, this survey examines and explores why providing security to IoT devices is important. Readers can ultimately get aware of the issues that are present in the IoT systems and how they can be overcome. The study is beneficial for those who are looking forward to deploying IoT applications. They can get to know what the prerequisites are to be met for a secure IoT system.

Keywords: Internet of things, Blockchain, authentication, hash security, privacy.

I. INTRODUCTION

The Internet of Things (IoT) is a combined system of interrelated mechanical and digital machines, computing devices, people or animals, objects that have their unique identification and able to transfer the data over the network without any human-to-computer or human-to-human interaction. During the process of data transfer there is a possibility of data leakage over the network hence data transfer needs to be secure. Blockchain is a growing list of records called as blocks that are linked together using cryptography. Each block comprises of the following things- cryptographic hash of the previous block, a timestamp, and transaction data.

The design of the block chain is such that it is resistant to the data modification. It is an open distributed ledger. Blockchain can record the transactions between the two parties efficiently in a permanent and verifiable way. Once recorded the data cannot be modified retroactively without the modification of all the subsequent blocks. The alteration of the subsequent block requires the consensus of the network majority. Hence blockchain can be considered as secure by design, because of the unalterable feature of blockchain records by are secure by design and have a distributed computing system. This system is equipped with high Byzantine fault tolerance. However, dense, pervasive collection, increasingly invisible processing and dissemination of data in the midst of people's private lives give rises to serious privacy and security concerns. Autonomous exchange of the information between the machines is achieved machine authentication. That is, by providing authorization to machines for both wired and wireless networks during the information exchange. machine authentication can be provided to the devices such as sensors and meters. In the Internet of Things (IoT) Machine-to-machine communication is a fundamental technology. Here every imaginable object composes of a unique identifier (UI) and has the capacity to exchange data automatically over a network. Privacy and security are the integral are area of concern in the IoT. Hence machine authentication is crucial for ensuring both.

II. LITERATURE SURVEY

There are several fields that deploy IoT systems for all the advantage that it provides such as the ability to capture the data and communicate with its peer devices without any human or machine intervention. During these interactions there is a high possibility of the data leakage. In order to overcome this there are various methods that are employed to address this area of security.

Importance of combining IoT with blockchain

For industries, IIoT (Industrial Internet of Things) is an inseparable part. Here, people are made mandate for delivering IIoT systems that are secure, general and scalable is stated by Junqin Huang et al. (2019), Linghe Kong et al. (2019), Guihai Chen et al. (2019), Min-You Wu et al. (2019), Liu et al. (2019) and Peng Zeng et al. (2019). Due to problems like malicious attacks and single point of failure the existing IIoT systems are unstable in providing services. Although blockchain is a technology that has qualities like security promise and recovery combing IoT and blockchain is interesting. Most of the IoT devices are power-constrained And are not suitable for blockchain though it has low- throughput and less power-intensive. For the purpose of protecting the sensitive data confidentiality,

Revised Manuscript Received on May 25, 2020.

Sujatha Kumari B A Professor, Department of Electronics and Communication, SJCE College Mysuru, JSS Science and Technology University, India.

Sadaf Farheen, Student, Department of Electronics and Communication, SJCE College Mysuru, JSS Science and Technology University, India.

authors came up with a method that regulates the access to sensor data. Due to these methods IIoT is more efficient.

Oscar Novo et al. (2018) states due to IoT attaining its maturity it can be considered in the future internet. Authors say there are several challenges of having to deploy billions of devices worldwide of which managing them is one of the major challenges. Managing the IoT models globally is very difficult despite having access management technologies as they are centralised. In order to overcome the authors, use the blockchain technology based IoT architecture which has distributed access control system. The architecture is for arbitrating roles and permission in the IoT. The proposed architecture evaluates for various real-world scenarios which concludes in scalable IoT situations blockchain can be used as access management technology.

Zhe Yang et al. (2019), Kan Yang et al. (2019), Lei Lei et al. (2019), Kan Zheng et al. (2019) and Victor C. M. Leung et al. (2019) told for the improvement of traffic safety and efficiency, vehicles will able to broadcast and generate their messages using vehicular networks. The credibility of the messages received is difficult to evaluate due to untrusted environments. For overcoming this problem, the author uses a trust management system which is decentralized and based on blockchain. Using Bayesian Inference Model neighboring vehicles can validate their received messages. The data collected from vehicles and the offset is calculated and is kept as a "block". Vehicles here maintain reliable, updated and trust consistent blockchain.

Blockchain used because of its decentralized nature in various applications

Authors Ali Dorri et al. (2017), Salil S. Kanhere et al. (2017), Raja Jurdaky et al. (2017) and Praveen Gauravaram et al. (2017) stated that because of IoT network's distributed nature and massive scale it is a major challenge. Decentralized Privacy and security are provided by the blockchain approaches, yet they aren't suitable for the devices which are resource-constrained due to delay, significant energy and computational overhead. These factors outline various core functions and components of smart home tier. For handling the internal and external communications of the home authors use a component named "miner". This component is high resource device and online all the time. The other roles of miner are auditing and controlling the communications. Security goals namely integrity, availability and confidentiality are preserved using blockchains.

Due to the various security attacks imposed on the global IoT network the benefits that can be gained from the IoT networks can outweigh says [Haifeng Yu et al. (2010), Phillip B. Gibbons et al. (2010), Michael Kaminsky et al. (2010), and Feng Xiao et al. (2010)]. Data kept at the central server is exposed to attacks like DDoS and Sybil along with being vulnerable to single point failure which does not guarantee availability of the services and disclosing the sensor data present at the data center.

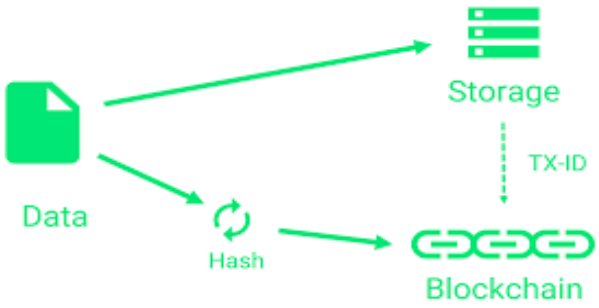

Figure 1. Data stored earlier and data stored on blockchain.

The IoT enabled with blockchain is the key technology states Mohamed Amine Ferrag et al. (2019), Makhlouf Derdour et al.(2019), Mithun Mukherjee et al (2019), Abdelouahid Derhab et al.(2019), Leandros Maglaras et al.(2019) and Helge Janicke et al.(2019) Blockchain is successfully been applied in energy trading, smart buildings and data trading as blockchain enables trust for managing and storing decentralized trust. Authors present an overview of the applications of the blockchains in the IoT along with taxonomy and a side-by-side comparison of the state-of-the-art methods using which we can preserve privacy and security of blockchain. They also talk about the various security issues that are present in the blockchain with respect to security, limitations, computation complexity, and communication overhead which can be considered as the future work.

Drawbacks to be addressed in blockchain

There are various disadvantages that are present in the block chain and a detailed discussion is presented in AHMED AFIF MONRAT et al. (2019), OLOV SCHELÉN et al. (2019) AND KARL ANDERSSON et al. (2019). Authors present a comparative study and discuss challenges which include interoperability, privacy, scalability, regulatory issues, and energy consumption. Authors also highlight blockchain technology future scope.

Since blockchain overcome the problem of single point of failure and offer the security in distributed manner they are very much suited for providing security to the IoT devices. There could be a lot of enhancements done to the IoT systems and the blockchain itself in order provide more data security. Some of the researches are listed below.

Chao Lin et al.(2018), Debiao He et al.(2018), Xinyi Huang et al.(2018), Muhammad Khurram Khan et al.(2018), And Kim-Kwang Raymond Choo et al.(2018) presented that Blockchain can be deployed in wide range of applications due to its decentralized nature of transparency, and immutability for the identity management systems authors design cryptographic membership authentication scheme which is based on blockchain. Using this we can bind the digital identity of the object to the real-world entity. For the authentication purpose authors use the digital signature.

Importance of authentication in IoT systems

Alireza Esfahani et al. (2019) , Georgios Mantas et al. (2019), Rainer Matischek et al. (2019), Firooz B. Saghezchi et al. (2019), Jonathan Rodriguez et al. (2019) , Ani Bicaku et al. (2019) , Silia Maksuti et al. (2019) , Markus G. Tauber et al. (2019) , Christoph Schmittner et al. (2019) ,

and Joaquim Bastos et al. (2019) concluded in their research article, in order to provide effective security authentication is the core stone There are several authentication schemes deployed in the IoT systems and m2m applications. These authentication mechanisms are light weight which are based on XOR operations and hash for communicating inside IIoT environment. The main issue in many IoT networks is leakage of important data Muhammad Shahzad et al. (2017) and Munindar P. Singh et al. (2017). Authors also state, the main reason being IoT networks lack authentication mechanisms. Authors propose various methods for authentication and authorization of users for IoT, where they lack conventional user interfaces for IoT networks. Authors talk about why authentication is important in the IoT network. They also propose a methodology where they can overcome lack of conventional user interface for IOT networks.

Various problems in IoT despite authentication and best methods for incorporating security

There are various problems that come into picture when there is authentication mechanism is concluded by Zhen Ling, Junzhou Luo et al. (2017), Yiling Xu et al. (2017), Chao Gao et al. (2017), Kui Wu et al. (2017) and Xinwen Fu et al. (2017). The main reason for that is the lack of authentication mechanism in the IoT. Even though there is authentication powered in most of the IoT applications yet there are security issues that lead data leakage some of the issues are as follows. Authors present a case study on smart plug system where they exploit the protocols and launch the attacks successfully namely brute force attack, device scanning attack, firmware attack and spoofing attack. Their experiments show that they can gain the user authentication credentials by performing these attacks.

For efficiency, Xiaojiang Du et al. (2009), Mohsen Guizani et al. (2009), Yang Xiao et al. (2009) and Hsiao-Hwa Chen et al. (2009) suggest adopting lightweight cryptographic methodologies the reason being most of the IoT devices have resources that are limited in computing. Authors suggest SHA-256 and ECDSA cryptographic schemes are well suited for security. For efficiently managing the key design for sensor nodes authors use Elliptic Curve Cryptography method. The evaluation which was based on security analysis show reductions on communication overhead, offer better security, energy consumption and storage space by using key management scheme.

Some authors use PKI mechanism for authenticating IoT identity users. PKI makes use of certificates for authenticating origin of a key and validation, since all the certificates demand certificate authorities for conforming origin and validity as it consumes time and leads to computational burden Yong Yu et al. (2018), Yannan Li et al. (2018), Junfeng Tian et al. (2018), and Jianwei Liu et al. (2018). Authors after investigating the issues related to privacy and security in IoT they came up with a framework that integrates IoT and blockchain together. This framework powers functionality of IoT with assuring IoT data along with desirable scalability factors such as decentralized payment, authentication and so on.

There are various mechanisms each manufacture implements which are based on protocols, technology and security mechanism. This activity produces safe commercial IoT devices. Every IoT device is exposed to a certain attack type.

there is an urgent need for developing standards and security related policy for IoT products. Yuchen Yang et al. (2017), Longfei Wu et al. (2017), Guisheng Yin et al. (2017), Lijie Li et al. (2017), and Hongbin Zhao et al. (2017) presented a study which was based on issues of IoT and its application system relating to privacy and security. They found limitations in IoT which included computing resources and battery. For these limitations' authors presented solutions for extending battery life and light weight computation. The study shows existing classification approaches for IoT attacks and security mechanisms. Then, authors reviewed the recently proposed IoT authentication schemes and architectures. The last part of this paper analysed the security issues and solutions in four layers, including the perception layer, network layer, transport layer, and application layer.

III. RESULT

The summary of various papers is tabulated in the table below. There are a lot of techniques deployed in various research works addressing the issues and the solutions for it. A quick glance is of the same is present in the table.

Table-1. Summary of the Survey for IoT systems and their issues.

Author and year	Method proposed	Merits	limitations
Junqin Huang et al. (2019)	Method that regulates the access to sensor data	IIoT is more efficient.	No authenticatio n provided
Oscar Novo (2018)	Blockchain technology based IoT architecture	Scalable IoT situations	Attacks on IoT are not addressed
Zhe Yang et al. (2019)	Trust management system which is decentralized	Vehicles maintain reliable, updated and trust consistent blockchain	Hash of the blockchain is not provided with security.
Ali Dorri et al. (2017)	Miner component for handling internal and external communications of the home	Auditing and controlling the communicat ions.	Authenticaio n is not provided
Haifen g Yu et al. (2010)	Addressing DDoS and Sybil attacks	Overcoming effect of these attacks	Authenticaio n is not addressed

Mohamed Amine Ferrag et al. (2019)	Overview of the applications of the blockchains	Various security issues that are present in the blockchain with respect to security	Minimal discussion on the problems to be prioritised.
Ahmed Afif Monrat et al. (2019)	Comparative study and discuss challenges on blockchain	Highlight blockchain technology future scope	Solution on how to overcome existing problems
Chao Lin et al. (2018)	Cryptographic membership authentication scheme	Bind the digital identity of the object to the real-world entity	Light weight cryptographic algorithm not used
Alireza Esfahani et al. (2019)	Authentication using XOR operations and hash	Effective security for authentication	Attacks not addressed
Muhammad Shahzad et al. (2017)	Methodology to overcome lack of conventional user interface for IOT networks	Securing the IoT networks effectively	Time consuming
Zhen Ling et al. (2017)	Case study on smart plug system	Exploit protocols and launching attacks	Not addressed on how to overcome the attacks
Xiaojiang Du et al. (2009)	Suggesting SHA-256 and ECDSA cryptographic schemes are well suited for security	Reductions on communication overhead, offer better security, energy consumption	Other security issues were not addressed
Yong Yu et al. (2018)	Framework that integrates IoT and blockchain together	Framework powers functionality of IoT with assuring IoT data along with desirable scalability factors	Time consuming
Yuchen Yang et al. (2017)	Study which was based on issues of IoT and its application system	They found limitations in IoT	More detailed study must have been provided

IV. CONCLUSION

The paper discusses about the various issues that are present in the IoT system, most of which were related to security. These issues were overcome by using blockchain technology in most of the research work as blockchain was suitable for the IoT devices. The study also concludes why block chain and IoT networks are important and various security issues that are involved in the blockchain and IoT networks. In order to overcome the problems that are involved the study shows what are the measures that can be taken up. We can observe the main reason for the lack of security is because authentication is not incorporated. In the future work there are various fields that can go under enhancements such as the hash key that is generated in the blockchain is not secure there can be mechanisms implemented to address this area of concern. Even though authentication is provided in IoT networks there exists many attacks through which the data is under threat, hence there can be methods implemented in future to overcome this problem.

ACKNOWLEDGMENT

First and foremost, Authors like to express their sincere gratitude to Dr. T N Nagabhushan, Principal, SJCE, Mysuru, for having supported them for the academic endeavors. Authors are grateful to Dr. Shankraiah Head of the Department of Electronics and Communication Engineering for providing them timely suggestions, encouragement and support. Authors are grateful to all the faculty members at their college for their support and guidance.

REFERENCES

1. Junqin Huang, Linghe Kong, Guihai Chen, Min-You Wu, Liu and Peng Zeng," Towards Secure Industrial IoT: Blockchain System with Credit-Based Consensus Mechanism", IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, VOL. 15, NO. 6, JUNE 2019.
2. Oscar Novo," Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT", IEEE INTERNET OF THINGS JOURNAL, VOL. 5, NO. 2, APRIL 2018.
3. Zhe Yang, Kan Yang, Lei Lei, Kan Zheng and Victor C. M. Leung, " Blockchain-Based Decentralized Trust Management in Vehicular Networks ", IEEE INTERNET OF THINGS JOURNAL, VOL. 6, NO. 2, APRIL 2019.
4. Ali Dorri, Salil S. Kanhere, Raja Jurdaky and Praveen Gauravaram," Blockchain for IoT Security and Privacy: The Case Study of a Smart Home", 2017 IEEE.
5. Haifeng Yu, Phillip B. Gibbons, Michael Kaminsky, and Feng Xiao," SybilLimit: A Near-Optimal Social Network Defense Against Sybil Attacks", IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 18, NO. 3, JUNE 2010.
6. Mohamed Amine Ferrag, Makhlouf Derdour, Mithun Mukherjee, Abdelouahid Derhab, Leandros Maglaras and Helge Janicke, "Blockchain Technologies for the Internet of Things: Research Issues and Challenges", IEEE INTERNET OF THINGS JOURNAL, VOL. 6, NO. 2, APRIL 2019.

7. Ahmed Afif Monrat, Olov Schelén And Karl Andersson," A Survey of Blockchain From the Perspectives of Applications, Challenges, and Opportunitie", August 19, 2019, date of current version September 4, 2019.
8. Chao Lin, Debiao He, Xinyi Huang, Muhammad Khurram Khan, And Kim-Kwang Raymond Choo," A New Transitively Closed Undirected Graph Authentication Scheme for Blockchain-Based Identity Management Systems", IEEE 2018.
9. Alireza Esfahani, Georgios Mantas, Rainer Matischek, Firooz B. Saghezchi, Jonathan Rodriguez, Ani Bicaku, Silia Maksuti, Markus G. Tauber, Christoph Schmittner, and Joaquim Bastos," A Lightweight Authentication Mechanism for M2M Communications in Industrial IoT Environment", IEEE INTERNET OF THINGS JOURNAL, VOL. 6, NO. 1, FEBRUARY 2019.
10. Muhammad Shahzad and Munindar P. Singh," Continuous Authentication and Authorization for the Internet of Things", Published by the IEEE Computer Society, 2017 IEEE.
11. Zhen Ling, Junzhou Luo, Yiling Xu, Chao Gao, Kui Wu and Xinwen Fu,"Security Vulnerabilities of Internet of Things: A Case Study of the Smart Plug System", IEEE INTERNET OF THINGS JOURNAL, VOL. 4, NO. 6, DECEMBER 2017.
12. Xiaojiang Du, Mohsen Guizani, *Yang* Xiao, and Hsiao-Hwa Chen, "A Routing-Driven Elliptic Curve Cryptography Based Key Management Scheme for Heterogeneous Sensor Networks", IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 8, NO. 3, MARCH 2009.
13. Yong Yu, Yannan Li, Junfeng Tian, and Jianwei Liu," Blockchain-Based Solutions to Security and Privacy Issues in the Internet of Things", IEEE Wireless Communications December 2018.
14. Yuchen Yang, Longfei Wu, Guisheng Yin, Lijie Li, and Hongbin Zhao," A Survey on Security and Privacy Issues in Internet-of-Things", IEEE INTERNET OF THINGS JOURNAL, VOL. 4, NO. 5, OCTOBER 2017.

AUTHORS PROFILE

Sujatha Kumari B A Prof at SJCE college Mysuru, Dept Electronics and Communication. JSS Science and Technology University.

Sadaf Farheen MTech student at SJCE college Mysuru in Networking and Internet Engineering, Dept Electronics and Communication. JSS Science and Technology University.