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 rise 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 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, IoT (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,
Security of IoT System using Blockchain

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

Blockchain used because of its decentralized nature in various applications

Authors Ali Dorri et al. (2017), Salil S. Kanhere et al. (2017), Raja Jurdak 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.

The IoT enabled with blockchain is the key technology states Mohamed Amine Ferrag et al. (2019), Makhlof 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 authenticity purpose authors use the digital signature.

Importance of authentication in IoT systems

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 IoT 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 came 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.

For efficiency, Xiaojiang Du et al. (2009), Mohsen Guizani et al. (2009), Hsiao-Hwa Chen et al. (2009). 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.

**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.**

<table>
<thead>
<tr>
<th>Author and year</th>
<th>Method proposed</th>
<th>Merits</th>
<th>Limitations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Junqin Huang et al. (2019)</td>
<td>Method that regulates the access to sensor data</td>
<td>IoT is more efficient.</td>
<td>No authenticatio n provided</td>
</tr>
<tr>
<td>Oscar Novo (2018)</td>
<td>Blockchain technology based IoT architecture</td>
<td>Scalable IoT situations</td>
<td>Attacks on IoT are not addressed</td>
</tr>
<tr>
<td>Zhe Yang et al. (2019)</td>
<td>Trust management system which is decentralized</td>
<td>Vehicles maintain reliable, updated and trust consistent blockchain</td>
<td>Hash of the blockchain is not provided with security.</td>
</tr>
<tr>
<td>Ali Dorri et al. (2017)</td>
<td>Miner component for handling internal and external communications of the home</td>
<td>Auditing and controlling the communications.</td>
<td>Authenticatio n is not provided</td>
</tr>
<tr>
<td>Haifeng Yu et al. (2010)</td>
<td>Addressing DDoS and Sybil attacks</td>
<td>Overcoming effect of these attacks</td>
<td>Authenticatio n is not addressed</td>
</tr>
</tbody>
</table>
Security of IoT System using Blockchain

<table>
<thead>
<tr>
<th>Authors</th>
<th>Section</th>
<th>Discussion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mohamed Amine Ferrag et al. (2019)</td>
<td>Overview of the applications of the blockchains</td>
<td>Various security issues that are present in the blockchain with respect to security</td>
</tr>
<tr>
<td>Ahmed Afif Monrat et al. (2019)</td>
<td>Comparative study and discuss challenges on blockchain</td>
<td>Highlight blockchain technology future scope</td>
</tr>
<tr>
<td>Chao Lin et al. (2018)</td>
<td>Cryptographic membership authentication scheme</td>
<td>Bind the digital identity of the object to the real-world entity</td>
</tr>
<tr>
<td>Alireza Esfahani et al. (2019)</td>
<td>Authentication using XOR operations and hash</td>
<td>Effective security for authentication</td>
</tr>
<tr>
<td>Muhammad Shahzad et al. (2017)</td>
<td>Methodology to overcome lack of conventional user interface for IoT networks</td>
<td>Securing the IoT networks effectively</td>
</tr>
<tr>
<td>Zhen Ling et al. (2017)</td>
<td>Case study on smart plug system</td>
<td>Exploit protocols and launching attacks</td>
</tr>
<tr>
<td>Xiaojing Du et al. (2009)</td>
<td>Suggesting SHA-256 and ECDSA cryptographic schemes are well suited for security</td>
<td>Reductions on communication overhead, offer better security, energy consumption</td>
</tr>
</tbody>
</table>
| 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 | SECURITY OF IoT SYSTEM USING BLOCKCHAIN

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 blockchain 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


8. Chao Lin, Debiao He, Xinyi Huang, Muhammad Khurram Khan, And Kim-Kwang Raymond Choo,” A New Transitivity Closed Undirected Graph Authentication Scheme for Blockchain-Based Identity Management Systems”, IEEE 2018.


10. Muhammad Shalzad and Munindar P. Singh,” Continuous Authentication and Authorization for the Internet of Things”, Published by the IEEE Computer Society, 2017 IEEE.


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.