International Journal of Academic Multidisciplinary Research (IJAMR)
ISSN: 2643-9670
Vol. 4 Issue 2, February – 2020, Pages: 60-65

Internet of Things Security Issues and Their Solutions with Blockchain Technology

[1]Ibrahim frank, [2]Tumain mbinda
[1]School of Computer Science
Hubei University of Technology, Wuhan China
frankibrahim25@gmail.com

[2]College of information and communication technology
Mbeya University of science and technology, Tanzania
trmbinda@gmail.com

Abstract: *The technology behind bitcoin and other cryptocurrencies is a distributed ledger database for recording transaction, usually known as blocks. Blockchain technology enables users to share their ledger of transactions. The application of this technology in the field of IoT seek to guarantee the security and privacy of the data of the digital interconnection of physical devices via the internet. This paper analyses the application of blockchain as best countermeasure to combat the IoT security vulnerabilities. Then the analysis of blockchain is done and the benefits the combination of this technology with the IoT can provide.*

Keywords— Internet of Things, Blockchain, IoT security, and application of blockchain.

1. INTRODUCTION

The IoT is growing exponentially year by year with its aim in 5G technologies, like Smart Homes and Cities, e-Health, distributed intelligence etc. but it has challenges in security and privacy. The IoT devices are connected in a decentralized approach. So, it is very complex to use the standard existing security techniques in the communication among IoT nodes. The Blockchain is a technology that provide the security in transactions among the IoT devices. It provides a decentralized, distributed and publicly available shared ledger to store the data of the blocks that are processed and verified in an IoT network. The data stored in the public ledger is managed automatically by using the Peer-to-peer topology. The Blockchain is a technology where transactions fired in the form of a block in the Blockchain among IoT nodes. The blocks are linked with each other and every device has its previous device address. This paper explores the process of incorporating blockchain with a very vulnerable centralized IoT data transactions.

2. LITERATURE REVIEW

The first step of this paper was through literature review. The goal of the literature review was to gain enough understanding in the field of IoT and blockchain. Ten papers were reviewed from different authors and below are their short summary. In the first article, the authors explore the security techniques that are designed or applicable to the IoT. The article are then sorted into reactive (intrusion detection system and collaborative security approaches) and proactive approach. In the article [2], the authors presents a new architecture of managing IoT devices. The architecture provide decentralized access control system connected to geographically distributed sensor networks. The solution based on blockchain technology where the access control policies are enforced by it.

In the article [3], the author propose IoT chain that combines OSCAR and the ACE authorization of information exchanged between two nodes in an IoT networks. In the article [4], the authors focus on significant of security issues for IoT alongside the current attacks. They presented blockchain technology as the remedy to take care of numerous IoT security issues. The authors in article [5], pointed out the challenges of IoT and blockchain, also analyzed the advantage of the combined two (IoT and blockchain technology). In article [6], the authors pointed out that the exchange of information between the things and IoT network

architecture results huge data generation at centralized data managements systems (CDMS). This lead to various security and privacy issue in IoT making it as the challenge to encounter. The author continue explaining that to address the security and privacy issue in IoT we can eliminate centralized maintenance of the Network Plentiful Things(NPT) produced data and there by introducing the new distributed ledger-based technology called a blockchain technology.

In the article [7], the authors presented the overview of blockchain technologies in IoT and provide a threat of classification models which are identity based attacks, manipulation based attacks, cryptanalytic attacks, reputation based attacks, and service based attacks. In article [8], the authors explore the major security issues in IoT with regard to IoT layered architecture. Also they explain protocols used for networking, communication and management. Sarika and Nishtha in article [9], they presents the routing attacks such as sinkhole and selective forwarding. They presented an algorithm for detection and prevention i.e. KMA (Key Match Algorithm) and CBA (Cluster Based Algorithm).

3. INTERNET OF THING

Internet of Things means that everyday objects like cars and refrigerators will be able to interact and communicate via embedded systems. This will lead to a distributed network of devices that can communicate with both humans and between each other. Other terms like Industrial Internet, Machine-to-Machine (M2M) communication and Internet of Everything have also been used to describe this phenomenon. IoT includes all devices and objects whose state can be altered via Internet with or without the interaction of a human. IoT was first introduced in the context of supply chain management but today there is a wide range of possible application areas. The main goal is to make computers manage information with no help of a human. Application of IoT could for example lead to the tracking of parking arrangements, tracking of pollution levels, managing traffic signals, home automation, energy consumption monitoring, supply chain control monitors, product tracking and M2M communication.

3.1 IoT ARCHITECTURE

There have been discussions about how to approach the architecture of the IoT system and yet there is no established reference model. The basic model is to approach a three-layer architecture consisting of the Physical Perception Layer (PPL), the Network Layer (NL) and the Application Layer (AL). But in recent literature, the five-layer architecture (shown in figure 1) seems to be the most applicable model for IoT applications. Therefore the five-layer model will be used in this summary to describe the architecture of an IoT system.

Application layer	Business layer
	Application layer
Network layer	Processing layer
	Transport layer
Perception layer	Perception layer

Figure 1. The 3-layer architecture on the left and 5-layer architecture on the right

3.2 IOT TECHNOLOGIES AND VULNARBILITIES

According to Jie Lin, Wei Yu, Nan Zhang, Xinyu Yang, Hanlin Zhang, and Wei Zhao on their survey paper (2017) there exist five essential IoT technologies that are widely used for IoT-based products and services. These are Radio frequency identification (RFID), Wireless sensor networks (WSN), Middleware, Cloud computing and IoT application software which will be explained in this section.

Radio frequency identification (RFID), captures data using radio waves, a tag and a reader. The tag can store data and contains it in the form of an Electronic Product Code (EPC). Three different types of tags can be used that are passive tags, active tags or semi-passive tags. Passive tags do not have any batteries but instead rely on power from radio frequency energy. These sorts of tags are common in supply chains, passports and item

tracking. Active tags have batteries and can have external sensors that can monitor conditions like temperature and pressure and are commonly used in manufacturing and laboratories. Semi-passive tags have batteries for the microchip but have to get power from the reader. Active tags and semi-passive tags cost more than passive tags. The most common vulnerabilities for RFID are;

- Dos attacks, these attacks want to consume the resources of the system. This attacks is accomplished by flooding the targeted machine with superfluous in an attempt to overcharge system and prevent request from being fulfilled.

- Skimming, the attack observe the information exchanged between a legitimate tag and legitimate reader. Through the extracted data the attacker attempts to make a cloned tag which imitates the original RFID tag. The data stored in RFID chips in credits cards, and password can be read without your knowledge then duplicated.

- Eavesdropping, an authorized individual uses an antenna in order to record communication between legitimate RFID tags and readers. Eavesdropping attack can be done in both direction: tag to reader and reader to tag.

- Replay attack, the communication signal between reader and tag is intercepted, recorded and then duplicated.

- Side channel attacks, the information that is targeted include power consumption, timing information, and electronic fields. These attacks require a deep knowledge of the internal system on which cryptographic algorithms are implemented.

Wireless sensor networks (WSN), can monitor physical or environmental conditions and are used with RFID tags to better track temperature and location for example. WSN also handles different network topologies and communication that needs to hop over numerous systems to reach the final destination. WSN have been used for tracking food that is sensitive for changes in temperature. The most common attacks are;

- Use Sybil, the attacker make multiple identities and replicate a single node. The identities could be stolen or fabricated.

- Wormhole, an attacker receives the packet at one point in the network, relocates them to another point in the network and then replace them in the network from that point.

- Spoofing, the attacker falsifies the origin of the packages making the victim believe that they are from trusted host to prevent the victim from detecting it.

Middleware is software that acts as a layer between an operating system or database and applications. This facilitates the work for software developers to perform communication.

Middleware also simplifies the integration of new technologies into new ones, which is really needed in the development of IoT services. One example is Global Sensor Networks (GSN) that is open middleware software that enables the deployment of sensor services with very little programming needed.

It is called cloud computing when using a network for on-demand access to Internet for storing, managing and processing data instead of using a local server. Cloud computing is a shared pool of configurable resources like computers, networks, servers, services and applications. It can either supply as an Infrastructure as a Service called IaaS or as a Software as a Service called SaaS. Cloud computing is needed in IoT services because of the massive amount of data that IoT devices are harvesting. That data needs to be stored, processed and streamed which cloud computing can provide. The security issues in cloud computing include;

- Wrapping attack, this is made by duplication of the user account and password in the log-in phase and SOAP2 messages that are exchanged during the setup phase between the web browser and the server are affected by the attackers.

- Flooding attack, it happen when an attacker generate fake data, which could resource some type of code to be run in the application of the legitimate user.

International Journal of Academic Multidisciplinary Research (IJAMR)
ISSN: 2643-9670
Vol. 4 Issue 2, February – 2020, Pages: 60-65

IoT applications provide interaction between device-to-device as well as human-to-device. IoT applications on devices make sure that data or messages have been received and acted upon. For example monitor applications are used in transports to monitor the temperature and humidity on food as well as on the packaging to make sure that no one has tampered with it. In the best of worlds the applications have intelligence in a way that the IoT devices can communicate with each other so that they can identify and solve problems without the help of humans.

4. BLOCKCHAIN

Blockchain is a distributed database that registers an ordered list of records of transaction which are immutable linked together through a chain, on block. The block form a linear sequence where each block reference the harsh of the previous block, forming a chain of blocks. Blockchain is maintained by a network of nodes and each one of them executes and records the same transactions. Any node in the network can read the transaction.

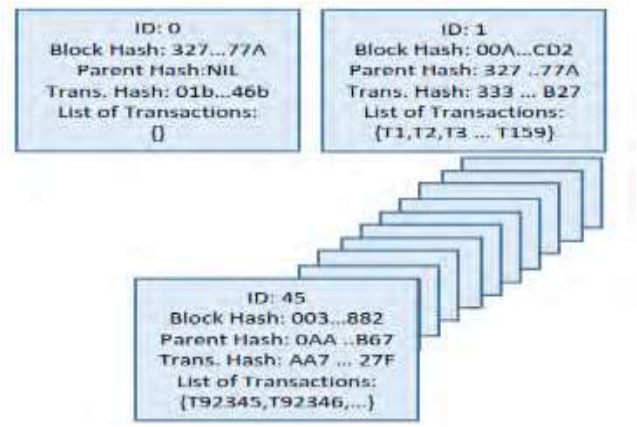

Figure 2. A sample blockchain

This technology has several key characteristics that include: decentralization, persistency, anonymity, and auditability. Apart from what has been mentioned above, it should also be added that the most interesting feature of the blockchain is that it can work in a decentralized environment. This environment is enabled by integrating several core technologies such as cryptographic hash, digital signature (based on asymmetric cryptography) and distributed consensus mechanism.

However, there might arise the question that to what extent is this "decentralized" blockchain technology reliable. In order to make it more reliable, the solution proposed by Nakamoto to use a protocol implemented by the timestamp server. In the blockchain model, the work of the timestamp server is to take a hash of a block of items, timestamp it and then widely publish the hash. The objective of the timestamp is to prove that the data exists at the time, and as a result, can get into the hash.

4.1 *Public and private block chain*

Public blockchains are open network that enable anybody to take part in the network. Such a network relies on the quantity of members for its prosperity, and thus encourages more participation through an incentivization mechanism. The best case of a public blockchain is Bitcoin where members in the network (miners) are remunerated with BTC tokens. By letting other nodes in the network verify transactions and information exchange there is no need for trust between operating nodes. These types of blockchains are regarded as fully distributed.

4.2 Private Blockchain

Participation in a private blockchain requires an invitation, which itself is also validated by the network starter or a set of rules that can put into place. Such a network is known as a permissioned network, and puts a restriction on who is allowed to join. Restrictions are put in the network, such as the rights to modify, read and write information. These rights are kept centralised to one party, for example a company, and since the power is centralised there is often no need for a consensus protocol.

4.3 Smart Contract

Is a piece of code that reside on a block chain, it is identified by unique address and includes a set of executable functions and state variables. These functions are executed when transaction are made to those functions. Input parameters are included

in the transaction and are required by functions in the contract. Etherum is an open and programmable blockchain platform that is powered by peers who run the Etherum nodes. Everybody can sign up for the platform and create an Etherum account and create smart contract and also build decentralized applications.

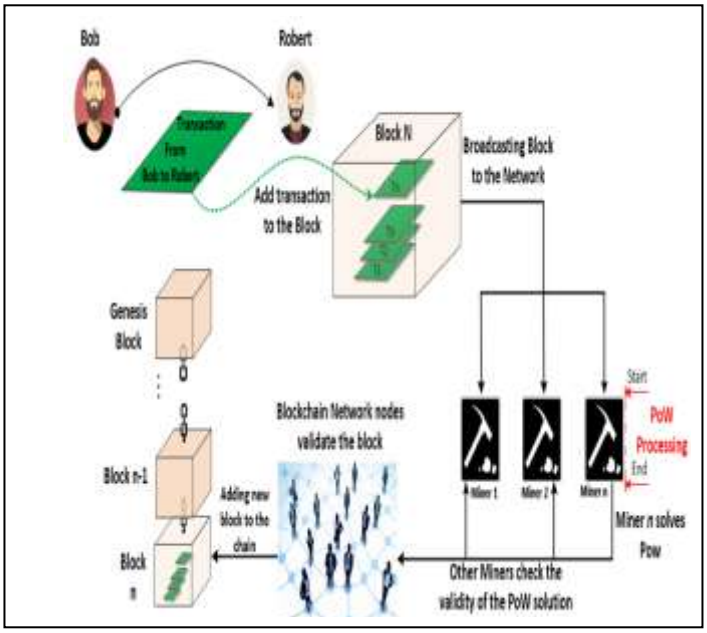

Figure2 Example of a IoT with blockchain

5. BLOCKCHAIN AND INTERNET OF THING

IoT and blockchain may work together in the way that blockchain technology may be the solution of some challenges that IoT are facing. Blockchain might be used to strengthen the IoT security and have been used for storing information about provenance of goods, identity and credentials. The goal is to get data securely to the right place, at the right time, in the right format but this is easier said than done for many reasons. But by applying blockchain technology to IoT devices, treating information transfers as cryptocurrency transactions (like bitcoin), trust less information sharing between devices might be possible to achieve. Devices will leverage smart contracts to model the agreement between two parties.

Decentralization and scalability, another advantage that could be achieved if blockchain was implemented to IoT, is lack of central control. This would ensure scalability and robustness by spreading the resources among the participation nodes and it would eliminate the single point of failure risk.

Autonomy, blockchain can allow IoT devices to communicate with each other and for transaction in an autonomous way as each device has its own blockchain account and there is no requirement for a trusted third-party.

Security, blockchain provide secure and more integrity for data vulnerabilities through verification. Transaction are signed and verified cryptographically to prove that the originator is one who have sent the message.

Reliability, IoT data can stay immutable and distributed over time in block chain. Members of the system are able of confirming the realness of the information and have the certainty that they have not been altered with.

6. CONCLUSION

This paper presents an overview of the IoT paradigm and the blockchain technology from a security approach. We have seen typical IoT architecture which are 5- layer architecture, there is no general consensus to establish a reference architecture. Moreover the most important technologies within IoT have been discussed and the main threat of them.

Blockchain technology can be the best solution to cover the need for quicker growth of smart connected devices that look for safe and reliable environments for data storage and management.

Implementation of blockchain into the IoT system comes with some challenges. For example the mining process of blockchain consensus protocol PoW is very computationally intensive and IoT devices are normally resource restricted. The mining time of blocks are also relatively time consuming while low latency is highly desirable in many IoT devices.

REFERENCES

[1] Mandrita Benerjee, Junghee Lee, Kim-Wang, Raymond Chao A blockchain future for internet of thing security.

[2] Olivier Alphand, Michele Amoretti, Timothy Claeys, Simone Dall 'Asta, Andrzej Duda, Gianluigi Ferrari, Franck Rousseau, Bernard Tourancheau, Luca Veltri, Francesco Zanichelli: A Blockchain Security Architecture for the Internet of Things.

[3] Abid Sultan, Muhammad Sherez, Arshad malick and Azhar Mushtaq: IoT security issues and their solution with blockchain technology.

[4] Oscar Novo Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT.

[5] Ana Reyna , Cristian Martín, Jaime Chen, Enrique Soler, Manuel Díaz: On blockchain and its integration with IoT. Challenges and opportunities.

[6] Nallapaneni Manoj Kumara, Pradeep Kumar Mallickb: Blockchain technology for security issues and challenges in IoT.

[7] Mohamed Amine Ferrag, Makhlouf Derdour, Mithun Mukherjee, Member, IEEE, Abdelouahid Derhab, Leandros Maglaras, Senior Member, IEEE, Helge Janicke: Blockchain Technologies for the Internet of Things: Research Issues and Challenges.

[8] Minhaj Ahmad Khan a, Khaled Salah; IoT security: Review, blockchain solutions, and open challenges.

[9] Sarika Choudhary, Nishtha Kesswani; Detection and Prevention of Routing Attacks in Internet of Things.

[10] Yuchen Yang, Longfei Wu, Guisheng Yin, Lijie Li, and Hongbin Zhao; A Survey on Security and Privacy Issues in Internet-of-Things.

[11] Rezaei M, Shirazi A M, Karimi B. (2017). IoT-based framework for performance measurement: A real-time supply chain decision alignment. Industrial Management & Data Systems. Vol. 117, Iss. 4, pp. 688-712.

[12] Schiener D. (2017). A Primer on IOTA (with Presentation). URL: https://blog.iota.org/a-primer-on-iota-with-presentation-e0a6eb2cc621 (Accessed: 2018-03-13).

[13]] Statista. (2016). Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions). URL: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/ (Accessed: 2018-01-25).

[14] Thompson C. (2016). The difference between a Private, Public & Consortium Blockchain: A Simple Explanation for Dummies. URL: https://www.blockchaindailynews.com/The-difference-between-a-Private-Public-Consortium-Blockchain_a24681.html (Accessed: 2018-01-26).

[15] Vigna P, Casey M. (2015). The age of cryptocurrency: how bitcoin and digital money are challenging the global economic order. New York: St. Martin's Press. Vigna P, Casey M. (2015). *The age of cryptocurrency: how bitcoin and digital money are challenging the global economic order*. New York: St. Martin's Press.