Authenticating IoT Devices issues based on Blockchain

Hosny. H. Abo Emira[3]

[3]Faculty of Computers and Information, Nahda University, Computer Science Department, hosny.aboemira@gmail.com

Abstract: The Internet of Things (IoT) has become a growing reality today. However, special attention remains to be paid to some key challenges in order for IoT solutions to support the growing demand for connected devices and services provided. Given the importance and sensitivity of facilities, IoT solutions should address security and privacy concerns near these devices and the data that they collect, generate and process. Recently, Blockchain technology has gained a lot of interest in IoT solutions. There are their primary use scenarios in the financial field, as Blockchain creates a promising and useful application world for solving security and privacy issues However, this emerging technology has great potential in the most diversified technological fields and can greatly help in achieving IoT vision in various aspects, increasing decentralization capacity, enabling new transaction models, and allowing independent coordination of devices. The paper's goal is to provide the ideas about the structure and operation of Blockchain and, typically, analyze how the use of this technology can be used to deliver security and privacy in IoT.

Keywords: The Internet of Things (IoT); Blockchain; Man-in-the-Middle Attack; A distributed denial-of-service (DDoS) Attack; Replay Attack; Sybil Attack.

1. Introduction

Internet of Things (IoT) and Blockchain are considered developing concepts and technologies. At the same time, they transform concepts and create new possibilities, each in their respective scenarios, and there is an opportunity to create applications that can share the inherent features of both, traveling how the IoT can advantage from the decentralized nature of the Blockchain.

The Internet of Things (IoT) is expanding at a fast pace and some reports predict that IoT devices will grow to 26 billion this year 2020, which are 30 times the estimated number of devices deployed in 2009 and is far more than the 7.3 billion smartphones, tablets, and PCs that are expected to be in use This year 2020. Moreover, some predictions anticipate a fourfold growth in Machine-to-Machine (M2M) connections in the next years, which may be related to a broad range of applications like home automation, transportation, defense and public safety, wearables or augmented reality.

Security solutions and privacy should be implemented according to the characteristics of heterogeneous IoT devices. There is a demand for security solutions that can deliver equivalent levels of security for various types of devices and demand mechanisms capable of audit and access control in these environments.

In this background that Blockchain also falls, because this technology can be used to authenticate, authorize, and review data generated by devices. Also, because of its decentralized nature of work, it eliminates the need to trust in the third party and does not have a single point of failure.

Blockchain (also known as "the protocol of trust") is an idea that aims to decentralize as a security measure, has a function to create a global index for all transactions that happen in each network, and makes them unchallengeable. It works as a shared, public, and universal ledger. It creates agreement and confidence in direct communication between two parties, without any third party. We also can use Blockchain in the supply chain, smart contracts, and digital identity management and some other applications.

DOI: 10.5281/zenodo.3687226

This paper goals to explain newly interested, as well as updating the readers who have some previous knowledge of Blockchain, and this includes the recent applications in security and privacy, and how their use can control the IoT. The approach offered will be a review of the state-of-the-art articles in which the Blockchain is used to deliver some level of privacy and security to IoT.

2. Security issues in IoT

Securing IoT from a variety of possible attacks is a quite complex job. However, it becomes controllable to some extent when referenced under its layered architecture. Every layer has its limitations and vulnerabilities that need to be identified to ensure its security by preventing it from different types of attacks. Preventing such attacks needs a proper security system that addresses existing vulnerabilities present in an IoT device. For that we need to first zoom in the term weakness and how does it donate to an attack. A vulnerability in a system represents the incompetence of the system that enables the attacker to find out the scope to invade the system security. It can lead to a threat that in turn lead to an attack when get ignored. In this section, we present the list of vulnerabilities along with its contributing factors which are accountable for the occurrence of any cyber-attack on IoT devices.

2.1 *Man-in-the-Middle Attack in IoT*

At the point when the devices are authorized into a system, important keys, security, and space parameters can be vulnerable towards prying eyes. The vital keys can uncover the most secured key among devices and originality of the correspondence channel could be endangered. MITM attack is one sort of overhearing stealthily imaginable in the appointing period of devices to IoT. The key foundation convention is defenseless against man-in-the-middle attack and can trade off device confirmation as devices as a rule don't have earlier information about one another. As device validation includes the trade of device characters, an impersonation of the identity can become a reality because of man-in-the-middle attack.

2.2 *A distributed denial-of-service (DDoS) Attack in IoT*

DDoS attacks is a threatening endeavor to disturb typical traffic of a focused-on server administrationor system by overpowering the objective or its encompassing framework with a surge of Web traffic. DDoS attacks achieve effectiveness by employing multiple compromised computer systems as sources of attack traffic. Utilized machines can include computers and other networked resources such as IoT devices. A DDoS attack is like a traffic congestion blocking up with highway, preventing regular traffic from arriving at its desired destination.

2.3 *Replay Attack in IoT*

During the transfer of authentication data or different accreditations in IoT, this data can be modified, adjusted, or replayed to repulse the traffic. This causes an intense replay attack. Replay attack is basically one type of dynamic man-in-the middle attack. A replay attack happens when a cybercriminal pries in on a protected system correspondence, blocks it, and afterward deceitfully delays or resends it to mislead the collector into doing what the programmer needs. The additional danger of replay attack is that a programmer doesn't require high-level technical knowledge to decode a message subsequent to catching it from the system. The attack could succeed just by resending the entire thing. A case of it can be a person at an organization requests a monetary exchange by sending an encoded message to the organization's account major. An impersonator pries in on this message, catches it, and is now in total control of a situation to resend it. Since it is a credible message that has been produced, the message is as of now effectively scrambled and looks genuine to the account officer.

2.4 *Sybil Attack in IoT*

A Sybil attack is a kind of security danger on an online system where one person tries to take over the network by creating multiple accounts, nodes, or computers. This can be as simple as one person creating multiple accounts on social media. But in the world of cryptocurrencies, a more

DOI: 10.5281/zenodo.3687226

applicable example is where somebody runs multiple nodes on a blockchain network. The word "Sybil" in the name comes from a case study about a woman named Sybil Dorsett, who was preserved for Dissociative Identity Disorder also called Multiple Personality Disorder

• Attackers may be able to defeat the honest nodes on the network if they create enough fake identities (or Sybil identities). They can then reject to receive or transmit blocks, successfully blocking other users from a network.

• In Sybil attacks large-scale, where the attacker's control on most of the network computing power or hash rate, they can carry out a 51% attack. In such issues, they may change the planning of transactions, and prevent transactions from being confirmed. They may even reverberate transactions that they made while in control, which can lead to double spending. Over the years, computer scientists have devoted a lot of time and research to figure out how to detect and prevent Sybil attacks, with varying degrees of effectiveness. For now, there is no ensured defense.

3. Taxonomy of defense mechanisms in IoT network

3.1 Blockchain based MITM defense

The network security is a pending challenge for the IoT industry which is quite trending. The proposed model **Figure.1** in [1] uses Blockchain for providing secure access control to IoT devices. The proposed model adventures the stability feature of Blockchain to store the whitelist of devices. The account number in Blockchain resolves the issue of no unique identifier in IoT. As the whitelist is stored on Blockchain, no one can alter its contents providing better access control and authentication. The timestamp and device id combination help in combating man in the middle attack. The proposed model scales and is quite efficient for access control and uses a combination of IoT and Blockchain. Man-in-the middle attack: For authentication, the devices send SHA of current timestamp the authentication token is encrypted, and the hash changes every time a device makes a request. For access control, the man in the middle attack is possible if the attacker eavesdrops on the Id but as the token is hashed no one can extract device id from it.

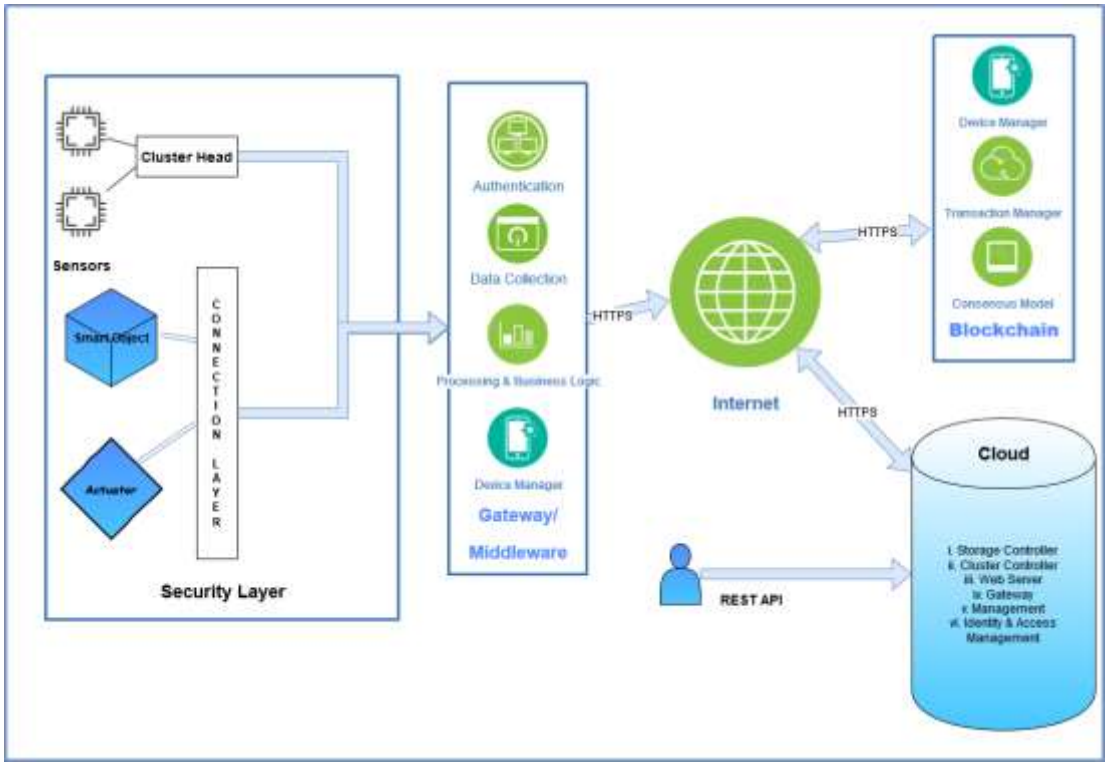

Fig. 1. Architecture of Proposed System for IoT - Blockchain

3.2 Blockchain based DDoS defense

DOI: 10.5281/zenodo.3687226

This proposed model uses the blockchain which is an online distributed ledger consuming a list of blocks containing a hash of the previous block along with an arranged recorded timestamp. These model blockchains are used for the self-executable computer programs called Smart contracts. The smart contract in the system is responsible for simplifying secure communication between the IoT devices and the distributed servers. One of such smart contracts is called Ethereum, one of the largest online established software platforms. It allows smart contracts and decentralized applications (DApps) to be built on blockchains along with their state. State in Ethereum denotes to the data present in the blockchain and a state transition occurs when a transaction happens. Ethereum has a gas limit attribute to ensure that no further resources can be consumed once the limit is exceeded. This limit is set for each transition processed through it which prevents the system from getting overloaded. The word 'gas' used here is analogous to the word "resource" in Ethereum terms i.e. a certain amount of gas for a function refers to the number of resources a function has for its execution. Blockchain has been used here because of its transparent and decentralized approach of storing the data across the network. **Figure.2** shows the IoT blockchain system for defending DDoS.

Fig. 2. The IoT blockchain system for defending DDoS

3.3 *Replay Attack*

Preventing such an assault is tied in with having the correct technique for encryption. Encoded messages convey "keys" inside them, and when they are decoded toward the finish of the transmission, they open the message. In a replay assault, it does not make a difference if the assailant who captured the first message can peruse or decode the key. All the person in question needs to do is catch and resend the whole thing — message and key — together. To counter this chance, both sender and collector ought to set up a totally irregular meeting key, which is a sort of code that is just substantial for one exchange and cannot be utilized once more. Another deterrent measure for this sort of assault is utilizing timestamps on all messages. This keeps programmers from resenting messages sent longer prior than a specific period of time, along these lines lessening the lucky opening for an aggressor to listen in, redirect the message, and resend it.

The proposed Firmware-Over-the-Blockchain system in **[3]** comprises of four procedures. The main procedure is the making of a firmware update contract. Every gadget maker is required to make a firmware update contract after discharging another variant of firmware, and the made firmware update contract must

DOI: 10.5281/zenodo.3687226

pass the p2p check process inside the blockchain arrange. The subsequent procedure is the formation of outsider refreshed firmware. There are two purposes for the outsider refreshed firmware process. To begin with, it empowers the firmware merchant to change a current adaptation of firmware to give an auspicious fix on the issues found in the current distributed firmware. Second, it empowers the conveyed IoT gadgets to acquire the bona fide and the most recent form of firmware expeditiously from different alternatives: the comparing merchant storehouses and the outsider firmware archives. The third procedure is the PUSH update component that permits a refreshed firmware to be effectively disseminated to doors after the relating firmware update contract passes the p2p confirmation process. The last procedure is the Draw update instrument that permits an IoT gadget to physically download the new form of firmware from the steady merchant store or the outsider firmware archives.

3.4 Sybil Attack

The proposed model in [4] uses permission blockchain's architecture to securely enroll IoT devices and issue their identities Figure.4. Every IoT device holds a blockchain identity that is verified ahead of transaction execution. In addition to verifying that a submitted transaction carries a valid IoT device signature, it is evaluated for proper format. Additionally, submission timestamp is checked to ensure the transaction has not been submitted before. This protects our model from being affected by message replay attacks. Through this validation, Sybil nodes cannot influence the network, as they cannot replicate this type of identity. If the transaction passed these checks, the blockchain uses defined logic to determine whether to approve or reject the transaction. This is determined in trust evaluation. By implementing a proof-of-concept of our IoT trust model prototype.

The Sybil attack, where a malicious node generates several identities to hide its real identity, was addressed in [5]. The authors proposed Sybil Free APIT (SF-APIT), a secure localization scheme for antagonistic distributed wireless sensor networks that can detect Sybil nodes. The detection mechanism is based on the received signal strength.

4. CONCLUSIONS

Trust in most IoT networks is presumed implicitly. Trust issues in IoT environment are one of the main causes of Sybil attacks. Sybils in the IoT network hold replicated identities. By controlling multiple identities that appear valid, adversaries can disrupt the network and manipulate reputations of trusted devices. An important aspect of securing IoT networks is maintaining a trusted IoT environment.

It should be noted that none of the presented examples of blockchain-based IoT security solution suggestions give full protection in contradiction of all possible security threats and attacks. Moreover, the applied deployment of these security solutions is still a future issue. A practical security solution for an IoT system can, therefore, combine a choice of blockchain-based security solutions with a set of other security solutions. The current rapid increase of IoT implementations and the IoT security incidents that have hitherto occurred emphasize the necessity of continued research on improving decentralized security measures and the reliability of IoT systems.

References

[1] Ghadekar, P., Doke, N., Kaneri, S. and Jha, V. (2019). Secure Access Control to IoT Devices using Blockchain. *International Journal of Recent Technology and Engineering*, 8(2), pp.3064-3070.

[2] Uzair Javaid, Ang Kiang Siang, Muhammad Naveed Aman, and Biplab Sikdar. (2018). Mitigating IoT Device based DDoS Attacks using Blockchain. In Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems (CryBlock'18). Association for Computing Machinery, New York, NY, USA, 71–76.

[3] Yohan, A. and Lo, N. (2019). FOTB: a secure blockchain-based firmware update framework for IoT environment. International Journal of Information Security.

[4] S. Asiri and A. Miri, "A Sybil Resistant IoT Trust Model Using Blockchains," 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 2018, pp. 1017-1026.

DOI: 10.5281/zenodo.3687226

[5] Y. Yuan, L. Huo, Z. Wang and D. Hogrefe, "Secure APIT Localization Scheme Against Sybil Attacks in Distributed Wireless Sensor Networks," in IEEE Access, vol. 6, pp. 27629-27636, 2018.
[6] M. Pilkington, Blockchain technology: principles and applications. research handbook on digital transformations, F. X. Olleros andM. Zhegu, Eds., 2016.
[7] Jesus, E., Chicarino, V., de Albuquerque, C. and Rocha, A. (2018). A Survey of How to Use Blockchain to Secure Internet of Things and the Stalker Attack. Security and Communication Networks, 2018, pp.1-27.
[8] Gartner. Report: “Forecast: The Internet of Things, Worldwide, 2013”.Nov. 2013.
[9] Cisco Systems. White paper: Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2016–2021. March 2017.
[10] Fraga-Lamas, P., Fernández-Caramés, T. M., Castedo, L. "Towards theInternet of Smart Trains: A Review on Industrial IoT-Connected Railways" in Sensors, vol. 17 (6), no. 1457, pp.1–44, June 2017.
[11] Pulkkis, Göran, et al. "Blockchain-based security solutions for iot systems." Internet of Things A to Z: Technologies and Applications 20180501 (2018).

DOI: 10.5281/zenodo.3687226