International Journal of Pure and Applied Mathematics
Volume 119 No. 16 2018, 3677-3686
ISSN: 1314-3395 (on-line version)
url: http://www.acadpubl.eu/hub/
Special Issue

http://www.acadpubl.eu/hub/

Blockchain Security for Internet of Things: A Literature Survey

Ms.S. Madumidha
Assistant Professor/IT, Sri Krishna College of Technology,
Coimbatore, Tamilnadu
madumidhas@hotmail.com

Dr. P. SivaRanjani
Professor/ECE, Kongu College of Engineering,
Coimbatore, Tamilnadu
sivaranjani@kongu.ac.in

Mr.Siddharth Rajesh
Information Technology, Sri Krishna College of Technology,
Coimbatore, Tamilnadu
sidiyerofficial@gmail.com

Mr. Santhosh Sivakumar
Information Technology, Sri Krishna College of Technology,
Coimbatore, Tamilnadu
santhoshsivakumar12@gmail.com

Abstract:

The Internet of Things (IoT) is experiencing a tremendous growth in areas of research and industry; however, still suffers from security issues. Conventional security mechanisms haven't really proven to offer optimum security. BlockChain (BC) is a new revolutionary technology that utilizes the crypto-currency Bitcoin, which has been used recently to provide security and privacy in peer-to-peer networks. The Internet of Things (IoT), blockchain, and peer-to-peer methodologies assumes an imperative part in the improvement of decentralized information serious applications. Our objective is to understand whether the blockchain and IoT design can be utilized in the encourage of decentralized applications. As an initial phase in our examination procedure, a methodical writing survey on IoT engineering and its present issues with the countermeasures for vulnerabilities in IoT design are talked about. We discovered countermeasures that tends to the assaults in the IoT engineering. To assemble learning on the present utilization of innovation, a blockchain display is archived its present level of Honesty. We likewise found a few issues in respectability and found that the blockchain generally relies upon the trouble of the Proof-of-Work and trustworthiness of miners. We archived and considered the present employments of the blockchain and addresses the previously mentioned issues.

Keywords-*Internet of Things, Blockchain, Integrity, Security, Proof-of-Work.*

I. INTRODUCTION

The Internet is definitely one of the most valuable inventions in the history of humankind. It has made our lives simpler and has made the entire world, a global village. The Internet has ensured that we enjoy the privileges offered by it such as fast and efficient communication, access to knowledge at our fingertips and so many offers that are more exciting. The Internet is evolving and getting more advanced every day, every moment. Internet of Things is a wide field and a great application of the Internet to control the daily used objects, known as 'things' via sensors through the Internet. IoT [1] can be described in simple words as a network of connected heterogeneous devices or so called 'things' which enable us to communicate with them using the protocol of machine-to-machine communication. IoT was developed with the sole intention to make our lives better by allowing us to communicate with daily objects and control those using sensors [2], which are available for quite a cheap price such as Raspberry Pi, Arduino Uno, etc. Though IoT [15] [16] has achieved the desired success by the perfect implementation of communication of objects with each other, demonstrating machine-to-machine communication, the main concern is the data security [3] provided by all the currently used IoT security mechanisms as none of them assures perfect data security. Various security vulnerabilities have been discovered in the connected devices ranging from vehicles to smart-locks. The security issues have concerned many users throughout the world, as they fear their data being leaked, or in worse conditions, stolen by a hacker who could misuse that stolen data [4]. Usual security mechanisms applied in IoT systems [5] are AES-256 (Advanced Encryption System) or sometimes lightweight encryption techniques such as SHA [6] (Simple Hashing Algorithm) i.e. SHA-1. SHA-256,etc. are used to secure the data. IoT can also be called as the base for the future of the development of the Internet, if not the future as it has led to new technologies such as WoT, etc. WoT [7] can be defined as Web of Things. It is based on IoT and is a futuristic technology designed to make our lives better and simpler. However, every technology is destined to either be replaced or be improved upon by another technology. In this paper, we shall discuss about the implementation of blockchain technology in IoT.

So, what is blockchain technology? Is it the new Internet? The blockchain [8] technology is a highly innovative and revolutionary invention, which allows digital information to be distributed but not to be replicated. It has created the backbone for a whole new type of Internet. Blockchain technology was originally devised for bitcoins, a digital form of currency, also termed as "digital gold". Blockchain powers the popular cryptocurrency named Bitcoin and bitcoin mining is immensely popular nowadays. Bitcoin solves many issues through what is known as "Blockchain Implementation".

A. Distributed Public Ledger

Each person on the network has a copy of the ledger, as there is no centralized original copy of it. Ledger here, means the copy of all the data transactions which

have occurred. The following diagram explains the centralized and decentralized ledger. All these transactions are stored in the Blockchain which acts as a distributed database.

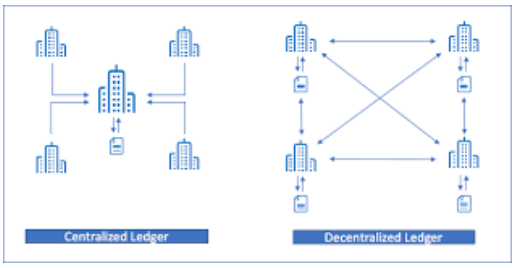

Fig 1: Centralized and Decentralized Ledger

B. Hash Encryption

All the data stored on the blockchain is encrypted at all the ends using HASH functions [9]. Bitcoin uses SHA-256 encryption. Unlike encryption algorithms, hash functions cannot be decrypted. It is one of the most secure functions as even minute input differences gives a fully different hash. The encryption level is so strong here that brute attacks would require multiple attempts and still might find a completely different input value.

C. Proof of Work

It is a new concept invented in bitcoin to validate the transactions by solving a complex mathematical puzzle, which is called proof of work. There is a hash target designated to each block.

II. Cloud Storage

In some cases, devices may wish to store their data in the cloud storage, so that a third party Service Provider can access the stored data and offer certain smart services. The cloud storage [10] groups the user's data in identical blocks associated with a unique block-number. The user for authentication uses Block-number and hash value of the stored data. If the storage can successfully locate data with given block-number and hash, then the user is authenticated. Received data packets from users are stored in a First-In-First-Out (FIFO) order in blocks along with the hash of stored data. After storing data, the new block-number is encrypted. This ensures that whoever possesses the key is the only one, who knows the blocknumber. Since hashes are resistant to collision and only the true user knows the block-number, we can guarantee that no one other than the true user can access her data and also chain new data to an existing ledger.

III. Transaction Handling

Having witnessed the basic topology of the BC-based IoT architecture of privacy and security, let us concentrate on the transaction handling part now.

A. Storage

Every device has the option to store the data in local, shared or the cloud storage [11]. For example in most cases, a smart thermostat stores the data in cloud storage such that the SP to put into effect of some smart services can utilize it. Consider Alice has opened up an account in cloud storage and provided permission to upload the data from her thermostat to this cloud storage facility. When bootstrapping the cloud sends a pointer to the first block of data. If the smart thermostat wants to store the data in the cloud storage, it sends its data to the miner.

First of all the miner checks for the permission and after this it extracts the previous blocks number and hash. After this process, it generates a random Id and sends the data along with the id to the storage. It is assumed that no two nodes can have the same Id. After this, the storage will check the transaction validity and it will check the space availability in cloud storage. Then it determines the amount of hash of received data packets and compares with the received hash. If the two hashes coincide then the data are stored in storage, a new block number is created, and it is sent to the miner. Now the signed hash of the data is signed by the storage and sends it to the overlay network so that it can be mined in the overlay BC. By this any changes made by the user is visible to all.

Remember that the shared storage is nothing but the local storage governed by the owner at homes which is trusted. As a result, no accounting is done and ultimately there is no need for the miner to send the data during the store operation. In addition, the storage does not sends the hash data to the overlay network. Rest of the process remains the same with the cloud storage. If the user has a local storage all the process remains the same with only one difference that no ID is necessary because all the communication is performed locally in the smart home.

B. Accessing

The SP will have to access the data for particular amount of time or the entire history of data for one particular device in order to execute certain actions upon it. In order to have permission to use the information, the SP has to create and sign a new multi-signature transaction and the same has to be signed by the requester's SP and the requester (smart home's miner) and send it to its own cluster head. The CH will now check both the PK's list. If any of the tow multi-signature transactions are present in requester's PK list or the requester's PK list, the transaction is broadcasted to its entire cluster. If else, the transaction is broadcasted to the requester to other CH and PK's if put in the forward list. When the miner gets the multi-signature transaction it has to check the in its BC whether the SP has the permission to use the data which the user must have

guaranteed previously. If this condition is satisfied then the miner seeks for the packets from the storage and delivers it to the requester after encrypting it with requester's PK. Before delivering the packets this can use safe answer or introduce methods to provide additional privacy also. Binary 1,s and 0,s is set by the miner to the output of the multi-signature transaction to verify whether requester has the permission to access the data. The miner stores the transaction in the Local BC after sending it to the requester.

In addition to this, the miner sends the transaction to the anonymous set of CH's to be stored in the overlay network. This stored transaction can be used as a verification that the user had sent the data and any misbehaving of other nodes can also be found out. The miner acts as a deciding authority where it decides to send the transactions to overlay BC or not. If it has no intention to reveal the data to others, it need not send it. This not only helps the users' privacy but it also helps the attackers. There might arise many conditions where the user needs to access the entire chain of data. At the time in order to prevent network overhead delays, policy levels are used. They are,
If the requester is a user or a SP which has the permission to use the whole chain of data, then the miner sends the block number and hash of data in storage.
If else only limited amount of the data is given as per the request that can satisfy the user by implementing many techniques like adding noise or safe answer.

IV.MONITORING

In some cases, the user may access information from their home itself. For example, the user may check his/her status of working of smart thermostat. A monitor transaction [12] is being used where the miner seeks for the real time data from the requested device and sends it to the user. The data is sent conterminously where a live camera being viewed by the user.

V. DISTRIBUTED TRUST

Now we shall get into the appliances of ensuring the distributed trust in overlay network. Each CH in the overlay network trusts other CH on rating based on the Beta Reputation system, which depends on the direct and indirect evidence. When a CH produces a new block, it has to generate multi-signature transaction to other CH's also. When a new block comes to CH, it tries to verify its related transactions. If this has direct evidence with the miner or other CH's who signed the contraction then it randomly checks for the signatures in certain parts randomly in the transaction. The number of verified transactions of CH highly depends upon the degree of direct evidence with the miner and it evaluates the trust assessment of CHs that provides the indirect evidences also. Approximate portions of the transaction have to be checked when dependable evidence comes in. However, when indirect evidence comes in the whole transaction is checked.

VI. EVALUATION

In this section lets us discuss about the overhead and performance issues of our architecture along with the security and privacy threats. Possible threats include a device in the home, one in the CH, a node in the overlay network, or the storage. These opponents are capable of disclosing the communications, getting rid of transactions, pinging false blocks and transactions, deleting the data in storage. The main Advantage is that they are incapable of breaking transactions. The main area of threats is

Threat to accessibility: This is where the user is blocked by the opponent to use his/her data.

Threat to anonymity: The challenge here is to find the true identity of the user among all the available identities and transactions in the environment.

Threat to authentication: The opponent himself tries to access the data showing his identity as a legal authentication tool.

These are the attacks that threaten the user from accessibility:

- **Denial of Service [13] (DOS):** In this type of attack, the adversary tries to block a true user accessing his/her data. In our proposed architecture, the ally does this by sending a false transaction to the overlay network or smart homes. However, our PK's list in CH's list of requester acts as a firewall and destroys this act by forwarding it to other CH's if it is not present in the former. Further, if a PK sends many anonymous requests then the CH has the ability to block that PK such that no further requests will be guaranteed by the CH. However, the ally will succeed if it uses different PK's to attack.
- **Modification Attack [14]:** To perform this attack the attacker will have to sacrifice the cloud storage security. Usually the ally tries to change or delete the data stored by the specific user. However, the user has the greatest advantage of detecting the changes occurred in the data by comparing it with the hash of the data in the cloud storage with the hash of the local BC. If the user finds a contravention the user creates a transaction which will have both multi-signature transaction signed by both the user and the cloud storage containing the true hash of the data and the access transaction signed by both the storage and the user containing invalid hash of the data. This is sent to other CH's which will verify the true transaction being cited. However, the disadvantage here is that the user cannot recover his/her lost data.
- **Dropping Attack:** First, the ally gains the control of a particular or group CH's. After gaining the control, all the transactions and blocks will be dropped. However, the identification of this breach could easily be identified where the nodes under that cluster will not receive any messages that the network sends it. But in our architecture such a problem could be overridden where an awareness is created to all the nodes and since the nodes in the cluster has the ability to elect a new cluster head, a new CH is elected.
- **Mining Attack [15]:** Here the attacker will have the access to multiple CH's which works together to sign the multi-signature transactions. However, in our proposed system, the validations will take place only if CH has the direct

evidence with block miner and if it matches, also a certain portion of the transaction is tested. Our architecture will not be able to find the fake blocks all the time. But there is a slight advantage is there where even if one CH cannot find it, the other will be able to find it. That is highly useful because it can warn all the CH about the breach.

For anonymity breach, the ally will have to send different links with different ID's for a particular user in the real world. However, the user has the ability to overcome this problem by sending an arbitrary transaction to the overlay network. Additionally different ID's and PK's can also be used for different transactions.

The last and the final threat is where it is against the authentication. Here the attacker generally tries to have control over the existing object in the home. The user can easily detect it since all the devices are mined in the local BC. The other way is that the attacker tries to add a new device in the home. But this is not possible because all the devices should have been pre-defined initially and transactions have to be mined in the local BC.

However, in other cases the adversary will pose as SP then when it receives the block number and hash, it acts as a true user and blocks the authentication. However, here each block is stored in the storage is chained to another block. Even an empty block is stored and points it back to the one, which the requester will be adding it. By this, the requester cannot ping his data to the user's one because it is already chained.

VII. Conclusion

Though IoT is in its peak of its career, privacy and security still remain a major challenge to deal with. This blockchain based IoT architecture handles efficiently most of the privacy and security constraints and it provides the best possible methods to avoid overhead delays. There are many challenges to be solved like the Denial of Service (DOS) attacks, modification attacks. However, along with the questions, so many effective answers unfold such as decentralization, intrinsic broadcast medium with which we can achieve accuracy. However, this architecture stays as a basement for further studies in this regard by giving efficient privacy and security in the field of IoT while preserving to have most of blockchain technology.

VIII. References

[1] Louis Coetzee, Johan Eksteen, "The Internet of Things-promise for the future? An Introduction", IST-Africa Conference Proceedings, December (2011)

[2] Sheikh Ferdoush, Xinrong Li, "Wireless Sensor Network System Design Using Raspberry Pi and Arduino for Environmental Monitoring Applications", Elsevier Volume 34, pages 103-110 (2014).

[3] Hui Suo, Jiafu Wan, Jianqi Liu, "Security in the Internet of Things", Computer Science and Electronics Engineering (ICCSEE), (2012), DOI:10.1109/ICCSEE.2012.373.

[4] Xinlei Wang, Eve M. Schooler, Mihaela Ion, "Performance evaluation of Attribute-based Encryption: Towards data privacy in the IoT", (2014),DOI:10.1109/ICC.2014.6883405.

[5] Hui Solo, Jiafu Wan, Caifeng Zou, " Security in the Internet of Things: A Review", April (2012), DOI:10.1109/ICCSEE.2012.373.

[6] Masanobu Katagi, Shiho Moriai, " Lightweight ryptography for the Internet of Things".

[7] Vinita Shirley, Rithvik Pamidi, "Web of Things".

[8] Satoshi Nakamoto, "Bitcoin: A peeer-to-peer Electronic Cash System", (2013).

[9] Lawrence Carter, Mark Wegman, "Universal classes of hash functions", (1979), Journal of Computer and System Sciences, Volume 18, Issue 2, pages 143-154.

[10] Cong Wang, Kui Ren, Jin Li, "Toward publicly auditable secure cloud data storage services", IEEE Network, (2010), DOI:10.1109/MNET.2010.5510914.

[11] Sherman S M Chow, Qian Wang, Kui Ren, "Privacy-Preserving Auditing for secure Cloud Storage",pages 362-375, (2016).

[12] Philip V Jr., Wiles, "Synthetic Transaction Monitor", (2003).

[13] Krishnamoorthy, D., & Chidambaranathan, S. (2017). Clever Cardnovel Authentication Protocol (NAUP) in Multi-Computing Internet of Things Environs.

[14] N Long, R Thomas, "Trends in denial of service attack technology", (1999).

[15] Peter Huitsing, Rodrigo Chandia, "Attack taxonomis for the Modbus Protocols", pages 37-44, (2008).

[15] Wang Li, Li Dong, Lei Jei, "Attack scenario construction with a new sequential mining technique", (2007), DOI:10.1109/SNPD.2007.

[16] Ranjeethapriya K, Susila N, Granty Regina Elwin, Balakrishnan S, "Raspberry Pi Based Intrusion Detection System", International Journal of Pure and Applied Mathematics, Volume 119, No. 12, 2018, pp.1197-1205.

[17] V. Anandkumar, Kalaiarasan T R, S.Balakrishnan, "IoT Based Soil Analysis and Irrigation System", International Journal of Pure and Applied Mathematics, Volume 119, No. 12, 2018, pp.1127-1134.

[18] Sitharthan, R., and M. Geethanjali. "Application of the superconducting fault current limiter strategy to improve the fault ride-through capability of a doubly-fed induction generator–based wind energy conversion system." Simulation 91, no. 12 (2015): 1081-1087.
[19] Sitharthan, R., M. Geethanjali, and T. Karpaga Senthil Pandy. "Adaptive protection scheme for smart microgrid with electronically coupled distributed generations." Alexandria Engineering Journal 55, no. 3 (2016): 2539-2550.
[20] Sitharthan, R., and M. Geethanjali. "An adaptive Elman neural network with C-PSO learning algorithm based pitch angle controller for DFIG based WECS." Journal of Vibration and Control (2015): 1077546315585038.