Adaptive Security Framework for the Blockchain on IOT

Vytarani Mathane, P V Lakshmi

Abstract: ***Current blockchain technologies lack adapt- ability required to accommodate incoming heterogeneous devices as nodes in the Blockchain network. This inability becomes more pronounced when it comes to blockchains for Internet of Things (IOT) due to varied capabilities and heterogeneity of constituent devices in IOT network. Specifically, security solutions which are used by Blockchain in IoT domain lack support for adapting with different network resources, ranging from low power devices to high end servers. This paper presents an adaptive security framework for blockchain based IOT architectures. The security framework consists of a dynamic resource computation algorithm based on which the network adapts to the existing resources and decides which security services to offer.***

Index Terms: IOT, Blockchain, Adaptive security framework, Distributed ledger, Sensor Networks.

I. INTRODUCTION

IOT is a network of uniquely identifiable devices connected to the internet [1]. Different devices in typical IOT network have different resources. For example, consider IOT network in connected cars where the applications include car sharing, delivery, infotainment, connectivity, on demand rentals EV charging etc. The IOT nodes in this scenario are sensors, gateways, wearables, general purpose CPU, vehicle to infrastructure communication devices, vehicle to vehicle communication devices. Thus, a typical IOT network would have de- vices with different computing resources and security primitives.

Blockchain technology is auditable, immutable and transparent distributed ledger maintained by a peer-to- peer decentralized network of devices. The key elements of Blockchain are nodes, immutable transactions and smart contract. These key elements are responsible to provide essential services for functioning of Blockchain which most often are routing to participate in peer-to- peer interactions, storage to maintain copy of all trans- actions, wallet to provide security keys needed for trans- actions and mining to create new transactions.

A node is a computing device on blockchain net- work connected to the internet in addressable fashion. It could be communication endpoint or relay device linking to other nodes. All nodes in a Blockchain are considered equal but depending upon Blockchain architecture nodes will have distinct roles to support functioning of that Blockchain [2]. Typical types of nodes in a Blockchain are: full node, light node, miner node, pruning node etc. A full node will store

complete copy of Blockchain transactions locally, light node only stores headers of all the blocks in a blockchain, miner node work on proof of work (PoW), pruning node had verified all previous transactions but has reduced storage. Requirements to add new node to Blockchain and subsequently maintain it would vary between different Blockchain implementations. Fig. 1 presents generalized protocol stack of Blockchain.

Distributed ledger is composed of blocks which are immutable transaction records. Each block contains contents and an identifying header. Each block is time stamped and linked to the preceding and following blocks thus forming a blockchain. A block is added to the Blockchain when distributed network of computers reaches consensus based upon certain consensus protocols of that Blockchain on whether a transaction is valid, a process where each node arrives at its own conclusion about validity of transaction independent of others. Once added to the Blockchain, blocks cannot be altered and are protected by public and private keys to prevent unauthorized access to data. Processing such Blockchain trans- actions may need significant amount of computing re- sources and abilities based upon role of node. Traditional Blockchains tend to address these needs by employing powerful Central Processing Units (CPUs) and Graphical Processing Units (GPUs) as nodes but in general there is certain minimum computing abilities taken granted. Such an assumption about minimum computing abilities becomes very unattainable in case of IOT networks as member devices are embedded in nature with very wide-ranging resources and abilities at their disposal.

This type of variation in resources and abilities avail- able to each device in typical IOT network and fact that Blockchain transactions always increase with time thus dynamically changing computing needs of potential new nodes over period warrants further research to define

Revised Manuscript Received on July 10, 2019.

Dr.R.Punniyamoorthy, · Department of Computer Science and Engineering, Gitam University, Vishakhapatnam, India

P V Lakshmi, Department of Information Technology, Gitam University, Vishakhapatnam, India.

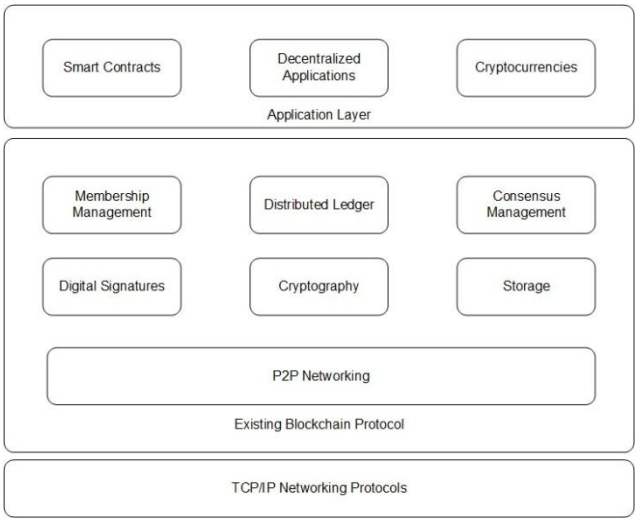

Fig. 1. Generalized sectional view of Blockchain protocol stack

methods for smart and adaptable frameworks to allow heterogeneous nature of IOT and Blockchain working together. Existing security solutions are limited in offering dynamic adaptable security framework because of their inability to adapt to the new devices, offering security services according to the available resources to meet minimum requirements of end users.

II. RELATED WORK

Different security solutions [3–7] have been proposed for blockchain IOT. LNSC uses elliptic curve cryptography (ECC) to calculate hash functions [5]. DistBlockNet [6] combines the best of Blockchain and SDN technologies. The aim of this architecture is to address the issues of high number of connected devices such as availability, flexibility, security, scalability, efficiency, mitigate Denial of Service (DOS) and Distributed Denial of Service (DDOS) attacks, spoofing and other network attacks. But it does not cover key attack, modification attack, cryptanalytic attacks, reputation based attacks etc. [8]. Conoscenti [7] focus on the scalability issue that Bitcoin has to deal with. Their research analyses by different simulations how scalability behaves. They highlight the Bitcoin Lightening Network [9] as one of the possible solutions.

Security services offered by different papers include authentication [3] [10], privacy preserving [11] [12] [13], trust [14] [15]. Authentication is ensured in [3] using secure remote user authentication and by a threshold authentication protocol in [10]. Privacy preserving is ensured by using node verification approach in [11] , by hiding non content data in [12] and by using a public key system in [11]. Distributed trust is ensured in different papers using two layer approach [14] or a mechanism where every participant maintains their own chain of transactions [15].

According to survey paper [8], a security solution resilient against combined attacks is needed by taking into account low power IOT devices. And the solution should initially adapt to the existing resources, and decide which security services to offer, so as to meet the end used minimum security requirements of end users. Trust based adaptability for IOT is proposed in [16]. Many are risk based [17] adaptable solutions for IOT security. We are proposing for heterogeneous networks where different nodes have different computing powers.

This paper proposes a dynamic adaptable security solution for the blockchain based IOT which adapts to the new devices added and offers security services to meet minimum requirements based on the resources.

III. DESIGN OF THE DYNAMICALLY ADAPTABLE SECURITY FRAMEWORK FOR IOT

Different nodes in a typical IOT network will have different resources such as CPU power, storage memory, system memory etc. At the same time an incoming node in a Blockchain is expected to have different minimum level of computational resources depending upon role it is aiming for. Existing Blockchain architecture and implementations do not have methods to determine whether an incoming node could meet minimum security requirements.

The proposed design consists of adaptive module which evaluates the computing resources of the incoming device requesting to be new node to the Blockchain for appropriate role and allow the Blockchain switch to appropriate security services in case of successful addition of new node. This proposed adaptive module is activated whenever new device is being added to the Blockchain. This dynamic adaptive module consists of two components: Blockchain Device Manager and Blockchain Security Service Manager described in following subsections.

This paper proposes two-fold solution, one to address the need to establish methods to help Blockchain make dynamic determination whether the device meets minimum required security capabilities as incoming node or not and second to allow the Blockchain to be adaptable to resources and abilities of the incoming node. Fig. 2 presents the snapshot of the adaptive module within the main node when a new device is added to the Blockchain.

A. Blockchain Device Manager

Blockchain Device Manager is responsible to determine computing resources available to the device requesting to be added as new node on the Blockchain and to provide required interfaces or APIs to communicate those retrieved device properties to specific nodes in the rest of the Blockchain. Typical way to implement such determination of computing resources would be in the existing methods or scripts which are used by popular Blockchain protocols when new device requests to be added to the Blockchain. This determination would include querying device for parameters of interest through its existing system calls. Fig. 3 represent various interactions within all stakeholders when new node is being added to the Blockchain.

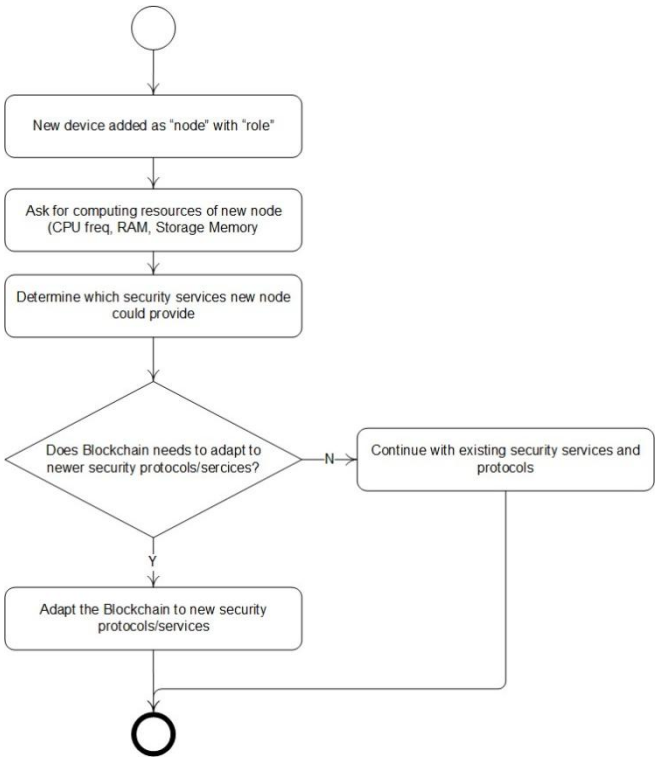

Fig. 2. Snapshot of the adaptive module in main node when a new device is added to the Blockchain

B. Blockchain Security Service Manager

The Blockchain Security Service Manager resides in the main node. It is responsible to query information on computing resources of newly added node, evaluate most appropriate security mechanisms based on the resources available to all nodes and broadcast those to rest of the Blockchain. This component could also be entrusted with ability to reject newly added node if it fails to meet all necessary computing and security requirements and update all nodes in the network accordingly.

Blockchain Security Service Manager needs to determine minimum security services to meet the end user requirements and be able to deduce new node's ability to fulfill those based upon computing resources available to it. Security services include authentication methods, privacy preserving methods and, trust. Based on the computation resources of total network, the Blockchain protocols could choose secure remote user authentication or threshold authentic/ B or magnetic field strength symbolized as μ0H. Use the center dot to separate compound units, e.g., "A•m2." Embedded Prototype Implementation Intel UP2 IoT platform is used for prototyping these experiments. While implementation of these proposed APIs is highly hardware and software specific, proto- type APIs are quite generic and applicable to most of the platforms. Blockchain Device manager offers APIs to request data on CPU computing power represented by CPU frequency, system memory and storage capacity. This information once retrieved from an incoming node is shared with the main node. The main node leveraging Blockchain Security Service Manager makes decision about most appropriate security services for entire Blockchain and informs rest of the nodes. Hence implementation should have following set of APIs to retrieve and broadcast above said parameters.

```
get_device_resources(cpu_frequency, system_memory, storage_memory) {
  -get cpu frequency;
  -get system memory;
  -get storage memory;
  -return success;
  };

send_device_resources( (cpu_freq, system_mem, storage_mem) {
  -send cpu frequency, system memory, storage memory;
  -return success;
  };

broadcast_security_sercices ( authentication_mode, privacy_mechanism, trust, attack_defense) {
  -send authentication_mode, privacy_mechanism,
  trust, attack_defense;

  };
```

Intel UP2 hardware platform showed in Fig. 4 is used in prototype testing.

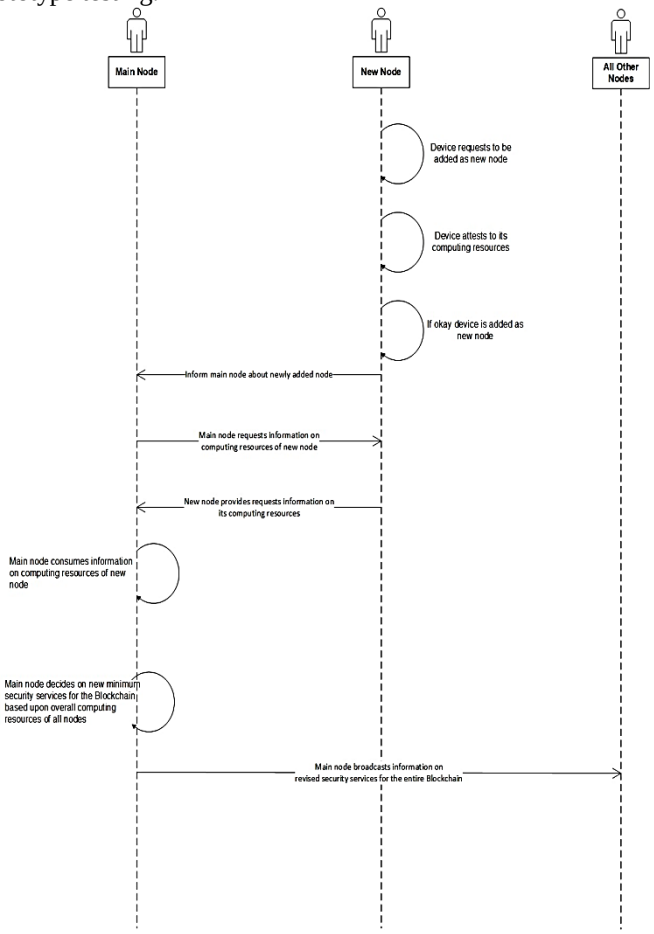

Fig. 3. Interactions between main device and all the other nodes

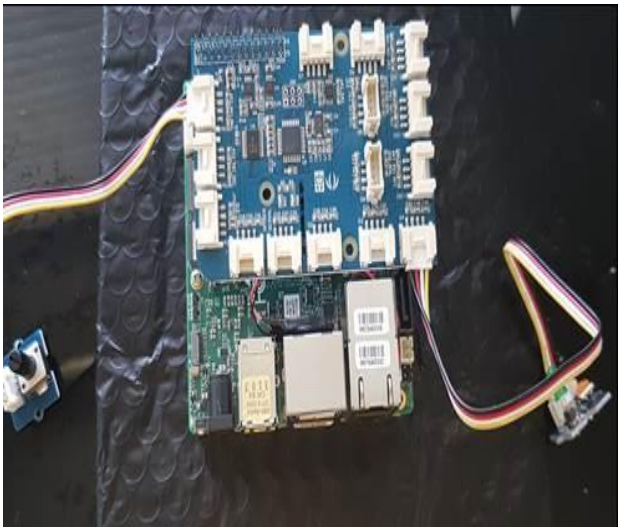

Fig. 4. Intel UP2 Hardware Platform Used In Prototype Testing

IV. EVALUATION

A. Performance Analysis

The simulation environment we used is Intel processor with 2 gz frequency and Intel up2 board as client node. The implementation of adaptive client uses 2MB of program memory. Implementation of adaptive server uses 0.7 MB of program memory. Fig. 5 shows the simulation test results for the average time taken to get resource information from the new device. Fig. 6 shows the simulation test results for the average time taken to send security solution changes to each node on the network.

The test results show that on an average 5.7 ms will be taken to get resources from the new added node and for sending changes to each node will take average of

0.07 ms. Table 1 shows average time taken in getting resources from the new node and sending security solution changes to each node on the simulation network.

Table 1 Average time taken in getting resources from the new node and sending security solution changes to each node on the simulation network.

Average simulation time in	Time taken
Getting resources from new node	5.7 ms
Sending changes to each node	0.07 ms

B. Scalability

The proposed framework is scalable to IOT needs where the devices can be many in number, the main node work can be distributed in other nodes and all the main nodes can be form a group to communicate with each other regarding changes.

V. CONCLUSION

This paper proposed and developed an adaptive security framework for blockchain based IOT architectures. The security framework consists of a dynamic resource computation algorithm based on which the network adapts to the existing resources and decides which security services to offer.

In the future we will extend the adaptive framework to attest the new devices.

ACKNOWLEDGMENT

We would like to thank Sudhir Mathane for the help in carrying out the experiments.

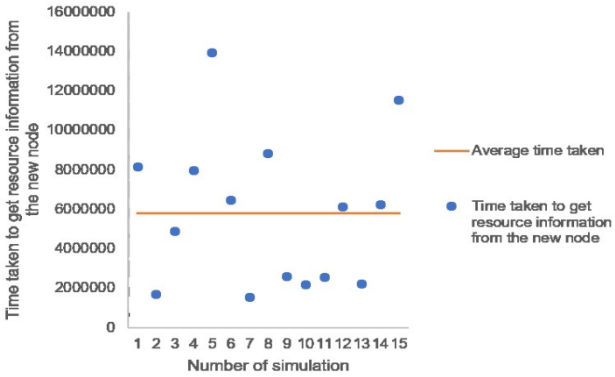

Fig. 5. Average time to get resource information from new node

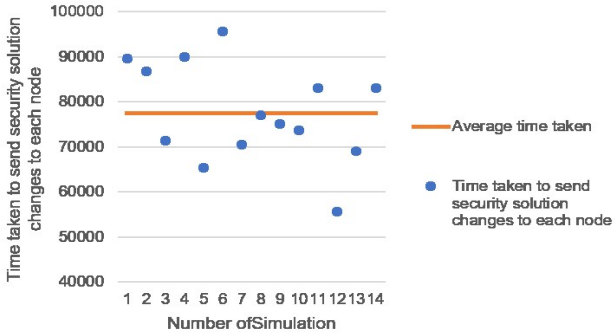

Fig. 6. Average time to send security solution changes to each node

REFERENCES

1. Roberto M., Abyi B., Domenico R., "Towards a definition of the Internet of Things (IoT)", IEEE internet Initiative (2015), https://iot.ieee.org/definition.html, Published 27 May 2015
2. Ana R., Cristian M., Jaime C., Enrique S., Manuel D., "On blockchain and its integration with IoT", Challenges and opportunities. Future Generation Computer Systems 88, 173-190 (2018)
3. C. Lin, D. He, X. Huang, K.-K. R. Choo, and Vasilakos A.V., "Bsein: A blockchain-based secure mutual authentication with fine grained access control system for industry", 4.0 Journal of Network and Computer Applications, volume 116, 42-52 (2018)
4. Liang G., Weller S. R., Luo F., Zhao J., and Dong Z. Y., "Distributed Blockchain-Based Data Protection Framework for Modern Power Systems against Cyber Attacks", IEEE Transactions on Smart Grid, 1-1 (2018).
5. Huang X., Xu C., Wang P., and Liu H., "LNSC: A security model for electric vehicle and charging pile management based on blockchain ecosystem", IEEE Access, vol. 6, 13565-13574 (2018)
6. Sharma P. K., Singh S., Jeong Y.S, and Park J. H., "DistBlockNet: A Distributed Blockchains Based Secure SDN Architecture for IoT Networks", IEEE Communications Magazine, vol. 55, 78-85 (2017).
7. Marco C., Antonio V., Juan C. D. M., "Peer to Peer for Privacy and Decentralization in the Internet of Things", IEEE, ACM 39th International Conference on Software Engineering Companion (ICSE-C) (2017). https://doi.org/10.1109/ICSE-C.2017.60

8. Ferrag M. A., Makhlouf D., Mithun M., Abdelouahid D., Leandros M., Helge J., "Blockchain Technologies for the Internet of Things: Research Issues and Challenges", Cryptography and Security (2018). https://arxiv.org/abs/1806.09099
9. Lighting Network, https://en.wikipedia.org/wiki/Lightning_Network.
10. Li L., Liu J., Cheng L., Qiu S., Wang W., Zhang X., Zhang Z., "CreditCoin: A Privacy-Preserving Blockchain Based Incentive Announcement Network for Communications of Smart Vehicles", IEEE Transactions on Intelligent Transportation Systems, Volume: 19, 2204-2220 (2018)
11. Jingzhong W., Mengru L., Yunhua H., Hong L., Xiao K., Chao W., "A Blockchain Based Privacy Preserving Incentive Mechanism in Crowdsensing Applications", IEEE Access, Volume: 6, 17545-17556 (2018).
12. Aitzhan N. J., Svetinovic D., "Security and Privacy in Decentralized Energy Trading through Multi-signatures, Blockchain and Anonymous Messaging Streams", IEEE Transactions on Dependable and Secure Computing (2016), volume 15, 840-852 (2018).
13. Wang Q., Hu J., Qin b. b., Xiao F., "Preserving transaction privacy in bitcoin", Future Generation Computer Systems (2017), https://doi.org/10.1016/j.future.2017.08.026.
14. Yining H., Ahsan M., Parinya E., Madhusanka L., Kanchana T., Guillaume J., Aruna S., Mika E Y., "A Delay-Tolerant Payment Scheme Based on the Ethereum Blockchain", Computers and Society (2018). https://arxiv.org/abs/1801.10295
15. Pim O., Martijn de V., Johan P, " TrustChain: A Sybil-resistant scalable blockchain", Future Generation Computer Systems (2017). https://doi.org/10.1016/j.future.2017.08.048
16. Hamed H., Abdelmadjid B., Mouloud K, "TAS-IoT: Trust-Based Adaptive Security in the IoT", IEEE 41st Conference on Local Computer Networks (LCN) (2016). https://doi.org/10.1109/LCN.2016.101
17. Hany F. A., Alenezi A., Robert J. W., Gary B. W., Joshua D, " Developing an Adaptive Risk-Based Access Control Model for the Internet of Things", IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communica- tions (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (Smart- Data) (2017). https://doi.org/10.1109/iThings-GreenCom- CPSCom-SmartData.2017.103

AUTHORS PROFILE

Vytarani Mathane, research scholar, GITAM University.

P V Lakshmi, professor, GITAM University.