Poster Abstract: Blockchain-based Scalable Authentication for IoT

Munkenyi Mukhandi
CISUC, Dep. of Informatics
Engineering, University of Coimbra,
Portugal
mshomarim@dei.uc.pt

Eduardo Andrade
CISUC, Dep. of Informatics
Engineering, University of Coimbra,
Portugal
eandrade@student.dei.uc.pt

Francisco Damião
PDMFC
Lisbon, Portugal
Francisco.Damiao@pdmfc.com

Jorge Granjal
CISUC, Dep. of Informatics
Engineering, University of Coimbra,
Portugal
jgranjal@dei.uc.pt

João P. Vilela
CRACS/INESCTEC, CISUC and
Dep. of Computer Science,
Faculty of Sciences,
University of Porto, Portugal
jvilela@fc.up.pt

Abstract

Device identity management and authentication are one of the critical and primary security challenges in IoT. In order to decrease the IoT attack surface and provide protection from security threats such as introduction of fake IoT nodes and identity theft, IoT requires scalable device identity management systems and resilient device authentication mechanisms. Existing mechanisms for device identity management and device authentication were not designed for huge number of devices and therefore are not suitable for IoT environments. This work presents results of a blockchain-based identity management approach with consensus authentication, as a scalable solution for IoT device authentication management. Our identity management approach relies on having a blockchain secure tamper proof registry and lightweight consensus-based identity authentication.

CCS Concepts • **Security and privacy** → **Authentication**; **Access control**.

Keywords Identity management,Internet of Things

ACM Reference Format:
Munkenyi Mukhandi, Eduardo Andrade, Francisco Damião, Jorge Granjal, and João P. Vilela. 2020. Poster Abstract: Blockchain-based Scalable Authentication for IoT. In *The 18th ACM Conference on Embedded Networked Sensor Systems (SenSys '20), November 16–19, 2020, Virtual Event, Japan.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3384419.3430465

SenSys '20, November 16–19, 2020, Virtual Event, Japan
© 2020 Copyright held by the owner/author(s).
ACM ISBN 978-1-4503-7590-0/20/11.
https://doi.org/10.1145/3384419.3430465

1 Introduction

IoT has great potential to provide many benefits in our world. Unfortunately, production of cheaper IoT devices with less security features creates massive problems in terms of IoT security. Identity management for IoT has been vastly studied and frequently implemented using centralised architectures with low scalability[5]. These hinder usage for huge number of devices because it creates bottlenecks and single points of failure. To address these problems, recent works have put forward blockchain-based approaches to eradicate centralised models, promote trust and provide resilient architectures against several cyber security threats.

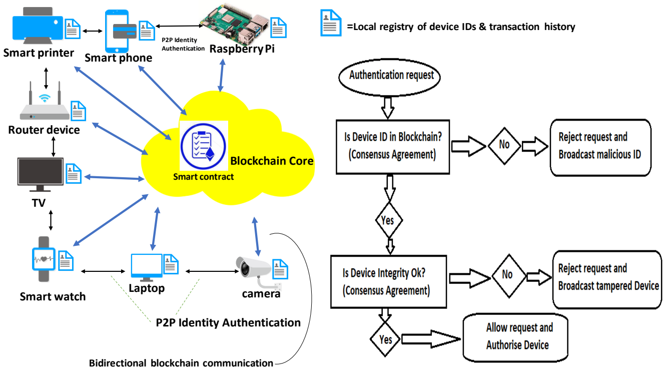
=Local registry of device IDs & transaction history
Smart printer
Smart phone
P2P Identity Authentication
Raspberry Pi
Router device
TV
Smart watch
Laptop
camera
Blockchain Core
Smart contract
P2P Identity Authentication
Bidirectional blockchain communication
Authentication request
Is Device ID in Blockchain? (Consensus Agreement)
No
Reject request and Broadcast malicious ID
Yes
Is Device Integrity Ok? (Consensus Agreement)
No
Reject request and Broadcast tampered Device
Yes
Allow request and Authorise Device

Figure 1. Proposed architecture & Authentication flow

Blockchain has been used for access and identity management by utilising digital certificates for authentication. Other approaches achieved authentication with usage of sub chains[3] and use of tokens[2]. In this work, we propose a scalable decentralised identity management with a novel consensus P2P authentication relying on majority node agreement using hashed identities securely stored in the blockchain. We use blockchain and smart contracts to achieve acceptable level of security with scalability.

2 Proposed solution and Results

Our proposed approach involves identity creation, creation of tamper proof device registry and consensus-based identity authentication involving all nodes. Our hashed device identities are extracted from device attributes such as device name, firmware, MAC address and its configuration files[6], and also we add device clock to ensure uniqueness and enhance identity security. The created identities are stored in the blockchain, thus providing a secure way of guarding identity data because of its tamper-proof Merkle tree structure. Each device in the blockchain network has a copy of the device registry to facilitate the authentication process. The blockchain has three purposes: (1) store the generated device identities in a distributed manner, (2) protect integrity of generated identities and devices and (3) facilitate the consensus authentication process. The smart contracts are used by nodes for verification and validation of created identities. The step by step authentication process as illustrated in Fig.1 uses Elliptic Curve Digital Signature Algorithm which is compatible with IoT context. It starts with an authentication request, the receiving node performs identity validation by checking its local blockchain registry and broadcasts the request to other IoT nodes to verify the identity of the requester to achieve a consensus agreement. The other nodes will alert by sending a blockchain transaction if there is a difference between the received request and the stored identity in their local blockchain registries otherwise they send an approval transaction that can be read by the requester in the blockchain. The second part is the device firmware integrity check which follows a similar procedure of consensus agreement. At the end, nodes authentication is achieved by the identity validity check without performing heavy computations such as creation of session keys or generation of tokens which are not suitable for huge number of IoT devices.

We evaluated scalability of our approach by assessing the delays and throughput for increasing number of simultaneously nodes(20,25,30,35,40) in our Ethereum system. The collective delay to authenticate simultaneously was measured for each category number of nodes whereas the throughput was measured as number of bytes per second collectively sent from simulated nodes to the blockchain. We performed 30 simulation experiments for five minutes for each group of nodes by using an industry standard testing tool HPE Loadrunner[1] designed to measure system behaviour[1]. By using crafted Loadrunner scripts we were able to simulate Ethereum transactions to a blockchain emulator[2] installed in a Ubuntu machine(Intel(R) Core(TM) i5-3230M CPU @ 2.60GHz) with our deployed smart contract. During experiments, we observed a nearly linear increase of the delay with the number of nodes, going from 12 seconds for 20 nodes, up to 25 seconds for 40 nodes, as depicted in Fig. 2. Our work compares favourably for a centralised authentication mechanism[4] based on MQTT where average authentication delay of 2.137 seconds for a single node will increase significantly with increase of nodes. Our approach rely on private blockchain which makes it considerably faster than other Ethereum authentication mechanisms[2] that have an additional 14s delay of public blockchain. Further, as seen in Fig.3, we observed stable average throughput as we increased number of nodes. This shows the system does retain its performance while increasing more nodes.

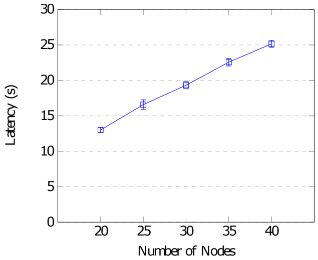

Figure 2. Latency.

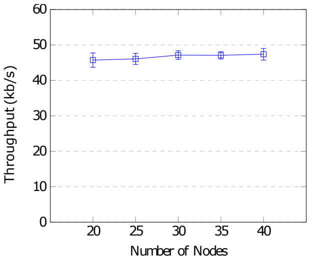

Figure 3. Throughput.

3 Conclusion

We present demo results of a blockchain-based authentication mechanism based on consensus authentication. Our results show that the system is a scalable lightweight mechanism for authentication of constrained devices.

Acknowledgments

This work is supported by the European Regional Development Fund(FEDER), through the Regional Operational Programme of Lisbon(PORLISBOA 2020) and the Competitiveness and Internationalisation Operational Programme (COMPETE 2020) of the Portugal 2020 framework[Project 5G with Nr.024539 (POCI-01-0247-FEDER-024539)].

References

[1] Rabiya Abbas, Zainab Sultan, and Shahid Nazir Bhatti. 2017. Comparative analysis of automated load testing tools: Apache JMeter, Microsoft Visual Studio (TFS), LoadRunner, Siege. In *2017 International Conference on Communication Technologies*. IEEE, Rawalpindi, Pakistan, 39–44.

[2] Mohamed Tahar Hammi, Badis Hammi, Patrick Bellot, and Ahmed Serhrouchni. 2018. Bubbles of Trust: A decentralized blockchain-based authentication system for IoT. *Computers & Security* 78 (2018), 126–142.

[3] Dongxing Li, Wei Peng, Wenping Deng, and Fangyu Gai. 2018. A Blockchain-Based Authentication and Security Mechanism for IoT. In *2018 27th International Conference on Computer Communication and Networks (ICCCN)*. IEEE, Hangzhou, China, 1–6.

[4] Ankur Lohachab and Karambir. 2019. ECC based inter-device authentication and authorization scheme using MQTT for IoT networks. *Journal of Information Security and Applications* 46 (jun 2019), 1–12.

[5] Ola Salman, Sarah Abdallah, Imad H. Elhajj, Ali Chehab, and Ayman Kayssi. 2016. Identity-based authentication scheme for the Internet of Things. In *2016 IEEE Symposium on Computers and Communication (ISCC)*. IEEE, Messina, Italy, 1109–1111.

[6] Bo Tang, Hongjuan Kang, Jingwen Fan, Qi Li, and Ravi Sandhu. 2019. IoT Passport. In *Proceedings of the 24th ACM Symposium on Access Control Models and Technologies*. ACM Press, New York, NY, USA, 83–92.

[1] https://software.microfocus.com/en-us/products/loadrunner-load-testing/overview

[2] https://truffleframework.com/ganache