Blockchain-based Device Identity Management with Consensus Authentication for IoT Devices

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

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

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

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

***Abstract*—To decrease the IoT attack surface and provide protection against security threats such as introduction of fake IoT nodes and identity theft, IoT requires scalable device identity and authentication management. This work proposes a blockchain-based identity management approach with consensus authentication as a scalable solution for IoT device authentication management. The proposed approach relies on having a blockchain secure tamper proof ledger and a novel lightweight consensus-based identity authentication. The results show that the proposed decentralised authentication system is scalable as we increase number of nodes.**

***Index Terms*—IoT, D2D authentication, device identity management, blockchain technology.**

I. Introduction

In recent years, we have witnessed rapid deployments of Internet of Things (IoT) devices, employed in application areas such as home automation, industrial control, smart metering among others. IoT is enabling development of intelligent systems that have great potential to provide many benefits. Unfortunately, IoT device manufacturers current trend of producing cheaper IoT devices and neglecting expensive security features creates massive problems in terms of security and mitigation of cyberattacks. According to Gartner, the latest forecast for enterprise IoT platform's market will grow to $7.6 billions in 2024, a 31% increase from 2020 with significant increase of IoT deployments in many sectors [1]. Most IoT devices have many vulnerabilities that can allow cyber attackers to compromise them and use them to launch further attacks. For example, Mirai malware [2] and its latest variants were capable to compromise IoT devices and create botnets to launch DDoS attacks. With IoT devices becoming the main targets to cause damage, it is extremely important to have mechanisms to identify, manage and authenticate IoT devices. This is true in applications that have strict requirements in terms of security. Existing solutions [3]–[5] use centralised models with low scalability. These hinder usage in IoT because it creates bottlenecks and single point of failures.

II. Related Works

IoT device authentication mechanisms can be categorised into three types of approaches: solutions that rely on usage of digital certificates, device fingerprinting approaches and blockchain-based approaches. In [3] and [6] digital certificates are used with Elliptic Curve Cryptography (ECC) to secure IoT devices. The approaches rely on a centralised server to manage all security operations. [7] proposed a device authentication mechanism that combines session keys with Public Keys, however, a centralised authentication server is used to maintain certificates and mutual authentication. In [8] it is proposed an authentication protocol using certificateless Public Key Cryptography (PKC) but the proposed mechanism could be compromised due to the usage of long-term symmetric keys. The work [5] proposed identity-based authentication using digital certificates. Device identities are created by hashing virtual IPv6 addresses which are signed by using the public key of the SDN controller. The work of [9] suggested mechanisms in use for User to Device (U2D) identity management can be adopted with modifications in Device to Device (D2D) communications. The work proposes usage of a centralised identity store that keeps records of IoT devices. However, the drawback is the centralised store and once compromised then the whole system becomes insecure.

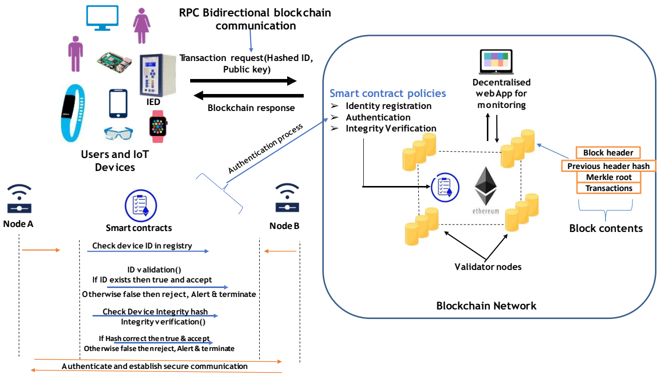
Unlike above approaches, [10] and [11], utilised device fingerprinting to uniquely identify and authenticate IoT devices. However, the approach is limited to Radio Frequency devices and fingerprinting approaches are highlighted as ineffective when dealing with identification of unknown devices [12]. Other device identification approaches can be seen on [13]–[15] however, they are limited to U2D interactions and most of IoT is expected to be characterised by D2D autonomous communications. Recently, there have been several device identity managements and IoT device authentication mechanisms leveraging blockchain technology that eliminates centralised model of management in device authentication.

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)]

The works [16]–[18] presented blockchain-based solutions for identity and access management to eliminate single point of failures and provide tamper proof systems. Others such as [19] proposed a trust and authentication model utilising blockchain technology and Web of Trust concepts. Nodes rely on other nodes for approval to join the network. Authentication data and trust information is stored in blockchain to guarantee integrity. IoT nodes use the blockchain network to verify data and authenticate each other. The work by [20] proposed a cross domain authentication model using blockchain. The approach utilises root Certificate Authorities (CA) as validator nodes and the model reduces encryption and decryption operations. The work [21] presented a decentralised authentication mechanism called bubbles of trust. In this solution IoT devices are placed in secure zones (bubbles). Each bubble has a master node that issue tickets to follower devices to associate themselves with the master by presenting their tickets to the blockchain platform. The blockchain is then utilised to authenticate devices and establish secure communication between devices within the same bubble. The work had limitations such as there were no inter-communications between nodes from different bubbles. In [22] identity-based P2P authentication using blockchain is proposed for IoT devices to overcome single point of failure (CA server). Device authentication is based on public and private keys and the solution utilises the sub-chain of blockchain validator nodes for authentication. However, the proposed authentication algorithm relies on trusted authenticator and the validator nodes are involved only if the receiver node failed to authenticate the requester. This means a malicious node may authenticate other malicious nodes without the extended check from validator nodes. Therefore, the approach may be susceptible to attacks. Derived from the literature review, non-blockchain based authentication approaches do not scale well in the presence of high number of IoT devices and they rely on centralised architectures. Such limitations hugely affect the overall performance, because as the number of nodes increase, performance decrease due to heavy reliance on the central server to manage authentication and security credentials. Furthermore, the server is seen as the single point of failure. Although there have been several studies using blockchain technology to authenticate devices addressing single point of failure of IoT systems, they still use PKC for device authentication. PKC requires repetition of heavy computations, which is a burden for constrained IoT. In this work we propose lightweight identity authentication with consensus agreement between nodes leveraging blockchain. Our approach provide scalable authentication with less delays and computations.

III. Proposed solution

This section describes the proposed solution which leverages blockchain for secure management of devices. The motivation of using blockchain technology comes from the benefits widely associated with its features, such as its resilience nature, tamper proof and extensive built-in cryptographic mechanisms for data confidentiality and Integrity. Furthermore, the way the blockchain replicate data is unique compared to other generic distributed storage because the underlying cryptography protects message exchanges, and it is nearly impossible to modify data compared to other generic solutions. Moreover, blockchain has built-in mechanisms to prevent replay attacks and sibyl attacks [23]. In this article we build on our previous work [24], focusing on the computational impact of the proposed approach. we have added a brief literature review, an extended security analysis and a new set of performance experiments that examine CPU utilisation of the proposed approach.



RPC Bidirectional blockchain communication
Transaction request(Hashed ID, Public key)
Blockchain response
IED
Users and IoT Devices
Authentication process
Node A
Smart contracts
Node B
Check device ID in registry
ID validation()
If ID exists then true and accept
Otherwise false then reject, Alert & terminate
Check Device Integrity hash
Integrity verification()
If Hash correct then true & accept
Otherwise false then reject, Alert & terminate
Authenticate and establish secure communication
Smart contract policies
➢ Identity registration
➢ Authentication
➢ Integrity Verification
Decentralised web App for monitoring
ethereum
Block header
Previous header hash
Merkle root
Transactions
Block contents
Validator nodes
Blockchain Network

Fig. 1: System Model & Authentication flow

A. *System model*

This section describes the system model for the proposed authentication approach and its components. The system model as illustrated in Figure 1 has three main components, which are IoT devices, identity registry ledger and blockchain network. The IoT devices have capability to store identity registry and interact with the other blockchain network nodes during authentication. The blockchain network has three purposes as follows: firstly, to store in a distributed manner generated device identities. Secondly, to protect integrity of generated identities and thirdly, to facilitate the consensus authentication process. Moreover, the blockchain increases the system resilience due to its replication of data. The scheme has the following assumptions: (1) Each IoT device has a pair of keys, in where the private key is used to sign its hashed ID to secure it from threats such as Man in the Middle and modification attacks. (2) IoT nodes are protected against physical attacks such as impersonation and side channel attacks this can be achieved by making sensitive data readable only by the device itself. (3) Each IoT node stores a Merkle tree of the public keys of all participating nodes as well as digital identities of all blockchain nodes. This information is later sent to any node that has an invitation to join the network.

The IoT calls for strong device identity to provide a Root of Trust at its foundation. Device identity is essential in establishing security. The device can achieve authentication, but a malicious attacker can steal its identity, modify and create backdoor for further malicious use. To address this problem, we protect device identity and its integrity [23] by using a secure blockchain registry. We create hashed device identities by extraction of device attributes such as device name, firmware, MAC address and its configuration files, and we add device clock to ensure uniqueness and enhance identity security. The created identities are stored in blockchain ledger and the ledger is effective in guarding sensitive data because of its tamper-evident Merkle tree structure.

B. Consensus-based Authentication

This section briefly describes the step-by-step authentication process in the proposed scheme. Figure 1 illustrates the step-by-step authentication of two nodes. When an IoT node sends an authentication request with its signed identity to another node, the smart contract code performs identity validation by checking the blockchain registry ledger. The local registry contains registered device identities and is identical to every participating node in the blockchain network. The blockchain network broadcasts the request to other IoT nodes to verify the identity of the requester to achieve a consensus agreement. The smart contract will reject and terminate the authentication process if the identity is invalid and other nodes will alert if there is a difference between requester identity and stored identity in their local blockchain registries. If the identity is valid then, integrity check follows with consensus agreement, a similar procedure as the identity check. At the end of the consensus process, IoT node is authenticated by device ID verification, where both the ID and the invoked transaction to request verification are protected by Elliptic Curve Digital Signature Algorithm (ECDSA) utilised by blockchain technology. After the verification the device is considered authenticated and message exchanges can be made with the second node. We note that identity authentication between the nodes is performed without requiring heavy computations. On the contrary, the existing PKC solutions requires every time to perform repeated cryptographic computations for node authentication. The presented communication exchanges uses ECDSA for secure communications and is considered suitable in IoT context [25] with better performance with large keys compared to similar algorithms such as RSA.

C. Security Analysis

In this section, we cover the security analysis of the proposed approach. The main goal is to check correctness and safety of the scheme against replay and man-in-the-middle attacks using a Dolev-Yao model because the model considers the intruder to have complete access to the network but lacks capability to break cryptography. We consider two types of attackers: a malicious internal blockchain node and malicious external node. Based on these two actors, we have considered 4 main security requirements:

1) Integrity and non-repudiation: In the proposed scheme, data integrity is achieved by signing it using the private key of the sender. This is achieved by using the ECDSA.

2) Replay attack protection: Blockchain communications are considered as transactions and every transaction has a timestamp and an ID and needs majority agreement to be confirmed. Once accepted by the consensus, any incoming transactions with the same ID regardless of time delay will be rejected, hence achieving message replay protection.

3) Eclipse attack protection.: The proposed device integrity check provides protection against eclipse attacks because for an attacker to succeed it must compromise node integrity, which will lead to hash mismatch and the node to be flagged as malicious during the authentication process.

4) Spoofed identity protection.: In the proposed scheme, the transaction history recorded in the blockchain ledger in form of Merkle tree is utilised to prevent identity spoofing attacks. The Merkle tree data structure contains cryptographic hashes of parent and child data blocks that protect the integrity of identities. Hash mismatch's of the parent or child data blocks enables identifying modification attacks.

IV. Experiments and Results

This section presents the experiments conducted to evaluate the authentication delay, throughput and CPU utilisation when the proposed scheme is in use and we compare against other approaches in the literature. The experiments were divided in two categories with two different software tools. For the first category, we measured latency and throughput by using HPE LoadRunner simulator designed to generate network traffic, detect errors, and measure performance [26]. LoadRunner was installed in a machine (AMD Ryzen 3, CPU @ 2.60GHz) with 8 GB of RAM running a Windows OS. Scripts were created to simulate Ethereum transactions to Ganache test platform, installed in an Ubuntu machine (Intel(R) Core (TM) i5-3230M CPU @ 2.60GHz with 8 GB of RAM). Truffle framework was used to compile and deploy the smart contract written in Solidity [27]. During experiments, 20,25,30,35 and 40 Virtual nodes (Vusers) were generated in LoadRunner to send blockchain transactions. The collective delay to authenticate simultaneously was measured for each set of nodes whereas the throughput was measured as number of bytes per second collectively sent from simulated nodes to the blockchain. While LoadRunner was useful for the first category of experiments, it had limitations in CPU utilisation experiments. The motivation of analysing CPU computation cost is because the authentication process involves invoking a blockchain transaction to verify the device identity to achieve device authentication. Blockchain transactions are considered computationally heavy especially when used in constrained IoT environments. We consider the computation test as essential in the feasibility of our authentication solution in IoT. We utilised a Common Open Research Emulator (CORE) emulator [28] in CPU computation tests with similar blockchain functionalities. We run a CPU monitoring tool s-tui [29] in the emulated nodes to collect CPU utilisation during experiments before and when our scheme is in use and we used similar number of nodes to achieve consistency. During experiments, we observed a nearly linear increase of the delay while increasing the number of nodes, going from 12 seconds for 20 nodes, up to 25 seconds for 40 nodes, as depicted in Figure 2. The latency results compare favourably to a centralised IoT authentication mechanism [30] based on MQTT where average authentication delay of 2.137 seconds for a single node will increase significantly with increase of nodes. For instance, with 20 nodes the latency

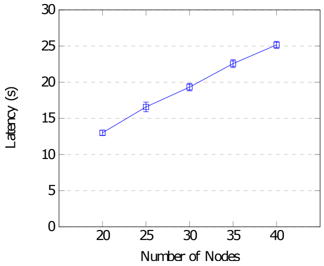


Fig. 2: Latency.

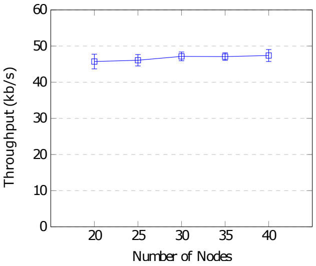


Fig. 3: Throughput.

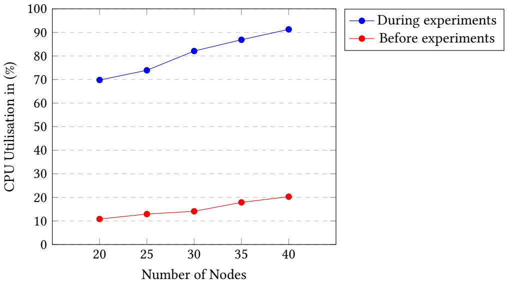


Fig. 4: CPU utilisation.

will reach approximately 40 seconds in the centralised model. Furthermore, in general, relying on a centralised solution with a single point of failure will hinder scalability and will cause higher latency values. Our approach relies on a permissioned blockchain which makes it considerably faster than other blockchain-based authentication mechanisms that have an additional 14s delay of public blockchain [21]. Furthermore, as shown in Figure 3, we observed stable average throughput as we increased number of nodes. This shows the system does retain its performance while increasing the number of nodes. In these results, it should be noted that the underlying Wi-Fi network at 433.3 Mbps used on site, provided a stable connection and no packet losses were detected by the simulator at any time. Moreover, as evident from the Figure 4 graph, there is a steep increase of CPU utilisation before and when our scheme is in use and gradual increase of CPU utilisation as we increased the number of nodes. This is only natural because as we increase number of nodes more transactions are sent during authentication process and this means more CPU computations are recorded collectively with the CPU monitoring tool. Overall, in terms of node scalability the latency, throughput and CPU utilisation with respect to number of nodes, the results suggest our solution is less impacted by all three metrics when scaling to more nodes.

V. Conclusion and Future Work

In this work, we presented the blockchain-based consensus authentication. To the best of our knowledge the solution has never been used for IoT device authentication. In future work, we will increase number of nodes in experiments, integrate decentralised authorisation service, optimisation protocol for the scheme and address privacy issues that may arise when storing device information in the blockchain.

References

[1] P. Middleton, A. Velosa, and F. Biscotti, “Forecast analysis: Enterprise iot platforms, worldwide.” Gartner, Apr. 2020.

[2] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis, D. Kumar, C. Lever, Z. Ma, J. Mason, D. Menscher, C. Seaman, N. Sullivan, K. Thomas, and Y. Zhou, “Understanding the mirai botnet,” in *USENIX Security Symposium*, 2017.

[3] J. Liu, Y. Xiao, and C. P. Chen, “Authentication and access control in the internet of things,” in *2012 32nd International Conference on Distributed Computing Systems Workshops*, IEEE, Jun 2012.

[4] C. H. Liu, B. Yang, and T. Liu, “Efficient naming, addressing and profile services in internet-of-things sensory environments,” *Ad Hoc Networks*, vol. 18, pp. 85–101, Jul 2014.

[5] O. Salman, S. Abdallah, I. H. Elhajj, A. Chehab, and A. Kayssi, “Identity-based authentication scheme for the internet of things,” in *2016 IEEE Symposium on Computers and Communication (ISCC)*, (Messina, Italy), pp. 1109–1111, IEEE, Jun 2016.

[6] B. Ndibanje, H.-J. Lee, and S.-G. Lee, “Security analysis and improvements of authentication and access control in the internet of things,” *Sensors*, vol. 14, pp. 14786–14805, Aug 2014.

[7] C.-J. Chae and H.-J. Cho, “Enhanced secure device authentication algorithm in p2p-based smart farm system,” *Peer-to-Peer Networking and Applications*, vol. 11, pp. 1230–1239, Jan 2018.

[8] D. Q. Bala, S. Maity, and S. K. Jena, “Mutual authentication for IoT smart environment using certificate-less public key cryptography,” in *2017 Third International Conference on Sensing, Signal Processing and Security (ICSSS)*, (Chennai, India), pp. 29–34, IEEE, May 2017.

[9] M. Trnka, T. Cerny, and N. Stickney, “Survey of authentication and authorization for the internet of things,” *Security and Communication Networks*, vol. 2018, pp. 1–17, Jun 2018.

[10] G. Baldini, R. Giuliani, G. Steri, and R. Neisse, “Physical layer authentication of internet of things wireless devices through permutation and dispersion entropy,” in *2017 Global Internet of Things Summit (GIoTS)*, (Geneva, Switzerland), IEEE, Jun 2017.

[11] Y. S. Dabbagh and W. Saad, “Authentication of wireless devices in the internet of things: Learning and environmental effects,” *IEEE Internet of Things Journal*, Apr 2019.

[12] F. Tehranipoor, N. Karimian, P. A. Wortman, A. Haque, J. Fahrny, and J. A. Chandy, “Exploring methods of authentication for the internet of things,” in *Internet of Things*, pp. 71–90, Chapman and Hall/CRC, 2017.

[13] P. N. Mahalle, *Identity Management Framework for Internet of Things*. PhD thesis, Aalborg University, 2014.

[14] D. van Thuan, P. Butkus, and D. van Thanh, “A user centric identity management for internet of things,” in *International Conference on IT Convergence and Security*, Oct 2014.

[15] A. Majeed and A. Al-Yasiri, “Consolidate the identity management systems to identify the effective actor based on the actor relationship for the internet of things,” in *Third International Congress on Information and Communication Technology*, pp. 755–765, Springer, 2019.

[16] X. Zhu, Y. Badr, J. Pacheco, and S. Hariri, “Autonomic identity framework for the internet of things,” in *International Conference on Cloud and Autonomic Computing*, Sep 2017.

[17] M. Nuss, A. Puchta, and M. Kunz, “Towards blockchain-based identity and access management for internet of things in enterprises,” in *International Conference on Trust and Privacy in Digital Business*, pp. 167–181, Springer, 2018.

[18] A. S. Omar and O. Basir, “Identity management in IoT networks using blockchain and smart contracts,” in *IEEE International Conference on Internet of Things and IEEE Green Computing and Communications and IEEE Cyber, Physical and Social Computing and IEEE Smart Data*, Jul 2018.

[19] A. Moinet, B. Darties, and J.-L. Baril, “Blockchain based trust & authentication for decentralized sensor networks,” *arXiv preprint arXiv:1706.01730*, Jun 2017.

[20] W. Wang, N. Hu, and X. Liu, “BlockCAM: A blockchain-based cross-domain authentication model,” in *IEEE Third International Conference on Data Science in Cyberspace*, Jun 2018.

[21] M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, “Bubbles of trust: A decentralized blockchain-based authentication system for iot,” *Computers & Security*, vol. 78, pp. 126–142, Sep 2018.

[22] D. Li, W. Peng, W. Deng, and F. Gai, “A blockchain-based authentication and security mechanism for IoT,” in *2018 27th International Conference on Computer Communication and Networks (ICCCN)*, IEEE, Jul 2018.

[23] N. Kshetri, “Can blockchain strengthen the internet of things?,” *IT professional*, vol. 19, pp. 68–72, Aug 2017.

[24] M. Mukhandi, E. Andrade, F. Damião, J. Granjal, and J. P. Vilela, “Blockchain-based scalable authentication for IoT,” in *Conference on Embedded Networked Sensor Systems*, Nov 2020.

[25] T. K. Goyal and V. Sahula, “Lightweight security algorithm for low power IoT devices,” in *2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, (Jaipur, India), pp. 1725–1729, IEEE, sep 2016.

[26] R. Abbas, Z. Sultan, and S. N. Bhatti, “Comparative analysis of automated load testing tools: Apache jmeter, microsoft visual studio (tfs), loadrunner, siege,” in *International Conference on Communication Technologies (ComTech), 2017*, pp. 39–44, IEEE, 2017.

[27] “Ganache.” https://www.trufflesuite.com/docs/ganache/overview, 2019.

[28] J. Ahrenholz, T. Goff, and B. Adamson, “Integration of the CORE and EMANE network emulators,” in *2011 - MILCOM 2011 Military Communications Conference*, IEEE, Nov 2011.

[29] A. Manuskin. https://github.com/amanusk/s-tui, 2020.

[30] A. Lohachab and Karambir, “ECC based inter-device authentication and authorization scheme using MQTT for IoT networks,” *Journal of Information Security and Applications*, vol. 46, pp. 1–12, Jun 2019.