Distributed Authentication in a Multi-Zone Direct Acyclic Graph Blockchain for IoT Environment

Salaheddine Kably[1,2*], *Tajeddine* Benbarrad[1], *Nabih* Alaoui[2], *Antonio* Guerrero-González*oz*[3] *and Mounir* Arioua[1]

[1]Laboratory of ENSA, Abdelmalek Saadi university, Tanger, Morocco TICLab, International University of Rabat, Morocco
[2]Ecole Supérieure d'Informatique et du Numérique, TICLab International University of Rabat, Morocco
[3]Department of Automation, ElectricalEngineering and Electronic Technology,Universidad Politécnica de Cartagena, Cartagena, Spain

Abstract. This research paper presents an in- depth examination of the security aspects of the Multiple Zone Direct Acyclic Graph Blockchain (MZ-DAG Blockchain) framework. The MZ-DAG Blockchain features a security layer that implements a non-clonable physical function-based validation mechanism for the authentication of multiple certificates within the blockchain. To enhance the security of this layer, this study proposes the integration of a lightweight intrusion detection system specifically designed for the MZ-DAG Blockchain. This work is a contribution to the ongoing efforts to secure and streamline the implementation of blockchain networks in resource- constrained environments**.**

1 Introduction

The Internet of Things (IoT) has a significant presence in various domains such as smart healthcare, smart homes, and many others[1]. However, this wide range of applications and constant need for connectivity has brought about significant security challenges in this technology[2]. In today's world, billions of devices are connected to the internet, exchanging vast amounts of data among inter-connected objects. This data often includes private and sensitive information that is vulnerable to security threats such as eavesdropping and tampering[1]. This puts the confidentiality of private data at risk[1]. Additionally, the IoT is a combination of different existing technologies like wireless sensor networks and cloud computing, thereby inheriting and magnifying all the security vulnerabilities of each technology[3].

To address these security challenges, researches are continuously exploring the integration of blockchain technology with IoT. The blockchain is a distributed ledger, replicated by all the nodes in its peer-to-peer network[1]. It eliminates the need

for a central entity of trust, and deploys a mechanism of transparency by maintaining a historical record of all transactions in a constantly synchronized registry[3]. The consensus algorithm ensures the security, orchestration, and validation of transactions[5]. The blockchain network is made up of various peer-to-peer nodes and shares a set of validated blocks. Each block contains a hash of the previous block, creating a chain of

* Corresponding author: salaheddine.kably@gmail.com

blocks from the genesis block to the last block[6]. Recent innovative research has led to the development of the multiple-zone Direct Acyclic Graph (MZ- DAG) blockchain, which is well-suited for the IoT environment[7]. This blockchain is based on the Proof-of-Authentication (PoAh) consensus, delegating heavy computational tasks to fog nodes and preserving the limited energy resources of IoT devices[7]. IoT and fog nodes are authenticated using a non-cloneable physical function-based validation mechanism (DPUF-VM)[8]. The lightweight CubeHash algorithm is used to store each transaction in the blockchain, signed by the Four-Q Curve algorithm[8]. Sensitive data is stored as ciphertext in the cloud, and fog nodes provide added data security to avoid the energy consumption and complexity of IoT nodes. The fog node performs a redundancy analysis using the Jaccard Similarity Measure (JS) and sensitivity analysis using the Neutrosophic Neural Intelligent Network (N2IN) algorithm[8].

In this work, we aim to enhance the MZ-DAG Blockchain by adding a security layer that performs an intrusion detection system (IDS). IDS is an emerging topic in the IoT due to the increasing number of cyber-attacks that cause significant damage. Traditional IDS requires a unified architecture for security monitoring and control, but most machine learning approaches for attack detection have low accuracy and precision[9]. The widespread deployment of Internet of Things (IoT) and Industrial Internet of Things (IIoT) devices has resulted in a need for efficient and effective security solutions[1]. Conventional network security tools, such as firewalls and honeypots, are often insufficient due to their vulnerability to attacks and their lack of suitability for resource constrained IoT and IIoT devices[10]. This is due to the limited storage capacity and computation power of these devices. The accuracy of intrusion detection systems and security tools is also a concern, as it is challenging to predict the presence of attackers and respond to their behavior in a timely manner[11].

The current heterogeneous IoT environment is susceptible to a range of severe security threats, including spoofing, DDoS attacks, disruptions, energy exhaustion, and insecure communication[12]. The exponential growth of IoT devices results in a corresponding increase in vulnerabilities, making it difficult to monitor and secure these devices effectively[13]. The dynamic nature of normal and anomalous behavior in IoT devices further complicates the task of detecting and preventing security attacks[14].

The impact of security attacks on IoT devices can vary widely[3]. For this reason, it is crucial to develop and implement effective intrusion detection schemes that take into account the diverse security requirements and capabilities of IoT devices[8]. These requirements include event handling, memory, bandwidth, computational power, and energy consumption[7]. An efficient and effective intrusion detection system must be able to address these heterogeneous requirements in order to ensure the security of IoT devices in the face of evolving threats[8].

2 Research aim and motivation

Before A proposed device for distributed authentication in a Fog-IoT environment that leverages distributed blockchain technology [15] presents several significant technical challenges that need to be addressed.

Firstly, while the proposed approach restricts access to non-authorized users, it also increases complexity through the use of the Elliptic Curve Digital Signature Algorithm (ECDSA) and Secure Hash Algorithm 1 (SHA-1) algorithms, both of which are computationally intensive. ECDSA is a public-key cryptography algorithm used for digital signatures and key agreement, while SHA-1 is a cryptographic hash function. The use of these algorithms in the authentication mechanism results in increased computational overhead, which may be a concern in resource-constrained IoT environments.

Additionally, the authentication mechanism is based on unprotected parameters such as the system ID and public address, which can be easily falsified. This vulnerability reduces the overall security of the system and undermines the authenticity of the authentication process. Furthermore, the public address is transmitted via a public network, which increases the risk of exposure and makes it more vulnerable to attacks.

The work also utilizes the Proof of Work (PoW) consensus algorithm, which requires all participating nodes to validate transactions and broadcast proof. The use of PoW results in increased resource consumption, particularly for nodes with lower resources. For example, a node with a higher load or lower computational power will consume more resources to validate transactions, leading to a reduced overall efficiency of the network. The use of PoW also results in scalability issues, even with the use of a blockchain filter, as the conventional blockchain structure is not suitable for IoT environments, which generate millions of data and result in data redundancy, leading to unlimited growth of the blockchain. An alternative approach, the Efficient Lightweight Integrated Blockchain [15] (ELIB) design proposes a lightweight consensus algorithm that restricts the number of blocks generated in the blockchain, reducing the time consumption of the validation process. However, this process still increases time consumption, particularly in IoT environments with millions of transactions, where the waiting time for all transactions in the network is increased. The BFAN[16] (fog-based blockchain and network architecture) approach deploys fog nodes, but the consensus algorithm is still executed by the resource-constrained IoT nodes, leading to inefficiency and increased computational overhead. The use of the Secure Hash Algorithm 2 (SHA-2) and ECDSA further increases complexity and reduces security levels, as both algorithms require increased computational power. Data encryption also leads to increased data size and network complexity, adding further challenges to the deployment of a secure and efficient distributed authentication system in a Fog-IoT environment.

Moreover, while the proposed device for distributed authentication in a Fog-IoT environment leverages the benefits of distributed blockchain technology, it still faces several technical challenges, including increased complexity, reduced security, scalability issues, and increased computational overhead. Further research is required to address these challenges and improve the efficiency and security of the proposed system.

3 Proposed framework

Our proposed framework employs a Dynamic Physically Unclonable Functions based Validation Mechanism (DPUF-VM) in conjunction with the blockchain network to ensure the authentication of IoT nodes and fog nodes. The DPUF-VM system generates

a unique random identifier (RID) for each IoT node dynamically, based on its sensor ID, MAC address, PUF, and the last sensed value. The RID is then registered with the blockchain network as a hash function along with other identification pieces of information. This approach ensures that the RID is unique and cannot be cloned by any attacker. Additionally, the framework uses the CubeHash algorithm for hash generation to enhance the security of the credential registration process.

The proposed algorithm consists of two main steps, device registration and credential registration. In device registration, the devices register their identification information to the blockchain network through BGW. For each sensor, the identification pieces of information are SID, SMAC, PUF, and the last sensed value. The RID is then generated as :

$$RID(i) = SID(i) \oplus \rho i \quad (1)$$

which changes dynamically based on the current sensed value. In credential registration, the credentials are stored in the blockchain network as hash values using the CubeHash algorithm. The CubeHash algorithm uses five major parameters to generate the hash values, which increases the security of the framework. Overall, the proposed framework provides a dynamic and secure approach for authenticating IoT and fog nodes using DPUF-VM with the blockchain network. The framework ensures that the RID is unique and cannot be cloned by any attacker, and the CubeHash algorithm enhances the security of the credential registration process.

Here is a proposed algorithm steps for the Dynamic Physically Unclonable Functions based Validation Mechanism with blockchain assistance:

3.1 Device Registration

a. Each IoT node and fog node generates a random identification number $RID(i)$ using the formula above, where $SID(i)$ is the sensor ID, and ρi is the last sensed value by the sensor.

b. The devices then register their identification information, including SID(i), SMAC(i), PUF(Sc- r,(i)), and $RID(i)$, with the blockchain network through BGW.

3.2 Credential Registration

a. The CubeHash algorithm is proposed for generating hash values for credentials.

b. The CubeHash algorithm uses the following parameters for hash generation: message, hash length, number of rounds, key, and salt.

c. The devices store their credentials, including $RID(i)$, SID(i), SMAC(i), PUF(Sc-r,(i)), and the hash value generated by the CubeHash algorithm, on the blockchain network.

3.3 Authentication

a. When a device requests access to the network, it sends its identification information to the blockchain network.

b. The blockchain network uses the identification information to verify the hash value generated by the CubeHash algorithm.

c. If the hash value matches the stored value, the device is authenticated and granted access to the network.

d. If the hash value does not match, the device is rejected, and access is denied.

3.4 Dynamic Update of RID

a. At predefined time intervals, or when the sensed value changes significantly, the device updates its RID using the formula :

$$RID(i) = SID(i) \oplus \rho i \quad (2)$$

where ρi is the new sensed value.

b. The updated RID is then sent to the blockchain network for registration and authentication.

This algorithm provides a dynamic and secure approach for authenticating IoT and fog nodes using DPUF-VM with the assistance of the blockchain network. It ensures that the RID is unique and changes dynamically, and the CubeHash algorithm enhances the security of the credential registration process as shown in figure 1.

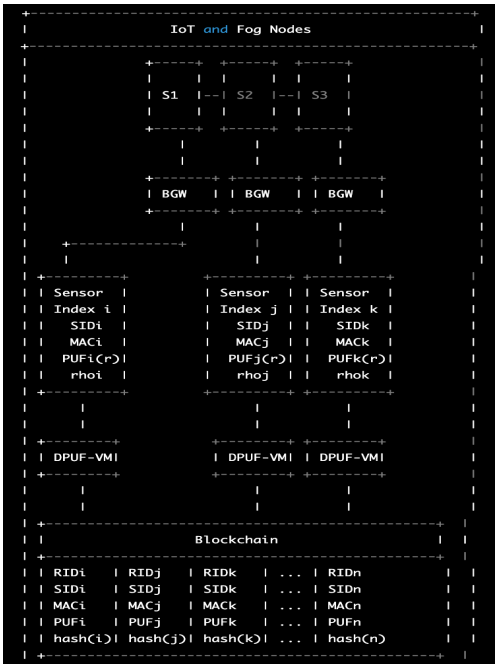

Fig. 1. Figure 1: DPUF-VM authentication mechanisms in the Multizone DAG Blockchain

4 Conclusion

In conclusion, the proposed framework for distributed authentication in a Fog-IoT environment that leverages distributed blockchain technology addresses a significant problem in IoT and fog computing, namely ensuring secure and dynamic authentication.

However, the proposed system also faces several technical challenges that need to be addressed. These challenges include increased complexity, reduced security, scalability issues, and increased computational overhead. The use of computationally intensive algorithms, such as ECDSA and SHA-1, results in increased computational overhead, which is a concern in resource-constrained IoT environments. Additionally, the use of unprotected parameters, such as the system ID and public address, increases the vulnerability of the authentication process. The proposed system also utilizes the PoW consensus algorithm, which results in increased resource consumption and scalability issues. Further research is required to improve the efficiency and security of the proposed system, and alternative approaches such as the ELIB design and BFAN approach can be explored to address these challenges. Despite these challenges, the proposed framework provides a significant contribution to the development of secure and efficient authentication mechanisms in IoT and fog computing environments.

References

1. N. Alaoui, S. Kably, and M. Arioua, "Lightweight blockchain network architecture for IoT devices," in The 3rd International Symposium on Advanced Electrical and Communication Technologies (ISAECT2020), 2020, pp. 1-6, doi: 10.1109/ISAECT50116.2020.9308458.
2. B. Mackenzie, R. I. Ferguson, and X. Bellekens, "An Assessment of Blockchain Consensus Protocols for the Internet of Things," in Proceedings of the 2018 International Conference on Internet of Things, Embedded Systems and Communications (IINTEC), 2018, pp. 183–190, doi: 10.1109/IINTEC.2018.8695298.
3. D. Zakariae, E. Abdellah, and B. A. Saïd, "A lightweight blockchain framework for IoT integration in smart cities," Turkish Journal of Computer and Mathematics Education, vol. 12, no. 5, pp. 889–894, 2021, doi: 10.17762/turcomat.v12i5.1731.
4. N. Kably, S. Alaoui, M. Arioua, and N. Alaoui, "Lightweight blockchain network architecture for IoT devices," 2020. [Online]. Available: https://www.researchgate.net/publication/344716424_Lightweight_blockchain_network_architecture_for_IoT_devices.
5. S. Biswas, K. Sharif, F. Li, S. Maharjan, S. P. Mohanty, and Y. Wang, "PoBT: A Lightweight Consensus Algorithm for Scalable IoT Business Blockchain," IEEE Internet of Things Journal, vol. 7, no. 3, pp. 2343–2355, 2020, doi: 10.1109/JIOT.2019.2958077.
6. Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," in Proceedings of the 2017 IEEE 6th International Congress on Big Data (BigData Congress), 2017, pp. 557–564, doi: 10.1109/BigDataCongress.2017.85.
7. S. Kably, M. Arioua, and N. Alaoui, "Lightweight Direct Acyclic Graph Blockchain for Enhancing Resource-Constrained IoT Environment," Computational Materials and Continua, vol. 71, no. 2, pp. 5271–5291, 2022, doi: 10.32604/cmc.2022.020833.

8. S. Kably, T. Benbarrad, N. Alaoui, and M. Arioua, "Multi-Zone-Wise Blockchain Based Intrusion Detection and Prevention System for IoT Environment," Computational Materials and Continua, vol. 74, no. 1, pp. 253–278, 2023, doi: 10.32604/cmc.2023.032220.
9. C. Liang, Z. Guan, J. Shao, L. Zhang, and Q. Wang, "Intrusion detection system for the internet of things based on blockchain and multi-agent systems," Electronics, vol. 9, no. 7, pp. 1–27, 2020, doi: 10.3390/electronics9071120.
10. A. A. Elsaeidy, A. Jamalipour, and K. S. Munasinghe, "A Hybrid Deep Learning Approach for Replay and DDoS Attack Detection in a Smart City," IEEE Access, vol. 9, pp. 154864-154875, 2021, doi: 10.1109/ACCESS.2021.3128701.
11. K. Zhang, F. Zhao, S. Luo, Y. Xin, and H. Zhu, "An Intrusion Action-Based IDS Alert Correlation Analysis and Prediction Framework," IEEE Access, vol. 7, pp. 150540-150551, 2019, doi: 10.1109/ACCESS.2019.2946921.
12. W. Li, Y. Wang, J. Li, and M. H. Au, "Toward a blockchain-based framework for challenge-based collaborative intrusion detection," International Journal of Information Security, vol. 20, no. 2, pp. 127-139, 2021, doi: 10.1007/s10207-020-00488-6.
13. O. Alkadi, N. Moustafa, B. Turnbull, and K. K. R. Choo, "A Deep Blockchain Framework-Enabled Collaborative Intrusion Detection for Protecting IoT and Cloud Networks," IEEE Internet of Things Journal, vol. 8, no. 12, pp. 9463-9472, 2021, doi: 10.1109/JIOT.2020.2996590.
14. R. Qaddoura, A. M. Al-Zoubi, H. Faris, and I. Almomani, "A multi-layer classification approach for intrusion detection in IoT networks based on deep learning," Sensors, vol. 21, no. 9, pp. 1-21, 2021, doi: 10.3390/s21092987.
15. S. N. Mohanty et al., "An efficient Lightweight integrated Blockchain (ELIB) model for IoT security and privacy," Future Generation Computer Systems, vol. 102, pp. 1027-1037, 2020, doi: 10.1016/j.future.2019.09.050.
16. P. Singh, A. Nayyar, A. Kaur, and U. Ghosh, "Blockchain and fog based architecture for internet of everything in smart cities," Future Internet, vol. 12, no. 4, pp. 1-12, 2020, doi: 10.3390/FI12040061.