Enhancing Internet of Things Security and Efficiency: Anomaly Detection via Proof of Stake Blockchain Techniques

Seyed Salar Sefati
Telecommunications Department
National University for Science and Technology POLITEHNICA Bucharest
Bucharest, Romania
sefati.seyedsalar@upb.ro

Ahmed M. Nor
Telecommunications Department
National University for Science and Technology POLITEHNICA Bucharest
Bucharest, Romania
ahmed.nor@upb.ro

Octavian Fartu
Telecommunications Department
National University for Science and Technology POLITEHNICA Bucharest
Bucharest, Romania
octavian.fratu@upb.ro

Simona Halunga
Telecommunications Department
National University for Science and Technology POLITEHNICA Bucharest
Bucharest, Romania
simona.halunga@upb.ro

***Abstract*—Advances in communication technology and embedded systems have ushered in a new paradigm known as the Internet of Things (IoT). Currently, IoT is one of the most significant trends in industrial transformation and beyond 5G networks. Blockchain techniques have become essential features for applications, primarily due to their potential in ensuring security and privacy. Consequently, there is a growing interest in utilizing Blockchain for these purposes in modern IoT devices. In this paper, we introduce the Proof of Stake (PoS) algorithm as a mean to achieve consensus among nodes for anomaly data detection. The Blockchain model in IoT encompasses four elements: $Hash_{prev}, Hash_{next}$, Transactions, and Randomness. During the election process in Blockchain, the sensor nodes consider two parameters: firstly, node identification based on the Internet Protocol (IP), and second, the Uniform Resource Name (URN). Our findings show that the proposed method outperforms existing schemes in terms of the Quality of Experience (QoE) metrics, such as the Processing Time Reduction Ratio (PTRR), Resource Gain (RG), and latency.**

***Index Terms*—Internet of Things, Security, Blockchain, QoS**

I. Introduction

The Internet of Things (IoT) has emerged as a pivotal technology, garnering substantial attention from both academic and industry researchers. Presently, IoT holds paramount significance in information technology (IT) and computer engineering, enabling researchers to assemble, test, and disseminate data. Projections suggest that by the end of 2025, most individuals will possess approximately nine smart devices in their daily lives [1]. Within an IoT network, sensors play an indispensable role as they capture, collect, transfer, and process environmental data, subsequently transmitting it to Cloud Computing (CC) [2]. Consequently, IoT can bolster a range of 5G and beyond scenarios, e.g., business applications, encompassing smart farming, smart factories, smart cities, and the food industry.

The advent of Blockchain networks can address myriad security challenges in IoT. Fundamentally, Blockchain can oversee both large and small scale distributed systems and IoT networks [3]. Within IoT networks, Blockchain serves as a system for logging and communicating information to CC. What distinguishes Blockchain from other systems is its distributed information storage across all IoT sensors. As a result, encryption and data distribution techniques substantially diminish the potential risks of hacking, deletion, and data manipulation. Blockchains facilitate decentralized transaction validation, leading to significant cost reductions [4].

Cryptocurrency protocols employ the Proof of Stake (PoS) mechanism [5] to achieve consensus. In PoS-based Blockchains, transaction verification depends on the tokens that participants have staked or secured within the network as collateral. In this study, we introduce an anomaly detection method leveraging the PoS algorithm. Collective anomalies are identified based on typical time series patterns, such as recurring patterns observable across multiple IoT devices [6]. The PoS algorithm adopts a dual-faceted approach for reliable data acquisition: node identification based on the Internet Protocol (IP) [7] and the Uniform Resource Name (URN) [8]. A detailed discussion of the proposed method is presented in Section III. The principal objectives of the present study are:

- To examine Quality of Experience (QoE) methodologies rooted in Blockchain techniques for specific IoT systems.
- To enhance the Processing Time Reduction Ratio (PTRR) and Resource Gain (RG) utilizing the PoS algorithm.

- To mitigate latency by augmenting the number of applications.

II. Related work

The primary objective of this article is to detect anomalous data within IoT environments. Consequently, the related research should primarily address three essential topics: QoS, QoE, and the QoE/QoS relationship.

Uthansakul, et al. [9] introduced an Artificial Neural Network (ANN) algorithm to assess QoE utilizing Drive Tests. The data for this study were gathered with the aid of sensor devices and multimedia services. Their approach demonstrated commendable performance, being cost-effective and efficient in processing time. Li, et al. [10] put forth a smart routing protocol based on collaborative theory to identify anomalous data. Their study underscores crucial determinants influencing data transmission and implements multi-hop wireless network (MWN) applications. When juxtaposed with the Ad-hoc On-Demand Distance Vector (AODV) and Dynamic Source Routing protocol (DSR), their method consumed less energy and exhibited reduced latency. Mahmud, et al. [11] presented a QoE-aware application founded on fog computing and the fuzzy logic algorithm. They employed the fuzzy logic approach to compute the ratings of anticipated services and to maximize QoE. Their research stood out for its average application placement time, cost-effectiveness, and minimal data packet loss during transfer. Baranwal, et al. [12] introduced the Topsis algorithm to detect anomalies in data, drawing upon fog computing. Their approach leveraged the Topsis algorithm to categorize challenges and seek solutions aligned with algorithmic features. Their findings highlighted that their method's processing time and network congestion outperformed other techniques. Sefati and Halunga [13] advocated for data forwarding in IoT networks with a keen awareness of fault tolerance, employing clustering methodologies. To counteract anomalous data, they implemented techniques emphasizing high remaining energy and low buffer queues for data transmission to neighboring devices. Their approach showcased superiority over metaheuristic algorithms in energy conservation and latency reduction. Jinha Song et al. [14] focus on enhancing IoT Blockchain networks' security through the development of a novel anomaly detection method and a corresponding visualization tool. Their work introduces a dynamic threshold-based anomaly detection technique, which is particularly suited for IoT devices, and develops a tool for the real-time monitoring of Blockchain health and IoT data. Furthermore, their study addresses the unique challenges in applying traditional anomaly detection methods within the Blockchain context, especially for resource-constrained IoT environments.

III. The parameters of QoE

QoE, or Quality of Experience, gauges a customer's overall satisfaction level with a vendor. It operates similarly to Quality of Service (QoS). In QoE, both hardware and software metrics can be measured, and guarantees regarding these metrics can be provided to customers [15]. Some primary criteria in QoE include the PTRR, RG, and low latency. This section will delve into the mathematics of these parameters.

$$PTRR_{ij} = \frac{e_i^{pt} \times o^{ps}}{dss_i} \tag{1}$$

where e_i^{pt} indicates the value of the application required by resources. In this metric, pt indicates to the processing time and i is a working application on the cloud. o^{ps} demonstrate the processing speed of computing, where ps is the processing speed and o is number of computing. dss_i is the data signal size of application. The average PTTR can be demonstrated as:

$$PTTR_{avg} = \frac{1}{NoA} PTRR \tag{2}$$

where NoA represents how many applications were successfully installed on the CC instances. Moreover, RG is a metric that evaluates the resource consumption of a users [12], and can be expressed as:

$$RG_{ij} = \frac{o_j^{Ra}}{e_i^{Rr}} \tag{3}$$

where O_j^{Ra} demonstrates the resource availability of computing instance j. Ra is the available resource at j time. e_j^{Rr} is the expected value of the required resources of the application. Rr is the required resource.

$$\mathrm{RG}_{avg} = \frac{1}{NoA} RG \tag{4}$$

where NoA represents how many applications were successfully installed on the CC instances.

The low latency is the consumed time for the successful end-to-end transmission of one packet to the cloud and can be represented as:

$$\mathrm{T}_{total} = \mathrm{T}_{proc-TX} + \mathrm{T}_{access} + \mathrm{T}_{TR} + \mathrm{T}_{proc-RX} + \mathrm{T}_{Ack} \tag{5}$$

where $T_{proc-TX}$ demonstrate the signal processing, and $T_{Proc-RX}$ shows delay in the receiver. T_{Access} shows the devices access to the channel, and T_{TR} is the delay for packet transmission in space.

A. Blockchain model

The Blockchain in the IoT model consists on four approaches: $Hash_{Prev}$, $Hash_{next}$,Transactions and Randomness. The duty of $Hash_{Prev}$ is to capture the first input data in the network, and this Hash can no longer be changed once set. $Hash_{next}$is responsible for selecting the next block based on the previous block. For example, if an IoT sensor inputs data for the first time with this IP address: 172.16.154.47 and URN: isbn: 9780470114872, the $Hash_{next}$ must accept the new data with this IP and URN.

Fig 1 demonstrates that $Block_{n+1}$ is newly generated based on the previous block. Transactions save all information packets in both $Block_{n+1}$ and $Block_n$. Meanwhile, Randomness, in this context, refers to a predictable sequence used to

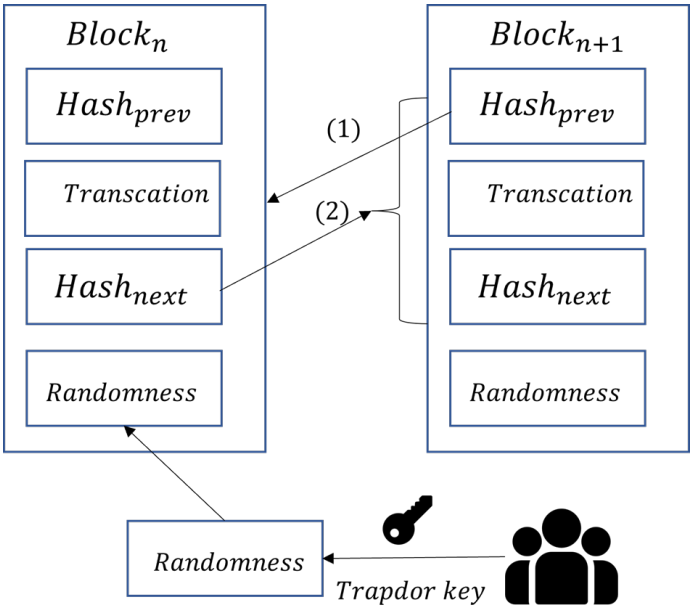

Fig. 1. Blockchain based on Hash

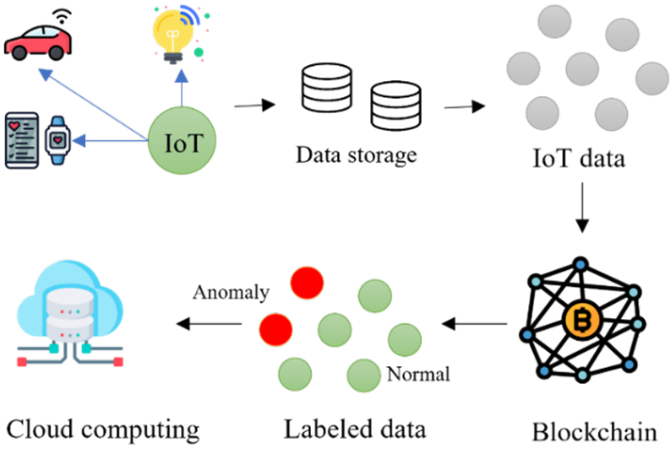

Fig. 2. Blockchain based on Hash

calculate the progression from the previous block to the next during generation.

When the Blockchain system want to select $Block_{n+1}$, $Hash_{next}$, and randomness, it works as equation (6).

$$\mathrm{r}_n = \frac{\mathrm{m}_n + tk_n r_n - m_n}{tk_n} \tag{6}$$

where m_n demonstrates the original value of the first block. After record the previous $Block_n$, $Hash_{next}$ become m'_n. Tapdor key is tk_n.Tapdor key is 256 binary digits long and often consists of 64 numbers and letters.

B. Proposed method

PoS is a consensus mechanism employed within Blockchain networks to achieve agreement among nodes. Such consensus mechanisms are vital for validating the authenticity of data and ensuring network security. Bitcoin, the pioneering digital currency, employed a Proof of Work (PoW) algorithm for this purpose. Nevertheless, several researchers have highlighted the significant energy consumption, high costs associated with block mining, and relatively slow transaction confirmation speeds inherent to PoW algorithms. In this study, we introduce a method to detect anomalous data utilizing the PoS algorithm. In supply chain contexts, shipment delays are frequent; however, when these delays become recurrent, they warrant further investigation [16]. Fig 2 illustrates the method proposed in this study.

By using this algorithm, we can reach reliable data and send it to users. In which, data is first collocated from the environment, then sent to the Blockchain system to find the anomaly data, where the Blockchain system is divided into 8 steps:

- Step 1: The Blockchain system is distributed in all sensors in each cluster.
- Step 2: When each sensor wants to add new data from the environment to the network, they must use 4th method: $Hash_{prev}$,$Hash_{next}$,Transactions and randomness.
- Step 3: In this method, all sensor nodes in the network are committee members. Therefore, all committee members should accept approval to add new information to the network.
- Step 4: When new data is extracted from the environment, the public key of the new data will propose to the recommender.
- Step 5: Before the start of the election, a new seed is set randomly for each term. A seed is a particular node that authorizes the incorporation of new nodes into the network and maintains the strength of the network at all times by allowing them to synchronize and obtain a copy of the network's data. This process is so important to find the anomaly data in a network because, without randomness, sensor nodes (committee members) can predicate the data and cannot find the anomaly. Furthermore, new data used a previous $block_n$ as a new seed for next generation and $Hash_{next}$ will be new seed.
- Step 6: For identify the anomaly data we used the 2 parameters for evaluation. First, Identity addressing based on IP: In order to send and receive data in an IoT system, each node needs to have an IP address. It is similar to a telephone number, and it should be unique. In this proposed method the object name service (ONS) first captures the IP address of each node and this process called $Hash_{prev}$and after each extracting the $Hash_{next}$ compare this evaluation.
- Step 7: In this study, we have focused on evaluating identity addressing based on both the URN and the IP between the nodes. It is crucial to clarify the use of terminologies Uniform Resource Identifier (URI) and URN as they are used interchangeably at certain points in the paper. While URIs and URNs are conceptually similar, their functional roles can differ significantly, especially in Blockchain-based systems like the one discussed in our paper. In our

methodology, we predominantly deal with URNs when discussing identity addressing within the Blockchain network. The URN is produced by the Internet engineering task force (IETF). The IETF describes the syntax possible addressing method and registration method. A URI is a string of characters used to identify or name a resource on the IoT. URI schemes include the Hypertext Transfer Protocol (HTTP) and File Transfer Protocol (FTP). In the context of the IETF community, two distinct syntax types are recognized: Prefix and Suffix. For the purposes of our method, we specifically employed the Suffix syntax. Fig 3 shows the difference between these 2 approaches.

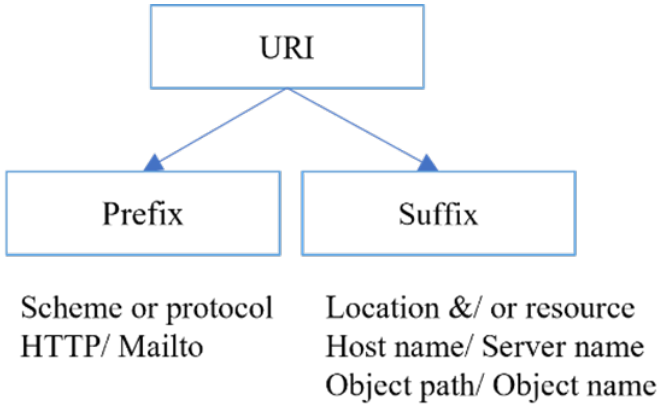

Fig. 3. Blockchain based on Hash

- Step 8: The committee member is elected based on those parameters. The committee member used this formula:

$$\gamma = \frac{hash}{2hashlen} \tag{7}$$

hashlen is the bit-length of hash. γ is the value used to verify committee member. Table I shows the encoding message and the trusted data elected between the 30 nodes. In this table, sensors were accepted based on the IP checker and URN. The data is transformed into JSON (JavaScript Object Notation) messages, and these messages are encoded using the IOTA API methods.

IV. Results

The proposed method in this paper has been simulated in Network Simulator (NS3) and compared with Fuzzy based QoE aware placement (FQP) [12] and Topsis based QoE aware placement (TQP) [13]. The dataset is used in a real environment and the simulation parameters are summarized in table I.

The first metric, PTRR, shows that the proposed method has an excellent experimental in comparison with FQP and TQP. The FQP has used fuzzy logic, hence this algorithm takes time to process. Fig 5 shows the PTRR.

The second metric shows that the proposed method performs well in resource gain. The TQP also has an immediate answer to the proposed method. TQP used a Topsis algorithm for

TABLE I
Simulation Parameters

Parameters	Value
Access rate	2-10 per sec
Resource requirement	1-8 CPU
Processing time	30-120 ms
Service cost	0.1-0.15 per min
Data signal size	1000-2000 instructions
Round trip time	100-600 ms

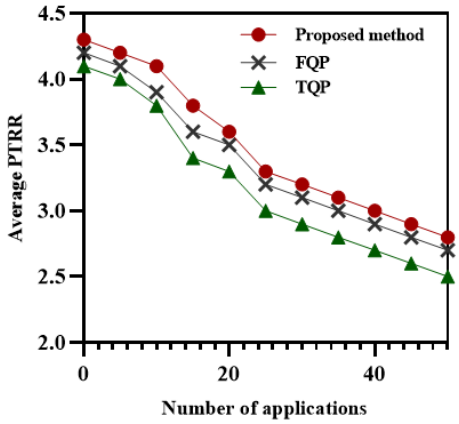

Fig. 4. Processing Time Reduction Ratio

awareness of the QoE. Fig 4 shows the average RG in the same dataset.

Concerning the delay, Fig 6 are shown the results obtained regarding delay in ms versus the number of applications. The result shows that the proposed method has a lower latency in compering with other algorithms.

V. Conclusion

An up-to-date networking and computing approach for the IoT, sensor networks, and other applications has recently been acclaimed as CC. There are several benefits of using available networks in conjunction with CC. One of the main challenges with cloud-based IoT systems is establishing an algorithm that can efficiently detect anomalous data. This paper employs the Blockchain PoS approach to detect such data. In the PoS algorithm, we employed election techniques, of which two types are discussed. We have evaluated identity addressing based on both the URN and the IP between the nodes. If 51 percent of nodes agree on a data value, this information can be added to the network. The results indicate that our proposed method offers improved PTRR and RG compared to other methods with lower latency.

Acknowledgment

This study has been conducted under the project 'MObility and Training fOR beyond 5G eco-systems (MOTOR5G)'. This project has funded from the European Union's Horizon

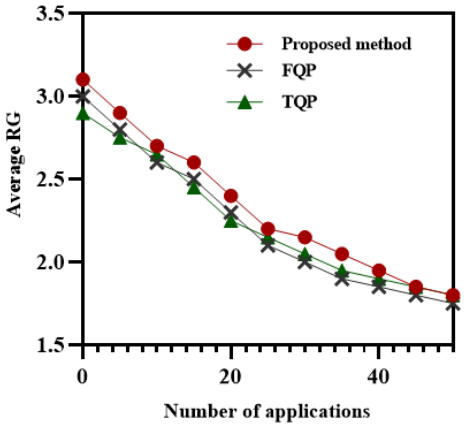

Fig. 5. Average of resource gain in cloud

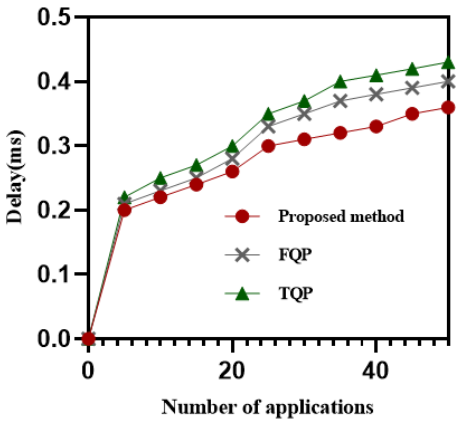

Fig. 6. Latency in a different number of applications

2020 programme under the Marie Skłodowska Curie Actions (MSCA) Innovative Training Network (ITN) under grant agreement No. 861219.

REFERENCE

[1] Li L. China's manufacturing locus in 2025: With a comparison of "Made-in-China 2025" and "Industry 4.0". Technological forecasting and social change. 2018 Oct 1;135:66-74.

[2] Sefati SS, Arasteh B, Halunga S, Fratu O, Bouyer A. Meet User's Service Requirements in Smart Cities Using Recurrent Neural Networks and Optimization Algorithm. IEEE Internet of Things Journal. 2023 Aug 8.

[3] Biswas S, Sharif K, Li F, Maharjan S, Mohanty SP, Wang Y. PoBT: A lightweight consensus algorithm for scalable IoT business blockchain. IEEE Internet of Things Journal. 2019 Dec 6;7(3):2343-55.

[4] Sefati SS, Halunga S, Farkhady RZ. Cluster selection for load balancing in flying ad hoc networks using an optimal low-energy adaptive clustering hierarchy based on optimization approach. Aircraft Engineering and Aerospace Technology. 2022 Apr 22;94(8):1344-56.

[5] Niya SR, Schiller E, Cepilov I, Maddaloni F, Aydinli K, Surbeck T, Bocek T, Stiller B. Adaptation of proof-of-stake-based blockchains for IoT data streams. In2019 IEEE international conference on blockchain and cryptocurrency (ICBC) 2019 May 14 (pp. 15-16). IEEE.

[6] Sharma B, Sharma L, Lal C. Anomaly detection techniques using deep learning in IoT: a survey. In2019 International conference on computational intelligence and knowledge economy (ICCIKE) 2019 Dec 11 (pp. 146-149). IEEE.

[7] Wu M, Lu TJ, Ling FY, Sun J, Du HY. Research on the architecture of Internet of Things. In2010 3rd international conference on advanced computer theory and engineering (ICACTE) 2010 Aug 20 (Vol. 5, pp. V5-484). IEEE.

[8] Singh D, Tripathi G, Jara AJ. A survey of Internet-of-Things: Future vision, architecture, challenges and services. In2014 IEEE world forum on Internet of Things (WF-IoT) 2014 Mar 6 (pp. 287-292). IEEE.

[9] Uthansakul P, Anchuen P, Uthansakul M, Khan AA. Estimating and synthesizing QoE based on QoS measurement for improving multimedia services on cellular networks using ANN method. IEEE Transactions on Network and Service Management. 2019 Oct 8;17(1):389-402.

[10] Li L, Chang L, Song F. A smart collaborative routing protocol for qoe enhancement in multi-hop wireless networks. IEEE Access. 2020 May 25;8:100963-73.

[11] Mahmud R, Srirama SN, Ramamohanarao K, Buyya R. Quality of Experience (QoE)-aware placement of applications in Fog computing environments. Journal of Parallel and Distributed Computing. 2019 Oct 1;132:190-203.

[12] Baranwal G, Yadav R, Vidyarthi DP. QoE aware IoT application placement in fog computing using modified-topsis. Mobile Networks and Applications. 2020 Oct;25:1816-32.

[13] Sefati SS, Halunga S. Data forwarding to Fog with guaranteed fault tolerance in Internet of Things (IoT). In2022 14th International Conference on Communications (COMM) 2022 Jun 16 (pp. 1-5). IEEE.

[14] Song J, Nang J, Jang J. Design of anomaly detection and visualization tool for IoT blockchain. In2018 International Conference on Computational Science and Computational Intelligence (CSCI) 2018 Dec 12 (pp. 1464-1465). IEEE.

[15] Sefati SS, Abdi M, Ghaffari A. QoS-based routing protocol and load balancing in wireless sensor networks using the markov model and the artificial bee colony algorithm. Peer-to-Peer Networking and Applications. 2023 May;16(3):1499-512.

[16] Sefati SS, Halunga S. Mobile sink assisted data gathering for URLLC in IoT using a fuzzy logic system. In2022 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom) 2022 Jun 6 (pp. 379-384). IEEE.