Edge AI and Blockchain for Privacy-Critical and Data-Sensitive Applications

A. Nawaz[1,2], T. N. Gia[2], J. Peña Queralta[2] and T. Westerlund[2]

[1] Shanghai Key Laboratory of Intelligent Information Processing, Fudan University, China
[2] Turku Intelligent and Embedded Robotic Systems (TIERS), University of Turku, Finland
Emails: [1]{nanum18, hbkan}@fudan.edu.cn, [2]{jopequ, tunggi, tovewe}@utu.fi

***Abstract*—The edge and fog computing paradigms enable more responsive and smarter systems without relying on cloud servers for data processing and storage. This reduces network load as well as latency. Nonetheless, the addition of new layers in the network architecture increases the number of security vulnerabilities. In privacy-critical systems, the appearance of new vulnerabilities is more significant. To cope with this issue, we propose and implement an Ethereum Blockchain based architecture with edge artificial intelligence to analyze data at the edge of the network and keep track of the parties that access the results of the analysis, which are stored in distributed databases.**

***Index Terms*—Blockchain; Edge Computing; AI; E-Health; U-Health; IoT; Internet of Things; Fall Detection; Ubiquitous Health; Ethereum;**

I. Introduction

Users and organizations are becoming increasingly aware of the importance and significance of protecting personal data and online privacy. This is a particularly critical issue in the IoT, where numerous security challenges have been identified by the research community. In recent years, a wide variety of IoT platforms and applications have adopted the use of blockchain technology to mitigate multiple privacy risks and allow secure transactions without the need for a trusted party. Nevertheless, current integrations of blockchain within the IoT have been focusing on securing communication without changing the interaction topology. Exploiting the fog and edge computing paradigms, we propose an extension of the Ethereum blockchain to resource-constrained devices. With our proposed platform, end-devices can negotiate directly with third parties regarding the use of their data. This ensures data owners are always aware of transactions involving their data. In addition, because of the immutable nature of the blockchain, all transactions are recorded and auditable, which further reduces the possibilities of misuse of private data. We have implemented and validated the proposed platform in a real application, demonstrating its potential for integration of IoT devices with scarce computational capabilities. To enhance privacy-critical systems, edge based AI techniques has been implemented to restrict raw data to its producers only. But, this domain still lacks the owner control over their sensitive health data, where owner can process sensitive information by using neural networks and sell statistics to the interested clients. Furthermore, this reduces the network load and the latency of Blockchain transactions [1], [2].

II. Related Work

To make data access policies accessible at each level researchers proposed blockchain based systems integrated with edge computing. By implementing AI at edge nodes further decreased privacy vulnerabilities. Mamoshina. P *et. al* proposed access policies to accelerate the private patients data and implement deep learning algorithms to turns raw data into strong useful information which can be used in bigger perspectives [1]. In [3], Mackey *et. al* proposed blockchain based data privacy control opportunities and challenges which are significant enough in healthcare applications. A similar approach was presented by Peterson *et. al* [4].

III. Ethereum Blockchain with Edge AI

To exclude intermediaries involve in data transactions in edge devices, we define a platform in which the Blockchain paradigm is extended into scarce computing devices. Ethereum blockchain is used as a service platform to run smart contracts to make the system autonomous in therms of its' communication, processing and data dealing. A private ethereum blockchain network is created by creating a genesis file. To add every device, a pair of private and public key is generated which will be used as a identifier of a device.

In our proposed system, all resource constrained sensor nodes are directly connected to and rely on the edge gateways which are often implemented by powerful single board computers able to work as miner nodes to store, analyze and aggregate raw data. Miner nodes can run neural networks to process the raw data received from sensor nodes. With a predefined time interval, edge nodes process the raw data, and save this processed information into a new data block by creating a unique hash. This data block consists of two parts, header and body. The body apart contains processed information and header part consists of general characteristics about the processed information. This includes hash of previous block, time stamp, raw data definition and the type of data, which can be further use for combining heterogeneous data at bigger level for the sake of intelligent systems. To protect the hash of data block, symmetric cryptography is used. After encryption, the data blocks are saved on a blockchain cloud and key is only hold by the end-device. Which will be later used by a client to decrypt the desired data. Moreover, every access to the data will be recorded. The proposed architecture is illustrated in Figure 1, which is composed of four layers.

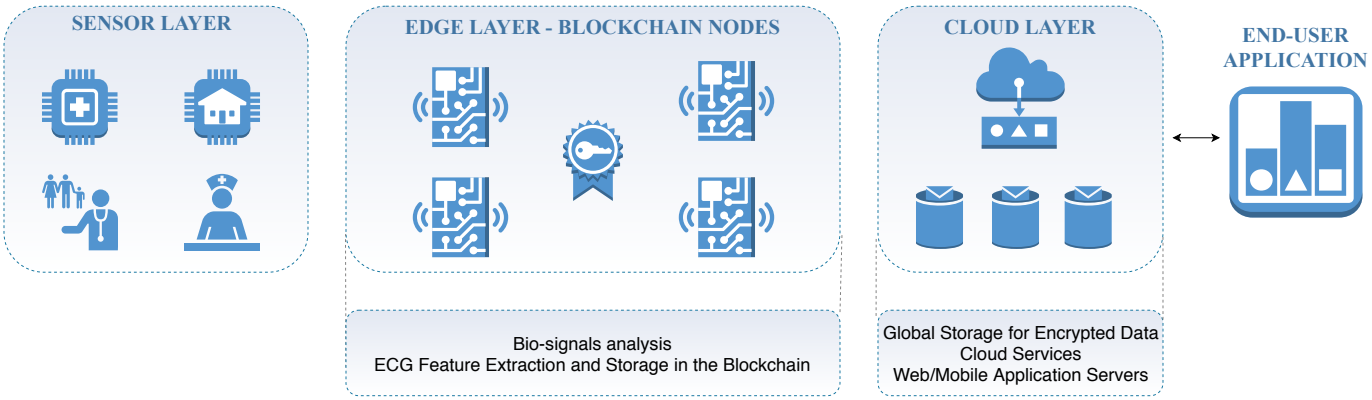
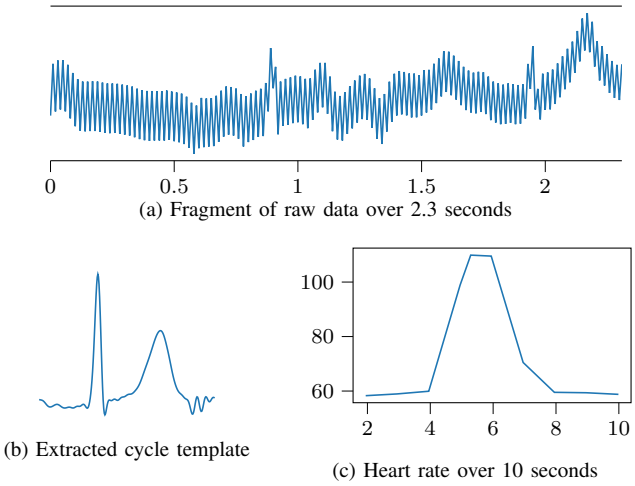


Fig. 1. Proposed System Architecture



(a) Fragment of raw data over 2.3 seconds

(b) Extracted cycle template

(c) Heart rate over 10 seconds

Fig. 2. Results of the data analysis at the edge gateway.

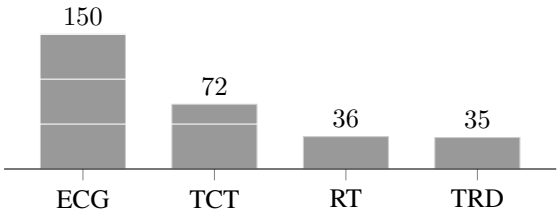


Fig. 3. Execution time of the different processes (ms).

IV. Experiment and Results

The raw ECG data collected from a healthy 30 year-old male person is shown in Figure 2. The data is sent to a smart Edge-assisted gateway which extracts different ECG features such as heart rate [5]. We have utilized a Raspberry Pi model 3 as the edge gateway, which in turn runs a node of the Ethereum Blockchain. In order to test the feasibility of the proposed model, we accumulate data for 10 seconds and then analyze it. The data analysis requires around 150ms for the feature extraction. Then, the results are encrypted and stored in a distributed storage solution. The metadata is stored in the blockchain. Figure 3 shows the execution time of the analysis process (ECG), a data retrieval transaction (TRD), a transaction confirmation (TCT) and the response time (RT). In total, the system needs around 300ms to process one batch of data, which runs every 10 seconds. Therefore, one gateway could support up to 20 or 30 end-devices with the proposed architecture.

V. Conclusion and Future Work

Integrating Blockchain with Edge computing opens new paradigms in privacy-critical and data-sensitive applications. Our proposed architecture, combining a distributed ledger with AI at the edge, creates secure database of processed information which can only be used with the permission of its owner. By Edge AI we refer to local decision making and data processing at the edge computing layer. End devices can directly control all the processing, analyzing and sharing of their data by updating their policies via ethereum smart contracts. Implementing AI at edge nodes reduces resource consumption like bandwidth required to upload data to blockchain cloud as well as local storage. This data analysis step also increases privacy by storing only processed information rather than raw data.

In future work, we will analyze the scalability of the proposed approach and alternative applications and experiment with the integration of more complex deep learning algorithms. We will study the utilization of Ethereum 2 for more scalable systems.

References

[1] P. Mamoshina *et al.* Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare. *Oncotarget*, 9(5):5665, 2018.

[2] J. Peña Queralta *et al.* Edge-AI in LoRa-based healthcare monitoring: A case study on fall detection system with LSTM Recurrent Neural Networks. In *42nd TSP*, 2019.

[3] T. K. Mackey *et al.* 'fit-for-purpose?'–challenges and opportunities for applications of blockchain technology in the future of healthcare. *BMC medicine*, 17(1):68, 2019.

[4] K. Peterson *et al.* A blockchain-based approach to health information exchange networks. In *NIST W. Blockchain Healthcare*, 2016.

[5] C. Carreiras *et al.* BioSPPy: Biosignal processing in Python, 2015–. [Online; accessed Aug. 2019].