








Artificial Intelligence at the Edge in the Blockchain of Things

Tuan Nguyen Gia¹ , Anum Nawaz^{1,2} , Jorge Peña Querata¹ ,
Hannu Tenhunen¹ , and Tomi Westerlund¹ 

¹ Turku Intelligent Embedded and Robotic Systems (TIERS) Group,
Department of Future Technologies, University of Turku, Turku, Finland
{tunggi,jopequ,hatenhu,tovewe}@utu.fi

² Shanghai Key Laboratory of Intelligent Information Processing,
School of Computer Science, Fudan University, Shanghai, China
nanum18@fudan.edu.cn
<https://tiers.fi>

Abstract. Traditional cloud-centric architectures for Internet-of-Things applications are being replaced by distributed approaches. The Edge and Fog computing paradigms crystallize the concept of moving computation towards the edge of the network, closer to where the data originates. This has important benefits in terms of energy efficiency, network load optimization and latency control. The combination of these paradigms with embedded artificial intelligence in edge devices, or Edge AI, enables further improvements. In turn, the development of blockchain technology and distributed architectures for peer-to-peer communication and trade allows for higher levels of security. This can have a significant impact on data-sensitive and mission-critical applications in the IoT. In this paper, we discuss the potential of an Edge AI capable system architecture for the Blockchain of Things. We show how this architecture can be utilized in health monitoring applications. Furthermore, by analyzing raw data directly at the edge layer, we inherently avoid the possibility of breaches of sensitive information, as raw data is never stored nor transferred outside of the local network.

Keywords: Blockchain · Edge computing · AI · Edge AI · E-health · U-health · IoT · Internet of Things · ECG monitoring · ECG feature extraction · Ubiquitous health · Ethereum

1 Introduction

With an increasing ubiquity of connected devices penetrating smart homes, smart cities, smart factories or smart farms, the Internet of Things (IoT) is generating vast amounts of data [1, 2]. However, many challenges related to IoT data ownership, security, privacy, and information sharing still remain [3–6]. The increasing integration of third-party services into IoT applications further

increases the risk of security vulnerabilities and cyber attacks [7]. Even with the state-of-the-art encryption methods, the IoT presents a non-negligible threat to users' privacy and personal data security [8]. While the IoT was born with the boom in cloud computing, in recent years distributed computing approaches are extending its potential [9–16]. The edge and fog computing paradigms aim at migrating computational load towards the edge of the network. Data is processed at the local network level or radio access point station and only important information is transmitted over the network. For example, raw ECG data can be processed at a smart gateway for extracting important ECG features such as heart rate, P and T waves. Depending on the applications, raw data or processed data is stored at distributed edge storage. Edge approaches allow for reduced latency and more efficient use of both network and computational resources, but they also raise additional security considerations and requirements [17].

Blockchain technology has seen increasing penetration in multiple technological areas in the last decade [18], since its first introduction as part of the Bitcoin stack [19]. A blockchain platform can be seen a public and distributed digital data ledger that allows nodes to record proof of integrity and is unalterable a posteriori. Blockchain enables a decentralized manner of sharing data, and an immutable record of transactions, among other benefits. Compared to a centralized infrastructure, such as most cloud-based IoT Systems, blockchain technology has the advantage of allowing end-users or devices to exchange information, data and their assets directly without any intermediate third parties involved in the process while securing data integrity [20]. With these advantages, blockchain can be a suitable candidate to deal with some existing security challenges in many applications [21]. For instance, blockchain can be leveraged as a trading platform between data producers (i.e., the end-devices in an IoT system or the edge gateway where sensor node data is being analyzed and processed), and data consumers or (i.e., third-party applications or end-user applications) [22].

The integration of blockchain technology into the IoT has drawn growing attention of the research community in recent years. Significant efforts have been devoted to propose secured approaches which utilize blockchain technology to secure M2M transactions in the IoT [23]. An important part of the works to date is focused on either secure access policies, such as the direct connection between end-users and smart home appliances [24], or secure machine-to-machine communication [25]. Although these approaches can indeed provide high levels of security to IoT platforms [26], their integration within edge-assisted remote and real-time monitoring applications is not deeply investigated in those works.

In this paper, we present an architecture for the Blockchain of Things that integrates artificial intelligence at the edge (Edge AI) algorithms for efficient and secure information management and privacy protection in healthcare applications. The presented system architecture extends our previous work [27], and it is illustrated in Fig. 1. We also discuss further the potential of this application in various fields. The proposed architecture secures IoT data integrity with a distributed platform based on the Ethereum blockchain and utilizes Edge AI for computational offloading at the fog and edge layer. Integrating fog and

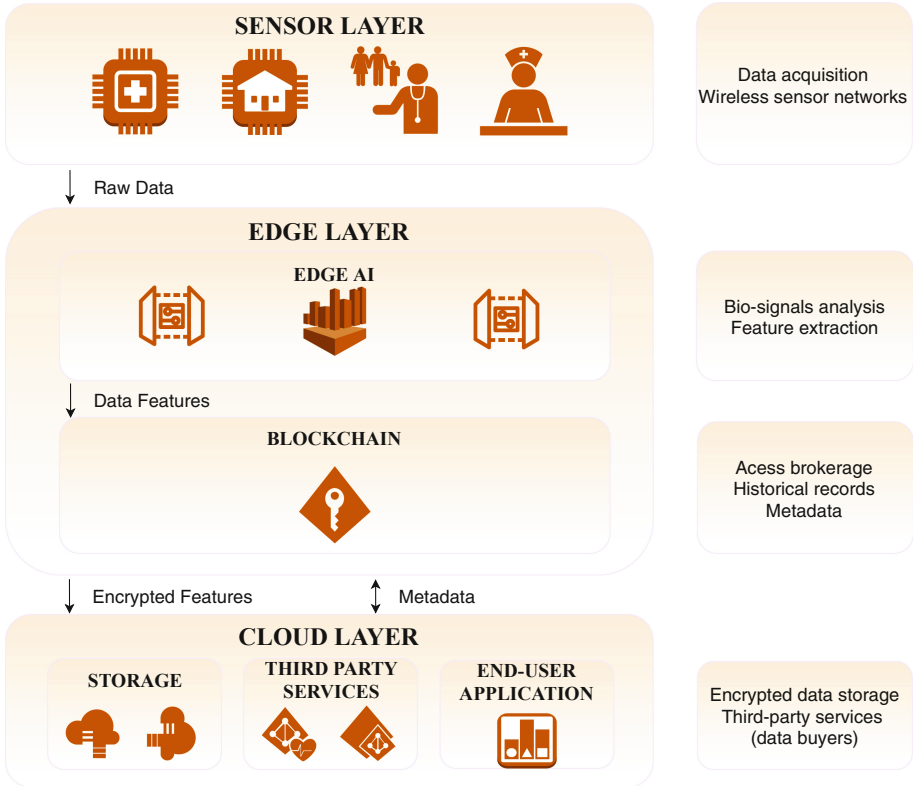


Fig. 1. Proposed system architecture

edge computing creates new opportunities for enhanced peer-to-peer security and authorized access [28,29].

The rest of this paper is organized as follows. Section 2 overviews previous works in the use of blockchain technology in the IoT, the Edge AI paradigm and the use of blockchain for healthcare applications. Section 3 then introduces the system architecture, and outlines the benefits of integrating Edge AI with blockchain for different applications in the IoT. Section 4 presents the experimental data and results. Finally, Sect. 5 concludes the work and lays out future work directions.

2 Related Work

In the healthcare IoT domain, it is often recommended that patients should have the ability to access their own health data. Nonetheless, the data should be consistent, protected and unaltered over time by any third parties or patients themselves [30,31]. Therefore, it is necessary to have a high level of security

methods which ensure that data transmitted over a network is secure and available to authorized parties, in addition to having an integrity check that ensures immutability of the data. Many efforts have been devoted to propose blockchain-based methods to improve security, transaction speed, and avoid fraud control in healthcare.

In [32], the authors introduced and discussed different access policies to protect the privacy of private patient's data. In addition, the authors implemented deep learning algorithms to extract useful information from private raw data. Although the proposed method and its algorithms focus on healthcare applications, they can be applied in different scenarios including cases in larger perspectives.

In [33], the authors presented a blockchain-based approach for sharing patient data within a network. In addition, the authors introduced a consensus algorithm for enabling data interoperability. Different measurements of security on blockchain were carried out and the authors claimed that the blockchain-based method is a promising solution for avoiding or overcoming problems in sharing private health data.

In [34], the authors introduced a blockchain-based method for proffering a proof of predefined endpoints in clinical trials. They claimed that applying blockchain methods can provide a high level of reliability while keeping costs low.

In [35], the authors introduced a framework which has a modified traditional blockchain method for suiting to IoT applications. The proposed method is suitable for resource-constrained devices while it maintains a high level of privacy and security. The framework ensures that transactions over a blockchain network are more anonymous and secure.

In [36], Simic *et al.* showed that it is feasible to apply blockchain into healthcare IoT systems to protect data transmitted over a network. The authors have examined several possibilities of utilizing smart contracts for healthcare IoT systems. They claimed that a combination of blockchain and IoT can benefit different distributed applications.

In [37], Pham *et al.* presented a remote health monitoring system utilizing blockchain. In this system, bio-signal sensor nodes collect and filter patient data. The useful information extracted from the collected data is written into blockchain. In case of abnormalities, the extracted information is written immediately to blockchain and a push notification is triggered to inform medical doctors.

3 Protecting Data Privacy with the Ethereum Blockchain

As compared to the original blockchain platform developed for the bitcoin by Satoshi Nakamoto [19], the Ethereum platform provides the Ethereum Virtual Machine (EVM) which is fully autonomous in terms of its system execution by using smart contracts. Smart contracts are scripts with predefined terms and conditions for system transactions. This peer-to-peer (P2P) distributed ledger

relies on its miner nodes. Miner nodes act as validator nodes for every new transaction block, which are created within certain time intervals. In general, a single transaction block is a combination of a header block and a data block. The data block stores the hash of the processed and analyzed data, while the header contains the hash of previous and current blocks, metadata, timestamp and a short characterization of the data. If another user or a third party service wants to access or exchange data, the header data characterization description can be utilized to see the details of the data block before the transaction is carried out. The data itself is stored encrypted in a cloud storage solution or in the device itself if the capacity is enough.

The proposed system architecture is illustrated in Fig. 1 and it consists of three layers. First, the data generation layer, which consists of sensors and actuators without any computational layer. These sensors and actuators depend on mining nodes which will collect data from these devices. Sensor and actuators merely communicate with one miner node which can be used as a gateway to transfer their data to other gateways or cloud servers. Bluetooth low energy (BLE) or Wi-Fi is often used this layer. BLE uses less energy whilst Wi-Fi can transmit a larger data packet size and offer higher bandwidth. Second, the network layer, where P2P networking is used in this private ethereum network for communication and data transfer. The distributed ledger topologies are defined on this layer. Different topologies like side chains, shard chains, off-chains can be used to handle scarce computing-devices issues and scalability. Smart contracts or scripts run to handle all the processes in a network. Finally, the third layer is the application layer. Smart applications of the IoT consists of a wide range of use-cases like smart homes, smart industries, digital medical and many more. To access these systems, end-users, third parties or control centers need to join the network first and then request data via the ethereum network.

3.1 Application Areas

In this section, we give an overview of potential applications for the proposed architecture. We outline the benefits and trade-offs of integrating our proposed platform in different IoT domains. We cover the areas of smart homes, smart cities, industrial applications, connected vehicles with vehicle-to-vehicle (V2V) and vehicle-to-everything (V2X) communication, and ubiquitous health.

A common problem of IoT devices in all application areas is their security vulnerabilities in terms of (1) third-party access and control, (2) unauthorized use of data, and (3) leakage of raw data. While previous works have studied the problem of protecting access to these devices by integrating blockchain technology extensively, we will focus on the benefits of the proposed for ensuring that data from sensor nodes is only accessed by authorized third parties, and that raw data is never made available to these parties through processing at the local network level and before inclusion in the blockchain. Furthermore, the blockchain provides an immutable record of all data requests from third parties.

Smart Home IoT Providers

In the smart home domain, an increasing number of industrial players are introducing a variety of commodities, from voice assistants to smart fridges. However, these are not exempt from security vulnerabilities [38], and many of them suppose a serious threat to privacy in users' homes. Previous works have been focusing on using blockchain for securing access and control of smart home appliances. This can significantly reduce the risk of having a spy inside our homes [39]. However, while communication between third-party services is secured, the use of data gathered by these devices is still being controlled by third-parties.

A smart gateway, which can replace a traditional home Wi-Fi router, serves as a bridge between sensor nodes and cloud storage or third-party applications, and at the same time the smart gateway can be utilized to deploy deep learning analysis and other AI processing which cannot run directly on resource-constrained devices. Moreover, because the processed data is only stored locally or encrypted in cloud storage, all data access requests are stored in the blockchain and therefore access to data is not managed by an external party but by smart gateways directly.

Cybersecurity in Open Smart Cities

The concept of Smart City mostly relies on IoT. A city is considered to be *smart* when it uses large amounts of IoT sensor data to efficiently improve the management of its assets and resources [40]. Another key aspect of smart cities is openness. By making public all or part of the IoT data that is gathered, city administrators can engage citizens, local business and large enterprises equally to develop new products and services based on the data. This benefits both the city management team and the involved parties, with a positive effect on the city's economy. In this case, however, it is essential to have a proper methodology for both sharing data with third parties and ensuring that public datasets are not misused.

With the implementation of the proposed architecture, administrators can have full control and monitor the access of third parties of this data. Moreover, transaction fees and data prices in the ethereum blockchain within the proposed solution can be used to naturally control the amount of data that each external user is accessing. In summary, our proposed solution not only provides a secure and safe way of distributing IoT data gathered around the city to external users or developers, but it also provides a base for edge computing and local network analysis and processing. By managing to which level the data is processed in edge gateways, which information is processed in the gateways, and which information or raw data is available to external applications.

Modular Smart Factories in Industry 4.0

The fourth industrial revolution, or Industry 4.0, has promised to develop more agile, modular and smart manufacturing environments where traditional production lines are replaced by automated and intelligent lines in which individual products can be customized *on the fly* [41]. The process towards Industry 4.0

requires the integration of the IoT in industrial environments and the installation of IoT sensor suites and actuators. This will allow managers to gather vast amounts of data and be able to adjust the manufacturing process dynamically to improve its efficiency.

Although autonomous machines and robots are heavily used in smart factories, they cannot replace humans completely. In some parts of a production chain, tight cooperation between machines and humans is unavoidable. Therefore, it is required that smart factories must guarantee a high safety level for humans working with autonomous machines. A method for enhancing situational awareness via intercommunication between everything can be applied in smart factories to address the target. In detail, a machine such as co-robot communicates and obtains useful information from other machines or even humans. For instance, a machine in a room can get a position and gesture of engineering who is walking in an adjacent room and is likely to come close to it. Based on both the received information and the data collected by the machine itself, it is able to forecast potential safety-critical situations and react in real-time to avoid accidents. In such a system, latency and security are essential because a piece of incorrect information provided by the third party or delayed information can cause a serious consequence. Therefore, smart factories need an advanced secured architecture which can guarantee a trusted intercommunication between machines and human with low latency.

Internet of Vehicles, V2V, and V2X

Nowadays, the number of connected vehicles is increasing significantly due to their benefits such as improving energy efficiency, reducing travelling time, or avoiding car accidents. The concept of connected vehicles often refers to a number of communication protocols used to connect the driver with other objects. For instance, communication in connected vehicles can be categorized into a vehicle to infrastructure (V2I), vehicle to vehicle (V2V), vehicle to Cloud (V2C), vehicle to pedestrian (V2P) and, in general, vehicle to everything (V2X) communication. In these scenarios, security is essential because incorrect or modified data introduced in the system by untrusted third parties can cause serious consequences such as a car accident or even death. Conventional security methods which need a central control system may not be completely suitable for some of the connected vehicles because those methods can cause an increase in communication latency. In such vehicle systems, real-time data and reaction are required. The proposed solution is a potential candidate for such real-time connected vehicle systems as it can provide high levels of security while the latency does not increase. With the proposed architecture, data related to other vehicles on a street can be exchanged directly with a connected vehicle through edge gateways in the near infrastructure. Moreover, the Edge AI opens multiple possibilities for computational offloading [42, 43]. The benefits of our proposed architecture are in the control of the use of private vehicle data by third parties. In the V2X scenario, these can be other vehicles (V2V) or infrastructure around the road (V2I) (Fig. 2).



Fig. 2. Sensor node

Ubiquitous Health

Privacy and private health data must be carefully protected because leaked information can cause serious consequences. For instance, the leakage information such as health status can be used for hijacking purposes or spreading false rumors which causes money and mental damages. It is required that remote and real-time health monitoring systems must ensure a high level of security. Nonetheless, there are still many challenges of security issues in these systems. Blockchain can play an important role in improving a security level in these systems [27]. By combining blockchain with artificial intelligence at the edge of the network, a system can provide end-to-end protection to users' privacy. First, sensitive raw data is processed at the local network level, and therefore the risk of raw data being leaked is eliminated. With the blockchain utilized to manage an access to processed data and features, end-users can have full control over their data while allowing third-party applications to have access only the information that has been processed already.

4 Experiment and Results

In order to test the feasibility of the proposed architecture, and the possibilities for deployment and real-time execution, we have targeted a use case of ECG feature extraction and arrhythmia detection with convolutional neural networks (CNN). We have used a complete remote health monitoring IoT-based system utilizing blockchain and edge/fog computing. However, in this paper, we just focuses on edge gateways which have been used for deploying the advanced algorithms such as ECG feature extraction and arrhythmia detection with CNN. Other parts of the system have been discussed in detail in our previous papers [12, 44, 45].

4.1 Sensor Node

In this paper, ECG is collected by our multi-channel ECG sensor node which will be described in detail in another work. The sensor node is able to collect

Table 1. Loading time of the different Arrhythmia classification requirements

	Execution time
Loading numerical libraries	960 ms
Loading tensorflow and keras	1478 ms
Loading trained model	6683 ms
ECG feature extraction	150 ms
Arrhythmia classification	849 ms

Table 2. Blockchain transaction average execution times

	Average execution time
Ethereum transaction request	17 ms
New data block creation	10 s

16-channel ECG signals with high resolutions (i.e., each channel can collect from 125 samples/s to 1000 samples/s). Then, depending on the requirements of each application, the data can be pre-processed and kept intact before being sent to a smart Edge gateway via BLE or Wi-Fi. In this paper, raw ECG data is collected from the sensor node with a sampling rate of 250 samples/s per channel and sent to a smart Edge gateway via Wi-Fi. The collected data is not processed at the sensor node because it is difficult or even not feasible to run heavy computation methods (e.g., ECG feature extraction based on wavelet transform) at the sensor node [46–48]. Instead the data will be processed at the Edge gateway which is capable of running heavy computations while fulfilling latency requirements [49]. The data rate of 250 samples/s can fulfill the requirements of common ECG data quality standards [50]. In general, BLE is preferred over Wi-Fi because BLE consumes much less energy than Wi-Fi for a similar transmissions. However, BLE cannot be chosen for this case because BLE cannot support this large data rate (i.e., about 3 Mbps for up to 12 channels in each sensor node) [51].

4.2 Gateway

The edge gateways used in our system are Raspberry Pi 3B+ single-board computer (1.4 GHz quad-core processor, 1 GB SRAM, BLE, Wi-Fi). The operating system running at the gateway is Ubuntu. The gateway is able to store different data and information such as parameters used for algorithms and temporary health data. The parameters are often kept intact and they are only modified by a system administrator. The gateway can reserve 20 GB for storing temporary health data. Raw data is not stored but only the extracted features. If the storage is near its full capacity, then part of the data is encrypted and transferred to cloud-based storage solutions. All the services (e.g., ECG feature extraction) run on the gateway. In our experiments, the Pi runs ECG feature extraction adapted from [52], while a deep learning based arrhythmia classification model

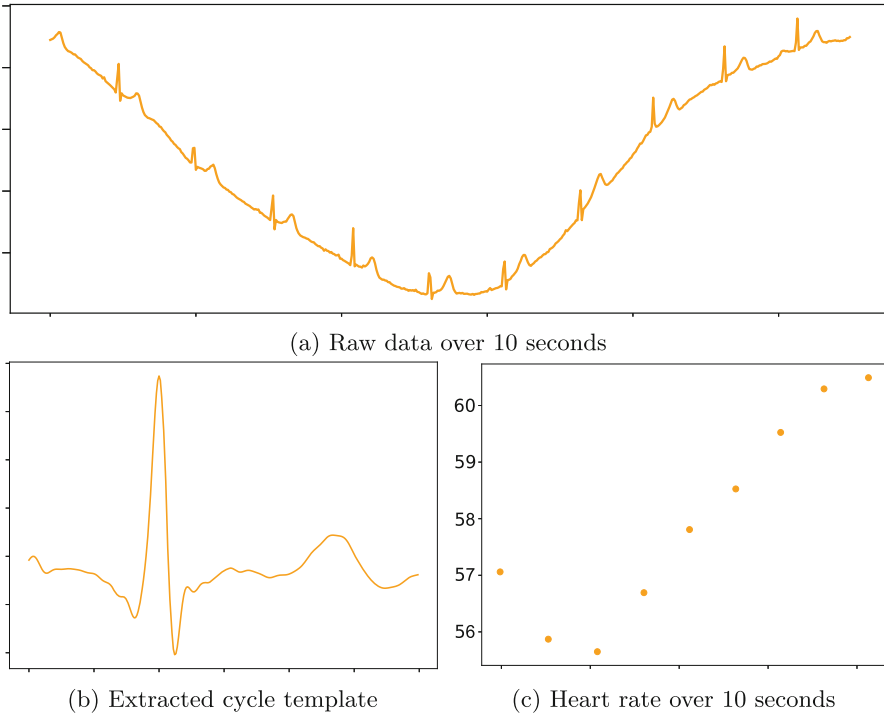


Fig. 3. Results of the data analysis at the edge gateway.

adapted from [53] is deployed in the as well. The Pi was used in order to prove the viability and effectiveness of the proposed architecture. If more computational resources are required, then this can be replaced by any other hardware capable of running Ubuntu.

4.3 Performance

To initialize the system, a private ethereum network is created, generating authority and transaction accounts. The first step is to configure a new genesis file to build the first block of the custom ethereum network. Smart contracts were written in solidity and tested by using Remix IDE. We have analyzed the execution times of the feature extraction, arrhythmia detection and blockchain requests in order to assess the possibilities of real-time operation. The execution times of the different processes are shown in Tables 1 and 2. The feature extraction and arrhythmia classification processes deployed in this use case are single-threaded and therefore executed within a single core. As the Raspberry Pi 3B+ has 4 cores, it is possible to concurrently execute the analysis of two sensor nodes in parallel together with other background processes. The analysis of ECG data is made in batches of 10 s, where an average ECG cycle template is extracted and the heart rate and other features are calculated.

An example of the raw and processed data is shown in Fig. 3. Then, the template is utilized for arrhythmia classification.

The loading times required for loading numerical libraries, the deep learning libraries Tensorflow and Keras, and the trained model are shown in Table 1. Taking these into account, we deploy the model in the edge gateway in a way that the required libraries and the deep learning model are only loaded every time the gateway is rebooted. Transaction requests time in the ethereum network was 17 ms as average while using public Wi-Fi. Miner nodes take 10 s as average to create a new data block.

In summary, since the analysis is carried out every 10 s, a single Raspberry Pi 3B+ board is able to handle multiple sensor nodes connected via Wi-Fi or Bluetooth. We can safely assume that around 8 sensor nodes can be handled in real-time without reaching the maximum level of performance and therefore allowing for uncertainties in the measurements.

After data processing, the extracted features are encrypted with AES-256 [54,55] and stored in a third party storage solution. A custom distributed storage solution can be employed instead if tighter control of the data storage is required. Then, metadata including device ID and type of data are stored in the blockchain through the execution of a series of smart contracts.

5 Conclusion and Future Work

We have utilized a blockchain-based architecture for managing data security and integrity in IoT applications, and improved it by integrating Edge AI techniques to enhance the applications' security and protect users' privacy further. This is of particular interest for mission-critical and data-sensitive applications such as health monitoring applications in the IoT. We have implemented our proposed approach using ECG sensor nodes and a Raspberry Pi Model 3B+ as an edge gateway. The gateway ran a full ethereum node and processed ECG data in real-time with feature extraction and arrhythmia detection algorithms deployed. We show that real-time computation with arrhythmia classification is possible with multiple nodes, and the analysis part utilizes more computation resources than a typical ethereum deployment.

In future work, we will further integrate how the AI algorithms are executed together with the smart contracts in an ethereum network. In addition, we will extend the current system to a larger number of applications in the domain of ubiquitous health monitoring and others.

References

1. Al-Fuqaha, A., et al.: Internet of Things: a survey on enabling technologies, protocols, and applications. *IEEE Commun. Surv. Tutor.* **17**(4), 2347–2376 (2015)
2. Gia, T.N., et al.: Edge AI in smart farming IoT: CNNs at the edge and fog computing with lora. In: *IEEE AFRICON-2019* (2019)

3. Moosavi, S.R., et al.: Session resumption-based end-to-end security for healthcare Internet-of-Things. In: 2015 IEEE CIT, pp. 581–588. IEEE (2015)
4. Gubbi, J., et al.: Internet of Things (IoT): a vision, architectural elements, and future directions. *Future Gener. Comput. Syst.* **29**(7), 1645–1660 (2013)
5. Moosavi, S.R., et al.: Sea: a secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways. *Procedia Comput. Sci.* **52**, 452–459 (2015)
6. Moosavi, S.R., et al.: End-to-end security scheme for mobility enabled healthcare Internet of Things. *Future Gener. Comput. Syst.* **64**, 108–124 (2016)
7. Fernandes, E., et al.: Security analysis of emerging smart home applications. In: 2016 IEEE Symposium on Security and Privacy (SP), pp. 636–654 (May 2016)
8. Aphorpe, N., Reisman, D., Feamster, N.: A smart home is no castle: privacy vulnerabilities of encrypted IoT traffic. arXiv preprint [arXiv:1705.06805](https://arxiv.org/abs/1705.06805) (2017)
9. Ali, M., et al.: Intelligent autonomous elderly patient home monitoring system. In: ICC 2019–2019 IEEE International Conference on Communications (ICC), pp. 1–6. IEEE (2019)
10. Gia, T.N., et al.: Edge AI in smart farming IoT: CNNs at the edge and fog computing with lora (2019)
11. Dastjerdi, A.V., Buyya, R.: Fog computing: helping the Internet of Things realize its potential. *Computer* **49**(8), 112–116 (2016)
12. Gia, T.N., et al.: Energy efficient fog-assisted iot system for monitoring diabetic patients with cardiovascular disease. *Future Gener. Comput. Syst.* **93**, 198–211 (2019)
13. Ali, M., et al.: Autonomous patient/home health monitoring powered by energy harvesting. In: GLOBECOM 2017–2017 IEEE Global Communications Conference, pp. 1–7. IEEE (2017)
14. Sarker, V.K., et al.: A survey on lora for IoT: integrating edge computing. In: 2019 Fourth International Conference on Fog and Mobile Edge Computing (FMEC), pp. 295–300. IEEE (2019)
15. Queraltà, J.P., et al.: Edge-AI in lora-based health monitoring: fall detection system with fog computing and LSTM recurrent neural networks. In: 2019 42nd International Conference on Telecommunications and Signal Processing (TSP), pp. 601–604. IEEE (2019)
16. Metwaly, A., et al.: Edge computing with embedded AI: thermal image analysis for occupancy estimation in intelligent buildings. In: INTelligent Embedded Systems Architectures and Applications, INTESA@ESWEEK 2019. ACM (2019)
17. Roman, R., Lopez, J., Mambo, M.: Mobile edge computing, fog et al.: a survey and analysis of security threats and challenges. *Future Gener. Comput. Syst.* **78**, 680–698 (2018)
18. Conoscenti, M., Vetró, A., De Martin, J.C.: Blockchain for the Internet of Things: a systematic literature review. In: 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), pp. 1–6 (November 2016)
19. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system. White Paper (2008)
20. Shafagh, H., et al.: Towards blockchain-based auditable storage and sharing of IoT data. In: Proceedings of the 2017 on Cloud Computing Security Workshop, CCSW 2017, pp. 45–50. ACM, New York (2017)
21. Huh, S., Cho, S., Kim, S.: Managing IoT devices using blockchain platform. In: 2017 19th International Conference on Advanced Communication Technology (ICACT), pp. 464–467. IEEE (2017)
22. Novo, O.: Blockchain meets IoT: an architecture for scalable access management in IoT. *IEEE Internet Things J.* **5**(2), 1184–1195 (2018)

23. Tang, B., et al.: A hierarchical distributed fog computing architecture for big data analysis in smart cities. In: Proceedings of the ASE BigData & SocialInformatics 2015, p. 28. ACM (2015)
24. Dorri, A., et al.: Blockchain for IoT security and privacy: the case study of a smart home. In: 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), pp. 618–623. IEEE (2017)
25. Christidis, K., Devetsikiotis, M.: Blockchains and smart contracts for the Internet of Things. *IEEE Access* **4**, 2292–2303 (2016)
26. Kshetri, N.: Can blockchain strengthen the Internet of Things? *IT Prof.* **19**(4), 68–72 (2017)
27. Nawaz, A., et al.: Edge AI and blockchain for privacy-critical and data-sensitive applications. In: The 12th International Conference on Mobile Computing and Ubiquitous Networking (ICMU) (2019)
28. Ndibanje, B., Lee, H.-J., Lee, S.-G.: Security analysis and improvements of authentication and access control in the Internet of Things. *Sensors* **14**(8), 14786–14805 (2014)
29. Bahga, A., Madiseti, V.: *Internet of Things: A Hands-on Approach*. VPT, New York (2014)
30. Li, M., Yu, S., Ren, K., Lou, W.: Securing personal health records in cloud computing: patient-centric and fine-grained data access control in multi-owner settings. In: Jajodia, S., Zhou, J. (eds.) *SecureComm 2010*. LNICT, vol. 50, pp. 89–106. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-16161-2_6
31. Mandl, K.D., et al.: Public standards and patients' control: how to keepelectronic medical records accessible but private. *BMJ* **322**(7281), 283–287 (2001)
32. Mamoshina, P., et al.: Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare. *Oncotarget* **9**(5), 5665 (2018)
33. Peterson, K., et al.: A blockchain-based approach to health information exchange networks. In: Proceedings of NIST Workshop Blockchain Healthcare, vol. 1, pp. 1–10 (2016)
34. Irving, G., Holden, J.: How blockchain-timestamped protocols could improve the trustworthiness of medical science. *F1000Research* **5**, 22 (2016)
35. Dwivedi, A.D., et al.: A decentralized privacy-preserving healthcare blockchain for IoT. *Sensors* **19**(2), 326 (2019)
36. Simić, M., et al.: A case study IoT and blockchain powered healthcare. In: International Conference on Engineering and Technology (ICET-2017) (June 2017)
37. Pham, H.L., Tran, T.H., Nakashima, Y.: A secure remote healthcare system for hospital using blockchain smart contract. In: 2018 IEEE Globecom Workshops (GC Wkshps), pp. 1–6. IEEE (2018)
38. Apthorpe, N., et al.: Spying on the smart home: privacy attacks and defenses on encrypted IoT traffic. arXiv preprint [arXiv:1708.05044](https://arxiv.org/abs/1708.05044) (2017)
39. Hernandez, G., et al.: Smart nest thermostat: a smart spy in your home. *Black Hat USA*, pp. 1–8 (2014)
40. Albino, V., Berardi, U., Dangelico, R.M.: Smart cities: definitions, dimensions, performance, and initiatives. *J. Urban Technol.* **22**(1), 3–21 (2015)
41. Lasi, H., et al.: Industry 4.0. *Bus. Inf. Syst. Eng.* **6**(4), 239–242 (2014)
42. Qingqing, L., et al.: Edge computing for mobile robots: multi-robot feature-based lidar odometry with FPGAs. In: The 12th International Conference on Mobile Computing and Ubiquitous Networking (ICMU) (2019)

43. Qingqing, L., et al.: Visual odometry offloading in Internet of vehicles with compression at the edge of the network. In: The 12th International Conference on Mobile Computing and Ubiquitous Networking (ICMU) (2019)
44. Gia, T.N., et al.: Fog computing approach for mobility support in Internet-of-Things systems. *IEEE Access* **6**, 36064–36082 (2018)
45. Jiang, M., et al.: IoT-based remote facial expression monitoring system with sEMG signal. In: 2016 IEEE Sensors Applications Symposium (SAS), pp. 1–6. IEEE (2016)
46. Gia, T.N., et al.: Fog computing in healthcare Internet of Things: a case study on ECG feature extraction. In: 2015 IEEE CIT, pp. 356–363. IEEE (2015)
47. Palacios-Enriquez, A., Ponomaryov, V.: Feature extraction based on wavelet transform using ECG signal. In: 2013 International Kharkov Symposium on Physics and Engineering of Microwaves, Millimeter and Submillimeter Waves, pp. 632–634. IEEE (2013)
48. Gia, T.N., et al.: Fog computing in body sensor networks: an energy efficient approach. In: Proceedings of IEEE International Body Sensor Networks Conference (BSN), pp. 1–7 (2015)
49. Gia, T.N., et al.: Customizing 6LoWPAN networks towards Internet-of-Things based ubiquitous healthcare systems. In: 2014 Norchip, pp. 1–6. IEEE (2014)
50. Steinberg, C., et al.: A novel wearable device for continuous ambulatory ECG recording: proof of concept and assessment of signal quality. *Biosensors* **9**(1), 17 (2019)
51. Sarker, V.K., et al.: Portable multipurpose bio-signal acquisition and wireless streaming device for wearables. In: 2017 IEEE Sensors Applications Symposium (SAS), pp. 1–6. IEEE (2017)
52. Carreiras, C., et al.: BioSPPy: biosignal processing in Python, 2015. Accessed Aug 2019
53. Jun, T.J., et al.: ECG arrhythmia classification using a 2-D convolutional neural network. arXiv preprint [arXiv:1804.06812](https://arxiv.org/abs/1804.06812) (2018)
54. Dhaou, I.B., et al.: Low-latency hardware architecture for cipher-based message authentication code. In: 2017 IEEE International Symposium on Circuits and Systems (ISCAS), pp. 1–4. IEEE (2017)
55. Gia, T.N., et al.: Low-cost fog-assisted health-care IoT system with energy-efficient sensor nodes. In: 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC), pp. 1765–1770. IEEE (2017)