Addressing Privacy and Security in Connected Health with Fog Computing

Conference Paper · September 2019

DOI: 10.1145/3342428.3342654

4 authors:

Ace Dimitrievski
Ss. Cyril and Methodius University in Skopje
19 PUBLICATIONS **132** CITATIONS
SEE PROFILE

Eftim Zdravevski
Ss. Cyril and Methodius University in Skopje
157 PUBLICATIONS **1,433** CITATIONS
SEE PROFILE

Petre Lameski
Ss. Cyril and Methodius University in Skopje
102 PUBLICATIONS **929** CITATIONS
SEE PROFILE

Vladimir Trajkovik
Ss. Cyril and Methodius University in Skopje
275 PUBLICATIONS **1,426** CITATIONS
SEE PROFILE

Addressing Privacy and Security in Connected Health with Fog Computing

Ace Dimitrievski
Faculty of Computer Science and Engineering
Ss Cyril and Methodius University
Skopje, Macedonia
ace.dimitrievski@gmail.com

Eftim Zdravevski
Faculty of Computer Science and Engineering
Ss Cyril and Methodius University
Skopje, Macedonia
eftim.zdravevski@finki.ukim.mk

Petre Lameski
Faculty of Computer Science and Engineering
Ss Cyril and Methodius University
Skopje, Macedonia
petre.lameski@finki.ukim.mk

Vladimir Trajkovik
Faculty of Computer Science and Engineering
Ss Cyril and Methodius University
Skopje, Macedonia
vladimir.trajkovik@finki.ukim.mk

ABSTRACT

One of the main pillars of connected health is the application of technology to provide healthcare services remotely. Electronic health records are integrated with remote patient monitoring systems using various sensors. However, these ecosystems raise many privacy and security concerns. This paper analyzes and proposes a fog-based solution to address privacy and security challenges in connected health. Privacy protection is investigated for two types of data: less invasive sensors, such as sleep monitor; and highly invasive sensors, such as microphones. In this paper, we show how adding computing resources in the edge can improve privacy and data security, while reducing the computational and bandwidth cost in the cloud.

CCS CONCEPTS

• **Computer systems organization** → **Embedded systems**; *Redundancy*; Robotics; • **Networks** → Network reliability.

KEYWORDS

Fog Computing, Connected Health, Privacy, IoT, AAL

1 INTRODUCTION

Fog computing, first proposed by Cisco [5], adds an extra layer to the cloud computing architecture, but it should not be treated as merely an extension of the cloud. Fog computing has the following characteristics: it spans to adjacent physical locations; supports online analytics; the service is provided by smart, but not very powerful devices; supports various communications networks, and is distributed computing [22]. The goals of the fog computing paradigm are to reduce the data volume and traffic to cloud servers, decrease latency, and improve quality of service (QoS) [3]. Fog computing consists of 3 main components, (a) IoT nodes, (b) fog nodes, and (c) back-end cloud [15].

Fog based IoT can be used in various health care scenarios from a patient monitoring system for ambient assisted living [27] to solutions for patient triage in an emergency after a disaster [25].

GoodTechs '19, September 25–27, 2019, Valencia, Spain
https://doi.org/10.1145/3342428.3342654

While there are benefits to technologies, associated privacy and security issues need to be analyzed to make these systems socially acceptable [17]. Without appropriate security and privacy protections for underlying connected health systems, providers and patients lack trust in the solutions [9]. News about lack of security of IoT devices and unethical practices of some corporations that gather and abuse personal data from owners of connected devices have made consumers wary of the technology and more proactive in protecting personal data [4]. Even when the IoT health care system itself is not compromised, the care receivers can be the victims of overzealous corporations that have questionable use of patient data with potential legal implications [6], as medical data in many countries is protected by law. Such is the case where algorithms were used to deny life-saving health-care to persons with handicap [14], or where an insurance provider abused data collection by a connected medical device for denying coverage to a person with sleep apnea [2].

The research field of cloud computing has received much attention, this exposure has resulted in the cloud being a target of attacks but has also contributed to researchers and companies working hard to develop state of the art security techniques. Considering that fog devices work at the edge of networks, fog faces new security and privacy challenges on top of those inherited from cloud computing [23, 28]. Attack vectors such as man-in-the-middle have the potential to become a typical attack in Fog computing [15, 19].

With these motivations, this paper addresses the privacy and security challenges of IoT-based health care systems and proposes to implement solutions in the fog layer. A summary of related work is presented in the next chapter. Chapter 3 analyses the challenges with two scenarios. The proposed architecture for fog layer processing to address these challenges is discussed in chapter 4. Next, chapter 5 discusses the benefits of the proposed architecture and finally, the paper is concluded in chapter 6.

2 RELATED WORK

A survey of security and privacy issues and corresponding solutions in fog computing is conducted in [28]. The paper highlights privacy issues in data privacy, usage privacy, and location privacy. Some of the mentioned solutions include techniques such as homomorphic

encryption which can be utilized to allow privacy-preserving aggregation at the local gateways; designing a smart way of partitioning the application, so the offloaded resource usages do not disclose privacy information; etc.

In [20], authors provide in-depth security and privacy analysis of some of the most popular freeware mobile health applications. Their findings reveal that the majority of the analyzed applications do not follow well-known practices and guidelines, not even legal restrictions imposed by contemporary data protection regulations, thus jeopardizing the privacy of millions of users.

Another extensive survey of privacy and security challenges in fog computing was presented in [19]. The authors give a summary of state-of-the-art and research challenges. They also make an overview of existing authentication and privacy-preserving schemes for fog computing.

A study of security with an emphasis on data protection and privacy is done by Stutz et al. in [24]. Taking relevant provisions from the European data protection directives and national laws from EU member states, the authors advocate for data economy and data avoidance. Avoiding data collection that is not related to the AAL system objectives, and providing only parts of the data that is relevant to the health care providers, reduces the risks of data exposure.

Analysis of e-health and AAL security mechanisms, with emphasis on the architecture is conducted in [18]. The paper provides an IoT protocol architecture and examines security tools and techniques that can be leveraged as part of the deployment of IoT in e-health and assisted living applications. The authors provide the following considerations for the IoT security challenges: IoT technology is relatively new, less understood than traditional ICT systems; are widely scattered geographically; are widely scattered administratively, where multiple, often heterogeneous, environments, processes, technologies, and security mechanisms exist; they tend to be silos of their own and tend to be vendor-specific; IoT systems tend not to follow an accepted layered architecture; they have limited memory and computing capabilities and consume limited power; IoT endpoints may use different addressing models.

While AAL access gateways can communicate with the cloud utilizing advanced security measurements, at the level of sensors, there are many restrictions in terms of memory, processing power, and hardware capabilities. To address this, Al-Hamadi et al. [1] present a lightweight security protocol to secure the medical information transmitted from the biosensor to the gateway. The security protocol comes with acceptable low computation overhead and hence results in a minimum processing delay.

Another secure system for ECG data transmission based on advanced encryption standard (AES) is proposed at [30]. The System-on-Chip (SoC) for the proposed algorithms was implemented by the authors on the Xilinx ZC702 prototyping board. The achieved hardware implementation results have shown that the proposed AES and ECG identification based system met the real-time requirements.

In [3], the authors discuss the security and privacy issues in IoT and propose a mechanism that employs fog for improved distribution of certificate revocation information among IoT devices.

The authors of [10] use Fog computing to design a face identification and resolution framework that preserves privacy and security. Their experimental results show that the proposed security and privacy preservation scheme only increases a small computation and communication overhead to provide security and privacy preservation for face identification and resolution service.

A light-weight privacy-preserving data aggregation scheme for fog computing-enhanced IoT (LPDA) is presented in [16]. The proposed LPDA is characterized by employing the Chinese Remainder Theorem to aggregate hybrid IoT devices data into one, and use the one-way hash chain to run the source authentication at the network edge to early filter the injected false data.

3 ANALYSIS

In this chapter, we analyze the privacy and security concerns from two types of sensors. In the first scenario, presented in section 3.1, a data is collected from a less invasive sensor to establish the sleeping patterns of a care receiver, such as the time it takes for the person to fall asleep. In the second scenario, discussed in section 3.2, security and privacy implications are analyzed from an always-on microphone(s) placed in the home or the institution where a care receiver resides and whose purpose is to detect presence and number of people and monitor for sound indications of potentially dangerous situations. Both scenarios have apparent privacy and security implications if the confidentiality, integrity, and anonymity of the data is compromised.

3.1 Sleep monitoring sensors

To monitor sleep patterns in Ambient Assisted Living (AAL) scenario, we have conducted the following experiment over 8 hours. Piezoelectric sensors were placed under a mattress, as shown in figure 1. These sensors have a piezoelectric element placed between two plates. The purpose of the plates is to mechanically amplify the movement of a person in bed. The piezoelectric element then generates a charge which is amplified by a charge amplifier circuit using operational amplifiers. The charge is transmitted via a wall connector to the central panel of the AAL lab, shown in figure 2.

In addition to the piezoelectric sensor, an additional PIR sensor module [7], shown in figure 3 is placed above the bed. This module will be able to verify events such as moving in bed that will appear in the readout of the under-mattress sensors.

After the data from the experiment is processed, and by analyzing the data, we found that 99% of the samples have a value close to zero, which indicates that no activity is detected. This can be seen from Table 1. The amplifier quickly goes to saturation, therefore most of the positive samples have value > 0.97.

Table 1: Distribution of (934141) samples by value

Value(x)	No. samples	% samples
$x \leq 0.03$	924823	99.00%
$0.03 < x < 0.97$	1874	0.20%
$x \geq 0.97$	7444	0.80%

From the close to one million data points obtained during the 8-hour window, most of the non-zero values are concentrated at

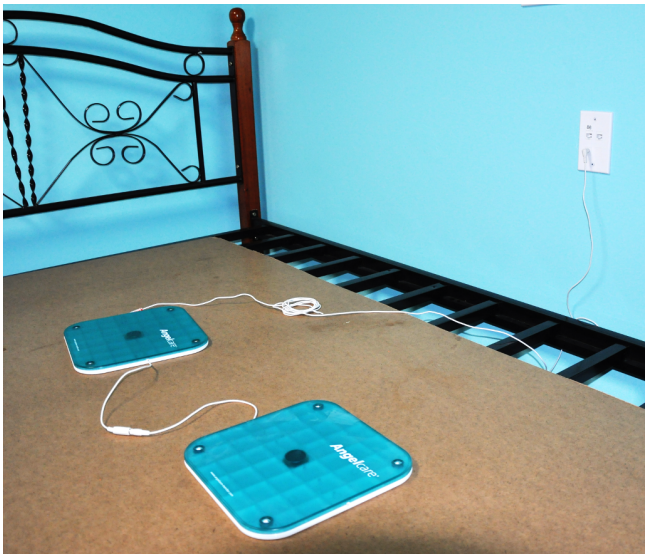

Figure 1: Piezoelectric sensors placed under the mattress

Figure 2: Connecting panel

Figure 3: Sensor module for PIR sensors

the beginning and the end of the period as can be seen in Figure 4. On the same figure, there are the data points for the piezoelectric sensor and the PIR sensor module. The events where at least one PIR sensor is activated are shown in the top part of the data plot. From the intensity of the movement, we notice that it took 25 minutes for the person to fall asleep. The activity towards the end is when the person woke up and got out of bed.

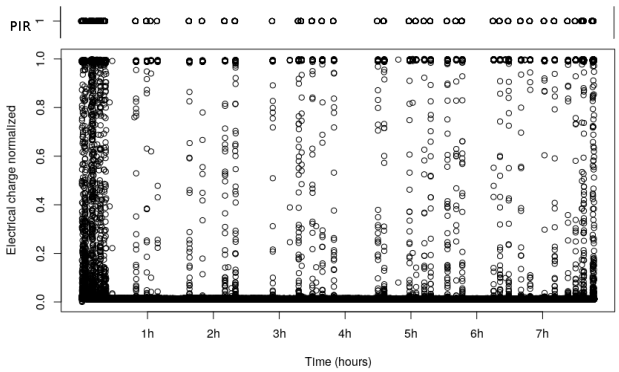

Figure 4: PIR and Piezo sensor activation (over 8 hour sleep)

Recalling that the original purpose is to measure how long it takes for the person to fall asleep and how long they sleep, as the health care provider might pose this question, it becomes evident that a data count of activity measured by piezoelectric and PIR sensors over time intervals and query it reached a threshold, is sufficient to answer that question. Additional information as to how much and when the person was moving in bed during sleep can be deducted from the raw data. The fog node can preserve patient privacy by receiving the raw data, then processing it to extract the time intervals with activity count over the set threshold and pass that data to the cloud. Additionally, if we encode the piezoelectric sensor with a resolution of one byte, the total size would be 913kB. If we add the PIR sensor data, the file becomes more than a megabyte in size. While this is not a large size for WiFi or wired network, in cases where transmission rate is limited, as is the case of protocols designed for low rate, low energy, such as LoRa-WAN, preprocessing the raw data and transmitting only the output can provide viable use of the protocol in cases where the raw data is beyond the transmission capacity.

3.2 Microphone sensors

In the quest to provide better services to beneficiaries of e-health technologies, researchers have proposed various techniques to measure a person's health or the environment. A medical state of a person is often evaluated by body sensors connected to the cloud that measure parameters such as oximetry [12] or ECG. Most of these sensors are invasive to the user and generate medical data regulated by law [8]. There are sensors to monitor the environment, some of which are less intrusive, while others such as sound sensing have the potential risk of compromising users' privacy [11]. A system where microphones are used in AAL scenario is presented in [26]. In [21], a systematic review of approaches for activity recognition based on environmental analyses using audio fingerprinting techniques is presented.

In this section, we consider a scenario where microphones are places to monitor a care receiver and their activity and his or her

environment. The purpose of this monitoring is to detect the number of people present in cases when the individual has visitors and also to detect environmental sounds that might indicate concern that should be addressed by the family or emergency services. The latter might include a non-connected smoke and carbon monoxide alarm is activated or an open faucet for a prolonged time. Such detection systems often are sensitive and can cause false detection and false alarms that lead to alarm fatigue, so tuning the model performance is very important [13].

There have been attempts at processing the sound as to preserve privacy while allowing for focused analytics to be conducted. Kumar et al. in [11] propose two simple yet highly effective methods called sound shredding and sound subsampling. Sound shredding creates random permutations of the raw sound frames akin to like paper shredding. Sound subsampling randomly drops sound frames without storing them. The resulting mutated sound recording makes the speech in the original sound record unrecognizable while preserving acoustic features, thus retaining the accuracy of context recognition. The authors analyze the sound shredding with different lengths of the sound frames. The results presented in figure 5, borrowed from the authors' original paper, reveal that the thinner the shredding is, the more difficult it is to reconstruct the audio.

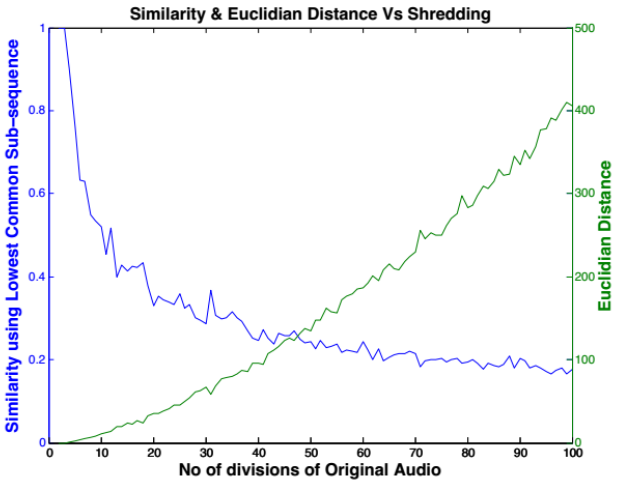

Figure 5: Euclidian distance and Similarity (using longest common sub-sequence) between Original and Reconstructed audio Vs No of divisions of Original Audio.[11]

Using machine learning (ML), the authors train a model to recognize distinct people and their gender. From the results, it is shown that shredding and subsampling do not lose information about gender and user identity. At the same time, if the audio is shredded or subsampled with a high rate, no speech content can be recovered.

Another technique is presented by Yonezawa et al. in [29]. They describe how to simplify the raw data from the microphone sensor using frequency/time domain for reducing the amount of data and for privacy protection. Their stated goals are to i) reduce the amount of calculation and ii) conceal vivid sound information by using simplified sound spectrogram. To enable the service, the system first gets raw sound data from the sound sensor and calculates simplified spectrogram to reduce the data amount. The simplified sound spectrogram is calculated by short-time Fourier transform (STFT) and calculating representing values within a particular frequency band. By using the simplified sound spectrogram instead of using the raw audio data, the user's privacy is protected.

For the proposed use case of counting people and detecting environment signals, the techniques described by this research are sufficient. In a fog network, the edge nodes might do the audio processing and implementation of ML models. If the computing power is not adequate to implement the ML models, the fog node could process the audio using sound shredding or sound subsampling, or in some cases calculate the simplified spectrogram before forwarding it to an ML model based in the cloud.

4 PRIVACY AND SECURITY DRIVEN ARCHITECTURE

In the previous chapter, two scenarios were analyzed. It was shown by experiment and by citing prior research that privacy can be increased and a preprocessing step could conserve cloud resources. In the case described in section 3.1, simple process of counting events in a time period and returning a binary output if the count is above a threshold is needed to prevent data leakage beyond what is requested by the query. A more complicated process of audio processing, described in section 3.2, is necessary to implement privacy mechanisms to obfuscate speech while preserving enough information to recognize sound events such as an audible alarm or to count the number and infer the gender of people in the room.

In this chapter, we propose an architecture for fog computing, as shown in Figure 6, it is based on the standard three layers: the sensor network, the fog, and the cloud services. The cloud services are multiple and the same fog network interfaces them.

The sensor network consists of a variety of sensors with a variety of interfaces. In the sleep monitoring experiment, we used commercially available piezoelectric sensors which were connected by custom build signal amplifier.

A cloud service can be set by a medical provider, by research organizations, by government-run medical databases, or by private companies providing additional services. In the sleep monitoring scenario, a separate cloud instance could be set by a private service provider in order to give high-level state of health to the family members, another cloud could be set up by the health care provider who will be entitled to more detailed medical information including insight into restless sleep that could indicate research institutions could set specific medical conditions and a third instance with access to anonymized and aggregate data.

The fog layer is the bridge between the sensor network and the cloud. The sensors interact with an e-health gateway which has many interfaces for data exchange including wired protocols such as I2C, CAN bus, USB; it also supports wireless protocols including WiFi, BTLE, ZibBee, LoRa, etc. The e-health gateway has sufficient computing capabilities for simple data processing, but its primary role is data aggregation and communication. Depending on the path to the cloud instances some nodes carry data that has been filtered to enhance privacy while other nodes carry data with more

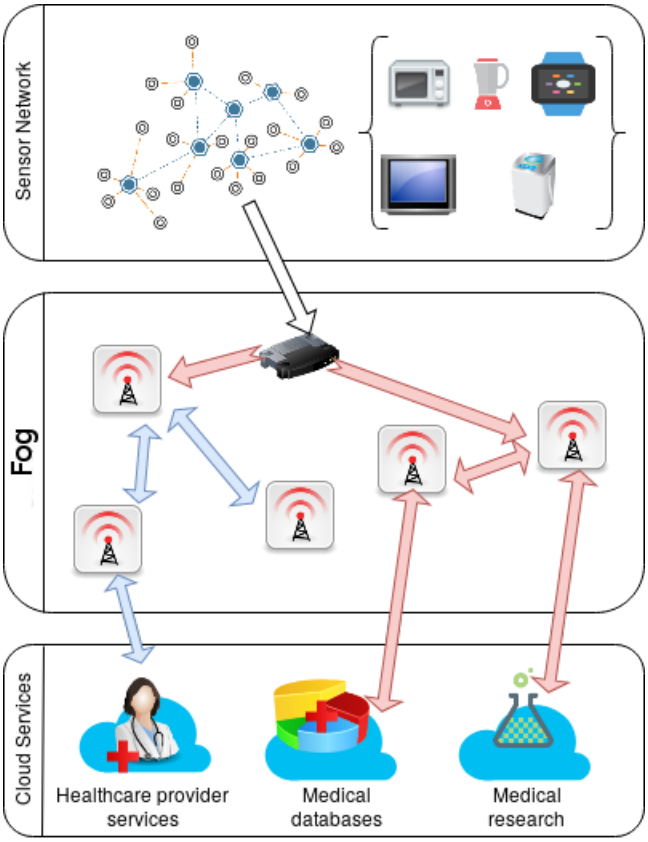

Figure 6: Data flow in fog architecture for personal health

physiological data which might be needed for health monitoring by health care providers or emergency services. In Figure 6, medical data with patient identification is carried by the blue lines that end with the healthcare provider services cloud, while anonymized and aggregated data are carried by the red lines that lead to the medical database and research institutions.

5 DISCUSSION

Utilizing the design described in the previous chapter, data exposure is minimized. As stated in the introduction, we should threat patient data with extreme sensitivity and evaluate risks even for data exposed to authorized users such as insurance companies and health centers to limit any possibility of harming the patient and restricting their autonomy to make personal health decisions, and even to protect their freedoms. Informed consent must be the ultimate factor if any data should be shared with any external entity. This consent cannot be absolute and should always be revocable. That is why the e-health gateway should have a clear interface with the care receiver to allow full control while preserving usability.

Health gateway is the first line of defense in the proposed architecture. It must compartmentalize data received by various sensors and should implement end-to-end encryption with the cloud to provide confidentiality, integrity, and anonymity. Even when raw data is transmitted to the cloud, as some low-powered microcontrollers do not possess processing power to use encryption protocols such as TLS, this would be offloaded to the e-health gateway. In-the-bed sensors experiment the piezoelectric and the PIR sensors were connected to Arduino boards that are not capable of TLS even with the network shield.

As shown, this approach protects user privacy and also increases security and by offloading processing in the edge, initial hardware investment could be recovered by reducing cloud cost. Compared to cloud only solution, in the sleep monitor case, raw data never reaches the cloud and thus reduces the risk of service provider obtaining information that is not intended to be collected and might expose other aspects of the private life of the patient. In the sound recording scenario, private conversations made by the care receiver should never be disclosed to any external person, including non-present family members and doctors. The presented techniques accomplish this goal. The data is still captured, but beyond the e-health gateway, the scrambling of the sound leaves speech unrecoverable while leaving enough data for targeted sound recognition.

6 CONCLUSION AND FUTURE WORK

As personal health become more pervasive and part of daily life, and as the data generated by it increases in volume, fog computing offers a solution for many critical issues. The added flexibility of the fog architecture enables better placement of computing and network resources. Smarter data flow could protect personal data, bandwidth cost could be reduced and more scalable, secure and interoperable systems can be designed.

In this paper, we have shown the applicability of fog computing and its ability to accomplish computational and bandwidth savings and to protect care receivers' privacy by preprocessing.

In the future, we will work to improve the sleep monitoring experiment by placing additional sensors, including pulse oximeter sensors, ECG sensors, pressure based sensors under the mattress and other environmental sensors. The more invasive sensors such as pulse oximeter and ECG would present additional challenge of privacy protection as they generate data protected by HIPAA regulations so the setup should also be evaluated to be HIPAA compliant. Additionally, we would work to improve the amplifier circuitry to prevent over-saturation so that the signal is spread out and can be better sampled to detect smaller and larger movements.

One should also implement sound privacy features, like the ones described in section 3.2 using the fog, and to verify the performance of the fog and the cloud for the described scenario. Frequency bands reduction should be evaluated to make speech unidentifiable while still being able to recognize specific sounds.

ACKNOWLEDGMENT

This work was partially financed by the Faculty of Computer Science and Engineering at the Ss. Cyril and Methodius University, Skopje, Macedonia.

This publication is based upon work from COST action CA16226 - Indoor Living Space Improvement: Smart Habitat for the Elderly (Sheld-on), supported by COST (European Cooperation in Science and Technology).

COST is a funding agency for research and innovation networks. Our Actions help connect research initiatives across Europe and

enable scientists to grow their ideas by sharing them with their peers. This boosts their research, career and innovation.

REFERENCES

[1] H. Al-Hamadi, A. Gawanmeh, and M. Al-Qutayri. 2017. Lightweight security protocol for health monitoring in Ambient Assisted Living environment. In *2017 IEEE International Conference on Communications Workshops (ICC Workshops)*. IEEE, Piscataway, NJ, USA, 1282–1287. https://doi.org/10.1109/ICCW.2017.7962835

[2] Marshall Allen. 2018. You Snooze, You Lose: Insurers Make The Old Adage Literally True. https://www.propublica.org/article/you-snooze-you-lose-insurers-make-the-old-adage-literally-true

[3] Arwa Alrawais, Abdulrahman Alhothaily, Chunqiang Hu, and Xiuzhen Cheng. 2017. Fog computing for the internet of things: Security and privacy issues. *IEEE Internet Computing* 21, 2 (2017), 34–42.

[4] Mahmoud Barhamgi, Mu Yang, Chia-Mu Yu, Yijun Yu, Arosha K Bandara, Djamal Benslimane, and Bashar Nuseibeh. 2017. POSTER: Enabling End-Users to Protect their Privacy. In *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*. ACM, New York, NY, USA, 905–907.

[5] Flavio Bonomi, Rodolfo Milito, Jiang Zhu, and Sateesh Addepalli. 2012. Fog computing and its role in the internet of things. In *Proceedings of the first edition of the MCC workshop on Mobile cloud computing*. ACM, New York, NY, USA, 13–16.

[6] Kelsey Clubb, Lisa Kirch, and Nital Patwa. 2015 (last accessed 10.06.2019. *The Ethics, Privacy, and Legal Issues around the Internet of Things*. University of California-Berkley. https://www.ischool.berkeley.edu/sites/default/files/projects/w231-internetofthingsfinalpaper.pdf

[7] Ace Dimitrievski, Eftim Zdravevski, Petre Lameski, and Vladimir Trajkovik. 2016. Towards application of non-invasive environmental sensors for risks and activity detection. In *Intelligent Computer Communication and Processing (ICCP), 2016 IEEE 12th International Conference on*. IEEE, Piscataway, NJ, USA, 27–33.

[8] Alexis Guadarrama. 2017. Mind the Gap: Addressing Gaps in HIPAA Coverage in the Mobile Health Apps Industry. *Hous. L. Rev.* 55 (2017), 999.

[9] Joseph L. Hall and Deven McGraw. 2014. For Telehealth To Succeed, Privacy And Security Risks Must Be Identified And Addressed. *Health Affairs* 33, 2 (2014), 216–221. https://doi.org/10.1377/hlthaff.2013.0997 arXiv:https://doi.org/10.1377/hlthaff.2013.0997

[10] Pengfei Hu, Huansheng Ning, Tie Qiu, Houbing Song, Yanna Wang, and Xuanxia Yao. 2017. Security and privacy preservation scheme of face identification and resolution framework using fog computing in internet of things. *IEEE Internet of Things Journal* 4, 5 (2017), 1143–1155.

[11] Sumeet Kumar, Le T Nguyen, Ming Zeng, Kate Liu, and Joy Zhang. 2015. Sound Shredding: Privacy Preserved Audio Sensing. In *Proceedings of the 16th International Workshop on Mobile Computing Systems and Applications*. ACM, ACM, New York, NY, USA, 135–140.

[12] Marcelo M Lamego, Abraham Mazda Kiani, Don Sanders, Jeroen Poeze, Massi Joe E Kiani, and Anthony Amir Davia. 2014. Cloud-based physiological monitoring system. US Patent App. 14/203,243.

[13] P. Lameski, E. Zdravevski, S. Koceski, A. Kulakov, and V. Trajkovik. 2017. Suppression of Intensive Care Unit False Alarms Based on the Arterial Blood Pressure Signal. *IEEE Access* 5 (2017), 5829–5836. https://doi.org/10.1109/ACCESS.2017.2690380

[14] Colin Lecher. 2018. What Happens When an Algorithm Cuts Your Health Care. https://www.theverge.com/2018/3/21/17144260/healthcare-medicaid-algorithm-arkansas-cerebral-palsy

[15] Kanghyo Lee, Donghyun Kim, Dongsoo Ha, Ubaidullah Rajput, and Heekuck Oh. 2015. On security and privacy issues of fog computing supported Internet of Things environment. In *Network of the Future (NOF), 2015 6th International Conference on the*. IEEE, IEEE, Piscataway, NJ, USA, 1–3.

[16] Rongxing Lu, Kevin Heung, Arash Habibi Lashkari, and Ali A Ghorbani. 2017. A lightweight privacy-preserving data aggregation scheme for fog computing-enhanced IoT. *IEEE Access* 5 (2017), 3302–3312.

[17] M. Meingast, T. Roosta, and S. Sastry. 2006. Security and Privacy Issues with Health Care Information Technology. In *2006 International Conference of the IEEE Engineering in Medicine and Biology Society*. IEEE, Piscataway, NJ, USA, 5453–5458. https://doi.org/10.1109/IEMBS.2006.260060

[18] Daniel Minoli, Kazem Sohraby, and Benedict Occhiogrosso. 2017. Iot security (IoTsec) mechanisms for e-health and ambient assisted living applications. In *Proceedings of the Second IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies*. IEEE Press, IEEE Press, Piscataway, NJ, USA, 13–18.

[19] Mithun Mukherjee, Rakesh Matam, Lei Shu, Leandros Maglaras, Mohamed Amine Ferrag, Nikumani Choudhury, and Vikas Kumar. 2017. Security and privacy in fog computing: Challenges. *IEEE Access* 5 (2017), 19293–19304.

[20] A. Papageorgiou, M. Strigkos, E. Politou, E. Alepis, A. Solanas, and C. Patsakis. 2018. Security and Privacy Analysis of Mobile Health Applications: The Alarming State of Practice. *IEEE Access* 6 (2018), 9390–9403. https://doi.org/10.1109/ACCESS.2018.2799522

[21] Ivan Pires, Rui Santos, Nuno Pombo, Nuno Garcia, Francisco Flórez-Revuelta, Susanna Spinsante, Rossitza Goleva, and Eftim Zdravevski. 2018. Recognition of Activities of Daily Living Based on Environmental Analyses Using Audio Fingerprinting Techniques: A Systematic Review. *Sensors* 18, 1 (2018), 160.

[22] Yingjuan Shi, Gejian Ding, Hui Wang, H Eduardo Roman, and Si Lu. 2015. The fog computing service for healthcare. In *Future Information and Communication Technologies for Ubiquitous HealthCare (Ubi-HealthTech), 2015 2nd International Symposium on*. IEEE, IEEE, Piscataway, NJ, USA, 1–5.

[23] Ivan Stojmenovic and Sheng Wen. 2014. The fog computing paradigm: Scenarios and security issues. In *Computer Science and Information Systems (FedCSIS), 2014 Federated Conference on*. IEEE, IEEE, Warsaw, Poland, 1–8.

[24] Oliver Stutz, Sascha Todt, Sven Venzke-Caprarese, Susanne Boll, Wilko Heuten, and Torben Wallbaum. 2016. Implementing Data Protection and Information Security in AAL. In *Ambient Assisted Living*. Springer International Publishing, Cham, 59–68.

[25] Montbel Thibaud, Huihui Chi, Wei Zhou, and Selwyn Piramuthu. 2018. Internet of Things (IoT) in high-risk Environment, Health and Safety (EHS) industries: A comprehensive review. *Decision Support Systems* 108 (2018), 79–95.

[26] Michel Vacher, François Portet, Anthony Fleury, and Norbert Noury. 2010. Challenges in the processing of audio channels for ambient assisted living. In *e-Health Networking Applications and Services (Healthcom), 2010 12th IEEE International Conference on*. IEEE, IEEE, Piscataway, NJ, USA, 330–337.

[27] Jayneel Vora, Sudeep Tanwar, Sudhanshu Tyagi, Neeraj Kumar, and Joel JPC Rodrigues. 2017. FAAL: Fog computing-based patient monitoring system for ambient assisted living. In *e-Health Networking, Applications and Services (Healthcom), 2017 IEEE 19th International Conference on*. IEEE, IEEE, Piscataway, NJ, USA, 1–6.

[28] Shanhe Yi, Zhengrui Qin, and Qun Li. 2015. Security and privacy issues of fog computing: A survey. In *International conference on wireless algorithms, systems, and applications*. Springer, Springer, Cham, 685–695.

[29] Tomoko Yonezawa, Naoki Okamoto, Hirotake Yamazoe, Shinji Abe, Fumio Hattori, and Norihiro Hagita. 2011. Privacy protected life-context-aware alert by simplified sound spectrogram from microphone sensor. In *Proceedings of the 5th ACM International Workshop on Context-Awareness for Self-Managing Systems*. ACM, ACM, New York, NY, USA, 4–9.

[30] Xiaojun Zhai, Amine Ait Si Ali, Abbes Amira, and Faycal Bensaali. 2017. ECG encryption and identification based security solution on the Zynq SoC for connected health systems. *J. Parallel and Distrib. Comput.* 106 (2017), 143–152.