Privacy and Security of IoT Based Healthcare Systems: Concerns, Solutions, and Recommendations

Ibrahim Sadek[1(✉)], Shafiq Ul Rehman[2], Josué Codjo[3], and Bessam Abdulrazak[3]

[1] Faculty of Engineering, Biomedical Engineering Department, Helwan University, Cairo, Egypt
ibrahim_ibrahim@h-eng.helwan.edu.eg
[2] ST Electronics-SUTD Cyber Security Laboratory, Singapore University of Technology and Design, Singapore, Singapore
[3] Département d'Informatique, Faculté des sciences, Université de Sherbrooke (UdeS), Sherbrooke, Canada

Abstract. Although emerging IoT paradigms in sleep tracking have a substantial contribution to enhancing current healthcare systems, there are several privacy and security considerations that end-users need to consider. End-users can be susceptible to malicious threats when they allow permission to potentially vulnerable or leaky third-party apps. Since the data is migrated to the cloud, it goes over insecure communication channels, all of which have their security concerns. Moreover, there are alternative data violation concerns when the data projects into the proprietor's cloud storage facility. In this study, we present some of the existing IoT sleep trackers, also we discuss the most common features associated with these sleep trackers. As the majority of end-users are not aware of the privacy and security concerns affiliated with emerging IoT sleep trackers. We review existing solutions that can apply to IoT sleep tracker architecture. Also, we describe a deployed IoT platform that can address these concerns. Finally, we provide some of the recommendations to end-users and service providers to ensure a safer approach while leveraging the IoT sleep tracker in caregiving. This incorporates recommendations for software updates, awareness programs, software installation, and social engineering.

1 Introduction

The 2019 "World Economic Forum" global risk report[1] has nominated cyber attacks and data breaches as the fourth and fifth deliberate risks facing the world today. It is the second year in a row that these threats feature in the top five list of risks. Healthcare, among others, was offended with more cybersecurity breaches, in which several situations can lead to these breaches, for example,

[1] World Economic Forum. The Global Risks Report 2019. Retrieved May 29, 2019, from https://www.weforum.org/reports/the-global-risks-report-2019.

J. Pagán et al. (Eds.): ICOST 2019, LNCS 11862, pp. 3–17, 2019.
https://doi.org/10.1007/978-3-030-32785-9_1

credential-stealing malware, an insider who either systematically or accidentally unveils patient data, or lost laptops or other mobile devices. On the illegal market, "Protected Health Information" (PHI) is more important than credit card credentials or even personally identifiable information. Hence, there is a higher motivation for cybercriminals to target medical databases, and so they can sell the PHI or adapt it for their benefits.

Throughout the world, healthcare challenges can exist in different shapes and forms. Subsequently, this presents tremendous pressure on the current system. Even though every society faces various demands and encounters several effects, it is still practicable to determine the overall global risk to current healthcare systems. These demands are a fundamental starting point for the work ahead. Population aging, the prevalence of chronic diseases, shortage of healthcare specialists, and the unpredictable rise of healthcare costs, among other reasons, are the considerable challenges facing today's healthcare systems. For dealing with these issues, public and private sector players should collaborate to find more innovative and affordable methods that can be deployed in out-of-hospital environments [14]. Healthcare IoT based systems are multiples and vary from wearable to mobile sensors going through actuators, that acquire patient biosignals, motion, or contextual information. Amongst those systems, we have Zio Patch depicted in [24] which measures heart rate and electrocardiogram (ECG) and Myo [9] which is a motion controller used in orthopedics for patients who need to exercise after a fracture. None of the above performs in multiple information gathering. Therefore, we have systems, which can combine biosignals, motion, and contextual information such as sleep trackers.

In this paper, we focus on sleep tracking as a significant vector of quality of life. Sleep is crucial to our health and sleep disorders can often be a symptom of a disease; or likewise may be a signal of a subsequent illness such as depression. As a result, assessment of sleep is a fundamental component of any health check. Understanding cardiovascular and respiratory systems are essential for analyzing sleep and sleep cycles. This is because the active processes in the human body are different in sleep and wakefulness.

Nowadays, we can render the Internet of Things (IoT) and Cloud services to improve access to caregiving by remotely strengthen the quality of caregiving and above all cut down the cost of caregiving. As different sleep trackers, i.e., IoT devices are used to collect the user data and transfer it to the cloud. The collected data is later being analyzed by sleep experts to enhance these devices for better results. According to the "ABI Research" report[2] currently, there are over 10 billion wirelessly connected IoT devices, and by 2020, the number will exceed 30 billion devices. Some of these devices will fall within the category of sleep-tracking devices. Nevertheless, these emerging technologies are vulnerable to adversarial attacks because of their design. The data breach can have severe consequences both on individual users and the company's reputation. Moreover,

[2] ABI Research. Over 30 Billion Devices Will Wirelessly Connect to the Internet of Everything in 2020. Retrieved May 29, 2019, from https://www.abiresearch.com/press/more-than-30-billion-devices-will-wirelessly-conne/.

compromised IoT sleep tracking devices can allow intruders to monitor the user's private lives actively.

The main contribution of this study is to highlight the privacy and security concerns of IoT sleep trackers and provide an insight into how precise mechanisms or approaches can be applied to prevent or mitigate such adversarial attempts. We anticipate this research to guide future researchers to use and apply specific solutions for IoT in healthcare problems based on the proposed approaches and mechanisms by security experts.

The rest of the paper is organized as follows: IoT sleep trackers and their types are described in Sect. 2. We state the security and privacy issues that are associated with IoT sleep trackers in Sect. 3. We present some existing solutions in Sect. 4, then we depict an IoT based case study in Sect. 5, while we mention the recommendations in Sect. 6. We outline the conclusion in Sect. 7.

2 IoT Sleep Trackers

The healthcare system desperately needs reform to rein in costs, improve quality, and expand access. Medical diagnosis consumes a large part of hospital bills. Technology can move medical check routines from a hospital (hospital-centered) to the home (home-centered) of the patient. A new paradigm, known as the IoT, widely applies in many areas, including healthcare. The full application of this paradigm in healthcare is a mutual hope, as it enables medical centers to function more efficiently and patients to receive better treatment. There are unique benefits with the use of this technology that could improve the quality and efficiency of treatments and thus improve patient health.

IoT technology permits and facilitates remote monitoring of patients who do not have ready access to adequate health monitoring. Likewise, it helps to thoroughly reduce costs and promote health by increasing the availability and quality of care [12]. The IoT is a network of smart devices and other objects integrated with electronics, software, sensors, and network connectivity that permit these objects to get and exchange data. The concept of IoT provides healthcare professionals and caregivers to access a patient's medical history, vitals, lab results, medical and prescription histories either on-site or remotely via tablets or smartphones. Patients can be observed and notified from anywhere [9]. We can use IoT based solutions to record patient health data securely from several sensors, apply complicated algorithms to analyze the data and then distribute it through wireless connectivity with medical specialists who can make suitable health recommendations [21].

Typically, examining a person's sleep requires an overnight sleep test (Fig. 1) or polysomnography (PSG) that allows the monitoring of several physiological functions besides sleep cycles [4,22]. Although the PSG, or as known as the gold standard for sleep monitoring, provides real-time and accurate information about sleep, it is cumbersome, expensive, and time-consuming. Thus, the healthcare community is inquiring novel nonintrusive solutions that can improve the quality of healthcare for the patient while sustaining the cost of the service provided [19].

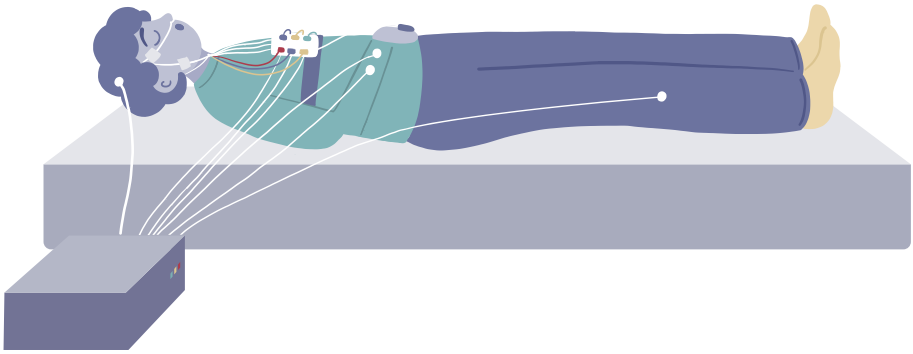

Fig. 1. An illustration of the location of the various electrodes and sensors used during the overnight sleep. Adapted from: mattressclarity.com

Actigraph is a very famous example that can be used for sleep analysis. The device is not as accurate as of the PSG. However, its information, which is based on the users' activity, is critical for healthcare professionals to interpret and analyze the sleep behavior of the users. As hardware and software technology is advancing quickly, several devices and mobile apps have been developed for general healthcare monitoring, including sleep. These devices could be wearables such as bracelets, smart-watches, smart-shirts, or smart-rings (Fig. 2) or non-wearable like bed-sensors that can be installed underneath the user's bed mattress (Fig. 3).

Sleep monitoring is described as getting qualitative sleep metrics by monitoring a person's sleep during the night. These serve two functions. One is to formulate an objective view of the quality of a person's sleep, while the other role is to determine the trends in sleep. Respiratory rate and body movements are considered the most detailed measurements for sleep monitoring during the sleeping session. The respiratory rate and respiratory rate variability are used for rapid eye movement (REM) sleep identification, while the movement metrics are utilized to discriminate between deep sleep, light sleep, and then waking stages of sleep. We can also extract several sleep parameters, for example, the duration of a sleep period, the number of awakenings, duration of disturbed sleep periods, and the time required to fall asleep. In recent years, various sensor technologies have been exploited, especially to monitor sleep-wake patterns simultaneously with the gold standard PSG and actigraphy; these sensor technologies are commonly denoted as consumer sleep tracking devices. Consumer sleep tracking devices are just like actigraphs because they allow users to be mobile and sleep as usual while being monitored closely.

Most of the consumer sleep monitors pretend to help provide information about sleep duration and quality of sleep, enabling subjects to awaken only from the light sleep. Typically, the data gained from consumer sleep tracking devices are not intended for routine diagnosis of sleep disorders. However, scientific improvements in hardware and software, accessibility, and ready availability

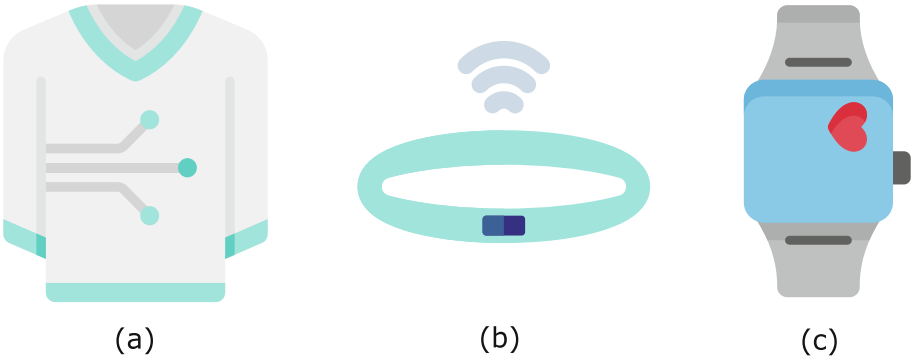

Fig. 2. Illustrations for wearable sleep trackers; (a) smart-shirt, (b) smart-bracelet, and (c) smart-watch. Icons made by Freepik from: flaticon.com

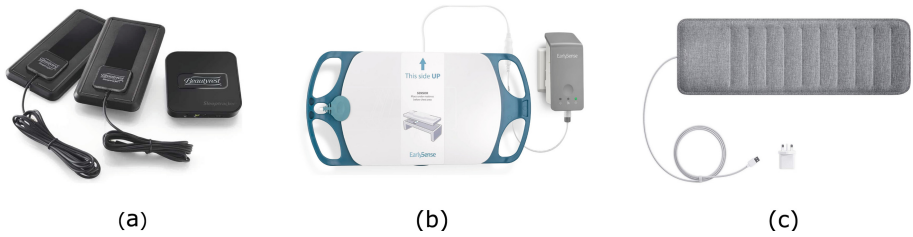

Fig. 3. Some examples of non-wearables sleep trackers; (a) Beautyrest © 2019 Simmons Bedding Company LLC, (b) EarlySense © 2019 Early Sense, and (c) Withings © 2019 Withings.

allow the public to adopt them for clinical purposes. These devices include *Emfit QS*, *Beddit*, *Withings*, *Sleepace Reston*, *Beautyrest*, and *Juvo*. Figure 3 shows three examples of existing bed-based sleep trackers.

These sensors are designed and packaged in a way that makes them invisible to the subjects. For instance, we can easily integrate them into home furniture such as beds, pillows, chairs, or even weighing scales [26]. These sensors technologies are preferred than those popular sensors (e.g., ECG) when we are considering long-term (trend over time, early detection and intervention by sending alarms to family members or caregivers through well-designed user interfaces), mobile, convenient and practical (aging-in-place, senior activity centers). However, in critical situations, gold-standard methods should be considered [20].

Most of the existing products implement the piezoelectric technology for nonintrusive monitoring of vital signs (for example, *Beddit*, *Withings*, *Sleepace Reston*, and *Beautyrest*) which shows the popularity and suitability of the piezoelectric material for measuring the slight vibrations caused by the heart movements that is transmitted through the bed mattress. Another famous sleep tracker sensor using a piezoelectric sensor is *EarlySense*. The system can report information about heart rate, respiration, snoring, coughing, and movement. A

recent study showed good agreement between *EarlySense* and the gold standard PSG for sleep staging [23]. The device provided promising results for sleep apnea detection [7].

On the one hand, there are some standard features that these sensors claim to measure, such as heart rate, respiration, sleep and wake-up time, and sleep interruptions. There are several publications in the existing literature that can support these claims, as mentioned in [20].

Insufficient publications are available in existing literature that can support other claims such as sleep efficiency (i.e., the time in bed spent asleep before waking up), sleep score (i.e., summarizes your night's sleep quality and quantity in a single number, it takes your sleep time, sleep efficiency, restfulness, snoring, and heart rate into account), smart alarm (i.e., to awaken the wearer at an optimal time within a time-window that ends in the final alarm setting) and sleep stages. For example, to get accurate results about the different stages of sleep, the patient should undergo a full-night sleep study or as known as polysomnography [25]. It seems that *Emfit QS* is the only device claiming to measure heart rate variability. Similarity, Withings is claiming to measure a breathing disturbance metric that can contribute to identifying abnormal sleep patterns such as apneas. A power supply is required for operating most of these sensors. However, *Sleepace Reston* is a battery-powered. It is worth mentioning that these sensors are only designed to monitor a single person overnight. However, the *BeautyRest* sleep tracker comes with two sensors, so couples can independently track their sleep.

Having said that, although the security and privacy feature of these sensors are essential, most of the end-users might not fully know of weaknesses and potential risks in their existing devices. Therefore, we present in the ensuing sections, the security and privacy features associated with existing IoT sleep trackers.

3 Privacy and Security Concerns

According to Deborah Lupton's report[3], during her Research she found there are risks associated with data collection (a) from IoT tracking devices such as devices' storage, (b) while transmitting it over the network and (c) finally, in the cloud where data is stored for analyses. The same risk applies to the IoT Sleep Tracker Architecture, where these devices are being used for collecting data while users are asleep, later transmitted to cloud via wireless communication.

Sleep tracking devices aid us in practical applications in gaining quality sleep, thus improving our lives by measuring our heart rates and movements as described in Sect. 2. However, they can possess severe security and privacy risks. Since the sleep tracker users can become a victim to malware by downloading the insecure third-party apps and thus gives permission to the potential adversary to access the device remotely, Later, the users operate these sleep

[3] The Irish Times. Fitness trackers run into resistance over data security concerns. Retrieved May 29, 2019, from https://www.irishtimes.com/business/technology/fitness-trackers-run-into-resistance-over-data-security-concerns-1.3119483.

trackers knowingly or unknowingly in their private places, i.e., home, considering their devices are secure enough to be compromised. Mostly IoT sleep-tracking devices communicate over the public networks. As the data is being transferred to the cloud, the adversary can intercept over the communication channel by carrying out various attacks such as Botnet, Denial of Service (DoS) and Man in the Middle (MITM) attacks. Moreover, there are data breach concerns, as the adversary can remotely access the data stored in the cloud by compromising it via malicious software. Once the device/storage is hacked, a hacker can gain the user's confidential data about sleeping habits such as sleep talking, snoring sounds, and sensual activities. Such a data breach can have a severe impact on the user's reputation. Besides, a hacker can induce the noise by speaking or producing some sounds to disturb the user while asleep, which can consequently result in inadequate sleep.

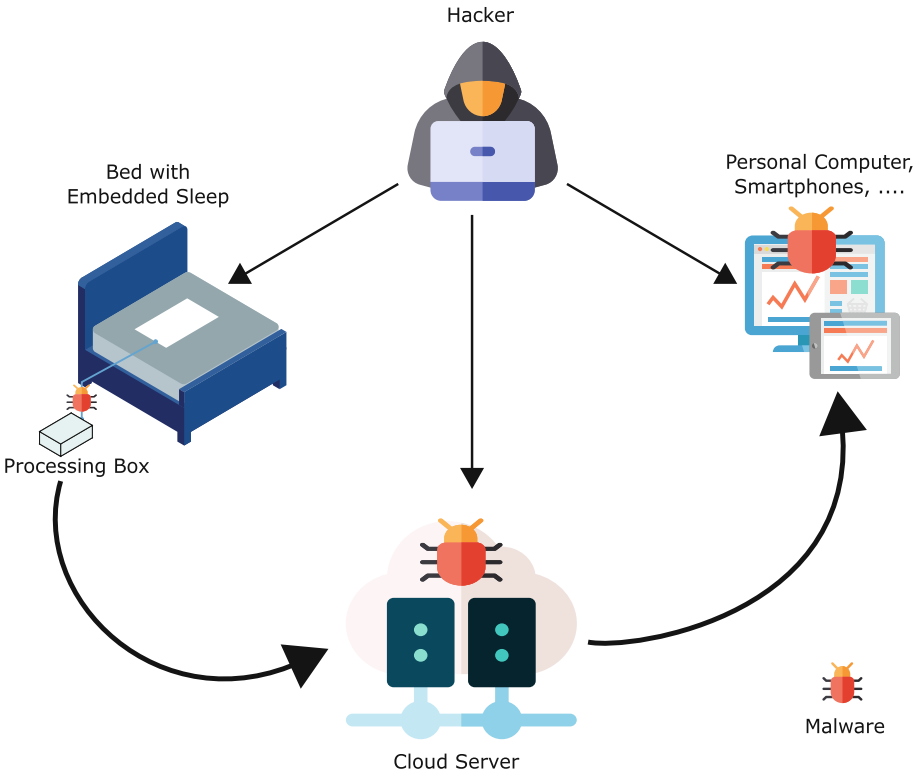

Fig. 4. An illustration of a sleep-tracking mat as an example of an IoT device in a medical setting and how an attacker can exploit the several stages of data processing, i.e., from data acquisition to end-users.

Similarly, there is a risk of data profiling which is defined as "collecting a person's behavior and analyzing psychological characteristics to predict or assess

their ability in a certain sphere or to identify a particular group of people." This means the data generated by the sleep tracker devices can be exploited to create profiles of such device users, which can be afterward used for target advertisements. The reason being that an individual's data is collected through wirelessly connected devices means there is a need for advanced measures to ensure the security and privacy of end-users. Research has shown [1], that because of the heterogeneous nature of IoT, it has raised various privacy and security concerns. For instance, data confidentiality, integrity, availability, user authentication, authorization, and anonymity. Figure 4 depicts the different attack scenarios that can affect the remote monitoring of sleep.

4 Existing Security and Privacy Solutions

While considering these IoT privacy and security concerns, the researchers and security experts around the globe from different domains, i.e., academia, industry, and technical backgrounds are attempting to mitigate these flaws in IoT infrastructure by fulfilling the necessary security and privacy measures as mentioned in Sect. 3. Some existing proposed mechanisms that also apply to sleep-tracker architecture are as follows:

Bruening and Waterman [5] introduced a concept of data tagging to ensure data privacy while transferring the sensor data over the network. It appends an additional tag to data transfer to ensure trusted communication, hence can hide the user's identity. Similarly, Chatzigiannakis *et al.* [6] proposed another approach to preserve user identity, which is known as the zero-knowledge proof (ZKP). Based on this concept, the sender can show to receive specific properties of transferred information that can ensure its authenticity without revealing its identity. Moreover, Henze *et al.*, [11] have examined the clustering technique known as the k-anonymity model to hide the location of sensor nodes to protect the sensitive data being transferred over the wireless network (WSN). The idea behind this is to gather the data from these nodes at different positions without being easily traced. Furthermore, Google[4] proposed a solution that is a part of the Google cloud platform. Scalability is the main feature of this platform, which allows connecting the devices, collecting the data, and visualizing them.

Besides, IoT solutions, namely IBM Bluemix Platform offered by IBM, is an IoT-enabled cloud solution. This platform can be used for the development of cloud-based applications managing data generated by several sensors and devices, and it supports secure data transfers.

Moreover, Internet Protocol version 6 (IPv6) [8] is the next-generation Internet protocol, which is being deployed as a communication protocol in the IoT environment. However, because of its nature, it is vulnerable to DoS attacks [17]. Such vulnerability can interrupt the communication between the nodes in a network. To resolve this problem, the Rule-based mechanism [16] and a lightweight, encrypted scheme known as Secure-DAD [18] have been proposed by Rehman

[4] Google Cloud IoT - Fully managed IoT services — Google Cloud. Retrieved May 29, 2019, from https://cloud.google.com/solutions/iot/.

and Manickam. The former technique can detect any attempt of the DoS attack, while a later system can prevent it from occurring. Thus, by deploying such mechanisms, we can ensure a trusted communication between the IoT nodes in a heterogeneous environment.

Recently, Dwivedi *et al.* [10] proposed an IoT framework based on a modified blockchain model. The authors claim that the proposed framework provides a solution that is based on advanced cryptographic primitives for IoT data applications and secure transactions. Also, it can provide anonymity of users over the blockchain-based network.

To complement, in Sect. 5, we present an IoT-based case study (i.e., AMI-IoT platform) to show how these security concerns as aforementioned can be addressed in a real-life scenario.

5 AMI-IoT Deployed Platform

The Ami-lab has been developing several IoT architectures for the past decade and following; we described how we addressed the previously discussed security issues. We have mainly focused on privacy, data profiling, the man-in-the-middle-attack, data corruption, which can undermine the end-to-end communication from the environmental nodes to the database. The AMI-IoT platform as depicted in Fig. 5 is composed of three main components, which are, end-users environment, network, and cloud architecture. Based on the work of Mendonça *et al.* [2], we assume that the three elements, Sensing Approach (SA), Awareness & Security (AS) and Responsibility & Actions (RA), are essentials to address the IoT security concerns.

5.1 Sensing Approach (SA)

The SA element is the entry point of the architecture. It ensures data detection and its migration from environmental nodes to the database. It also represents the listening state of other components as well as the architecture. At this point, making sure of the working state of environmental nodes is crucial. Data gathered by nodes will be sent through a network path built by the node and its peer. This element is the foundation of IoT architecture, enabling endpoint sleep trackers and allowing them to submit information through the entire network, giving the opportunity to experts to process the data. Sleep tracker such as a smart mat has been used, transmitting data to a node that will serve as a broker and publish the information. On the other hand, a unique peer will be subscribing to that broker getting the data in time through a canal. A gateway will be used to monitor and redirect the traffic from the peer to the smart mat. Nevertheless, during the SAP, neglecting the user's privacy, the authenticity of the information sent, and the security of the database on which information is stored does not respect the security standards Raza *et al.* [15]. It's from this perspective that we build the same element.

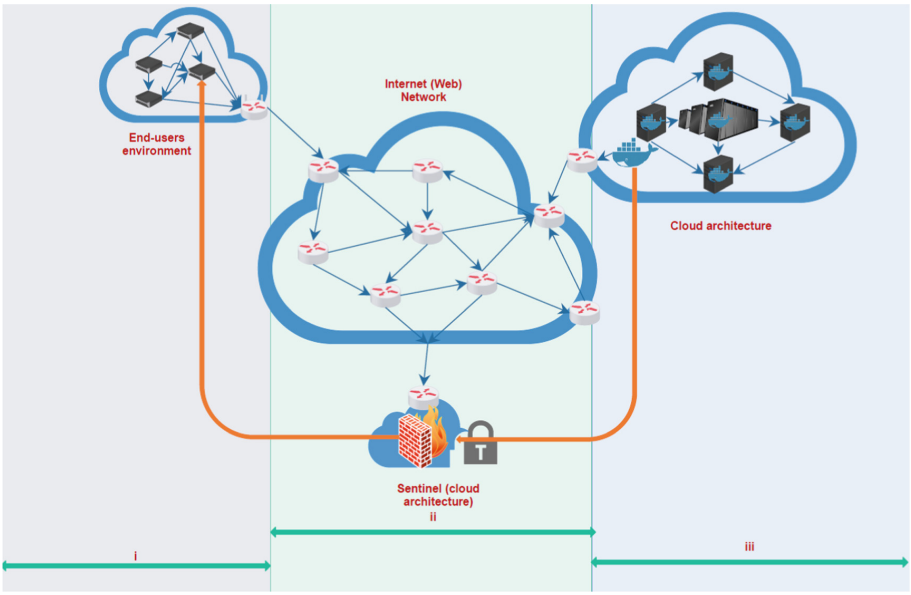

Fig. 5. Ami-IoT Architecture issues addressed (i. Jamming, Flooding, Phishing, Connection Timed out, Battery, Not responsible, Privacy, Data profiling; ii. The sinkhole, Man-in-the-middle, Hello Flood, Connection persistence, Packet loss, Botnet; iii. Flooding, Dos, Data stealing, Data loss, Data modification, privacy)

5.2 Awareness and Security (AS)

This element intends to make the system aware of abnormalities and breaches, which can occur and put the needed security to prevent a possible attack. On this note, a system cannot be protected if we are not aware of the situations and the risks surrounding it. Based on that, the Ami-lab will be relying on the three components of the architecture.

End-User Environment. It regroups all the environmental nodes gathering the data. This component is the favorite spot of attackers due to the negligence of users and their compliance with the attacks mentioned previously. This component is subject to external attacks and faces issues such as privacy, access, data profiling. To face those challenges, Ami-lab implemented firewalls Raza *et al.* [15] in every node deployed on the end-user side. Those firewalls have been added, preventing external attacks and allowing just one communication at a time. Regarding privacy, we concluded that even the node should be identified by their ID and not the users. Thus, yet if the attacker has the identifier, he won't be able to know whose information he has access to. Moreover, rules have also been applied so that the user will have limited access to the node. It will restrict phishing attacks, which can compromise the system. Also, all incoming

connections are blocked, accepting just the one responsible for collecting data. These techniques lead to securing the End-users environment component.

Cloud Architecture. It represents the core of the Ami-lab system. It's all the technologies and methods put together to enable a peer for each environmental node and the storing in the database. Data corruption, data stealing, data loss, privacy, data modification are various problems undermining this component. Ami-lab took some countermeasures such as defining a firewall on each server composing this part, to restrict intrusion. Every rule is set carefully, to block every incoming traffics and allowing single traffic from the listener to its peer (environmental node). Every outgoing traffic is controlled. Self-configuration and optimization being part of our architecture, everything adapts itself to the new configuration in our cloud. Thus, we are avoiding "data corruption" and any other kind of intrusion. We are keeping the use of the environmental node identifier and data compression to address the privacy issue. It comes to another concern, the bridge.

Internet (Network). Named in IoT architecture, the weak link, due to its public nature, it can be subject to many attacks mentioned in the previous sections. It relates the end-users environment to the cloud environment serving as a bridge. While an attack cannot reach the first component of the architecture, there is still a chance to intercept the data while it's been sent. Then, botnet attacks, man-in-the-middle attacks, which will block the transaction or worst prevent data from storing in the database. To avoid this weak point, we created a secure tunnel known just by our peers. The Internet will serve to, will be retrieving the certificates and then establishing a secured channel between the environmental node and the cloud node. Every communication has been made to guarantee that each environmental node has its peer and can communicate just with that peer. In case something happened, it won't affect the whole system since we made them independent. To reinforce the security, a high level of encryption has been used as well as data compression.

5.3 Responsibility and Actions (RA)

This element is the last piece conferring "responsibility" feature to a system and is based on Angarita and Kelaidonis *et al.* work [3,13]. Making a system able to take action, depending on the outcome of a situation is the key role of this part. Being part of our future work, Ami-lab strives to achieve a self-healing architecture. The concept of "responsibility" should be transmitted to the architecture enabling its self-management. A responsible environment based on awareness feature should be able to react in time when a situation occurs. A system should be able to define the right action to take and complete it in an optimal way. Indeed, an IoT system, when facing an intrusion issue, should be able to take action and keeps working. For instance, if there is an attack on the environmental node, the node should be able to detect and close all the connections, then

re-enable the peer connection. We achieved "the responsibility" feature on the environmental nodes. It allows them to take action against intrusion, connectivity issues, and data transmission issues. Processing information, and creating an adapted virtual object dynamically to decipher the correct information, is also part of our future work. This feature grants autonomy to the applications letting the system creating an environment suited to the end-user. It gives the required access to the user, based on its knowledge and background. Regarding the listening peers for data retrieval, our system can take action upon peers' failure by replacing them in time. A monitoring system such as Prometheus or Zabbix will be listening to applications, environmental nodes, cloud nodes, and servers and networks to transmit the right information, while the nodes themselves will decide the communication state.

6 Recommendations

Apart from the given possible solutions as described in Sects. 4, and 5 certain things need to be considered by both parties, i.e., sleep tracker end-users as well as the healthcare service providers, to ensure a safer approach while leveraging the IoT sleep tracker in caregiving. This section outlines some of these recommendations.

- **Application/Firmware Updates:** Hackers are always in search of finding the weak links to attack victims, which could be via mobile apps, IoT sleep trackers. For instance, outdated mobile apps are the most vulnerable to security threats. Similarly, healthcare system providers rarely provide the latest firmware updates on existing IoT sleep trackers, which open the doors for possible side-channel attacks on end-user devices. Therefore, healthcare service providers should offer the regular updates on mobile apps and ensure availability of sleep tracker device's latest firmware to mitigate the zero-day attacks i.e., latest security threats which are unknown to security systems, while end-users should update their device apps and keep IoT sleep tracker's firmware updated to prevent possible security breaches.
- **Software Installation:** After ensuring the mobile app and IoT sleep tracker are updated. End-users should also refrain from downloading any untrusted third-party software, applications or click on any adware link by doing so, and they are inviting the malware into their mobile devices. For example, end-users receive any health promotion ads by clicking on the link or by downloading a malicious app, IoT sleep tracker users allow the attacker to gain access, thus can monitor their privacy remotely. After compromising the mobile user device, an attacker can secretly get the private information that most of the time, IoT sleep tracker users are unaware of. Therefore, before downloading any app or clicking such links, IoT sleep tracker users should confirm their source or authenticity to prevent malware installation into their mobile devices.

- **Social Engineering:** With the massive impact of social media, end-users share their personal information publicly on social media sites such as Facebook, Instagram, etc. With such a large user-base, these platforms are seen by cybercriminals as a new and lucrative platform to spread malware. Therefore, IoT sleep tracker users should not reveal their personal details with an unknown person over these sites or the phone's calls.
- **Awareness Program:** Moreover, healthcare service providers should conduct awareness programs such as online surveys and workshops to keep educating their IoT sleep tracker customers regularly so that end-users can gain awareness about the latest hacking tactics, cybercrimes, and their possible countermeasures.

By applying these suggestions into practice, the possibilities of privacy and security threats targeted against the IoT sleep tracker environment can be prevented. Thus, to enable a safe and secure remote caregiving.

7 Conclusion

With the rapid advancement and deployment of the IoT in the healthcare domain, these technologies are closely related to people; therefore, privacy and security are major concerns. To highlight these two critical aspects of IoT, we reviewed in this paper the progress of the research works related to IoT sleep trackers and found that these concerns need to be addressed. Moreover, to mitigate such threats, some proposed solutions from researchers and security experts are described. Furthermore, there are certain things that we recommend for both end-users and service providers to deploy a resilient IoT infrastructure to ensure a secured sleep tracker.

References

1. Aldowah, H., Ul Rehman, S., Umar, I.: Security in internet of things: issues, challenges and solutions. In: Saeed, F., Gazem, N., Mohammed, F., Busalim, A. (eds.) IRICT 2018. AISC, vol. 843, pp. 396–405. Springer, Cham (2019). https://doi.org/10.1007/978-3-319-99007-1_38
2. de Almeida, F.M., de Ribamar Lima Ribeiro, A., Moreno, E.D.: An architecture for self-healing in internet of things. In: UBICOMM 2015, p. 89 (2015)
3. Angarita, R.: Responsible objects: towards self-healing internet of things applications. In: 2015 IEEE International Conference on Autonomic Computing, pp. 307–312, July 2015. https://doi.org/10.1109/ICAC.2015.60
4. Boulos, M.I., Jairam, T., Kendzerska, T., Im, J., Mekhael, A., Murray, B.J.: Normal polysomnography parameters in healthy adults: a systematic review and meta-analysis. Lancet Respir. Med. **7**(6), 533–543 (2019). https://doi.org/10.1016/S2213-2600(19)30057-8. http://www.sciencedirect.com/science/article/pii/S2213260019300578
5. Bruening, P.J., Waterman, K.K.: Data tagging for new information governance models. IEEE Secur. Priv. **8**(5), 64–68 (2010). https://doi.org/10.1109/MSP.2010.147

6. Chatzigiannakis, I., Pyrgelis, A., Spirakis, P.G., Stamatiou, Y.C.: Elliptic curve based zero knowledge proofs and their applicability on resource constrained devices. In: 2011 IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems, pp. 715–720, October 2011. https://doi.org/10.1109/MASS.2011.77
7. Davidovich, M.L.Y., Karasik, R., Tal, A., Shinar, Z.: Sleep apnea screening with a contact-free under-the-mattress sensor. In: 2016 Computing in Cardiology Conference (CinC), pp. 849–852, September 2016. https://doi.org/10.23919/CIC.2016.7868876
8. Deering, S., Hinden, R.: Internet protocol, version 6 (IPv6) specification. RFC 8200, RFC Editor, July 2017. https://tools.ietf.org/pdf/rfc8200.pdf
9. Dimitrov, D.V.: Medical internet of things and big data in healthcare. Healthcare Inform. Res. **22**(3), 156–163 (2016). https://doi.org/10.4258/hir.2016.22.3.156
10. Dwivedi, A.D., Srivastava, G., Dhar, S., Singh, R.: A decentralized privacy-preserving healthcare blockchain for IoT. Sensors **19**(2) (2019). https://doi.org/10.3390/s19020326. http://www.mdpi.com/1424-8220/19/2/326
11. Henze, M., Hermerschmidt, L., Kerpen, D., Häußling, R., Rumpe, B., Wehrle, K.: A comprehensive approach to privacy in the cloud-based internet of things. Future Gener. Comput. Syst. **56**, 701–718 (2016). https://doi.org/10.1016/j.future.2015.09.016. http://www.sciencedirect.com/science/article/pii/S0167739X15002964
12. Islam, S.M.R., Kwak, D., Kabir, M.H., Hossain, M., Kwak, K.S.: The internet of things for health care: a comprehensive survey. IEEE Access **3**, 678–708 (2015). https://doi.org/10.1109/ACCESS.2015.2437951
13. Kelaidonis, D., et al.: A cognitive management framework for smart objects and applications in the internet of things. In: Timm-Giel, A., Strassner, J., Agüero, R., Sargento, S., Pentikousis, K. (eds.) MONAMI 2012. LNICST, vol. 58, pp. 196–206. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-37935-2_15
14. Niewolny, D.: How the internet of things is revolutionizing healthcare. Healthcare Segment Manager, Freescale Semiconductor, October 2013. freescale.com/healthcare
15. Raza, S., Wallgren, L., Voigt, T.: SVELTE: real-time intrusion detection in the internet of things. Ad Hoc Netw. **11**(8), 2661–2674 (2013). https://doi.org/10.1016/j.adhoc.2013.04.014. http://www.sciencedirect.com/science/article/pii/S1570870513001005
16. Rehman, S.U., Manickam, S.: Rule-based mechanism to detect denial of service (DOS) attacks on duplicate address detection process in IPv6 link local communication. In: 2015 4th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO)(Trends and Future Directions), pp. 1–6. IEEE (2015)
17. Rehman, S.U., Manickam, S.: Denial of service attack in IPv6 duplicate address detection process. Int. J. Adv. Comput. Sci. Appl. **7**, 232–238 (2016)
18. Rehman, S.U., Manickam, S.: Improved mechanism to prevent denial of service attack in IPv6 duplicate address detection process. Int. J. Adv. Comput. Sci. Appl. **8**(2), 63–70 (2017)
19. Sadek, I., Seet, E., Biswas, J., Abdulrazak, B., Mokhtari, M.: Nonintrusive vital signs monitoring for sleep apnea patients: a preliminary study. IEEE Access **6**, 2506–2514 (2018). https://doi.org/10.1109/ACCESS.2017.2783939
20. Sadek, I., Biswas, J., Abdulrazak, B.: Ballistocardiogram signal processing: a review. Health Inf. Sci. Syst. **7**(1), 10 (2019). https://doi.org/10.1007/s13755-019-0071-7
21. Sadek, I., Demarasse, A., Mokhtari, M.: Internet of things for sleep tracking: wearables vs. nonwearables. Health Technol. (2019). https://doi.org/10.1007/s12553-019-00318-3

22. Shustak, S., et al.: Home monitoring of sleep with a temporary-tattoo EEG, EOG and EMG electrode array: a feasibility study. J. Neural Eng. **16**(2), 026024 (2019). https://doi.org/10.1088/1741-2552/aafa05
23. Tal, A., Shinar, Z., Shaki, D., Codish, S., Goldbart, A.: Validation of contact-free sleep monitoring device with comparison to polysomnography. J. Clin. Sleep Med. **13**(3), 517–522 (2017). https://doi.org/10.5664/jcsm.6514
24. Tung, C.E., Su, D., Turakhia, M.P., Lansberg, M.G.: Diagnostic yield of extended cardiac patch monitoring in patients with stroke or TIA. Front. Neurol. **5**, 266 (2015). https://doi.org/10.3389/fneur.2014.00266. https://www.frontiersin.org/article/10.3389/fneur.2014.00266
25. Tuominen, J., Peltola, K., Saaresranta, T., Valli, K.: Sleep parameter assessment accuracy of a consumer home sleep monitoring ballistocardiograph beddit sleep tracker: a validation study. J. Clin. Sleep Med. **15**(03), 483–487 (2019). https://doi.org/10.5664/jcsm.7682
26. Zaunseder, S., Henning, A., Wedekind, D., Trumpp, A., Malberg, H.: Unobtrusive acquisition of cardiorespiratory signals. Somnologie **21**(2), 93–100 (2017). https://doi.org/10.1007/s11818-017-0112-x