Security and Privacy Issues in IoT Healthcare Application for Disabled Users in Developing Economies

Kwame Assa-Agyei, Funminiyi Olajide, Ahmad Lotfi
Department of Computer Science, Nottingham Trent University, UK

Abstract

In this paper, we explore the security and privacy issues of Internet of Things (IoT) healthcare applications for special needs users. IoT enables health-related organizations to lift important data from diverse sources in real-time and this helps in precise decision-making. The transformation of the health sector, required enhancement and efficiency of protective systems, thereby reducing data vulnerability and hence, providing opportunities for secure patient data, particularly, for special needs patients. A quantitative method for purposive sampling technique was adopted and eighty-eight respondents provided the process of how the IoT technology was utilised. Data findings indicated that IoT monitoring devices have the detective ability for a person with special needs living alone with problems related to vital signs of diseases or disabilities. Personal patient health records are integrated into the e-health Centre via IoT technologies. For data privacy, security, and confidentiality, patients' records are kept on Personal Health Record Systems (PHRS). The research revealed suspected breaches of information due to cyber-attacks on the probability of false data errors in the PHRS, leading to special needs personal data leakage.

Keywords: Internet of Things (IoT), privacy and security requirement, Healthcare application, Personal Health Record Systems (PHRS), Ambient Assisted Living (AAL)

1. Introduction

The main idea of the Internet of Things (IoT) is to connect various objects or devices (Things) through wired and wireless connections via unique addressing schemes. This is a pervasive condition for global Internet connections where individuals can interact at any given time with the physical world and also in the digital world. IoT enhances a wide range of smart services and applications to be able to cope with the challenges that the Health Sectors or individual faces. For instance, it has a dynamic ability to connect T2R (Tag-to-Reader), M2H (Mobile-to-Human), S2M (Sensor-to-Mobile), D2M (Doctor-to-Machine), P2M (Patient-to-Machine), P2D (Patient-to-Doctor), O2O (Object-to-Object), D2M (Device-to-Machine) [26]. As World Health Organization (WHO) postulated, the global population of individuals that are aged 60 years and above, which are expected to reach 2 billion by the year 2050 [26]. Therefore, to avoid the overwhelming health service challenges, there is a real need of prolonging the independent living of special needs persons (which include an elderly person with special needs), while in their own different homes. Although, this does not enhance their life quality, but also lowered the costs incurred by their families to integrate them into society in general. As there is increased growth in the population of older adults, healthcare expenditures are constantly growing, while at the same time, limiting the special needs access. The lack of specialized caretakers and medical professionals including the required facilities for people with special needs is particularly acute in most rural areas [29]. In this regard, this trend with special needs requires healthcare services in high-cost healthcare centers or other large hospitals. Therefore, IoT is meant to offer an exciting opportunity of extending proper medical care to them at their doorstep. Hence, reducing the high costs involved in in-service requirements for people with special needs people. This proposed exploratory research using IoT focused on the developing communities and thereby, enabled knowledge information for gaining recognition. Our objectives and research questions are out below:

- To identify and classify the range of IoT health applications for people with special needs.
- To explore the privacy and security issues for these IoT applications.
- To identify privacy and security requirements for the IoT applications for people with special needs.

The following are the research questions:

- What are the identities and the classifications of the range of IoT applications for people with special needs?

Copyright © 2022, Infonomics Society | DOI: 10.20533/jitst.2046.3723.2022.0095

- What are the privacy and security issues related to these IoT Applications?

- What are the privacy and security requirements for IoT Applications?

The significance of this study can be investigated along with research data including policy development for practice. It will contribute to the current learning of the Internet of Things. The findings from the study may be useful to healthcare providers by indicating the security and privacy issues in IoT healthcare applications, for users with special needs. This may enhance the efficiency of the healthcare provider. It may also be beneficial to the policymakers in the healthcare sector and specific to the application of the Information Systems.

2. Related works

Based on a patient's unique behavioural, biological, cultural, and social characteristics, the integrated practice of the patient's wellbeing, patient, and healthcare support is referred to being personalized healthcare services. This enables each and every individual to strictly follow the healthcare principles of "the right care for the right person at the right time". These resulted in good data findings for service improvement and satisfaction for people with special needs, making healthcare provisions to be more cost-effective. In fact, sustainable service for people with special needs should focus on preventing and detecting early pathology as well as home care, instead of in a more expensive clinical setting. The latter must include checking the overall well-being of the anticipated needs and making sure that there is compliance with the plans in healthcare advancement. IoT is geared to managing personalized services as well as maintaining a digital identity for every individual.

2.1. Identities and Classifications of IoT Applications Range

A person with special needs who live alone, that is home or not, may control further disabilities and diseases by the use of a monitoring device that has the ability to detect among other problems or a fall with his/her signs (for instance, by use of ECG in the latter case). Any individual, specifically a person with special needs or rather his/her caretaker is able to track their condition progressively [17]. Even active and healthy people can befit their day-to-day activities right from IoT healthcare monitoring Apps. The concept of remote monitoring is another aspect of demanding technology in developing nations. These result in restricted access to the general population, but elites in the community can afford adequate healthcare provisions [20]. However, effective remote monitoring solutions useful to capture special needs' health information records from diverse sensors, have thus, led to application development. This is using complex algorithms to analyse the health data, and whenever required, an enhanced early control mechanism is an important factor for preventing future disabilities or diseases. For instance, the patients that suffer from diabetic diseases who are being treated with digitalis can be monitored by the use of IoT applications on daily basis to control drug intoxication [11].

In the treatment of the institutionalized special needs patients, those that live within the nursing homes or in long-term care facilities, and/or those who stay in hospitals can benefit from the continuous monitoring of their important signs by means of IoT healthcare monitoring applications [7]. Particularly, the solutions of this kind employed the sensory to collect physiological data and to utilize the cloud technologies to analyse and store the data of the patient for security purposes. The analysed information was sent to appropriate caregivers for further review and analysis. In fact, such a continuous automated flow of data that provides an uninterrupted patient monitoring system can improve the quality of care as well as reduces costs. Overview of the Ambient Assisted Living (AAL) aimed at the extent of time required for the independent life for the special needs patient, while at the same time offering confidence that he/she will not be left lonely, in event of the occurrence of health-related issues. The patient can then be helped in his/her usual day-to-day activities with the help of IoT-based AAL solutions [13]. The Ambient Assisted Living (AAL) model is made up of ubiquitous communication systems, ubiquitous sensing, and computing technology for the intelligent user interface. Ubiquitous computing and sensing are integrated into the embedded framework with common day-to-day objects. For instance, the sensors for people with special needs can also be implanted in the patients' bodies (such as the heartbeat stimulus). This is attached to the patient's body or rather embedded within the reach and as a physical object in their homes. The sensors can be networked to get and share information that is received from the sensors, thereby, carrying out the analysis of such data, sending data through cloud computing technology and for easy access to the caretaker or medical professional for further reviews. According to authors in [6], the special needs patient can be monitored by the use of an ECG alarming and monitoring system that is based on android smartphones. There are wearable ECG signal monitoring solutions that rely on Wireless Body Area Networks (WBANs), of the ZigBee communication technology for low power wireless sensors. Various applications of smart technology for network communications can help special needs

Copyright © 2022, Infonomics Society | DOI: 10.20533/jitst.2046.3723.2022.0095

people in making an independent life [2]. The Home Automation System (HAS) provides remote access connection from the Laptop/PC or the smartphone to an AAL system situated in the home of special needs patients. Another proposed IoT-based system provides the management for diabetes therapy in the AAL environment [21].

2.2. Privacy and Security Issues

The sensed data of the special needs patient is often transmitted wirelessly to their respective caregivers (members of the family, nurses, or, doctors). The data transmitted could be tracked while still in the transit process within the wireless channel (Hernández-Ramos et al., 2014). Unfortunately, the adversary can be able to capture the data transmitted within the wireless channel. Therefore, in order to curb these adversaries, a paper in [29] proposed a secure IoT transmission system based on PKI/CA and IBE.

Authors in [1] recommended a chaotic synchronization framework that is meant to solve the security issues related to data transmission within the wireless network. In fact, the proposed framework is made up of two chaotic systems which are kept synchronized in order to realize a comprehensive data recovery of any given encrypted signal. He further recommended a DNS protocol in order to enhance the security related to the Object Naming Service (ONS) questioning process within the tag. This idea helped in solving the issues related to the security problems of the transmitted data in plaintext. In enhancing these security assertions, the authors in [31] have further recommended peer-to-peer (P2P) systems and provided end-to-end security protocols in order to enhance the protection of the transmitted data. This is as well to provide high security for more efficient data transmission at a low-cost rate. The P2P secure communication includes elements such as messenger handler (encapsulation/message de-routing) for the security configuration. This also includes security manager (operations for secure communication).

According to authors in [12] recommended encryption and decryption techniques for accessing data within the cloud. In this regard, the security approach uses a Ciphertext-Policy-Attribute-Based Encryption (CPABE), which is based on an Elliptic Curve Cryptography (ECC), Attribute-Based Encryption (ABE), and Bilinear Maps. The process of encrypting the PHRs rely on the healthcare providers, whereas decrypting PHRs require a set of attributes for the proper access process. Therefore, the Role-Based Access Control (RBAC) cryptographic approaches have so far been developed in order to include the cryptographic nature of the access control and approaches to protect and secure the protected data in the Cloud. In this regard, RBAC enables the data owners to share and manage individual data in the Cloud [12]. The majority of the IoT devices are often small and wirelessly connected. It is therefore essential to ensure that there is maximum protection of the stored data within the IoT devices, as well as providing secure storage tools within the context of the Internet of Things (IoT). This is because expected information of the patient is transmitted and as compared to the traditional architectures, which are at higher risk of the realization of external attacks and hence, obtaining non-authorised access to sensitive information in transit [9].

A systemic approach for IoT security is defined by authors in [19]. According to these scholars, the system is often made up of four elements: the person, the technological ecosystem, the process, and the intelligent object. These elements interact through security factors, which include trust, identification, safety, privacy, responsibility, reliability, and auto-immunity. Also, an edge technology layer can be characterized as a sub layer and each layer contains its own security requirement. According to Said [21], these sub-layers include an image, multimedia, and digital or text. Conventionally, the process of integrating WSNs into an IoT system provides limited energy for computational resources for intelligent applications. Therefore, they are better powered and are also connected through the lossy links causing vulnerability of being attacked by an adversary. In fact, an attacker can deploy some malicious nodes which have the ability to function together and cause damage to any given network. For instance, the physical attack within the nodes can get access to the critical data, such like the critical data, the source code as well as other important data. Another issue is the manner in which to secure the channel between the Internet host and Sensor node [18]. Indeed, WSNs have since been used in various sensitive applications in the IoT for healthcare, therefore, in case the security of the WSNs is compromised, it may lead to loss of resources and also leads to human harm [15]. Hence, there are various security requirements for WSNs which must be considered. For example, the encryption and the calculation metric of the Message Authentication Code (MAC) for information integrity and confidentiality. These are specific to a security protocol for the secure availability and location detection of the device.

The IoT applications have an increasing number of objects such as the sensor nodes, people, medicine, laptop, and many other essential components that enable an efficient operation of resources [4].

However, there are various identification schemes that are recommended for the IoT framework, for example, IPv6, RFID object identifier, IPv4, Near Field Communication Forum

(NFC), and EPC global among others. This identification is normally an attribute that identifies the objects in a more unique way, managing its identities while at the same time considerate of the security awareness of issues for high scalability aspects of the Internet of Things. According to Chun et al., [5], a scalability physical object naming system (PONS) is proposed and has the ability to reuse the existing ontologies as well as the signs that are URL Based on semantic identifiers. In the process, the PONS often construct the semantics and then assign them to the IoT objects. These then lower the risk of the occurrence of security and privacy problems, as with regards to the patients' data.

In the process of authentication, the corroboration involved individual identity, which is the one claimed as the source of information that is received. This is the exact data claimed. In this regard, authentication refers to identity verification. It plays an important role before the establishment of a communication channel between any two given identities. This often confirms an existing mutual trust between various objects and the users. This is by the means of authentication of their identities [5]. Authentication and the access methodology for IoT application is proposed by the authors in [14]. Normally, authentication is gained by mainly defining the simple, efficient key establishment based on the ECC. At the same time, the access control is achieved by the adoption of the Role-based Access Control (RBAC) and these are based on authorization methodology. A cluster-based authentication methodology was proposed by the authors in [33] as well as the authentication that is based on the signal properties of the node that was proposed by the authors in [24]. In addition, Huth et al., [10] proposed a system that offered authenticity and confidentiality of devices for the lightweight key distribution mechanisms. These systems are made up of two technologies, which are Physical Unclonable Function (PUF) and the Physical Key Generation (PKG), which are accessible over given wireless communication channels. These two technologies when combined can improve the physical properties of a communication channel, hence, providing a specific overall improvement of healthcare operations for special needs patients.

2.3. Privacy and Security Requirements

It is important to identify the privacy and security requirements for the IoT application in order to enhance efficiency in healthcare provisions for the special needs. In this regard, the authors in [27] proposed integrated systems and methodology approach that was considered to secure the transmission of information of the WLAN-based IoT applications. The scholars analysed various experiments as well as theoretical analysis in order to evaluate the performance of the recommended integrated security methodology. The scholars indicated that the integrated methodology is an effective and new way of securing the transmission of data of the WLAN that is related to IoT applications. Moreover, the authors in [32] recommended an integrated approach that is able to secure the transmission of data of WLAN-based IoT applications. The scholars performed several experiments as well as theoretical analyses. In order to evaluate the performance of the integrated security and the methodological approach adopted, the integrated methodology is found as an effective paradigm, a new and efficient way to secure the transmitted message of the WLAN that is related to the IoT applications.

Bohan et al., [13] recommended encryption nodes and as designed in IoT which is based on the features of the fingerprints. This is useful to make sure that there is a security of the transmitted data between the nodes, as well as the access permission control for the purpose of sensing node. This is a pair of encryption nodes and the access control nodes which are often assigned based on the Advanced Encryption Standard (AES) algorithm. As the AES security coprocessor of the CC2530 is utilized, the hardware and the software methodologies of the encryption nodes are also presented. The scholars carried out the data transmission experiments between the nodes. It was investigated that the encryption nodes can be achieved for the wireless encryption transmission and for the data nodes, thereby enhancing the security. As for the security issues, the IoT application is expected to face more severe challenges. These are sensitive because of the following reasons. According to Suo et al., [25]:

i. The IoT offers the 'Internet' through the traditional Internet, the mobile network, and also the sensor network among others.

ii. Everything can be connected to the 'Internet'.

iii. Such things can communicate with one another. In this process, therefore, new privacy and security are likely to occur, raising the concerns for research issues on authenticity, confidentiality, as well as the integrity of the information in the IoT applications.

In general terms, the context of information technology and the consideration for security and privacy issues are not new. But the characteristics of various IoT implementations offer unique prospects and new security challenges. Paying attention to these challenges and making sure that security in the IoT services and products should be made a fundamental priority at all times [22]. In fact, the users need to trust the IoT devices, as well as their related data services, as more secure from external vulnerabilities. In particular, this is because such technology become more integrated and pervasive in everyone's life. The significant challenge is related to the integration of user acceptance and the security mechanisms. The users ought to feel that they can control any given information which is related to them rather than feeling that they are being controlled by some observers. This shows that the IoT represents a dark world of privacy, surveillance, and security violations as when the consumer log-in. The attention-grabbing headlines concerning the hacking of internet-connected automobiles, surveillance issues came from the voice recognition features within the "smart" devices such like the televisions, and the privacy fears arising from the potential misuse of the IoT information which have already received substantial public attention. This is "promise vs. peril" and on discussions with the influx of data through popular marketing and media can make the IoT application a complex topic to comprehend. He further explained that the requirements for network security are subdivided into authentication, confidentiality, integrity, and availability. Elements such as constrained resources and heterogeneity have to be considered when applying appropriate IoT architectures. Therefore, the process of interconnecting the IoT devices must have a better confidentiality interface, so that the technologies such as transport layer security and IPSec are put in place in order to meet the requirements [28]. Authenticity indicated that the connection that is established is often with an authenticated entity and the authenticity is incorporated into the integrity of the data, but this process is needed separately, for the purpose of detecting and recovering the failures of various mechanisms such as TLS and TCP suffice for these requirements. According to Vasilomanolakis et al., [28], privacy issues are often considered to be one of the major challenges in the IoT architectures because of the involvement of humans as well as the exceedingly ubiquitous information collection. The privacy issue incorporates a confidential transmission of data in a manner that cannot expose certain undesired properties, such as a person's identity. This requirement is often considered a great challenge since almost every other sensing device gathers personal data and a large amount of such data becomes "Personally Identifiable Information" (PII) when they are combined together and enough to identify a particular person [30].

It is important to pay attention to the 'identity management that is, the management within the IoT of the number of devices as well as the complex relationship existing between the services, devices, users and owners. The approaches of authorization, authentication, incorporating renovation, and non-reputation or accountability are required. In this regard, there are various domain scenarios within the IoT, and authorization solutions.

Steiner et al., [23] gave an assumption on a single domain that encloses the devices, users, owners, and services. There is a need for a new authorization solution that functions with un-trusted devices, allowing delegation of access across domains, and is capable of quick revocation are required. Therefore, the accountability in the management of trust ensures that every action taken is apparently bound to an authentication entity, hence posing another challenge in IoT applications for the special needs. An appropriate system must be able to deal with large amounts of entities, delegating access, the actions that span the organizational domains together with a continuous deviation of information. Robust and resilience against any form of attack and failure is also another noted challenge arising from a large number of devices. Therefore, IoT architecture must offer appropriate mechanisms in order to effectively select things, and services according to their robustness, as well as the transmission paths. According to authors in [26], the recovery and fail-over mechanisms ought to be provided in order to maintain an effective operation that is under attack or failure and also to return to normal operations.

3. Methodology

We adopted a quantitative approach study through the use of Amazon Mechanical Turk (MTurk) [16]. The study targeted the healthcare practitioners dealing mainly with special needs patients in different healthcare centres. The study further used a purposive sampling of four (4) healthcare practitioners in each selected hospital to get the desired number of respondents and this gives a total of 88 respondents. The purposive sampling method helped to obtain different insights about IoT best practices.

Survey questionnaires mounted on Amazon MTurk were tailored toward answering the research questions. All the participants received emails inviting them to participate in the study. The quantitative data from the surveys gathered from the participants was cleaned, coded, transformed, and then analysed by use of the Minitab 19. The analysed data was in form of percentages presented in form of charts for the findings.

4. Results

Our research study investigates security and privacy issues in IoT healthcare applications for special needs users with a sample size of eighty-eight (88) health practitioners. We achieved a 100% response rate because of the professionalism demonstrated by the researchers in carrying out the study. We survey the identities and the classification of the range of IoT applications for special needs patients. The study findings indicated that 42% of the healthcare practitioners agreed that they are using IoT monitoring devices with the ability to detect falls or problems with vital signs for a special needs person living alone (homestead or not) to prevent further diseases or disabilities. The study further sought to determine whether the respondents use appropriate monitoring devices that enabled early prevention, essential in avoiding future disease or disabilities. The study revealed that 35.2% strongly agreed, 36.4 agreed, 11.4 neutral, and 9.1% disagreed with the study findings. The study indicated that the special needs who are living in nursing homes or in long-term care facilities or staying in hospitals benefit from the continuation of their state and vital signs by the IoT healthcare monitoring application with 42.0% agreeing with the study findings. The study also indicated that 33.0% of the respondents agreed that the emerging model of IoT and using IoT for healthcare for the special needs promises much more patient-friendly and highly personalized care as presented below in Figure 1.

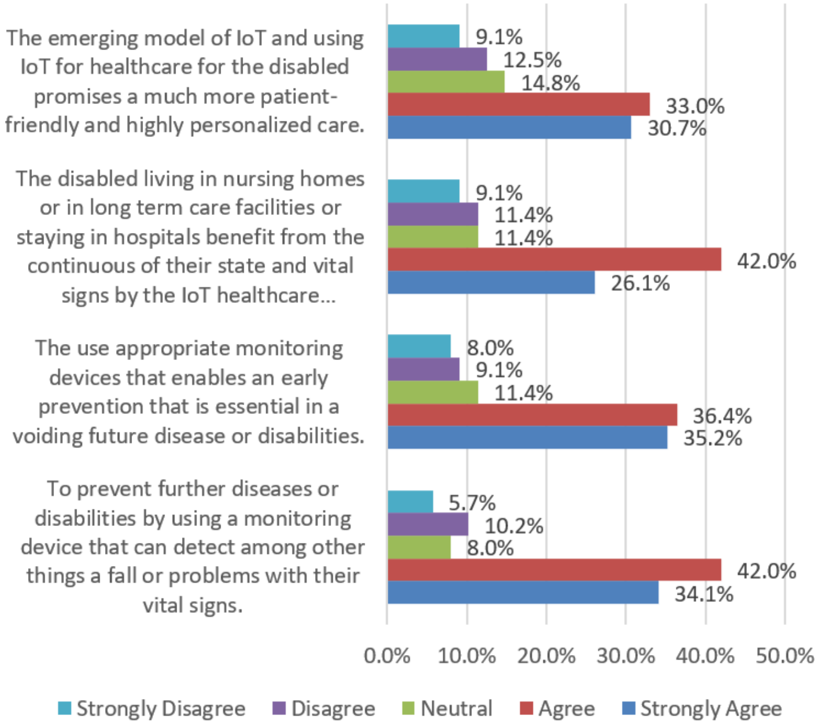

Figure 1. The Identities and the Classifications of the Range of IoT Applications

The study findings revealed that 30.7% strongly agreed, 31.8% agreed, 10.2% were neutral, 12.5% disagreed whereas 14.8% strongly disagreed with the fact that the Personal Health Record (PHRs) is reported to the e-health center directly, and the primary privacy and security issue is to keep the patients' PHRs confidential. The study also showed that 36.4% strongly agreed, 25.0% agreed, 10.2 neutral, 19.3% disagreed whereas 9.1% strongly disagreed that cyber-attack injects false data into the system, causing critical damage in the IoT applications, hence compromising the security of the special needs' personal data. The study further indicated that 35.2% agreed and 19.4 disagreed that data confidentiality can be improved by using Public Key Encryption (KPI) which creates an effective approach to data encryption as it is able to provide high levels of confidence for exchanging information in an insecure environment. Also, the findings from the study indicated that 39.8% agreed as compared to 13.6% disagreed on the fact there is an increased risk of realization of attacks as well as obtaining non-authorized access to the data being transmitted within the IoT application.

The study focused on investigating the privacy and security requirements for IoT applications. The findings revealed that 38.6% of respondents agreed that they often encourage people with special needs to know who owns their health data, while 6.8% of the respondents disagreed with the same idea.

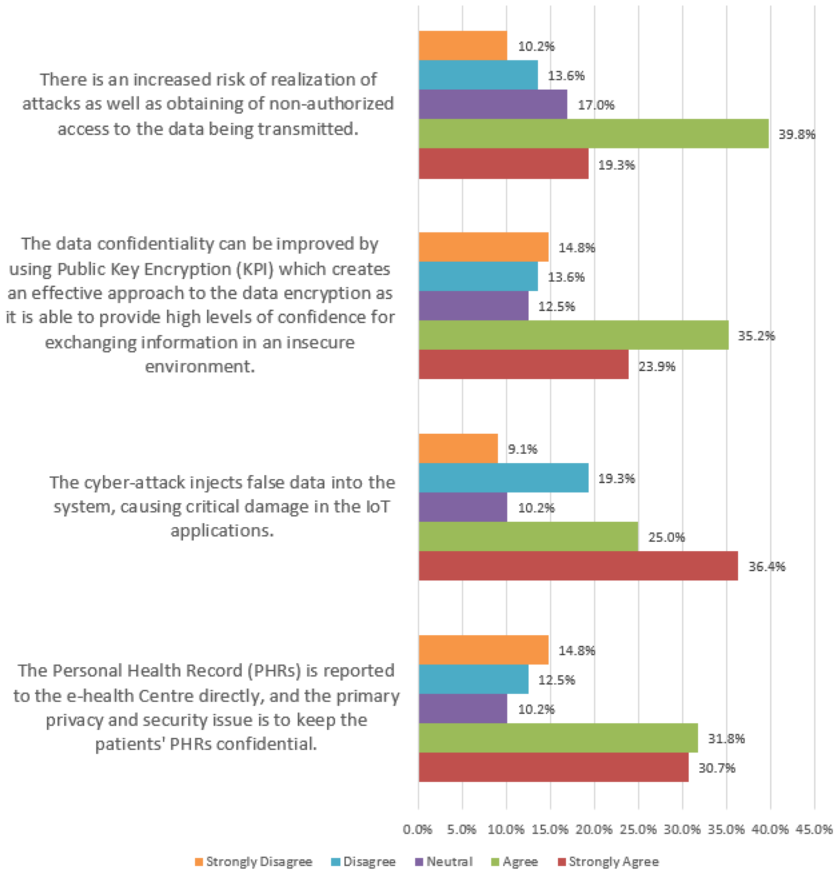

Figure 2. The Privacy and Security Issues Range of IoT Applications

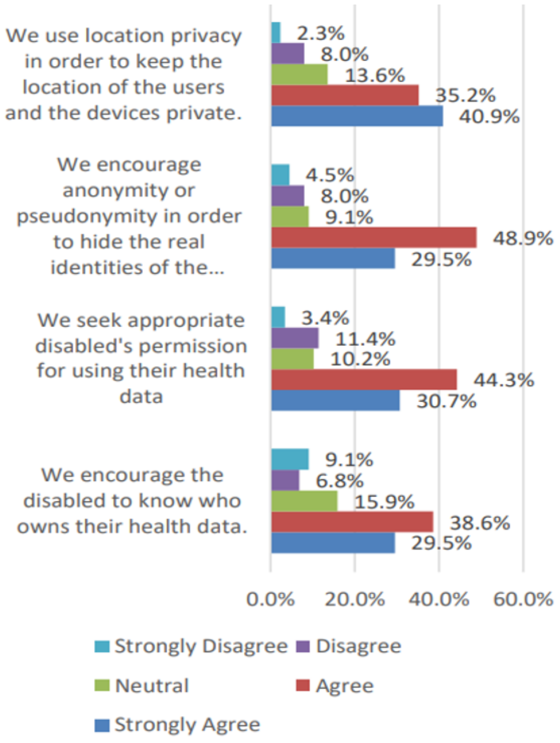

Figure 3. The privacy and security requirements for the IoT Applications

Also, the study findings indicated that 44.3% of the respondents agreed that they seek appropriate special needs permission for using their health data, compared to 11.4% of the respondents who disagreed. Moreover, 48.9% agreed, while 8.0% disagreed that they encourage anonymity in order to hide the real identities of special needs users by means of dividing the identities of the persons into sub-identities. Finally, the study findings indicated that 40.9 strongly agreed that they use location privacy in order to keep the location of the users and the devices private, whereas 8.0% of the respondents disagreed with the same assertion.

5. Conclusion

The IoT monitoring devices with the ability to detect falls or problems with vital signs for a person with special needs living alone (homestead or not) are used to prevent further diseases or disabilities. In fact, the appropriate monitoring devices that enable early prevention are being utilized to avoid future diseases or disabilities. The research came to a conclusion The that the healthcare facilities surveyed indicated that the people with special needs living in nursing homes or in long-term care facilities or staying in hospitals benefit from the continuation of their state and vital signs by the IoT healthcare monitoring application. It also concludes that the emerging model of IoT and using IoT for healthcare for the special needs promises much more patient-friendly and highly personalized care.

The milestone of IoT applications in the healthcare provision for the special needs users such as the use of Personal Health Records (PHRs) directly to the e-health centers, there is an occurrence of security issues such as cyber-attacks injecting false data into the system, causing critical damage in the IoT applications, hence compromising the security of a special needs personal data.

Our survey results show that healthcare practitioners take the privacy and security of special needs patients more seriously than expected. This was revealed by the respondents’ ability to encourage the special needs to know who owns their health data, seek permission from people with special needs before using their data, encourage anonymity as well as use the location privacy in keeping the location of the users and the devices private from any form of cyber hackers.

6. Recommendation

Our research study indicated that the area of the Internet of Things presents a greater promise of providing solutions for healthcare, which include healthcare for special needs persons. However, there is still the existence of some privacy and security challenges within the IoT healthcare applications for special needs users. This was revealed by the findings that cyber-attack injects false data into the system, causing critical damage in the IoT applications, hence compromising the security of the special needs’ personal data. Therefore, we recommended that healthcare facilities should review confidentiality as the intersection of privacy and security. For future research work, we suggested a comparative study on other users apart from people with special needs.

7. References

[1] AL-mawee, W. (2012). *Privacy and Security Issues in IoT Healthcare Applications for the Disabled Users a Survey*. 50. https://scholarworks.wmich.edu/cgi/viewcontent.cgi?article=1661andcontext=masters_theses. (Access Date: 20 November 2021)

[2] Asadullah, M., and Ullah, K. (2017). Smart home automation system using Bluetooth technology. *ICIEECT 2017 - International Conference on Innovations in Electrical Engineering and Computational Technologies 2017, Proceedings*. DOI:10.1109/ICIEECT.2017.7916544.

[3] Bohan, Z., Xu, W., Kaili, Z., and Xueyuan, Z. (2013). Encryption node design in internet of things based on fingerprint features and CC2530. *Proceedings - 2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing, GreenCom-IThings-CPSCom 2013*, 1454–1457. DOI: 10.1109/GREENCOM-ITHINGS-CPSCOM.2013.256.

[4] Che, W., Han, Q., Wang, H., Jing, W., Peng, S., Lin, J., and Sun, G. (2016). *Social Computing*. https://link.springer.com/content/pdf/10.1007/978-981-10-2098-8.pdf. (Access Date: 05 October 2021)

[5] Chun, S., Jung, J., Jin, X., Cho, G., and Lee, K. H. (2014). Poster abstract: Semantically enriched object identification for internet of things. *Proceedings - IEEE International Conference on Distributed Computing in Sensor Systems, DCOSS 2014*, 141–142. DOI:10.1109/DCOSS.2014.64.

[6] Guo, X., Duan, X., Gao, H., Huang, A., and Jiao, B. (2013). An ECG Monitoring and Alarming System Based On Android Smart Phone. *Communications and Network, 05*(03), 584–589. DOI: 10.4236/CN.2013.53B2105.

[7] Hassanalieragh, M., Page, A., Soyata, T., Sharma, G., Aktas, M., Mateos, G., Kantarci, B., and Andreescu, S. (2015). Health Monitoring and Management Using Internet-of-Things (IoT) Sensing with Cloud-Based Processing: Opportunities and Challenges. *Proceedings - 2015 IEEE International Conference on Services Computing, SCC 2015*, 285–292. DOI: 10.1109/SCC.2015.47.

[8] Hernández-Ramos, J. L., Bernal Bernabé, J., and

Skarmeta, A. F. (2014). Towards privacy-preserving data sharing in smart environments. *Proceedings - 2014 8th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, IMIS 2014*, 334–339. DOI: 10.1109/IMIS.2014.44.

[9] Hussain, S., Schaffner, S., and Moseychuck, D. (2009). Applications ofwireless sensor networks and RFID in a smart home environment. *Proceedings of the 7th Annual Communication Networks and Services Research Conference, CNSR 2009*, 153–157. DOI:10.1109/CNSR.2009.32.

[10] Huth, C., Zibuschka, J., Duplys, P., and Güneysu, T. (2015). Securing systems on the Internet of Things via physical properties of devices and communications. *9th Annual IEEE International Systems Conference, SysCon 2015 - Proceedings*, 8–13.DOI:10.1109/SYSCON.2015.7116721. (Access Date: 10 November 2021)

[11] Jara, A., Alcazar, N., Zamora, M., and Skarmeta, A. (2010). Diabetes management and insulin therapy in the hospital and AAL environments based on mobile health. *In: International Workshop on Ambient Assisted Living*. http://eprints.kingston.ac.uk/id/eprint/18306. (Access Date: 05 November 2021)

[12] Jha, R. K., and Khurshid, F. (2015). Performance analysis of enhanced secure socket layer protocol. *2014 International Conference on Communication and Network Technologies, ICCNT 2014, 2015-March*, 319–323. DOI:10.1109/CNT.2014.7062777.

[13] Kouicem, D. E., Bouabdallah, A., and Lakhlef, H. (2018). Internet of things security: A top-down survey. *Computer Networks*, *141*, 199–221.DOI:10.1016/j.comnet.2018.03.012

[14] Liu, J., Xiao, Y., and Chen, C. L. P. (2012). Authentication and access control in the Internet of things. *Proceedings - 32nd IEEE International Conference on Distributed Computing Systems Workshops, ICDCSW 2012*, 588–592. DOI:10.1109/ICDCSW.2012.23.

[15] Mainetti, L., Patrono, L., and Vilei, A. (2011). Evolution of wireless sensor networks towards the Internet of Things: A survey. *2011 International Conference on Software, Telecommunications and Computer Networks, SoftCOM 2011*, 16–21.

[16] Paolacci, G., Chandler, J., and Ipeirotis, P. G. (2010). Running experiments on Amazon mechanical turk. *Judgment and Decision Making*, *5*(5), 411–419.

[17] Rajabzadeh, A., Manashty, A. R., and Jahromi, Z. F. (2010). *A Mobile Application for Smart House Remote Control System*. 80–86. http://arxiv.org/abs/1009.5557. (Access Date: 12 November 2022)

[18] Reyna, A., Martín, C., Chen, J., Soler, E., and Díaz, M. (2018). On blockchain and its integration with IoT. Challenges and opportunities. *Future Generation Computer Systems*, *88*(2018), 173–190. DOI:10.1016/J.FUTURE.2018.05.046.

[19] Riahi, A., Challal, Y., Natalizio, E., Chtourou, Z., and Bouabdallah, A. (2013). A systemic approach for IoT security. *Proceedings - IEEE International Conference on Distributed Computing in Sensor Systems, DCoSS 2013*, 351–355. DOI:10.1109/DCOSS.2013.78.

[20] Rohokale, V. M., Prasad, N. R., and Prasad, R. (2011). A cooperative Internet of Things (IoT) for rural healthcare monitoring and control. *2011 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace and Electronic Systems Technology, Wireless VITAE 2011*. DOI:10.1109/WIRELESSVITAE.2011.5940920.

[21] Said, O. (2013). *Development of an Innovative Internet of Things Security System*. *10*(6), 155–161.

[22] Schäfer, G., and Rossberg, M. (2016). *Security in fixed and wireless networks*. https://books.google.co.uk/books?hl=enandlr=andid=rEMxBwAAQBAJandoi=fndandpg=PR13anddq=Schäfer,+G.+and+Rossberg,+M.,+2016.+Security+in+fixed+and+wireless+networksandots=JJtezc2RRcandsig=2FQjlqz-UYTIvVhU4sdUZoiZfig. (Access Date: 10 November 2021)

[23] Steiner, J., Neuman, B., and Schiller, J. (1988). Kerberos: An Authentication Service for Open Network Systems. *USENIX Winter*, 191–202. http://www.cse.nd.edu/~dthain/courses/cse598z/fall2004/papers/kerberos.pdf. (Access Date: 10 October 2021)

[24] Suen, T., and Yasinsac, A. (2005). Ad hoc network security: Peer identification and authentication using signal properties. *Proceedings from the 6th Annual IEEE System, Man and Cybernetics Information Assurance Workshop, SMC 2005*, *2005*, 432–433.DOI:10.1109/IAW.2005.1495987.

[25] Suo, H., Wan, J., Zou, C., and Liu, J. (2012). Security in the internet of things: A review. *Proceedings - 2012 International Conference on Computer Science and Electronics Engineering, ICCSEE 2012*, *3*, 648–651. DOI:10.1109/ICCSEE.2012.373.

[26] Tesoriero, R., Gallud, J. A., Lozano, M. D., and Penichet, V. M. R. (2009). Tracking autonomous entities using RFID technology. *IEEE Transactions on Consumer Electronics*, *55*(2), 650–655.DOI:10.1109/TCE.2009.5174435.

[27] Ullah, I., Zeadally, S., Amin, N. U., Asghar Khan, M., and Khattak, H. (2021). Lightweight and provable secure cross-domain access control scheme for internet of things (IoT) based wireless body area networks (WBAN). *Microprocessors and Microsystems*, *81*(August 2020), 103477. DOI:10.1016/J.MICPRO.2020.103477.

[28] Vasilomanolakis, E., Daubert, J., Luthra, M., Gazis, V., Wiesmaier, A., and Kikiras, P. (2016). On the Security and Privacy of Internet of Things Architectures and Systems. *Proceedings - 2015 International Workshop on Secure Internet of Things, SIoT 2015*, 49–57. DOI:10.1109/SIOT.2015.9.

[29] Yang, P., Wu, W., Moniri, M., and Chibelushi, C. C. (2013). Efficient object localization using sparsely distributed passive RFID tags. *IEEE Transactions on Industrial Electronics*, *60*(12), 5914–5924. DOI:10.1109/TIE.2012.2230596.

[30] Ye, N., Zhu, Y., Wang, R. C., Malekian, R., and Lin, Q. M. (2014). An efficient authentication and access control scheme for perception layer of internet of things. *Applied Mathematics and Information Sciences*, *8*(4), 1617–1624. DOI:10.12785/AMIS/080416.

[31] Zhang, H., and Zhang, T. (2015). Short Paper: "A peer to peer security protocol for the internet of things": Secure communication for the sensiblethings platform. *2015 18th International Conference on Intelligence in Next Generation Networks, ICIN 2015*, 154–156. DOI:10.1109/ICIN.2015.7073825.

[32] Zhu, Q., Wang, R., Chen, Q., Liu, Y., and Qin, W. (2010). IOT gateway: Bridging wireless sensor networks into Internet of Things. *Proceedings - IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, EUC 2010*, 347–352. DOI:10.1109/EUC.2010.58.

[33] Zou, Y., Zhu, J., Wang, X., and Hanzo, L. (2016). A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends. *Proceedings of the IEEE, 104*(9), 1727–1765.DOI:10.1109/JPROC.2016.2558521.

| DOI: 10.20533/jitst.2046.3723.2022.0095