Identification of Information Security Controls for Fitness Wearable Manufacturers

Sophia Moganedi[1,2(✉)] and Dalenca Pottas[1]

[1] Nelson Mandela University, Port Elizabeth, South Africa
s209078565@mandela.ac.za, Dalenca.Pottas@Mandela.ac.za
[2] CSIR, Pretoria, South Africa
smoganedi@csir.co.za

Abstract. Statista suggests that there would be 368.2 million wearables shipped globally in 2020 with a projection of 500 million by 2024. These predictions are becoming a reality considering the fast growing of Intent of Things (IoT) domain. These wearables come in different forms, shapes, and sizes. The existence of fitness wearables encourages people to participate in a healthy lifestyle through tracking of health and fitness-related activities. The functionality of these devices includes gathering, processing, transmitting, and storing user data. However, these devices carry with them vulnerabilities that can negatively affect the security and privacy of a user. Therefore, the primary objective of this study is to identify security controls to mitigate the vulnerabilities that affect fitness wearables from a security and privacy perspective. However, to identify these security controls, the researcher firstly identifies the vulnerabilities affecting these fitness wearables. This study executed a methodology in two stages. The first stage conducted a literature review to identify the vulnerabilities affecting fitness wearables and related components within the ecosystem of fitness wearables. The second state follows a systematic analysis approach to identify security controls for the fitness wearable manufacturers to mitigate these vulnerabilities. The final output of this study indicates the security complexities surrounding the fitness wearables by presenting the study limitations.

Keywords: Fitness wearables · Vulnerabilities · Security controls · Internet of Things

1 Introduction

Fitness wearables are a part of the bigger interconnected world of the Internet of Things (IoT) [1, 2]. A fitness wearable is defined as a wireless sensor that is embedded in a device and can be worn on the body by the user [3]. This device incorporates a variety of capabilities including gathering, processing, transmitting, and storing user data [4, 5]. Fitness wearables are manufactured and put into the market to encourage users to participate in self-care through excises and health monitoring efforts [6].

The popularity of these fitness wearables is influenced by the increasing interest in self-tracking notion, where users can track and monitor their daily fitness-related

H. Venter et al. (Eds.): ISSA 2020, CCIS 1339, pp. 112–128, 2020.
https://doi.org/10.1007/978-3-030-66039-0_8

activities [7–10]. However, the growing popularity of fitness wearables and their use poses security concerns [11]. These security concerns around the fitness wearables are not surprising, given the fact that these devices gather real-time data that tends to be at a personal and detailed level [12]. Hence, the discussions around personal privacy increase these concerns as users lose control of the data privacy [13].

The remainder of this paper is organised as follows: Sect. 2 presents the methodology employed in this study. Section 3 presents the findings and the output of this study, which is the information security controls for the fitness wearable manufacturers to mitigate the vulnerabilities affecting the fitness wearables ecosystem. Section 4 presents the limitation of this study and make recommendations for future research based on the limitations discussed. The limitations opens an opportunity to further this study. Section 4 concludes the study and highlight the contribution made by this study.

2 Methodology

This section discusses the methodology followed by this study. This study executed the methodology in two stages to achieve the identified objective/s. In Stage 1, the researcher conducted a literature review to identify vulnerabilities that affect fitness wearables from a security and privacy perspective. Stage 2 employed a systematic analysis approach to identify security controls for the fitness wearable manufacturers to mitigate the vulnerabilities. Subsections 2.1 and Subsect. 2.2 provide a more detailed discussion on each of these stages.

2.1 Stage 1: Literature Review

This subsection discusses the literature review followed to identify the vulnerabilities affecting fitness wearables from a security and privacy perspective.

Firstly, the researcher adopted the Open Web Application Security Project (OWASP) Internet of Things (IoT) 2018 project as a baseline to identify the vulnerabilities that exist in the IoT domain. This project started in 2014 to assist developers, manufacturers, and users to make better security decisions when designing and using IoT systems [14]. The OWASP IoT project released the top 10 IoT vulnerabilities that the broader IoT academic community endorses. Hence, the adoption by this study.

The literature identified the "Lack of Erasing Personal Data" as an additional vulnerability that is significant to the IoT domain and yet not on the OWASP list [15]. Therefore, this study will be focusing on eleven (11) vulnerabilities. The conducting of the literature review was to find earlier and recent published work that presents these vulnerabilities from the fitness wearable context. This study conducted comparison analysis of three source to understand the approach followed to identify vulnerabilities and security controls to mitigate those vulnerabilities. The findings from this analysis indicates that each of the sources follows the risk assessment approach which is the well-known approach for identifying vulnerabilities and security controls in an organizational context.

Furthermore, through the literature, the researcher identifies the components that these vulnerabilities affect within the fitness wearable ecosystem. Figure 1 below depicts the fitness wearables ecosystem to demonstrate the fitness wearables and their related

components for the full fitness tracking and monitoring functionality. This study notes that there are various mode of communication and additional functionalities found in different fitness wearable brands and such include Apple smart watch that offers the fitness functionality and inbuilt cellular access. However, this study is focusing on general fitness wearables that offer fitness functionality and not on a specific brand or additional functionality within the wearables. A letter as presented in Fig. 1 represents each component in the ecosystem.

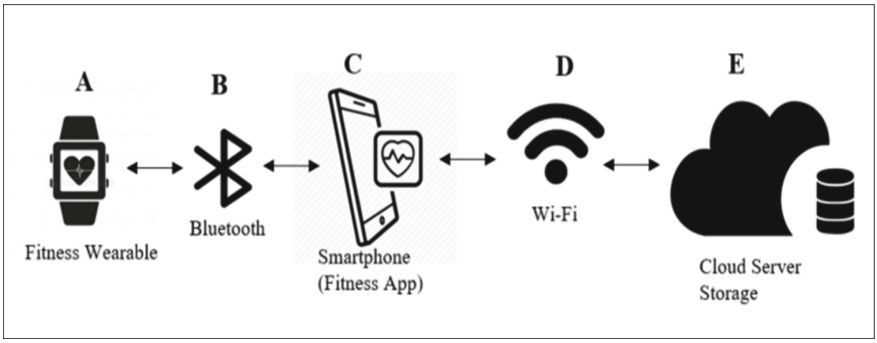

Fig. 1. Fitness wearables ecosystem

2.2 Stage-2: Analysis Approach

This subsection discusses the analysis approach followed in this study. The purpose of this analysis is to identify a set of security controls for the fitness wearable manufacturers to mitigate the vulnerabilities affecting the fitness wearable ecosystem. Therefore, the identification of these security controls is done by determining the relevance of the security controls in the context of this study. In addition to determining the relevance, the identification aims to select critical security controls that will provide a high impact when implemented. These security controls are for fitness wearable manufacturers to mitigate the list of these vulnerabilities identified through the OWASP IoT Project.

The execution of this analysis was in a two-phased approach. This study used the NIST SP800-53 revision 5 to identify the security controls for mitigating the list of vulnerabilities identified. Figure 2 below depicts a high-level process followed in each phase. Each phase presents the steps involved. The subsections below presents a more detailed discussion on each the phases.

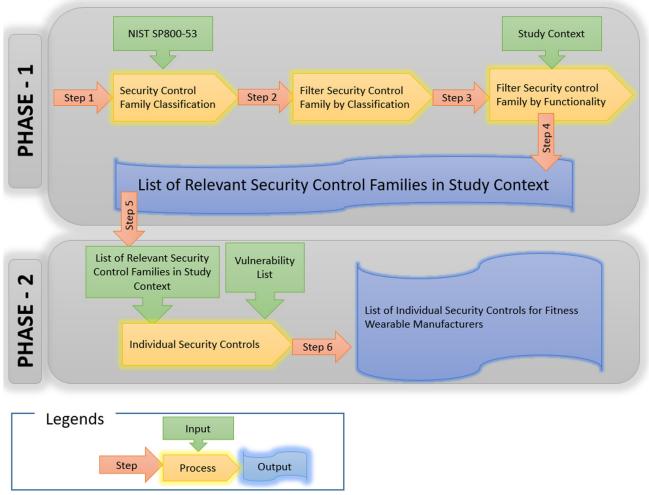

Fig. 2. High-Level Two-phased APPROACH

Phase 1 Analysis

Phase 1 aims to identify the relevant security control families from the NIST. The NIST SP800-53 Rev 5 has 20 security control families and each consists of a set of security controls relating to the security functionality of that family. The main goal of Phase 1 is to identify the security control families that are relevant in the context of this study. However, Subsection A and Subsection B presents the two levels of relevance in the context of this study.

A. *Security Control Family Classification Filtering*

The first level of relevance focuses on whether the technical and operational aspect of the security control families are possible for implementation. The technical aspect focuses on the implementation of security measures before the fitness wearable and its related components are in the public market. While the operational aspect focuses on security measures to ensure that the fitness wearable and related components are secure when used in the market and their security posture can always be improved. As a result, the researcher adopted the classification of security control family from NIST SP800-53 revision 1. The reason for adopting this classification from the earliest revision 1 (Rev 1) of NIST is simply because the latest revision (Rev 5) of NIST does not provide such classification. Furthermore, the earliest revision (Rev 1) provides only seventeen (17) security control families; therefore, the researcher had to classify the remaining security control families that did not exist in Rev 1. The additional classification emerges from the overall functionality of the security control family.

The NIST provides three classifications for the security control families. These classifications are namely: Management, Operational, and Technical. The selection of the security control families that are relevant in the context of this study is on two classifications, which are technical and operational. As a result, this study excludes security

control family classified as management from this analysis. The researcher started with twenty (20) security control families, and after filtering out all the security control families falling under the management classification, the researcher identified sixteen (16) security control families (Table 1).

Table 1. NIST SP800-53 security control families

Selected	Security control family name	Classification	Description/Functionality
✓	Access Control	Technical	Facilitates the permitted activities of legitimate users' access systems to preventing unauthorised access to system resources
✓	Awareness and Training	Operational	Implements security awareness and training to information system users
✓	Audit and Accountability	Technical	Determines audit events, ensure recording of events, and ensure reliability and protection.
	Assessment, Authorization, and Monitoring	Management	Assesses the current security posture of an organization as well as assessing the potential security risks.
✓	Configuration Management	Operational	Ensures critical assets are properly configured at all times and configuration changes are only restricted to authorised users
✓	Contingency Planning	Operational	Ensures the continuity of critical operations and restoration of information systems during compromises
✓	Identification and Authentication	Technical	Ensures claimed user identity and rights to access the information system
✓	Incident Management	Operational	Implement an organised approach to address and manage the aftermath of security incidents.

(*continued*)

Table 1. (*continued*)

Selected	Security control family name	Classification	Description/Functionality
✓	Maintenance	Operational	Ensures sustainability in the capability of information systems to provide the designated services
✓	Media Protection	Operational	Ensures the security of digital and non-digital media
✓	Physical and Environment Protection	Operational	Aim to prevent the loss or damage to information assets and interruption to the business activities from unauthorized access
	Planning	Management	Determines security requirements and identify security controls. It includes describing how security controls will meet those security requirements
✓	Personnel Security	Operational	Ensures that individuals within an organisation are not posing security risks to the organisation and the information systems
	Risk Assessment	Management	Identifies and assesses the security risks in an organisation and information systems. This is to determine the likelihood and the impact of security harm
	System and Services Acquisition	Management	Focuses on new system design methods, major changes in existing systems, support, resource allocation, system documentation, and system minimum requirements
✓	System and Communication Protection	Technical	Focuses on the protection of information systems and the communication processes
✓	System and Information Integrity	Operational	Aim to protect information systems, communication, and preserve the integrity of information

(*continued*)

Table 1. (*continued*)

Selected	Security control family name	Classification	Description/Functionality
✓	Program Management	Operational	Focuses on managing security-related programs in the organisation
✓	PII Processing and Transparency	Operational	Focuses on the processing of PII, which includes gathering, processing, transmitting, storing, disclosure, and disposal of such information
✓	Supply Chain Risk Management	Operational	Focuses on managing day to day risks that come with the supply chain in an organisation

B. *Security Control Family Functionality*

The functionality of a particular security control family in the context of this study determines the second level of relevance. These criteria determines the inclusion or exclusion of the security control families. The focus was on filtering out security control families that are not relevant in the context of this study addressing fitness wearables and their related components. The previous subsection identified relevant security control families based on the technical and operational classifications. However, some of these security control families were irrelevant in the context of this study.

The **Awareness and Training** security control family focuses on training users in an organisational context and as a result, this security control family is irrelevant in the context of this study.

Another example of a security control family that falls under a relevant classification but is irrelevant in the context of this study is the **Physical and Environmental Protection** security control family. This security control family focuses on ensuring the protection of an organisation in terms of actual physical security to protect the physical infrastructure. This is relevant in the context of an organisation but is irrelevant in the context of fitness wearables and their related components. Table 2 presents the excluded security control families. These exclusions were because these security control families are applicable in an organisational context but not in the context of this study. The exclusion of a security control family excludes the individual security controls within that family.

At the end of Phase 1, the researcher had six security control families that are relevant in the context of this study addressing the fitness wearables and their related components. Table 3 presents these security control families.

Phase 2 Analysis

In Phase 2, the researcher focused on identifying individual security controls within security control families for the fitness wearable manufacturers to mitigate the list of vulnerabilities.

Table 2. Filtering security controls: based on study context

Security Control Family Name	Classification
Access Control	Technical
Awareness and Training	Operational
Audit and Accountability	Technical
Configuration Management	Operational
Contingency Planning	Operational
Identification and Authentication	Technical
Incident Management	Operational
Maintenance	Operational
Media Protection	Operational
Physical and Environment Protection	Operational
Personnel Security	Operational
System and Communication Protection	Technical
System and Information Integrity	Operational
Program Management	Operational
PII Processing and Transparency	Operational
Supply Chain Risk Management	Operational

Table 3. Relevant security control families for study context

Security control family name	Classification
Access Control	Technical
Audit and Accountability	Technical
Identification and Authentication	Technical
System and Communication Protection	Technical
System and Information Integrity	Operational
PII Processing and Transparency	Operational

For this phase, the researcher took the list of vulnerabilities affecting various components within the fitness wearables ecosystem as an input into this Phase 2 analysis. In addition to the list of vulnerabilities, the researcher also took the six (6) security control families that were an output in Phase 1 to be an input in Phase 2. The purpose of using these two outputs as an input in this Phase 2 is to identify relevant security controls for the fitness wearable manufactures to mitigate these vulnerabilities.

This phase executes a more detailed analysis by going through each security control family and identifying individual security controls that are relevant in the context of the vulnerabilities and the manufacturer can use to mitigate these vulnerabilities. Furthermore, the identification of the security controls for the mitigation of the vulnerabilities

is in three levels. The first level identifies security controls that will mitigate the vulnerability; the second level identifies security controls that will strengthen the security control identified for the first level. Finally, the third level identifies security controls as reactive measure in case of an incident. This structure presents Security control, Related Control, and Control enhancements. According to NIST, the "Security Control" as the main security control and recommends related controls to strengthen the main security control. These related controls are controls from other security control families. Lastly, the control enhancements are within the main security controls, which NIST recommends to strengthen the main Security controls. However, for this study, the adoption of the presentation structure is different. The "related controls" are not necessarily those recommended by the NIST, but they fit the context of this study and the same applies to the "control enhancements".

Table 4 presents the identification of individual security controls. The study presents one example of vulnerability with mitigation security controls and the affected components. The components A, B, C and E are those presented in Fig. 1. The summary later is the study presents the rest of the vulnerabilities with their identified security controls.

3 Findings and Presentation

This section presents the main contribution of this study, which is the result of the methodology discussed in the previous section.

3.1 Vulnerabilities Affecting Fitness Wearables

This section presents a brief discussion and presents the vulnerabilities that affect fitness wearables and related components. The purpose of this discussion to illustrate how each vulnerability as described by the OWASP IoT project affects the fitness wearable and related components. The literature supports and validate the applicability of these vulnerabilities in the context of the fitness wearables.

Table 5 below presents the list of vulnerabilities adopted from the OWASP IoT project and a mapping of each vulnerability to the components it affects. A letter as seen in Fig. 2 above represents each affected component. However, this study excludes the component labeled "D" from this analysis as its security requirements are not the responsibility of the fitness wearable manufacture.

3.2 Identification of Security Controls

There are several internationally known security control standards, frameworks, and guidelines that provide a huge list of security controls that can be used to mitigate security risks [56]. These security control standards, frameworks, and guidelines include the International Organization for Standardization and International Electrotechnical Commission (ISO/IEC), Control Objective for Information and Related Technology (COBIT), and National Institute of Standards and Technology (NIST), just to name a few. However, for this study, the researcher selected the NIST as a baseline to identify

Table 4. Identification of security controls for insecure data transfer snd storage

Components	Vulnerability	Security control family	Security controls	Reason for selection/Recommendation reason
A, B, C, E	Insecure Data Transfer and Storage	SC	[SC-8] Transmission Confidentiality and Integrity	**SC-8** recommends the implementation of an encryption mechanism to protect the confidentiality and integrity of information as it is being transmitted [16]. Encryption ensures the security of the information [17]
			[SC-20] Protection of Information at Rest	**SC-28** recommends the implementation of an encryption mechanism to protect the integrity of information at rest. This will prevent unauthorized disclosure or modification of information [16]. The encryption technique has proven to increase the level of data protection for assuring integrity and availability [18]
			[SC-13] Cryptographic Protection	**SC-18** supports different security solutions that include the protection of information. The encryption technique help to maintain the confidentiality, integrity, and availability of the data [19].
			[SC-23] Session Authenticity	**SC-23** focuses on protecting the authenticity of communication sessions. Fitness wearable ecosystem allow data to travel from one point to another, protection of communication session ensures confidentiality and integrity

Table 5. List of vulnerabilities affecting fitness wearables and related components

Components	Vulnerabilities	Cause/Impact of the vulnerability
A, C, E	Weak, Guessable, or Hardcoded Passwords	Unchangeable credentials that are shipped with the devices which include a backdoor to firmware or software can be used to grand unauthorised access to the device [14, 20–27]
A, C, E	Insecure Network Services	Unneeded and insecure services can compromise the confidentiality, integrity, and availability of the data [14, 28–30]
A, B, C, E	Insecure Ecosystem Interface	Any insecure component within the infrastructure can be used to compromise the entire ecosystem [14, 31–34]
A, B, C	Lack of Secure Update Mechanisms	Lack of the ability to update the devices in a secure manner. Security updates are not validated and encrypted [14, 31, 35]
A, C	Use of Insecure or Outdated Components	Devices operating from unpatched or outdated software components and libraries lead to an easy compromise. [32, 36–39]
A, B, C, E	Insufficient Privacy Protection	Storing of user's data insecurely, improperly or without the consent of the user in any components [2, 27, 48, 40–47]
A, B, C, E	Insecure Data Transfer and Storage	Lack of encryption or access control to data at any point within the ecosystem [27, 42, 53].
A, C	Lack of Device Management	Devices deployed lack the security support in an operational environment [14]
A, C	Insecure Default Settings	Devices shipped with default settings can be easily reconfigured for malicious purposes [33, 51, 52]
A, C	Lack of Physical Hardening	Lack of physical hardening measures will enable a potential malicious attacker to gain sensitive data [23, 38, 53]
A, C, E	Lack of Erasing Personal Data	There is a lack of the ability to allow for wiping off the gathered data in case of theft, loss or reselling of the device [15, 58]

security controls that will be relevant in the context of this study, which addresses the fitness wearables and related components.

The purpose of selecting the NIST standard as a baseline is because, this standard is a combination of several internationally recognized standards and best practices which include the ISO/IEC 27002 [57]. The specific NIST standard referred to by this study is NIST Special Publication 800-53. This publication presents security and privacy controls that are published for Federal Information Systems and Organisation [58].

Although the researcher identified one standard to use for identification these security controls, this standard presents a long list of security controls to select from, and selecting the best set of security controls is a challenge [59]. The identification of the most effective security controls has always been problematic and many approaches and techniques have developed over time to do this in the most effective manner possible [59,[60]. Barnard and Von Solms [59], acknowledges the existence of baseline manuals, however, they argue that these baseline manuals provide a little guidance on how to determine the best set of security controls to provide adequate security. Therefore, with this little guidance provided in the baseline manuals, there is a high potential of selecting irrelevant security controls and excluding the relevant ones [59, 61].

The literature recognizes the use of various mechanisms to identify a set of security controls to provide adequate security against security risks. However, such mechanisms are relevant in the context of implementing adequate security in an organisation. Hence, such mechanisms are irrelevant in the context of this study, which addresses the fitness wearables.

Table 6 below presents a summary of all the identified security controls for fitness wearable manufactures to mitigate each vulnerability.

Table 6. Summary of the identified security controls

Components	Vulnerabilities	Security controls	Related security control	Reactive security control	NIST supportive documents
A, C, E	Weak, Guessable, or Hardcoded Passwords	[IA-5], [SI-3], [SI-7]	[AC-7], [IA-9]		NIST SP800-118
A, C, E	Insecure Network Services	[SC-13], [SC-23]	[SC-28] [SC-8]		NIST SP800-123
A, B, C, E	Insecure Ecosystem Interface	[IA-9], [IA-3], [SC-8], [SC-13], [SC-23], [SC-28]	[IA-5]		NIST SP800-183

(*continued*)

Table 6. (*continued*)

Components	Vulnerabilities	Security controls	Related security control	Reactive security control	NIST supportive documents
A, B, C	Lack of Secure Update Mechanisms	[SI-2], [SI-3], [SI-7]	[SC-13], [SC-13]		NIST SP800-123
A, C	Use of Insecure or Outdated Components	[SI-2], [SI-3], [SI-7]	[SC-13]		NIST SP800-123
A, B, C, E	Insufficient Privacy Protection	[PT-2], [PT-3], [PT-4], [PT-5] [PT-6], [SC-28], [SC-42]	[SC-13], [SI-18]	[AU-10], [AU-9]	NIST SP800-122
A, B, C, E	Insecure Data Transfer and Storage	[SC-8], [SC-28], [SC-13]	[SI-18]		NIST SP800-111
A, C	Lack of Device Management	[SI-2]	[SC-13], [SI-3], [SI-7]		NIST SP800-124
A, C	Insecure Default Settings	[IA-5]	[SC-13]		NIST SP800-123
A, C	Lack of Physical Hardening	[IA-5], [AC-11] [SI-2]	[IA-11]		NIST SP800-123
A, C, E	Lack of Erasing Personal Data	[AC-4], [SI-19]	[SI-21]	[AU-3], [AU-10] [AU-11], [AU-8] [AU-9]	NIST SP800-88

4 Limitation and Future Research

This study identified a set of security controls to mitigate the list of vulnerabilities adopted from the OWASP IoT project. Through the NIST SP800-53, the researcher identifies the security controls that were relevant in the context of this study. However, the limitation of this study is the evaluation process of these security controls. Through the literature, it was evident that selecting the best set of security controls can be a great challenge and there is a potential to include unnecessary security controls while excluding the important ones. This is due to the lack of guidelines for selecting the best security controls. Therefore, for future research purposes, this study foresees a need to

conduct further research that will propose and develop an evaluation process or model or framework to evaluate these sets of security controls for completeness, accuracy, and to verify if they will be implementable in the context of fitness wearables.

5 Conclusion

The fast growing market of fitness wearables has changed the way people are viewing their health habits. These devices motivate people to track and monitor their health habits daily. However, the fast growing of these fitness wearables has shown security and privacy to be an issue to this day. This study identified vulnerabilities and security controls for the mitigation of these vulnerabilities. The identification of security controls will enable the fitness wearable manufacturers to mitigate the most common vulnerabilities that affect the fitness wearables and entire IoT domain. Furthermore, these security controls identified simplifies the selection and implementation. Each security control mitigates a particular vulnerability, and the fitness wearable component affected.

References

1. Wei, J.: How wearables intersect with the cloud and the internet of things: Considerations for the developers of wearables. In: IEEE Consumer Electronics Magazine, pp. 53–56 (2014)
2. Zhou, W., Piramuthu, S.: Security/privacy of wearable fitness tracking IoT devices. In: 2014 9th Iberian Conference Information systems and Technologies (CISTI) (2014)
3. Britton, K.E.: IoT big data: consumer wearables data privacy and security. Landside A Publ. ABA Sect. Intellect. Prop. Law **8**(2), 1–8 (2015)
4. Bond-myatt, C.: Health wearables. In: Apps & Information Protection (2015)
5. Hiremath, S., Yang, G., Mankodiya, K.: Wearable internet of things : concept, architectural components and promises for person-centered healthcare. In: 2014 4th International Conference on Wireless Mobile Communication and Healthcare - "Transforming Healthcare Through Innovations in Mobile and Wireless Technologies" (MOBIHEALTH), pp. 304–307 (2014)
6. Bender, C.G., Hoffstot, J.C., Combs, B.T., Hooshangi, S., Cappos, J.: Measuring the fitness of fitness trackers. In: 2017 IEEE Sensors Applications Symposium (SAS) (2017)
7. Das, A.K., Pathak, P.H., Chuah, C., Mohapatra, P.: Uncovering privacy leakage in BLE network traffic of wearable fitness trackers. In: HotMobile'16 Proceedings of the 17th International Workshop on Mobile Computing Systems and Applications, pp. 99–104 (2016)
8. Michaelis, J.R., et al.: Describing the user experience of wearable fitness technology through online product reviews. In: Proceedings of the Human Factors Ergonomics Society 2016 Annual Meeting 1073, vol. 60, no. 1, pp. 1073–1077 (2016)
9. Lunney, A., Cunningham, N.R., Eastin, M.S.: Wearable fitness technology: A structural investigation into acceptance and perceived fitness outcomes. Comput. Human Behav. **65**, 114–120 (2016)
10. Anzaldo, D.: Wearable sports technology – market landscape and computer SoC trends. In: 2015 International SoC Design Conference (ISOCC), pp. 217–218 (2015)
11. Popat, K.A., Sharma, P.: Wearable computer applications a future perspective. Int. J. Eng. Innov. Technol. **3**(1), 213–217 (2013)
12. Martini, P.: A secure approach to wearable technology. Netw. Secur. **2014**(10), 15–17 (2014)

13. Huang, K.-C., Hsu, J.-F.: Balance between privacy protecting and selling user data of wearable devices. In: 14th International Telecommunications Society (ITS) Asia-Pacific Regional Conference: "Mapping ICT into Transformation for the Next Information Society" (2017)
14. OWASP, "OWASP Internet of Things Top 10 2018" (2018)
15. Bhattacharya, S.: The 10 Internet of Things Security Vulnerabilities (2019). https://resources.infosecinstitute.com/the-top-ten-iot-vulnerabilities/#gref. [Accessed: 20-Jun-2019]
16. Thambiraja, E., Ramesh, G., Umarani, R.: A survey on various most common encryption techniques. Int. J. Adv. Res. Comput. Sci. Softw. Eng. **2**(7), 226–233 (2012)
17. Justin, J.M., Manimurugan, S.: A survey on various encryption techniques. Int. J. Soft Comput. Eng. **2**(1), 2231–2307 (2012)
18. Albugmi, A., Alassafi, M.O., Walters, R., Wills, G.: Data security in cloud computing. In: 5th International Conference on Future Generation Communication Technologies, FGCT 2016, pp. 55–59 (2016)
19. Kaur, G.: Efficient data confidentiality and portability in cloud storage. Int. J. Adv. Res. Comput. Sci. **9**(2), 40 (2018)
20. Barcena, M.B., Wueest, C.: Insecurity in the Internet of Things (2015)
21. Lindqvist, U., Neumann, P.G.: Inside risks the future of the internet of things. Commun. ACM **60**(2), 26–30 (2017)
22. Mendoza, F., et al.: Assessment of fitness tracker security: a case of study. In: Proceedings, UCAmI 2018 The 12th International Conference on Ubiquitous Computing and Ambient Intelligence (UCAmI 2018), vol. 2, p. 1235 (2018)
23. Ching, K.W., Singh, M.M.: Wearable technology devices security and privacy vulnerability analysis. Int. J. Netw. Secur. Its Appl. **8**(3), 19–30 (2016)
24. Mnjama, J., Foster, G., Irwin, B.: A privacy and security threat assessment framework for consumer health wearables. In: Information Security for South Africa (ISSA) 2017 (2017)
25. Cisneros, R., Bliss, D., Garcia, M.: Password auditing applications. J. Comput. Sci. Coll. **21**(4), 196–202 (2006)
26. Li, S., Romdhani, I., Buchanan, W.: Password pattern and vulnerability analysis for web and mobile applications. ZTE Commun. **14**(S0), 32–36 (2016)
27. Saini, H., Saini, A.: Security mechanisms at different levels in cloud infrastructure. Int. J. Comput. Appl. **108**(2), 1–6 (2014)
28. Fredric, P.: Top 10 IoT Vulnerabilties. NetworkWorld (2019). https://www.networkworld.com/article/3332032/top-10-iot-vulnerabilities.html. Accessed 09 Jun 2019
29. Drolet, M.: 7 potential security concerns for wearables (2016)
30. Hilts, A., Parsons, C., Knockel, J.: Every step you fake: a comparative analysis of fitness tracker privacy and security (2016)
31. Classen, J., Wegemer, D., Patras, P., Spink, T., Hollick, M.: Anatomy of a vulnerable fitness tracking system: dissecting the fitbit cloud, app, and firmware. Proc. ACM Interact. Mob. Wearable Ubiq. Technol. **2**(1), 1–24 (2018)
32. Vaughn, G.: IoT Security Best Practices (2019)
33. Pathak, A.K.: Security challenges in Internet of Things (IoT). Int. J. Adv. Res. Comput. Sci. Softw. Eng. **7**(6), 648–652 (2017)
34. Goyal, R., Dragoni, N., Spognardi, A.: Mind the tracker you wear - a security analysis of wearable health trackers. In: Proceeding SAC'16 Proceedings of the 31st Annual ACM Symposium on Applied Computing, pp. 131–136 (2016)
35. Airehrour, D., Gutierrez, J., Ray, S.K.: Secure routing for internet of things: a survey. J. Netw. Comput. Appl. **66**, 198–213 (2016)
36. Karthik: List of IoT Vulnerabilities (2019). http://secureapplication.org/blog/blogReadMore.php?id=1230. Accessed 17 June 2019
37. SecurityInstituteInformation.in, "Security Challenges in securing IoT," (2019). http://informationsecurityinstitute.in/security-challenges-in-securing-iot/. Accessed 09 June 2019

38. Rahman, A.F.A., Daud, M., Mohamad, M.Z.: Securing sensor to cloud ecosystem using internet of things (IoT) security framework. In: ICC'16 Proceedings of the International Conference on Internet of things and Cloud Computing, pp. 1–5 (2016)
39. Rieck, J.: Attacks on Fitness Trackers Revisited : A Case-Study of Unfit Firmware Security, pp. 33–44 (2016)
40. Radomirovi´c, S.: Towards a model for security and privacy in the internet of things. In: 1st International workshop on the Security of the Internet of Things (2010)
41. Wicks, P., Chiauzzi, E.: 'Trust but verify' - five approaches to ensure safe medical apps. BMC Med. **13**(1), 1–5 (2015)
42. Arias, O., Wurm, J.: Privacy and security in Internet of Things and wearable devices. IEEE Trans. Multi-Scale Comput. Syst. **1**(2), 99–109 (2015)
43. Barcena, M., Wueest, C., Lau, H.: How safe is your quantified self? (2014)
44. Kumar, M.: Security issues and privacy concerns in the implementation of wireless body area network. In: Proceedings - 2014 13th International Conference on Information Technology, ICIT 2014, pp. 58–62 (2014)
45. Bouhenguel, R., Mahgoub, I., Mohammad, I.: Bluetooth security in wearable computing applications. In: 2008 International Symposium on High Capacity Optical Networks and Enabling Technologies, HONET 2008, pp. 182–186 (2008)
46. Alfaiate, J., Fonseca, J.: Bluetooth security analysis for mobile phones. In: Iberian Conference on Information Systems and Technologies, CISTI (2012)
47. Hale, M.L., Ellis, D., Gamble, R., Waler, C., Lin, J.: Secu wear: an open source, multi-component hardware/software platform for exploring wearable security. In: Proceedings - 2015 IEEE 3rd International Conference on Mobile Services, MS 2015, pp. 97–104 (2015)
48. Musolesi, M.: Big mobile data mining: Good or evil? IEEE Internet Comput. **18**(1), 78–81 (2014)
49. Segura Anaya, L.H., Alsadoon, A., Costadopoulos, N., Prasad, P.W.C.: Ethical implications of user perceptions of wearable devices. Sci. Eng. Ethics **24**(1), 1–28 (2017). https://doi.org/10.1007/s11948-017-9872-8
50. Addonizio, G.: The privacy risks surrounding consumer health and fitness apps, associated wearable devices, and HIPAA's limitations (2017_
51. Algan, B.: Continuous Security Validation. ISACA Now BLog (2019). https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2019/continuous-security-validation. [Accessed: 18-May-2020]
52. Williams, P.A.H., McCauley, V.: Always connected: the security challenges of the healthcare Internet of Things. In: 2016 IEEE 3rd World Forum on Internet of Things, WF-IoT 2016, pp. 30–35 (2017)
53. Mahinderjit, M.S., Ching, K.W., Manaf, A.A.:A novel out-of-band biometrics authentication scheme for wearable devices. Int. J. Comput. Appl., 1–13 (2018)
54. Messerges, T.S., Dabbish, E.A., Sloan, R.H.: Examining smart-card security under the threat of power analysis attacks. IEEE Trans. Comput. **51**(5), 541–552 (2002)
55. R. Adhikari, D. Richards, and K. Scott, "Security and privacy issues related to the use of mobile health apps," in *Proceedings of the 25th Australasian Conference on Information Systems, ACIS 2014*, 2014
56. Breier, J., Hudec, L.: On selecting critical security controls. In: 2013 International Conference on Availability, Reliability and Security, pp. 582–588 (2013)
57. Huijben, K.: A lightweight, flexible evaluation framework to measure the ISO 27002 information security controls," Radboud University (2014)
58. Lord, N.: What is NIST SP 800–53? Definition and Tips for NIST SP 800-53 Compliance (2018). https://digitalguardian.com/blog/what-nist-sp-800-53-definition-and-tips-nist-sp-800-53-compliance. Accessed 28 June 2019

59. Barnard, L., Von Solms, R.: A formalized approach to the effective selection and evaluation of information security controls. Comput. Secur. **19**(2), 185–194 (2000)
60. Hasheminejad, S.M.H., Jalili, S.: Selecting proper security patterns using text classification. In: Proceedings - 2009 International Conference on Computational Intelligence and Software Engineering, CiSE 2009, pp. 1–5 (2009)
61. Otero, A.R.: An information security control assessment methodology for organizations. Nova Southeastern Univerrsity (2014)