Security In Intellegent Home

Mario Garcia and Yeshihareg Hailu

Southeast Missouri State University

Cape Girardeau, Missouri, USA

Abstract

As human needs of intelligent aid are growing higher and higher, People's lives are becoming more dependent on various technologies. One of the fastest-growing Internet of Things' (IoT') technologies, Intelligent Home is becoming more involved in people's life. Controlling and monitoring home appliances remotely with justa single click or touch of a smart device or a laptop is becoming a common practice. This is possible through IoT likeIntelligent/Smart Home System. Since home appliances are required to be connected to the internetto makethem accessible and monitored remotely, it is obvious that they are vulnerable for cyber-attack. Thus, security and privacy are the main concerns when implementing smart home systems. This paper has discussed and analyzedsecurity constraints, identify major potential security risks, security requirements, the nature of attacks, the security threats at each layer of IoT architecture on smart home and finally the design of secured smart system.

1. Introduction

The internet of Things (IoT) refers to the network of devices that are embedded with sensor, software, and other technologies for the purpose of connecting and exchanging data with other devices and system over the internet connection. Therefore, smart homes are benefiting from these IoT technology. It is easy to handle the home lights, switches, doors, cameras, and other electric appliances using a laptop or smart phones with just a single touch.

People can control homeappliances from the officeor anywhere else using their laptop or smartphone. Sensors are used in almost all theconnected house appliances. This paper focuses on security issues of intelligent home systems and proposes a solution that secure an intelligent home system. Layer based security solutions which include physical protection, implementing smart home firewalls, hub, encryption, and cryptographic strategies are proposed.

2. Problem Description

2.1. Security Requirements

Security and privacy are the main concerns during the implementation of IoT as devices in the IoT system need to be connected to internet in order to be accessed remotely.

The major security requirements of IoT are Confidentiality, Authenticity, Integrity and Availability [1][2].Violationofanyoftheserequirementscancauseadisasterinthesystem. Figure 1 illustrates the data security requirements of IOT.

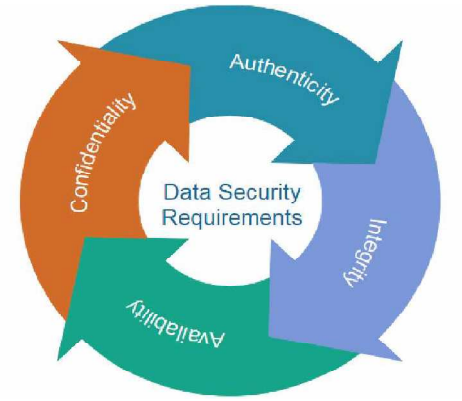

Fig. 1. Security Requirements(Reference: 2020 International Conference on Computing and Information Technology, University of Tabuk,Kingdom of Saudi Arabia.Volume: 01, Issue: ICCIT- 1441, Page No.: 258 - 263, 9th & 10th Sep. 2020, IoT: Security Challenges and Issues of Smart Homes/Cities, Figure2)

2.2. Security Challenges

Fulfilling the above-mentioned security requirements during the implementation of intelligent interconnected systems such as smart home always faces challenges. The major challenges could be Limited devices capabilities[1], Data Management[14], Radio Frequency Identification (RFID)Tags Vulnerability[14], Diverse Communication Protocols[12], Cascading Effect[13][14], Autonomic control[1][12][14] and Physical liability.

Different layers of IoT network architecture are vulnerable for different types of security attacks. Thus, Security attacks can be broadly classified as Attack based on IoT architecture and RFID and WSN Classifications [1] [12] [2][15][16][17][18]. Figure2 illustrates general and layer-based security issues and attacks of IoT architecture.

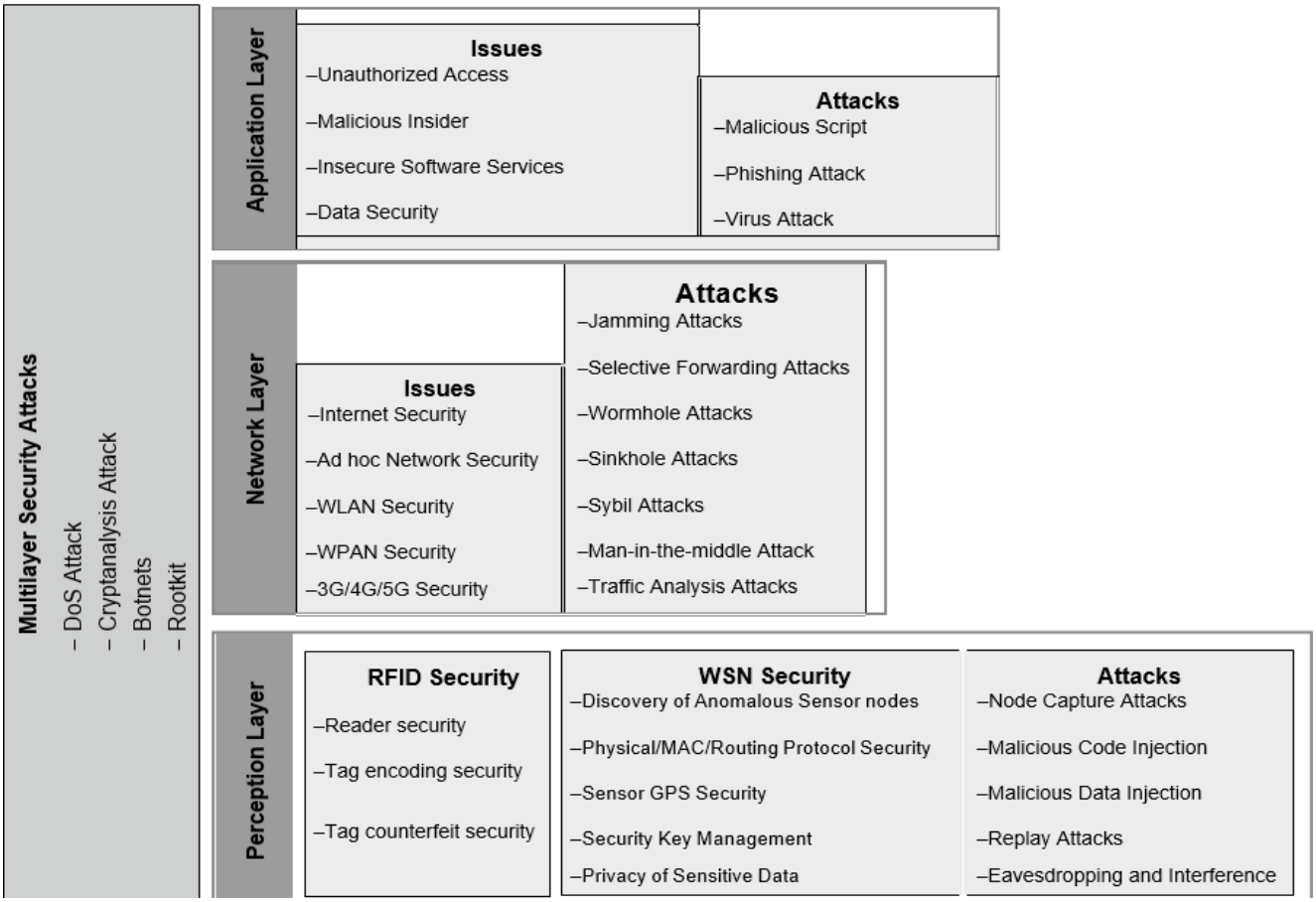

Figure2 IoTarchitectureandsecurityissues/attack(Reference:IoT Security, 8.5.1 Perception Layer Security, Figure 8.3, Book Chapter)

2.3. Security Threats and Constraints

When planning to implement IoT systems such as smart home, security is always a major concern. Thecapability of accessing house appliances through the smart home system exposes cyber-attack andunauthorized access of personal information and data by third party who has special interest about onextracting one's personal data. The IoT system security attack can be classified into main categories as Physical Attack, network attack, Software Attack and EncryptionAttack. IPcamerahackingthroughbufferoverflowattacks[3], aDistributedDenial□of□Service(DDoS)attack[4], BotnetattacktohackIoTdevices[5], SQLinjectionattacks and cross□site scripting attack[6] are the major potential security threats that IoT is exposed to.

Resource constraints, along with the above-mentioned and other types of IoT threats, are the other security problems that IoT system suffering from [7]. Due to lower hardware size of device of IoT, thin operating system installed in some types of IoT devices, and the characteristics of IoT devices which are (heterogeneity, scalability, presence of multiple communication protocols and portability) are barriers of implementing expensive security algorithm, robust communication protocol, dynamic security patches, and conventional security protocol respectively in IoT system.

As mentioned above, Smart Home System is possible through connection of several digital appliances

with theuseof IoT. Mostly,enduserscommunicatethroughsmartphonestocontrol home appliances. Attackers can easily compromise the users' privacy and security of homedevices and related data [8]. Table 1 illustrates security issues of smarthomesintermsofthevulnerabilitiesassociatedwithfewsmarthomedevices.

Table1. Smart home devices, functionality, and associated security threats.(Reference:IoT Security, 8.7.1 Smart Home Security,Figure8.1, Book Chapter)

Smart device	**Functionality**	**Potential security threat**
Smart Lock	● Lock/unlock without physical key ●Lock/unlock through mobile device or web interface ● Automatically lock after a specified period of time ● Alarms ringing on forced entry or break□ins	● Lock/unlock by attackers to enter/exit from home ● Changing of lock/unlock password remotely ● Turn off the alarm in case of break□in
Smart Bulb	●Light bulb controllable remotely through mobile application ● Scheduling of turning on/off and coloring of light bulbs	● Control the turning on and off behavior of lights ● Overload power system by turning on unnecessary lights
Voice Automated Device	● Turn devices on or off based on voice Commands	● Steal private credentials from voice data ● Issue voice commands to order unwanted stocks by voice commands ● Steal voice data as credentials for use in other voice command systems
Smart Vacuum Cleaner	● Automatically map home layout and conduct automatic and scheduled cleaning in dry or wet mopping modes	● Monitor room activities and stealing of home layout
Smart Refrigerator	● Create grocery list and send order to shops through the Internet ● Set expiration data and send related alerts to residents ● Suggest recipes based on available ingredients	● Send order with modified grocery list ● Modify expiration date of food items in refrigerator or ruin food items by changing temperature
Smart Toilet	● Allow users to remotely set water temperature and pressure ● Sense and adjust right water amount to clean itself or for flushing wastes ● Notify residents about needed supplies (e.g. toilet paper, soap, and air freshener)	● Turn water tap on and leave water flowing without any need ● Remotely control smart toilet's lid and flush nozzles

Since smart home systems are controlled and monitored via smart mobile phone Apps like Geolocation Services that can track one's location, the privacy and security of the smart home users are compromised[9]. Oneoftherisksofusingthistechnologyisthatusersarenotawarethattheir location is being tracked by a third party.Geolocationandmapping are Appscommonly used by criminal [10].

The other risk is using Wi-Fi. All Wi-Fi clientstestedwerevulnerabletotheattackagainstthegroupkeyhandshake [11].Figure3showsSmart Home objects internet connection via Wi-Fi.

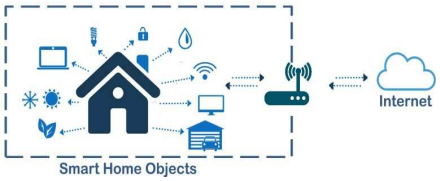

Figure3 Smart Home internet connection via Wi-Fi.(Reference:2018 IEEE 6th International Conference on Future Internet of Things and Cloud, creating smart environments: Analysis of improving security on smart homes)

These limitations,the risks, threats, and constraints of IoT system discussed above, make implementation of secured IoT system a challenge. Thus, having Efficient Cryptography Techniques, Interoperability, ScalableSolution, PrivacyProtection, ResiliencetoPhysicalAttacks, AutonomousControl, and CloudSecurity are challenges that need to be consideredduring designing security mechanisms toprevent risksandthreatsofpersonalinformationmisuse.

3. Proposed Solution

For the above-mentioned security attacks, the respective counter measures are described in brief below.

3.1. **Physical Attack**:

ToProtect the IoT from Physical Attack,useofthe correct safety efforts on IoT devices is essential. This is best done by utilizingequipment-basedsecurity. HardwaresecuritycanalsobeusedtoauthenticatedeviceID.This meansthataseriesofsecuritymeasurescanbeputbetweentheserverandthe device itselftoestablishtheauthenticityofthatdevice. Human□based physical attacksand natural disaster threats are to be addressed and managed as follows:

- Securesensor design
- Securesensordeployment
- Secureinfrastructure
- Efficientuserauthenticationapproach(biometricorsmartcard)toimplementforlegitimateaccesst ophysicaldevicesandconfidentialinformation.
- Implementefficientaccessibilitycontrolmechanisms.
- Efficientimplementationoftrustmanagement
- Efficienthardwarefailurerecoveryschemes

3.2. **Network Attack:**

Thefirst and the main measure to protect from network attack is to make sure that only

required ports areexposedandavailable.Afterthatpreparetheservicesthatmustnotbevulnerabletobufferoverflowandfuzzingattacks. The other proposed solution to close the security hole of smart home systemsis usingfirewall both at software and hardware level. A firewall is a network security device or software that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules. Figure 4 illustrates the smart home secured architecture using firewall.

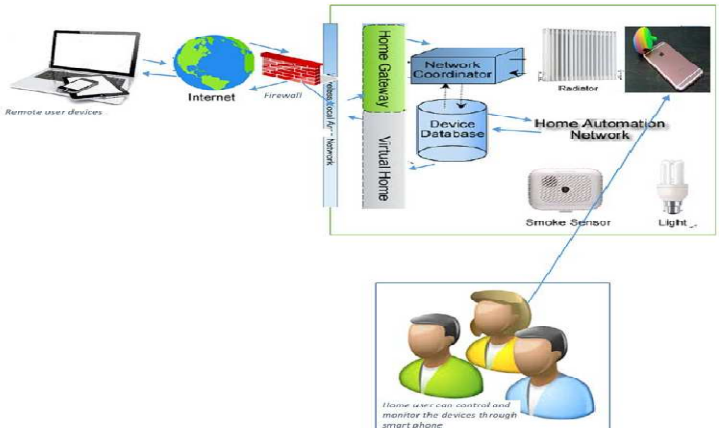

Fig.4 Secure architecture for Smart Home(Reference: 2018 Fifth International Conference on Software Defined Systems (SDS), An Approach to Secure Smart Homes in Cyber-Physical Systems/Internet-of-Things, Figure2)

The other important proposed solution is using smart home hub[26] network devices. The proposed smart home hub hardware device can connect the appliances which are nodes of the smart home network and provides an intrusion detection system that controls and monitors where and how the information should be exchanged. The device may also include computing resources that send a warning message when unauthorized access is detected.

After this, the detailed security measure that should be taken to protect network attack is listed below.

- Renaming the router instead of keeping the name provided by the manufacturer.
- Use strong encryption method for Wi-Fi router setting:
- Alter the default username and passwords**.**
- SettingupaguestnetworkinWi-Fi access to prevent the privatedata in the network from being accessed by intruders.
- Disabling the features whichare alreadyenabled by the manufacturer likeremoteaccessifitisnotrequired.
- Changethedefault privacy and security settings ofthedevices which are provided by the manufacturer.
- Software updating regularly.
- Avoid connecting to public Wi-Fi networks.
- Two step verifications to easily understand whether the communication iswiththegenuinesender.
- Use strong, unique passwords for Wi-Fi networks and device accounts:StronganduniquepasswordsareessentialforWi-Finetworksanddevices.

- DisableTelnet loginand use SSH [19] wherepossible.
- AuditingoftheIoTdevicesatregularintervals.
- Haveanindividualuseraccountforeachemployee.
- Limitedaccessibility**:** Grantinglimitedauthority to employees.
- Passwordsshouldbechangedatregularintervals.
- Trainedcybersecurityprofessionalsareneeded.
- Usepropercertificationforaccessingtheinternet.

In addition to above mentioned, important technique to prevent the IoT from network attack is connecting the IoT devices to the0Gnetworkbecausethisisadedicated,lowpowerwirelessnetworkspecially designed for sending small and critical messages from any IoT device to theInternet[20]. The0Gnetworkdoes not supportnetwork-initiateddownlinks,itonlysupportsdevice-initiateddownlinks.Thesepropertiesmakethe0Gnetworknotsusceptibletonetworkattackers.

3.3. **SoftwareAttacks:**

This attack, which affects the application layer atthetopof thethree□layerof IoTarchitecture can be overcome bycontrols the legitimacy of authorized users(through authentication and access control systems), protection of application software,OS, and end□user interfaces through the utilization of high□level programming languageswhich assists to avoid insecure programming. Regular updating and installation of antivirus and antispyware software, installingupdatesthatarerequiredbytheoperatingsystemandapplication software, taking a backupofbusinessdataandinformation, Controlling Physicalaccesstothe systemandnetworkcomponents.

3.4. **EncryptionAttack:**

Thepublickeyinfrastructure(PKI) has ensured that the encryption of data must be done through asymmetric and symmetricencryptionprocesses.

3.5. **CryptographicStrategies:**

Cryptographicalgorithmssuchassymmetrickeycrypto-graphic algorithms, and advanced encryption standard (AES) [21], Secure hash calculations (SHA) [22], Diffie Hellman (DH) [24],Revest Shamir Adelman(RSA) [23] ,Elliptic curve cryptography (ECC), and Key Administration are utilized tosafeguard information secrecy. Even though the mentioned cryptography algorithms are secure and efficient but that they require more CPU power and consume more battery power. For this reason, they are not a feasible way to verify IoT devices, so there has been an emergence of new cryptographic calculations or advances the existing ones for battery operated IoT devices.

3.6. **AuthenticationandAccessControl:**

TheIoTconcentratesonamachinetomachine(M2M)methodofcorrespondence[25].Table 3 summarizes the security attacks with counter measures on different layers of the IoT network architecture.

Table 2 Summery of attacks on different layers of IoT with counter measures.(Reference: Security Attacks in Internet of Things RajitNair1,*, Preeti Sharma2, and Dileep Kumar Singh3 table14.2)

User side layer or application layer	Code injection, data access and authentication	IDS diglossia [19]
	Virus, worms, malware attacks, phishing attacks, spyware	Anti-virus, firewall, IDS [14], secure application code, educating users to use complex passwords, access control mechanisms, key agreement, log monitoring, file and database monitoring tools, anti-malwares to protect applications against malwares.
Support layer security	DoS, wormhole, black hole, interoperability and portability, business continuity and disasterrecovery, cloud audit, virtualization security	IDS designed for IoT [15] Lightweight encryptiontechniques like CLEFIA [22] andPRESENT [17], need forcontinuous cloud audits,implementation of cloud securityalliance standards, securevirtualization technologies, tenant's separation, storageencryption for user's dataconfidentiality and integrity
Network layer security	Side-channel attacks: Sybil	Malicious firmware/software detection [24], randomized delay [19], intentionally generated noise [20], balancing Hamming weights [21].
	Battery-draining, sleep deprivation attack, routing attacks, node jamming in WSN	Policy-based mechanisms and intrusion detection systems (IDSs)
	RFID tag	Personal RFID firewall [22], anonymous tag, lightweight cryptographic protocol [23]
Physical layer or edge layer security	Node tampering, fake node, malicious code injection, side channel attack,	Authentication with encryption techniques. Physical security in nodes vicinity, need for lightweight encryption algorithms for constrained nodes,
	Mass node authentication, protecting sensor data	authentication and access control mechanisms for devices, anti
	Physical damage	It is better to keep some physical protection for the devices.

4. Conclusion

This paper hasintroduced IoT and smart home which is one of the implementations of IoT in the introduction section. The problem description sectionidentified Security Requirements, Challenges, and discussed them in detail. In addition to that, different security Risks, threats and IoT device constraints in terms of hardware, software, and communication protocols which are barrier for implementation of standard security guard are investigated. Cyber-attack and the respective security issues at each layer of IoThave been discussed. Finally, in the proposed Solution section,

solutions to fulfill the identified security requirements and to protect the smart home system from the mentioned cyberattack such as physical attack, network attack, software attack, encryption attack, and others are proposed and discussed.

Reference

[1] P. I. R. Grammatikis, Radoglou, P. G. Sarigiannidis, and I. D. Moscholios, "Securing the Internet of Things: challenges, threats and solutions", Internet of Things, Vol. 5, pp. 41-70, 2018.
[2] E. Leloglu, "A review of security concerns in Internet of Things", J Comp. Comm., Vol. 5, No.1, pp.121-136, 2016.
[3] Chirgwin, R.(2016). Get pwned: Web CCTV cams can be hijacked by single HTTP requestserverbuffer overflow equals remote control. www.theregister.co.uk/2016/11/30/iot_cameras_compromised_by_long_url.
[4] Hilton, S. (2016). Dyn analysis summary of Friday October 21 attack. https://dyn.com/ blog/dyn□analysis□summary□of□friday□october□21□attack.
[5] Antonakakis, M., April, T., and Bailey, M. (2017). Understanding the mirai botnet. In: 26th USENIX Security Symposium, 1093–1110. USENIX Association.
[6] Ling, Z., Liu K., Xu Y. et al. (2018). IoT security: an end□to□end view and case study. arXiv preprint arXiv:1805.05853,2018.
[7] Hossain, M.M., Fotouhi, M., and Hasan, R. (2015). Towards an analysis of security issues, challenges, and open problems in the internet of things. In: IEEE World Congress on Services, 21–28. IEEE. 13 Aman, M.N., Sikdar, B., Chua, K.C. et al. (2018). Low power data integrity in IoT systems.
[8] Chang, Z. (2019). IoT device security locking out risks and threats to smart homes. In: Trend Micro Research. https://documents.trendmicro.com/assets/white_papers/IoTDevice□ Security.pdf.
[9]S. Tanimoto, R. Kinno, M. Iwashita, T. Kobayashi, H. Sato, and A. Kanai, "Risk assessment of home gateway/smart meter in smart grid service," Proc. - 2016 5th IIAI Int. Congr. Adv. Appl. Informatics, IIAI-AAI 2016, pp. 1126–1131, 2016.
[10]W. Xi, "[8] Research on IoT Privacy Security Risks," 2016 Int. Conf. Ind. Informatics - Comput. Technol. Intell. Technol. Ind. Inf. Integr., pp. 259–262, 2016.
[11]M. Vanhoef, F. Piessens, and K. U. Leuven, "Key Reinstallation Attacks : Forcing Nonce Reuse in WPA2," Comput. Commun. Secur., 2017.
[12] C. Lee, et al, "Securing smart home: Technologies, security challenges, and security requirements", 2014 IEEE Conference on Communications and Network Security, IEEE, pp.67-72, 2014.
[13] B. Ali, and A. Awad, "Cyber and physical security vulnerability assessment for IoT-based smart homes", Sensors, Vol. 18, No. 3, 2018.
[14] E. Leloglu, "A review of security concerns in Internet of Things", J Comp. Comm., Vol. 5, No.1, pp.121-136, 2016.
[15] T. Braun, et al, "Security and privacy challenges in smart cities", Sustainable cities and society, Vol. 39, pp. 499-507, 2018.

[16] L. K. Bysani, and A. K. Turuk, “A survey on selective forwarding attack in wireless sensor networks”, 2011 International Conference on Devices and Communications (ICDeCom), IEEE, pp. 1-5, 2011.
[17] O. E. Mouaatamid, M. Lahmer, and M. Belkasmi, “Internet of Things Security: Layered classification of attacks and possible Countermeasures”, Electro. J. Info. Tech., Vol. 9, 2016.
[18] H. A. Khattak, et al, “Perception layer security in Internet of Things”, Future Generation Computer Systems, Vol. 100, pp.144164, 2019.
[19] SSH Communications Security. SSH Protocol – Secure Remote Login and FileTransfer | SSH.COM. ssh.com. 2017.
[20] Mir MM ud in, Kumar S. Evolution of Mobile Wireless Technology from 0G to5G. Int J Comput Sci Inf Technol. 2015.
[21]Heron S. Advanced Encryption Standard (AES). NetwSecur. 2009.
[22]RSA Public Key Cryptography Algorithm A Review. Int J Sci Technol Res.2017.
[23] Gueron S, Johnson S, Walker J. SHA-512/256. In: Proceedings - 2011 8th International Conference on Information Technology: New Generations, ITNG 2011. 2011.
[24] McCurley KS. A key distribution system equivalent to factoring. J Cryptol. 1988.
[25] Ali A, Shah GA, Farooq MO, Ghani U. Technologies and challenges in developing Machine-to-Machine applications: A survey. Journal of Network and
[26]A. Wilde, O. Ojuroye, and R. Torah, “Prototyping a voice- controlled smart home hub wirelessly integrated with a wearable device,” Proc. Int. Conf. Sens. Technol. ICST, vol. 2016–March, pp. 71–75, 2016.