A COMPARATIVE STUDY ON AUTHENTICATION VULNERABILITIES AND SECURITY ISSUES IN WEARABLE DEVICES

V Vamsi Krishna[1], Y Rupa[2] ,G Koushik[3] ,T Varun[4] ,B V Kiranmayee[5] and Karnam Akhil[6*]

[1,2,3,4,5,6] VNR Vignana Jyoti Institute of Engineering and Technology
Hyderabad, India
akhilresearch18@gmail.com

Abstract. Wearable gadgets are technological devices with limited computational power that can be worn by users, providing them with information and seamless access to their master devices. It allows gadgets to connect and exchange data, enabling various tasks to be completed online. Wearables have revolutionized human health monitoring, capturing data like blood-oxygen levels, step counts, and GPS tracking, which is stored in the cloud. However, additional user identification methods like PIN entering are cumbersome and prone to security breaches like assaults involving visual hacking. In response to these concerns, various advanced authentication techniques have emerged. In our study, we thoroughly examined different user validation mechanisms intending to provide thorough direction for further study in wearable technology domain.

Keywords: Wearable Devices, Authentication, Security, Google Glass, Fitbit, Smart Watch, Internet of Things (IoT), Bluetooth, Layered Adaptive Security.

1 Introduction

Wearable Tech has seen a significant growth in the recent years. Smartwatches and fitness bands are two examples of commercial wearables as shown in Figure 1 that are being widely used. According to a recent report [1] the wearable market is predicted to grow three times as much by 2022, at $57,653 million, then it did in 2016 ($19,633 million). Six key characteristics—non-monopolizing, non-restrictive, observable, attentive, controllable, and communicative—define wearable technology [2]. However, WT faces a few difficulties, including power consumption, design limitations, communication capacity and security issues [3]. Basic data related to heartbeat, data on temperature and humidity, the user's location, and his daily routines are just a few examples of the information that may be gathered which can impose some Privacy issues. Additionally, given that some of these devices have always-on network access and have a variety of usage styles, these devices may be the target of malware, which would increase the likelihood of

C. Kiran Mai et al. (eds.), *Proceedings of the Fourth International Conference on Advances in Computer Engineering and Communication Systems (ICACECS 2023)*, Atlantis Highlights in Computer Sciences 18,
https://doi.org/10.2991/978-94-6463-314-6_11

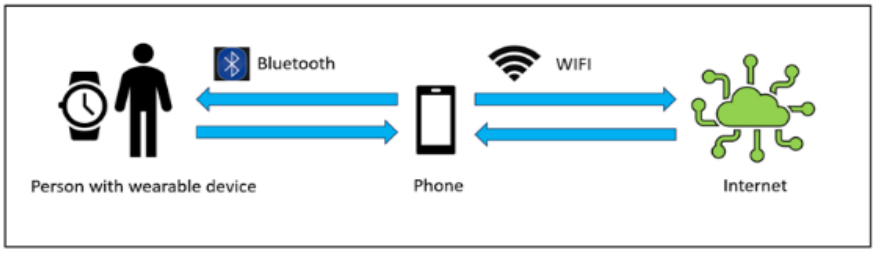


Fig. 1. Wearable Technology's Generic Data Acquisition Architecture

harmful usage [4]. Because of their restricted bandwidth and computing power, wearable devices demonstrate less robust security measures when compared to other computing devices [5].

2. Evaluation of Security on Real-world devices

2.1 Smart Glasses (Google Smart Glasses): Google's Smart glasses are a set of glasses with an integrated computer, offering innovative features that enhance people's lives. However, concerns about privacy and security issues were expressed out of several sources which could potentially threaten the user. Research findings have identified vulnerabilities in both the privacy and security aspects of Google's Smart Glass. One notable concern is the absence of an authentication method or secure PIN system, as highlighted by studies [6,7]. It has been discovered that taking videos and pictures without the user's awareness is possible, which is against privacy policies [6]. Without the wearer's knowledge, Google's smart glass could connect to a rogue Wi-Fi access station by reading a QR code, enabling remote control. It's a good thing that Google was informed of this problem, as a quick solution was made available.

2.2 Samsung smartwatch: Another wearable that provides important, cutting-edge features is the Samsung Smartwatch. Account harvesting is a form of attack that uses weak passwords and a lack of account lockout to obtain access to the system and data, was able to compromise 3 out of 10 watches. Only 50% of the tested devices have a PIN or pattern lock option for the screen. As a result, it is simple to decipher using a brute force assault and acquire usage of the gadget. Experts from the Romanian company Bitdefender [8] have demonstrated a proof-of-concept hack that gained access to a Samsung Gear Live Smartwatch paired with a Google Nexus 4. The findings revealed that the Bluetooth connection and the 6-digit unique PIN code shared between the two devices were susceptible to decryption through a brute force attack employing readily available open-source sniffer tools.

3. Privacy, Security Vulnerability Issues in Fitness Trackers /Bands:

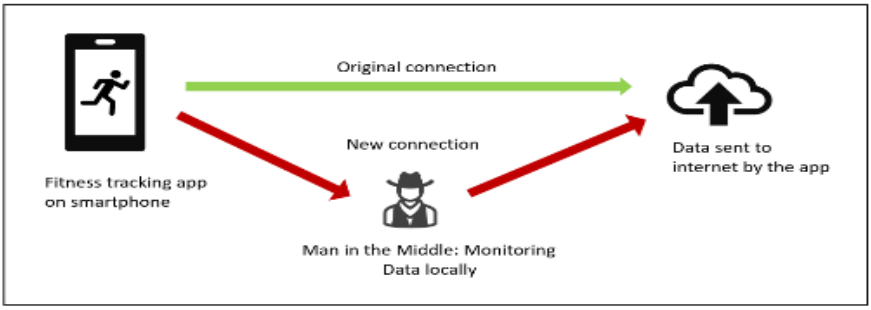


Fig. 2. Man-in- the- Middle-Attack (MITM)

Fitness trackers and smartwatches are subject to three basic categories of security risks: software, hardware and network sided. Compared to smartwatches, activity trackers have less computational processing power. This increases their reliance on the device to which they are linked, and because they frequently run on the user's handheld portable gadget's operating system, they also share its vulnerabilities [9] [10].

Tracking devices have the potential to collect various types of data including confidential user details such as location, gender, sleep cycle, and food habits. It is essential to conduct comprehensive research on the security and privacy requirements outlined in data protection laws like the General Data Protection Regulation (GDPR) in the EU. One significant vulnerability to be aware of is the man-in-the-middle attack scenario, which is shown in Figure 2. where the data transmitted is revealed. [11].

3.1 Fitbit: Fitbit [12] is well known for its products, including its intelligent fitness band. It offers measurements of human activities including distance travelled, the degree of sleep, and other indicators of one's health like heart rate and body temperature. Lack of authentication is one of Fitbit's main security flaws. Fitbit's absence of authentication on the tracker side means that potential attackers can readily obtain user data without their knowledge. [13,14]. The leaky BTLE (Bluetooth Low Energy) technology makes the Fitbit Flex susceptible. Consequences include a breach of privacy since third parties can monitor the activity of users. [15,16]. This benefit may also be used by insurance firms to establish a "grey market" for obtaining customer health information. For instance, it enables criminal individuals to track users' locations or the locations they visit to carry out phishing attacks such as sending phony emails with bargains attached that connect to spyware or a virus [14].

4.Various approaches to reduce security risk

4.1 Opting a sub-GHz band to improve communication reliability:

Wearable sensors typically work in the 2.45 GHz Industrial, Scientific, and medical (ISM) frequency band [17]. However, this band is becoming increasingly crowded, which can impact the reliability of communication. The sub-GHz band serves as a substitute for the 2.45 GHz frequency, which is less crowded and offers better communication reliability. Most widely used sub-GHz bands for IoT applications are '433' MHz, '868' MHz and '915' MHz for Asia, Europe, and the United States respectively [18]. These bands offer several advantages over the 2.45 GHz band, including: 1. Lower power consumption,2. longer battery life, 3. Better penetration through walls and other obstacles 4. Reduced interference from other devices. Let us compare a sub-GHz (868MHz) with 2.45 GHz to understand and technically support above mentioned statements.

4.1.1 Path Loss in Free Space. : It is also referred as Free-Space-Path-Loss (FSPL) which is calculated using the length of separation (d) between two antennas and the radio signal's free-space wavelength (λ0), as depicted in Figure 3 below. In this representation, 'TX' denotes the transmitter, and 'RX' defines the receiver, with their separation denoted as d. The transmitted power is indicated as PT, while PR stands for the received power, and GT and GR indicate, respectively, the gain of the transmitting as well as receiving antennas.

$$FSP(\text{dB})=10\ log(4\pi d/\lambda 0)^2$$

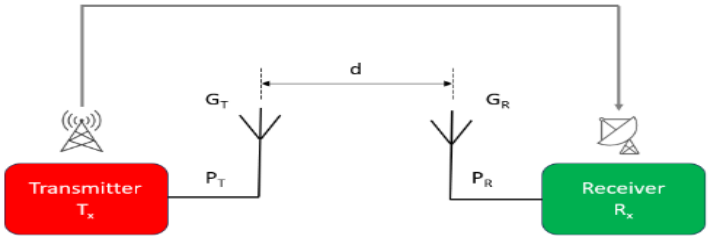


Fig. 3. Free Space Path Loss Transmitter and Receiver setup

At a frequency of 868 MHz, the free-space wavelength (λ0) is '0.345 m', and for '2.45 GHz', it becomes '0.122 m'. Considering a distance (d) of 3 m connecting the transmitting and receiving antennas, the FSPL is calculated using Equation as '40.8 dB' at '868 MHz' and '49.8 dB' at '2.45 GHz'. Consequently, by reducing operating frequency from '2.45 GHz' to '868 MHz', it decreases by '9 dB'. To put it another way, the attenuation is '9 dB' less in the '868 MHz' band than in the '2.45 GHz' band [19].

4.1.2. Attenuation of Radiofrequency in Indoor Environment: The characteristics of RF signals as they traverse materials is significantly influenced by the operation's frequency [20]. Unlike '2.45 GHz' band, the Sub-GHz band offers distinct advantages

in terms of penetrable RF signal through obstacles [20,22]. When traversing through an 8-inch concrete wall, an additional attenuation of '7dB' is observed in '2.45 GHz' band at '1GHz'. This indicates that a '1 GHz' system's transmission range is twice as large as that of a '2.45 GHz' band system [21].

4.1.3 Integration Difficulties: At present, numerous wireless technologies like Bluetooth, ZigBee, Wi-Fi, and various rules function within the unlicensed '2.45 GHz' band, resulting in a co-existence challenge. This adversely affects the wireless performance of devices, causing problems such as Loss of data packets and elevated transmission delays [23,24]. By operating in these less crowded frequency bands, the Sub-GHz approach can improve the quality of service (QoS) [25,26].

4.1.4 Power Consumption: Minimizing consumption of power is a crucial aspect for WT reliant on battery power [27, 28]. The Integration challenges faced for '2.45 GHz' band may impose several retransfers resulting in higher power consumption [23, 24]. Conversely, an operational radio transceiver at '868 MHz' exhibit reduced energy requirements for achieving equivalent transmission ranges in contrast to the '2.45 GHz' band [20, 22, 27].

4.2 Multifactor Authentication (MFA) & Authentication Biometrics:

Multi-factor authentication (MFA) enhances security by incorporating additional layers. Alongside the primary authentication method, like a password, it requires sending another verification to the user's email address or mobile device, generating a time-based code. This process ensures the verification of at least two factors. [29]. The fundamental tenets of security in the use of MFA are privacy, unification, and accessibility. MFA is the initial barrier of defence that attackers must get through to cause any harm. By gathering sufficient evidence to confirm a user is who they say they are, MFA applies numerous authentication concepts to the login process of a system over multiple devices [30].
To connect a person with the recognized credentials, three different factor groups are now accessible [31]:

a. Intellect-element—something the user is aware of, such as a PIN/Passcode.

b. Possession-element—a user-possessed item, like cards, cell phones, or some indicators.

c. A Biometric-element— such as a user's biometric information or behaviour pattern, identifies them as such.

Following this, MFA had been suggested to offer a greater degree of safety and permit ongoing safeguarding of computing machine and various essential services from unauthorised access [32,33,34]. Biometrics, which is automatic identification of persons based on their biological [38] as well as behavioural [35,36] attributes, is a major component of MFA. Due to the user's obligation to provide identification documentation that is based on two or more distinct variables, this step increased security [38]. Multi-factor authentication of wearable devices provides a promising path towards stronger

security and improved user experience. As wearable technology continues to advance, MFA will likely become an integral part of securing our digital lives, protecting our sensitive data from unauthorized access. However proactive efforts from manufacturers and users are necessary to ensure the effectiveness of MFA.

4.3 Secure Data Transfer Protocols Evaluation. Comparing and choosing the best protocol to ensure maximum security:

Data Transfer protocols consist of a defined set of rules and conventions governing the exchange of data among devices or systems within a computer network.

AES (Advanced Encryption Standard): AES utilizes variable-length keys (128-bit, 192-bit, or 256-bit) for the encoding and decoding process. Its strength lies in its ability to securely scramble and unscramble data, making it exceptionally challenging for unauthorized individuals to decipher the original information without the key as shown in Figure 4.

RSA (Rivest-Shamir-Adleman): RSA is an asymmetric encryption algorithm. Differing from symmetric algorithms, A public key is used for encoding, and a private key is used for decoding, in the RSA algorithm. The private key is only needed for decoding, while the public key is shared widely and allows anyone to encode messages.

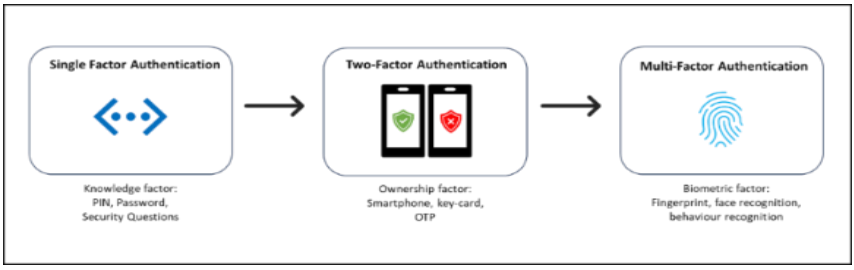


Fig. 4. The transition from SFA to MFA in the Authentication Mechanism

TLS (Transport Layer Security): Evolving from the earlier Secure Sockets Layer (SSL) protocol, TLS functions as a protective layer between applications and the underlying network infrastructure. Whenever you visit a website that employs "HTTPS" in its URL, TLS comes into action. It encrypts the data exchanged between your browser and the website's server, effectively shielding it from interception or tampering by malicious actors. Let us see how RSA/AES (considered in same case as they have similar security strength) is compared with TLS on a variety of parameters. Based on [39] 3 types of attacks were considered.

AttackType1: By manipulating broker data, the attacker impersonates a client to compel changes in other clients.

Attacktype2: Through popular topics data extracted from broker. A potential attacker would choose a popular/active topic, register to it, and try to interpret the information.

AttackType3: Attacker uses utilised topic to alter previously recorded data in the broker.

4.3.1. Attack Cost (AC): While calculating AC, the effort necessary to exploit the vulnerability and the time to success are considered. Cost will go up if expensive equipment or specific Knowledge is required [39].

Attack cost (AC)= (Sum (AW, VER))/2.

Attack Work (AW): Table 1 demonstrates how the resources required to exploit a vulnerability are added to assess the intensity of attack labour. The term "work" in Table 1 describes the arrangement of the attack's basic equipment, such as the computer and software. "Time" refers to the additional time needed to set up basic equipment.

Table 1. Attack Work levels & Frequency of Attack Attempt

Prerequisites	***Le***	***Time pe-***
None	0	≤ 1s
Work	2	≤ 1hr
Work, Knowledge	4	≤ a day
Work, Knowledge, Time	6	≤ a month
Work, Knowledge, Time, Costly equipment	8	≤ a year
Work, Knowledge, Costly equipment, huge amount of Time	10	> a year

Vulnerability Exploitation Rate (VER): Based on the length of time required to exploit a weakness, Table 1 illustrates the calculation of weakness exploitation rate.

4.3.2Attack Success Probability (ASP): It is set in relation to attack cost the attack success probability can never be more than (10 AC)/10. When evaluating ASP, the following factors are considered: data, topic and destination accessibility, frequency of attack, and attack tool requirements. [39].

$$ASP \leq (10 - AC)/10$$

4.3.3Attack impact (AIM): The damage that a successful attack might cause to the involved parties, including harm to their property, was estimated using Table 2. [39].

Table 2. Measuring Attack Impact level

Intensity of Attack	***Corresponding Attack***
Attack occurs and no damage is incurred	1
Attack occurs and it is detectable and reversible	3
Attack occurs and it is detectable but not reversible	6
Attack occurs and it is neither detectable nor reversible	10

Case1: No Security protocol

AttackType1: AC1 = (Sum (4,2))/2 = 3 ASP1 = 0.6 AIM1 = 10
AttackType2: AC2 = (Sum (2,2))/2 = 2 ASP2 = 0.7 AIM2 = 10
AttackType3: AC3 = (Sum (2,2))/2 = 2 ASP3 = 0.8 AIM3 = 10
TC1 =7 ASP_Avg1 = 0.7 AIM_Avg1 = 10

Case2: RSA or AES

AttackType1: AC1 = (Sum (10,10))/2 = 10 ASP1 = 0.1 AIM1 = 6

AttackType2: AC2 = (Sum (2,2))/2 = 2 ASP2 = 0.7 AIM2 = 10

AttackType3: AC3 = (Sum (10,10))/2 = 10 ASP3 = 0.1 AIM3 = 3

TC2 = 22 ASP_Avg2 = 0.3 AIM_Avg2 = 6.33

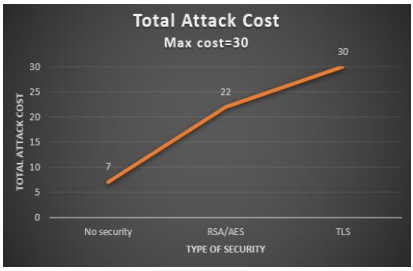
Case3: TLS

AttackType1: AC1 = (Sum (10,10))/2 = 10 ASP1 = 0.1 AIM1 = 3

AttackType2: AC2 = (Sum (10,10)/2 = 10 ASP2 = 0.1 AIM2 = 3

AttackType3: AC3 = (Sum (10,10))/2 = 10 ASP3 = 0.1 AIM3 = 3

TC3=30 ASP_Avg3 = 0.1 AIM_Avg3 =3



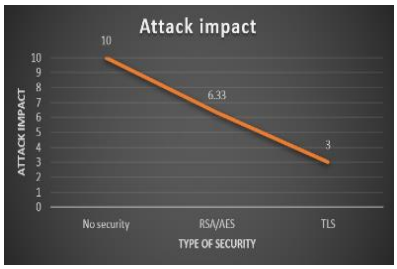


Fig. 5. Total Attack Cost and Impact of attacks

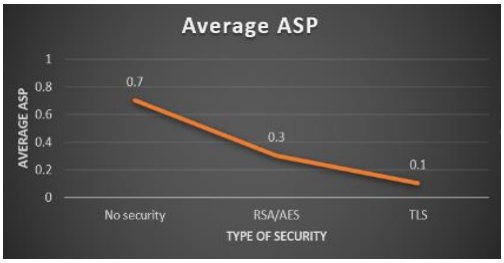


Fig. 6. Average ASP of attacks

From the line plots as shown in figure 5, figure 6 we can clearly observe that TLS has Highest attack cost, Lowest Average ASP, and Lowest Attack impact. Based on above calculations & these line plots it is evident that TLS is the best and most secure Data Transfer Protocol.

5. Conclusion:

Wearable Technology is becoming more advanced and while it offers superior features it also rises security and privacy concerns. This review article conducts an extensive

evaluation of real-world devices, advocates for the adoption of sub-GHz bands to enhance communication reliability and emphasizes the significance of multifactor authentication (MFA) and authentication biometrics and assesses secure data transfer protocols. By implementing sub-GHz bands and multifactor authentication, the overall security landscape can be substantially fortified. The article also highlights the importance of choosing the right Data transfer protocol for utmost security. Continuous research and vigilance are paramount to tackle emerging security challenges in WT.

References

1. Wearable technology market global opportunity analysis and industry forecast, http://www.prnewswire.com/news-releases/, 2017.
2. Viral M. (01 Apr 2012). Wearable Computer. [Online] Available: http://www.slideshare.net/fbviralmehta/wearable-computer-12242345
3. Ching, Ke & Mahinderjit Singh, Manmeet (Mandy). (2016). Wearable Technology Devices Security and Privacy Vulnerability Analysis. International Journal of Network Security & Its Applications. 8. 19-30. 10.5121/ijnsa.2016.8302.
4. Arias, O., Wurm, J., Hoang, K. and Jin, Y., 2015. Privacy and security in the Internet of Things and wearable devices. *IEEE transactions on multi-scale computing systems*, *1*(2), pp.99-109
5. Al-Muhtadi, J., D. Mickunas, and R. Campbell. Wearable security services. in Distributed Computing Systems Workshop, 2001 International Conference on. 2001.
6. Safavi, S. and Z. Shukur, Improving googles glass security and privacy by changing the physical and software structure. Life Science Journal, 2014. 11(5): p. 109-117.
7. Geran S. (18 Apr 2014). Is Google Glass a Security Risk? Available: https://blog.bit9.com/2014/04/18/is-google-glass-a-security-risk/
8. Liviu A. (12 Sep 2014). Bitdefender Research Exposes Security Risks of Android Wearable Devices.Available: http://www.darkreading.com/partnerperspectives/bitdefender/bitdefender-research-exposes-security-risks-of-android-wearable-devices- /a/d-id/1318005
9. Aktypi, A., Nurse, J.R. and Goldsmith, M., 2017. Unwinding Ariadne's identity thread: Privacy risks with fitness trackers and online social networks. In *Proceedings of the 2017 on Multimedia Privacy and Security* (pp. 1-11). Doi: 10.1145/3137616.3137617
10. Ho, J.J.; Novick, S.; Yeung, C. A snapshot of data sharing by select health and fifitness apps. In Proceedings of the Seminar on Privacy Implications of Consumer Generated and Controlled Health Data, Washington, DC, USA, 7 May 2014.
11. Hu et al., "Securing Communications between External Users and Wireless Body Area Networks," Proc. 2nd ACM Wksp. Hot Topics on Wireless Network Security and Privacy, 2013, pp. 31–36
12. fitbit. (Cited 2023). [Online] Available: https://www.fitbit.com/my
13. Michael S. (11 Jun 2015). Internet of Things Security Evaluation of nine Fitness Trackers.Available: https://www.av-test.org/fileadmin/pdf/avtest_2015- 06_fitness_tracker_english.pdf
14. J acob B. (03 Aug 2015). Surveillance Society: Wearable fitness devices often carry security risks.Available: http://www.post-gazette.com/news/surveillancesociety/2015/08/03/Surveillance-Society-Wearable-fitness-devices-often-carry-securityrisks/stories/201508030023
15. Cyr, B., et al., Security Analysis of Wearable Fitness Devices (Fitbit). Massachusetts Institute of Technology, 2014.

16. Carly P. (24 May 2015). iPhone users' privacy at risk due to leaky Bluetooth technology.Available: http://www.v3.co.uk/v3-uk/news/2409939/iphone-users-privacy-atrisk-due-to-leaky-bluetooth-technology
17. Kumar, S.; Buckley, J.L.; Barton, J.; Pigeon, M.; Newberry, R.; Rodencal, M.; Hajzeraj, A.; Hannon, T.; Rogers, K.; Casey, D.; et al. A Wristwatch-Based Wireless Sensor Platform for IoT Health Monitoring Applications. Sensors 2020, 20, 1675. [http://doi.org/10.3390/s20061675] [http://www.ncbi.nlm.nih.gov/pubmed/32192204]
18. Ioannidou, I.; Sklavos, N. On General Data Protection Regulation Vulnerabilities and Privacy Issues, for Wearable Devices and Fitness Tracking Applications. Cryptography 2021, 5, 29. https://doi.org/10.3390/cryptography5040029
19. Kumar, S.; Buckley, J.L.; Barton, J.; Pigeon, M.; Newberry, R.; Rodencal, M.; Hajzeraj, A.; Hannon, T.; Rogers, K.; Casey, D.; et al. A Wristwatch-Based Wireless Sensor Platform for IoT Health Monitoring Applications. Sensors 2020, 20, 1675. https://doi.org/10.3390/s20061675
20. S. Aust, R. V. Prasad and I. G. M. M. Niemegeers, "Performance evaluation of Sub 1 GHz wireless sensor networks for the smart grid," 37th Annual IEEE Conference on Local Computer Networks, Clearwater Beach, FL, USA, 2012, pp. 292-295, doi: 10.1109/LCN.2012.6423632.
21. Texas Instruments: Achieving Optimum Radio Range. Available online: http://www.ti.com/lit/an/swra479a/swra479a.pdf (last accessed on 4/8/2023).
22. S. Denis, R. Berkvens, B. Bellekens and M. Weyn, "Large Scale Crowd Density Estimation Using a sub-GHz Wireless Sensor Network," 2018 IEEE 29th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), Bologna, Italy, 2018, pp. 849-855, doi: 10.1109/PIMRC.2018.8580840.
23. R. Cavallari, F. Martelli, R. Rosini, C. Buratti and R. Verdone, "A Survey on Wireless Body Area Networks: Technologies and Design Challenges," in IEEE Communications Surveys & Tutorials, vol. 16, no. 3, pp. 1635-1657, Third Quarter 2014, doi: 10.1109/SURV.2014.012214.00007.
24. H. Karvonen, M. Hämäläinen, J. Iinatti and C. Pomalaza-Ráez, "Coexistence of wireless technologies in medical scenarios," 2017 European Conference on Networks and Communications (EuCNC), Oulu, Finland, 2017, pp. 1-5, doi: 10.1109/EuCNC.2017.7980744.
25. De Poorter, E., Hoebeke, J., Strobbe, M. et al. Sub-GHz LPWAN Network Coexistence, Management and Virtualization: An Overview and Open Research Challenges. Wireless Pers Commun 95, 187–213 (2017). https://doi.org/10.1007/s11277-017-4419-5
26. Uddin, M.A.; Mansour, A.; Jeune, D.L.; Ayaz, M.; Aggoune, E.-H.M. UAV-Assisted Dynamic Clustering of Wireless Sensor Networks for Crop Health Monitoring. *Sensors* 2018, *18*, 555. https://doi.org/10.3390/s18020555
27. Di Serio, A.; Buckley, J.; Barton, J.; Newberry, R.; Rodencal, M.; Dunlop, G.; O'Flynn, B. Potential of Sub-GHz Wireless for Future IoT Wearables and Design of Compact 915 MHz Antenna. *Sensors* 2018, *18*, 22. https://doi.org/10.3390/s18010022
28. Uddin, M.A.; Mansour, A.; Jeune, D.L.; Ayaz, M.; Aggoune, E.-H.M. UAV-Assisted Dynamic Clustering of Wireless Sensor Networks for Crop Health Monitoring. *Sensors* 2018, *18*, 555. https://doi.org/10.3390/s18020555
29. Suleski T, Ahmed M, Yang W, Wang E. A review of multi-factor authentication in the Internet of Healthcare Things. DIGITAL HEALTH. 2023;9. doi:10.1177/20552076231177144
30. Suleski T, Ahmed M, Yang W, Wang E. A review of multi-factor authentication in the Internet of Healthcare Things. DIGITAL HEALTH. 2023;9. doi:10.1177/20552076231177144

31. Harini, N. and Padmanabhan, T.R., 2013. 2CAuth: A new two factor authentication scheme using QR-code. International Journal of Engineering and Technology, 5(2), pp.1087-1094.
32. Scheidt, E.M. and Domangue, E., Tecsec Inc, 2006. Multiple factor-based user identification and authentication. U.S. Patent 7,131,009.
33. Bhargav-Spantzel, Abhilasha et al. 'Privacy Preserving Multi-factor Authentication with Biometrics'. 1 Jan. 2007: 529 – 560.
34. R. K. Banyal, P. Jain and V. K. Jain, "Multi-factor Authentication Framework for Cloud Computing," 2013 Fifth International Conference on Computational Intelligence, Modelling and Simulation, Seoul, Korea (South), 2013, pp. 105-110, doi: 10.1109/CIMSim.2013.25.
35. M. Frank, R. Biedert, E. Ma, I. Martinovic and D. Song, "Touchalytics: On the Applicability of Touchscreen Input as a Behavioral Biometric for Continuous Authentication," in IEEE Transactions on Information Forensics and Security, vol. 8, no. 1, pp. 136-148, Jan. 2013, doi: 10.1109/TIFS.2012.2225048.
36. Zach Jorgensen and Ting Yu. 2011. On mouse dynamics as a behavioral biometric for authentication. In Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security (ASIACCS '11). Association for Computing Machinery, New York, NY, USA, 476–482. https://doi.org/10.1145/1966913.1966983
37. National Research Council and Whither Biometrics Committee, 2010. Biometric recognition: Challenges and opportunities.
38. X. Huang, Y. Xiang, E. Bertino, J. Zhou and L. Xu, "Robust Multi-Factor Authentication for Fragile Communications," in IEEE Transactions on Dependable and Secure Computing, vol. 11, no. 6, pp. 568-581, Nov.-Dec. 2014, doi: 10.1109/TDSC.2013.2297110.
39. Carlsson, F., & Eriksson, K. (2018). Comparison of security level and current consumption of security implementations for MQTT.