Analysis on Security Vulnerabilities of Medical Wearable Devices (Fitness Trackers)

Mohammed Saleh
Department of Computer Information Sciences
Higher Colleges of Technology – Sharjah Men's Campus
Sharjah, United Arab Emirates

Issam T. Hamdan
Department of Computer Information Sciences
Higher Colleges of Technology – Sharjah Men's Campus
Sharjah, United Arab Emirates

***Abstract*—Nowadays, many smart and wearable devices are invented and sometimes utilized for human use. The advantage of these devices provides efficient and convenient communication with users within seconds, these smart devices are demonstrated to serve humans. Two of the major advantages of wearable devices are collect and analyze the body health conditions and signals in real-time monitoring. Also significant features of wearable technology provides connectivity and flexibility for users to access online information and communicate with others. These devices depend on wireless systems such as Bluetooth and Wi-Fi. Wearable devices are becoming a hot topic in many fields such as medical, fashion, education, etc. On the other and, they are becoming one of the vulnerable health devices, and it can be a potential security risks and threat. In this project, we will discuss the comparative analysis of fitness wearable devices, and we will emphasize the importance of this topic by revealing the potential security concerns. In recent years, Blockchain technology is becoming a primary option to secure systems. Blockchain could be used to enable smart and wearable devices to secure patient health records. Both the patient and the doctor will have access to repository health information of the patient.**

Keywords—wearable devices, fitness trackers, blockchain,

I. INTRODUCTION (*HEADING 1*)

Wearable technology utilizes electronic devices that people are wearing on the body. There are several types of wearable technologies, like fitness trackers and smartwatches. Fitness trackers consists of micro sensors for physical signals collections. Many wearable devises are used in healthcare that monitors user activities in real time to help the hospital and patients track patient's health conditions and illnesses. Wearable devices are now the new trend, and it will be the future of mobile phone devices, and one of the popular devices that we are using now is the Apple smartwatch, but it's still the beginning because many other companies are trying to develop wearable devise like Google. The wearable devices used in multiple areas and one of them is health care. They are popular in health care and also helpful to monitor user activities in real time and serve patient needs. The Smart Suite is one of the technologies that provides mobile health care that connects human and cloud in a naturally effective way.

The medical systems in many countries are taking substantial weights, while the quantity of medical facilities is truly lacking. A huge and vast amount of healthcare data, they invent a smart system for monitoring health based on smart clothing which's born at the right moment that will help to monitor patient health status to heal faster before medical conditions becomes more critical. People that can see patient information are the patients themselves, providers healthcare enterprises and others. Using it will cause a potential risk of gathering and storing all related health data, moreover it allows the users to be able to track more than simple information. The impact of wearable technology becomes significant when people start using it, and it can't alarm users of risk of security and privacy vulnerabilities. Any ignored simple medical information can be as a valuable resource for hackers and an entry to other sensitive systems. Data is the most valued resource to any organization and people, and it must be kept or stored in either cloud-based servers or physical datacenters. Those personal data like the user's habits and medical information provided by the fitness wearable devices might be shared with third parties who might use it in a way that will violate the privacy and security of users.

The breaches and vulnerabilities in health records are increasing such as user authentication issues, account harvesting, poodle attack, However, these concerns can be addressed by a deployment of comprehensive security that is backed by wearable device manufacturers.

In this research paper, we will compare different wearable fitness devices, which are also called "fitness trackers". Those devices became very popular in healthcare. It motivates people to exercise to reach their fitness goal. Moreover, we are going to research more on the security issues that might occur to the users of these devices and how they can protect themselves and prevent the misuse of their private information. Because developers of these trackers don't care that much on security and the end user lack of awareness, hackers can use what these devices capture for their malicious practices. In an effort to remove the existence of security weakness and vulnerabilities in manufacturing of these wearable devices and fitness trackers, organizations are becoming more interested in applying Blockchain technology in their system in an effort to protect the users data of these wearable devices from cyber-attacks.

II. LITRATURE REVIEW

Based on the review of the literature, the wearables database indicates that there are 43 devices used in entertainment, 188 in fitness, 24 in gaming, 68 in industrial, 88 in medical, and 225 in lifestyle [1]. So, it is becoming trendy in people's lives. For fitness trackers, it has increased rapidly due to the development of technologies. Social media is the primary reason for the rise in these technologies.

Customers want to share information everywhere in real time. [1], Wearable fitness devices have specific capabilities that feature the functionality and the purpose of it. For example, calories burned, heart rate, number of steps taken, and sleep rhythm, which can include technologies to support these types of functions like sensors, microprocessor, and transmitters. [2] In a previous study, research presented a brief discussion of the security of the wearable fitness devices that are like smartwatches – e.g., Google glasses, Fitness trackers – e.g., Fitbit, and Wearable medical devices – e.g. Medtronic Continuous Glucose Monitoring system and the ZIO Wireless Patch which demonstrates the major security issues of wearable fitness devices. One of the biggest concerns is signal interception which considers one of the data breaches, especially if the user connected the device in a workplace network where sensitive information stored which will compromise the company's reputation and integrity. After the issues are recognized, researchers suggested that users should demand from the manufactures some features to minimize wearable technology security issues like Remote erase feature, Bluetooth encryption, Cloud security and Encryption of critical data elements [3]. Nowadays, new technologies continually introduced, which means cybercrime is increasing, and further malicious attacks are created to exploit or find any vulnerability. Cybersecurity has become a significant concern because many crimes are committed on the internet, and many cases are considered unresolved, and in consequence, criminals are hiding behind the computer. It's important to educate our self about issues that can affect our lifestyle, which can put us in danger.

All wearable devices operate the same way using Bluetooth signals to stay connected to a monitoring app in the user's smartphones that translate the data captured by these devices in an attractive way that users can understand such as graphs and statistics about their daily habits. The apps themselves creates an opportunity to leak that information since it is using https to transmit the data and developer's servers to store them, increasing a potential risk to man-in-the-middle attacks. They can send wrong data to the user's trackers or even malicious data that might harm them without the user's attention. Moreover, they can trick the company servers into accepting any change of data also if it is unreliable. As Gavin Phillips stated in his article "Open Effect and Citizen Lab created several applications designed to trick the fitness tracker servers into accepting false information, with Bella beat LEAF, Jawbone UP, and Withings Health Mate coming up short (We sent a request to Jawbone stating that our test user took ten billion steps in a single day)". They find an approach to allocating these vast number of steps into a realistic distribution to prevent any future detection. Another fitness trackers called Smart Suite consists of microsensors for physical signals collections and the significant difference between the standard warble device and the smart suite is how to deploy the body sensors are integrated with many components such as Textile clothing, Flexible wire, Battery, Signal collecting intelligent terminal, Pulse sensor, Body temperature sensor, Electrocardiography sensor, and Blood oxygen sensor [17].

The wearable devices are willing to connect cloud apps through the corporate network, this means that hackers can find a way to compromise the smartphones and reach all other organization resources that are in a relationship within the same system gaining sensitive data for their malicious purpose. Fitbit is still the top fitness tracker makers according to the researches because they keep raising the security of the devices by updates and including built-in encryption when sharing data with the cloud. IT should treat wearables like any other computing device on their network, Manzuik says. "When possible, consider segregating internet of things devices to their network and don't connect them directly to the internet." An organization should only allow these devices to connect with a separate network to prevent any access to corporate internal resources like offering a guest WIFI network. As demonstrated in Fitness trackers have a lot to tell about their users, and if they get hacked, much information can be known, such as the mileage that you are covering. When and where you usually go running, age, gender, height, weight, steps taken, vacation time and etc. maybe they will think that even if its disclosed they will not get harmed because it's a usual information, but there are companies that have interests on these type of data and hackers can be sold your personal information to third parties to use them for marketing purposes for example.

III. FINDINGS

A. *Vulnerabilities of Fi bits*

A study by the University of Edinburgh about the weaknesses of fitness trackers; it focuses on the Fi bits devices which offer heart rate tracking, it found that hackers can extract the data, because of the researcher's test in trying to reach the data between two devices which are: fiber one and fi bit flex, and it worked. This data was personal and sensitive information of the users. Moreover, they were able to manipulate the data. They said that the main problem is stealing personal data. According to Mansfield [3], hackers can use them also to blackmail users. As the research showed how these devices suffer from hackers, Fitbit has enhanced its software to fix the security issues and maintain the privacy of its customers, and they said that they would design security measures for their new products to improve device security and ensure encrypted communications for the trackers. [3]

B. *Blockchain*

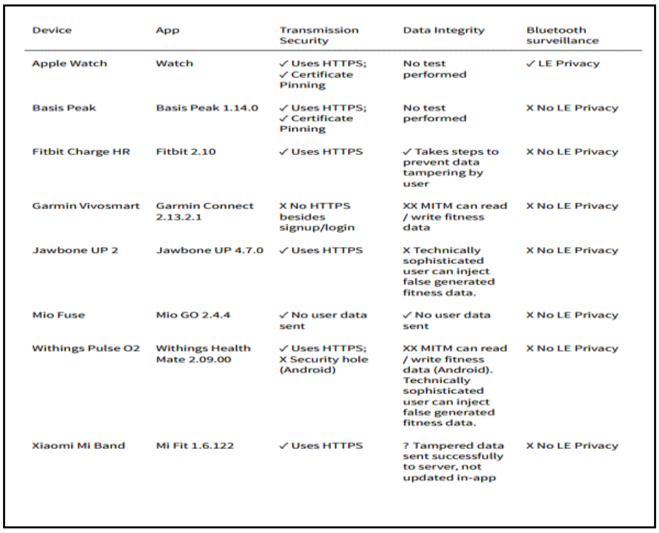
Blockchain technology is a database that holds data shared across a network of computers that uses special software to ensure data remains identical. Data is secured using cryptography and not changed except by authorized people. The block can hold various types of data and contain a timestamp to create the hash, which is the unique identity of a neighborhood. Also, the block includes a mixture of the previous block, creating a chain of interconnected blocks. As mentioned by McGoogan, In the blockchain, anyone can verify at any time how many units in circulation, who owns them, and the history of ownership, because the registry will distribute to everyone. [4] A new blockchain technology called Sidera has developed Bit smart integrated smartwatch with incredible features, considered as the first wearable decentralized device. It is the first hardware wallet you can carry on your wrist and fully secured by the blockchain. It also protects the funds from being stolen, and even if you lost it, you have a cover with multi-layers of security. This device is fully encrypted, and aim to give its users an easy, innovative, and secure way to manage the Crypto environment. [5]

What makes blockchain a unique way for data storage and exchange? The blockchain has no ownership by an authority or a specific group or an organization; it's there open for everyone to see. And everyone uses it to take the responsibilities of their actions. Usually, it is used for the transaction on industry world but not specifically as we said before it works in such a way that makes it bounded and firmly secure because each one of these blocks has encryption with a unique cryptography hash making a very secured chain. The block chain database is not in a single place; it was valid and published on the internet and accessible for everyone. What makes it hard for hackers to corrupt the data stored on it that there is no centralized location for the information to destroy it, so there is no direct goal for hackers. Hashing means taking a string input of any length and giving out an output of a fixed length no matter whether it is one word or hundred words. The cryptographic hash has so many unusual properties, but we will focus on one of them, which is called "Avalanche Effect." It means that any small change on the data will cause a significant shift on the hash. The blocks are linked together and contain a hash pointer that point each block to the previous one. If a hacker tried to hack one block, it would cause a change on the last block's hash, and this will change the mixture of prior blocks and so on.

There are many key benefits of adopting the blockchain for data storage and exchange information while utilizing the wearable devices. As demonstrated in [6], One of the advantages is security; there is no central point for exploitation because the system has guarded against hacking or attacks. The other benefits that considered, its reliable, customizable, [7] fraud minimization, Immutable, temper-resistant transactions, allows more people in business to trade, blockchain network can be public and open, or privet with restricted members.

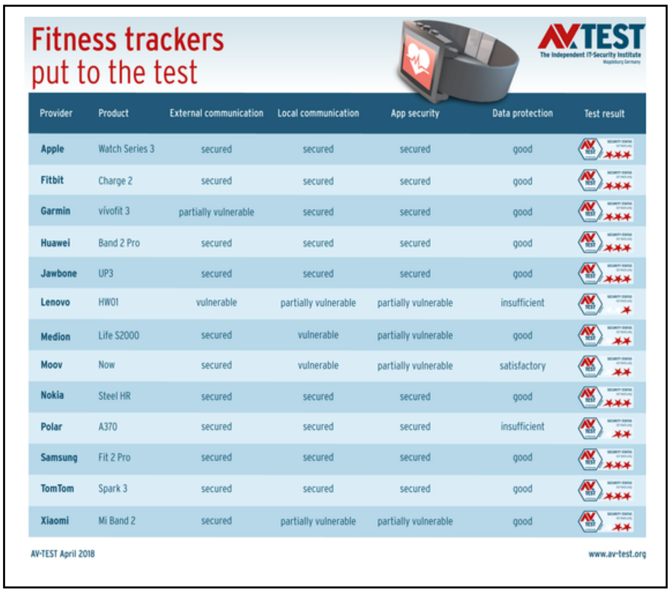
C. *Fitness trackers comparison table*

Table 1 and table 2 show the result of AV-TEST that has been conducted to the most common fitness trackers in the market. They focused on the security of internal and external communication, applications safety, and user's data protection. As it's shown above, apple watch series three by apple and charger2 by Fitbit are in the top of the list



Device	App	Transmission Security	Data Integrity	Bluetooth surveillance
Apple Watch	Watch	✓ Uses HTTPS; ✓ Certificate Pinning	No test performed	✓ LE Privacy
Basis Peak	Basis Peak 1.14.0	✓ Uses HTTPS; ✓ Certificate Pinning	No test performed	X No LE Privacy
Fitbit Charge HR	Fitbit 2.10	✓ Uses HTTPS	✓ Takes steps to prevent data tampering by user	X No LE Privacy
Garmin Vivosmart	Garmin Connect 2.13.2.1	X No HTTPS besides signup/login	XX MITM can read / write fitness data	X No LE Privacy
Jawbone UP 2	Jawbone UP 4.7.0	✓ Uses HTTPS	X Technically sophisticated user can inject false generated fitness data.	X No LE Privacy
Mio Fuse	Mio GO 2.4.4	✓ No user data sent	✓ No user data sent	X No LE Privacy
Withings Pulse O2	Withings Health Mate 2.09.00	✓ Uses HTTPS; X Security hole (Android)	XX MITM can read / write fitness data (Android). Technically sophisticated user can inject false generated fitness data.	X No LE Privacy
Xiaomi Mi Band	Mi Fit 1.6.122	✓ Uses HTTPS	? Tampered data sent successfully to server, not updated in-app	X No LE Privacy

Table 1: Device list features



Fitness trackers put to the test

AV-TEST The Independent IT-Security Institute Magdeburg Germany

Provider	Product	External communication	Local communication	App security	Data protection	Test result
Apple	Watch Series 3	secured	secured	secured	good	★★★
Fitbit	Charge 2	secured	secured	secured	good	★★★
Garmin	vívofit 3	partially vulnerable	secured	secured	good	★★★
Huawei	Band 2 Pro	secured	secured	secured	good	★★★
Jawbone	UP3	secured	secured	secured	good	★★★
Lenovo	HW01	vulnerable	partially vulnerable	partially vulnerable	insufficient	★
Medion	Life S2000	secured	vulnerable	partially vulnerable	good	★★
Moov	Now	secured	vulnerable	partially vulnerable	satisfactory	★★
Nokia	Steel HR	secured	secured	secured	good	★★★
Polar	A370	secured	secured	secured	insufficient	★★
Samsung	Fit 2 Pro	secured	secured	secured	good	★★★
TomTom	Spark 3	secured	secured	secured	good	★★★
Xiaomi	Mi Band 2	secured	partially vulnerable	partially vulnerable	good	★★

AV-TEST April 2018

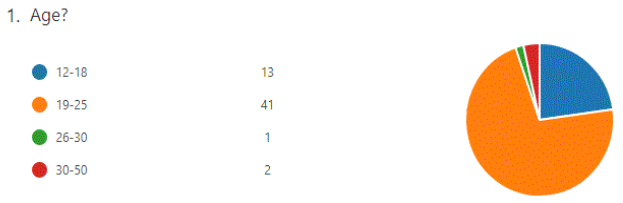
www.av-test.org

Table 2: Comparison between various fitness trackers

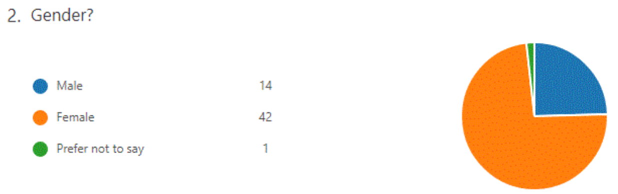
Wearable device (Fitness Trackers) comes with their application that will simplify the user's life. These Apps helps them to translate all the data that the trackers capture it, to a piece of helpful understandable information. It produces statistics about the data and charts to make the user able to track the progress of any activity. However, they discovered that these applications could lead to the disclosure of information; it is like an open the door to leak personal information without the user's attention.

IV. Findings

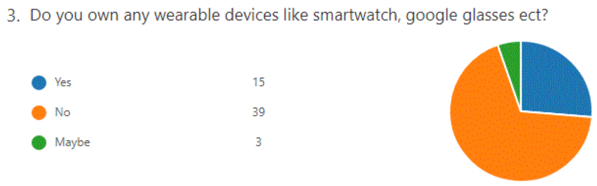
We surveyed the use of fitness trackers for teenagers; we received 57 responses, and here are the results.



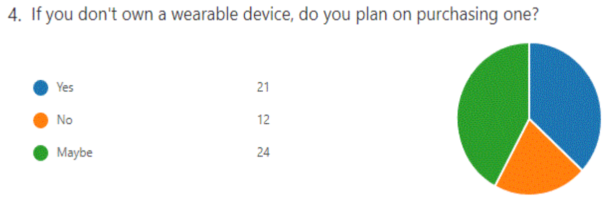
22.8% of the respondent's ages between 12-18, 71.9% are between 19-25, 1.7% are between 26-30, and 3.5% between 30-50.



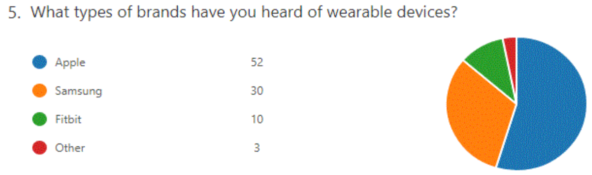
24.5% of the respondents are males, 73.6% are females, and 1.7% prefer not to say.



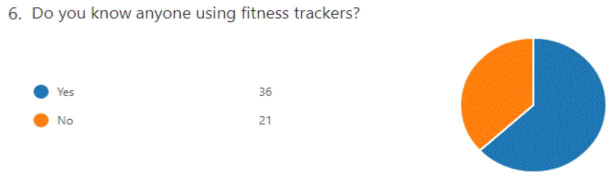
26.3% of the respondents own a wearable device, 68.4% do not own one, and 5.2% maybe own one.



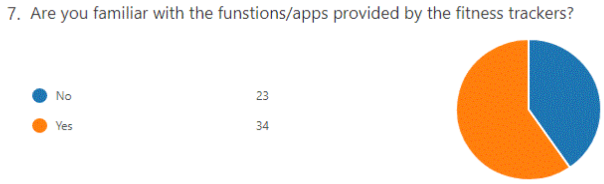
36.8% of the respondents are planning to purchase a wearable device, 21.0% are not thinking of buying one, and 42.1% are not sure about it.



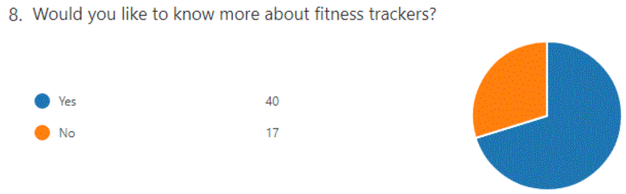
91.2% of the respondents have heard of apple, 52.6% have heard of Samsung, 17.5% have heard of Fitbit, and 5.2% have heard of others.



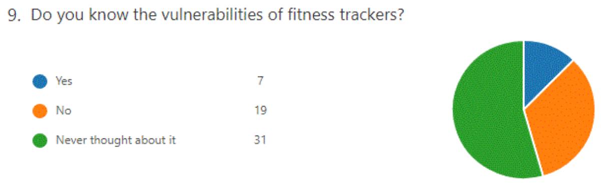
63.1% of the respondents know someone using fitness trackers, and 36.8% do not know anyone using fitness trackers.



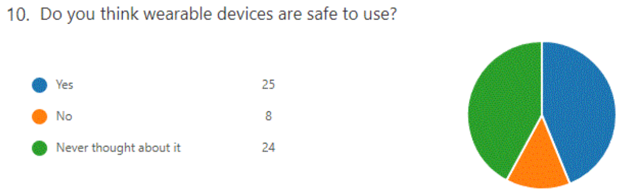
59.6% of the respondents are familiar with the apps provided by fitness trackers, and 40.3% are not.



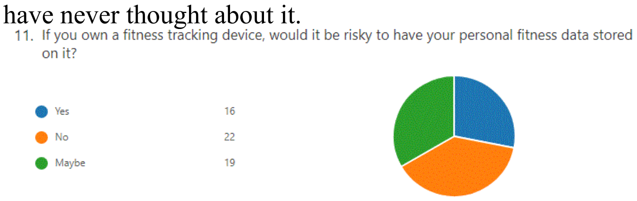
70.1% of the respondents would like to know more about fitness trackers, and 29.8% would not want to.



12.2% of the respondents know the vulnerabilities of fitness trackers, 33.3% do not know it, and 54.3% have never thought about it.



43.8% of the respondents think the wearable devices are secure to use, 14.0% do not believe it is safe, and 42.1% have never thought about it.



28.0% of the respondents think it is risky to store their fitness data on these devices, 38.5% do not believe it is dangerous, and 33.3% are not sure about it.

We Also surveyed the wearable devices on individuals as in “Figure 3”. We asked five questions, and a total of 26 answered, those questions were asked to the nurses and doctors in the hospital and also to the HCT health students. After they answered those 5 questions we analyzed the data, the first question was about if they trust their medical wearable devices, and the results of the survey showed that 16 persons answered yes while the rest 10 answered no. The individuals who answered no sure don't trust their devices but still use them every single day just because they need them. The argument about why do they need those devices? Of course, a lot of us store our data on these devices but still, if we log into the Internet there is a possible way that we will get hacked, and our data will be lost! So that's why those ten people don't trust their devices. Now let's talk about the way that people like to authorize or secure their wearable devices. Twelve individuals surveyed said they like to secure with their Fingerprint and eye scanning technologies. However, six individuals said they like to adopt username & password methods. But five 5 individuals said they like to secure it with their face scanning technologies. As we noticed, a lot of people chose different information security methods, but most of them chose the fingerprints which is used widely nowadays.

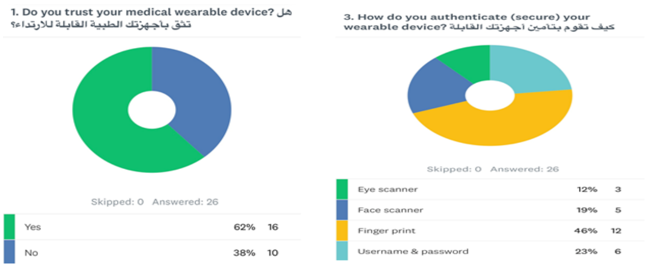


Figure 3: Sample survey results

V. Conclusion

In the end, we discovered that all fitness trackers have issues and challenges regard cybersecurity, especially for teenagers, and if they did not implement the proper security methods, hackers would take place. Also, we noticed that adults and teenager do not consider the safeness of the wearable devices; however, the companies must be aware of the consequences if their fitness trackers have been compromised, and apply more security measures, to limit the chances of obtaining security breaches.

In summary, our research recommended some changes can be made for the wearable devices to strengthen its security measures, especially when popular brands releasing new high-tech tools. In addition to that, we compared the wearable devices of different brands, to find the difference between them. In terms of the data protection, app security, types of communications made, the safeness of communication, and the result will be available for the users to see the security measures taken by the different brands which will be helpful for them when considering to buy a wearable high-tech device

In the end, we can say that smart suite provides better real-time data communication, but also it poses greater security and privacy risks. This is the significant challenges that are trading in the market. Most of the users concerning about the safety of smarty clothing because the collected data consist of sensitive information about themselves such as health-related information .although smart clothing are benefited and helpful to people but it still has some security loophole and privacy issues that required extra efforts from the designer and the responsible companies for its manufactures .we are expecting in the future that it will be more studies to handle the security issues in smart clothing and better mechanism will be presented.

VI. References

[1] Wearable Devices Used for Workplace Safety", vandrico, 2019. [Online]. Available: https://vandrico.com/wearables/device-categories/workplace-applications/workplace-safety. [Accessed: 03- Jul- 2019].

[2] "Wearable Technology Database", vandrico, 2019. [Online]. Available: https://vandrico.com/wearables/wearable-technology-database. [Accessed: 03- Jul- 2019].

[3] M. Mansfield, "Can Wearable Technology Threaten the Cyber Security of Your Business?," smallbiztrends, 28 Dec 2018. [Online]. Available: https://smallbiztrends.com/2016/02/wearable-technology-security-issues.html.

[4] C. McGoogan, "Fitbit devices can be hacked, research shows ," The Telegraph, 14-Sep-2017. [Online]. Available: https://www.telegraph.co.uk/technology/2017/09/14/fitbit-devices-can-hacked-research-shows/. [Accessed: 23-Feb-2019].

[5] C. G. I. Nederland, YouTube, 22-Jun-2018. [Online]. Available: https://www.youtube.com/watch?v=J9k8emtlqUo. [Accessed: 23-Feb-2019].

[6] Sidera Blockchain Technologies Launches World's first Wearable Decentralized Device", Wearable Technologies, 2019. [Online]. Available: https://www.wearable-technologies.com/2018/09/sidera-blockchain-technologies-launches-worlds-first-wearable-decentralized-device/. [Accessed: 03- Jul- 2019].

[7] "What are the advantages of a block chain", quora, 2019. [Online]. Available: https://www.quora.com/What-are-the-advantages-of-a-blockchain-over-other-methods. [Accessed: 03- Jul- 2019].

[8] "Benefits of BlockChain Technology," imarticus, 30 Jun 2018. [Online]. Available: https://imarticus.org/benefits-of-blockchain-technology/.

[9] J. S. Sekhon and J. S. Sekhon, "Smart Textiles with Blockchain - A Match Made in Heaven .," medium.com, 10-Apr-2016. [Online]. Available:https://medium.com/@jna1x3/smart-textiles-with-blockchain-a-match-made-in-heaven-b268bfca035c. [Accessed: 02-Mar-2019].

[10] "LOOMIA Smart Textile Technology," TodayCoinIndex. [Online]. Available:http://todaycoinindex.com/loomia-smart-textile-technology/. [Accessed: 02-Mar-2019].

[11] S. Kumari, "Smart textile," slideshare, 15 Apr 2015. [Online]. Available: https://www.slideshare.net/shantikumari/smart-textile-33563803.

[12] Study.com. [Online]. Available: https://study.com/academy/lesson/what-are-smart-textiles.html. [Accessed: 04-Mar-2019].

[13] "Fitness Trackers – 13 Wearables in a Security Test," Statistics & Trends Report | AV-TEST, 05-Mar-2019. [Online]. Available: https://www.av-test.org/en/news/fitness-trackers-13-wearables-in-a-security-test/. [Accessed: 06-Mar-2019].

[14] J. A. Martin, "10 things you need to know about the security risks of wearables," CIO, 28-Mar-2017. [Online]. Available: https://www.cio.com/article/3185946/10-things-you-need-to-know-about-the-security-risks-of-wearables.html. [Accessed: 06-Mar-2019].

[15] L. Magid, "Safety, Security And Privacy Risks Of Fitness Tracking And 'Quantified Self'," Forbes, 01-Aug-2014. [Online]. Available: https://www.forbes.com/sites/larrymagid/2014/07/31/safety-security-and-privacy-risks-of-fitness-tracking-and-quantified-self/#115d33dd4ade. [Accessed: 06-Mar-2019].

[16] G. Phillips, "Is Your Fitness Tracker Putting Your Security At Risk?," MakeUseOf, 19-Apr-2016. [Online]. Available: https://www.makeuseof.com/tag/fitness-tracker-putting-security-risk/. [Accessed: 06-Mar-2019].

[17] Min Chen, Yujun Ma,Jeungeun Song,Chin-Feng Lai,Bin Hu. "Smart Clothing: Connecting Human with Clouds and Big Data for Sustainable Health Monitoring." mobile networks and applications 21.5 (2016): 825-845.