IoT for 5G/B5G Applications in Smart Homes, Smart Cities, Wearables and Connected Cars

Hasna Uddin, Marcia Gibson and Ghazanfar Ali Safdar
School of Computer Science and Technology
University of Bedfordshire
Luton LU1 3JU, UK
hasna.uddin@study.beds.ac.uk, {marcia.gibson, ghazanfar.safdar}@beds.ac.uk

Tahera Kalsoom and Naeem Ramzan
School of Engineering and Computing
University of West of Scotland
Paisley PA1 2BE, Scotland, UK
{tahera.kalsoom, naeem.ramzan}@uws.ac.uk

Masood Ur-Rehman and Muhammad Ali Imran
James Watt School of Engineering
University of Glasgow
Glasgow G12 8QQ, Scotland, UK
{masood.urrehman,muhammad.imran}@glasgow.ac.uk

***Abstract*— Internet of things (IoT) is referred to as smart devices connected to the internet. A smart device is an electronic device, which may connect to other devices or are part of a network such as Wi-Fi. The increase of IoT devices has helped with advancing technology in many areas of society. Application of IoT in 5G/B5G devices has provided many benefits such as providing new ideas that can become projects for tech companies, generating big data (large volume of data which can be used to reveal trends, patterns and associations) and providing various ways of communicating. This has also had an impact on how companies improve their business with the use of advanced technology. However, the rapid growth of IoT has introduced a new platform for cybercriminals to attack. There has been published security measures on IoT to help deal with such risks and vulnerabilities. This survey paper will explore IoT in relation to smart homes, smart cities, wearables and connected cars. The benefits, risks and vulnerabilities will be discussed that comes along with using such devices connected to the internet.**

Keywords— Internet of Things (IoT), 5G/B5G, IoT Advantages, IoT Challenges, IoT Risks and Vulnerabilities.

I. INTRODUCTION

Improvements made to devices have introduced new ways of staying connected to the internet. There are also protocols on using IoT, for example, 'CoAP, IEEE 802.15.4, RPL, Quic, CCIN, etc' [1]. Table 1 shows the layers involved in IoT with protocols included.

Real-time data is possible due to the movement towards IoT. This has allowed devices to be controlled in various ways without much human interaction, for example, the emergence of smart cities such as Amsterdam, Barcelona and Singapore. This is a vision to create efficiency within the city with the use of technology [2] For example, IoT devices have provided new infrastructure for managing traffic daily. Wireless network technology has been used to detect surroundings. Installing sensors on traffic lights helps to provide the best direction for vehicles to avoid delays or traffic congestion. Integration of technologies has enabled automatic decision making for traffic lights [3]. IoT has helped with reducing manual labour in areas such as managing traffic; this can help to reduce costs. This also indicates that IoT has been introduced as a way of providing surveillance. Generating big data from IoT devices has played a role in making plans and improvements to the environment within a city.

Many IoT devices can also be used for different purposes within homes. For example, Amazon Echo allows calls to be made by talking to the device. Many homes have also got a smart TV, which allows them to access the internet. This shows IoT has been introduced as a way of improving sustainability within the environment and improving everyday lives within homes. Like IoT devices for traffic management, there are also smart devices within homes that can be used as surveillance, this is a way of improving security when not at home. Such devices can be connected to a smart phone to see and record who is near the house [4]. Security systems have been implemented with the use of advanced technology. This has made it more difficult for criminals to avoid getting caught when trespassing.

IoT allows both device-to-device connection and device-to-human interaction. Transmission Control Protocol/Internet Protocol is a set of communication protocols, which allows network devices to be interconnected [5]. This has helped the business world to flourish in gaining new consumers by introducing and promoting such devices. Regarding IoT, wearables and connected vehicles have also been continuously marketed by companies. IoT has provided various solution or improvements to different parts of society. However, with advanced technology being embedded within everyday

lives, there has been an emergence of new risks and vulnerabilities associated with IoT. Although IoT can help to provide ways of improving security by staying interconnected to devices and providing surveillance, such devices have also led to new risks and vulnerabilities.

TABLE I
IOT STACK

IoT Stack		
TCP/IP Model	**IoT Applications**	**Device Management**
Data Format	Binary, JSON, CBOR	
Application Layer	CoAP, MQTT, XMPP, AMQP	
Transport Layer	UDP, DTLS	
Internet Layer	IPv6/IP Routing	
	6LoWPAN	
Network/Link Layer	IEEE 802.15.4 MAC	
	IEEE 802.15.4 PHY / Physical Radio	

Devices that are interconnected can give cybercriminals more of an opportunity to attack. A voluntary Code of Practice was introduced by the UK government for manufacturers to deal with security issues for internet-connected devices [6]. IoT has introduced the need for new projects on boosting security when staying connected to the internet through devices. The security of IoT continues to be a challenge; therefore security measures have been introduced. This has opened discussions about the effectiveness of using IoT devices.

Section II will identify four areas where IoT devices have been applied. This will narrow down certain areas where IoT devices have been implemented. Section III will focus on the benefits of the applications of IoT devices. This will highlight the purpose of why there has been a movement towards using IoT devices as a way of making improvements. Section IV will explore what the risks and vulnerabilities are when using IoT devices. This will help to compare the advantages and disadvantages of using IoT devices.

II. APPLICATIONS OF IOT

There are numerous devices that have been implemented in different areas of society. IoT devices have introduced various approaches on how to stay connected to the internet. this has created a new area for companies to create more revenue for themselves. IoT has, therefore, had an impact on the economy in many cities. The use of IoT is also estimated to 'grow to over 80% by 2025, leading to a potential global economic uplift' [7].

There are many areas of application for IoT, not all smart devices can be easily identified or accessed for more information. For this paper, four areas have been selected to narrow down and explore IoT devices. These areas have been chosen because they are widely known and will help to open discussion for further review as IoT devices develop over time. The focus will be based on the following areas of application for IoT:

A. Smart Homes

Home automation system with the use of IoT provides a new approach to controlling and connecting devices. This provides more features to household various items such as air conditioners, lights, security systems, TV, etc. Many features can include sensors, cameras, commanding or performing actions [8]. New devices continue to be introduced to provide more of a proficient approach to using household devices.

B. Smart Cities

Smart city with the use of IoT was introduced as a way of having an embedded operational system through information technology integration [9]. This also involves a 'comprehensive application of information resources' [10]. A smart city is an approach through strategic planning to change the functioning of people's lives in cities. Using IoT devices has been used as a way of coming up with new ideas to face various challenges. These challenges are in relation to the increasing population in various cities, particularly in urban areas. A smart city is a movement towards using technology to find solutions to make improvements to the environment. This is another area where IoT devices can be remotely monitored, managed and controlled. IoT devices are used as a way of exchanging information and communication within a smart city. This has played a vital role in the changes to operational systems within various cities.

C. Wearables

Wearables in relation to IoT, these devices have enabled companies to come up with new trends and ideas with the use of technology. For example, fitness tracking devices have used as a way of monitoring health [11]. Wireless devices have introduced more flexibility regarding wearables. This has enabled devices to be used almost everywhere. Other examples include smart glasses, smartwatches and health fitness trackers. Various wearables devices can connect to the internet. Many wearable devices can also connect to a smart phone. This shows how interconnected devices through the internet can be portable

D. Connected Cars

A connected car is part of the IoT by being able to access the internet. Car manufacturers have had an interest and explored the emergence of connected cars. There have also been discussions regarding self-driving vehicle with the use of connecting to the internet [12]. A connected car can provide communication between the passenger's smartphone and the vehicle itself. Just like other IoT devices, a connected car can also provide new features for more control.

The four areas above where IoT has been implemented, this will be discussed altogether rather than separately in Section III and Section IV. Combining the four areas will highlight whether there are similar benefits, risks and

vulnerabilities for different IoT devices. This will also help to compare various IoT devices being used.

III. Benefits of IoT Devices

A. Safety and Security

Many IoT devices have been used as a way of implementing strategies for enhancing safety and security. Safety and Security relates to the CIA triad (confidentiality, integrity and availability). IoT devices can provide security with the use of data encryption. This is when sensitive data is translated into code; this makes it difficult for attackers to access the data. For example, Cisco systems provide IT solutions by using an algorithm that includes elliptic curve cryptography, Galois/Counter Mode, and SHA-2 [13]. There are also various IoT devices, which can be considered as a movement towards a smart city which uses technology for enhancing security. For example, Smart cameras and infrared sensors (which detect energy radiating from vehicles) [14]. Wireless network technology can be beneficial in generating new statistics for public areas where incidents frequently occur.

IoT devices can be beneficial to analyse real-time situations without much human interaction. This is similar to surveillance within homes with the use of smart cameras. Wearables can be connected to such devices for those that want to know as soon as possible if their home security system has been breached. It is evident that some IoT devices have been used to enhance security and to make people feel safer.

Singh [15] suggested that vehicles connected the internet with dashboard camera (Smart-Eye), this can help with accident prevention/monitoring services. Connected cars with a camera can be used as a way of sending data of real-time incidents directly to the nearest authorities, ambulance and hospital. This would be beneficial by getting instant access to monitoring the area, saving people's lives that need immediate attention and resolving the cause of road accidents quicker. IoT devices have therefore been useful in bringing about the discussion on strategies for preventing and dealing with issues.

B. Mobility and Health

Some IoT wearables are similar in terms of increasing safety within public spaces. Various companies have been focusing on how wearables connected the internet can improve quality of life. For example, Toyota has been developing a wearable device that can help blind and visually impaired to navigate better [16]. This illustrates that IoT devices can be developed to make everyday tasks easier. There are many control devices connected to the internet being continuously made for ease of use. Companies have put forward various wireless network devices for different purposes; this would benefit many businesses by being creative with technology (Figure 1).

Some wearables are comparable to the purpose of some IoT devices for smart cities, smart homes and connected cars by focusing on safety. However, wearables may also be beneficial in terms of monitoring health. For example, the use of IoT in fitness bands can be another approach to health care application.

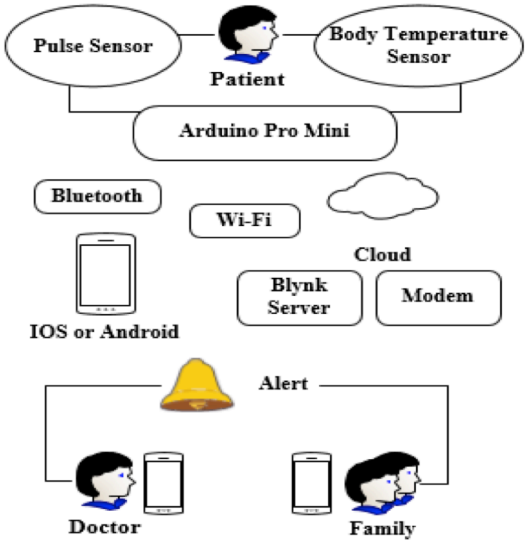

Fig. 1. IoT in remote health monitoring.

There have been reviews on how IoT could be beneficial for getting real-time data on health. This shows how wearable IoT devices not only help with monitoring health but could potentially help patients get treated faster to avoid further health risks. Wearable IoT devices can, therefore, be used as a way of improving health care services or coming up with new solutions. This idea is comparable to the idea of connected cars discussed previously, using IoT devices to alert others to get immediate attention. IoT devices in many areas might be beneficial in finding new approaches to improve interaction and communication.

C. Creativity and Customisation

Many IoT devices have played a vital role for various purposes such as improvements to health, safety and security. However, IoT devices can have more than one purpose, which can make them more valuable. For example, Amazon Echo can also be used for entertainment purposes when playing music, not just for performing actions for tasks like calling. The advantage with IoT devices is that new type of controls can be developed to increase their capacity of how useful they can be. Many companies can focus on upgrading such devices to allow room for customisation, for example, smartphones are continuously being upgraded. Smartphones have much more features that allow people to use the internet in various ways. These relate to improving security by combating new risks with new features. The emergence of IoT devices has given many companies the opportunity to continue to find new ideas and projects.

IV. IoT Risks and Vulnerabilities

IoT can be useful in many ways; nevertheless, IoT does not come without possible security risks and vulnerabilities. The misuse of IoT devices continues to be a challenge that is difficult to resolve. IoT devices are beneficial in many ways, however, Table II highlights the need to address various risks and vulnerabilities.

There are constantly new risks occurring while technology continues to be developing over time. The complexity of devices could increase security vulnerabilities. This allows criminals to find more loopholes, which increases security threats. The complexity of devices also makes it difficult to prevent security issues before they occur. It is impossible to cover all threats that occur which is a disadvantage. With the use of IoT, many security risks and vulnerabilities can go undetected for a long time. Certain risks and vulnerabilities will be explored to highlight the impact IoT devices have had on bringing about new issues.

A. Surveillance Abuse

Smart cameras have been useful in assisting in areas such as management for home security and traffic management. Nevertheless, IoT devices for surveillance can also create new issues that can affect the safety and security of others. For example, smart cameras can be installed but their purpose for why they have been installed may be hidden or not fully disclosed. Another issue is that this can have an impact on privacy protection; people may not always know when they are being recorded. Connected devices via the internet, this also brings the questions of how many people have obtained the footage [17]. If the cameras are in control by criminals or companies misuse devices, this can put many people at risk in being safe.

IoT devices can be used in various ways is beneficial, however, this also raises the concern of not always being aware of what active devices are in the environment. Schneier [18] states that 'IoT has eyes, ears, but also hands and feet'. This statement expresses the concern for IoT evolving to the point where it is difficult to manage and identify surveillance abuse. He puts forward the argument that companies are not competing for IoT security and there isn't a large enough market for security experts [19]. This leads to more issues of dealing with the dangers of IoT devices. There have been concerns of companies such as Huawei (telecommunications equipment company) using devices that may be used as surveillance from the Chinese government [20]. There continues to be an interest in improving the technology by having faster internet such as 5G, however many are concerned about this becoming a national security risk.

B. Unauthorised Access to IoT Devices

With the emergence of IoT devices that can even be wearables that are portable. This increases the chance of a wireless network device to be accessed by others. System hardware or software can have design flaws that make it difficult to fix, this allows exposure for criminals to gain access to information [21]. Having devices connected to each other via internet is useful, however, this may create a bigger impact when security is breached. These issues give criminals the opportunity to access multiple IoT devices. This also relates to surveillance abuse, in terms of being unaware of how many people have unauthorised access to sensitive data via the internet. IoT devices also provide criminals different ways of phishing. For example, smartphones increase the risk of spear phishing and whaling [22]. This contradicts the concept of IoT enhancing and improving security.

TABLE II
SECURITY CHALLENGES IN IOT

IoT Devices	Security Risks and Vulnerabilities
Smart camera connected to the wireless network of devices	Misuse of surveillance by spying on others or person of interest, ethical issues on privacy, gaining access to control devices
IoT devices that require user credentials	User impersonation, access to sensitive data, possible cyberattacks by making changes
IoT smart home system	Enabling modifications to access home, vulnerable to attacks
IoT wearables	Wearable devices increase the likelihood of stolen or misplaced devices with sensitive data, vulnerable to social engineering, owner of IoT wearable may lend device to others who can then access personal information.
Mobile apps	Malicious attacks through installation, unauthorised modifications, access to sensitive data

Unauthorised storage of personal information on smartphones, people not even be away from what is being shared others which put them more at risk. IoT devices, therefore, have many issues in relation to data confidentiality, user privacy and reliability of authentication mechanism. This is also an indication that multiple IoT devices can be a disadvantage due to non-standardisation. This puts people at risk of user personation, misuse of personal information or making modifications without consent [23]. Companies and individuals, therefore, can be targeted with the use of IoT devices, this is a disadvantage in terms of everyone having to deal with this constant challenge against security threats.

C. Cost of Preventing/Resolving IoT Security Issues

The use of wireless network devices can be used as a way of reducing costs, however, IoT can lead to financial risks or increasing money spent on security. Criminals can use IoT as a way of stealing money from another person. Statistics show that in the UK, £190,000 a day is lost by victims of cyber-crime [24]. This shows that individuals would need to be careful with IoT devices because it is

difficult to detect straight away even when a cyber-attack happens.

Criminals may also use IoT as a way of selling other people's personal information for money. Gathering personal information from devices that are part of a global network can lead to a bigger impact and affect more people. This increases the chance of being a victim when having to make an account on devices connected to the internet.

There are also many cases where companies fail to protect themselves and their customers from attackers. This can become a security threat to largescale. IoT, therefore, makes it easier for such risks to affect many people at once. Many firms may also underreport cyber-attacks when disclosing information to the public [25]. If a cyber-attack is underreported, it would be unclear of whether the issue has been completely resolved. This is another disadvantage, which can put the company or the customers at risk of financial loss, leaked information that can be misused for various purposes.

V. Conclusion

IoT devices have created in many areas of society and have different or multiple purposes. IoT will continue to grow and develop over time. This will introduce even more ways of how IoT devices can be useful. Such devices can improve people's lives and many companies regarding safety, security, mobility, health, creativity, customisation and many other ways. Nevertheless, the more IoT devices are being used, the more potential there is for security threats. This continues to be a constant challenge for both companies and individuals to protect themselves from various attacks. IoT can both enhance but also threaten the security of homes, cities, cars and wearables. It is difficult to manage the risks of IoT, yet IoT is being used to manage other problems in society such as traffic management and home security system. Overall it depends on how IoT devices are made to prevent security threats, however, it is useful to become aware of how criminals are coming up with new ways to breach IoT devices. There continues to be a movement towards both the need for IoT devices and the concerns that come with using such devices.

References

[1] V. P. N. Nikshepa, "Survey on IoT Security Issues and Security Protocols," International Journal of Computer Applications, vol. 180, no. 42, pp. 16-21, 2018.

[2] S. Ijaz, "Smart Cities: A Survey on Security Concerns," International Journal of Advanced Computer Science and Applications, vol. 7, no. 2, p. 612, 2016.

[3] M. Awadalla, "A Smart Traffic Information System," International Journal of Computer Applications, vol. 180, no. 31, pp. 7-11, 2018.

[4] D. Anwar, "IOT based Smart Home Security System with Alert and Door Access Control using Smart Phone," International Journal of Engineering and Technical Research, vol. 5, no. 12, 2016.

[5] T. Gonnot, "Home Automation Device Protocol (HADP): A Protocol Standard for Unified Device Interactions," Advances in Internet of Things, vol. 05, no. 04, p. 27, 2015.

[6] GOV.UK, "Leading tech companies support code to strengthen security of internet-connected devices," GOV.UK, 14 October 2018. [Online]. Available: https://www.gov.uk/government/news/leading-tech-companies-support-code-to-strengthen-security-of-internet-connected-devices. [Accessed 19 April 2019].

[7] M. Walport, "Internet of things: making the most of the second digital revolution," The Government Office for Science, UK, 2014.

[8] V. Nakrani, "A Review: Internet of Things(IoT) Based Smart Home Automation," International Journal of Recent Trends in Engineering and Research, vol. 3, no. 3, p. 231, 2017.

[9] P. Siano, "Introducing Smart Cities: A Transdisciplinary Journal on the Science and Technology of Smart Cities," Smart Cities, vol. 1, no. 1, pp. 1-3, 2018.

[10] T. Kim, "Smart City and IoT," Future Generation Computer Systems, vol. 76, no. 1, p. 159, 2017.

[11] J. Wei, "How Wearables Intersect with the Cloud and the Internet of Things : Considerations for the developers of wearables.," IEEE Consumer Electronics Magazine, vol. 3, no. 3, p. 53, 2014.

[12] M. M. R. Coppola, "Connected Car: Technologies, Issues, Future Trends," ACM Computing Surveys, vol. 49, no. 3, p. 1, 2016.

[13] Cisco, "Next Generation Encryption," Cisco, October 2015. [Online]. Available: https://www.cisco.com/c/en/us/about/security-center/next-generation-cryptography.html#1. [Accessed 22 April 2019].

[14] N. Lanke, "Smart Traffic Management System," International Journal of Computer Applications, vol. 75, no. 7, pp. 19-22, 2013.

[15] M. S. D. Singh, "Internet of Vehicles for Smart and Safe Driving," in ICCVE, Shenzhen, 2015.

[16] BBC, "Toyota develops wearable device for blind people," BBC, 8 March 2016. [Online]. Available: https://www.bbc.co.uk/news/technology-35753978. [Accessed 20 April 2019].

[17] R. Chow, "The Last Mile for IoT Privacy," IEEE Security & Privacy, vol. 15, no. 6, pp. 73-76, 2017.

[18] B. Schneier, "IoT Security: What's Plan B?," IEEE Security & Privacy, vol. 15, no. 5, p. 96, 2017.

[19] B. Schneier, "IoT Security: What's Plan B?," IEEE Security & Privacy, vol. 15, no. 5, p. 96, 2017.

[20] BBC, "Huawei: US official warns 'no safe level' of involvement with tech giant," BBC, 29 April 2019. [Online]. Available: https://www.bbc.co.uk/news/uk-48098362?intlink_from_url=https://www.bbc.co.uk/news/topics/cjnwl8q4qz2t/huawei&link_location=live-reporting-story. [Accessed 1 May 2019].

[21] M. Abomhara, "Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks," Journal of Cyber Security and Mobility, vol. 4, no. 1, pp. 65-88, 2015.

[22] B. Amro, "Phishing Techniques in Mobile Devices," Journal of Computer and Communications, vol. 06, no. 02, pp. 27-35, 2018.

[23] I. Makhdoom, "Anatomy of Threats to The Internet of Things," 11 October 2018. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8489954&isnumber=5451756. [Accessed 22 April 2019].

[24] BBC, "UK cyber-crime victims lose £190,000 a day," BBC, 27 January 2019. [Online]. Available: https://www.bbc.co.uk/news/uk-47016671. [Accessed 22 April 2019].

[25] "Firms failing to disclose IoT vulnerabilities," Network Security, vol. 18, no. 12, pp. 1-2, 2018.