

Article

Not peer-reviewed version

Designing and Adapting IoTs for the Next-Generation Smart Systems

[Cajetan M. Akujuobi](#) *

Posted Date: 25 February 2025

doi: 10.20944/preprints202502.2032.v1

Keywords: Internet of Things (IoT); Broadband Wireless networks; Cybersecurity; Generations of Technology; 5G; Smart Technologies



Preprints.org is a free multidisciplinary platform providing preprint service that is dedicated to making early versions of research outputs permanently available and citable. Preprints posted at Preprints.org appear in Web of Science, Crossref, Google Scholar, Scilit, Europe PMC.

Copyright: This open access article is published under a Creative Commons CC BY 4.0 license, which permit the free download, distribution, and reuse, provided that the author and preprint are cited in any reuse.

Article

Designing and Adapting IoTs for the Next-Generation Smart Systems

Cajetan M. Akujuobi

Center of Excellence for Communication Systems, Electrical and Computer Engineering Department, Prairie View A&M University, Texas, USA; cmakujuobi@pvamu.edu

Abstract: The Internet of Things (IoT) is a network of physical objects embedded with sensors and other technologies that allow them to connect and exchange data. The IoT is a link between objects in the real world and the virtual world, thereby enabling anytime, anywhere connectivity for anything. This paper explores what it will take for IoT to meet the demands of next-generation intelligent systems in terms of design and adaptability. The possible challenges are also explored, and recommendations necessary to meet those challenges are made as well.

Keywords: Internet of Things (IoT); broadband wireless networks; cybersecurity; generations of technology; 5G; smart technologies

1. Introduction

The Internet of Things (IoT) is a giant network of connected things and people. Most researchers have worked using IoTs in different applications and most recently in 5G applications [1–6]. Kevin Ashton is known to be the father of IoT because he coined the term "Internet of Things" in 1999 and played a pivotal role in conceptualizing the vision of an interconnected world of smart devices through his early work [7]. IoT refers to the billions of physical devices connected to the wireless Internet that allow data exchange worldwide. It is a global infrastructure for the information society, connecting devices/things to the Internet and each other using wired or wireless technology, as shown in Figure 1. The devices include smartphones, tablets, desktop computers, autonomous vehicles, refrigerators, toasters, thermostats, cameras, pet monitors, alarm systems, insulin pumps, industrial machines, intelligent wheelchairs, wireless sensors, mobile robots, etc. The IoT connects people, places, and products, offering new opportunities to generate value in products and business processes. IoT must also be designed to be competent in meeting the challenges as these devices become smart, as shown in Figure 2. Secondly, Since the 1970s, technology has undergone generational changes from 1G to 5G. If IoT is to meet technological and generational changes, it has to be designed to be innovative and meet the demands of next-generation intelligent systems.

IoT is a revolutionary technology that has the potential to disrupt our lifestyle; various technologies and businesses connect smart things or devices equipped with sensors. When it comes to the Internet, the Internet of Things (IoT) has taken center stage for the next generation of intelligent systems. The IoT has revolutionized practically every aspect of life, and it is challenging to identify everyday activities that IoT does not impact. IoT aims to integrate and automate everything from home appliances to plants on factory floors. The Internet of Things (IoT)-centric concepts like augmented reality, high-resolution video streaming, self-driven cars, innovative environment, e-health care, etc. are ubiquitous now. These applications require higher data rates, large bandwidth, increased capacity, low latency, and high throughput. In light of these emerging concepts, future IoTs require smart systems providing seamless connectivity between heterogeneous networks (HetNets), as shown in Figure 3. The eventual aim of IoT will be to introduce plug-and-play technology, providing the end-user ease of operation, remote access control, and configurability. In this paper, we will explore what it will take for IoT to meet the demands of next-generation smart systems in

terms of design and adaptability. We will also explore the challenges and make necessary recommendations.

In Section 2, we discussed the generations of wireless broadband networks, while in Section 3, we discussed the Internet of Things for 5G related Smart technologies. The IoT and Smart Cities and the importance of providing IoT security in future generations of Smart systems are discussed in Sections 4 and 5, respectively. Sections 6 and 7 discussed the possible attack challenges on IoT systems and IoT security solutions for future generations of smart systems, respectively. Finally, we have the recommendations in Section 8, while Sections 9 and 10 are the conclusions and references respectively.

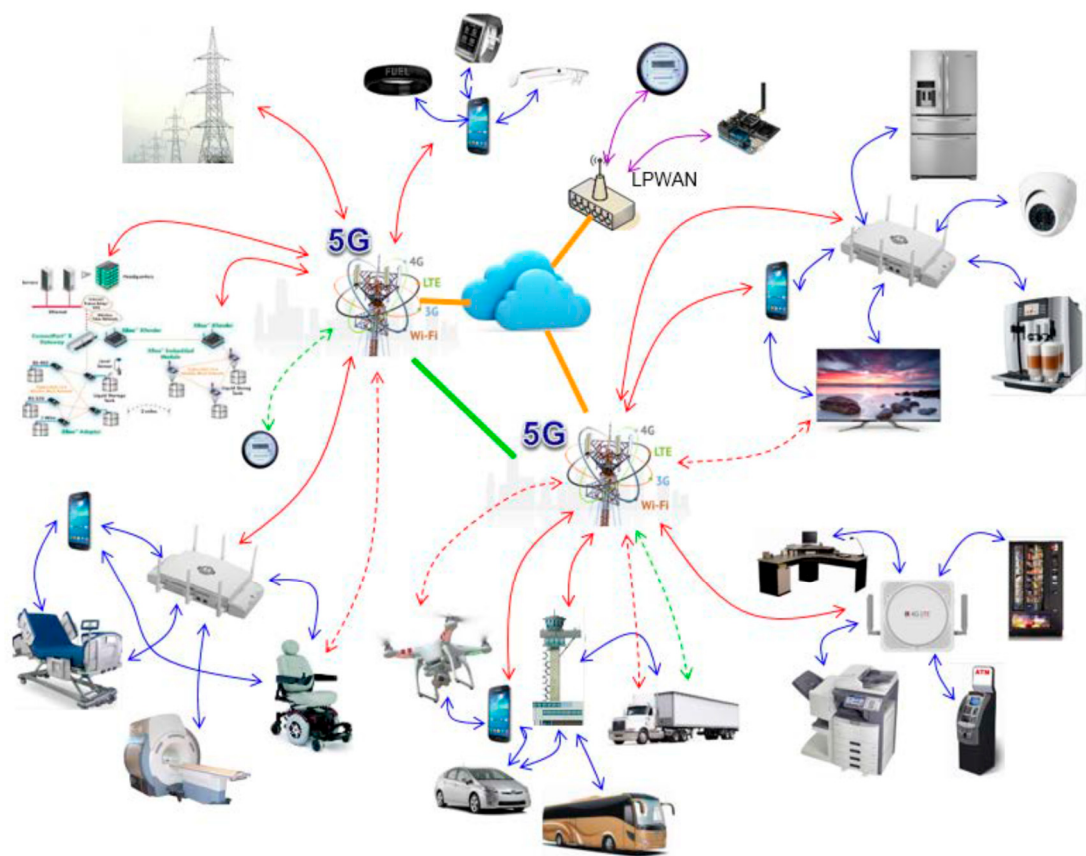


Figure 1. IoT Serving as a Global Infrastructure for the Information Society. Scheme 2. Typical IoT Applications. Source: K. K. Patel and S. M. Patel, "Internet of things – IOT: Definition, characteristics, architecture, enabling technologies, application & future challenges," *International Journal of Engineering Science and Computing*, vol. 6, no.5, May 2016, pp. 6122-6131.

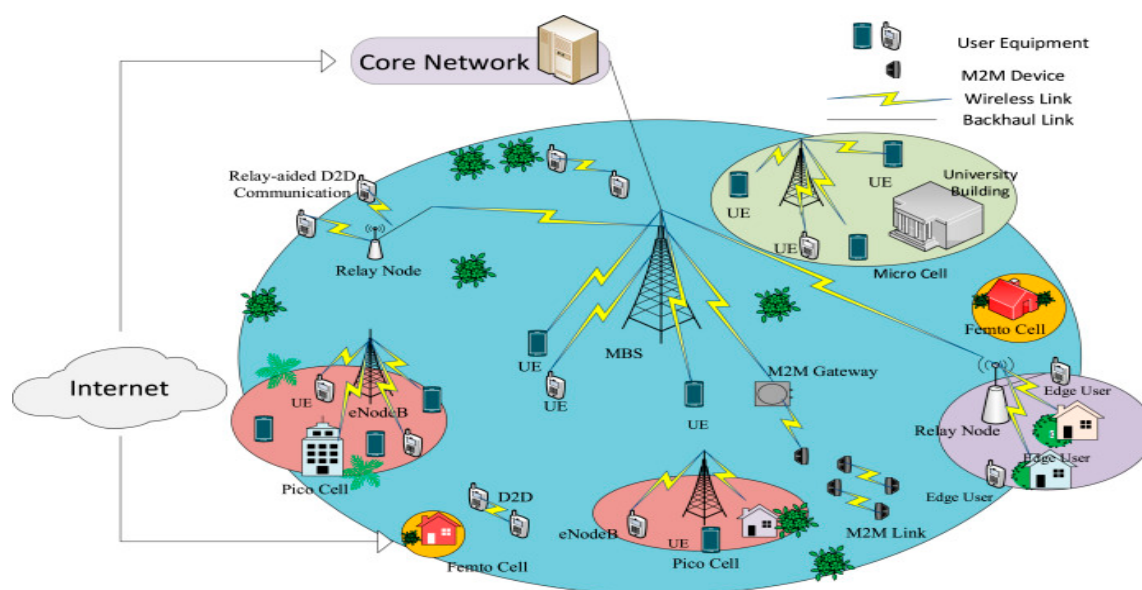


Figure 3. Heterogeneous Networks (HetNet) for Broadband 5G – IoT. Source: <https://www.sciencedirect.com/topics/engineering/heterogeneous-network-communication-system>.

2. The Generations of Broadband Wireless Networks

The Internet of Things (IoT) for the next generation of smart systems must progressively meet the generations of different technologies in this 21st century, as shown in Table 2.1. In this section, we will discuss the history and evolution of broadband wireless networks from the first generation (1G) to the fifth generation (5G). Table 2.1 shows a short historical summary of generational technology evolutions.

First generation: Analog systems are usually called first generation (1G) systems. Most of the devices from this generation had military/Defense as their origin and then moved to civilian services. Most are analog systems, and voice was considered the primary traffic. Some 1G standards are Advanced Mobile Phone Service (AMPS), Nordic Mobile Telephone (NMT), Cellular Digital Packet Data (CDPD), Mobitex, and Data Total Access Communication System (TACS).

Second generation: All the standards belonging to this generation are commercial-based and digital in form. Two main groups were involved, one from Europe and the other from America. The second-generation standards are Global Systems for Mobile (GSM), Digital Advanced Mobile Phone Service (D-AMPS), Personal Digital Cellular (PDC), Communication Service for the Deaf (CSD), and Code Division Multiple Access 2000 (CDMA2000) Enhanced Data for global evolution (EDGE). Second-generation (2G) Technology GSM is widely used worldwide. However, the problem with 2G technology is limited data rates. This makes it inefficient for data transfer applications like video conferencing, music or video downloads, etc. Various new technologies have been developed to increase the speed. The first is 2.5G General Packet Radio Service (GPRS) technology, which transfers data faster than GSM.

Third generation: This deals with systems integrating voice and data, providing higher data rates than 2G systems. The systems in this standard are a linear enhancement of 2G systems. Some 3G standards are wideband CDMA (W-CDMA), Universal Mobile Telecommunications System (UMTS), (3GSM), Freedom of Mobile Multimedia Access (FOMA), 3.5G - High-Speed Downlink Packet Access (HSDPA), and 3.75G - High-Speed Uplink Packet Access (HSUPA). The maximum theoretical data transfer with this 3G technology is 2Mbps.

Fourth generation: This generation is expected to complement and replace the 3G systems. The features of a 4G system might be summarized with one word – integration. The system serves as an open platform where innovations can go with it. Some standards that pave the way for 4G systems are WiMax, WiBro, the proposed third-generation partnerships project (3GPP), and Long-

Term Evolution work-in-progress technologies such as High-Speed Orthogonal Frequency Division Multiplexing (OFDM) Packet Access (HSOPA). The 4G technology allows data transfer up to 100Mbps outdoors and 1Gbps indoors.

Fifth generation (5G): The 5G describes technology developed to send data to mobile phones faster than fourth-generation devices. The deployment of 5G started around 2014/2015. The bandwidth is greater than 1 Gbps. The core network is the Internet. The multiplexing is CDMA. This model of the mobile phone provides fifth-generation technology. In contrast, the 4G utilized microprocessors and personal computers, and the 5G focused on parallel processing, artificial intelligence, and natural language processing. Fourth-generation programming languages are designed for a specific application domain, while fifth-generation programming languages allow computers to solve problems independently.

Table 2.1. A summary of the evolution of the network generations.

Technology	1G	2G/2.5G	3G	4G	5G
Deployment	1970/1984	1970/1999	1990/2002	2000/2010	2014/2015
Bandwidth	2kbps	14-64 kbps	2 Mbps	200 Mbps	> 1gbps
Technology	Analog Cellular	Digital Cellular	Broad bandwidth CDMA/IP technology	Unified IP & seamless	4G + WWW
Service	Mobile telephony	Digital voice, short messaging	Integrated high-quality audio, video, and data	Dynamic information access, variable devices	Dynamic information access, variable drivers with AI capabilities
Multiplexing	FDMA	TDMA/CDMA	CDMA	CDMA	CDMA
Standards	AMPS, TACS, NMT, etc.	TDMA, CDMA, PDC EDGE	WCDMA, CDMA2000	Single standard	3GGP
Switching	Circuit	Circuit/ circuit for access network & air interface	Packet except for air interface	All packet	All packet
Core Network	PSTN	PSTN	Packet network	Internet	Internet
Handoff	Horizontal	Horizontal	Horizontal	Horizontal & Vertical	Horizontal & Vertical

Scheme 2.1. any IoT system must be futuristic in its design to meet the demands of the generations of smart systems of these future generations, such as 5G and beyond. In the next section, we look at how IoT has adapted and continues adapting to 5G smart technologies.

3. Internet of Things for 5G-Related Smart Technologies

One of the technologies that IoT must designed to adapt to is broadband communication smart systems technologies [8]. The "Internet of Things for 5G broadband communication systems" refers to the integration of numerous connected devices (sensors, actuators, etc.) - known as the "Internet of Things" (IoT) - with the high-speed, low-latency capabilities of 5G broadband networks, allowing for real-time data exchange and advanced automation across various industries and applications, like smart manufacturing, smart cities, and connected healthcare. Many authors have discussed how IoT is adapting to the 5G related smart technologies [5,6,8–11]. Figure 4 shows some of the technologies associated with 5G and IoT.

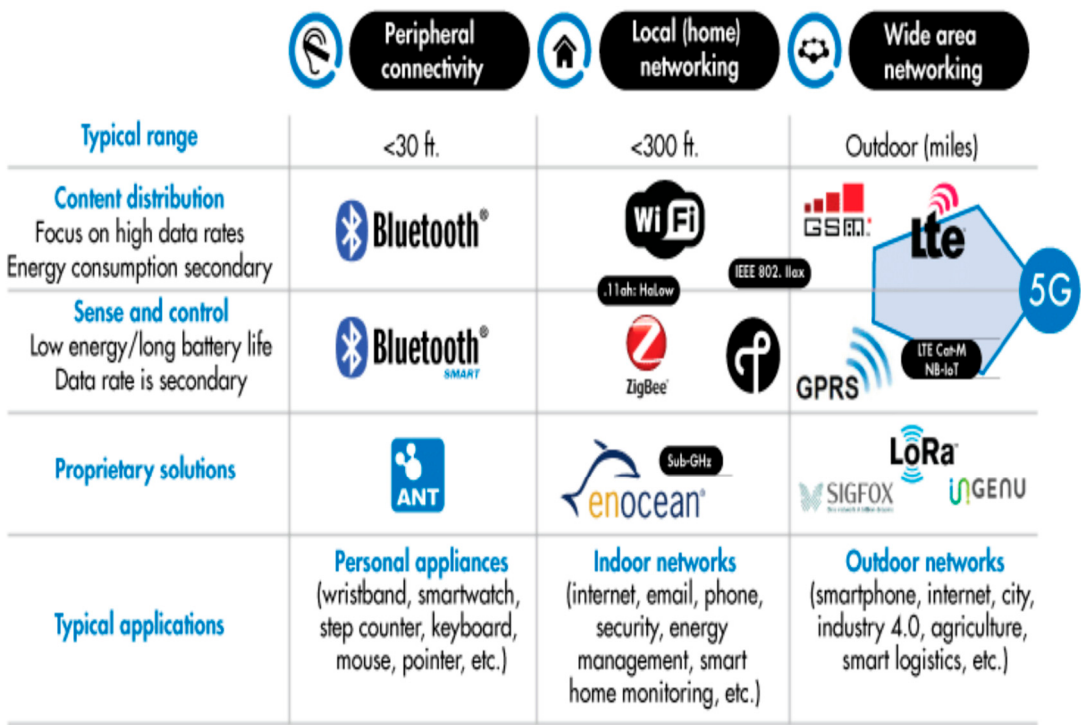


Figure 4. Technologies Associated with 5G-IoT. Source: https://www.researchgate.net/figure/Technologies-associated-with-5G-IoT-21_fig1_332407851.

3.1. Key Points About 5G and IoT

- The Key points about 5G and IoT are as follows:
- **Enhanced connectivity**
5G's high bandwidth and low latency significantly improve the ability to connect many IoT devices simultaneously, enabling rapid data transmission between them.
 - **Real-time applications**
This fast data transfer allows for real-time monitoring and control of IoT devices, enabling applications like predictive maintenance, remote asset tracking, and immediate response to environmental changes.
 - **Massive Machine-Type Communication (mMTC)**
A key feature of 5G designed explicitly for IoT is allowing for efficient communication between many low-power devices.

3.2. Examples of Broadband 5G IoT Applications

- Some examples of broadband 5G IoT applications include:
- **Smart Manufacturing:** Monitoring machine health, optimizing production lines, and real-time quality control.
 - **Smart Cities:** Traffic management, environmental monitoring, street lighting control.
 - **Connected Healthcare:** Remote patient monitoring, wearable devices, and real-time medical data analysis.
 - **Logistics and Supply Chain:** Tracking assets and optimizing delivery routes.

3.3. Facilitation of IoT Using Broadband 5G

The 5G also facilitates IoT in the following ways:

- **Network Slicing:**

Allows dedicated network segments tailored to specific IoT applications, ensuring optimal performance for different device types.

- **Edge Computing**

Processing data closer to the source (IoT devices) reduces latency and improves responsiveness

- **Improved Power Efficiency**

5G technologies like NB-IoT (Narrowband IoT) are designed for low power consumption, ideal for battery-operated IoT devices

4. IoT and Smart Cities

One of the application areas of the IoT and 5G broadband communication systems is “smart cities.” The European Commission defines a smart city as “a place where traditional networks and services are made more efficient using digital and telecommunication technologies for the benefit of its inhabitants and business [12].” Diffusion and the availability of new technologies are required to transform a city into a smart city, contributing to a high level of sustainable urban development and improved quality of life for its citizens.

As shown in Figure 5, smart cities use the Internet of Things (IoT) to collect real-time data to understand better how demand patterns are changing and respond with faster and lower-cost solutions. Digital city ecosystems are designed to run on ICT frameworks that connect several dedicated networks of mobile devices, sensors, connected cars, home appliances, communication gateways, and data centers. It is estimated that by 2025, IoT trends suggest that the number of connected devices worldwide will rise to 75 billion [14]. The increasing number of objects that interconnect generates an unprecedented volume of data that the city can analyze locally to make more informed decisions about what changes or new projects will most benefit residents. The term “Massive IoT” is an apt description of the enormous number of IoT sensors and devices communicating with each other.



Figure 5. A Typical Smart City. Source: <https://www.colourbox.com/vector/smart-city-concept-vector-25128272>.

To achieve a vision in which millions of devices are connected, the IoT standard must ensure both scalability and versatility, offering enough capacity and network efficiency to connect millions

of devices while also providing advanced features—such as longer battery life and a wider coverage area—to facilitate the expansion of new use cases. The existing 4G network was designed primarily to enhance mobile data services; however, it still suffers from numerous limitations. These limitations include poor support for simultaneous connections, high power consumption, and too high a price per bit. 5G is expected to unlock the potential of the IoT and be a driving force for the smart city by addressing and overcoming these issues.

5. The Importance of Providing IoT Security in Future Generations of Smart Systems

IoT (Internet of Things) is growing rapidly and being implemented into devices in many everyday activities such as industrial and commercial environments and personal life, utilizing smart sensor devices at home. However, these IoT devices are faced with many cybersecurity-related issues. The IoT has different layers with different vulnerable areas. Therefore, to defend against these attacks, IoT of the future must consider privacy, security, and trust. We want them to be secure. Hence, finding different ways to secure IoT devices is a necessity in 21st-century applications and implementations. Users' privacy and data protection are critical challenges that need to be addressed in Internet of Things (IoT)-based sensor applications. As IoT technology becomes more closely integrated into everyday systems, lifestyles, and businesses, it generates a greater need for cybersecurity. Cybersecurity encompasses all the technology and operations to safeguard sensor devices and their respective platforms and networks from cyber-attacks. Privacy and cybersecurity are essential considerations for IoT applications because IoT-based sensor devices can collect and store sensitive data. The IoT spawns new businesses and makes buildings, cities, and transport smarter. The IoT allows for ubiquitous data collection or tracking. Still, these useful features are also examples of privacy threats that are already limiting the success of the IoT vision when not implemented correctly. Privacy should be protected in the device, storage, communication, and processing. IoT in monitoring patient healthcare using sensors and devices comes with tremendous security concerns. The recent sophisticated attacks like data integrity, data breaching, and data collusion are significant safety and confidentiality concerns of IoT in IoT-based applications such as healthcare monitoring systems. The IoTs of the future must have the latest advances and developments in algorithms, schemes, and architectures for adequate privacy and cybersecurity application issues.

6. Possible Attacks Challenges on IoT Systems

Some of the possible challenges of the IoT systems are shown in Figure 6. Some of these challenges are security-related. The types of attacks on IoT systems that should be avoided in future generations of Smart systems are as follows:

- **Sybil Attack**

In the Sybil attack, the attacker is presented with more than one identity in a single node, making it challenging to locate the culprit [15]. In the Network layer, this could disturb other nodes and cause them to lose usefulness through incorrect information. More can be seen in Figure 6.

- **Sleep Deprivation Attack**

In the sleep deprivation attack, the attacker keeps the system running to consume the battery, eventually leading to a shutdown [15]. The attack is possible because the Wireless Sensor Network, in the network layer, is powered by finite batteries. An example would be to keep a smart device on until it is powered off.

- **Denial of Service**

A DOS (Denial of Service) attack jams a network with much traffic, causing exhaust or drain resources in the systems [15]. When this type of attack is used in the IoT network layer, it can cause it to be unavailable, thus denying service [16,17]. This type of attack has also evolved into DDoS

(Distributed Denial of Service) when multiple attackers aim for a singular target [18,19]. A DDoS is much more dangerous than a DoS attack.

- **Man-in-the-Middle**

A man-in-the-middle attack is when the attacker sneaks into the communication between two parties [15]. Once inside, the attacker can control or monitor all communication between the two parties they attacked, filtering all information sent between them.

- **Malicious Code Injection**

This is the kind of attack in which the system is injected with malicious code [15]. The attack would give the attacker complete control over the entire network, possibly leading to a shutdown. The injection is done through a node. An example would be a user accidentally downloading malicious code, allowing the attacker to tamper with the user's account(s).

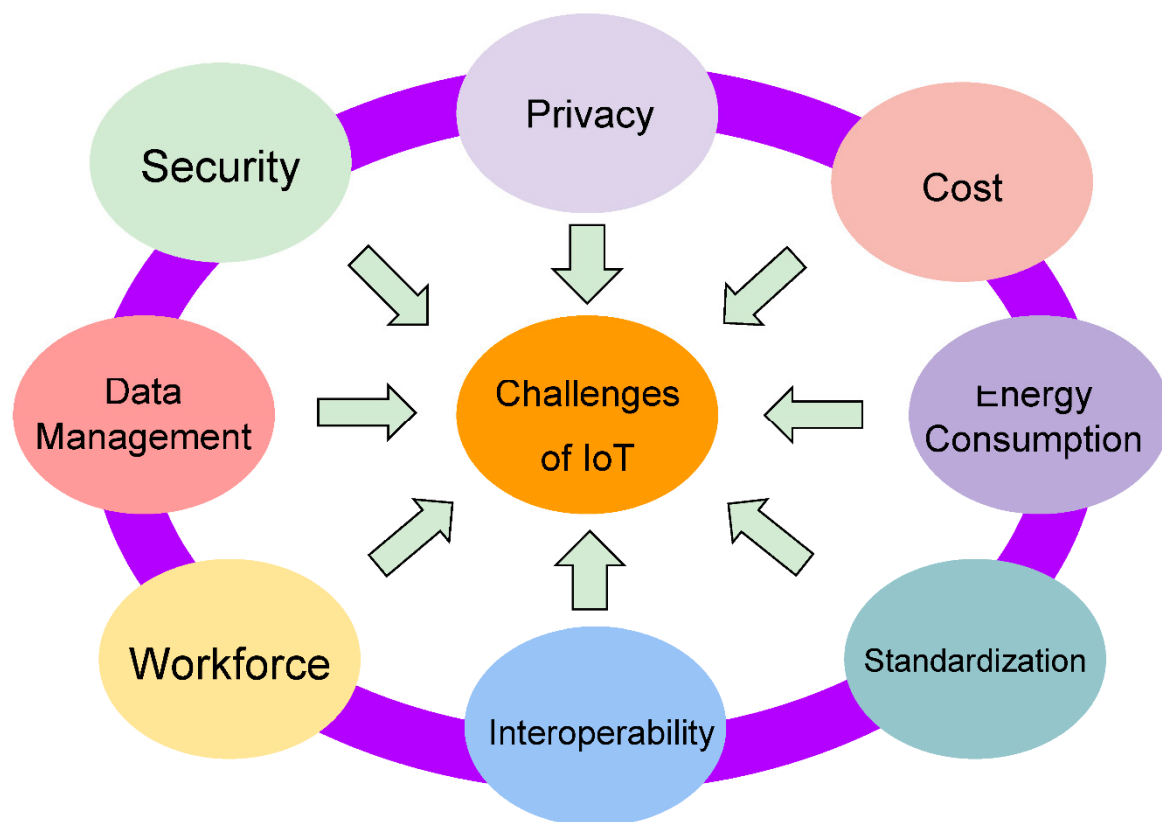


Figure 5. Some Challenges of IoT.

7. The IoT Security Solutions for Future Generations of Smart Systems

The IoT security solutions should closely follow the security solutions for 5G broadband communication systems. It includes strong encryption algorithms, robust authentication methods, network slicing for segmentation, advanced threat detection, secure key management, device identity verification, location privacy protection, and a zero-trust security approach to ensure data integrity and user privacy across the network, especially considering the increased connectivity and potential vulnerabilities introduced by the new technology.

7.1. The Key Aspects of the 5G Security Solutions that Are Pertinent to IoT Security Solutions Are as Follows:

- **Encryption**

Advanced encryption protocols like AES-256 protect data in transit across the network, including user and signaling information.

- **Authentication**

Implement strong authentication mechanisms like SIM-based authentication and enhanced authentication protocols like EAP (Extensible Authentication Protocol) to verify user identities and devices before granting access.

- **Network Slicing**

Creating isolated virtual networks (slices) within the 5G network to segregate critical data from less sensitive data, mitigating the risk of unauthorized access.

- **Device Identity Verification**

Employing mechanisms to verify the authenticity of connected devices through techniques like Equipment Identity Register (EIR) checks to prevent unauthorized devices from accessing the network.

- **Key Management**

Implementing robust key management systems to securely distribute, store, and manage encryption keys across the network, ensuring their integrity and preventing unauthorized access.

- **Threat Detection and Response**

Utilizing advanced threat detection systems with machine learning capabilities to identify and respond to potential security threats in real time.

- **Location Privacy**

Employing techniques like location masking and pseudonymization to protect user location data and prevent tracking.

- **Zero Trust Network Architecture**

Implementing a "never trust, always verify" approach where every device and user must be authenticated and authorized before accessing network resources, even within the trusted network.

7.2. Other Solutions for Security Issues with IoT

There are many ways in which the IoT can be used as an attack. If these problems were left alone, important information could be stolen and IoT devices hacked. We need solutions to these problems. The solutions we find may not rely on cybersecurity.

- **Trust, Privacy, and Security**

Key things to remember when working with cybersecurity in IoT are security, privacy, and trust [20]. These factors apply to the people behind the machine and the machine itself. Trust must be gained between machines to grant access [21]. One solution is for parties to exchange requirements and capabilities to settle privacy, trust, and confidentiality [22]. Intrusion detection systems can decrease the amount of cyberattacks [23].

- **Logistic Regression**

Logistic regression is a model to determine the probability of an event [15]. In [24], logistic regression is tested to detect botnets apart from the IoT. The result is that Logistic regression can be used to find botnets during a propagation phase. To learn more, read into [24].

- **Proper Application**

Using the proper application of IoT would also help improve its security. Using the IoT for what it was not intended for could expose it to dangers it was unprepared for. An example of improper application would be using a water sensor for something other than water.

- **Improved defensive measures**

Improving the defensive measures of already existing cybersecurity techniques. Using the vulnerabilities mentioned in [25], one could develop a new defense against possible threats.

- **Implementing defense practices**

Apply defense practices to everyday life. Some cases of victims getting hacked are mainly because they are unaware of how vulnerable their smart devices. Some IoT devices do not have their defensive measures activated and suffer. If everyone practiced applying the basic defense of their IoT devices, there would be fewer cases.

8. Recommendations

The Internet of Things (IoT) for Next-Generation Smart Systems must have the following:

1. It must be designed to adapt to future generations of technologies, such as 5G and beyond.
2. The IoT standard must ensure scalability and versatility, offering enough capacity and network efficiency to connect millions of devices while providing advanced features—such as longer battery life and a wider coverage area—to expand new use cases.
3. The IoTs of the future must have the latest advances and developments in algorithms, schemes, and architectures for adequate privacy and cybersecurity application issues.
4. The IoT security solutions should closely follow the security solutions for 5G and beyond broadband communication systems.
5. To achieve a vision in which millions of devices are connected smartly, the IoT standard must ensure both scalability and versatility, offering enough capacity and network efficiency to connect millions of devices while also providing advanced features—such as longer battery life and a wider coverage area—to facilitate the expansion of new use cases.
6. The smart IoT of the future must require new network capabilities to support a massive number of smart devices and efficient software and hardware platforms for both devices and networks.
7. The future IoT should require close partnerships among many industries and ecosystems to offer integrated computing and communication capabilities.
8. IoT of the future must consider privacy, security, and trust issues in its cyber security framework.

9. Conclusion

IoT is a revolutionary technology that has the potential to disrupt our lifestyle; various technologies and businesses connect smart things or devices equipped with sensors. When it comes to the Internet, the Internet of Things (IoT) has taken center stage for the next generation of intelligent systems. In this paper, we have discussed what it will take for IoT to meet the demands of next-generation smart systems in terms of design and adaptability. We have also discussed the possible challenges and made appropriate recommendations necessary to meet those challenges. The future IoT must be designed to adapt to future generations of technologies, such as 5G and beyond, and be smart enough to meet these security challenges.

References

1. Connected Things, IoT & 5G by Dr.-Ing. Eueung Mulyana <https://eueung.github.io/ET3010>)
2. <http://postscapes.com/what-exactly-is-the-internet-of-things-infographic>
3. Li, Shancang, Li Da Xu, and Shanshan Zhao. "5G Internet of Things: A survey." *Journal of Industrial Information Integration* 10 (2018): 1-9.

4. J. Liu, N. Kato, J. Ma, and N. Kadowaki, "Device-to-device communication in LTE-advanced networks: A survey, *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 19231940, 2015.
5. Rahimi, Hamed, Ali Zibaeenejad, and Ali Akbar Safavi. "A Novel IoT Architecture based on 5G-IoT and Next Generation Technologies." *2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*. IEEE, 2018.
6. Ahmed, Rizwan, et al. "Comprehensive Survey of Key Technologies Enabling 5G-IoT." *Available at SSRN 3351007* (2019).
7. Kramp, Thorsten & Kranenburg, Rob & Lange, Sebastian. (2013). Introduction to the Internet of Things. 10.1007/978-3-642-40403-0_1, 2013.
8. Shahram G.N. Reshaping mobile broadband with 5G communication technologies, 5G World Summit, 2014.
9. Connected Things, IoT & 5G by Dr.-Ing. Eueung Mulyana (<https://eueung.github.io/ET3010>)
10. Li, Shancang, Li Da Xu, and Shanshan Zhao. "5G Internet of Things: A survey." *Journal of Industrial Information Integration* 10 (2018): 1-9.
11. Rahimi, Hamed, Ali Zibaeenejad, and Ali Akbar Safavi. "A Novel IoT Architecture based on 5G-IoT and Next Generation Technologies." *2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*. IEEE, 2018.
12. Ahmed, Rizwan, et al. "Comprehensive Survey of Key Technologies Enabling 5G-IoT." *Available at SSRN 3351007* (2019).
13. Smart Cities, <https://commission.europa.eu/eu-regional-and-urban-development/topics/cities-and-urban-development/city-initiatives/smart-cities>, retrieved February 20, 2025.
14. https://www.researchgate.net/figure/Internet-of-Things-prediction-from-2014-to-2025-in-billions_fig2_339121533
15. A. Abdullah, R. Hamad, M. Abdulrahman, H. Moala, and S. Elkhediri, "CyberSecurity: A Review of Internet of Things (IoT) Security Issues, Challenges, and Techniques," in 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, 2019.
16. C. Sharma and N. K. Gondhi, "Communication Protocol Stack for Constrained IoT Systems," in 2018 3rd International Conference On Internet of Things: Smart Innovation and Usages (IoT-SIU), Bhimtal, 2018.
17. L. Liang, K. Zheng, Q. Sheng and X. Huang, "A Denial of Service Attack Method for an IoT System," in 2016 8th International Conference on Information Technology in Medicine and Education (ITME), Fuzhou, 2016.
18. B. Kepçeoğlu, A. Murzaeva and S. Demirci, "Performing energy consuming attacks on IoT devices," in 2019 27th Telecommunications Forum (TELFOR), Belgrade, 2019.
19. L. Huraj, M. Simon and T. Horák, "IoT Measuring of UDP-Based Distributed Reflective DoS Attack," in 2018 IEEE 16th International Symposium on Intelligent Systems and Informatics (SISY), Subotica, 2018.
20. J. R. C. Nurse, P. Radanliev, S. Creese and D. D. Roure, "If you can't understand it, you can't properly assess it! The reality of assessing security risks in Internet of Things systems," in *Living in the Internet of Things: Cybersecurity of the IoT - 2018*, London, 2018.
21. V. B. Reddy, A. Negi, S. Venkataraman, and V. R. Venkataraman, "A Similarity-based Trust Model to Mitigate Badmouthing Attacks in the Internet of Things (IoT)," in 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), Limerick, 2019.
22. U. M. Mbanaso and G. A. Chukwudebe, "Requirement analysis of IoT security in distributed systems," in 2017 IEEE 3rd International Conference on Electro-Technology for National Development (NIGERCON), Owerri, 2017.
23. R. Gurunath, M. Agarwal, A. Nandi and D. Samanta, "An Overview: Security Issue in IoT Network," in 2018 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2018 2nd International Conference on, Palladam, 2018.

24. A. O. Prokofiev, Y. S. Smirnova, and V. A. Surov, "A Method to Detect Internet of Things Botnets," in 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), Moscow, 2018.
25. N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum and N. Ghani, "Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations," IEEE Communications Surveys & Tutorials (Volume: 21 , Issue: 3 , third quarter 2019), vol. 21, no. 3, pp. 2702-2733, 11 April 2019.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.