EasyChair Preprint

№ 6954

The Impact of IOT on Real-World Decisions in the next Stage

Abdulhakeem Amer Abdulameer and Raafat K. Oubida

October 30, 2021

THE IMPACT OF IOT ON REAL-WORLD DECISIONS IN THE NEXT STAGE

Abdulhakeem Amer Abdulameer [1, a], Raafat K. Oubida[2.B]

[1] *Al-Nahrain University, Collage of Information Engineer (CoIE) , Baghdad, Iraq*
[2] *Al-Nahrain University, Collage of Information Engineer (CoIE) , Baghdad, Iraq*

[a)] *abdulhakeem@coie-nahrain.edu.iq*
[b)] *raafatoubida@gmail.com*

Abstract. Technology and IoT have improved significantly in recent years. The Internet of Things (IoT) allows devices to self-identify. IoT uses electronic and RFID technology to collect and distribute data. The IoT is supposed to change our lives. Thus, IoT connects everyone. It lets things communicate, share information, and make judgments. The future of IT matters a lot. Physical items will be related to boosting decision-making intelligence. Outside of metropolitan areas, satellite-based Geographic Guidance Systems (SGGS) is the most cost-effective and efficient way to gather geographic and temporal distribution data. Thirty billion connected IoT devices worth $2.5 trillion by 2022. Some estimates put the IoT's global commercial impact at $15 trillion by 2025, with 120 billion linked devices. Regulators can help IoT adoption and implementation by protecting customers and network security. Regulators can consider ways to promote IoT growth. Improve LTE Advanced and 5G networks and assess IoT spectrum needs. They encourage commercial use of IPv6 through government programs and public procurement. They facilitate interoperability and give consumers easy access to their data. Encourage global standards and remote SIM usage. Regulators should prioritize privacy and security to enhance public trust and IoT adoption. On the IoT sector, SGGS, theoretical foundations, legal and regulatory ramifications.

INTRODUCTION

Due to incorporated computational intelligence, 5G enables speeds of up to 10Gbit/s, higher data bandwidth, and lower latency. Connectivity will be enhanced through the usage of a variety of connected devices and services. It will be made possible by vast computer power and the architecture of virtual systems. Connecting millions of devices and sensors to robust digital networks would assist healthcare, transportation, and other industries.

Bear in mind that 5G is a comprehensive technology for data transfer to computers. 5G can sense data from billions of devices rather than just a few with the right processing platform [1].

Wherever linked devices exist, personalized, immersive, and enhanced experiences will be possible. Invisible connectivity will be enabled via low-cost devices and sensors [2]. In the future, systems will behave according to user preferences rather than following a computational command.

Technological advancements are bringing us closer to establishing a networked civilization. M2M learning is enabled via the IoT [3]. The IoT enables the safe exchange of data between physical objects and applications. It is what the IoT is all about.

The number of connected gadgets continues to expand. Smartphones and personal digital assistants are highlighted intelligent decision-making and data transmission through the Internet. Constructing a sensor network with personal, professional, and financial rewards is doable.

Making judgments and acting are two distinct systems. They are easily recognizable and easy to use via cyberspace. These items are supplied with RFID devices or are equipped with advanced sensor systems that can read barcodes. The processing unit receives sensor data through the Internet, and you can increase your efficiency with sensors. The decision-making and action-invoking systems determine which automated actions should be performed. The evolution of the Internet with IoT services is depicted in Figure 1. Things can contribute to the development of a more synergistic Internet. This essay considers the prospects for a future Internet in which "things" are fully supported. The article discusses current, and prospective IoT uses [4]. The IoT is a hot topic in academia, industry, and government.

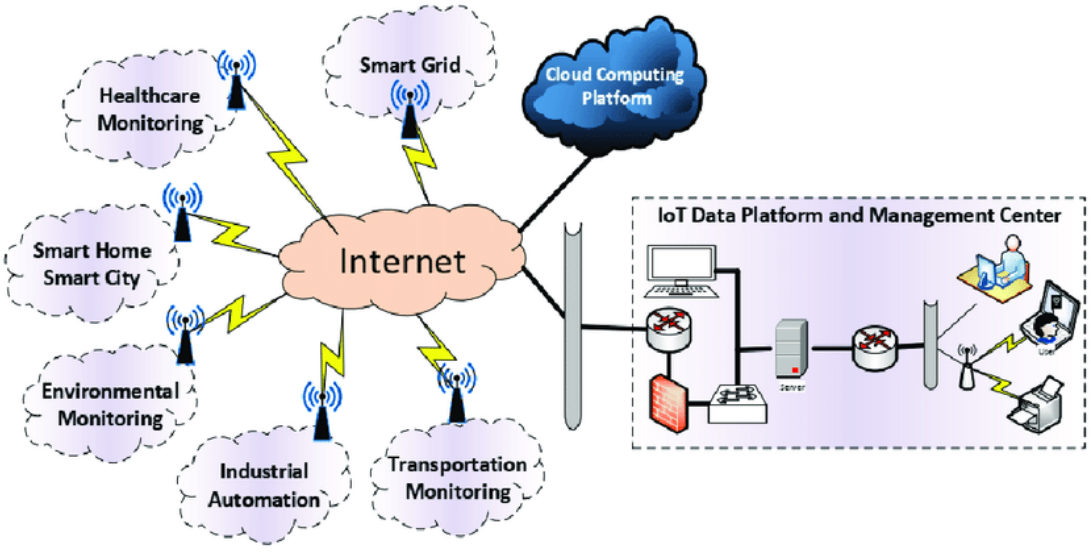

Figure1: The generic IoT scenarios

BUSINESSES AND RESEARCH ORGANIZATIONS

The businesses and research organizations have forecasted the IoT impact on the Internet and financial system in the following years. Before 2020, it is anticipated that there will be roughly 24 billion Internet-connected devices. Huawei expects 145 billion IoT networks by 2025 [5]. The global economic effect will be $11.1 trillion. Users will receive around 90% of the value generated by IoT applications (businesses, other organizations, and consumers). By 2025, remote patient monitoring may save $1.1 trillion annually.

By 2020, 5G will connect 50 billion devices, 212 billion sensors, and 44 zettabytes of data. There will be coverage of all types of mobile devices and remote monitoring systems. Such a large amount of "useful data" will be generated. Academics assert that this networked environment will enable a 35% increase in digital data consumption over the previous 8%. In the coming years, the amount of bandwidth generated by internet-connected gadgets is likely to increase. Cisco forecasts a 40% growth in Internet traffic from non-PC devices by 2020. According to Cisco, M2M links (commercial, housing, healthcare, transportation, and some other IoT Devises) will increase from 25% in 2016 to 45% in 2020. These changes may result in a redefining of the term "online" during the next decade. By 2020, roughly 8 billion SGGS units will be installed worldwide, up from 5.8 billion in 2017. As of 2017, there were 5.4 billion smartphones and 380 million SGGS receivers in use worldwide. Even though the professional market has fewer SGGS devices than the mass market, it has grown. Every day, millions of people profit from their use in sustainable agriculture, efficient transportation, and SGGS-synchronized communications. These downstream markets offer services such as transportation fleet management systems and smartphone apps. By 2025, sales of SGGS-enabled added-value services will exceed € 200 billion, more than 2.75 times the projected revenue from SGGS devices and services. Latest technology concepts for example the IoT as well as Intelligent Cities [6] enable hybrid and crosscutting applications.

GENERIC ARCHITECTURE

As recommended long ago, the Online world uses the TCP/IP network protocols for network communication. However, as the Internet links smart objects, traffic and storage requirements will increase exponentially. As a result, the IoT growth [7] is contingent upon new applications and technological advancements. The IoT topology is depicted in Figure 2 as a four-tiered structure. The following is a brief description of these layers:

1) Additionally, the Perception layer is referred to as the Device Layer [8]. There are both physical and sensory devices included in this category. Depending on the object, it may be RFID, 2D barcodes, or infrared. This layer is primarily concerned with detecting and collecting information about things. Indicators can provide information on the position, temperature, direction, motion, humidity, and chemical changes in the air. They can also be used to detect explosives. The network layer secures the data transit from the data processing system to the network layer.
2) Transmission Layer is another name for Network Layer [9]. This layer secures data transmission from sensors to the information processing system. Infrared, Wi-Fi, Bluetooth, and 3G are examples of technologies used to transmit data. As a result, data is sent from Perception to Middleware via the Network layer
3) Between the application and the network layers, there is a divide [10]. This layer provides services to clients and stores data from the lower layers in a database. Visualization techniques [11] are becoming increasingly crucial as the IoT generates vast volumes of data. It analyzes data and computes ubiquitous calculations before making an independent conclusion.
4) The application layer manages applications using data that has been analyzed and obtained by the middleware [12] They are also used in e-health and environmental and energy management. [13].

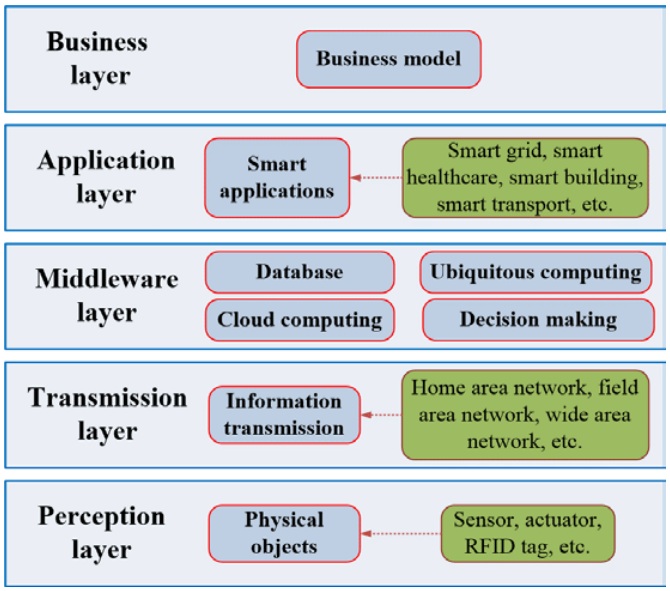

Figure 2: IoT foundation layers

APPLICATIONS FOR IOT

Even though the IoT is a segmented deployment environment, it comprises a varied range of applications, some of which are listed here.

1) Smart cities [14] can better manage resources, withstand disasters, and integrate critical behavior. We can use the IoT to help solve urban issues like intelligent lighting, water/gas leak detection, dynamic parking costs, and automated parking assistance. Ubiquitous Vision can also provide crucial information on population behavior and citizen needs [15]. The IoT idea provides omnipresent and augmented surveillance by monitoring human impacts and improving service matching. It may also produce real-time remotely sensed data of cities to reduce pollution and identify noise hazards [16]. Smart watering of parks and green spaces is another potential use of IoT. The IoT will also help secure smart infrastructures (e.g., Unattended baggage and suspicious conduct can be identified automatically by software) [17] In addition to reliable automatic meter reading, the IoT architecture will help clients get their energy, gas, and water bills. Motion-activated streetlights can be turned on and off dynamically based on zone activity. It can save energy (and money) while preserving security. Smart tourism promises to provide guests with an immediate experience of the city, including

accessibility, crowded areas, and peace of main attractions—improved material management by identifying potentially hazardous waste that requires specialized disposal.

2) Healthcare: IoT technologies can be applied in a variety of ways [18]. They can help improve existing assisted housing situations. A patient's body temperature, blood pressure, heart rate, glucose, and oxygen levels will be continuously monitored by sensors. The data from other sensors will be used to monitor people's health behaviors at home. To provide comprehensive remote monitoring and prompt response, data from the local site will be collected and transmitted to small medical institutes [19]. Because such sensors are interconnected, they could provide a comprehensive view of health indicators, triggering immediate treatment when situations threatening health are discovered.
3) The availability of massive patient data allows for unprecedented correlation studies, model development, early treatment, and much more efficient and successful medication discovery [20]. The elderly and disabled face similar concerns, as continual non-intrusive monitoring improves care while safeguarding individual autonomy and relieving hospitals. Remote supervision also allows specialists to work with more people and patients, reducing costs [21].
4) Modern sensor, information, and network technologies will make it possible to regulate and manage transportation operations more effectively. For example, computerized highway tolls, mobile emergency command and scheduling, traffic congestion avoidance, reporting, and delay reduction are all possible applications of intelligent transportation technology. Sensors and/or actuators can be found in automobiles, trains, buses, and bicycles, resulting in a Mobile Sensor Network (MSN) [22]. Tags and sensors for traffic control are mounted on highways, railroads, and freight vehicles. External sensors can be installed in cars to monitor pollution, humidity, and temperature. Innovative vehicles can assist in making transportation more environmentally friendly, brighter, and safer. Driving guidelines, for example, can help you save money on gas and prevent pollution. Google Traffic uses User-contributed data to track traffic. Intelligent traffic signals allow cyclists and vehicles to cycle and drive safely [23]. Automated traffic light orchestration may be achieved by merging smartphone data from cyclists and sensors with metropolitan traffic signal infrastructure. It may monitor space environments across the

supply chain, track products, and process payments depending on geography or activity time for public transit, theme parks, and other applications. It includes directing clients around the store using a predefined list, speedy fee procedures like biometric order-out, recognition of possible allergies in products, and fully automated rotations in shelves and warehouses. Items are located, fleets are tracked, containers are opened for insurance purposes, items are searched on the surface such as warehouses, and warnings are emitted on containers holding flammable goods near containers containing explosive devices.

5) An improved power system saves energy, reduces pollution, increases supply security and reliability, and reduces grid transmission. Sensors for energy in smart grids can help track and measure faults and usage. Home and building energy management [24] are also linked concepts Manufacturing companies may increase their energy productivity and competitiveness by collecting data from IoT devices.
6) Using advanced metering and knowledge management, Facilities Smart Energy software tracks reports and warns operational staff in real-time. These methods can give real-time building and infrastructure performance data. Materials and equipment data from other subsystems can also be shown.
7) Heat and light in a room are adjusted according to the number of audience members, time of day, weather, and a utility bill, by Increasing the amount of energy produced and consumed. The HEM system contains apps that monitor energy usage [25] and power management sensors that respond to a fluctuating power source. Combining these technologies can significantly minimize total energy use and carbon pollution from homes. The IoT can also help identify and prevent crimes.

SMART AGRICULTURE

A network of sensors can detect sensitive portions of land and inform the farmer via telecommunications infrastructure [26], such as text messaging. Improved seeds storage, fertilizer, as well as pest management technology are aspects of this. Intelligent agriculture systems will help agronomists comprehend plant growth models and optimal farming practices by knowing land and climate. Eliminating inefficient farming practices will significantly increase agricultural output. Watching water level differences in rivers, bridges, and reservoirs are all instances of IoTs role in water management [9].

MONITORING OF THE ENVIRONMENT

Wireless devices and IoT technologies that have been identified will be used in eco-friendly maintenance and other green requests in the future [27]. Biomonitoring, remote sensing, soil, water, and environmental monitoring will become more prevalent in environmentally friendly projects worldwide. The IoT can help collect recyclables and dispose of electronics (RFID used to identify electronic subcomponents of personal computers, mobile devices, and other consumer electronics products to increase the re-usage of these subparts and to reduce e-waste). An important IoT application. Industry, transportation, and agriculture must cut emissions. They track emissions and forecast fire conditions to detect forest fires. All of these variables are recorded. Water Quality Keep an eye out for garbage and hazardous substances being dumped into rivers and oceans to prevent contamination and preserve drinking water quality [28]. River Floods, Waters, rivers, and lakes are all monitored on wet days. Wild animals are tracked using GPS/GSM collars and their positions are communicated via SMS [29].

EMERGENCIES & PROTECTION

Controlling perimeter access, detecting the presence of liquids, monitoring radiation levels, and detecting explosive and poisonous gases just are a few examples. Monitoring secure areas, tracking personnel and assets, administering infrastructural facilities, and generating alarms are all possible with perimeter rights. Liquid presence detection is used to detect liquids in baseline performance, warehouses, and the fields of important buildings. Nuclear power plants monitor radioactivity to determine whether there is a leak. The final IoT application monitors [30] gas levels and detects leaks in industrial, industrial, and mining settings. By detecting vibrations and taking appropriate action in advance, sensors, autonomous coordination, and modeling can aid in the prediction of earthquakes and tsunamis.

IOT, AS A PRACTICAL SYSTEM.

Tsunami Detection Technique is an IoT application [31]. This technology is often used in Japan to identify tsunamis early by continuously monitoring the sea level. Numerous sensor-equipped buoys and miniature earth stations will be deployed around Japan. The sensors detect variations in wave height and transmit the data to the satellite via the small ground stations. It will require many sensor terminals to cover the entirety of Japan swiftly. Due to the base train's remote

location, it is difficult to relay data quickly to the base station through ground-based wireless networks from many sensors' terminals Figure 3.

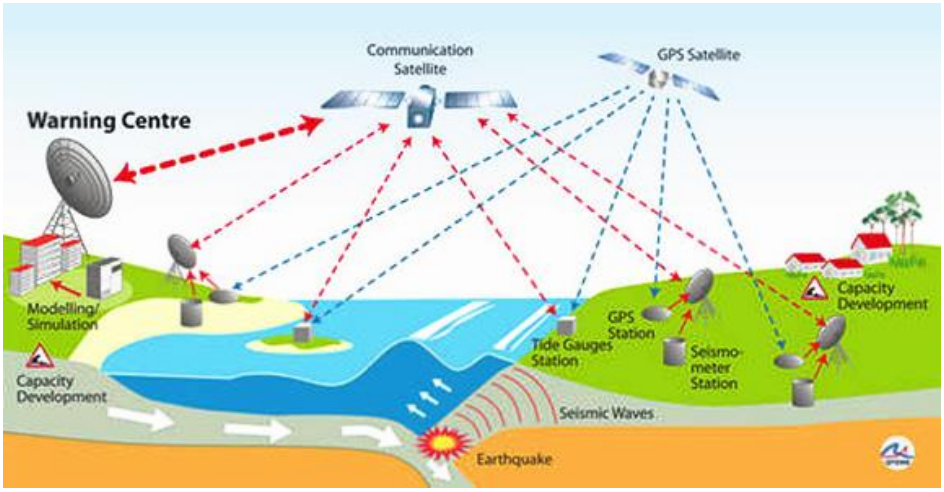

Figure 3: Tsunami warning system

As a result, data from measuring device stations to the base station is delivered through satellite broadcasting. The satellite's extensive coverage allows data from sensing stations all over Japan to be collected. Figure 3 shows a Tsunami warning system architecture [32]. This system's sensors use GPS to track changes in Z-axis location, and the Z-axis shows a change in water levels. The data is sent by satellite to a base station and analyzed to distinguish tsunamis from ordinary waves. As a result, the ground station can detect tsunamis. This technology will help identify tsunamis early, saving lives.

OPPORTUNITIES AND CHALLENGES

The Internet should benefit everyone, regardless of their geographic location, socioeconomic status, or geographic location. The abilities and values that drive our lives and technology's growth are global. The same logic applies to the future benefits and problems of the IoT. The IoT introduces new legal aspects and may exacerbate previously existing ones. Sharing, deciding, and respecting users are critical concerns for a law that is evolving. This section discusses these subjects, as well as legal, regulatory, and human rights issues. We'll start by analyzing these themes, highlighting the major components of each, and offering conversation points.

1) The security of IoT devices and apps is critical to their widespread adoption [33].

Decision-makers are hesitant to implement IoT solutions globally unless system-level secrecy, authenticity, and privacy are assured. People are much less likely to use the Internet if they doubt their connected devices and secure data. Indeed, the industry should prioritize IoT product and service security. As more devices connect to the Internet, more chances arise to exploit security holes. Bad actors can re-program or break IoT devices, opening doors for cyberattacks. Poorly constructed devices leave data streams unsecured, allowing data theft. Device failure or malfunction might lead to security issues. The IoTs tiny, low-cost intelligent machines and the traditional Internet connectivity endpoints (PCs) face these challenges. Manufacturers of IoT devices have economic and technical constraints that make adequate security precautions challenging to design into these devices, thus exposing them to more security and long-term maintainability issues.

2) The proliferation of the IoT nodes may open the door to attack chances [34]. Because of the increasing interconnection of IoT devices, any unsecured device linked to the Internet could threaten the overall security of the global Internet. No item can be guaranteed to be safe, and we're becoming more interconnected and reliant on Smart nodes for essential tasks like healthcare. Physical access to IoT equipment may be accessible while actual protection is difficult or impossible. The danger of a device being hacked dictates its security. These figures are influenced by present and future security concerns, the anticipated costs of harm, and the estimated cost of risk mitigation. They recommend two types of internet security measures.
3) Each network with restricted access should contain all IoT devices that require direct internet connectivity. It will be simpler to keep an eye on the network part of a gadget for unusual traffic. The protection of personal information and data security must be improved. Businesses should invest in a secure structure. The training and understanding on how to secure IoT devices will significantly reduce the potential threat.
4) IoT Privacy governs how data about a user can be accessed. IoT privacy is required due to the envisioned application domains and technology. Because of a lack of adequate methods for preserving the confidentiality of private or confidential data in the healthcare industry, the installation of IoT technologies has accelerated. With the IoT concept, development in technology will play a significant role as well [35]. The widespread use of wireless data transfer may result in the emergence of a new privacy concern. Wireless

channels' remote access capabilities increase the risk of compromise, exposing the system to surveillance and disguised attacks.

5) Because IoT devices transform how personal data is gathered, processed, used, and secured, it reframes the privacy debate. Occasionally, when the person's privacy desired response and those of the measurement device, the user may be completely unaware that an IoT device is collecting and potentially disclosing personal information to a third party. Consumer goods, such as smart TVs and game consoles, are increasingly collecting data. These systems employ voice control or Vision to continually listen to conversations or watch room activity and transfer data to the cloud service, including a third party, for processing. Without a person's knowledge, these devices can record their conversations or activities. These features may be valuable to a knowledgeable user. Those ignorant of their existence and therefore unable to control how their data is used may face a privacy danger. Customized data streams can be beneficial for businesses and organizations looking to collect and profit from IoT data. The requirement for providing information draws attention to the legal issues around data privacy. People are concerned about security and have expectations about the information collected about them because of how third parties can utilize it to benefit them. This privacy protection principle applies to the IoT data. Still, the ability of the user to express and implement privacy preferences could well be limited by the devices used to collect the data. Privacy concerns may hamper the rise of the IoT.
6) Interoperability/Standards for the IoT Interoperability enables innovators and cost-cutters in the IoT device industry, improve the market's total value [36]. The primary need for Internet connectivity is interoperability; "connected" machines must "share a language" of protocols and encodings. Internet users' ability to connect, communicate, exchange, and invent, all of which are necessary components of interoperability, can be disallowed. Any IoT device or system can communicate with another IoT device on a network and exchange data as required. It occurs at various tiers of the protocol stack that connects the devices. The issue of IoT interoperability is centered on the standardization and acceptance of protocols that define these communication characteristics. Due to a lack of guidelines and principles, the ability of IoT machines is limited. In the lack of set standards, IoT devices may act erratically. Appliances that are not designed and set

correctly can significantly impact the networks to which they connect and the Internet. Interoperability, along with technological aspects, influences the economic consequences of IoT. Interoperability that is well specified can drive innovation and efficiency among makers of IoT devices, hence improving the market and the global economic value. To accomplish these goals and it is necessary to implement open standards and to develop new ones.

7) Both parties face constraints. Advanced computing and current services are increasingly integrated into items [37]. Additionally, it has accelerated the development of compact, low-cost sensor devices that are at the heart of many IoT applications. As the number of Devices connected increases, their traffic increases as well. Increased network capacity is required to evaluate and store a massive amount of data. Large and dynamical databases enable large-scale data gathering, correlation, and analysis. Manufacturers must address technology, thing, and economic constraints while creating IoT products. Specific devices are limited by technical limits, such as processing speed, memory capacity, and battery consumption. To lower unit costs, companies also should reduce expenditures associated with equipment and the manufacturing industry. - Companies do cost-benefit studies to see if the higher costs and, in some circumstances, decreased performance related to standardization outweigh the benefits of standardization in their industry. In the short term, designing connectivity into a product and testing for standard conformity may be costly.
8) Using proprietary protocols and systems can save money in some circumstances [38]. However, the benefits of compatibility throughout a product's lifecycle must be evaluated. Because many IoT devices are not correctly disposed of away after use, the IoT requires billions of batteries. Energies harvested from ambient sources (such as vibration, light, or temperature) could become the accepted practice for future energy-efficient products. These devices have recently proven to be as good as their rechargeable equivalents, and they are a long-term solution.
9) Instruction and Public Strategy Concerns Several regulatory and legal difficulties are raised by the adoption of IoT devices, and these issues must be thoroughly explored. Legal and regulatory frameworks are lagging technological advancements. The IoT creates a slew of legal, regulatory, and privacy concerns. IoT devices worsen current

legal and policy difficulties while also making new ones. When new IoT devices are released while conforming to existing accessibility standards and guidelines, accessibility issues for people with impairments develop. However, the sheer number of wireless IoT methods and the resulting wireless broadcasting interference and delay make the already tricky task of managing RF spectrum consumption even more difficult. Intellectual capital, environmental (e.g., device disposal), and legal ownership are emerging legal and regulatory issues for IoT devices.

10) Complexity increases when determining where in an IoT system design the intended objectives should be achieved. Should the device, data flow, gateway, user, or cloud storage be regulated? Consumer protection rules and regulations are increasingly being incorporated in IoT device regulatory analyses. Assessing the legal implications of IoT devices can help with privacy and security issues, among other things. Sometimes, IoT devices present new legal, regulatory, and human rights issues.
11) Data Security on the IoT. Data collected by IoT devices can be freely sent across national borders, and they communicate over the Online platform, which allows them to communicate across all geographical boundaries. Using IoT devices makes it feasible to collect data on people in one location and send it to the next for storage or processing. If the information gathered is deemed personal or confidential, it may rapidly become a matter of legal significance. Cross-border data transfers raise concerns regarding the legitimacy of any applicable rules in the face of these concerns [39].
12) How does the applicable regulatory framework control the equipment that collects data and its storage and uses? A lot of questions arise because of this predicament. Are there ways to minimize Internet fragmentation while yet maintaining customers' rights? Should a jurisdiction with stricter tech data protection laws automatically enforce those regulations on other jurisdictions? With these devices and systems connected automatically in the future, data can be transmitted across national borders. Even if users are entirely unaware of the facts, they may be held guilty for passing data transfer responsibilities. These are complex issues, which are complicated even more by the fact that technology advances at a faster rate than policy.

Liability exists for devices connected to the IoT. Because the IoT devices is becoming more complex, it's essential to investigate intricate liability issues. Devices connected to the IoT, for example, could be used in unexpected ways by the maker. Before delivering a product, IoT device makers cannot possibly consider all possible eventualities. The IoT can link and interact in unforeseen ways. Eventually, these gadgets may be able to establish their own ad-hoc networks. As a result, neither the manufacturer nor the user can predict all complications. Intelligent cars will adjust their driving behavior in response to sensor inputs from the IoT devices using adaptive machine-learning algorithms IoT. These systems' actions are impossible to predict or test thoroughly. These situations make me anxious. How well do existing responsibility standards identify the parties' liability risk? Can IoT applications that learn from their surroundings be held accountable? What happens when users, not algorithms, control decision support systems? Should IoT devices obey me? The present product liability laws will be extended to internet-connected goods. Is there whatsoever the public can do to assist elites avoid biased information?

CONCLUSION

In today's increasingly linked world, the IoT refers to the billions of connected gadgets that exist. The potential of this technology is enormous, connecting machines and people and enabling new levels of world inquiry. It's a huge potential, but it's also a risky proposition for society and infrastructure. Knowledge, protection, confidentiality, interoperability and standardization, legislation and official strategy, and worldwide challenges were all considered in this article. In the event of IoT cyberattacks, device performance and dependability must be adequately examined. Separating valuable network assets could be the most effective approach to safeguard them. In a future of apparent ubiquity and an omnipresent network of networked devices, new communication and middleware systems, high-performance implants, and computer technologies will be required. It's vital to standardize IoT communication protocols and technical enablers. More importantly, every IoT design, development, and deployment should consider security, privacy, vulnerability management, and interoperability. The legacy of devices must be felt when they are used for a long time. Interoperability with future IoT devices is a must. 'Secure by default' should be the default setting on all devices. Owners of IoT devices, networks, and data

must be organized responsible when problems arise, specifically as AI and machine learning become more common. When agreeing to send data to service providers, users should be informed. Laws and regulations must be rewritten in a networked society to accommodate IoT data and its power. Users should know who gathers their data and how it is utilized. The industry is more likely to push for IoT standards than the government. Restrictions on public procurement may have an impact on the creation and acceptance of norms. The IoT dynamic nature generates questions and concerns. We also understand the need for more outstanding research and development to achieve large-scale IoT adoption.

ACKNOWLEDGMENTS

I am thankful for all those with someone whom I do have the pleasure of collaborating on this and other projects during my career. Several family members and friends have provided me with considerable personal and professional mentoring, and I have learned a great lot about scientific research as well as life in general because of their efforts. I would like to express my gratitude to how for his assistance in completing this thesis; he has educated me far more than I've ever express my gratitude to him for here. He has demonstrated to me, via his research and thoughts, what a smart person should be.

REFERENCES

[1] G. Knieps and J. M. Bauer, “Internet of things and the economics of 5G-based local industrial networks,” Telecomm. Policy, p. 102261, Oct. 2021, doi: 10.1016/J.TELPOL.2021.102261.

[2] W. Youn, H. Ko, H. Choi, I. Choi, J.-H. Baek, and H. Myung, “Collision-free Autonomous Navigation of A Small UAV Using Low-cost Sensors in GPS-denied Environments,” Int. J. Control. Autom. Syst. 2020 192, vol. 19, no. 2, pp. 953–968, Aug. 2020, doi: 10.1007/S12555-019-0797-7.

[3] Abdulhakeem Amer A., 2018. “Improve The Performance of The CNPV Protocol in VANET Networks”. International Journal of Civil Engineering and Technology (IJCIET), 11: 304 – 314

[4] Y. Chen, W. Wang, W. Hu, and X. Xu, “M2M: Learning to Enhance Low-Light Image from Model to Mobile FPGA,” pp. 276–287, Sep. 2021, doi: 10.1007/978-3-030-89029-2_22.

[5] P. Shah, A. K. Jain, T. Mishra, and G. Mathur, “IoT-Based Big Data Storage Systems in Cloud Computing,” pp. 323–333, 2021, doi: 10.1007/978-981-15-6707-0_30.

[6] H. Heidari, O. Onireti, R. Das, and M. Imran, “Energy Harvesting and Power Management for IoT Devices in the 5G Era,” IEEE Commun. Mag., vol. 59, no. 9, pp. 91–97, Sep. 2021, doi: 10.1109/MCOM.101.2100487.

[7] Abdulhakeem Amer A., Omeed Kamal Khoursheed, Nizar Kamal Khorsheed Design an Wireless Sensing Network by utilizing Bit Swarm enhancements., International Journal of Computer Science and Network Security , IJCSNS Symmetry 2017, 17, 5.

[8] Sami Hasan and Abdulhakeem Amer, “A Vehicle ID identification Architecture: A Parallel-Joining WSN Algorithm”, eijs, pp. 267-270, Jan. 2021

[9] C. S. Lai et al., “A Review of Technical Standards for Smart Cities,” Clean Technol. 2020, Vol. 2, Pages 290-310, vol. 2, no. 3, pp. 290–310, Aug. 2020, doi: 10.3390/CLEANTECHNOL2030019.

[10] A. Nordrum, “The internet of fewer things [News],” IEEE Spectr., vol. 53, no. 10, pp. 12–13, Oct. 2016, doi: 10.1109/MSPEC.2016.7572524.

[11] Sami Hasan and Abdulhakeem Amer, “Smart Routing Protocol Algorithm Using Fuzzy Artificial Neural Network OSPF”, eijs, pp. 155-160, Jan. 2021.

[12] J. Zhang, M. Ma, P. Wang, and X. dong Sun, “Middleware for the Internet of Things: A survey on requirements, enabling technologies, and solutions,” J. Syst. Archit., vol. 117, p. 102098, Aug. 2021, doi: 10.1016/J.SYSARC.2021.102098.

[13] G. Tricomi, C. Scaffidi, G. Merlino, F. Longo, S. Distefano, and A. Puliafito, “From Vertical to Horizontal Buildings Through IoT and Software Defined Approaches,” 2021 IEEE Int. Conf. Smart Comput., pp. 365–370, Aug. 2021, doi: 10.1109/SMARTCOMP52413.2021.00074.

[14] B. N. Silva, M. Khan, and K. Han, “Towards sustainable smart cities: A review of trends, architectures, components, and open challenges in smart cities,” Sustain. Cities Soc., vol. 38, pp. 697–713, Apr. 2018, doi: 10.1016/J.SCS.2018.01.053.

[15] “ From GUI to UUI: Interfaces for Ubiquitous Computing,” pp. 251–298, 2018, doi: 10.1201/9781420093612-10.

[16] M. S. Munir, I. S. Bajwa, and S. M. Cheema, “An intelligent and secure smart watering system using fuzzy logic and blockchain,” Comput. Electr. Eng., vol. 77, pp. 109–119, Jul. 2019, doi: 10.1016/J.COMPELECENG.2019.05.006.

[17] S. Aleksic, “A Survey on Optical Technologies for IoT, Smart Industry, and Smart Infrastructures,” J. Sens. Actuator Networks 2019, Vol. 8, Page 47, vol. 8, no. 3, p. 47, Sep. 2019, doi: 10.3390/JSAN8030047.

[18] S. Selvaraj and S. Sundaravaradhan, “Challenges and opportunities in IoT healthcare systems: a systematic review,” SN Appl. Sci. 2019 21, vol. 2, no. 1, pp. 1–8, Dec. 2019, doi: 10.1007/S42452-019-1925-Y.

[19] M. Sharma, M. K. Singla, P. Nijhawan, S. Ganguli, and S. S. Rajest, “An Application of IoT to Develop Concept of Smart Remote Monitoring System,” EAI/Springer Innov. Commun. Comput., pp. 233–239, 2020, doi: 10.1007/978-3-030-44407-5_15.

[20] J. Ramkumar, C. Karthikeyan, E. Vamsidhar, and K. N. Dattatraya, “Automated Pill Dispenser Application Based on IoT for Patient Medication,” EAI/Springer Innov. Commun. Comput., pp. 231–253, 2020, doi: 10.1007/978-3-030-42934-8_13.

[21] P. Garcia, M. Parra, E. Guillen, and C. Ramos, “Design of an Intrusion Detection System for IoT Environments with Remote Supervision,” Proc. Int. Conf. Internet Comput., pp. 38–42, 2018, [Online]. Available: http://0-search.proquest.com.pugwash.lib.warwick.ac.uk/docview/2139475878?accountid=14888%0Ahttp://webcat.warwick.ac.uk:4550/resserv??genre=proceeding&issn=&title=Proceedings+on+the+International+Conference+on+Internet+Computing+%28ICOMP%29&volume=&issue=.

[22] E. Schlickman, N. Andrikanis, C. E. B. Harrell, and P. Nelson, “Prototyping an affordable and mobile sensor network to better understand hyperlocal air quality patterns for planning and design,” J. Digit. Landsc. Archit., vol. 2021, no. 6, pp. 94–100, 2021, doi: 10.14627/537705006.

[23] Y. Wang, Q. Wang, D. Suo, and T. Wang, “Intelligent traffic monitoring and traffic diagnosis analysis based on neural network algorithm,” Neural Comput. Appl. 2020 3314, vol. 33, no. 14, pp. 8107–8117, Apr. 2020, doi: 10.1007/S00521-020-04899-3.

[24] V. M. Kuthadi, R. Selvaraj, S. Baskar, P. M. Shakeel, and A. Ranjan, “Optimized Energy Management Model on Data Distributing Framework of Wireless Sensor Network in IoT System,” Wirel. Pers. Commun. 2021, pp. 1–27, Jun. 2021, doi: 10.1007/S11277-021-08583-0.

[25] A. Kelati and H. Gaber, “IoT for Home Energy Management (HEM) Using FPGA,” pp. 54–57, Sep. 2021, doi: 10.1109/SEGE52446.2021.9534986.

[26] M. L. Jovanović, M. Koprivica, and N. Nešković, “Implementation of IoT System for Securing Telecommunications Infrastructure Based on LoRaWAN Operator’s Network,” EUROCON 2019 - 18th Int. Conf. Smart Technol., Jul. 2019, doi: 10.1109/EUROCON.2019.8861632.

[27] M. Muniswamaiah, T. Agerwala, and C. C. Tappert, “Green computing for Internet of Things,” Proc. - 2020 7th IEEE Int. Conf. Cyber Secur. Cloud Comput. 2020 6th IEEE Int. Conf. Edge Comput. Scalable Cloud, CSCloud-EdgeCom 2020, pp. 182–185, Aug. 2020, doi: 10.1109/CSCLOUD-EDGECOM49738.2020.00039.

[28] P. Liu, J. Wang, A. K. Sangaiah, Y. Xie, and X. Yin, “Analysis and Prediction of Water Quality Using LSTM Deep Neural Networks in IoT Environment,” Sustain. 2019, Vol. 11, Page 2058, vol. 11, no. 7, p. 2058, Apr. 2019, doi: 10.3390/SU11072058.

[29] N. Mangla, G. Sivananda, A. Kashyap, and Vinutha, “A GPS-GSM predicated vehicle tracking system, monitored in a mobile app based on Google Maps,” 2017 Int. Conf. Energy, Commun. Data Anal. Soft Comput. ICECDS 2017, pp. 2916–2919, Jun. 2018, doi: 10.1109/ICECDS.2017.8389989.

[30] J. Fang and A. Ma, “IoT Application Modules Placement and Dynamic Task Processing in Edge-Cloud Computing,” IEEE Internet Things J., vol. 8, no. 16, pp. 12771–12781, Aug. 2021, doi: 10.1109/JIOT.2020.3007751.

[31] S. R. Nimbargi, S. Hadawale, and G. Ghodke, “Tsunami alert & detection system using IoT: A survey,” 2017 Int. Conf. Big Data, IoT Data Sci. BID 2017, vol. 2018-January, pp. 182–184, Apr. 2018, doi: 10.1109/BID.2017.8336595.

[32] M. Esteban et al., “Tsunami awareness: a comparative assessment between Japan and the USA,” Nat. Hazards 2018 933, vol. 93, no. 3, pp. 1507–1528, Jun. 2018, doi: 10.1007/S11069-018-3365-1.

[33] G. Lally and D. Sgandurra, “Towards a Framework for Testing the Security of IoT Devices Consistently,” Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 11263 LNCS, pp. 88–102, Sep. 2018, doi: 10.1007/978-3-030-04372-8_8.

[34] Y. Yılmaz and S. Uludag, “Timely detection and mitigation of IoT-based cyberattacks in the smart grid,” J. Franklin Inst., vol. 358, no. 1, pp. 172–192, Jan. 2021, doi: 10.1016/J.JFRANKLIN.2019.02.011.

[35] K. Janjua, M. A. Shah, A. Almogren, H. A. Khattak, C. Maple, and I. U. Din, “Proactive Forensics in IoT: Privacy-Aware Log-Preservation Architecture in Fog-Enabled-Cloud Using Holochain and Containerization Technologies,” Electron. 2020, Vol. 9, Page 1172, vol. 9, no. 7, p. 1172, Jul. 2020, doi: 10.3390/ELECTRONICS9071172.

[36] V. R. Konduru and M. R. Bharamagoudra, “Challenges and solutions of interoperability on IoT: How far have we come in resolving the IoT interoperability issues,” Proc. 2017 Int. Conf. Smart Technol. Smart Nation, SmartTechCon 2017, pp. 572–576, May 2018, doi: 10.1109/SMARTTECHCON.2017.8358436.

[37] A. Vamseekrishna, B. T. P. Madhav, T. Anilkumar, and L. S. S. Reddy, “An IoT Controlled Octahedron Frequency Reconfigurable Multiband Antenna for Microwave Sensing Applications,” IEEE Sensors Lett., vol. 3, no. 10, Oct. 2019, doi: 10.1109/LSENS.2019.2943772.

[38] J. Men et al., “Finding Sands in the Eyes: Vulnerabilities Discovery in IoT with EUFuzzer on Human Machine Interface,” IEEE Access, vol. 7, pp. 103751–103759, 2019, doi: 10.1109/ACCESS.2019.2931061.

[39] P. Gonzalez-Gil, J. A. Martinez, and A. F. Skarmeta, “Lightweight Data-Security Ontology for IoT,” Sensors 2020, Vol. 20, Page 801, vol. 20, no. 3, p. 801, Feb. 2020, doi: 10.3390/S20030801.