ISBN: 978-628-96613-1-6. ISSN: 2414-6390. Digital Object Identifier: https://dx.doi.org/10.18687/LACCEI2025.1.1.1764

Positve and Negative Impacts of IoTs in the Daily Lives of Individuals

Rodolfo Andrés Rivas Matta
College of Eletrical Engineering and Computer Science
Florida Atlantic University
Boca Raton, United States
rrivasmatta2021@fau.edu

Meir Barber
College of Business
Florida Atlantic University
Boca Raton, United States
mbarber2019@fau.edu

Laith Abu Samir
College of Electrical Engineering and Computer Science
Florida Atlantic University
Boca Raton, United States
labusamir2020@fau.edu

Sheevenson Desravines
College of Business
Florida Atlantic University
Boca Raton, United States
sdesravines2012@fau.edu

***Abstract*— The Internet of Things (IoT) is a new field that has already affected many aspects of people's lives. It is already happening in households, healthcare providers, smart cities, the energy sector, agriculture, and more. Nonetheless, people do not always accept it with open arms. There are debates on whether it has positively or negatively impacted people's lives. This article avoids taking a side and tries to explore different areas and ways in which IoTs have affected lives.**

More specifically, it will explore reliability, security, privacy, interoperability, scalability, power consumption, cost-effectiveness, and user experience in the shade of different lights. All these aspects have both positive and negative effects, and this article tries to explore them objectively. It is not a complete analysis of all the possible consequences IoTs can have on people, but it serves as a survey on the matter. It is an informative article that leaves opinions to the reader and leaves the path open for others to explore.

Keywords—internet of things, impact of IoTs

I. Introduction

As technology progresses, further integration with the internet occurs in the devices and systems we use daily. The Internet of Things (IoT) has become the status quo for modern devices, allowing users to access information easily [1]. IoT has changed how individuals work, collect information, and operate systems [1]. However, since the Internet of Things is relatively recent in terms of developments, some aspects of IoT must be studied and researched further as they could also provide potential dangers and vulnerabilities [2]. Every day, more devices/things and processes are becoming increasingly integrated into IoT, which presents potential positives and negatives [2]. IoT has demonstrated reliability, cost-effectiveness, scalability, interoperability, etc. [2]. IoT will also play a significant role in collecting data for industry purposes such as server management, Artificial Intelligence (AI), and other prevalent uses [2]. The more technology advances, the further IoT comes in as a part of technologies in social media, home use, healthcare, and even government use, like intelligent cities [1]. In this paper, we'll be reporting on IoT's positive and negative impacts from a general perspective for the working individual. This is not being done to favor whether IoT has been more positive or negative. This paper is only to assess the objective positive and negative impacts of IoTs on these aspects to inform and provide further insight and research into this developing sector of information collection and sensor network technologies. The sections will inform the reader on positive impacts regarding these general aspects of IoT, and then the same will be done with negative impacts in the proceeding section.

II. The Impact of IoTs

A. Positive Impact

1) Reliability

The reliability of IoT systems significantly enhances various aspects of daily life and industry, yielding numerous positive impacts. Reliable IoT systems ensure high uptime and availability, which is crucial for continuous operations in sectors like healthcare, industrial automation, and smart city infrastructure, thereby minimizing downtime and ensuring consistent service availability. These systems collect and transmit accurate data, essential for real-time decision-making in healthcare, where timely information can improve patient outcomes, and in industrial settings, where it can optimize operations and prevent failures [3][4]. Ensuring reliable IoT device operation streamlines business processes, reduces manual interventions, and boosts productivity [5]. For instance, reliable IoT systems in supply chain management enable real-time tracking of assets and inventory, reducing errors and enhancing efficiency. Additionally, reliable IoT systems enhance safety and security by ensuring that smart locks, security cameras, and environmental sensors function correctly, preventing unauthorized access, detecting anomalies, and responding promptly to emergencies [6]. This reliability also translates to significant cost savings by reducing maintenance costs and preventing costly downtimes. Predictive maintenance with reliable IoT sensors can identify potential equipment failures early, allowing for timely repairs and avoiding expensive breakdowns [6]. In summary, the reliability of IoT systems positively impacts service availability, decision-making, efficiency, safety, cost savings, and scalability, making them indispensable in modern applications across various sectors.

2) Security

The aspect of security is a pressing topic regarding the Internet of Things. Although there have been recent concerns

regarding security on IoTs as a whole, there have been many positive impacts on security for IoTs. IoTs have provided enhanced data monitoring and event surveillance [7]. Many processes and businesses have been positively enhanced using monitoring with cameras and sensors for lights. For instance, farming has seen this impact a lot. With IoT and sensors, farmers can now see information regarding soil quality, irrigation control, pest control, and growth monitoring [7]. With cameras and sensors, the ability to see pests, predators, and other factors contributing to the harmed security of crops has grown significantly, and there are no signs of stopping anytime soon. This is becoming the industry standard now [7].

Agriculture is not the only sector positively affected by security monitoring and remote data monitoring, but many facilities that utilize remote technologies solely rely on IoTs for security purposes [8]. IoTs have allowed end-users to remotely access security devices to allow for adjustments or to address security tasks remotely, as well as do things like lock/unlock doors and arm/disable security systems [8]. A higher level of control over security tools has improved incident response times and a higher level of convenience regarding monitoring potential harmful activity [8]. Although there have been concerns about the actual security protocols of IoT devices, the technology has allowed users to monitor data, systems, networks and remotely access tools needed to carry out routine security checks and tasks. These several milestones in security for IoTs will most likely only advance further as these technologies develop more.

3) Privacy

Privacy is a complex aspect of IoT. IoTs collect much data and information depending on their purpose and use. Concerns about how this data is collected, stored, and used have been brought up by the public and continue to be a bit of a divisive topic [9]. Some systems and services utilize IoTs exclusively to collect and process data, so these concerns are valid. However, IoTs still have some positive impacts in the realm of privacy.

Many IoT systems have been designed to give end-users control over their personal data [9]. Many services today ask users what information they want to be collected, if any, and many will even allow users to delete their data outright [9]. These tools allow for transparency in what data is collected, stored, and processed and give users significant control over their privacy regarding what is collected from them. This is especially relevant today when more companies are making databases and customer profiles using data from data brokers [9].

Measures for not letting information be sent from IoT systems have also been set for many devices, such as home appliances like fridges [2]. Many IoT devices will only utilize on-device processing for sensitive data, meaning that the information collected by the IoT device will only be processed on the device itself and not sent anywhere else, like an external server or database [10]. Although there are many valid concerns with privacy in IoT, many benefits have been drawn and are still being developed to this day.

4) Interoperability

In the context of IoTs, interoperability is the ability of devices to communicate and work together even though they come from different brands or ecosystems. In IoTs, that means different devices must share information and use others' data in their operations.

Different IoTs with different functions can work together for a bigger purpose. For example, different devices can do different things like hearing, seeing, and processing information. That has many applications; for example, smart cities could use these IoTs to coordinate critical decisions that saves lives [11]. That has an impact in the daily lives of humans. However, it does not have to go that far. There are simpler applications that already exists in people's homes that assist their daily lives.

One benefit is the optimization of different applications. For instance, IoTs could help minimize energy utilization in households. Interoperability could allow thermostats and smart blinds to work together and adjust a room's temperature based on sunlight levels. Of course, it is possible that one single brand makes both the thermostat and smart blinds. However, modern households rarely buy all their IoTs from the same brand. Interoperability allows them to purchase products that belong to different ecosystems and use them together; for example, people can control all their IoTs from a single app like Alexa.

Another way in which interoperability improves people's lives is by giving them personalized and better experiences. Smartwatches, for example, keep collecting data about the person who wears them. Healthcare providers could use that data, like heartbeats or sleep cycles, to come up with better diagnoses. In turn, that would also require interoperability between smartwatches and healthcare systems.

Sustainability is also improved thanks to interoperability. As a previous example of smart homes mentioned, households could purchase their IoTs from different brands, so realizing that it would cause less waste is important. If households had to purchase all their ecosystems again when getting a new device, the old ones would be discarded. That kind of flexibility, as a result of their interoperability, aids sustainability.

5) Scalability

Scalability in IoTs occurs when new devices can be added to a system without compromising its performance. This is known as horizontal scalability, which is the opposite of vertical scalability, which involves replacing computers with more powerful ones [12].

Following from the previous examples, having a few devices at home would allow the system to work as well as if there were many devices working together. This attribute has many positive impacts on individuals' daily lives.

Scalability can positively impact individuals' lives by giving them convenience and flexibility. People can start using IoTs with a small investment and purchase a few IoT devices like smart lights or speakers. As previously mentioned, if they wanted to get new devices, they would not have to replace the ones they already have. Scalability and interoperability allow households to keep adding devices to their homes without affecting their performance.

Similarly, scalability allows progressive enhancements in services. For example, as healthcare providers were previously mentioned, businesses can also slowly integrate new IoTs and

IoT support into their environments. That will, in turn, allow them to continuously improve personalization and customer experiences. Again, that is only possible if scalability and interoperability are at play.

6) Power Consumption

The adoption of IoT applications is projected to result in significant energy savings, with estimates suggesting a reduction of over 1.8 petawatt-hours (PWh) of electricity by 2030 and total energy savings of approximately 5.2 PWh [13]. IoT-enabled smart grids and energy management systems improve energy efficiency by optimizing electricity usage, leading to reduced overall consumption. Additionally, IoT devices are expected to conserve nearly 230 billion cubic meters of water by 2030 through enhanced water grid operations and smart irrigation techniques [14]. Predictive maintenance enabled by IoT sensors can identify potential equipment failures before they occur, thereby preventing energy waste. In both home and industrial settings, IoT-enabled automation optimizes lighting, heating, cooling, and machinery operations, significantly minimizing energy waste [14]. The integration of renewable energy sources into power grids is facilitated by IoT, promoting cleaner energy use. Furthermore, by optimizing energy usage, IoT systems help reduce energy costs for both businesses and consumers. Efficient power management strategies, such as employing low-power components and implementing sleep modes, extend the battery life of IoT devices, contributing to overall energy efficiency.

7) Cost

IoTs can lead to significant cost savings in many aspects of daily life, particularly using smart home devices. For example, smart thermostats, lighting systems, and energy monitors are designed to improve energy consumption, reducing utility bills [15]. For example, smart thermostats learn users' preferences and then adjust cooling or heating depending on location to ensure efficient energy use. The American Council for an Energy-Efficient Economy (ACEEE) reports that smart thermostats can save users up to 10-15% on heating and cooling costs [16].

Similarly, smart lighting systems can be programmed to turn off when unoccupied rooms are not in use, further contributing to cost savings. These systems often include motion sensors and timers that ensure lights are only used when needed, which can significantly reduce electricity consumption over time.

Additionally, energy monitors offer detailed insights into household energy use by identifying areas where energy can be conserved. Monitoring and controlling home energy use remotely through IoT applications allows households to manage their energy consumption more effectively. For example, users can adjust settings or turn off appliances from their smartphones, even when they are not at home, preventing unnecessary energy use and reducing costs.

These smart devices contribute to individual cost savings and promote more sustainable energy practices on a broader scale. By adopting IoT technologies, households can reduce their environmental footprint while enjoying the financial benefits of lower utility bills. This dual advantage makes IoT an attractive solution for modern energy management.

8) User Experience

Integrating IoT devices can significantly enhance user experience by providing convenience and improving the quality of life [15]. Smart home assistants like Amazon Alexa and Google Home enable voice control over various devices, simplifying daily tasks such as setting reminders, playing music, or controlling smart appliances. This ease of use is highlighted by research from NPR and Edison Research, which found that 69% of smart speaker owners use their devices daily, underscoring their role in everyday convenience [17].

Wearable devices, such as fitness trackers and smartwatches, also play a crucial role in enhancing user experience. These devices offer real-time health monitoring and personalized feedback, promoting healthier lifestyles. According to a report by Deloitte, over 60% of individuals use wearables to monitor health metrics, which can lead to improved health outcomes [18]. Wearables track various health indicators such as heart rate, sleep patterns, and physical activity, enabling users to make informed decisions about their health and well-being.

IoT applications extend beyond personal health to healthcare systems, where they have transformative potential. Remote patient monitoring, for example, allows for better management of chronic conditions and prompt medical interventions. A study published in the Journal of Medical Internet Research found that remote monitoring systems can reduce hospital readmissions for chronic diseases by 25% [19]. These systems allow healthcare providers to check patient's health data in real-time, enabling early detection of potential issues and prompt medical responses, thereby improving patient outcomes and reducing healthcare costs.

Furthermore, IoT devices can enhance home security and safety. Smart security systems, including cameras, sensors, and alarms, can be monitored and controlled remotely, providing peace of mind to homeowners. These systems can alert users to potential security breaches or hazards, such as fires or gas leaks, enabling quick responses to protect property and loved ones.

Overall, integrating IoT devices improves user experience by offering increased convenience, improved health management, and enhanced security. These technologies simplify daily tasks, offer valuable health insights, and ensure safety, all of which contribute to a higher quality of life for users. As IoT evolves, its impact on user experience will likely grow, offering even more innovative solutions to improve everyday living.

B. Negative Impact

1) Reliability

The Internet of Things (IoT) promises significant advancements across various sectors, but its deployment and maintenance face several challenges that impact performance and reliability. IoT devices are prone to technical issues, software bugs, and connectivity problems, which can disrupt their functionality. Maintenance challenges arise from managing updates and regular maintenance across numerous devices, potentially leading to reliability issues if not properly managed [20]. The proliferation of IoT devices adds complexity to networks, making them harder to manage and maintain. Security vulnerabilities in IoT devices make them prime targets

for cyberattacks, compromising system reliability and data integrity. Environmental factors such as temperature, humidity, and physical wear can degrade device performance over time [21]. IoT systems' heavy reliance on network connectivity means that unreliable or inconsistent connections can significantly affect their reliability. The distributed nature of IoT systems often limits visibility into data flows, leading to potential reliability issues in data transmission and processing. Additionally, the limited service lifetimes of IoT devices require careful planning for failures and replacements to maintain solution reliability. Addressing these challenges necessitates robust testing, maintenance, security, and monitoring strategies to enhance the reliability and effectiveness of IoT solutions [22].

2) Security

While IoTs have provided advantages for security, like surveillance and monitoring, the actual security methods and protocols on IoT devices are usually insufficient to protect against significant threats [23]. Since many IoT devices use little power to operate and function, there is a problem with proper methods for encryption and computation over networks using IoT devices [23]. There are methods in place now that are being researched, such as using machine learning to encrypt information on IoT devices, but they are still being explored [23].

Furthermore, with the low number of security protocols in place on IoT devices, there is the possibility of network attacks by bad actors [24]. Devices integrated with IoT can be hijacked and used to form botnets, being used and controlled without the end-user's knowledge and compromised by Dedicated Denial of Service attacks (DDoS) that may overwhelm and turn off networks altogether [24]. This stems from a lack of standardization for security protocols on IoTs, and methods on how to prevent and mitigate these weaknesses, which are currently being further researched and developed.

In addition to the network side of things, the physical components of IoTs could be compromised due to a lack of security measures [8]. For instance, homes or buildings with smart locks and doors can be compromised without sufficient security measures, enabling a risk of either being locked in or locked out of the area. Since so many IoT devices can be widely different from each other, it may be daunting to monitor their security and update their security protocols as it can be resource-heavy and time-consuming, all of which costs money [7].

3) Privacy

The negative impacts of this aspect may be one of the most controversial regarding what kind of data has been collected, how it has been collected, and the channels for consent for which it is allowed to be collected. Ever since IoTs have been more integrated into devices for daily use like home utilities, cell phone devices, and other smart home services like doorbells, consumer interest has heavily shifted toward the want for proper protection of privacy regarding information collection on the consumer and end-user [25]. Many services today fail to explain in detail what kind of data is collected from consumers, which makes for cloudy consent mechanisms when asking customers for their data [25]. Not only that, but most of this data ends up being sold in one way or another to third parties by these companies that collect it, like data brokers, for example [26].

Additionally, some IoT devices collect data in ways consumers believe to be intrusive [25]. This can include intelligent assistants logging conversations, smart cameras monitoring private spaces, etc. [26]. The vagueness of consent on the end-user's part doesn't necessarily help with this either, as legally, they may have consented to data being collected in this manner, but how it was expressed to the consumer may have been too vague to let them know [26]. With this data, several profiles can be made on individuals for marketing purposes to target specific kinds of advertisements, products, and services that the profile may indicate the consumer will find interesting. Some consumers also see this as invasive and beyond what is needed for IoT data collection and privacy [26].

4) Interoperability

As mentioned in the positive impacts section, interoperability refers to the ability of devices from different ecosystems to communicate and work together. Undoubtedly, interoperability has many positive qualities. However, there are challenges that still affect IoT devices that interoperate with others.

Interoperability, as already established, allows different ecosystems to work together. However, the data-sharing process must be simple and available for other devices to use. It is crucial that information resources stay available for other devices; however, that opens the opportunity for bad actors to access that information, too. Security easily becomes a point of interest for IoT environments where privacy is also important "when networking between different entities" [27]. In other words, there is somewhat of a trade-off between interoperability and security.

Reliability is another area where interoperability may negatively affect individuals' daily lives. As more IoTs participate in bigger systems, individuals become more dependent on those systems. However, interoperability is difficult to maintain. For example, as companies try to mitigate security risks, they may launch updates that change the way their devices interact with others. That could easily cause issues in the interoperability of ecosystems and result in system failures. Finally, people's dependency on these systems will result in disruptions when those failures happen.

5) Scalability

Interoperability and scalability have already proven to be intertwined, thus they face very similar challenges. As IoTs are scalable, the cost to maintain them is also higher. As more IoTs join systems, they become more complicated. Updates may not be compatible with other IoTs in the network, and disruptions can happen.

One such example where individuals may grow dependent on IoTs is in the electrical power sector. There are already power grids that use IoTs to balance loads and even use the energy from solar panels in households to supply the demand [28]. If there was a failure in part of these IoTs, which also have been scaling progressively, there may be a power disruption until the issue is fixed. However, some communities rely heavily on electrical power.

In fact, a cyber-attack happened in 2021 in a Georgia-based gas pipeline. Although it was a case where actors caused the

problem rather than just failures in the system, it still proves the dependency and effect that malfunction in systems may have on the lives of individuals. The attack caused an interruption in the gas supply, and prices rose considerably in the following months [29].

In other words, scalability can have many positive impacts on the lives of individuals, but it can also affect negatively when issues happen at systems that have already scaled out.

6) Power Consumption

The proliferation of IoT devices brings about increased energy demand, as their collective power consumption strains power grids and raises carbon footprints. Many IoT devices depend on batteries, necessitating frequent replacements or recharging, particularly in remote applications where power sources are scarce. This reliance on batteries also raises environmental concerns due to the production and disposal processes involved [20]. Efforts to minimize power consumption can sometimes lead to performance trade-offs, compromising the functionality of these devices. Additionally, temperature sensitivity affects power consumption, with extreme conditions potentially reducing efficiency or shortening battery life. Network energy costs are significant, as transmitting data over satellite or cellular networks for remote IoT applications is energy-intensive. As IoT deployments expand, managing the power consumption of numerous devices becomes increasingly complex and costly. In remote locations, the dependency on reliable power sources poses a challenge, limiting the effectiveness of IoT solutions. Furthermore, inefficient IoT implementations or poorly optimized devices can lead to unnecessary energy consumption, counteracting the potential benefits of IoT technology.

7) Cost

While IoTs could offer cost-saving benefits, the initial investment and ongoing maintenance costs can be substantial [15]. General higher-end IoT devices often come with a hefty price tag, and the need for continuous updates and potential repairs can add to the overall expense. For instance, a smart thermostat can cost between $200 and $300, and smart security systems can range from $300 to $500, excluding installation fees [30]. These upfront costs can be a significant financial burden for many households.

In addition to the initial purchase price, adopting IoT technology often requires upgrading existing infrastructure. Improved internet connectivity is often necessary to support the increased data traffic generated by multiple smart devices. This might involve subscribing to higher-speed internet plans or investing in more robust Wi-Fi routers and extenders, which can add to the costs. For homes with older electrical systems or insufficient wireless coverage, added expenses may include professional installation and configuration services to ensure the devices function correctly.

Moreover, maintaining IoT devices involves regular software updates to protect against security vulnerabilities and to ensure the best performance. These updates sometimes require new hardware if the existing devices become outdated or incompatible with new software. Repairs and replacements due to wear and tear or technological obsolescence also contribute to the ongoing costs associated with IoT devices.

The financial implications of these costs are significant. A survey by Gartner found that 63% of households considered the prohibitive cost of IoT devices a significant barrier to adoption [31]. This belief is likely due to the combined effect of initial expenditures, potential infrastructure upgrades, and continuous maintenance expenses, which can make implementing IoT technology prohibitive for many consumers.

Furthermore, the cost considerations are not limited to residential settings. Businesses looking to implement IoT solutions to streamline operations and improve efficiency face similar financial challenges. The need for comprehensive network upgrades, cybersecurity measures, and specialized personnel to manage and maintain IoT systems can lead to substantial capital and operational expenditures.

In summary, while IoT devices can offer substantial long-term cost-saving benefits and enhanced convenience, the initial and ongoing costs associated with their purchase, installation, and maintenance can be substantial. These financial barriers can deter many individuals and businesses from fully embracing IoT technology, highlighting the need for more affordable solutions and cost-effective implementation strategies to make IoT accessible to a broader audience.

8) User Experience

The user experience with IoT devices can sometimes be problematic due to various issues, including compatibility between IoT devices and platforms, security vulnerabilities, and privacy concerns [15]. These challenges can lead to users' frustration and limit IoT technology's overall effectiveness and satisfaction.

One major issue is compatibility because IoT devices require smooth integration to function properly, but this is not always the case. A smart home setup may need devices from the same manufacturer or those that support the same protocols to work together seamlessly, which limits user choice and flexibility. According to a study by Parks Associates, 44% of smart home device owners reported experiencing interoperability issues [32]. Nearly half of the users faced problems connecting and managing devices from different brands or platforms, resulting in a fragmented and often frustrating user experience.

Security and privacy concerns also significantly impact user experience with IoT devices. These devices are often vulnerable to hacking and data breaches, posing risks to personal information and overall security. The constant connectivity and data exchange inherent in IoT technology can lead to concerns about surveillance and loss of privacy. A report by Symantec highlighted that 60% of IoT devices are susceptible to medium- or high-severity vulnerabilities [33]. This important level of susceptibility makes users wary of adopting IoT devices, knowing that their data and security could be compromised.

Moreover, the General Data Protection Regulation (GDPR) emphasizes the importance of data protection, but many IoT devices do not fully comply with these regulations. This non-compliance further exacerbates privacy concerns among users. The European Commission has noted that ensuring GDPR compliance is crucial for protecting consumer data and

supporting trust in IoT technology [34]. However, the lack of widespread adherence to these regulations by IoT manufacturers means that users often must contend with potential privacy and data security breaches.

In addition to these issues, the user experience can be hindered by the complexity of setting up and managing IoT devices. Many users find these devices' initial installation and configuration challenging, particularly involving multiple devices and platforms. This complexity can discourage users from fully using the capabilities of their IoT systems or lead to frequent technical problems that require troubleshooting and support.

To address these challenges, manufacturers and developers must focus on creating more interoperable, secure, and user-friendly IoT solutions. This includes standardizing communication protocols, enhancing security measures, and ensuring compliance with data protection regulations. By improving these aspects, the user experience with IoT devices can be significantly enhanced, leading to greater consumer adoption and satisfaction.

III. Conclusions

The impact of IoTs on daily life is multifaceted, offering benefits and challenges. Future trends in IoT technology suggest further integration into various aspects of daily living, potentially leading to even greater convenience and efficiency. Emerging technologies such as edge computing and advancements in artificial intelligence (AI) may help address some of these challenges by providing more secure and cost-effective solutions. However, addressing the associated costs and improving security measures will be crucial in mitigating negative impacts and ensuring that IoT advancements contribute positively to society [15].

References

[1] F. Amin *et al*, "Recent Advances in Internet of Things and Emerging Social Internet of Things: Vision, Challenges and Trends," *Electronics*, vol. 11, (13), pp. 2033, 2022. Available: https://go.openathens.net/redirector/fau.edu?url=https://www.proquest.com/scholarly-journals/recent-advances-internet-things-emerging-social/docview/2685978417/se-2. DOI: https://doi.org/10.3390/electronics11132033.

[2] C. Silvestru *et al*, "A STEP FORWARD: FROM INTERNET OF THINGS TO INTERNET OF EVERYTHING," *Proceedings in Manufacturing Systems*, vol. 16, (4), pp. 157-161, 2021. Available: https://go.openathens.net/redirector/fau.edu?url=https://www.proquest.com/scholarly-journals/step-forward-internet-things-everything/docview/2697726350/se-2.

[3] Asergaz, "Reliability in your IOT workload - microsoft azure well-architected framework," Microsoft Azure Well-Architected Framework | Microsoft Learn, https://learn.microsoft.com/en-us/azure/well-architected/iot/iot-reliability

[4] S. J. Moore, C. D. Nugent, S. Zhang, and I. Cleland, "IOT Reliability: A review leading to 5 key research directions," *CCF Transactions on Pervasive Computing and Interaction*, vol. 2, no. 3, pp. 147–163, Aug. 2020. doi:10.1007/s42486-020-00037-z.

[5] N. Joshi, "3 ways in which IOT reliability can be improved," LinkedIn, https://www.linkedin.com/pulse/3-ways-which-iot-reliability-can-improved-naveen-joshi/

[6] "Positive and negative impacts of internet of things on Society," What are the Positive and Negative Impacts of Internet of Things on Society, https://www.zrix.com/blog/impacts-of-internet-of-things-on-society

[7] R. Chaganti *et al*, "Blockchain-Based Cloud-Enabled Security Monitoring Using Internet of Things in Smart Agriculture," *Future Internet*, vol. 14, (9), pp. 250, 2022. Available: https://go.openathens.net/redirector/fau.edu?url=https://www.proquest.com/scholarly-journals/blockchain-based-cloud-enabled-security/docview/2716527447/se-2. DOI: https://doi.org/10.3390/fi14090250.

[8] O. Yousuf and R. N. Mir, "A survey on the Internet of Things security: State-of-art, architecture, issues and countermeasures," *Information and Computer Security*, vol. 27, (2), pp. 292-323, 2019. Available: https://go.openathens.net/redirector/fau.edu?url=https://www.proquest.com/scholarly-journals/survey-on-internet-things-security/docview/2230562607/se-2. DOI: https://doi.org/10.1108/ICS-07-2018-0084.

[9] B. P. Luis Alberto, P. A. Eduardo Adilio and M. B. Priscila América Solís, "Device-Based Security to Improve User Privacy in the Internet of Things †," *Sensors*, vol. 18, (8), pp. 2664, 2018. Available: https://go.openathens.net/redirector/fau.edu?url=https://www.proquest.com/scholarly-journals/device-based-security-improve-user-privacy/docview/2108865424/se-2. DOI: https://doi.org/10.3390/s18082664.

[10] M. Eltayeb, "Internet of Things: Privacy and Security Implications," *International Journal of Hyperconnectivity and the Internet of Things*, vol. 1, (1), pp. 1-18, 2017. Available: https://go.openathens.net/redirector/fau.edu?url=https://www.proquest.com/scholarly-journals/internet-things-privacy-security-implications/docview/2904645209/se-2. DOI: https://doi.org/10.4018/IJHIoT.2017010101.

[11] T. Salman and R. Jain. "Networking Protocols and Standards for Internet of Things" in *Internet of Things and Data Analytics Handbook*, 1st ed. Palo Alto, California, United States: Wiley, 2016, ch. 13.

[12] S. Dzalev and M. Gusev, "Evaluation of Scalability and Multi-tenancy: A Use-Case," *2021 29th Telecommunications Forum (TELFOR)*, Belgrade, Serbia, 2021, pp. 1-4, doi: 10.1109/TELFOR52709.2021.9653373.

[13] "IOT technology to deliver positive energy impact," Welcome to our blogs, https://blog.nordicsemi.com/getconnected/iot-technology-to-deliver-positive-energy-impact

[14] J. Pohl, "Power consumption monitoring systems using IOT help to identify energy saving opportunities," Leading adaptive buildings company, https://www.buildingsiot.com/blog/power-consumption-monitoring-systems-using-iot-help-to-identify-energy-saving-opportunities-bd

[15] A. Stevenson, "The Double-Edged Sword of IoT: Benefits and Drawbacks," Tech Innovations Journal, vol. 34, no. 2, pp. 45-58, 2018. [Online]. \Available: https://www.iotinsider.com/iot-insights/the-emergence-of-iot-a-double-edged-sword/

[16] S. Nadel, "Smart Thermostat Initiatives Reveal," The American Council for an Energy-Efficient Economy (ACEEE), 2017. [Online]. Available: https://www.aceee.org/blog/2015/10/smart-thermostat-initiatives-reveal#:~:text=In%20that%20report%2C%20ACEEE%20reviewed,plan%20to%20revise%20this%20estimate

[17] NPR, "The Smart Audio Report," 2018. [Online]. Available: https://www.npr.org/about-npr/630085002/smart-audio-report-2018-release

[18] M. Casey, C. Wigginton, and C. Calugar-Pop, "Global Mobile Consumer Survey 2019," Deloitte, 2019. [Online]. Available: https://www2.deloitte.com/us/en/insights/industry/telecommunications/global-mobile-consumer-survey-2019.html

[19] Journal of Medical Internet Research (JMIR), "Impact of Remote Patient Monitoring on Chronic Disease Management," 2018. [Online]. Available: https://www.jmir.org/2018/4/e123

[20] "Positive and negative impacts of internet of things on Society," What are the Positive and Negative Impacts of Internet of Things on Society, https://www.zrix.com/blog/impacts-of-internet-of-things-on-society

[21] "How the internet of things could be bad for business," Business News Daily, https://www.businessnewsdaily.com/5996-how-smart-devices-could-compromise-your-business.html

[22] "The negative impacts of internet of things (IOT): Security," Course Sidekick, https://www.coursesidekick.com/information-systems/2439447

[23] T. Althiyabi, I. Ahmad and M. O. Alassafi, "Enhancing IoT Security: A Few-Shot Learning Approach for Intrusion Detection," *Mathematics,* vol. 12, *(7),* pp. 1055, 2024. Available: https://go.openathens.net/redirector/fau.edu?url=https://www.proquest.com/scholarly-journals/enhancing

-iot-security-few-shot-learning-approach/docview/3037523236/se-2. DOI: https://doi.org/10.3390/math12071055.

[24] S. Thota and D. Menaka, "Botnet detection in the internet-of-things networks using convolutional neural network with pelican optimization algorithm," *Automatika,* vol. 65, *(1),* pp. 250-260, 2024/02//. Available: https://go.openathens.net/redirector/fau.edu?url=https://www.proquest.com/scholarly-journals/botnet-detection-internet-things-networks-using/docview/2913118962/se-2. DOI: https://doi.org/10.1080/00051144.2023.2288486.

[25] L. F. Cranor, Y. Agarwal and P. Emami-Naeini, "Privacy: Internet of Things Security and Privacy Labels Should Empower Consumers," *Association for Computing Machinery.Communications of the ACM,* vol. 67, *(3),* pp. 29, 2024/03//. Available: https://go.openathens.net/redirector/fau.edu?url=https://www.proquest.com/scholarly-journals/privacy-internet-things-security-labels-should/docview/3055132158/se-2. DOI: https://doi.org/10.1145/3637630.

[26] S. Moyopo, "Quantifying the Data Currency's Impact on the Profit made by Data Brokers in the Internet of Things Based Data Marketplace." Order No. 30530026, Colorado Technical University, United States -- Colorado, 2023.

[27] E. Lee, Y. -D. Seo, S. -R. Oh and Y. -G. Kim, "A Survey on Standards for Interoperability and Security in the Internet of Things," in *IEEE Communications Surveys & Tutorials*, vol. 23, no. 2, pp. 1020-1047, Secondquarter 2021, doi: 10.1109/COMST.2021.3067354.

[28] D. K. Aagri and A. Bisht, "Export and Import of Renewable energy by Hybrid MicroGrid via IoT," *2018 3rd International Conference On Internet of Things: Smart Innovation and Usages (IoT-SIU)*, Bhimtal, India, 2018, pp. 1-4, doi: 10.1109/IoT-SIU.2018.8519873.

[29] K. Wood, "Cybersecurity Policy Responses to the Colonial Pipeline Ransomware Attack," *Georgetown Law*, Mar. 07, 2023. https://www.law.georgetown.edu/environmental-law-review/blog/cybersecurity-policy-responses-to-the-colonial-pipeline-ransomware-attack/

[30] D. Wroclawski, "Best Smart Home Devices of the Year," Consumer Reports, 2019. [Online]. Available: https://www.consumerreports.org/home-garden/smart-home/best-smart-home-devices-of-the-year-a5691424633/

[31] Gartner, "Smart Home Technology Survey," 2019. [Online]. Available: https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf

[32] Parks Associates, "Smart Home Device Market Data," 2018. [Online]. Available: https://www.parksassociates.com/storage/bento/shop/mktfcs_samples/ParksAssoc-QC-SmartHomeBuyerJourney-TOC.pdf

[33] Symantec, "Internet Security Threat Report," 2018. [Online]. Available: https://docs.broadcom.com/doc/istr-03-jan-en

[34] European Commission, "Data protection in the EU," 2019. [Online]. Available: https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en