The Internet of Things

The Internet of Things has become one of the most important technologies of the 21st century in the past through years. Internet of Things which is also called (IoT) is the network of objects that use software, sensors, and other technical software. They exchange and collect data from other devices and systems over the internet. IoT devices are usually cheap and contain sensors. Common objects that utilize the Internet of Things are watches, cars, microwaves, AI home systems, and even inhalers. Using big data and analytics, it was made possible for physical objects to share and collect data with the least human intervention possible. The concept of adding processing systems to basic technologies like microwaves has been an idea since the 1980s. It just wasn't possible because the technology was not efficient enough and the cost of chips to function this technology was very expensive. Many aspects allow IoT devices to function now. The cost has been a big concern with making IoT technology but more manufacturers are getting reliable seniors at an affordable cost. The strength of networks and the internet has made it easier for sensors to connect therefore making data transfer much easier. Improvement in AI technology has also made it possible for IoT to exist(Alexa and Siri) and they became appealing for home use and more affordable. Improvements in analytics have allowed large data to get stored in the cloud. It helps businesses with getting intel faster. All of these technologies have made IoT possible to use over the past few years. IoT can also be used to help boost businesses. Business operations can increase productivity and efficiency. Also, IoT makes it very easy to connect the physical business world to the digital world. Many industries benefit from the Internet of Things. Manufacturers use sensors to check for the accuracy of their equipment. Sensors can measure when the output of production is compromised. This helps the companies with improving performance management. The automotive industry uses IoT to detect the failure of equipment in vehicles. Because of the use of IoT, car owners can stay informed and the suppliers would learn better ways how to keep their cars running. Thanks to IoT sensor data, Transportation and logistical systems benefit. Ships or trains that carry certain inventory can be rerouted based on the availability of vehicles and drivers, and weather conditions. In retail, IoT applications can help improve the customer experience and reduce the cost of operations. Even in healthcare, doctors and nurses need to be aware of patient-assistance assets like crutches or wheelchairs. IoT technologies are used to track these assets so that medical workers can track them at all times. IoT devices are everywhere around us, even in our own homes. The Google Home Voice Controller is an IoT device that some homes have. Using the features on that device, you're able to sync your home features like alarms, lights, and A/C. From just using your voice, you can use your Google Home to control these functions. Another piece of technology is the August Doorbell Cam. With the doorbell cam, you're able to answer your door anywhere in your house or even outside your house. In health care, some IoT devices like apple watches and Fitbit's have heavily impacted fitness positively. With the apple watch, you're able to call, text, listen to music and you're even able to track your heart rate activity. The Fitbit is a wearable fitness and health track that helps users reach certain fitness goals.

The Internet of Things is still a very new concept. By the end of 2025, there will be an estimation of 64 million IoT devices. With new concepts, there come imperfections. These imperfections create new points of vulnerability. These imperfections are security and privacy issues that come with the Internet of Things. Protecting the privacy of consumers is increasingly becoming strenuous while the use of IoT becomes more prevalent. Privacy depends on the protection and the use of the customer's personal information. A fundamental human right is to preserve privacy for the average person. A high degree of reliability is needed for IoT devices to be used. Therefore, technical architects made a big deal to set up requirements/goals for these devices to run. The data that the device gathers has to be authorized by the user. It has to be resilient to attack and it has to adjust to breaches. The users also should be able to control how much data they should provide. Lastly, only the information provider has the right to look at his data. The average consumer is concerned about their privacy because they're not sure how much of their data they have given. If a lot of this user's life and data is connected through the internet of things, what isn't going to be used? A clamoring privacy issue with IoT is how much data IoT devices collect. A report by the Federal Trade Commission was done where they uncovered that less than 10,000 households create 150 million data points per day. This leaves room for hackers to poke holes for vulnerable and sensitive information. So the question is, is it necessary for IoT devices to store a lot of data? Hackers or manufacturers could also use an IoT device that is connected to a person's home and use it to invade that home. This is possible by intercepting unencrypted data from that device. IoT devices can also cause you to get an unwanted public profile. Some companies are legally allowed to make employment decisions off on a customer's data. Vulnerabilities in web applications can cause major data breaches. Hackers can exploit these vulnerabilities and enter through the system. Some IoT devices can collect data in a way where the user does not know their data is being stored so therefore their privacy is being invaded. Companies also have to invest in getting the best security control procedures for IoT devices so that any breaches in privacy will quickly be dealt with. It's also very possible to profile and track an individual with sensors that are deployed in different environments that are tied to one user. A lot of sensitive information is leaked just from unauthorized manipulation and poor handling of the hardware and software in the devices. In an article by TechCrunch, the author Christine Bannan states "The most dangerous part of IoT is that consumers are surrendering their privacy, bit by bit, without realizing it, because they are unaware of what data is being collected and how it is being used. The majority of consumers aren't aware of how much of their data is being used when they buy mobile applications. That is due to the confidentiality of many IoT devices. Many IoT devices are "live and listening" without their user's consent. Most people do not read privacy policies for certain devices and they tend to overlook how much sensitive information is being used. IoT devices collect an increasing amount of personal data. The more data that an organization collects, the more data that has to be safeguarded from being used or stolen. These devices also create new pathways into unauthorized environments. More data is being stored in unknown data storage areas. This is dangerous because the user might not be aware of these storage areas existing but hackers can. Also, unnecessary and unknown data sharing is very dangerous in protecting privacy. The user is usually unaware that many third and fourth parties could get their data from the user's environment. Some of that is due to a lack of corporate transparency to their consumers. Some of these industries won't improve on privacy until the customers demand it. Because the Internet of Things is still a very new concept that is being put into fruition, there are a lot of privacy issues that need to be addressed. That gives companies time to work on these issues and thankfully there has been effort put into protecting the customer first.

The Internet of Things is still a fairly new advancement in technology. Therefore there are still a lot of privacy leaks. Preserving the privacy of IoT devices should be one of the main priorities for the flourishing and successful development of the IoT system. Thankfully, there have been new approaches to address privacy concerns. A key feature to preserve privacy in the IoT environment is privacy by design. The ability to preserve privacy should already be within the device itself. In a book written by Hany F. Atlam, he states "The IoT customers should have the required features to control their information and define who can access it." Companies should be able to install built-in tools to preserve users' privacy better. One other solution to preserve privacy is to make IoT users more aware of privacy threats. The lack of public awareness is one of the biggest problems of privacy violation. Users of IoT devices need to be more aware of how to keep themselves more protected against privacy threats. There should also be more openness and transparency with consumers on how their information is being collected and why their data is being used. The consumer should also be aware of any third parties who get their hands on their information. IoT devices can gather millions of data per day. This amount of collection of data will increase the number of data threats. That much data isn't necessary for IoT devices to function. Personal data should be reduced to the point where the data is only related to the service that the IoT device provides. It should not be possible to track a user through events or geolocation. There should be a mutual agreement between the consumer and the provider to be able to respect the privacy of the consumer. More cryptographic techniques are being used to preserve privacy in IoT devices. Using these techniques to encrypt data is a good way to protect privacy. Unfortunately, it's not the most cost-friendly solution. There are limited storage and computation resources in IoT devices so it would cost more to increase storage amounts. Data anonymization is also a very good solution to address privacy concerns. Data anonymization is the process of protecting private or sensitive information by erasing key identifiers that connect a certain person to their stored data. Removing these sensitive identifiers will remove the identity of the individuals in the database. In the book "Privacy-preserving wireless medical sensor network", the authors X.Yi, J.Willemson, and F.Nait-Abdesselam proposed an integrated privacy protection scheme for end-to-end security. The security requirements of their technique include a concrete connection between gateway and IoT, the persistence of data into the IoT data storage, and lastly access to IoT data without disclosing the data to other servers or the user. This includes using an encryption scheme to split the data based on the server configuration. It also includes using a homomorphic encryption scheme which requires the user to provide public and private key pairs to access the data. However, even though it's still a rare case, computationally powerful attackers can break cryptographic puzzles and become a threat to these systems. One of the most capable solutions in enhancing the privacy of the IoT is to ensure that there is less user-identifying data outside the individual's sphere. To earn this goal it would require the IoT to focus more on the local processing of data rather than the centralization of it. There are possible mobile applications that help support customer privacy in IoT. A privacy coach is a mobile phone application that customers can use as support to help in privacy decisions. It helps the user with making informed privacy decisions in a user-friendly manner. There are a lot of approaches to addressing privacy concerns in the Internet of Things. Right now, these won't fix all of the privacy concerns at once, but breakthroughs in IoT technology and companies putting privacy first are 2 of the main reasons why there have been plenty of solutions.

The Internet of Things is a newer piece of technology that is changing as we speak. IoT can exist from a consumer's car to their microwave. IoT devices are now considered an everyday item for a consumer. Because IoT devices are very affordable, there's room to use plenty of them. Since IoT devices are still a new concept, users tend to have privacy concerns about them. These devices collect millions of data every day and even though that is unfathomable, it does put that consumer at risk. There hasn't been an emphasis on privacy because users for years have not been educated about their privacy. An IoT device collects sensitive information that it doesn't even need and it could pose a risk just by a faulty hardware issue. The more data that a company collects, the more data that has to be safeguarded from being used or stolen. So why is it necessary for the company to collect all of this data when it only creates a big responsibility to keep it from being stolen? Companies should only be using consented data and data that are relevant to the IoT devices that the company makes. Companies have also been more transparent now and consumers are getting more aware of how their information is being used and who it's being sent to. Making business decisions based on a customer's information is something that can't be done without their consent. There should be more stable confidentiality in the privacy of a consumer. Companies are investing more into security to make sure that customer privacy does come first. Overall, these approaches have made users comfortable with using IoT devices more and it should stay like that. Hopefully, more branches of technology have the same urgency and protect their consumers.

**Related References**

**What is the internet of things (IOT)? What Is the Internet of Things (IoT)? (n.d.). Retrieved December 1, 2021, from** [**https://www.oracle.com/internet-of-things/what-is-iot/**](https://www.oracle.com/internet-of-things/what-is-iot/)**.**

**Thomas, Mike, and Communications Specialist. “27 Top Internet of Things Examples You Should Know.” *Built-In*, https://builtin.com/internet-things/iot-examples.**

**Ranger, Steve. “What Is the Iot? Everything You Need to Know about the Internet of Things Right Now.” *ZDNet*, ZDNet, 3 Feb. 2020, https://www.zdnet.com/article/what-is-the-internet-of-things-everything-you-need-to-know-about-the-iot-right-now/.**

**“18 Most Popular IOT Devices in 2021 (Only Noteworthy IOT Products).” *Software Testing Help*, 29 Nov. 2021, https://www.softwaretestinghelp.com/iot-devices/.**

**Bannan, Christine. “The IOT Threat to Privacy.” *TechCrunch*, TechCrunch, 14 Aug. 2016, https://techcrunch.com/2016/08/14/the-iot-threat-to-privacy/.**

**Harvey, Cynthia. “85 Top IOT Devices.” *Datamation*, 7 Apr. 2021, https://www.datamation.com/mobile/85-top-iot-devices/.**

**Intelligence, Insider. “The Security and Privacy Issues That Come with the Internet of Things.” *Business Insider*, Business Insider, 6 Jan. 2020, https://www.businessinsider.com/iot-security-privacy.**

**Tawalbeh, Lo’ai, et al. “IOT Privacy and Security: Challenges and Solutions.” *MDPI*, Multidisciplinary Digital Publishing Institute, 15 June 2020, https://www.mdpi.com/2076-3417/10/12/4102/htm.**

**“Enabling Privacy and Security in Cloud of Things: Architecture, Applications, Security & Privacy Challenges.” *Applied Computing and Informatics*, https://www.emerald.com/insight/content/doi/10.1016/j.aci.2019.11.005/full/html#sec004.**

***A Survey on Internet of Things: Security and Privacy Issues*. https://course.ccs.neu.edu/cs7680su18/resources/pxc3894454.pdf.**

***IOT Security, Privacy, Safety and Ethics - Springer*. https://link.springer.com/chapter/10.1007%2F978-3-030-18732-3\_8.**

[**https://www.sciencedirect.com/science/article/pii/S0167739X17303308?casa\_token=W2gBdNu9UqwAAAAA:CEJL0l14LdukfhGWdBqw4IE6AF-KWhR8-JLHxIq5lv8ebeUZCD8NkArwr6pE-wHDj9ARI3-1CbE**](https://www.sciencedirect.com/science/article/pii/S0167739X17303308?casa_token=W2gBdNu9UqwAAAAA:CEJL0l14LdukfhGWdBqw4IE6AF-KWhR8-JLHxIq5lv8ebeUZCD8NkArwr6pE-wHDj9ARI3-1CbE)

***Privacy and Security Challenges and ... - Iopscience.iop.org*. https://iopscience.iop.org/article/10.1088/1755-1315/322/1/012013.**

***Hings T The Quest for Privacy in the Internet of Things*. https://www.researchgate.net/profile/Pardeep-Kumar-55/publication/299598126\_The\_Quest\_for\_Privacy\_in\_the\_Internet\_of\_Things/links/5a5f3c89aca272d4a3e0d669/The-Quest-for-Privacy-in-the-Internet-of-Things.pdf.**

***Security and Privacy Issues in IOT - Researchgate*. https://www.researchgate.net/profile/Malaika-Moiz-2/publication/313574376\_Security\_and\_privacy\_issues\_in\_IoT/links/5f8e1613458515b7cf8dbd62/Security-and-privacy-issues-in-IoT.pdf.**