6

AI, 5G, and IoT: Driving Forces Towards the Industry Technology Trends

6.1 Introduction

The world of Artificial Intelligence (AI), fifth-generation data networks (5G), and the rapidly growing Internet of Things (IoT) devices can be beneficial to us, but also present numerous flaws as they are all new and rapidly developing technologies. It is important to note that the 5G network has better security than the third generation (3G) and forth generation (4G) networks. Still, it has been said that some of the classic vulnerabilities and security flaws from 3G and 4G networks were directly carried over to the developing 5G network, thus presenting additional security flaws right out of the gate. Both AI and the IoT will benefit from the development of 5G networks where businesses can use such devices, which will be tied to the growing 5G network, and can serve several purposes throughout the business market, among other areas.

When it comes to consumer-based electronic devices, they are certainly on the rise. As technology improves, these devices will consume more bandwidth and data than ever before. The increase in data and bandwidth consumption from newly emerging technologies could include the ability to interpret human speech on-the-fly and identify various patterns throughout data or documents from a mobile device. This data can even adjust business efficiency, increasing overall profits with endless possibilities for automation in manufacturing. This is where the development of 5G data networks come into play. 5G networks will have the bandwidth needs for current and future data-hungry devices in a growing technological world.

AI technology is growing from ordinary scientists' simple tools to as far as the use within the professional development community for higher intelligence use. These various organizations can use AI technology to fill the current gap in the data science area, a big game-changer for data science! This also always gives end-consumers the ability to take their business and personal data wherever they go. This is a big deal when making end-consumers happy while retaining their privacy with their online data.

When it comes to data processing, with the help of 5G, AI, and the IoT, modern technology demands that data management and processing capabilities should have the data possessors brought to the data itself rather than sending the collected data processing elsewhere. This may also include the data processing and distributed data stores included within the data management process in order to guarantee that support is offered where

Intelligent Connectivity: AI, IoT, and 5G, First Edition. Abdulrahman Yarali.

the received critical data is being stored. 5G network technology will be revolutionary to end-consumers, businesses, and data processing centers worldwide.

6.2 Fifth Generation of Network Technology

The new 5G data networks will likely introduce many new network-connected devices along with it, and many of those devices will probably have capabilities and new functions we cannot imagine. The technology is so unique that it is still in rapid development, even though some larger cities will have 5G access when this document is published. 5G networks introduce a world of technological ease and sophistication, which was not possible in the past. Multiple virtual networks can be both supported and created, which can assist various markets and corporations.

Mobile IoT can benefit from 5G because they will support more connections with increased speeds and much lower latency. This could increase overall profits or even maximize business or corporate revenue, all from a little Mobile IoT device!

5G networks will also enable drones to make quick and secure deliveries straight to customers' homes. The 5G network will help coordinate large fleets to fly safely and avoid hitting buildings and other drones en route (GSMA 2018). This would be made possible with an AI-based on-board computer that collects data via in-flight sensors, will always monitor the drone's surrounding environment, and be able to adjust to almost any situation while in flight.

The development of 5G is quite revolutionary, with high capacity, network slicing, low latency, and incredibly fast speeds (Mo 2019). With the increase in data speeds with 5G, there is a lot of "wiggle room" for bandwidth control. Since 5G has the ability for network slicing, it can control the IoT uses that have various bandwidth needs for large or small amounts of data that need to be rapidly sent over the internet.

6.3 Internet of Things (IoT)

As the IoT technology grows and develops over time, it will likely mold into a global network with securely managed devices that will be slowly integrated into our day-to-day lives. This advancement will improve the overall quality of public life as we know it. Businesses will also have access to the luxuries of 5G networks. The 5G network will become an excellent opportunity for the growth of the IoT, which will have massive bandwidth, better coverage, and overall faster speeds compared to the previous cellular networks. Figure 6.1 depicts the vast reality of IoT descriptions and definitions. As illustrated in the schematic diagram, the top right section shows sensing and data collecting IoT smart objects with an IP address. The upper left section shows the connectivity of everything via a handheld device such as a smartphone – the internet of people. The lower part of the picture shows IoT non-IP connectivity – industry IoT (i-Scoop, n.d.).

5G also has capabilities to arm and disarm security alarms, sensors, and IP cameras, with real-time, high-quality videos for enhanced remote surveillance, which could help reduce the chances of theft or crime in general. The combination of AI with the massive capacity and endless possibilities that comes with 5G networks would significantly improve sensor-based systems, decreasing overall energy consumption.

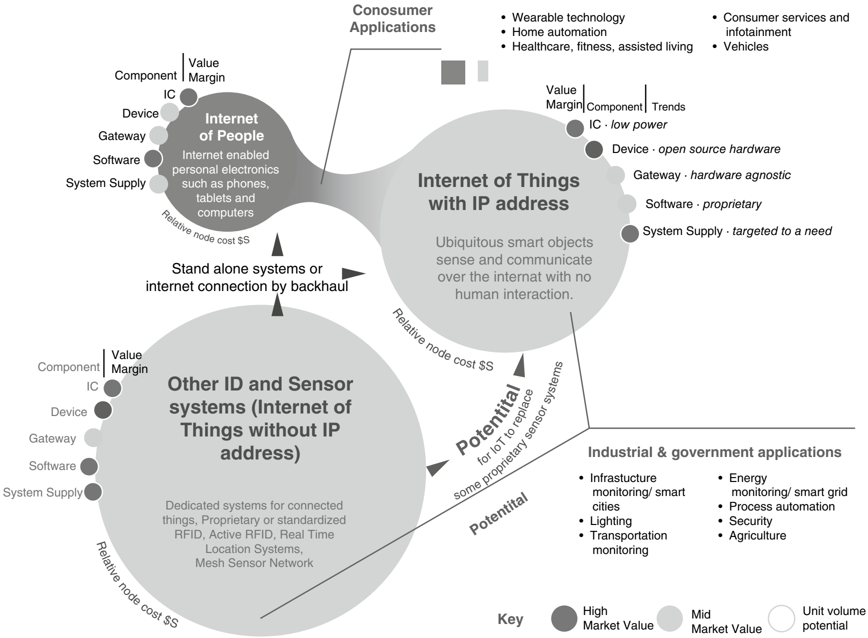
Conosumer Applications
• Wearable technology
• Home automation
• Healthcare, fitness, assisted living
• Consumer services and infotainment
• Vehicles
Component
Value Margin
IC
Device
Gateway
Software
System Supply
Internet of People
Internet enabled personal electronics such as phones, tablets and computers
Relative node cost $S
Stand alone systems or internet connection by backhaul
Value Margin
Component
Trends
IC · low power
Device · open source hardware
Gateway · hardware agnostic
Software · proprietary
System Supply · targeted to a need
Internet of Things with IP address
Ubiquitous smart objects sense and communicate over the internat with no human interaction.
Relative node cost $S
Other ID and Sensor systems (Internet of Things without IP address)
Dedicated systems for connected things, Proprietary or standardized RFID, Active RFID, Real Time Location Systems, Mesh Sensor Network
Relative node cost $S
Potentital
for IoT to replace some proprietary sensor systems
Potentital
Industrial & government applications
• Infrastucture monitoring/ smart cities
• Lighting
• Transportation monitoring
• Energy monitoring/ smart grid
• Process automation
• Security
• Agriculture
Key
High Market Value
Mid Market Value
Unit volume potential

Figure 6.1 IoT map illustration and definition (i-Scoop).

It has been said that 5G, as we know it, was initially built primarily for the IoT devices and their intended uses, not just for the average consumer with a cell phone. IoT can be viewed as a “three-layer cake” in layman’s terms (Mo 2019):

1) The very bottom layer where the IoT devices such as the GE engine, Google Nest, or Amazon Echo are.
2) The center layer where a communication “pipe” or network such as 5G provides internet connectivity between the devices themselves and the cloud servers.
3) Finally, the top layer where the IoT software applications are powered by AI, their algorithms, and Business Intelligence.

When it comes to IoT devices, there is no specific company or agency in charge of the IoT. Businesses and corporations will often find IoT devices and their software applications beneficial when used within a manufacturing or production environment. It should be known that the IoT devices are not an entirely separate entity from the internet itself but more of an extension or branch of the internet as we know it, which is continuing to grow daily. It has been estimated that the concept of the IoT is likely to be a widespread game-changer to the global economic system. However, it is still far too early to be certain as the IoT devices and their technology are still under rapid development.

Experts predict that IoT devices and their computing software will be revolutionary to the Information Technology fields, especially due to their small size and computing efficiency for the price (Mo 2019). When pairing IoT devices with the new 5G network, a whole new computing world in information technology (IT) will be developed for small, energy-efficient computing uses. The IoT technology even allows vehicles of all types and models to be equipped with technologies for a safer commute using an intelligent mass transportation system everywhere, all with the combined use of 5G networking technology (Fischer 2015).

The IoT devices and their corresponding technologies will make cities appear as "computers in the open air," where general public foot-traffic will have the ability to interact with the city's IoT technology systems in real-time out on the street. With the growing demand for technology, there will always be constant access to any kind of information one could ever want. Thanks to the IoT technology, these services have advanced to a whole new level with interactive technology right on the street corner. Some IoT technology experts have predicted that with the massive growth and expansion of the IoT technology, we will soon be living in an entirely "hyper-connected" society, where there will be seamless integration of everything. Perhaps this move will cause the internet to vanish and become a wholly separate phenomenon (Fischer 2015).

While they are in no way responsible for the IoT technology or the devices themselves, the United States Department of Defense has been a huge leader in the underlying development of the IoT devices and technology (Fischer 2015). Numerous other companies have assisted in the research and development of the IoT devices, but the United States Department of Defense is the largest contributor by far. The National Science Foundation has also participated in other contributing activities associated with various IoT technologies and software development.

The IoT devices are being deployed and developed daily for new uses in various industries, especially in the manufacturing sector. Some networking experts argue that the current network framework used for spectrum allocation may not benefit the IoT devices as well as it could be. For now, there are not any universally recognized technical standards for the IoT devices or their corresponding software uses, but that may change as the IoT technology grows and develops over time.

Cybersecurity for the IoT may be complicated by several things, such as the complexity and pervasiveness of networks and the increasing demand for industrial automation for cost-cutting measures, which may severely affect network security and network and device authentication. Cybersecurity legislation has addressed multiple issues concerning IoT applications, such as notification of data breaches and information sharing, but nothing has been "set in stone" for now.

- Spectrum Access Radio is a type of frequency spectrum that is considered a critical link in all kinds of IoT device communication systems. Affordable and reliable access to it is a significant requirement to accommodate the billions of new IoT devices expected to be deployed and go online, just within the next decade alone.
- According to Congressional Research, there are no official bills that have been introduced in the last two congressional meetings that directly relate to the IoT devices and their peripheral devices (Fischer 2015). Numerous bills have been introduced to Congress that refer directly to general concepts of the IoT technology, such as smart-connected vehicles, smart cities, cyber-physical systems, and the public smart-city grid. The IoT world is still under rapid development today but is expected to take off rapidly with the development of 5G networking technology to back it up.

6.4 Industrial Internet of Things

When it comes to the industrial sector of the IoT, many of these devices require extremely low latency for maximum operation efficiency, depending on their intended application. This is where 5G network technology comes into place. Low latency 5G networks are achieved initially through architecture where 5G networks only have 1 ms latency, compared to the standard Fourth Generation Long-Term Evolution (4G LTE) network with about 20–30 ms latency (Mo 2019). The 5G network is revolutionary when it comes to the Industrial Internet of Things (IIoT).

5G with the IIoT is a merger of the internet, intelligence, and electronic devices, all of which will be routed through the developing 5G network. It could help reduce the chances of theft or any other crime in general with devices that operate on the 5G network and support more connections with increased speeds and much lower latency. AI will have the ability to better grow and function efficiently with 5G technology that can make any process more efficient and improve our overall quality of life. The evolution and widespread use of 5G and AI technology is heavily anticipated, which is suspected to be revolutionary as the technology ages and is eventually perfected and implemented globally.

With the IIoT, businesses could be remotely operated and/or managed from the other end of the world at any time, if needed! With the intelligent connectivity of the IIoT, a business firm can interact with customers from any part of the world at any given time, leading to an increase in sales and an overall rise in the profit margin with reduced costs throughout the business.

- The data collected from IIoT devices can help businesses understand customers better and even bring in changes in various areas of the company to suit future consumer needs. This level of personalized customer experience is the only thing that will differentiate a specific brand from the rest of the industry, with an increase in financial income and profits and a positive impact on a company with higher conversion rates and an overall increase in customer loyalty. This approach is key to a striving company in today's evolving and monopolizing market.
- Digitization with IIoT devices can bring in that uniqueness to a business and offer unique opportunities to corporations to re-position their company in the market while creating advanced service offers for current and future customers. This move can make a business stand out from the rest of the market by using the IIoT devices efficiently.
- As businesses and corporations are rearranging themselves in the digitalization sector and making the shift towards intelligent connectivity with the smart IIoT devices, this is also a good time to be re-positioned in today's market by understanding customers' trends and demands. It is essential to understand consumer needs with 5G network technology, consumer IoT devices, and personalized and innovative services for the average person. This is key to a striving and successful company and consumer in today's growing and revolutionizing market, using the IIoT devices and 5G network technology.

6.5 IoT in the Automotive Industry

It has been predicted that technological advancements and changes will have significantly increased in the automotive industry alone in the next decade. In the automotive industry, end-consumer demands must be met in full for a modern-day tech-filled experience when researching, purchasing, and driving a new automobile. Today's technological advancements, combined with the development of the IoT technology, put the automotive industry under a lot of pressure for a rapid transition to modern technology in a vehicle. That is why inventions such as the IoT devices and AI make such a huge impression on today's automobile industry. The primary focus for auto manufacturers will be on smart-connected automobiles using the IoT technology. All this combined suggests new and revolutionizing trends applied within the automobile industry yearly.

- The consumer's overall automotive experience is being customized to their needs with modern technology trends. Unfortunately, these trends also pose numerous security risks and vulnerabilities. These technological advancements in the automobile industry are being implemented much sooner than expected. The automobile industry today has already been permanently changed, for good. We already have basic smart connected automobile technology and fully electric cars paving the path for more advancements soon!
- Of course, these modern automobile trends are still under rapid development today. Nevertheless, these developments and trends will likely forever change the basic automotive industry's manufacturing processes and how we use and operate these smart-connected automobiles as drivers. Unfortunately, the automotive manufacturing industry has recently decided to move away from national and regional manufacturing/production of certain cars for a broader connection and approach to the overall automotive manufacturing technology supply chain.

The trucking industry already utilizes many modern technological advancements with the IoT and smart-connected sensors to allow drivers and their employers to view and monitor the truck's information in real-time to ensure fuel efficiency and driver and truck safety.

Additionally, Lyft and Uber's services have started a new trend from owning personal vehicles for a service-based "private" transportation versus taking the local public transit bus. Partnerships are also rapidly growing with these ride-sharing companies. Online rumors say Volkswagen is currently developing its ride-sharing application, as well, although, if true, the development could fall through or become another top competitor in that market. This trend is just the start of the ever-growing ride-sharing path!

As we know, the automotive industry has made a considerable shift from a product-centered to a data-driven industry combined with the fusion of AI, IoT technology, and Big Data in this industry. New technology for predictive maintenance is based on unique sensors combined with the IoT technology that records and logs data on the automobile's current performance in real-time. The data is then sent to the "cloud," where any potential malfunctions of a vehicle's hardware, software, and physical components are evaluated.

After this recorded information is reviewed and processed automatically, the driver will then be notified of any necessary mechanical or software services to have completed in order to avoid any incidents or potential permanent damage to the automobile internally or electronically. This eliminates any guesswork when it comes to vehicle maintenance or repair, including anything else mechanically! Drivers can immediately be notified of any potentially serious on-board issues.

The system software can also predict any issues before they happen, thanks to AI technology. This is also likely to reduce the vast number of recalls that occur every year for newer vehicles. This system is likely to become so advanced that it will track something as simple as tire wear with carefully placed wheel-well sensors combined with AI and IoT technology. With over-the-air technology in automobiles, dealers and automobile companies can track common issues with their automobiles in real-time, a serious game-changer with safety in the automobile industry and manufacturing processes.

Another possibility with the combination of AI and the IoT technology is remote wireless service from anywhere at any given time. A digital interface in automobiles allows continuous over-the-air updates to automobile software. This eliminates the current necessity of having to go to the dealership with your car to have the computer software fixed and reprogrammed, assuming they even do it at all! This remote technology also allows for software fixes that could increase fuel efficiency or save battery life in all-electric automobiles.

Tesla's automotive manufacturing company already has this remote technology feature in their automobiles with "over-the-air" updates. Their incorporated automobile technology gives their vehicles the ability to connect to the consumer's home wireless network, where Tesla automobiles can receive software updates just as soon as the updates are released. Their cars receive regular updates that add new features and enhance existing ones over wireless networks (Tesla 2019).

It is no secret that the automobile industry is now the largest data-driven industry globally, next to data information security and protection. Today's world wants the ability to take modern technology wherever we go. Almost all new vehicles come with a wireless internet connection function; this means premium security is also needed and automobile manufacturers understand that.

Data security and overall protection are critical, so data security is always a top priority for technological advancements, especially in the automobile industry. Mass, rapid, widespread changes in the automobile industry still present considerable challenges during the initial development phase. In addition, the overall improvements and end-consumer benefits of these modern technological advancements significantly outweigh any of the challenges that come with them.

As most of us already know, basic, reliable automobiles that only get us from point A to point B are not the only top priority for automotive manufacturers. It also includes mass amounts of technology mixed in. These modern changes and technological improvements impact product development significantly. Although it is still the automobile industry's task to design and manufacture contemporary, reliable vehicles, the new mixture of old manufacturing techniques and new smart technologies requires placing modern-day automotive engineers under tremendous amounts of pressure. As the automotive industry makes a significant change towards modern technological product development in the manufacturing process, the pressure will only increase for it to be completed faster, more efficiently, with a shrinking budget, while produced in mass quantities with fewer resources available. This new trend is only getting started for the automotive side of the IoT.

6.6 IoT in Agriculture

As discussed so far, the IoT has drastically revolutionized and changed how we live and how we operate in areas such as the general manufacturing industry, smart-connected vehicles, and smart-connected cities. Taking all the IoT technology and specifically applying it to the agricultural sector as a whole is where we will all see an enormous impact, even as supermarket produce consumers.

The agricultural industry can use wireless sensors combined with the IoT devices that use specialized communication techniques to process and analyze gathered field information to improve the agricultural industry. Specialized sensors are available for specific agriculture applications, such as soil preparation, crop status, irrigation, and insect and pest detection, which can help the farmers throughout the crop growth stages, from sowing until harvesting, packing, and transportation. The use of unmanned aerial vehicles for crop surveillance and basic field monitoring for optimizing maximum crop yield can drastically change crop production for the agricultural industry.

"The global population is set to touch 9.6 billion by 2050" (Anonymous 2018). With the global population expected to grow to such numbers, the agricultural industry must team up with the IoT technology to accommodate such a rapidly growing and demanding population. With the fusion of IoT devices, commercial and independent farmers will both be able to take advantage of modern technology to cut costs and reduce overall waste and help save the environment from potentially aggressive and unfair farming practices.

As farmers adopt IoT devices with their farming techniques, the overall crop yield will significantly increase. The adoption also includes using wireless field sensors to monitor crops for their health or merely recording yearly local weather patterns to more accurately predict planting a specific type of crop to increase maximum quality and quantity upon each harvest. These sensors can include the ability to detect soil preparation, crop status, irrigation, insect/pest detection, light, humidity, temperature, soil moisture, etc. (Anonymous 2018). The use of wireless IoT sensors alone can help increase crop yield, resulting in increased profits while saving the process's environment.

Although we must face it, this is the real world we are talking about. Integrating this modern IoT technology with decades-old traditional farming techniques and practices is not always going to be easy, or sometimes even possible at times. Farmers do need to be willing to accept change for modern technology to operate at its best for maximum results. The IoT and the world of agriculture can be a great duo together if used correctly. Some older generation farmers may fear new technology such as this, which is very understandable. In general, the IoT devices or technology can be overwhelming to older generation farmers used to basic traditional farming practices with minimal to no advanced modern technologies in the mix. The willingness to accept a modern change is a huge benefit to everyone, even the environment!

IoT devices and their attached wireless sensors can offer unique communication techniques that can be coordinated together for a farmer's specific application, such as soil quality, crop health, or even livestock and their health for the cattle farmers. These various IoT devices and their sensors can be programmed to collect any kind of data necessary to enhance the agricultural experience, which results in better control over internal processes and variables with reduced production risks in the end. IoT devices equipped with AI technology operating on 5G network technology can easily predict the outcome of crop health, yield, and overall growth progress before the crop is even close to harvest. The same can be done with livestock farmers, such as cattle farmers. Specialized wireless sensors can use AI technology to monitor, predict, and log future livestock health and overall wellness outcomes. These sensors can also monitor any new or developing diseases livestock are subject to in the outdoors. This technology can find and track these diseases in the beginning stages before livestock shows any visible signs of illness, often too late for a cure. This advanced technology allows farmers to take immediate action much sooner than before, potentially lifesaving for livestock, preventing livestock farmers' additional financial losses, and thus increasing yearly profits over time.

One of the most popular wireless IoT sensors is the Weather Monitoring Station (Aleksandrova 2018). These stations can collect and monitor local ambient air temperature, humidity, and moisture levels over a specified period. AI technology combined with the IoT devices can then use this recorded information to predict the highest yielding crop type for that year that should be sown for maximum farmer's profits and minimum resource waste upon harvest. This smart connectivity through 5G wireless will provide precision farming.

Another popular IoT device technology used in agriculture is Greenhouse Automation (Aleksandrova 2018). The weather station sensors previously mentioned can be attached to irrigation equipment and/or lighting systems via wireless or Local Area Network (LAN) network technology and be controlled and operated to match specific pre-defined system parameters to maintain or improve crop health. There is a benchmark or normal data comparison with crop health conditions, whether it be soil moisture or specific lighting conditions necessary for a specific crop to grow or improve health. Specialized IoT sensors can be strategically placed throughout crop fields to collect live data. Artificial intelligence, paired with the IoT devices, is fully automated to operate in the most efficient manner possible.

Cattle and livestock monitoring sensors are wearable devices directly attached to livestock to monitor their health and log performance over time (Aleksandrova 2018). These sensors can monitor livestock body temperature, activity, health, and each cow's nutrition intake with down-to-the-minute live data. This data collection can be paired with the IoT technology to help farmers know what feed is best for a breed of livestock or know which ones are healthiest for breeding or slaughter. The use of the IoT technology in the agricultural sector has eliminated the traditional "guessing game" factor that can often be financially fatal, resulting in livestock farmers' financial losses.

One of a crop farmer's largest enemies is the inevitable insects! Thanks to modern technology, the IoT devices and their wireless sensors can monitor insects and unwanted pests. When this IoT technology is directly connected to pesticide equipment, the AI software can automatically deploy pesticide spray for crops if weather conditions are appropriate. Other sensors used for pest detection can include low-power sensors and cameras, high-power thermal sensors, fluorescence image sensors, acoustic sensors, and gas sensors (Biz Intellia 2019). These sensors can detect pests down to the smallest known species that cause crop diseases that are not even visible to the human eye!

Another advantage is the combination of AI and IoT technology, which can help crop farmers throughout crop growth stages by using a series of wireless field sensors paired with cloud computing technology. This integration will predict precisely when to plant a specific crop, based on gathered historical data from exterior on-site weather monitoring stations and their sensors. The AI technology can then use field sensors to mathematically predict when it is best to harvest the crop for maximum crop yield with minimum waste of local resources such as fuel used during the harvest and transport process.

The agricultural IoT devices can also compute how best to pack crop yield and transport it with maximum efficiency based on collected current and historical data combined with local wireless sensors. The AI technology can access local weather condition sensors mapped with current local fuel prices to identify the best day to transport the harvested crop to the local crop purchase center for maximum profit.

One of the most significant advancements using AI and the IoT technology in agriculture is the development and use of unmanned aerial vehicles (also known as drones) for crop surveillance and crop yield optimization mapping. Agricultural drones are becoming very popular in modern-day commercialized agriculture. These drones are used for precision farming with an aerial assessment of field crop health and surveillance, where standard IoT field sensors simply cannot operate. Aerial drones can map current field layouts better and analyze the soil conditions from above. The drone's altitude and image optimization quality can be selected based on the user's input.

Drones can also map objects and areas such as excess tree canopy coverage, shading crops from maximum sunlight, preventing healthy crop growth, excess field water ponding, and drainage. These issues can also cause crop growth and health issues, which can also initiate crop diseases and crop fungus. Aerial drones can be equipped with heat-mapping technology to scan crop fields from above and assess crop growth statistics where improvements can be made in the future (Aleksandrova 2018). The possibilities are nearly endless with agriculture-oriented aerial drones.

Like agricultural aerial drones, unmanned full-size aerial vehicles can be used in agriculture for various large-scale tasks. One of the most common uses is to spray field crops from above. Using an unmanned aerial vehicle allows farmers to spray pesticide or fertilize crops, even if field conditions are not favorable for traditional land-based man-operated spraying equipment. The unmanned aircraft can map out exactly how much pesticide or fertilizer to spray on each acre of the crop to maximize efficiency and minimize product waste. While spraying, the aircraft can also monitor and log current field conditions from an aerial perspective. AI and the IoT system can combine this collected information from field sensors and aircraft sensors and create a detailed live report on current field and crop conditions on-demand. Farmers can then use this collected data to know when and where to make corrections to field soil or where conditions may not be favorable for optimum crop growth.

The IoT has drastically changed and revolutionized how we live our day-to-day lives in areas such as the manufacturing industry, smart-connected cities, and even smart-connected vehicles. Taking all this modern IoT technology and applying it to the agricultural industry, operating on the 5G network, is where the largest impact is made that affects all of us. The agricultural industry can use wireless sensors with the IoT devices paired up with unique communication techniques to analyze and process collected current and historical field and crop information to improve the agricultural industry overall. This process results in less waste, environmental protection, and maximum profits from crop harvests.

Specialized sensors are available for specific agricultural applications, such as soil preparation, crop growth, health status, irrigation equipment monitoring, and insect and pest detection. These can help crop farmers throughout the crop growth stages, from sowing until harvesting, packing, and transportation. Finally, unmanned aerial drones and vehicles for crop surveillance or other favorable applications are important. Unmanned aircraft for crop production is a rapidly growing trend that can be used to optimize crop yield and aerial drone monitoring of field conditions, which can drastically change crop production and how much profit is made. Applying IoT devices and AI technology to the agricultural industry is where the biggest impact will be made.

6.7 AI, IoT, and 5G Security

Almost everything electronic that we see or use in our daily life will need some form of cybersecurity behind it. Even when we are offline just shopping around in the mall, there are IP cameras and many other digital devices. Security specialists who protect them from hacker intervention do not enhance this protection on a frequent and regular basis. The potential vulnerabilities of today's digital world should not cause any paranoia, but digital security basics are worth learning for everyone who uses modern civilization's benefits. Software updates and patches have become more important as technology has progressed and become more sophisticated over the years. They have numerous benefits like obvious security patches and add new features to user devices and other new software. These updates and patches to the IoT devices and AI software are now possible to do at revolutionary speeds, thanks to 5G network technology.

Firstly, what exactly are software updates and security patches? "Patches are software and operating system (OS) updates that address security vulnerabilities within a program or product" (NCCIC 2019). This means that software and firmware developers will often push out updates to provide security fixes and fix potential performance bugs throughout their software. It is also important to remember that hackers will often spoof work-related emails about out-of-date programs or computer software that will either contain a virus or provide a link to a malware-infected program disguised as an urgent "update."

There are no specifically defined standards for software updates and security patches. However, it is a very good practice in the information technology security field to maintain software/firmware updates and security patches. As most know, hackers love security flaws. Therefore, it is essential to keep the latest updates on any device no matter how often it is used. Hackers often write malware and viruses into code, so unprotected users become infected online if they click or download the wrong thing online. Suppose a device is connected to the internet in any way. In that case, it is fair game and vulnerable to hackers at any time, especially if the device is not updated regularly, which hackers often rely on. "These might include repairing security holes that have been discovered and fixing or removing computer bugs" (Symanovich 2019). It is always good to make sure your device runs the latest firmware with the most recent security patches to ensure the most cybersecurity while connected to the internet. This is the easiest step anyone can take to prevent hacker intervention.

Most computers are set to download new updates by default, but the average user is often guilty of clicking "install later" when the new updates window appears and is ready to install. This is an extremely bad habit for anyone to get into. This often happens because some updates and security patches can take longer than usual to install and ultimately disrupt what we are currently working on. Delaying updates far too often could reveal some significant security loopholes in older software/firmware that hackers love to take advantage of. The most recent Equifax data breach where more than 143 million American social security numbers were exposed had a well-known security vulnerability in one of their web applications. There was a fix for this well-known security vulnerability two whole months before the security breach occurred. Still, the Equifax security team failed to update their company software when the update was released for their systems (Davis 2017). This is a perfect example of why you should never delay software updates and security patches when available.

If your device contracts a virus or some form of malware, you have the potential to pass the infection on to other friends, family, and even work-related computers and devices. For example, suppose you forward what appears to be a legitimate email about an online work account to other co-workers or even your work email. In that case, you can infect other computers and devices as that infected email is opened and passed around. It is essential to maintain updates and security patches on your computers and maintain updates on your computer's anti-virus software and spam filters.

The future of device security updates is on the horizon. Updates will likely become fully automated in the future and be processed significantly faster, reducing overall downtime to install security updates and patches. Of course, no one can predict the future, but frequent updates will be vital to surviving an online world without hacker intervention as technology progresses with time. Most software, such as anti-virus programs, have automatic update features. These programs can still only do so much if you never update the device firmware to patch potential security holes. Make your best efforts to habitually check for updates manually on programs and firmwares that do not have automatic update features. Leaving any stones unturned could be a loophole to a network-wide security breach, which can be an extreme hassle for network security admins to resolve.

Businesses are some of the most vulnerable places subject to security attacks. "The 'gold standard' for the implementation of critical patches is 30 days and 90 days for non-crucial patches." (Security 2019). However, 30 days is still more than long enough for cyber attackers to damage when security loopholes are exploited. Unfortunately, many businesses and corporations approach things as "if it is not broke, do not fix it," and this business mentality can be the beginning stages of a virtual network disaster to that business. To a degree, some corporations cannot afford to shut down network operations at any given time to install updates and security patches, although downtime for the installation of network security patches and updates far outweighs any downtime due to a network-wide security breach.

It is vital to understand which software updates are necessary to install and which ones are not quite as vital for installation. It is overall good practice anyway to install any new software, firmware, or driver updates. Only apply automatic updates from trusted network locations (NCCIC 2019). This means only download the latest updates from trusted, reputable sites. Do not attempt to download updates from email attachments containing an "update" file or link to one somewhere on the dark web. Suppose you cannot install trusted updates over a secure network, such as your home or work network. In that case, it is best practice to set up a Virtual Private Network (VPN) connection for a fully encrypted online activity and then download the new updates.

Automatic updates are extremely important. For example, in 2012, the WannaCry ransomware attack hit more than 200 000 computers and networks before a 22-year-old cybersecurity whiz identified and activated a kill switch (ITRC 2012). Microsoft had already released a security patch update several weeks before this known security flaw was exploited. Still, most companies did not have automatic updates enabled, so the known security flaw could be patched. Software developers are often the only ones aware of any new potential security holes in their software. This approach will prevent hackers from being notified of new security holes in software that have already been released to the public, where hackers could push out new viruses and attacks. If you do not update your computers and network-attached devices, everything is fair game for hackers at any given time while online.

Some updates require you to restart your computer to go into effect, and you may not be notified when this is the case (UCSC 2015). Managed networks will often have software updates and patches downloaded and installed automatically. However, suppose they are not periodically rebooted. In that case, some of those important patches may not go entirely into effect, still leaving some network desktops and laptops exposed with open security loopholes that have yet to be patched. Some could argue that this is the network administrator's full responsibility to ensure the complete installation of updates to corporation-owned computers. Still, as an employee using company resources, it would only be appropriate for them to do their part, even if it is just rebooting a computer periodically.

Not only are security updates and patches critical in an online world, but the use of End-of-Life software is hazardous. Using End-of-Life software means that it is no longer supported by its maker (Martins 2018). This means there will be no more software security patches and updates, which means this is a honeypot for hackers! First, using any programs or operating systems beyond their support end date is the same as inviting hackers into the front door. Using software or firmware beyond its support date is never a good idea, especially in any business environment.

Secondly, using any End-of-Life software can also create compliance violations during an Information Technology (IT) audit. The IT department in any business setting must follow well-defined regulations to comply with any future audits. These audits are in place to ensure that large-scale businesses implement the highest security measures possible to reduce or eliminate as many potential security threats as possible. Using such outdated software is a direct violation of any security audit and leaves security loopholes wide open for hackers to come right in.

Thirdly, End-of-Life software can create software incompatibility issues in the future. Even if your local Information Technology Security Team has the know-how to develop security patches for End-of-Life software, there could still be compatibility issues with any other newer software business that may adopt it in the future. As a result, this could cause speed issues, efficiency problems, and/or security problems, just to name a few. These types of issues no business ever wants to come across, especially due to the use of End-of-Life software.

To wrap things up, everything electronic that we either see or use in our daily lives will need some form of cybersecurity behind it. Devices like IP cameras could be turned on us for evil use if the security specialists who protect them from hacker intervention do not enhance this protection regularly. However, it is important to remember that the vulnerabilities of today's digital world should not cause any paranoia. However, basic digital security is worth learning for everyone who uses the benefits of modern civilization and the devices that go with it. Software updates and security patches have become more important as technology has progressed and become more sophisticated over time. These updates have numerous benefits like obvious security patches and add new features to user devices and add other new software. Always keep your devices up to date to help prevent hacker intervention.

6.8 Conclusion

The world of AI, 5G data networks, and the rapidly growing IoT devices are beneficial to us. However, it presents numerous flaws as they are all new and rapidly developing technologies. It is important to note that the 5G network may have better security than the 3G and 4G networks, but it has been said that some of the classic vulnerabilities and security flaws from 3G and 4G networks were directly carried over to the developing 5G network, thus presenting additional security flaws. Both AI and the IoT will benefit from the development of 5G networks where businesses can use such devices, which will be tied to the growing 5G network, and can serve several purposes throughout the business market, among other areas.

When it comes to consumer-based electronic devices, they are certainly on the rise. As technology improves, these devices will consume more bandwidth and data than ever before. The increase in data and bandwidth consumption from newly emerging technologies could include the ability to interpret human speech on-the-fly and identify various patterns throughout data or documents from a mobile device. This data can even adjust business efficiency, increasing overall profits with endless possibilities for automation in manufacturing. This is where the development of 5G data networks come into play. 5G networks will have the bandwidth needs for current and future data-hungry devices in a growing technological world.

AI technology is growing from average scientific simple tools to as far as to use within the professional development community for higher intelligence use. These various organizations can use AI technology to fill the current gap in the data science area, a big game-changer for data science. This also always gives end-consumers the ability to take their business and personal data wherever they go. This is very important in making end-consumers happy while retaining their privacy with their online data.

When it comes to data processing with the help of 5G, AI, and IoT devices, modern technology and its data often demand data management and processing capabilities. This may also include data processing and distributed data stores. All must be included within the data management process to guarantee that support is offered where the received critical data is being stored. 5G network technology will be revolutionary to end-consumers, businesses, and data processing centers worldwide.

References

Aleksandrova, M. (2018, June 10). *IoT in Agriculture: Five Technology Uses for Smart Farming and Challenges to Consider*. DZone. https://dzone.com/articles/iot-in-agriculture-five-technology-uses-for-smart (accessed 22 June 2021).

Anonymous (2018, January 3). *IoT Applications in Agriculture*. IoT for All, https://www.iotforall.com/iot-applications-in-agriculture/ (accessed 22 June 2021).

Biz Intellia (2019, January 1). *A Complete Guide for IoT Based Pest Detection with its Benefits*. Biz Intellia. https://www.biz4intellia.com/blog/a-complete-guide-for-iot-based-pest-detection-with-its-benefits/ (accessed 22 June 2021).

Davis, G. (2017, September 19). *Why Software Updates Are So Important*. McAfee. https://securingtomorrow.mcafee.com/consumer/consumer-threat-notices/software-updates-important/ (accessed 22 June 2021).

Fischer, E. A. (2015). *The Internet of Things: Frequently Asked Questions*. Congressional Research Service. www.crs.gov (accessed 22 June 2021).

GSMA (2018, September 12). *New GSMA Report Highlights How 5G, Artificial Intelligence, and IoT Will Transform the Americas*. GSMA. https://www.gsma.com/newsroom/press-release/new-gsma-report-highlights-how-5g-artificial-intelligence-and-iot-will-transform-the-americas/ (accessed 22 June 2021).

i-Scoop (n.d.) The Internet of Things (IoT) – Essential IoT business guide. https://www.i--scoop.eu/internet-of-things-guide/ (accessed 22 June 2021).

ITRC (2012, June 17). *What are Security Patches and Why Are They Important*. Identity Theft Resource Center. https://www.idtheftcenter.org/what-are-security-patches-and-why-are-they-important/ (accessed 22 June 2021).

Martins, A. (2018, June 27). *5 Risks of Running End-of-Life Software*. Mail. https://www.atmail.com/blog/end-of-life-eol-software/ (accessed 22 June 2021).

Mo, D. (2019, January 1). *Internet of Things (IoT): The Driving Force Behind 5G*. Enterprisetechsuccess. https://www.enterprisetechsuccess.com/article/Internet-of-Things-(IoT):-The-Driving-Force-Behind-5G/c1dvY3UrWTBWS3pwY0pqbEpSMHpIUT09 (accessed 22 June 2021).

NCCIC (2019, November 19). *Understanding Patches and Software Updates*. CISA. https://www.us-cert.gov/ncas/tips/ST04-006 (accessed 22 June 2021).

Security, P. (2019, January 24). *The Importance of Updating your Systems and Software*. Panda Security. https://www.pandasecurity.com/mediacenter/tips/the-importance-of-updating-systems-and-software/ (accessed 22 June 2021).

Symanovich, S. (2019). *Five Reasons Why General Software Updates and Patches are Important*. Norton Security. https://us.norton.com/internetsecurity-how-to-the-importance-of-general-software-updates-and-patches.html (accessed 22 June 2021).

Tesla (2019, January 1). *Software Updates*. Tesla. https://www.tesla.com/support/software-updates (accessed 22 June 2021).

UCSC (2015, September 1). *Install Operating System and Software Updates*. UC Santa Cruz. https://its.ucsc.edu/security/updates.html (accessed 22 June 2021).