14

Artificial Intelligence, 5G, and IoT: Security

14.1 Introduction

The Internet of Things (IoT) has become a major phenomenon in the last few years. The heightened increase in smart devices has enabled service providers and consumers to retain and manage big data daily. The data that is being gathered has become more complex and uncertain. Therefore, most researchers have turned to Artificial Intelligence (AI) to tackle big data problems. Over the years, there have been two main motivations to expand the IoT. The first one is to increase the amount of information shared by databases and objects in the real world. The second one is to enable users to share information and control objects in the real world. These two motivations make IoT more attractive to people. Therefore, IoT has become a good advancement of the conventional internet.

However, it should be noted that IoT is still at a young stage in terms of technological development, but it can be greatly improved by endowing its functions with much more intelligence. The progress made in AI has been significant over the past few years. All AI technologies required to make IoT intelligent are currently feasible. However, the main issue that needs to be addressed is comprehending and effectively applying AI technologies to current IoT systems.

14.2 Understanding IoT

There are several building blocks for IoT, which operate simultaneously by operating and communicating with each other. These building blocks include application and user interaction, cloud server, network or connectivity, gateway, and physical objects and devices such as sensors and actuators. The main objective for understanding IoT is to increase the existing internet functions and ensure it is more effective. When using IoT, users can share information provided by human beings, which are contained in the database, as well as the information provided by things in the physical world. The IoT has sensors that get information about the state of things. This processor creates orders that regulate things, such as wireless technology for transferring information from sensors to the internet and the internet to the controller. It also has a control unit for executing human orders, thereby

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

regulating the state of things. For example, suppose an IoT is designed to regulate temperature. In that case, a standard room temperature will be established in advance, and the actual room temperature will be obtained by the sensor/sensors and transferred through a wireless medium, such as the internet. After the processor receives the actual room temperature, it compares it with the designated value. It establishes an order to regulate the room temperature and ensure it is within the specified range. However, if the interaction between the physical and the environment becomes complex, the embedded processor function becomes complex, making IoT unsatisfactory. The most successful approach that has been used to solve the complex problem is AI.

14.3 Artificial Intelligence

Conventionally, AI means the simulation of logical human thinking using computer technology (Merriam-Webster 2018). AI technologies include perception, cognition, decision-making, strategy-execution, and strategy optimization. The technology of perception is used to acquire the ontological information (OI) about the objects or problem within the environment. In addition, this technology is used to turn ontological information into epistemological information (EI). The latter is the information perceived by the subject regarding the trinity or the form information is perceived by the subject about the trinity of the form (syntactic information), content/meaning (semantic information), and utility/value (pragmatic information) concerning OI (Bughin 2017). Unlike the traditional concept of information proposed by Claude Shannon, EI comprises the trinity of the form, content/meaning, and utility/value and is the basis of learning. This is why EI is also often called comprehensive information.

On the other hand, the essential function of perception is to convert OI to EI. This is the first class of information conversion in AI. The main function of cognition technology is to convert EI, which the subject from OI perceives, into the object's corresponding knowledge. This is the second class of information conversion needed in AI. The only possible approach to convert EI to knowledge must be learning – there is no other way.

Thirdly, in decision-making EI converts to intelligent strategy (IS) based on knowledge support and is directed by problem-solving. The strategy is just the procedural guidance for problem-solving. This is the third class of information conversion in AI. The radical function of decision-making technology is learning to find the optimal solution for a given problem. There are usually several ways of achieving the designated goal from a starting point expressed by EI. A decision should be made through intelligent use, via learning, of the relevant knowledge provided.

In strategy execution, the technology is used to convert the IS into intelligent action (IA) to solve it. In strategy optimization, there are often errors when intelligent action is applied because of various non-ideal factors in all sub-processes. These errors are regarded as new information and are fed back to the input of the model's perception. With this new information, knowledge can be improved via learning, and the strategy can be optimized. Such an optimization process might continue many times until the error is sufficiently small. In sum, all the AI technologies hereto mentioned are learning-based, which is why AI is so powerful.

While trying to simplify AI, it is the scientific branch that assists machines to find solutions to complex problems in a human-like fashion. For instance, it involves borrowing human intelligence characteristics and applying them to algorithms in a computer-friendly way. AI solutions will depend on the flexibility or the requirements needed, ultimately influencing how artificial and intelligent behavior is manifested.

While attempting to achieve a successful AI transformation, similar elements need to be found in excellent digital and analytic transformations. These include concepts of sources of value, data ecosystems, techniques and tools, workflow integration, and open culture and organization. Firstly, in value sources, AI and IoT need to articulate business needs and create business cases. Secondly, data ecosystems involve breaking down data silos, deciding on the degree of aggregation and pre-assessment, and identifying high-value data. When it comes to AI tools, there needs to be the acquisition to plug capability gaps by assuming a "test and learn" approach.

On the other hand, in workflow integration, businesses or companies need to optimize the human/machine interface. Lastly, in open culture and organization, managers using IoT and AI should adopt an open-collaborative culture and establish trust in all the insights. Moreover, reskilling the personnel is necessary for ensuring complementarity.

The contemporary trends of AI research encompass key systems and various application areas. Firstly, the organization should embrace the concept of large-scale machine learning, which involves the creation and learning of algorithms. Nevertheless, it involves scaling the existing algorithms and managing extremely large data sets. Secondly, robotic utilization currently revolves around how robots can be trained to communicate with the world in generalizable and predictable ways. Robotics also deals with how to manipulate objects in interactive environments as well as interacting with people. According to Buchanan (2005), robotic development will depend on commensurate advances, which enhance the reliability and generality of computer vision and other types of machine perception. Moreover, computer vision has been the most important way of machine perception. It has greatly changed AI in that machines can now do some vision commands better than human beings.

In conclusion, AI means the simulation of logical human thinking using computer technology. AI technologies include perception, cognition, decision-making, strategy execution, and strategy optimization. The technology of perception is used to acquire the ontological information about the objects or problem within the environment. Therefore, the combination of AI and IoT will improve smart industries, ranging from health, education, infrastructure, education, transport, public service, and work.

AI goes past straightforward tedious assignments and into how data can be "acquired, put away, controlled, expanded, utilized, and transmitted" (Sloman 2010). This innovation's human-like profundity is rendering it to be appropriate in more than one or two ways. AI is being utilized in healing centers, cars, and industrial facilities. In reality, technology peculiarity, a term that has been coined more as of late, presents the prospect of super insights. In other words, innovation peculiarity implies coming to the point of refinement that dumbfounds human comprehension.

AI has a huge amount of capacity. Since it imitates people's insights and capabilities, they perform the same wide run of capacities a bit like them. With progress in innovation, calculations, and sheer compute control, it is presently advantageous to utilize AI strategies in regular applications within transportation, healthcare, gaming, efficiency, and media (Khatri et al. 2018). Many are recognizable as voice-based associates such as Apple's Siri and Amazon's Alexa that are "focused on brief, task-oriented intelligence, such as playing music or replying to basic topics" (Khatri et al. 2018). This AI shape essentially helps people exclude the exertion that comes with basic errands like checking the climate or making a phone call. It acts as an individual collaborator and companion to those who claim one by replying to vocalized themes. This shape of counterfeit insights has taken off over a long time, with the foremost recent release appearing within the third quarter of 2018 alone, when 19.7 million units of savvy speakers were shipped, in comparison to the 8.3 million transported within the third quarter of 2017.

Another huge advance of this technology in circulation as of late is mechanized cars. These vehicles do not require human interaction to move from one goal to another. A few Tesla cars have an autopilot highlight in which they can "regulate speed, alter paths, and stop without driver assistance" (Matousek 2018). Fake insights like this would modify transportation significantly. In connection with the therapeutic community, numerous instruments have emerged to help perform assignments that in the past people would have done. One case of this technology is hazard appraisal and decision-support devices. These apparatuses utilize scientific equations to use chronicled and factual information, such as national claims databases, medicine sedation databases, and risk-tolerance devices. Usually, an example of an innovation that helps those within the therapeutic field makes choices that are best for their patients.

The rise of innovations concerning surgery performance can supply more solid work than human specialists, increasing the successful rate for surgeries where this innovation is used. In expansion to surgeries and chance appraisals, counterfeit insights can act remedially for patients. For example, automated pets have been utilized to treat elderly patients diagnosed with dementia. They are programmed to memorize how to act unexpectedly with each quiet time through positive and negative inputs from the patients (Etzioni and Etzioni 2018). Understanding input to alter behavior could be a human-like capacity; fake insights have occurred and seem to offer assistance to patients with other diagnoses as they might feel a more comfortable connection without human nearness. In the exterior of the therapeutic world, it is pertinent to look at manufactured insights and protect missions.

Here calculations are utilized to overview the ethereal film of catastrophe zones to recognize rapidly where individuals are likely to be stranded (Etzioni and Etzioni 2018). Utilizing AI here gives casualties the next chance of being found. There are intelligent cameras, facial acknowledgment, and dreams for gadgets that can react to circumstances in order to list advanced illustrations of developing applications. There are numerous applications of counterfeit insights, but there remains much room for advancement. The innovation included in this range has boundless potential.

AI appears to complement the work of people, even though they state there is no denying that in a few businesses, economies, and parts – particularly those that include monotonous assignments – employment will alter or be eliminated. To supply a more particular piece of information, it was evaluated that in the over 29 nations analyzed, the share of employment at the potential hazard of robotization would be 1% by 2020. From a more financial point of view, the joined together States have been losing dominance in AI new companies to China, which plans to become a world pioneer of manufactured insights by

2030. More particularly, the US had 77% of value bargain offers in 2013 compared with the more minuscule 50% in 2017 (Chaturvedi 2018). Although still a strong sum, the Chinese advancement of AI appears to be overtaking US endeavors. The spar over AI may be a future slant that is likely to proceed over its advancement, as the potential of this innovation is boundless.

Innovation companies such as Amazon, Microsoft, and Letter set have all started to contribute new businesses in manufactured insights in an effort to progress computer security. Also, Palo Alto Systems, Fortinet, and Cisco Frameworks are all within the race to develop AI instruments. This can be since counterfeit insights have become a prevalent usage in cybersecurity items, which includes protective layers. In his proficient conclusion, Eric Jang states that he accepts profound intellect to be the number one company to investigate counterfeit insights, taken after by Google, Facebook, Open AI, and Baidu. The planned capabilities of fake insights have been recognized by numerous companies and are still being executed by more. A Story Science study found 84% of undertakings will be utilizing AI by the end of the decade (TATA 2017).

The run of manufactured insights that capacities can perform is exceedingly valuable for companies in all sorts of businesses. The case of mechanization innovation is not as it was being actualized by Tesla but is now also by Uber, Volkswagen, Lyft, and Waymo. Tesla happens to be actualizing an autopilot highlight with 360 visions that can see 250 m away. JPMorgan Chase, the biggest bank within the Joined together States, has executed a few AI-powered services for its clients, counting on the utilization of AI calculations to assist speculators in making superior venture and exchange choices. The capacity of AI to make exact human-like choices depicts the innovation as being exceedingly invaluable for companies to execute. Other companies that utilize AI are Affectiva, Panasonic, and Phillips.

To address the administrative issues encompassing fake insights, the concerns ought to be handled. “With its fast increasing speed, AI makes fear a robot course that will oppress humankind, annihilate it, or cause major financial disruptions” (Etzioni and Etzioni 2018). Even though as created as these machines may be, they have no inner inspiration, so typically not a concern. Other issues such as cyber assaults and work substitution that stem from human want make a requirement for direction. There are numerous concerns when it comes to the utilization of AI. A few of these, particularly concerning the criminal equity framework, are recorded by Delgado: “Does the government’s utilization of AI require a warrant to look at your online information? Can AI be utilized to tune in on American citizens’ phone calls without a warrant?”

Indeed, bias can be a potential concern for using AI within the criminal equity framework, as Delgado discussed in a case in 2016. A program was utilized to anticipate recidivism of individuals qualified for parole was found to be one-sided against African Americans. One-sided calculations demonstrate AI ought not to be a sole reliance in performing assignments. Elon Musk, the author of Tesla, tweeted, “We ought to be super cautious with AI. Possibly more dangerous than nukes. I’m progressively slanted to think there ought to be a few administrative oversights, possibly at the national and universal level” (Etzioni and Etzioni 2018). Even though Musk’s company, Tesla, is working with counterfeit insights, he still recognizes the innovation’s obscure capabilities. The direction is required; in any case, and there is an issue concerning taking a cost toll.

AI's direction is likely to regurgitate wrangles between nations with diverse suppositions on the worldwide level. In any case, a direction like this could happen, as shown by the recent panic comparable to the Cold War. Controls on a national level, be that as it may, are as of now input in a few nations. "The General Data Protection Regulation (GDPR) being actualized in Europe put extreme confinements on the use of fake insights and machine learning," particularly any robotized choices that "significantly affect" EU citizens. Controls like this ought to be executed all-inclusively to secure person rights and avoid any potential dangers.

AI has numerous worldwide suggestions. Manufactured insights empower individuals to re-examine how we coordinate data, analyze information, and utilize the emergence of bits of knowledge to progress decision-making. Alone, this innovation has the plausibility of altering how individuals think and make choices. It is not as it was, but efficiency is protected when counterfeit insights are permitted to require over-thoughtless assignments such as thoughtless driving. Moreover, it may decrease the fetched people of transportation, as transport and taxi drivers will not be required. In any case, by making straightforward assignments an unimportant career, numerous will be unemployed and incapable of getting work in other careers due to constrained work positions and immaterial foundation. Delgado moreover states that advertisements will end up being more brilliant and more implanted into our day-by-day lives. By analyzing the way people associate with advertisements based on their offer, AI can make choices on how to promote in a more profitable and viable way.

As AI becomes dynamically progressed, owing much to advances in computing control, data analysts' instruction, and the openness of machine learning rebellious for making advanced calculations, the Web of Things is getting closer to becoming an essential stream wonder. 5G speaks to the misplaced component to bring this progress to unused levels and to enable the brilliant network vision. The ultra-fast and ultra-low delay given by 5G frameworks, combined with the tremendous entirety of data collected by the Web of Things and the contextualization and decision-making capabilities of machine learning made experiences, will engage advanced transformational capabilities in each industry division, conceivably changing our society and the way we live and work.

14.4 5G Network

5G is called 5G because it is the fifth generation of wireless technology. The primary era was first generation (1G) when analog cell phones, to begin with, entered the world. Second generation (2G) came along when modern highlights such as content informing and voicemail were made. Not long after, higher information exchange rates permitted portable web browsing, picture sharing, and GPS area following, called third generation (3G). By the time fourth generation (4G) came along, individuals could do nearly anything on their smartphones. Figure 14.1 shows the evolution path of wireless mobile generations.

5G is one of the speediest, most affluent innovations the world has ever seen and experienced. 5G has faster downloads and an extraordinary arrangement of unwavering quality, which contains a theatrical, outstanding effect on how the world lives, works, and plays. The network advantage of 5G makes businesses more effective.

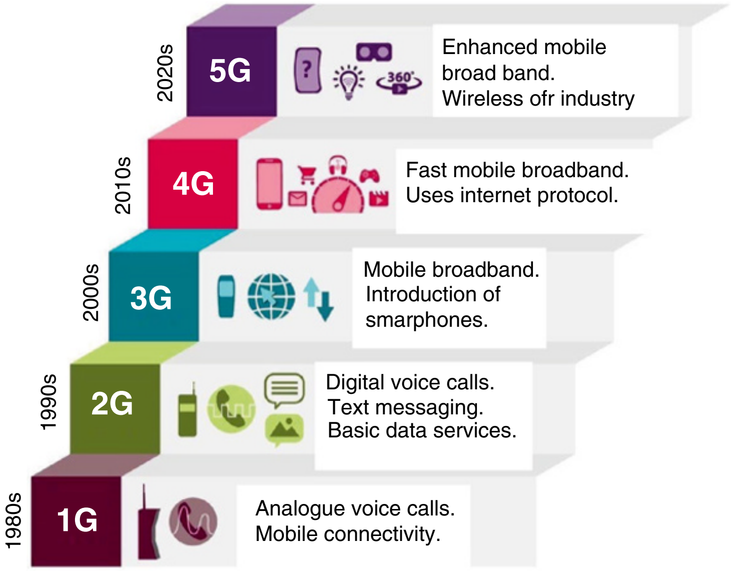
2020s
5G
Enhanced mobile broad band. Wireless ofr industry
2010s
4G
Fast mobile broadband. Uses internet protocol.
2000s
3G
Mobile broadband. Introduction of smarphones.
1990s
2G
Digital voice calls. Text messaging. Basic data services.
1980s
1G
Analogue voice calls. Mobile connectivity.

Figure 14.1 Evolution of wireless mobile systems (Katrodiya 2019).

5G systems utilize a framework of cell locales that partition their region into distinctive areas and send encoded information through radio waves. Each cell location has to be associated with an arranged spine, in any case, on the off chance that it is through a wired or remote association. Orthogonal Frequency Division Multiplexing (OFDM) is the sort of coding utilized for 5G. Even though it is comparative to the encoding that Fourth Generation Long-Term Evolution (4G LTE) employs, it is outlined for much less idleness and a much higher adaptability than Long-Term Evolution (LTE).

The objective for 5G is to have higher speeds and distant higher capacity per segment than 4G. The objective is additionally to have much lower idleness than 4G. 5G systems are much more intelligent than the past frameworks. They will boost capacity by four times over current frameworks by leveraging more extensive transfer speeds and will progress radio wave advances.

5G is coming, advertising an enormous boost in transmission capacity that will supply customers with fake insights and more spilling recordings. Even though there are numerous needs to involve the modern arrangement, it is more than likely that the normal buyer will not manage a 5G association. Certain companies, such as Verizon Remote, reported that they would have the primary real mobile 5G benefit within the Joined together States and would be called the 5G Ultra-Wideband. Verizon dispatched its services nationwide in 2021 (Alleven 2021).

The 5G Ultra-Wideband will, as it were, dispatch in select ranges within Chicago and Minneapolis cities. Concurring to Verizon, there will, as it were, be a $10 add-on charge. There will moreover be no additional charges for the primary three months. Even though the 5G comes with awesome highlights, it will be costly.

5G technology will result in awesome changes for customers and endeavors over the country. It will enable companies to form progressions such as being more astute, much better associated cars, progressions in therapeutic innovations, and move forward retail encounters through personalization. 5G will employ radio frequencies that are higher and more directional than the ones utilized by 4G. The directionality of 5G is exceptionally critical since, if towers were to send information everywhere, there would be an awesome sum of squandered control and vitality. It would also debilitate web access.

Since 5G employs shorter wavelengths than 4G, radio wires can be shorter without an interferometer with the wavelengths. As a result of wavelengths being shorter, 5G can back roughly 100 gadgets per meter more than 4G. 5G systems can get the information being requested and self-modulate the control mode, making gadgets more inviting.

5G employs one-of-a-kind radio frequencies that are higher and more directional than those utilized by 4G. The directionality of 5G is exceptionally vital since 4G towers send information everywhere. Since 4G does this, both control and vitality can be squandered and can eventually debilitate the web. The higher the recurrence, the more prominent is its capacity to bolster quick information without interference with other remote signals or to be excessively cluttered.

In expansion to higher frequencies than 4G, 5G will employ shorter wavelengths than 4G. Shorter wavelengths mean that receiving wires can be shorter without an interferometer with the heading of the wavelengths. More information will reach more individuals with less inactivity and disturbance to meet surging information requests. 5G systems can get the information better by being asked to self-modulate the control mode, making gadgets more user-friendly.

Video sharing skyrocketed with the entry of 4G and will heighten overall apps and administrations when 5G arrives. The Contract Manufacturing Organization (CMO) of the cellular supplier AT and T, Moment Katibeh, says that within the not-too-distant future, mirrors may well be supplanted with tall determination screens with cameras that permit individuals to attempt to try on handfuls of combinations of clothing. Moreover, independent cars may utilize live maps for the real-time route, vital to their adequacy. It seems moreover to dispense with a few of the issues that are now experienced with driving cars.

Figure 14.2 shows the requirements and different sets of enabling technologies to meet high throughput, less than a millisecond delay, and higher capacity.

Even though 5G systems come with parts of focal points, there are numerous drawbacks. Greater high-quality applications and user experience demands more transfer speeds than ever experienced recently. 5G systems are introduced to utilize the transmission capacity of amazingly high-frequency millimeter waves that travel for a very short distance. Because of this, they do not travel and penetrate well through buildings. They moreover tend to be ingested by rain and plants and in the long run drive into obstructions and decay.

The unimaginable modern organization brings to the world numerous health concerns. In 2011, the World Health Organization's Worldwide Office for Investigations on Cancer found that cell phones might lead to the creation of brain tumors since they utilize radio frequency radiation, known as RFR. RFR leads to an arrangement of other health issues, such as breaking the DNA strands, the disturbance of the cell digestion system, melatonin, disturbance of the brain glucose digestion system, and the era of stretch proteins.

Microwave radiation is exceptionally destructive to human skin. More than 90% of microwave radiation is ingested by the epidermis and dermis layers, so human skin essentially wipes for it. Moreover, human sweat channels within the skin's upper layer act as

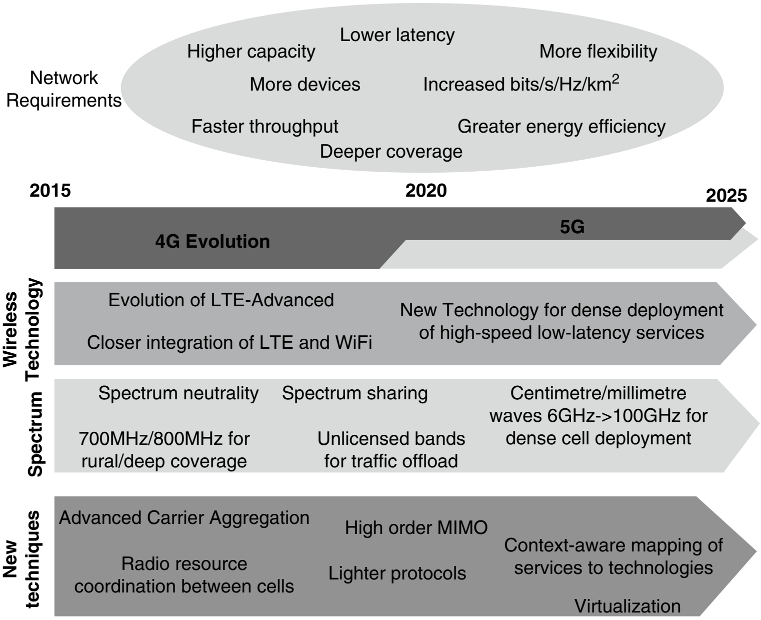
Network Requirements
Lower latency
Higher capacity
More flexibility
More devices
Increased bits/s/Hz/km^2
Faster throughput
Greater energy efficiency
Deeper coverage
2015
2020
2025
4G Evolution
5G
Wireless Technology
Evolution of LTE-Advanced
Closer integration of LTE and WiFi
New Technology for dense deployment of high-speed low-latency services
Spectrum
Spectrum neutrality
Spectrum sharing
Centimetre/millimetre waves 6GHz->100GHz for dense cell deployment
700MHz/800MHz for rural/deep coverage
Unlicensed bands for traffic offload
New techniques
Advanced Carrier Aggregation
High order MIMO
Context-aware mapping of services to technologies
Radio resource coordination between cells
Lighter protocols
Virtualization

Figure 14.2 Evolution to wireless 5G (El-Hassani et al. 2019).

helical radio wires. Helical radio wires are extraordinary radio wires that particularly react to electromagnetic areas. Since people have millions of sweat channels, our bodies will be exceptionally conductive to microwave radiation.

Rather as radiation hurts people, it moreover could have genuine health dangers for creatures. A Joined Together States Toxicology Program found that male rats exposed to radio frequency radiation create uncommon shapes of tumors within the brain and heart. It moreover demonstrated that rats of both sexes developed DNA harm. Analysts felt that the discoveries of dangers to rats could relate to people. The broad increment in cell phone utilization could lead to a noteworthy effect on people.

In another creature investigation, it was demonstrated that microwave radiation could harm the eyes and a safe framework. Moreover, it appeared that it influences the cell development rate and bacterial resistance. A test conducted at the Kanazawa Therapeutic College found that 60 GHz millimeter-wave receiving wires have a chance of creating warm wounds and rabbit eyes. Warm impacts can also reach underneath the eye's surface. It was also found that introducing versatile phone electromagnetic recurrence caused chickens to develop life retinal cells that separated.

Similarly exasperating, 5G innovation moreover puts the environment's health at risk in numerous diverse ways. Millimeter waves pose a genuine danger to plant health. In 2010, it was found that aspen seedlings exposed to radio frequency radiation displayed indications of rot, which debilitates plants and makes them more susceptible to infections and bugs.

Armenian scientists found that low-intensity millimeter waves caused a push reaction that harms cells in wheat shoots. Even though plant harm is lethal for the planet, it is terrible for people. When plants become sullied, that puts the human nourishment supply at hazard levels, which might inevitably kill people.

In addition to the harming of plants, 5G innovation also poses a risk to the Earth's environment. The usage of 5G will require May satellites that will be conveyed by suborbital rockets. Hydrocarbon rocket motors will impel the suborbital rockets. Propelling as well numerous suborbital rockets will discharge parcels of dark carbon into the air, in the long run contaminating worldwide air conditions and influencing dispersion of ozone and temperature. To form things more harmful still, solid-state rockets produce debilitating substances such as chlorine, which is an ozone-destroying chemical.

5G systems moreover debilitate normal environments. A few reports appear that low-level, non-ionizing microwave radiation have influenced the health of both fowls and bees over the last two decades. It drives winged creatures to leave their nests, conjointly causes crest weakening, motion issues, diminished survivorship, and death. Bee populaces suffer from decreased egg-laying capacities of ruler bees. Some individuals feel that 5G systems are terrible news for all living life forms and the planet that they are living on.

Completely mindful of the issues that 5G brings to the environment, corporations continue to keep their positive states of mind around the jaw-dropping, engaging innovation. The most reasons that business people are proceeding with their thoughts of 5G is the incredible amount of cash that it will bring in. Since companies make 5G seem engaging, business visionaries essentially have mind-control over the customers.

There are numerous ways that communities can come together to ensure themselves against the threats of 5G. Denying utilizing 5G phones, denying purchasing "smart" apparatuses, abstaining from buying shrewd meters, avoiding tall levels of 5G radiations in homes, and restricting introduction to radiation are ways to protect themselves and their families.

5G systems will be based on engineering that will produce an unused mechanical and venture advancements environment. The 5G design will bolster thousands of modern applications within the buyer and trade areas. These shopper and commerce areas incorporate vertical markets such as fabricating, vitality, healthcare, and automobiles.

The 5G design comprises numerous distinctive things that many individuals may know nothing about. The 5G organize layer will utilize level IP concepts so that diverse Radio Access Networks (RANs) or Radio Get-to Systems utilize the same single Nanocore for communication. Many recognizable RANs that are bolstered by 5G engineering are LTE, LTE-advanced, and WiFi.

Like progressive design where ordinary IP addresses are utilized, it has level IP engineering recognized gadgets by utilizing typical names. In this way, the number of organizing components in information is decreased, and costs are incredibly decreased. Inactivity is additionally minimized.

Another component of the 5G design is the aggregator. The aggregator totals all of the RAN traffic and courses them to the portal. 5G portable terminal houses diverse interfacing to supply back all the range in order to get to remote innovations.

Nanocore is additionally a component of the 5G design. It comprises nanotechnology, cloud computing, and all IP designs. In expansion to Nanocore, cloud computing moreover plays a tremendous part within the design of 5G. Cloud computing utilizes the internet and inaccessible central servers to preserve the clients' information and applications. It permits shoppers to utilize applications without any establishment and get to their records from any computer worldwide using the web.

Near the 5G organize engineering layer, there is a 5G convention stack. The convention stack comprises the OWA (Open Wireless Architecture) layer, the organize layer, the open transport layer, and the application layer. All of these layers are exceptionally diverse in numerous ways.

The OWA layer, or the Open Remote Design layer, is a physical layer and data-link layer of the convention stack. The arrange layer is utilized to course information from the source IP gadgets to the goal IP gadgets. It is partitioned into two layers, the upper and the lower arrange layers. Next, there is the open transport layer. The open transport layer combines the usefulness of both transport layers and session layers. Last, there is the application layer. The application layer marks information as per the appropriate organization required. It moreover does encryption and unscrambling of data. The application layer chooses the most excellent remote association for a given service.

The rising of the 5G organize layer is nearly here. By the conclusion of the year, it will be in full impact. Even though companies appear to have it all figured out, there will be parcels of challenges and necessities for the 5G organize layer to be as effective as arranged. Moreover, business visionaries ought to put into thought how hurtful the materials of 5G are. People, creatures, plants, and indeed the environment are influenced by millimeter waves utilized for the working of 5G. Although 5G is preparing to come, there are numerous things to think about. Everything that sounds and looks great is not always good for individuals. Figure 14.3 depicts how small technologies such as Multiple-Input Multiple-Output (MIMO), densification, spectrum aggregation, and farming help to enhance higher capacity and higher throughput.

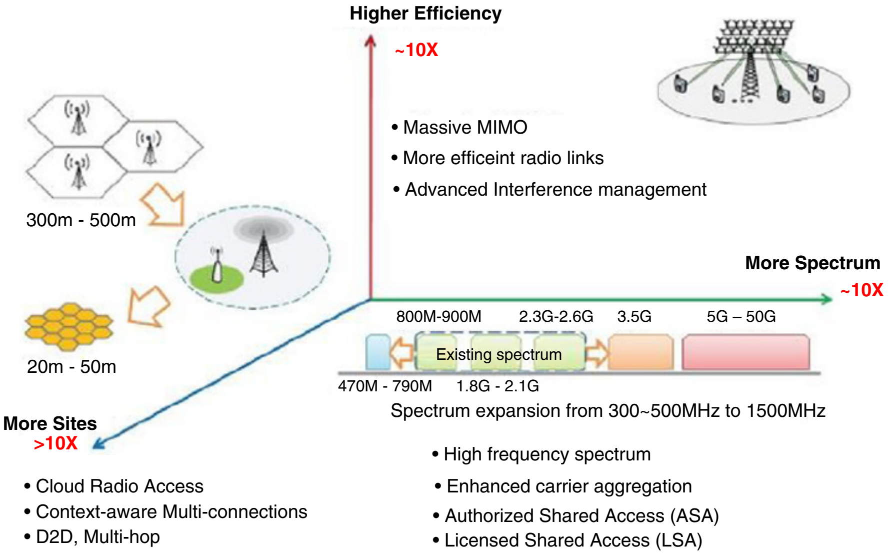
Higher Efficiency
~10X
• Massive MIMO
• More efficeint radio links
• Advanced Interference management
300m - 500m
20m - 50m
More Spectrum
~10X
800M-900M
2.3G-2.6G
3.5G
5G – 50G
Existing spectrum
470M - 790M
1.8G - 2.1G
Spectrum expansion from 300~500MHz to 1500MHz
More Sites
>10X
• High frequency spectrum
• Enhanced carrier aggregation
• Authorized Shared Access (ASA)
• Licensed Shared Access (LSA)
• Cloud Radio Access
• Context-aware Multi-connections
• D2D, Multi-hop

Figure 14.3 A breakthrough in three dimensions (El-Hassani et al. 2019).

14.5 Emerging Partnership of Artificial Intelligence, IoT, 5G, and Cybersecurity

Operations are revolutionized by information technology through smart connected products, which help in device miniaturization and processing power and wireless connectivity. Smart connected products provide greater reliability, expanding opportunities, much high utilization of the product, and its capabilities of transcending traditional products. It involves strategic choices of creating and capturing products, newly generated data, and relationships with conventional business partners. The new technology stack includes identifying and securing the product cloud layers, the external source of information, integration with a business system, interrelated connectivity, and form a product cloud. The product cloud involves smart product applications, rules or analytical engines, and its platform of the application and product data database.

AI works by developing new algorithms and models based on machine learning. Traditionally, AI was about creating human-like systems that can reason and do things like the human brain. AI can be further understood as narrow AI or general AI. Narrow AI, the intelligence that human beings interact with daily, is the intelligence that has been designed to carry out specific functions that surround a particular domain, for example, the translation of one language to another. On the other hand, general AI is hypothetical and does not work in a specific domain. This means that general AI can work in several areas by earning and performing different tasks differently. Both current and previous AI developments have led AI technology to be used diversely in various applications and avenues while simultaneously enhancing the scope of AI and the efficiency, as well as the impact of its different forms. Various applications of AI range from Machine Learning, Deep Learning, Automation, and Autonomy, to Human–Machine Teaming. The implementation of AI through the IoT in different sectors of human life will significantly impact business and job employment.

AI, 5G, and IoT advances are now enhancing each other, making the fifth wave of computing.

There have been some significant developments in Cybersecurity. One of the significant developments in the techniques and tools that are redeveloped is through the support of AI and Machine Learning (ML). With this partnership between AI and Cybersecurity, the current and future application possibilities for Cybersecurity are endless. The detection of threats is one of the significant concerns in Cybersecurity and has emphasized it substantially. Officials, authorities, and organizations have always been keen on developing newer and more advanced ways to detect a potential threat or to be prepared for any advanced threat and attack that can take place. Machine learning has played a vital role in this aspect of Cybersecurity and strengthened the overall relationship. It has provided effective approaches and outcomes in terms of threat detection in Cybersecurity and has been instrumental in detecting threats by analyzing data and identifying threats in the initial stages.

Each year, cyberattacks have been on the rise and are getting worse than their impacts in previous years. The sharp increase of cyberattacks has resulted in more and more security threats and made it complex due to AI's evolution in cyberattacks or the AI of the attackers. As a result, more sophisticated cyberattacks that are more complex than ever are taking place, which is one of the most significant challenges in AI and its implementation and usage in Cybersecurity despite all the promises it has fulfilled and will deliver.

14.5.1 The Current State of IoT Security

The subject that ought to be investigated is the current state of IoT security. The IoT has been developing at a fast rate as vehicles, computer programs, and wearable gadgets have progressed past the fundamental work. According to Ammar, Russello, and Crispo (2018), more than 3.7 billion devices are utilized on day-by-day premises with web associations. As a result, there is a desire for more activity and information on the congested associated web. Considering the development in IoT, it is critical to address the issues related to IoT security. The issues included can incorporate an increment in assaults, subsequently settling the issues to upgrade the IoT security level. The growth within the IoT sensors' entrance and heterogeneous smart gadgets requires a basic requirement for IoT administration arrangements that are dependable in terms of control and setup. Replying to the investigated subject will offer assistance in making organizations mindful of the measures they can take to boost IoT security. Numerous organizations are likely to put fitting measures input to boost the security of their IoT. This section investigates the current state of IoT security to create ways of upgrading the security level.

Ammar, Russello, and Crispo (2018) conducted an investigation that uncovered the fact that organizations need to introduce security frameworks to enhance IoT security. The creators contended that there is a requirement for IoT security due to the expanded utilization of internet-supported gadgets. Concurring to the creators, operations are becoming robotized in numerous organizations to upgrade effectiveness. As a result, web security concerns are expanding as numerous aggressors are focusing on organizational information. The IoT innovations are getting to be assorted due to the expanded network required to convert operations into numerous businesses, like framework, well-being, and funds. IoT security dangers increment as unused gadgets are presented on the web. The IoT security breaches that are now taking place are an indication that there is a requirement for IoT security.

The IoT has driven emotional changes within organizations' operations and the lives of individuals. As a result, numerous organizations are grasping rising innovations. A few firms have discovered that they are powerless due to the expanded number of programmers utilizing advances to hinder operations. Numerous huge firms are receiving IoT frameworks as they offer assistance in improving forms through progressed information analytics. Agreeing with Ammar, Russello, and Crispo (2018), the organizations receiving the IoT frameworks need to be mindful of the possible threats and misfortune that they could have in their systems if they are disturbed by programmers. This source is important to the investigation because it gives the arrangements that can be made to improve IoT security in organizations. It contributes to replying to the question about the theme by clarifying how security frameworks like firewalls can offer assistance in disposing of or minimizing the vulnerabilities of the IoT frameworks. From this source, we learned that the IT office plays a pivotal part in upgrading the IoT security.

Lee and Lee (2015) found that shopper mindfulness is pivotal in upgrading IoT security in organizations. Concurring with the creators, most organizations found that involvement with IoT security breaches can dodge such breaches through expanded buyer mindfulness. This may involve making sure beyond any doubt that the clients of IoT frameworks are mindful of the conceivable aggressors, and subsequently making them take the essential safeguards. One of the IoT security breaches that this source can be connected to is Cisco Talos. The security analysts revealed a botnet connected to Russia. These IoT breaches influenced more than 500 000 organizations to get to capacity gadgets and switches in Ukraine, consequently recommending a few political inspirations. The Virtual Private Network (VPN) Channel is the malware that made the takeover conceivable by allowing the programmers to control the tainted gadgets. The control included the chance to turn the tainted gadgets off and in this way taking them offline.

The IoT security breach is driven by the disease of numerous gadgets recommending the need for mindfulness among the buyers on securing the savvy situations. According to Lee and Lee (2015), shopper mindfulness might have made a difference in maintaining a strategic distance from the IoT security breach as the clients may be more cautious. This source is important since it gives a technique that organizations can utilize to minimize their IoT framework vulnerabilities. It may have made a difference in anticipating the IoT security breach by guaranteeing that the clients are mindful of conceivable assailants. Moreover, the source makes a difference in making Cisco Talos develop ways of arranging security that makes it clear that it is, without doubt, a necessary item. We learned from this source that locks in partners within the preparation of upgrading IoT system security are among the finest techniques that can help diminish vulnerabilities.

The study conducted by Nowodzinski, Łukasik, and Puto (2016) uncovered that encryption and verification are vital in improving IoT security. Agreeing with the creators, organizations ought to learn how to apply innovations to boost their arranged framework security. This is often true since programmers are grasping mechanical progressions in assaulting systems. This source seems to have made a difference in avoiding IoT security breaches that included Threat care and IBM, where security analysts distinguished around 17 vulnerabilities from the four keen cities. Rudimentary streams within the security plans, just like the utilization of default passwords, permitted entry to the frameworks, and having systems that were unsecured online was the lion's share of most of the vulnerabilities.

There were concerns after encryption issues and verification blemishes were found within the illustration's server communication frameworks. Concurring to Nowodzinski, Łukasik, and Puto (2016), verification and encryption are among the significant technologies within the avoidance of IoT security breaches. The IoT security breach made clients and merchants of the IoT systems realize the security challenges, particularly within the basic IT foundation. This source is important to the inquiry about points since it gives a few ways organizations can improve IoT security. Concurring to the creators controlling the way to get to the company's organized frameworks is vital in upgrading IoT security. From this source, we learned that the physical way is imperative in improving the security of arranging frameworks.

Addo et al. (2014) ponder whether judgment and confirmation are basic in making strides for IoT security. Confirmation makes a difference in making beyond any doubt that aggressors cannot get to an organization's frameworks. This source can be connected in fathoming the third IoT security breach that included Tesla, the electric car makers. Despite the basic security imperfections in Tesla, it was found that Show S-cars were powerless to key dandy assaults. Key coxcomb assaults are methods utilized within the preparation of taking high-end cars. The KU Leuven College group in Belgium cloned the Show S keys coxcomb and utilized it in the opening. The analysts utilized hardware worth $600 to examine radio and compute signals within the controlling part of learning the vehicle's identifier transmitted by the car.

As a result, the group may trigger the reaction from key parts by mimicking the performance of the cars. The analysts utilize reaction sets to narrow down real keys that may be utilized. As stated by Addo et al. (2014), the IoT breach may be anticipated by implementing tight confirmation frameworks within the electric car. This source is significant since it gives techniques that can be utilized by organizations within the procedure of boosting their IoT security frameworks. From this source, we learned that numerous IoT breaches could be related to destitute confirmation frameworks in organizations, making it simple for aggressors to get to vital frameworks.

Patel and Patel (2016) considered that coordination of human understanding and innovation is vital in upgrading IoT security. Agreeing to the creators, organizations must guarantee that the clients of the frameworks and systems have a legitimate understanding when applying fundamental security measures. This source is pertinent to the inquiry point since it prescribes the measures that organizations can grasp to improve IoT security. For example, fortifying the creators' security culture among the representatives is vital in minimizing vulnerabilities. It is through creating a security culture in an organization that the security of IoT can be moved forward. As a result, this source can help organizations to relieve the dangers of assaults confronting IoT frameworks. This illustrates the need for representatives to be enlightened on methods assailants use as they utilize developing advances.

According to Ammar, Russello, and Crispo (2018), the utilization of security programs can offer assistance within the anticipation of aggressors by denying access to systems and frameworks. This source can help arrange our investigation point because it suggests establishing firewalls and patches to deny unauthorized individuals. For instance, within the IoT security breach, including Cisco Talos, malware played a basic part in permitting the programmers to compromise information security. This included snooping on the activity that passed through influenced switches. This is intended to harm the company's notoriety as clients will question the security measures taken within the company. The circumstance was genuine to a point where the FBI had to intercede. The mediation included empowering the switch's proprietors to reboot the gadgets, utilize a security computer program, and introduce patches. The FBI declared that it was intended to seize the space that was utilized in supporting the botnet. This source might have made a difference in avoiding the IoT security breach as the creators investigated the ways organizations can upgrade IoT security by denying access.

Lee and Lee (2015) contended that mindfulness among the representatives in an organization is pivotal in upgrading IoT security. This source can offer assistance in replying to our investigation theme by presenting measures that should be put in place to boost IoT security frameworks. Nowodzinski, Łukasik, and Puto (2016) contended that confirmation and encryption by organizations are vital in guaranteeing that systems and frameworks are secure. As a result, this source can offer assistance in replying to the investigation point by clarifying how confirmation can be utilized to progress IoT security. As an illustration, within the IoT security breach, Tesla's dependence on a 40-bit figure that was effectively crackable and non-appearance of shared confirmation made key coxcomb innovation of the electric car go astray. The company incurred extra costs that influenced the productivity and image of the company within the industry. Tesla rolled out cryptography that was stronger for the key coxcomb framework utilized by Demonstrate S-cars.

Patel and Patel (2016) contended that innovations need to be coordinated with human understanding. The advances are changing at a fast rate, consequently expanding the plausibility of the need for information essential in understanding the developing security dangers posed by web utilization. This source can help in replying to enquiries about the theme by advising individuals how to find out about dangers that are likely to compromise IoT security.

14.6 Conclusion

In the coming years, AI will meet IoT at the edge of the computing layer. It is believed that many models that are trained in the public cloud could be deployed at the edge. At the top, there is industrial IoT for AI that will perform outlier detection, the main reason analysis, and the precaution maintenance of the equipment. Advanced machine learning models that are developed based on neural networks can be optimized at the edge. They will have the capability to deal with time-series data, unstructured data, and video frames, as well as devices such as sensors, mics, and cameras. IoT will be the most important driver of AI. All the edge devices will have special AI chips equipped with an ASIC (Application Specific Integrated Circuit) and an FPGA (Field-Programmable Gate Array). The following applications will be in operation:

1) Interoperability in neural networks. Selecting a suitable framework is very necessary for developing neural networks. There is a need to select the right tool from different choices, including Tensor Flow, MXNet, PyTorch, Caffe2, and MS Cognitive. Another challenge is that when a model is evaluated in one framework, it is very difficult to place it in another. Low interpretability in the neural network toolkits also affects the adoption of AI. Microsoft and Facebook have made a mutual platform to make an Open Neural Network Exchange that has helped reuse the trained neural network models. In the future, the Open Neural Network Exchange will act as an important technology. It will run as a standard runtime for inferencing.
2) Automated machine learning. Soon the facility of Machine Learning (ML) solutions will be changed to AutoML. This will give more power to business analysts to use ML models that can define complex scenarios. This will help the data scientist to proceed further without considering the typical ML model training. They can focus on business problems with AutoML, which requires less attention to workflow and processes. AutoML suits the cognitive ML platforms and APIs. It offers the best customization without the typical workflow. Unlike the typical APIs, which are considered important as black boxes, the AutoML offers the same flexibility and portability.
3) Automation of DevOps. For analytics, searching, and indexing, there are many different applications and complex infrastructures. There are complex, big data sets taken from

the operating system and application that can be examined and combined to locate patterns. Operations go from reactive to predictive when machine learning models are used. When the power of AI is used in operations, it redefines that infrastructure. The usage of machine learning and AI in IT and DevOps will add intelligence to operations. This is more effective because the analysis can be performed quickly as AIOps will be in the mainstream, allowing public cloud vendors to take advantage when AI is converted to DevOps (Janakiram, MSV 2018).

IoT security has been an issue of concern in numerous organizations as modern advances are rising within the market. Organizations have to be mindful of the security dangers confronting IoT and provide fitting measures for anticipating the assaults. It is critical to understand that the aggressors utilize current advances in assaulting the frameworks and systems. The sources discussed above have significantly contributed to the investigation by examining diverse ways to boost IoT security. Organizations ought to make sure, beyond any doubt, that they execute the security techniques they define, locking in the representative preventative measures. All the organizations' partners have to be aware of the security dangers and measures that ought to be taken. The suggestion of this conclusion is to expand mindfulness concerning the dangers of confronting IoT security in organizations.

References

Addo, I.D., Ahamed, S.I., Yau, S.S., and Buduru, A. (2014). A reference architecture for improving security and privacy in the internet of things applications. In: *IEEE International Conference on Mobile Services*, 108–115. IEEE.

Alleven, M. (2021). Verizon launces 5G Ultra Wideband in 3 more markets. *Fierce Wireless*. https://www.fiercewireless.com/operators/verizon-launches-5g-ultra-wideband-3-more-markets (accessed 22 June 2021).

Ammar, M., Russello, G., and Crispo, B. (2018). Internet of Things: A survey on the security of IoT frameworks. *Journal of Information Security and Applications* 38: 8–27.

Buchanan, B.G. (2005). A (very) brief history of Artificial Intelligence. *Computer Science, AI Magazine* 25th Anninversary Issue: 53–60.

Bughin, J. (2017). Ten big lessons learned from Big Data analytics. *Applied Marketing Analytics* 2 (4): 286–295.

Chaturvedi, A. (2018, July 11). Thirteen major Artificial Intelligence trends to watch for in 2018. https://www.geospatialworld.net/blogs/13-artificial-intelligence-trends-2018/ (accessed 22 June 2021).

El Hassani, S., Haidine, A., and Jebbar, H. (2019). Road to 5G key enabling technologies. *Journal of Communications* 14 (11): 1034–1048. http://www.jocm.us/uploadfile/2019/0930/20190930023333103.pdf.

Etzioni, A. and Etzioni, O. (2018, September 20). Should Artificial Intelligence be regulated? https://issues.org/perspective-should-artificial-intelligence-be-regulated (accessed 22 June 2021).

Janakiram, MSV (2018, December 9). Five Artificial Intelligence trends to watch out for in 2019. https://www.forbes.com/sites/janakirammsv/2018/12/09/5-artificial-intelligence-trends-to-watch-out-for-in-2019/#64c39a015618 (accessed 22 June 2021).

Katrodiya, R. (2019). A survey of 6th generation. https://www.researchgate.net/publication/338249511_A_Survey_on_6th_generation_1_st_Renil_Katrodya (accessed 22 June 2021).

Khatri, C., Venkatesh, A., Hedayatnia, B. et al. (2018, Fall). Alexa Prize — State of the Art in Conversational AI. *AI Magazine* 39 (3) https://ashwinram.org/2018/09/28/alexa-prize-state-of-the-art-in-conversational-ai/.

Lee, I. and Lee, K. (2015). The internet of things (IoT): applications, investments, and challenges for enterprises. *Business Horizons* 58 (4): 431–440.

Matousek, M. (2018, January 29). The most impressive things Tesla's cars can do in Autopilot. https://www.businessinsider.com/tesla-autopilot-functions-and-technology-2017-12#tesla-cars-made-since-october-2016-come-with-eight-cameras-that-have-a-complete-360-degree-range-of-vision-around-the-car-each-of-the-cameras-can-see-up-to-250-meters-away-2 (accessed 22 June 2021).

Merriam Webster (2018, October 23). Artificial Intelligence. Artificial Intelligence | Definition of Artificial Intelligence by Merriam-Webster (accessed 22 June 2021).

Nowodzinski, P., Łukasik, K., and Puto, A. (2016). Internet of things (IoT) in a retail environment. The new strategy for a firm's development. *European Scientific Journal* 12 (10).

Patel, K.K. and Patel, S.M. (2016). Internet of Things – IOT: Definition, characteristics, architecture, enabling technologies, application & future challenges. *International Journal of Engineering Science and Computing* 6 (5).

Sloman, A. (2010, April 11). What is Artificial Intelligence? http://www.cs.bham.ac.uk/research/projects/cogaff/misc/whatsai.html (accessed 22 June 2021).

TATA CS (2017). Getting smarter by the day: How AI is elevating the performance of global companies. TCS global study: Part 1. https://www.tcs.com/content/dam/tcs/pdf/Industries/global-trend-studies/ai/TCS-GTS-how-AI-elevating-performance-global-companies.pdf (accessed 22 June 2021).

15

Intelligent Connectivity and Agriculture

15.1 Introduction

Based on a Food and Agriculture Organization survey in 2018, the world population is projected to increase from 7.6 billion in 2018 to over 9.6 billion by 2050 (Biradar 2019). For arable areas, the augmentation forecasts are as low as 5%. The current agricultural output does not sufficiently feed the 7.7 billion world population, leaving approximately 821 million people suffering from hunger. This indicates that agricultural production will have to increase by 70% to compensate for the shortage. This poses significant challenges to the agricultural sector as the demand for natural resources, freshwater, and other foods surge to unprecedented levels (Biradar 2019). However, as modern urbanization and technological disruptions define almost every sphere of life, the fusion of Artificial Intelligence (AI), the Internet of Things (IoT), LTE, and fifth generation (5G) technologies are expected to spearhead the fourth industrial revolution. This potentially provides a solution that will shape future cultivation.

The implications of smart and efficient farming techniques on food production patterns will inevitably improve yield and reinforce land sustainability efforts. Many of these intelligent technologies provide alternative forms of collecting and processing farming data for real-time analysis and appropriate action. The rapid adoption of wireless sensor networks has led to low-cost designs of small sensor devices, thanks to the IoT input (TEAM 2019). These sensory automated tools aid accurate decision-making in agriculture in favor of high production. Equally, such innovations are mutually complemented by AI. As such, AI has opened the widely untapped cross-disciplinary potential to create a paradigm shift on how much the world derives from agriculture. With an enhanced mix of biological science and technology, IoT, Big Data analytics, and AI-powered elucidations, farmers can produce more quality food with less effort, time, and complexities. This chapter dissects how fusing AI, 5G wireless, and IoT technologies can transform the existing farming latency for future "smart agricultural" practices. Lastly, it explores the likely impact of this intelligent connectivity in farming using modern innovations.

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

15.2 The Potential of Wireless Sensors and IoT in Agriculture

Today agricultural activities are quickly changing how or how much farmers can produce, thanks to the IoT, which is a modern system that interrelates several devices to uniquely identify and transfer mass data over networks without human-to-computer or human-to-human interventions (Biradar 2019). Tools with such unique identifiers (UIDs) include mechanical, computing, and digital machines, all mutually working with objects, animals, or people (TEAM 2019). Through IoT gadgets in the healthcare sector, manufacturing, and many other innovative areas, smart farming is emerging as an enabler of increased efficient, intelligent crop management. Such developments could potentially help reduce food shortages across the globe, saving millions from the effects of drought, natural disasters, fires, and other calamities.

For instance, to effectively manage and control pests in agriculture, wireless IoT is now able to relay information seamlessly from farms. These low-resolution sensors analyze and send information from large tracts of land to required destinations about the crop health status or potential pest manifestations. They can capture both high-definition and microscopic images of plants that the naked eye cannot see. The IoT wireless sensors come embedded with nodes linked to a central processing unit (CPU) working with an interface, power, and transceiver units (TEAM 2019). A node is a small, minute centralized computer system. The sensory unit uses Radio Frequency (RF) technologies through which nodes communicate data monitored wirelessly to CPUs about farm humidity, temperatures, pressure, vibrations, crop health status, and much more.

The nodes are predefined with specific tasks. They could be located across several parts of the farm forming networks synchronized in structure to interconnect data collected about microclimatic conditions or any other user preferences. Likewise, these wireless IoT sensors can assemble statistics related to pest behavioral patterns straight from ranches to distant data operating centers (Biradar 2019). IoT device users can monitor such regular data for pest application technique adjustments, including when and how to apply pesticides. Interestingly, they can also capture the amount of sunlight received or released by a plant, commonly referred to as a spectral signature. In most cases, the location of these nodes takes into account farm topography for optimal functionality.

IoT data transmissions empower farmers to take timely action to prevent potential losses, further bolstering efforts to increase food production. Agriculturalists can analyze the facts and identify effective research-based methods, treatments, and technologies to control current and future manifestations based on influencing factors (Biradar 2019). Remarkably, the sensors also provide predictive futuristic preventive mechanisms, allowing farmers to explore appropriate pest treatment methods without remedial ideas. As a result, smart farming is now making it easy for farmers to understand the likely impact of pest control methods well in advance, which avoids wasting resources and time on non-productive or unhealthy crop-maintenance procedures.

Thankfully, these devices are comfortable to use across the world to supplement the often-inadequate conventional pest management practices. As IoT devices continue to evolve and significantly impact agriculture's future, for the better, many farmers will be able to avoid unnecessary low productive disappointments characterized by unprofitable farming seasons (Biradar 2019). These modern technologies seek to replace the time-consuming and tiresome manual approaches to maintaining healthy crops. They are likely to define a smart farming future, helping farmers to make informed decisions about healthy crop maintenance instead of hopefully waiting against the odds for good weather.

15.3 IoT Sensory Technology with Traditional Farming

"Smart agriculture" has immense potential to boost future food production and save millions suffering from food shortages or dying of hunger. Many farmers embracing traditional approaches lack fast, reliable internet connectivity through the IoT. The reason is that, to employ IoT sensory technologies, connectivity is necessary throughout the agronomic environment (TEAM 2019). Specifically, such an installation is essential in greenhouses, storehouses, barns, and many other farm places. The connection should also be uninterruptible and able to withstand adverse weather conditions outdoors, which might not work for farmers living in harsh climatic locations. Figure 15.1 depicts the five stages of a sample case of IoT analytics (EDUCB n.d.).

Nonetheless, technological advancement is underway to solve the design problems associated with these limitations. Until IoT sensory systems manufacture devices that can effectively work anywhere, including regions grappling with an unfavorable climate, adopting the know-how remains a challenge in some areas. Some growers or agrarian communities lack enough resources and time to embrace the IoT sensory technology in farms (TEAM 2019). For instance, employing drones with portable sensors linked through grids and operating stations is often expensive for many farmers. Others do not have the time to regularly monitor such functionalities due to several personal, agro

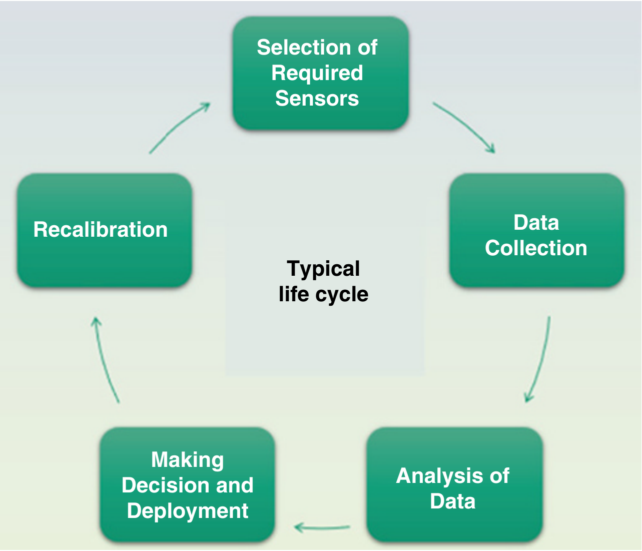

Figure 15.1 The typical life cycle of an IoT analytics-based agricultural use case (EDUCBA).

micro- and macro-environmental limitations. Others lack awareness of such technologies, the potential impact on increasing agricultural productivity and food sustainability, plus much more.

15.3.1 IoT Sensors Available for Specific Agriculture Applications

There are several IoT sensors dedicated to crop growth stages. Such stages include sowing, harvesting, packing, and transportation, among others. These sensors can detect and monitor soil moisture, humidity, solar energy levels, temperature, carbon dioxide, and many other aspects (Biradar 2019). An important factor to consider when selecting a sensor for its suitability to a particular application is to ensure accuracy of the signal report, range coverage, noise fluctuation, resolution and incremental changes, and repeatability performance for a measurement report. Smart vehicle stations are usually installed across the fields with sensors for data collection. Through diverse models from different manufacturers, they can predict how crops can grow in precision farming stages.

For instance, during the early stages of planting and sowing, actuators can provide farmers with invaluable information for the careful nursing of crops (Biradar 2019). These types of sensors scrutinize soil humidity and carbon dioxide levels, including plant health big data analytics. Consequently, farmers can exercise care, ensuring crops grow in a sustainable environment, like greenhouses (TEAM 2019). Actuators come together with the installation capability of intelligent LEDs for plant energy regulation and automation. They support sprinkler systems to activate automated irrigation and cooling mechanisms when temperatures are higher than anticipated levels. Once the crops grow to harvest and storage times, these sensors provide storage heating, including automated packing and transportation capabilities, as farmers reduce waste.

Likewise, digital lumen sensors can nurture crops from the early stages of planting, sowing to maturity before harvesting using an intelligent contiguous heat control. The combination of lighting controls and data collection seamlessly guarantees efficiency in crop growth management for superior farm performance (Biradar 2019). Adopting these types of sensors for smart greenhouses presents up to 10 times average yields compared to conventional agricultural methods. They require less water and minimal use of pesticides due to the healthy, controlled crop environment. Supplementary sensors include those with hydroponic technologies dedicated to smart gardening for urban environments like malls and other skyscraper structures, among other places. The resource-efficient sensors sanction, almost without soil, the growing of crops since they inform farmers of the nutrients that are necessary to provide plants during growth (TEAM 2019). The models have now become the much-sought solutions for twenty-first-century farming challenges in maintaining crops from an early age to maturity, including harvesting and storage.

A brief list is given of the field sensors in agriculture used for monitoring the following parameters:

1) Temperature
2) Humidity
3) Barometric pressure
4) Soil moisture
5) pH level

The modeling software collects data from these sensors and activates the Control Network. This helps farmers to start cultivation with optimal inputs of material. The Control Network has the following responsibilities:

1) Water pressure
2) Irrigation operation
3) Controlling animals
4) Sunlight
5) Pesticide dispersal
6) Heating/cooling

These sensors are also cheap, so many visionary farmers are implementing them.

15.3.2 Challenges Faced While Implementing Sensor Technologies

Though IoT is the future of agriculture, it still has some challenges to face.

Connectivity. Connectivity is a challenge because to work in an IoT system you need to provide connectivity throughout the agricultural environment from storehouses, fields, barn, and greenhouse. It also requires much space and strong connectivity, which should be able to work in certain weather conditions like storms, etc.

Design and durability. As it will be a network of IoT, it must have a proper design with reliability and robustness to work on the farm.

Limited resources and time. Those companies that design IoT for agriculture should design them so that these systems can withstand rapid climate changes and be compatible with limited land and resources.

15.4 IoT Devices and Communication Techniques

There are several IoT and communication devices available in the market to be used in the agriculture field. The following are some of the sensors with their functionality:

- Wireless sensors. These sensors are considered crucial when it comes to collecting crop conditions and other information. Acoustic sensors are used for pest monitoring and detection and classifying seeds into varieties. They are low in price; Field Programmable Gate Arrays (FPGA) sensors are starting to be used to measure real-time plant transpiration, humidity, and irrigation, but they have some limitations, such as size, cost, and greater power consumption. Optical sensors are used to test the soil's ability to reflect light, its moisture, and the presence of minerals and to gain yield information. Mass flow sensors are used.
- IoT-based tractors. Self-driving tractors have been manufactured that avoid revisiting the same area. They can be extremely helpful in the cultivation process, but farmers cannot afford them due to their high prices.
- Harvesting robots. Harvesting the field is a painful process, but thanks to AI and IoT it can now be automated. This saves time because robots work faster than humans, and the field is harvested at the right time and provides flexibility whenever needed.

Communications in agriculture. Communicating the relevant information at the right time is crucial in the agricultural field. Otherwise, it would be difficult to achieve real purpose until better connectivity is provided. There are many communication networks that could be selected based on the requirements of any specific field or availability of the resources. Some of them are mentioned below:

Cellular Communications. Communication modes from second generation (2G) to 5G could be used according to the field's requirements. Connectivity is again a major concern, especially in rural areas, where getting in touch with the satellites for transmission of the data could be the option. Still, its costs are high and would not be suitable for small farms. The need for 5G and wireless is critical for agricultural development. The enhancements and range of effects it will bring will allow for a much smoother transition for farmers worldwide. Wireless protocols like ZigBee will ensure that low-energy cost wireless communication occurs and will allow for adequate techniques to be utilized in wireless sensor networks. There is a wide range of protocols being developed and protocols that have already been developed that will allow sensors to communicate wirelessly without any hassle. In addition, the effectiveness and mobility that wireless will bring for agricultural AI and IoT as an exponential benefit will ensure a haven of great success.

Bluetooth. This is wireless communication and connects small head devices over short distances. Many farms are using this technology due to its low power consumption, user-friendliness, and low-cost benefits.

LoRa. This is a long-ranged type of communication with a low power requirement, considered to perform better in terms of lifespan, and does not require much maintenance. It is better than Bluetooth technology in terms of reliability and effectiveness.

SigFox. This is a French global network operator that provides connectivity to objects that need low power and provides high performance because of its ultra-narrow technology.

ZigBee. ZigBee is suitable for short-range area communications, like the greenhouse environment. Real-time data is transmitted through ZigBee to the end-user.

15.5 IoT and all Crop Stages

- Sowing. By using sensors, farmers can find optimal inputs to the crop. This helps them to save money, time, and energy because they know exactly how many seeds to sow, amount of water to provide, and spray pesticides.
- Harvesting. Robots reduce painful labor work and crops are harvested at the right time within less time.
- Packing. Automated packing would help reduce human effort, time, as well as labor costs. With automated robot packing, all from moving to retrieving of the product is done automatically, and a record of the items is maintained. A track record of the products is maintained as well through various sensors.
- Transportation. Through vehicle tracking systems and connectivity, farmers can be assured of their products' security, and these connected vehicle technologies can monitor tire pressure so that vehicles can carry the exact amounts of loads. They could also make a better choice to select the better route and time for transportation.

15.6 Drone in Farming Applications

Unmanned Aerial Vehicles (UAVs) dedicated to crop surveillance have reinforced the impact of the IoTs and AI in "smart agriculture." They provide superior future solutions, thanks to their spatial resolution, to execute a series of controlled measurements (TEAM 2019). Once activated, they can fly across vast agricultural fields monitoring crop health, including soil properties, while relaying the same information to farm stations. These UAVs seamlessly capture pest manifestations, diseases, irrigation challenges, including plant growth patterns. Technologically, UAVs are designed to tirelessly carry out such repeated tasks since they are smaller versions of computers, things that are dangerous or tedious for humans to do.

Today, UAVs can evaluate crop weed management, plant levels of chlorophyll, moisture content, soil texture, and much more. UAVs routinely spray various pesticides in "smart farms" and have become useful in semi-automated crop scouting. Semi-automated crop scouting is the virtual inspection of farms through image and video UAV relays with in-depth data interpretations to accurately manage their agricultural activities (Biradar 2019). These devices execute vegetation index mapping for real-time agroindustry analysis and significantly save revenue growth costs by optimized crop yields.

Drone technology has a variety of uses in the field of precision farming. Farm management activities involving observation, measurement, and taking action can be now be done based on real-time crop and livestock data. Drones can be used to obtain three-dimensional (3D) maps on soil and help in identifying issues related to soil. This is a great tool in soil and field analysis. The information gathered helps farmers to find effective ways to plant and manage their crops and soil. This results in better utilization of resources like soil and water. Agricultural drones can also aid in planting. This is a new technology that is still developing. These drones can plant vast areas over a short period, thus minimizing the need for an on-the-ground planting operation, which may be costly, time-insensitive, and strenuous.

Crops require constant spraying and fertilization to maintain high yields. Traditionally this was done using methods that were costly, inefficient, and tiresome. However, drones have revolutionized the way it is done today. These drones are usually equipped with reservoirs filled with fertilizers, herbicides, or pesticides and can spray large areas quickly. This method has proved to be cost-effective, efficient, and safer. Spot spraying is also possible using drone technology, and can be accomplished using less time than the traditional way.

Drone technology has become a critical component in large-scale crop and acreage monitoring. It is now easy to manage thousands of acres more effectively. Drones provide real-time footage and time-based animation, which gives a clear image of crop progress. Using drones, one can collect information on overall crop health, crop life cycle, and crop distribution. Therefore, crop mapping and surveying decisions can be made on real-time data rather than guesswork. The final result is the maximized use of land and other resources.

Irrigation can sometimes be cumbersome, especially in the case of large-scale irrigation. However, using drone technology, one can quickly identify regions with irrigation issues and solve them. This information can also aid in better crop layout and avoiding water pooling, which is detrimental to sensitive crops.

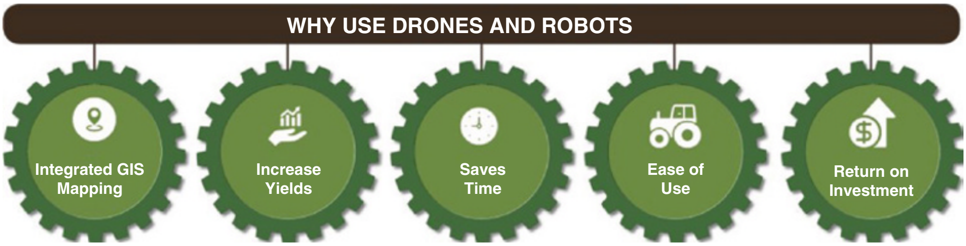

Figure 15.2 The benefits of using a drone in precision agriculture (Chuchra 2016).

Other than crop management, drones are one of the best tools for real-time livestock monitoring. Drones can be equipped with imaging cameras that enable a farmer to manage and monitor livestock. A farmer with a huge herd can identify any injured or missing animal and observe the process of giving birth from the comfort of his house. Also, drones can be used to spot predators, which is a huge advantage to the farmer. Figure 15.2 shows how drone usage in agriculture for soil and field analysis, planting, crop spraying, crop monitoring, irrigation, and health assessment can benefit farmers.

15.7 Conclusion

The fusion of AI and the IoT inevitably offers immense farming opportunities. As the world population continues to increase, the agriculture sector is under pressure more than ever to boost food production. Thankfully, the technologies behind IoT sensors and AI provide farmers with the ability to collect almost every piece of information about plant or crop health for real-time analytics. Today, wireless IoT sensors installed with nodes in farms analyze crop pest manifestations, surrounding humidity, temperatures, soil properties, and much more for effective crop management. UAVs help farmers fly across vast fields collecting index mapping data, spraying pesticides, and analyzing crop irrigation gaps, plus much more. Such integration has seen these mechanical, digital, and computing devices mutually work together with people.

These technologies predict necessary measures for plant and animal care, enhancing and further increasing food production. However, the lack of awareness of AI and IoT for “smart agriculture” continues to pose challenges for the maximum adoption of these technologies. Other problems include a lack of resources, time, and farmers’ commitment to utilize these solutions and solve food-related problems. Though several wireless IoT sensors now exist for greenhouse and crop health monitoring, today’s farming methods mainly remain conventional. A lot needs to be done to increase the adoption of AI and IoT technologies for “smart agriculture.” However, ambitious futuristic farming goals will involve removing existing limitations to increase food production and boost farmers’ revenues. In conclusion, extensive research shows that dedicated IoT sensors will significantly save farming time, resources, and costs. Such efforts will unlock smart farming integration of AI and IoT opportunities for maximum exploitation and help the world achieve sustainable futuristic agribusiness efficiency.

References

Biradar, C., El-Shamaa, K., Singh, R.K., Atassi, L., et al. (2018). Artificial Intelligence (AI) and Internet of Things (IoT) for Inclusive Agro-Ecosystems for Sustainable Development. *Geospatial World Forum*. Hyderabad, India: HICC. https://www.researchgate.net/publication/345807738_Artificial_Intelligence_AI_and_Internet_of_Things_IoT_for_Inclusive_Agro-Ecosystems_for_Sustainable_Development (accessed 22 June 2021).

Chuchra, J. (2016). Drones and robots: Revolutionizing farms of the future. https://www.geospatialworld.net/article/drones-and-robots-future-agriculture/.

EDUCBA (n.d.). IoT in agriculture. https://www.educba.com/iot-in-agriculture/ (accessed 22 June 2021).

TEAM, DIGITEUM (2019). Is IoT the future of agriculture?https://www.digiteum.com/iot-agriculture (accessed November 19, 2019).