EVALUATION OF INFLUENCE OF 'INTERNET OF THINGS' (IoT) ON TECHNOLOGIES AND DEVICES IN 21ST CENTURY

Khandakar Akhter Hossain, PhD

DOI: 10.31364/SCIRJ/v11.i7.2023.P0723950
http://dx.doi.org/10.31364/SCIRJ/v11.i7.2023.P0723950

Abstract: The Internet of Things (IoT) is revolutionizing computing by introducing networked devices into our daily lives that acquire and analyze information to serve an ever-increasing number of services and human life. It is about connecting everyday objects to the internet and letting them communicate with each other including human being. The Internet of Things (IoT) makes technologies smarter by enabling automation, personalisation, and remote control via networks of Internet-connected sensors. At the same time, IoT technologies raise significant privacy concerns, which may hinder their wider adoption. IoT applications range from smart homes and wearable gadgets to industrial automation, agriculture, healthcare, transportation, ecosystem, warfare, business, education, so on. The IoT has the potential to completely transform our lives by enabling smarter, more connected, flexible, more relax, and more efficient systems. IoT has the potential to develop industries efficiency, increase productivity, and improve our daily lives. IoT will influence more in technology, and more things will become internet-connected in future. It is an analytical paper to depict the influence of IoT on technologies and devices in our usual life, business, industry and other sectors along with challenges and suggestions for best harvest in 21st century.

Key Words: IoT, Security, AI, 5G, IIoT, AR, VR, 3D printing

Introduction

The internet of things (IoT) is a catch-all term for a growing number of electronic devices that aren't traditional computers but are linked to the internet to exchange data, information, orders, or/and instructions. Today, the Internet of Things encompasses a vast array of 'things'. Internet-connected 'smart' versions of standard appliances such as refrigerators, televisions, light bulbs, and gadgets may exist only in an internet-enabled environment. Again, internet-enabled sensors are altering manufacturing, healthcare, transportation, distribution centers, the service sector, industry, farms, and other industries.[1]IoT, on the other hand, is a term that refers to the increasingly sophisticated ecosystems of online, linked devices with which we share our world. Today, almost any item we use in our homes, businesses, factories, or even wear on our bodies can be online and connected, giving rise to the term "internet of things."[2]IoT is a trend that is driving the increasing digitalization and datafication of society in many innovative and remarkable ways.IoT is a new information processing, acquisitiona and evaluation method, and it has been widely used in intelligent transportation, environmental monitoring, efficiency maximization and other aspect of technologies and devices. Technologycan effectively integrate the infrastructure resources in communications, connectivity, management, marketing, finance, economy, engineering, medical, power system, environment aspect, and other service and industry related things by the influenced and effective use of IoT.[3]So, most of the technologies and devices will be influenced by IoT in 21st century.

The Internet of Things (IoT) often refers to the addition of network connectivity to ordinary objects or equipment that were previously not internet-enabled. As Tony Fadell, founder of the pioneering IoT startup Nest, stated, one trademark of the IoT field is to work on "unloved" and often "utilitarian" devices such as smoke detectors, doorbells, and other sensors and add never-before-possible functionality via network connectivity.[4]While consumer IoT has garnered a lot of attention due to the proliferation of smart speakers, televisions, and household appliances, the Internet of Things has also arrived in the enterprise, with companies using the internet to track valuable assets and enhance logistics and manufacturing. Because of these networks of connected things, self-driving automobiles, autonomous manufacturing robots, AI-operated vehicle, craft, and under water device/machine will be used in combat, as will remote medical equipment that allow doctors to diagnose patients and even do surgery.[5]Companies and universities all across the world are interested in building Artificial Intelligence (AI) systems, from Apple to Google to Facebook. AI is crucial in many engineering fields. Furthermore, 2021 has seen numerous fascinating breakthroughs in the field of AI and machine learning. As a result, many scholars from various fields will be fascinated about this SI. This Special Section aims to attract the attention of the

http://dx.doi.org/10.31364/SCIRJ/v11.i7.2023.P0723950

academic and industrial communities to developing advanced and innovative methodologies and techniques for AI for IoT by bringing together academic and industrial researchers to identify and discuss technical challenges and recent results related to AI for IoT. [6]

The Internet of Things links physical devices to the internet, enabling data processing and analytics. This entails interacting with the global information network without using a keyboard or a screen. The internet of things (IoT) can bring to industrial processes and distribution networks the same efficiency that the internet has long given to knowledge work.[7]Throughout the world, billions of embedded internet-enabled sensors provide an enormous amount of data that businesses can utilize to improve operational safety, track assets, and reduce human operations. Machine data can be used to predict whether equipment will break, giving manufacturers a heads-up and avoiding lengthy periods of downtime.[8]IoT devices can also be used by researchers to collect data, information, and other intelligence about client preferences and behavior, market demand, future requirements, potential risk, and so on. However, those may be serious implications for privacy and security.[9] IoT has the potential to develop industries efficiency, increase productivity, and improve our daily lives. At the same time, IoT will influence seriouslyto other technologies, and in future more things will be internet-connected. Today globally, there are around 17 billion active IoT devices, and more than 85% of firms have boosted their technical efficiency by implementing IoT technology into their products. The Internet of Things has been named "the next wave of innovation" as its impact on people's day to day lives evolves.[10]In fact, IoT is critical for operating large-scale businesses and the service industry in the twenty-first century. Furthermore, it was shown that IoT has a considerable impact on decision-making and corporate operation management.[11] It is an analytical paper to evaluate the influence of technologies and devices by IoT in daily life, global business, all industrial and service sectors along with challenges and suggestions for best yield of IoT in 21st century.

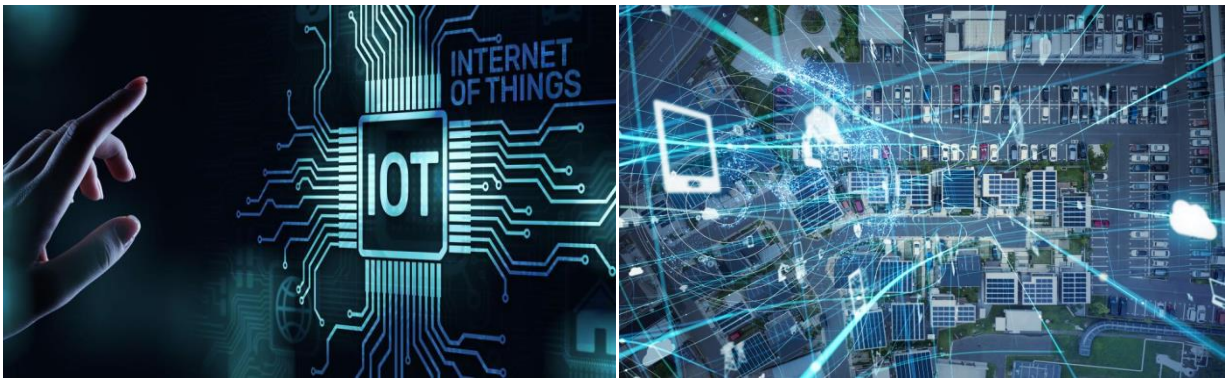

Figure 1: IoT has brought the world in our finger tips[12] and future of IoT[13]

History and Core Domains of IoT

The Internet of Things (IoT) is a network of physical objects, or things, that are integrated with sensors, software, and other technologies that enable them to connect to and exchange information with other devices and networks over the Internet, and that encompasses every part of our lives. IoT has its origins in the early 1980s, when the concept of connecting various devices and products to the Internet was first proposed. The term "Internet of Things" was invented in 1999 by Kevin Ashton, a British technology pioneer.The first known IoT-enabled equipment, a Coke machine that could report its inventory and temperature, was invented in the 1980s at Carnegie Mellon University's Computer Science Department. John Romkey developed the first internet-connected device, a toaster that could be turned on and off via the internet, in 1990.[14] The advent of wireless communication protocols such as Zigbee, Z-Wave, and Bluetooth enabled IoT devices to have low-power, short-range connection. IPv6 development gave a substantially bigger address space, which was critical for addressing the huge number of IoT devices. With the integration of IoT devices into many sectors such as manufacturing, transportation, and energy, IoT gained popularity in the industry. Machine-to-Machine (M2M) communication[15] has become common, allowing devices to interact and exchange data without the need for human interaction.

Thermostats, security cameras, and voice assistants have grown in popularity, providing consumers with greater convenience and control over their living areas. Several organizations and partnerships, like the Industrial IoT Consortium (IIC)[16] and the Open Connectivity Foundation (OCF)[17], worked to define IoT interoperability and security standards.[18] AI and machine learning (ML) technologies[19] are being integrated into IoT systems, allowing for improved data analytics and predictive capabilities. The expansion of 5G networks[20] enables quicker and more dependable connectivity, boosting the possibilities of IoT even further.The Fourth Industrial Revolution (4IR)[21] is the digital revolution that is occurring as a result of developing technologies such as robotics, IoT, and AI. The 4IR signifies a fundamental shift in how we live, work, and interact with one another.

http://dx.doi.org/10.31364/SCIRJ/v11.i7.2023.P0723950

4IR is a new chapter in the development of humanity, made possible by unprecedented technological developments comparable to those of the first, second, and third industrial revolutions. These advancements are fusing the physical, digital, and biological worlds in ways that hold enormous promise as well as possible danger. The revolution's pace, breadth, and depth are driving us to reconsider how countries evolve, how organizations create value, and even what it means to be human. The 4IR is about more than simply technological transformation; it is a chance for everyone, including leaders, policymakers, and people from all income levels and nations, to harness converging technologies in order to create an inclusive, human-centered future. Beyond technology, the true opportunity is to create ways to empower the greatest number of people to positively impact their families, companies, and communities.[22]Interestingly, COVID-19 has substantially expedited the implementation of IoT. IoT has the potential to play a big role in achieving a more viable, sustainable, and environmentally friendly future. There are three key domains that fall under the banner of IoT.[23] Those are:

- **Wearable IoT**—Devices that people can wear as accessories, such as watches, to monitor an individual's activity or vital signs. IoT-enabled wearables are internet-connected devices equipped with various sensors that can be worn as external accessories (for example, watches, glasses, rings, and so on) or embedded in textiles such as smart shoes or jackets. Many commercially available wearables, such as the Fitbit and Apple Watch, are expressly designed for health and fitness tracking.[24]Sensors gather individuals' movement and vital indicators, such as steps taken, heart rate, and sleep quality, to track activities and assist people in monitoring and improving their wellbeing and physical performance.[25]Other gadgets, such as Google Glass, aim to assist users monitor their engagement with the world around them by capturing audio and video of their daily lives. The purpose of all wearable technologies is to automatically and unobtrusively record an individual's bodily contact with the surroundings.[26]

Figure 2: Image of impact of IoT on smart city[27], [28]

- **Household IoT**—Devices that remain in homes of individuals, such as smart speakers, appliances, and thermostats. A smart house is one that has lighting, heating, air conditioning, security systems, or entertainment systems that interact with one another and work together to improve the occupants' experience and comfort. Smart home gadgets enable remote monitoring and control of home components such as the thermostat, lights, and door locks. Many smart gadgets, such as smart speakers and appliances, aim to improve household convenience and automation.[29]Using cameras, audio, and fire or water leak sensors, devices can also offer safety and security monitoring. Additional individuals and organizations may be involved in safety monitoring, with information and devices shared with family members, security corporations, or emergency services.[30]The impression of smart home data privacy differs per device. Some information, such as the state of smart lighting or thermostats, is not considered as very sensitive. However, video and audio from within the home are typically considered private, and users want strong safeguards against recordings being viewed without their knowledge or permission.[31]

- **Public IoT**—Devices that are used in public locations, such as smart water meters, autonomous vehicles, and Bluetooth beacons. Smart cities and smart buildings have increased the use of IoT technology in public infrastructure. The management and optimization of traditional public services, such as transportation and parking, lighting, ventilation, surveillance and upkeep of public places, and even cultural heritage protection, can all benefit from public IoT infrastructure. The New York City Department of Transportation, for example, incorporated a congestion management system to assess traffic speed at 23 crossings in Midtown Manhattan, reducing travel time by 10% on Midtown's arteries.[32]Smart cities and buildings, like smart homes, enable services to monitor the security and safety of areas and people, as well as intelligently automate controls in reaction to the environment. Furthermore, IoT is frequently utilized for resource management, cutting costs by utilizing resources more efficiently and intelligently. For example, the city of Dallas, Georgia, has implemented a smart water meter program that has assisted them in more efficiently detecting water leaks and minimizing water loss.[33]The autonomous car is another developing

http://dx.doi.org/10.31364/SCIRJ/v11.i7.2023.P0723950

type of IoT device in the public domain, which is rapidly being used in app-based taxi services (e.g., Uber), home delivery services, and consumer items (e.g., Tesla). Each autonomous car is outfitted with a plethora of sensors to collect data about its surroundings, such as people walking down the street, other vehicles on the road, and adjacent store information.[34]Furthermore, drivers and passengers in cars face a considerable quantity of data collection during and after their travel (for example, automobiles may collect information about their daily schedule).[35]

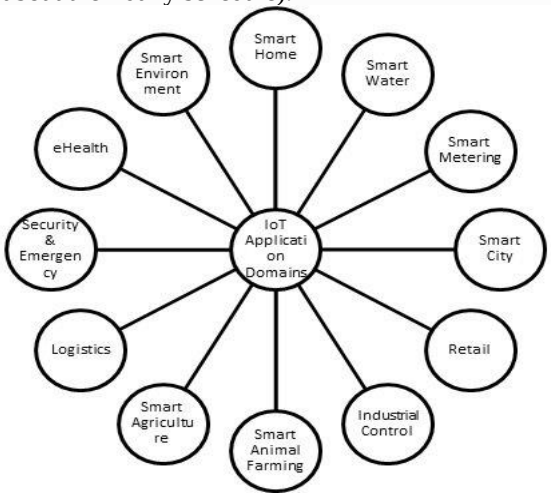

Figure 3: IoT application domains[36]

The energy consumption and carbon impact of IoT devices and systems, on the other hand, are becoming serious concerns. Federated learning (FL) is a novel and promising approach that allows numerous devices to train a common model jointly while maintaining individual data on-device. FL is distinguished by the ability to train models with far less data than centralized learning and to train models on low-power devices. Both federated learning and green/sustainable computing strive to increase the efficiency and sustainability of IoT systems. Federated learning allows numerous devices to learn a common model cooperatively while preserving data on-device, reducing the energy usage and carbon footprint of IoT devices and systems.This is due to the fact that FL allows models to be trained on low-power devices with far less data than centralized learning, which can assist to minimize the energy consumption of IoT devices. Integrating Federated learning with green/sustainable computing can potentially open up new IoT use cases and applications. FL, for example, can be used to train models for environmental monitoring, smart cities, and smart grid applications, which can aid in the optimization of energy usage and resource efficiency.[37]Again, the IoT process consists of numerous processes and components. Here's a high-level summary of the normal procedure for creating an IoT system:

- Determine the issue or opportunity.
- Define requirements.
- Select hardware.
- Develop and select software.
- Connect devices
- Data collection and transmission
- Cloud platform and storage
- Data processing and analysis
- Visualization and user interface
- Integration and action
- Maintenance and security

The information sector has boomed in the twenty-first century, and it is extensively injected with technological developments. This results in a plethora of alternatives that, if employed carefully and meticulously, can help achieve the United Nations (UN) Sustainable Development Goals (SDGs). The majority of respondents strongly believe that Green IoT can be a game changer in reaching SDG targets. Critical areas where these technologies can make a significant difference include the efficient and effective use of raw materials, the conservation of natural resources, and the reduction of greenhouse gas emissions and other waste. A sustainable environment necessitates the planned and structured application of IoT and G-IoT technologies, which have the potential to drastically

http://dx.doi.org/10.31364/SCIRJ/v11.i7.2023.P0723950

convert traditional development into sustainable development. Developing goods and services to improve renewable energy sources, energy-saving computing and power source modulation, green metrics, assessment tools, and techniques all contribute to this process.[38] Easy data storage and retrieval to support decision-making, reduced workload and complexity, improved operational efficiency, aids in identifying and correcting errors immediately, and improved system monitoring and control are discovered to be important applications of IoT for businesses in various industries and service sectors in the twenty-first century.[39]

Different Technologies Related to IoT

The Internet of Things contains and interacts with a wide range of technologies. We know that artificial intelligence (AI) is a branch of computer science aimed at developing computer systems capable of doing activities that would typically need human intelligence.[40]AI is often used to accomplish tasks such as object recognition, speech transcription, decision making, and so on. Deep neural networks, which require enormous quantities of data to train and work, are currently the most successful kinds of AI. The data acquired by IoT is highly suited for usage by AI, which may then give IoT devices with features such as voice command processing.[41] Again, the cloud refers to computer networks that are accessed remotely rather than locally. It is made composed of software, platforms, and infrastructure that are delivered to users on demand. Common cloud services include application execution as well as data storage, processing, and delivery.[42]IoT devices commonly make use of a variety of cloud services. Data collected by IoT devices is frequently stored or processed on cloud platforms, owing primarily to cloud scalability and storage and processing power limitations on small IoT devices, but also because many IoT organizations find additional value in being able to rapidly access data from IoT devices.

Internet of Things devices are virtually always linked to the internet or private networks. A variety of businesses require computer hardware and system software to maintain a network, necessitating the usage of network specialists.[43]Wearable, home, and office devices typically link to networks via short-range technologies like Ethernet, Bluetooth, or WiFi, whereas larger IoT ecosystems like those found in cities or farms sometimes employ longer-range technologies like cellular or satellite networks. 5G is a cellular network technology that will eventually replace 4G. 5G will be used to link a new range of IoT devices and applications by delivering more data faster and more securely. Its speed has the ability to support new business models, modify processes, and improve corporate performance. However, few use cases require 5G capabilities today, and most IoT applications are well supported by 4G or lower bandwidth network technology.[44]5G will bring a number of advantages to the Internet of Things, including the ability to connect many more devices at the same time,[45] and the ability to track the location of those devices with significantly greater precision and accuracy.[46]

Trend of IoT in 21st Century

In this revolutionary century, physical and virtual dimensions are increasingly intertwined day by day. Advanced technologies such as internet of things, big data and artificial intelligence, augmented reality, mixed reality, virtual reality, radio frequency identification technologies and smart spaces radically changes in many areas of life including business, industry, education, and service sector.[47]IoT has become a hot topic in the tech-driven world of 21st century. A strong framework of cloud computing, backed up by a seamless blending of sensors and actuators with the environment around us, is making this "network of networks of autonomous objects" a reality. From smart wearables to smart cities, from domestic life to industries, the IoT is expanding itself to different areas.[48] Smart security solutions, smart home automation, smart health care, smart wearables etc. are in-trend applications of IoT, and by the near future we expect to see its application to a city's transportation system or smart power grids. We must know the importance of cloud computing, autonomous control, artificial intelligence in the context of the IoT.[49]Augmented reality, high-resolution video streaming, self-driving cars, smart environments, e-health care, and other IoT-centric concepts are becoming commonplace.[50] Higher data rates, larger bandwidth, expanded capacity, reduced latency, and high throughput are required for these applications. In light of these new principles, IoT has transformed the world by enabling seamless connectivity between disparate networks.[51]

- **Growth in Data and Devices and increase Human-Device interaction.** Today, about 17 billion devices are actively connected to the Internet and are used for daily tasks. With the arrival of 5G, additional gadgets and data traffic will be possible.[52]We may add to this trend the increased usage of edge computing, which will allow businesses to handle data more quickly and near to the point of action.[53]

http://dx.doi.org/10.31364/SCIRJ/v11.i7.2023.P0723950

- **AI is the Powerful Player in IoT.** Making the most of data, and even comprehending how contemporary infrastructure works on a fundamental level, requires computer support via artificial intelligence. Amazon, Microsoft, and Google are among the main cloud vendors that are increasingly attempting to compete based on their AI capabilities. Several firms aspire to boost their market share by leveraging AI algorithms capable of leveraging machine learning and deep learning, allowing businesses to extract more value from their ever-increasing volumes of data. Artificial intelligence is the key component required to make sense of today's massive amounts of data and boost its business value.[54]AI will aid IoT data analysis in the following areas: data preparation, data discovery, streaming data visualization, data time series accuracy, predictive and advanced analytics, real-time geographic and position (logistical data).

- **Voice User Interface (VUI) is Now Reality.** It is a competition between industry leaders that want to control the IoT sector at an early stage. Digital assistant devices like as Alexa, Siri, and Google Assistant are the future hubs for the next generation of smart gadgets, and corporations are attempting to build "their hubs" with consumers in order to make it easier for them to continue adding devices with less trouble and annoyance. Taking a page from science fiction movies, conversing to robots such as R2D2, C-3PO, and Jarvis, to name a few, accounts for 80% of our daily communications. The use of voice to set up devices, alter settings, provide directions, and receive results will become the norm not only in smart homes, but also in factories but in between like cars, wearables, etc.[55]Today, we cannot discuss digitalization without mentioning IoT. It's a boon to technology, and in today's world, no firm can flourish without implementing IoT. [56]IoT has been seamlessly interwoven into many elements of our globalized economy and way of life, ranging from interconnected consumer devices to smart cities.

- **IoT Investment has Increased.** The undeniable influence of IoT has attracted and will continue to attract more startup venture capitalists to highly inventive initiatives in hardware, software, and services. IoT spending will reach 1.6 trillion dollars by 2025. IoT is one of the few markets that attracts both emerging and conventional venture capitalists. The proliferation of smart gadgets, as well as users' greater reliance on them to do many of their daily chores, will heighten interest in investing in IoT firms.[57]Customers will be looking forward to the next big innovation in IoT, such as smart mirrors that analyze your face and call your doctor if you appear sick, smart ATM machines that incorporate smart security cameras, smart forks that tell you how to eat and what to eat, smart beds that turn off the lights when everyone is sleeping, and smart shoes that will advise you about your health and what to do.[58]

- **Real Expansion of Smart IoT like Smart Cities.** Nothing will provide a finer example of IoT connectivity and processing than smart cities, yet smart cities have been in a bit of a holding pattern recently. Smart sensors placed throughout the area will track everything from walking paths to shared automobile use, building occupancy, sewage flow, and temperature preference 24 hours a day, seven days a week, with the goal of creating a place that is comfortable, convenient, safe, and clean for all who live there. Once finalized, the technology might serve as a blueprint for other smart communities and, eventually, smart cities. However, the potential benefits for cities make IoT technology particularly appealing. Cities of various sizes are investigating how IoT may improve efficiency and safety, and this infrastructure is spreading around the world.The auto industry is another area where smart IoT is developing, with self-driving cars becoming commonplace in the coming years.[59]Many vehicles now include a connected app that displays the most recent diagnostic information regarding the vehicle. This is accomplished through the use of IoT technology, which serves as the linked vehicle's brain.[60] Diagnostic data will not be the sole IoT innovation in the coming year or so. Other items that will revolutionize the way we drive are connected apps, voice search, and real-time traffic information.

- **Rise of Industrial IoT and Digital Twin Technology.** This new techno-industrial revolution is being driven by a convergence of technologies, with IoT playing a significant role in making production more efficient, less dangerous, and more profitable. Industrial IoT improves efficiency and production by integrating and analyzing data in ways that would not

http://dx.doi.org/10.31364/SCIRJ/v11.i7.2023.P0723950

be feasible without a linked manufacturing process. Digital twin technology is another trend that is gaining traction.[61]Organizations can use it to get a clear view of how their IoT devices interact with the manufacturing process. This provides keen businesses with insight into how their machines' life cycles run, allowing them to anticipate improvements that may be required ahead of time. A Gartner poll found that 48% of smart manufacturing adopters want to employ the digital twin concept.[62]

- **Increase movement to the Edge.** Edge computing is a technique that distributes processing burden and puts it closer to the network's edge (sensors in the case of IoT). The advantages of fog computing are particularly appealing to IoT solution vendors. Some of these advantages include the ability for users to reduce latency, conserve network capacity, operate reliably with quick judgments, collect secure a wide range of data, and move data to the optimal location for processing with improved analysis and insights of local data. Edge computing has grown in popularity in recent years, but the expanding scope of IoT technologies will amplify this trend. This shift is being driven by two factors: Powerful edge devices in a variety of form factors are becoming less expensive.[63]The importance of centralized infrastructure is growing. Edge computing also makes on-device AI a viable option because it enables businesses to exploit real-time data sets rather than needing to trawl through gigabytes of data in a centralized cloud in real time. It's likely that in the future years, if not decades, technology will change to a balance of cloud and increasingly distributed edge-powered devices.[64]Hardware manufacturers are designing edge infrastructure to be more physically rugged and secure, and security vendors will begin to offer endpoint security solutions to their existing services to prevent data loss, provide insights into network health and threat protection, and include privileged user control and application whitelisting and control, all of which will aid in the rapid adoption and spread of edge computing implementations by businesses.

- **Increase Social, Legal and Ethical Issues.** IoT devices are a relatively new and uncontrolled technology. In the foreseeable future, IoT will unavoidably face societal and legal challenges. This is especially true for data acquired by these devices, which may soon fall within the purview of the General Data Protection Regulation (GDPR).[65]The GDPR, a European Union rule on the handling of personal data and privacy, extends its reach beyond the European Union. Any company that wants to operate successfully in the EU must follow the criteria outlined in the 88-page paper. When it comes to the legal control of personal data, security concerns are critical. Development teams can assure the needed level of security and compliance at multiple levels, such as data encryption, active consent, various methods of verification, and other procedures.[66]Their purpose is to acquire data legally while limiting its accessibility, processing, and storage to the minimal required by the software product.[67]

- **Standardization is one of the biggest challenge/problem to growth of IoT**. It is a competition between industry leaders that want to control the IoT sector at an early stage. But we now have a situation of fragmentation. One possible solution is for a small number of vendors to dominate the market, allowing customers to choose one and stick with it for any additional connected devices, similar to how we now have operating systems with Windows, Mac, and Linux, where there are no cross-platform standards. To comprehend the complexity of standardization, we must consider all three areas during the standardization process[68]:Platform, Connectivity, Applications.All three criteria are interconnected, and missing one will break the model and impede the standardization process. Without a strong push from organizations like IEEE or government legislation to create universal standards for IoT devices, there is no way to overcome the fragmentation problem.[69]

- **Traffic Management.** Modern IoT developments indicate that IoT technology is relevant for addressing global concerns such as traffic and obstruction issues. Many firms are already offering plans and solutions that use IoT-installed technology in traffic systems and automobiles to create more intelligent traffic networks, with the goal of reducing unnecessary traffic and congestion. Cities that employ smart-mobility technologies, according to McKinsey, have the potential to reduce

http://dx.doi.org/10.31364/SCIRJ/v11.i7.2023.P0723950

commute times by 15 to 20% on average by 2025, with some people benefiting from far greater reductions. As a result, cities and leaders are finally learning, after a decade of trial and error, that smart-city initiatives cannot be realized without robust technology such as IoT.[70]

- **IoT Security.** According to Statista, the IoT security market will reach 38.7 billion in 2023, up from 34.2 billion in 2022. It's all connected to the growing number of connected devices that demand exceptional security. As a result, security system software will be more important than ever in the coming decade, which is why such IoT device security statistics are unsurprising. As a result, security is an evolving IoT trend, and many firms around the world are developing IoT solutions. When it comes to the extended level of connectivity that we are involved in these days, security is one of the key issues. The rising involvement of technology in people's lives has emphasized the ongoing threat to insecure connected devices.[71]As a result, security is an evolving IoT trend, with various organizations around the world producing IoT security solutions based on a variety of technologies.
- **Metaverse.** The worldwide metaverse market is estimated to reach $679 billion by 2030, according to Grandview Research. The Internet of Things (IoT) is a fundamental component of the Metaverse system, which depends on it to optimize its possibilities.[72]The interaction of the Internet of Things and the Metaverse will almost probably open up new opportunities for expansion and growth in the technology industry. Its growth is expected to be propelled by the metaverse's use in a range of businesses, including games, entertainment, media, eCommerce[73] and retailing, training, manufacturing, architecture, engineering, and others.

Growth of IoT Market and Boom of IoT Popularity

In 2025, there will be more than 25 billion IoT devices, producing 2.2 zettabytes of data. (A zettabyte is equal to one trillion gigabytes.) In comparison, IoT devices created only 100 billion gigabytes in 2013. The amount of money to be generated in the IoT sector is similarly astounding, with estimations putting the market's value in 2025 at roughly US$ 1.6 trillion. It may have seemed unthinkable a decade ago that our refrigerators could notify us when we were running low on milk, our doorbells could record our visitors, and our audio speaker system might mistakenly order toys online. Nonetheless, we live in the Internet of Things era, where these types of devices have surged in popularity and are literally everywhere. The Internet of Things has grown dramatically in terms of the number of devices, income earned, and data created, but most forecasts suggest that growth will increase. The number of connected devices is predicted to reach 25 billion by 2025 (up from 8.7 billion in 2012), and yearly income from IoT sales is expected to reach US$ 1.6 trillion by 2025 (up from US$ 200 billion in 2012). Perhaps most importantly, the volume of data generated by IoT is predicted to reach 2.2 zettabytes by 2025, up from 0.1 zettabytes in 2013.

Before delving into the data, it's necessary delineating what we consider an Internet of Things device and what isn't. In this research, we define IoT devices as those that were previously not linked to the internet ("dumb" devices), but are now network connected, allowing for a new set of applications. For example, while smartphones and computers are Internet-enabled, we do not classify them as IoT devices because they have "traditionally" been so. In this article, an internet-enabled toaster oven would be deemed an Internet of Things device because the equipment hasn't generally been connected to a network. With that concept in mind, how quickly is the IoT market expanding?There are a number of competing figures and projections with any market forecast, but all of them imply that growth has been blazing fast and may potentially increase. According to the NCTA, a trade organisation for internet and television providers, the installed base of connected devices is predicted to exceed 50 billion by 2020, representing a nearly 500% growth over 2012.[74]Almost every market prediction predicts that the industry will be worth a trillion dollars or more during the next decade. According to one of the more conservative forecasts from market research firm IoT Analytics, the business would be worth $1.6 trillion by 2025..[75] Growth of IoT market and revenue has been shown in figure 4 and 5 below.

http://dx.doi.org/10.31364/SCIRJ/v11.i7.2023.P0723950

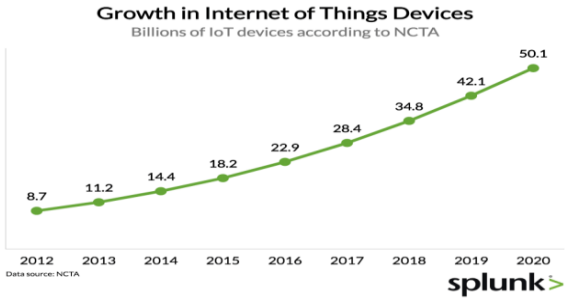

Fig 4: Growth of IoT Market [76]

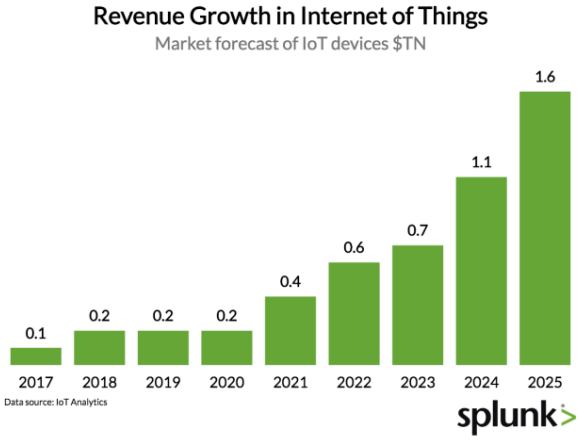

Fig 5: Revenue Growth of IoT[77]

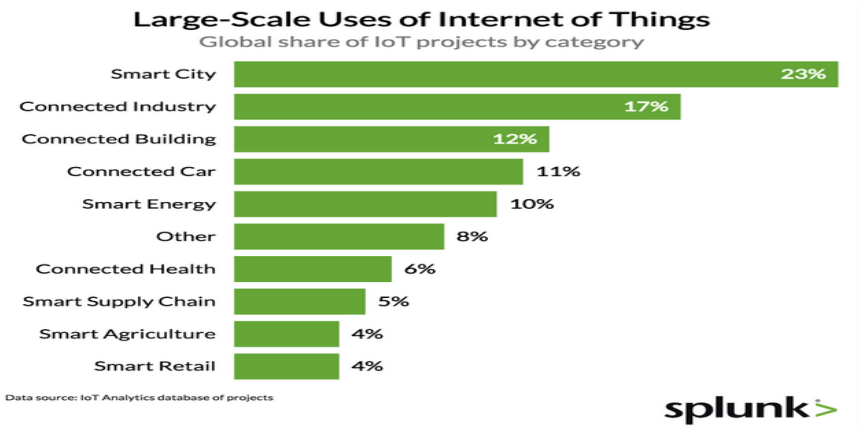

Fig 6: Use of IoT in percentage in different sectors[78]

Again, in another analysis it found that, The number of connected devices in use globally now exceeds 16 billion, with IoT devices accounting for 7 billion (this figure does not include smartphones, tablets, laptops, or fixed line phones). Global connection growth is mostly driven by IoT devices, both on the consumer (e.g., Smart Home) and enterprise/B2B (e.g., connected machinery) sides.[79]The number of active IoT devices is estimated to reach 10 billion by 2020 and 22 billion by 2025. This figure includes all current connections but excludes devices that were purchased in the past but are no longer in use.

1. Wireless Personal Networks (WPAN)

http://dx.doi.org/10.31364/SCIRJ/v11.i7.2023.P0723950

The biggest numbers of IoT devices are connected by short-range technology (WPAN) that normally does not surpass 100m in maximum range. These include Bluetooth-linked gadgets such as headsets but also Zigbee and Z-wave connected devices that can largely be found in smart homes e.g., for linking smoke alarms or thermostats. Many traditional IoT applications send data straight from the sensor network to the cloud via a gateway for further processing.[80]However, this common gateway application is not appropriate for all applications. For short-range IoT wireless protocols like, Bluetooth low energy (BLE), numerous gateways are necessary to gain larger coverage, which is problematic.[81]

2. Wireless Local Area Networks (WLAN)

Wireless Local Area Networks are another huge category, with connectivity of up to one kilometer. Wi-Fi is the most widely used standard in this category, and it is rapidly expanding, primarily through the usage of home assistants, smart TVs, and smart speakers, but also increasingly in industrial settings such as factories.[82]However, as compared to other technologies, it continues to play a limited role in those situations.

3. Low-power Wide Area Networks (LPWAN)

Low-power wide area networks are predicted to account for a major portion of future development in the number of IoT devices. More than 2 billion devices are estimated to be connected over LPWAN by 2025. The technology, which promises extremely long battery life and a maximum communication range of more than 20 kilometers, is used by three main competing standards, Sigfox, Lora, and NB-IoT, all of which are currently being rolled out globally, with over 25 million devices already connected, the majority of which are smart meters.[83]

4. Wired

When most people think about IoT, they don't think of wired connectivity. However, in many situations, a wired device connection is still the most cost-effective and dependable solution. Fieldbus and Ethernet technologies, particularly in industrial contexts, rely heavily on wired connections and are anticipated to do so in the next years.[84]

5. Cellular / M2M

For a long time, 2G, 3G, and 4G technology were the only options for distant device connectivity. As LPWA and 5G gain traction, it is projected that older cellular standards would lose market share to the new technologies, which offer a more lucrative potential to many end-users.[85]

6. 5G

http://dx.doi.org/10.31364/SCIRJ/v11.i7.2023.P0723950

The wildcard is 5G. Still under development in 2018, the technology, which promises a new era of communication with vast capacity and incredibly low latency, is being extensively supported by countries, particularly China. The Chinese government sees 5G adoption as a competitive advantage in its efforts to shift the balance of technical innovation away from the United States and Europe and toward China.[86]By the end of this year, the first pre-standard 5G networks in the United States will be providing Fixed Wireless Access (FWA) services to residential and small-business users.[87]While many additional use cases will be addressed once the final standard is ratified in 2020, we anticipate to see early adopters next year and rapid growth thereafter.

7. Wireless Neighborhood Area Networks (WNAN)

In terms of communication range, Wireless Neighborhood Area Networks (WNAN) fall somewhere between WLAN and long-range systems like cellular.[88]Mesh networks such as Wi-Sun and Jupiter Mesh are common supporters of this technology.[89]In certain circumstances, the technology is utilized as an alternative to LPWA/Cellular (for example, in Utilities Field Area Networks), while in others, it is used as a complementary element (for example, for metering deep within where nothing else can reach).

8. Other

Other technologies, such as satellite and unclassified proprietary networks, will continue to play a limited part in the Internet of Things.[90]The integration of many technologies is the key component of the Internet of Things concept. The Internet of Things is powered by the most recent advancements in RFID, smart sensors, communication technologies, Internet protocols, satellite, and several unclassified networks.[91]

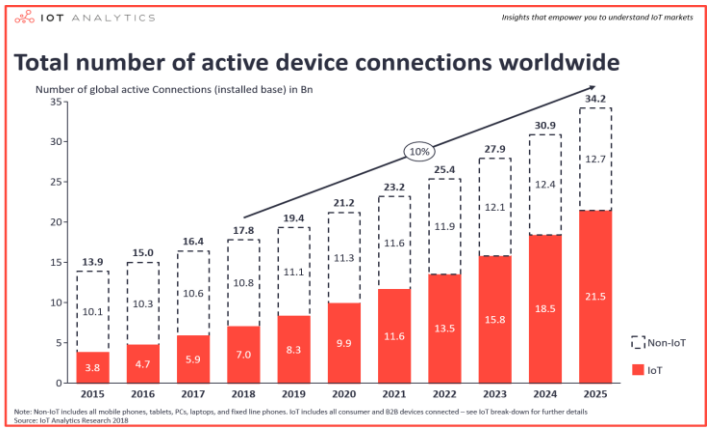

Fig 7: No of active device connected to worldwide[92]

http://dx.doi.org/10.31364/SCIRJ/v11.i7.2023.P0723950

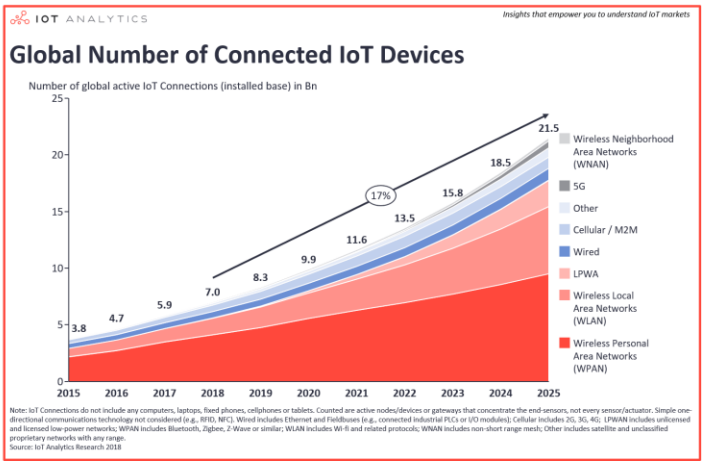

Fig 8: No of connected IoT device to worldwide[93]

The current market sentiment and short-term prospects are quite encouraging. As more data is migrated to the cloud, new IoT applications are released, and analytics become more important,software and platforms are projected to continue to drive the industry. The worldwide Internet of Things market (end-user spending on IoT solutions) is predicted to increase 37% from 2017 to US$151 billion. Because of the market acceleration for IoT (as stated above), those forecasts have been revised upwards, and the whole market is now estimated to reach US$1,567B by 2025.[94]

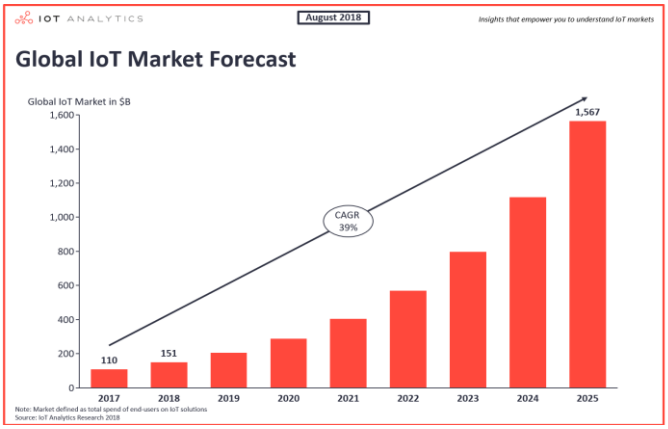

Fig 9: Forecast of global IoT market[95]

According to this projection, data collected by IoT devices has increased over 50 times in just seven years, providing some stunning problems for firms tasked with becoming data stewards. Steve Wilkes, an IoT professional, identifies three major issues that businesses face as a result of the IoT data explosion: [96]

- **Data Integration:** Using freshly generated IoT data alongside other company data sources such as log files, message triggers, and transactional data.[97]

- **Managing Data:** There is now insufficient storage in the globe to address the future data storage needs of IoT devices.[98]Developing a data management procedure to determine what data to retain and how to access it for analysis will be critical for these businesses.

- **Data Security:** IoT devices collect highly personal data from customers and extremely confidential data from businesses. As the last decade's high-profile hacks have proved, where there is data, there will be those attempting to steal it.[99]

http://dx.doi.org/10.31364/SCIRJ/v11.i7.2023.P0723950

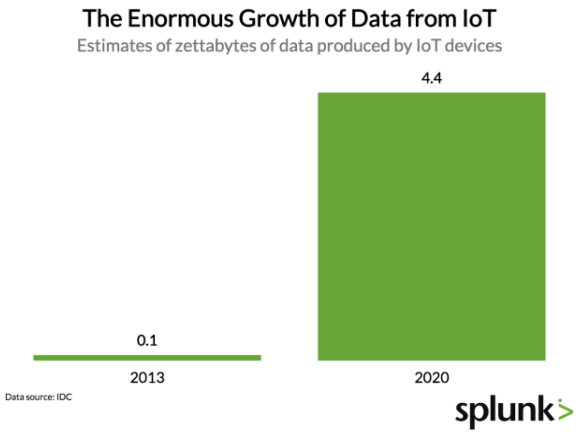

Fig 10: Growth of data from IoT[100]

Privacy and Business Challenges of IoT

The Internet of Things presents a variety of issues to information privacy. Organizations and people might encounter a variety of privacy challenges. The Internet of Things (IoT) is one of the most exciting and active developments in information and communications technology. Although networking technologies have become more prevalent during the last two decades, They were largely used to connect traditional end-user devices including mainframe computers, desktop and laptop computers, smart phones, and tablets. In recent years, a much broader range of devices have been linked to the network. Vehicles, household appliances, medical equipment, electric meters and controllers, streetlights, traffic controls, smart TVs, and digital assistants like Amazon Alexa and Google Home are all part of the list.Analysts predict that there are presently more than 16 billion such devices connected to the network, with this figure expected to grow to more than 22 billion by 2025. As these devices become more widely available, new applications for network technologies have emerged. According to some experts, the Internet of Things might produce up to $1.6 trillion in revenue by 2025.[101]

IoT systems usually connect highly specialized devices designed for specific activities with limited programmability and customization, as opposed to traditional cyber systems, which connect general-purpose computers. Furthermore, unlike the highly centralized method of aggregating storage and processing capacity in huge data centers, IoT devices frequently store and process data in a distributed manner. IoT systems are sometimes known as cyber-physical systems because, unlike exclusively cyber systems, they integrate sensors that collect data from the physical environment.[102]The distributed nature of physical sensors creates both new potential and weaknesses in terms of security and privacy. As a result, we must research how to prepare for the problems offered by the IoT technological environment.

- **The Personal Nature of the Information Collected.** One of the most defining characteristics of the IoT is the increasingly personal nature of the information collected. Others will be able to track cars' movements and operation by linking them to the network.[103]The adoption of smart gadgets in houses can disclose a wealth of information about occupants' routines and ways of life. Connecting medical devices to the network can provide a wealth of sensitive information about people's health care. When various sources of data are combined and predictive analytics are done on the resulting data, interested parties can deduce unexpectedly detailed levels of personal information about consumers who use IoT devices.[104]

- **The Distributed Nature of Data Storage and Processing.** Another variation between IoT systems and traditional systems is the frequency with which data is saved and processed locally. Because many IoT systems have minimal tolerance for delay, they frequently handle numerous data-related operations in the local device rather than relaying all data to a central location, such as a data center. Distributed data storage and processing offers both advantages and downsides. The absence of a single huge repository of data from various users minimizes the presence of a large appealing target with a single attack surface that can attract cyber attackers' attention.[105]At the same time, decentralized storage raises the chance that certain locations will fail to maintain adequate levels of security hygiene on a consistent basis. Distributed storage and processing, as

http://dx.doi.org/10.31364/SCIRJ/v11.i7.2023.P0723950

opposed to depending on a single, hardened point safeguarded by a small cadre of highly experienced security specialists, rely on the diligence of individual users to maintain the system's integrity.

- **Sensors as a New Attack Vector.** Everyone who has used the internet is fully aware of the daily barrage of cyber-attacks that bombard computers. Viruses, worms, trojans, botnets, and other forms of malware, as well as relentless attempts to breach security, have all become all-too-familiar aspects of the internet experience. Because IoT systems must have sensors that collect data from the actual world, they are vulnerable to an altogether new type of attack. Aside from the usual internet risks, overloading a sensor with electromagnetic radiation might lead it to malfunction. Worse, a more sophisticated attacker can provide the sensor precisely calibrated erroneous information, causing the system to perform actions that are not warranted by the actual circumstance. For example, faking location data can lead a connected car to deviate significantly from its intended path.
- **The Possible Corruption of IoT Devices.** The fact that IoT devices are both somewhat programmable and network-connected increases the likelihood that bad actors may attempt to takeover or cause them to malfunction. Unfortunately, most IoT solutions were not developed with security in mind. Many videos on video repositories like YouTube show how sophisticated actors may utilize laptops to take over the driving operations of cars. In the trade press, there have been multiple reports of hostile agents hacking smart refrigerators, televisions, baby monitors, and digital assistants. Perhaps most concerning, many medical equipment have no security built in at all. Many cases show how easily hackers can disable crucial devices like pacemakers and insulin pumps.

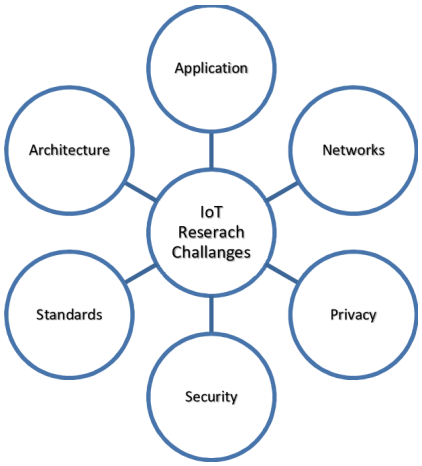

Figure 3: Challenges of IoT related domains[106]

- **Integrating IoT data.** Many solutions are now available that provide analytics on enterprise IoT data. However, this just solves part of the problem.[107]Before IoT, businesses generated enterprise data from log files, message queues, transactional data, and so on. This data is still highly valuable and should be considered alongside IoT data.[108]To get the most out of IoT data, businesses must integrate and correlate it with their existing corporate data, wherever it is kept, so that organizations can make crucial business decisions with a holistic picture.[109] The sheer number of various technologies at work makes merging IoT data with enterprise data difficult.[110]To establish how to merge historical technology with the new generation of IoT devices, businesses must assess their current architecture, which includes databases, ETL and batch, data lakes, messaging systems, and so on. The goal is for all of these technologies to work seamlessly together to meet business requirements.
- **Managing IoT data.** Another major difficulty with IoT is the volume of data generated and the rate at which it is generated. According to a 2017 IDC white paper, the world will generate 160 zettabytes of data by 2025, up from 16 zettabytes presently.[111]According to the estimate, by 2025, approximately 25% of all data would be in real time. 95% of this

http://dx.doi.org/10.31364/SCIRJ/v11.i7.2023.P0723950

25% will be generated via IoT.[112]The kicker is that, with all of this data being generated, only a small fraction of it can be saved (from 3-15%, depending on the source) — there just isn't enough physical storage on the world to retain all of this data. However, IDC recently produced a research on the ever-growing datasphere, or the collective world's data, and the numbers are startling, just like the recent Cisco study.[113]According to IDC, the total amount of data on the planet will increase from 33 zettabytes this year to 175ZB by 2025, representing a 61 percent compound annual growth rate.[114]With the bulk of businesses dealing with IoT data management operations via batch capture, this creates a big quandary over how to engage with data in the future.[115]

- **Securing IoT data.** One of the most significant concerns in the IoT arena is security. As firms continue to adopt connected devices for workplace purposes, monitoring and responding to digital threats becomes increasingly complicated; it's not uncommon for enterprise corporations to have 100+ security systems in place. According to a recent ForeScout analysis, more than half (52%) of questioned security leaders are experiencing significant levels of worry as a result of IoT security. [116]One of the most startling findings was that when asked who should be in charge of safeguarding IoT, 82% of respondents did not have a clear response. The combination of a complicated security technologies industry and an increasing number of connected devices in need of assistance eventually results in gaps throughout the ecosystem.[117]With the level of security demanded by IoT, businesses require a streamlined way to monitoring data and responding quickly and effectively when there is suspicious behavior on the network.

Collection, Use, and Revelation of IoT data

Sensors such as microphones, accelerometers, and thermometers are commonly used to collect data from IoT devices. Data from sensors like these is frequently detailed and precise. This granularity enables for the easy creation of new information via machine learning conclusions and other analysis approaches that can produce outcomes that would not be achievable with coarser data.[118]Furthermore, devices with numerous sensors or devices in close proximity can integrate their data in a process known as sensor fusion, allowing for more accurate and specific inferences that would not be achievable with data from a single sensor.[119] Sensor data concerning a room's temperature, humidity, light level, and CO2 levels, for example, can be integrated to track its occupancy with far greater accuracy than would be feasible with just one of those types of data.[120]

These kinds of inferences can be quite valuable for a variety of purposes, but they can also be extremely personal and surprising. Individuals are often uneasy about corporations inferring information about them from IoT data.[121] Inferences, for example, can be used to create sales pitches by IoT devices such as smart speakers.[122] However, using inferences in this way can drive consumers into making transactional decisions they would not have made otherwise, especially if they occur in a non-retail location such as a home.[123]When data is acquired from persons who have no choice, extra consideration should be given to the objectives for which it is utilized. For example, the energy efficiency provided by smart meters, as well as the ease with which they can be serviced, may force utility companies to discontinue supplying and supporting older energy meters, leaving households with no choice but to adopt smart meters.[124]

Smart energy meters, on the other hand, can expose a wealth of deeply personal information about individuals, including clear information like how frequently they use their washing machine and less obvious information like which television shows they watch.[125]Insurers, advertisers, employers, and law enforcement are likely to find data and conclusions from IoT devices like smart meters to be highly profitable.[126] However, where opting out is not an option, the appropriateness of using and revealing such data must be considered. When personal information is acquired via public IoT ecosystems such as smart cities, it is important to evaluate who will own and control the information, as well as how it will be used. When a public institution, like as a city, collaborates with a private organization to employ IoT devices or services, the city must ensure that personal information is used and released in the best interests of the city's inhabitants.[127] If private firms that provide IoT devices or services have access to IoT data, there is a risk that they would use or disclose personal information for non-public interest objectives such as profiling, targeted advertising, or data brokering.

On a more abstract level, when humans are aware that they are being observed, they adjust their behavior, causing them to self-police and self-discipline.[128] Users restrain and censor themselves online based on who might see their behavior.[129] When smartphones first became widely available, the ability to readily upload information generated a "chilling effect," in which people changed their "offline" behavior in response to the prospect of what may be made available online.[130] It is yet unknown what consequences broad data collecting could have on human behavior and freedom of expression; one potential is that the 'chilling effect' could spread to formerly private locations such as houses.[131]IoT devices can also enable previously online-only behaviors to take place in real settings. Retail businesses, for example, can restrict admission to customers who have made an account by using automated gates that require an app to pass through.[132] AI can be used online to estimate how much a buyer is prepared to spend, allowing a retailer to modify its

http://dx.doi.org/10.31364/SCIRJ/v11.i7.2023.P0723950

rates accordingly.[133] IoT devices might potentially make it easier for brick-and-mortar retailers to undertake comparable price targeting.[134]

The existence of these possible hazards highlights the importance of the IoT industry and academic community developing answers to these concerns. Surprisingly, the redundancy inherent in the distributed structure of the IoT can protect against cyber-attacks, including never-before-seen zero-day attacks. IoT systems can assign a number of other nodes to recheck each node's calculations on a regular basis. If the majority of the other nodes allocated to redo the calculation get a different result, the node being tested is considered to be at fault and disconnected from the system.If the system receives data from the sensor that is outside of that range, it can flag it for further investigation or even disconnect it from the system. scenarios that go beyond mere interference and into much more dangerous scenarios are easily imaginable.

Solution of IoT data

- **A streaming-first architecture.** A streaming-first design is required for IoT data integration, manageability, and security (as well as other enterprise data). We are entering a period in which CPU and memory are finally more cheap for businesses. Rather than capturing data, saving it, and then analyzing it, we may now gain insights from it as soon as it is created by processing and analyzing it in-memory, before it hits disk, in a streaming manner.[135]A vital initial step is the ability to continuously collect data in real time. Companies can use change data capture to transition databases into data streams to incorporate old technologies while reaping the benefits of a modern data architecture.[136]

- Now the question is, how does this help with our primary IoT data management issues? One of the major challenges in integrating IoT data with other company data is effectively integrating outdated technology with modern IoT devices. Companies may now connect and correlate all data assets in any digital environment without working on segregated information by enabling historical technologies to become streaming sources, improving context and time-based decision-making while the data is still active.[137]In addition, real-time data processing and analysis can assist address the data crisis that we are presently experiencing. Filtering, aggregation, and correlation tools performed on data in flight can help determine what is most important to preserve and what can be discarded, reducing the need to store every item of generated data.[138]Because of technological constraints, batch collection was required; dealing with data in real time is the next evolutionary step in data management.[139]A streaming-first approach to IoT security enables you to review logs from many endpoint security systems and varied infrastructure components in real time, allowing you to find flaws or breaches that would not be visible from a single security solution.[140]Whereas separate security technologies hunt for specific exploits, techniques like anomaly detection and pattern matching can examine all streams to discover abnormalities and potential harmful incursions.

- **Towards a streaming future.** After determining that IoT data must become a part of our broader business ecosystem, modern data architecture[141] assists organizations in accelerating their digital transformation projects by:
  - Having the capacity to connect everything from legacy historians and devices to new sensors and breakthroughs like blockchain and AI.[142]Bringing AI into blockchain today opens up new prospects in numerous areas, including health care, life science, financial services, and many more.[143]
  - To operate seamlessly across numerous digital settings, including on-premises, at the edge, and in the cloud. Access to a private cloud is restricted to members of an enterprise and partner networks. In contrast, subscribers in a public cloud have pay-per-use access to standardized resources such as infrastructure, multi-tenant devices, and services. A Multicloud is created by combining on-premise, private cloud, and public cloud components.[144]
  - Handling massive amounts of IoT data intelligently and effectively, storing only what is required while being responsive.[145]We must address the difficulties and resource needs associated with online and offline data processing, storage, and classification analysis.[146]
  - Continuously integrating and correlating IoT and other enterprise data in order to monitor and respond proactively to cyber-security threats.[147]In vital infrastructures, cyber security is critical. Physical and cyber-security domains are frequently seen as different entities, and they have not been designed to collaborate by exchanging data in order to

http://dx.doi.org/10.31364/SCIRJ/v11.i7.2023.P0723950

improve their performance. The two domains are becoming increasingly indistinguishable, and this trait should be utilized.[148]

Managing of IoT devices

Many consumer IoT devices are 'plug and play,' which means they do not need to be configured before usage; they simply function. However, the default settings of IoT devices often provide inadequate privacy and security measures,[149] and many people do not alter their default settings.[150]Furthermore, customers may be unaware that a device is an IoT device. A person upgrading their old refrigerator may be unaware that their new refrigerator is an IoT device and may be unaware of the ramifications. A particularly significant issue for enterprises is that many IoT devices lack centralized management functions, and those that do have those features frequently do not adhere to any particular standard.[151]This means that identical devices may need to be handled separately, and devices from different manufacturers may need to be managed using distinct interfaces. This can present considerable issues when administering large-scale IoT ecosystems. When management choices are not centralized or interoperable, the resources required to manage devices grow in direct proportion to the number and diversity of devices.[152]It would be nearly impossible to manage thousands of devices from dozens of manufacturers individually if an organization had thousands of them.

This problem can also affect consumer gadgets, which are frequently operated by smart-phone apps. If a person owns 20 IoT devices, they may require 20 distinct apps to handle them, thus leaving those devices unmanaged. Again, improperly managed devices can pose privacy and security problems. For example, an unmanaged device within an enterprise may continue to gather personal information when it is no longer required for any purpose. A device, on the other hand, may not receive updates and thus become vulnerable to assault, allowing an attacker to access the rest of an organization's network,[153] or may use the device to disrupt other organizations' networks.[154]In addition, as compared to traditional hardware, IoT devices often give less flexibility for administering or managing devices. For example, the user of an IoT device may be unable to determine when to update the device's software, with that decision being limited to the device's manufacturer. In contrast, it may be difficult to operate a device unless it is updated.

Accountability

Because of the large number of entities that can be involved in an IoT ecosystem, it can be difficult to determine who is or should be held accountable for what. A municipal council, for example, may own an IoT camera, with data relayed via a telecommunications operator, kept by a cloud service provider, and accessed by law enforcement.[155]Each entity in this case bears some level of responsibility for the personal information acquired by the device, and it may be difficult for an individual to know who to contact if they want to request access to the information collected about them by the camera. Because of the nature of IoT devices, it may be impossible for an organization to have complete control over them. Organizations, for example, frequently have little or no control over security and privacy issues associated with communication technologies such as satellite or 5G, because these are typically offered by third-party telecommunications firms.[156]This is also true for cloud services, which can give consumers anywhere from no control to complete control over the security and privacy settings of the services they use.

Organizations frequently have unmanaged 'rogue' IoT devices linked to their networks.[157] Employees can simply connect personal consumer IoT devices like smart speakers or watches to the organization's network. Groups within a company can also install devices such as IoT televisions in meeting rooms or smart appliances in kitchens. These devices can compromise privacy by gathering personal information from unknowing employees, and they can compromise security by providing attackers with an easy entry point into an organization's network.[158] These rogue IoT devices can be difficult for corporations to manage since the people who should be in charge of them are frequently unaware of their presence.

Transparency

Because many IoT devices are inactive, it might be difficult for users to be aware that their personal information is being gathered. Devices in public places can automatically gather information, and it is sometimes necessary for consumers to opt-out if they do not want their information collected. However, because many IoT devices are non-interactive, opt-out models are challenging to deploy. Users may be unaware that their information is being gathered, let alone that they have the option to opt out of it.[159]Furthermore, obtaining appropriate information when consumers want to learn about what personal information a device gathers and how that data is used may be difficult. Because IoT devices usually lack interfaces like screens and input mechanisms like keyboards, it is difficult for IoT devices to deliver explanatory information like privacy policies.[160]

http://dx.doi.org/10.31364/SCIRJ/v11.i7.2023.P0723950

Individuals are frequently prompted to visit to the gadget manufacturer's website or download an app instead. Even though IoT device privacy rules are easily accessible, many of them do not provide enough information on how personal information is collected, utilized, and shared.[161]Organizations trying to exploit intellectual property rights to safeguard the way an IoT device gathers or uses personal information, data acquired by devices, or inferences and insights gained from that data may complicate IoT device transparency even more.[162]Individuals requesting access to personal information acquired by IoT devices face additional obstacles. It is unrealistic to anticipate an IoT device to have only one user and that the user will own the device.[163] This means that an IoT device can gather and keep information about a variety of people and may allow users to access other people's personal information.[164] This is a difficult topic to solve since the lack of interfaces may make it difficult for devices to authenticate users so that they can only access information about themselves.

Present and Future of IoT in Advance Technologies and in Modern Devices

IoT in Advance Technologies. The Internet of Things (IoT) has enormous promise in sophisticated technology and is predicted to alter several sectors and parts of our life. Here are some important upcoming IoT trends and opportunities:

- Increased Connectivity. With the introduction of 5G networks and beyond, IoT devices will see quicker and more dependable connectivity.[165] This will enable real-time data transfer, low-latency connectivity, and seamless integration of IoT devices into diverse ecosystems.
- Edge Computing. Edge computing, in which data processing and analysis take place closer to the source or device, will become increasingly common. By processing data locally, this method minimizes latency, conserves bandwidth, and improves security and privacy.[166] IoT devices will have higher computational capability, allowing them to do advanced analytics and decision-making on the edge.
- Integration of AI. AI and machine learning will play an important role in IoT systems, enabling intelligent data analysis, predictive maintenance, and autonomous decision-making.[167] The large volume of data produced by IoT devices will be used by AI algorithms to draw insights, enhance operations, and improve overall efficiency.[168]
- Smart Cities and Infrastructure. By integrating numerous elements such as transportation systems, energy grids, public services, and infrastructure, IoT will convert cities into smart ecosystems.[169] Smart city efforts will improve traffic management, energy consumption, trash management, and public safety, making cities more sustainable and efficient.[170]
- Industrial IoT (IIoT). The Internet of Things (IoT) will continue to transform industries such as manufacturing, logistics, agriculture, and healthcare. IoT devices installed in industrial equipment will allow for real-time monitoring, remote control, predictive maintenance, and other benefits.[171]
- IoT Security and Its features. The precautions and protections for cloud-connected devices such as home automation, SCADA equipment, security cameras, and any other technology that links directly to the cloud are referred to as IoT security. The automatic cloud connectivity in gadgets distinguishes IoT technology from mobile devices (such as smartphones and tablets).[172]IoT security entails safeguarding devices that were previously poorly designed for data protection and cyber-security. Recent data breaches have demonstrated that IoT security should be a top focus for the majority of manufacturers and developers.[173]Only an integrated solution that provides visibility, segmentation, and protection across the whole network infrastructure, such as a holistic security fabric approach, can meet IoT and security needs.[174]
-
    - Learn. Security solutions with total network visibility may authenticate and classify IoT devices to create a risk profile and assign them to IoT device groups.[175]
    - Segment. IoT devices can be classified into policy-driven groups based on their risk profiles after the organization understands its IoT attack surface.[176]
    - Protect. Policy-driven IoT groups and internal network segmentation enable monitoring, inspection, and policy enforcement based on activity across the infrastructure.[177]

IoT in Modern Devices. The Internet of Things (IoT) is a physical object that connects to the Internet. It may be anything from a fitness tracker to a thermostat, a lock or appliance, or even a light bulb. Consider shoes that monitor our heartbeat and can alert us to potential health issues. We don't have to imagine because smart shoes already exist! The following are some of the most key drives and innovations in the field of IoT in the near future:[178]

- **IoT in healthcare.** The Internet of Things (IoT) is an appealing topic in medicine because it has significant potential for increasing care.[179]However, the application of IoT in healthcare is fraught with a slew of challenges, as well as numerous

http://dx.doi.org/10.31364/SCIRJ/v11.i7.2023.P0723950

vulnerabilities that translate to larger attack surfaces and deeper degrees of damage to both consumers and their trust in health systems as a result of patient-specific data being accessible. Furthermore, when IoT health devices (IoTHDs) are created, a wide variety of assaults are feasible.[180]Understanding the hazards in this new ecosystem requires an understanding of the architecture of IoTHDs, operations, and the social dynamics that may regulate their interactions.[181]It's no wonder that healthcare has been one of the most active areas of IoT development in the previous two years, given all that has happened in the world during the last two years. Of course, it's a broad use case that includes anything from the deployment of cameras in public places to monitor social disengagement to the use of fitness bands and trackers to monitor lifestyles, as well as the development in telemedicine and remote healthcare use.[182] Blood pressure and heart rate monitors, insulin pumps, wheelchairs, defibrillators, and oxygen pumps are all often connected now, allowing them to collect data to assist doctors in better understanding illnesses and patient lifestyles, as well as act autonomously to improve user quality of life.[183]Healthcare IoT devices allow medical workers to obtain data on patients' conditions without exposing themselves to the risks of bringing large groups of potentially contagious people together in close quarters.[184]However, they also allow clinicians to possibly examine, diagnose, and treat a larger number of patients, as well as spread healthcare to locations where actual access to doctors or hospitals is difficult due to remoteness or difficulty of access.[185]

- **Security.** The massive increase in the number of internet-connected devices necessarily means that there are an increasing number of methods for individuals with malicious intent to exploit our technology. The quantity and size of cyber-attacks are increasing year after year - security researchers at Kaspersky estimate 1.5 billion attacks on IoT devices in the first half of 2021 - and this trend is expected to accelerate in 2022. Because IoT devices are not always as secure as traditional devices used to hold sensitive data, such as PCs or smartphones, They act as gateways to our personal networks. Another threat vector derives from the fact that the IoT is made up of "things" - sometimes very little, light objects - that might be lost or stolen, needing an additional layer of protection to prevent unauthorized users from physically possessing your equipment.[186]However, there are hints that manufacturers are cleaning up their act when it comes to shipping gadgets with default passwords, and users are becoming more aware of the risks. Common attacks include denial-of-service (DDOS) attacks, which include overloading systems with connection requests, causing them to malfunction and potentially disclose data, or hijacking computing power from devices, which can then be used to construct botnets that attack other systems or just to mine crypto currencies.[187]IoT is more than simply a security risk; by collecting data on network traffic and usage, linked devices supply fuel for algorithms that forecast and prevent cyber attacks.

- **Edge IoT**. Edge computing and the Internet of Things go hand in hand. Simply expressed, it means designing devices with on-board analytics capabilities so that computation occurs as close to the source of the data being analyzed as possible. This is particularly relevant in the context of cloud computing, when data is collected by essentially "dumb" sensors such as simple cameras or microphones and sent to the cloud for processing.In edge devices, smart sensors such as cameras with computer vision capabilities or microphones with natural language processing functionalities are used.[188]The apparent benefit is that computing may take place considerably faster, and another benefit is that lowering the amount of data transported to and from the cloud lowers network congestion. Another benefit becomes evident when we consider the privacy issues of pervasive IoT; if a gadget is gathering personal data, users can have piece of mind knowing that they can access the insights it provides without it ever leaving their individual custody.[189]The increasing amount of computer power being available in ever smaller and more power-efficient devices, thanks to more efficient battery and user interface designs, is a primary driver here. Edge computing will become an increasingly significant element of the solution when it comes to delivering rapid, secure insights in 2022, as more enterprises continue to seek to hybrid cloud ecosystems to supply IoT services to their consumers.[190]

- **IoT in Business and Industry.** The industrial internet of things (IIoT) is the extension and application of the Internet of Things (IoT) in industrial sectors and applications. The IIoT, with a heavy emphasis on machine-to-machine (M2M) communication, big data, and machine learning, enables industries and companies to improve operational efficiency and dependability. The IIoT includes industrial applications such as robotics, medical devices, and software-defined manufacturing processes.[191]The Internet of Things, sometimes known as the industrial internet, has enormous ramifications for how we create items, deliver services, sell to customers, and give support.[192]Smart factories and logistics facilities are becoming increasingly automated, and the availability of "as-a-service" robots and IoT infrastructure means that more and smaller enterprises will begin to benefit on the opportunities in 2022.[193]By incorporating IoT automation into business models, firms can enjoy enhanced efficiency while acquiring a data-driven insight of their operations and processes.Wearable gadgets, such as augmented reality (AR)[194] and virtual reality (VR)[195] headsets, will be increasingly employed for a variety of applications, including training, equipment maintenance, and process simulation[196] using digital twin approaches. [197]In manufacturing processes, IoT technology comprises sensors installed on machinery to assess performance and enable predictive maintenance - forecasting where faults and breakdowns will occur in order to replace and repair problematic

http://dx.doi.org/10.31364/SCIRJ/v11.i7.2023.P0723950

equipment more efficiently.[198]IoT technologies also include the rapidly expanding field of additive manufacturing methods, such as 3D printing, which will provide increasingly new ways to manufacture and create goods, allow for greater levels of customisation and personalisation, and reduce waste.[199]

- **IoT for Resilient Organizations.** Following the extraordinary upheaval of the last two years, resilience is high on the agenda, and IoT technology offers significant opportunity to construct more resilient and disaster-resistant enterprises. This contains measures such as ensuring a company has the proper abilities to deal with widespread change, such as the transition to home and remote working that occurred in 2020 and 2021, as well as ensuring the company does not lose out owing to the activities of competitors or markets. IoT can improve supply chain resilience by tracking inventory movement between a company, its suppliers, and its consumers, for example, to forecast where delays may occur and give contingencies in the event of global challenges. Monitoring systems that track staff movements around facilities and worker efficiency can be used to assess workplace turnover and predict where shortages, or skills shortages, may indicate a business is headed for issues.[200]IoT solutions meant to help businesses forecast and respond to disruption from a variety of sources will definitely continue to be a source of significant innovation in 2022 and beyond.

- **A fog-based IoT platform.** Using an open Jackson network with feedback, a fog-based IoT platform paradigm with three layers, namely IoT devices, fog nodes, and the cloud, was presented. Individual subsystem performance was examined, and the whole system was evaluated using various input parameters.[201]Analytical results yielded some intriguing performance data. The Internet of Things (IoT) is a network of physical items embedded with sensors, microcontrollers, software, and other technologies that connect to and exchange data with other devices and systems via the Internet.[202]In a typical IoT platform, data is continuously sent, received, and processed in a feedback loop. IoT devices are nonstandard computing devices that can connect wirelessly to a network and transfer data, such as smart TVs, smart sensors, smartphones, and smart security robots. The data is gathered and processed at fog devices.[203]

  Fog computing, also known as edge computing, is an architecture that employs fog nodes to receive tasks from IoT devices and execute a considerable amount of computation, storage, and communication locally, before routing processed data to the cloud for additional processing. Fog computing aims to increase the efficiency of local and cloud data storage. Fog computing can handle huge amounts of data initiated by IoT devices at network edges. Fog computing, also known as a fog-based IoT platform, is often regarded as the finest platform for IoT applications because to properties such as low latency, mobility, and heterogeneity.For example, fog computing decreases the quantity of data that must be transferred to the cloud while also minimizing latency, which is critical for time-sensitive applications such as IoT-based healthcare services.[204]In a fog-based IoT platform for smart buildings, for example, information about the indoor ambience is collected in real-time by IoT devices and transferred to the fog for aggregation and preprocessing before being forwarded to the cloud for storage and analysis. Proper decisions are made and relayed back to the appropriate actuators to establish the ambience or fire an alarm.[205]More research on the main components of fog-based architecture for IoT systems, as well as their implementation methodologies, is covered in.[206] The concepts of fog and cloud are fairly similar, however there are some variances.Let's see the comparison of fog computing and cloud computing:

  - Cloud architecture is centralized, with giant data centers placed all over the world; fog architecture is dispersed, with numerous small nodes located as close to client devices as possible.
  - In cloud computing, data is processed in remote data centers. Fog processing and storage occur at the network's edge, close to the source of information, which is critical for real-time control. In terms of processing power and storage capacity, cloud outperforms fog, but fog is more secure owing to its dispersed architecture.
  - Because of its slower reaction, cloud focuses on long-term deep analysis, whereas fog focuses on short-term edge analysis.
  - Without an Internet connection, a cloud system fails. Because to the use of numerous protocols and standards, fog computing has a substantially lower failure rate. Overall, while both cloud and fog computing offer advantages, it is crucial to highlight that fog computing supplements cloud computing rather than replacing it. Choosing between these two systems is mostly determined by the user's or developer's individual demands and aims.

Fog computing is especially significant in IoT deployment because it frees resource-constrained IoT devices from having to visit the resource-rich cloud on a regular basis.[207]Because IoT tasks such as demanding fog computing resources and service kinds are changing, dynamically supplying fog computing resources to ensure maximum resource usage while meeting a certain constraint will be a difficult challenge. The system modeling and performance analysis for a fog-based IoT platform is a crucial development phase for commercial IoT network deployment in order to maximize the fog computing resources and ensure the required system performance.

http://dx.doi.org/10.31364/SCIRJ/v11.i7.2023.P0723950

Conclusion

The Internet of Things is the unique identification and 'Internetization' of common objects. This enables human contact and control of these 'things' from anywhere in the world, as well as device-to-device interaction without human intervention. The Internet of Things is predicted to grow rapidly, increasingly linking various elements of our life and blurring the borders between the online and offline worlds. Finally, it is a tool that has the potential to benefit everyone. However, as the Internet of Things expands, additional types of personal information will be acquired, as will the overall amount of personal information collected. The way this data is used will have a big impact on how much benefit the IoT brings. Traditional approaches for protecting privacy and properly informing individuals about how their personal information is gathered, utilized, and released are incompatible or inadequate for IoT devices. It is possible that new and inventive solutions that can work with gadgets and services that fundamentally form infrastructure will be required. To gain the benefits of IoT, strong governance, improved accountability, and transparency are also required. Individuals should not have to choose between their privacy and the ease and effectiveness of IoT; both should be available to everyone. Again, in the twenty-first century, we cannot escape using IoT to manage large-scale businesses and the service industry. Furthermore, it was shown that IoT has a considerable impact on decision-making and corporate operation management including daily personal matters.

Traditional methods of safeguarding privacy and adequately educating people about how their personal information is obtained, used, and published are incompatible or inadequate for IoT devices. It is possible that new and inventive solutions that can work with gadgets and services that fundamentally form infrastructure will be required. To gain the benefits of IoT, strong governance, improved accountability, and transparency are also required. Individuals should not have to choose between privacy and the convenience and efficiency of IoT; both should be available to everyone. Again, in the twenty-first century, we cannot escape using IoT to manage large-scale businesses and the service industry. Furthermore, it was shown that IoT has a considerable impact on decision-making and corporate operation management. Smart speakers, which were a small niche a few years ago, are now a ubiquitous presence in homes throughout the world. And, when businesses invest in capital improvements, such assets are increasingly being outfitted with internet connectivity for monitoring, maintenance, and optimization. The Internet of Things revolution has arrived, and it is just growing. That means one massive byproduct of all these linked devices: data. Companies that design and deploy IoT devices will increasingly have to consider not only how to use IoT devices, but also what to do with the data and how to protect it from threats. As a result, in the twenty-first century, IoT will govern every element of human life.

References:

[1]https://www.networkworld.com/article/3207535/what-is-iot-the-internet-of-things-explained.html, accessed on 31 May 2023
[2] https://www.sciencedirect.com/journal/internet-of-things,accessed on 31 May 2023
[3] http://journal.esperg.com/index.php/tijee/article/view/3085, accessed on 31 May 2023
[4]Zhang, H.T.; Park, T.J.; Islam, A.N.; Tran, D.S.; Manna, S.; Wang, Q.; Mondal, S.; Yu, H.; Banik, S.; Cheng, S.; et al. Reconfigurable perovskite nickelate electronics for artificial intelligence, Science, 2022
[5]Costa, L.; Barros, J.P.; Tavares, M. Vulnerabilities in IoT devices for smart home environment. In Proceedings of the 5th International Conference on Information Systems Security and Privacy, ICISSP, Prague, Czech Republic, 23–25 February 2019; SciTePress: Vienna, Austria, 2019; Volume 1
[6] https://www.sciencedirect.com/journal/internet-of-things/vol/22/suppl/C, accessed on 31 May 2023
[7]Apthorpe, N., H.D. Yuxing, R. Dillon, N. Arvind and F. Nick. 2019. Keeping the smart home private with smart(er) IoT traffic shaping, Proceedings on Privacy Enhancing Technologies, 2019 (3): 128–148
[8]https://www.mdpi.com/journal/IoT, accessed on 31 May 2023
[9]Desai, B.C. 2017. Iot: imminent ownership threat. In Proceedings of the 21st International Database Engineering & Applications Symposium, 82–89
[10] What is IoT: The Internet of Things explained | McKinsey.https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-the-internet-of-things, accessed on 31 May 2023
[11]http://it-in-industry.org/index.php/itii/article/view/702,accessed on 31 May 2023
[12] https://imageio.forbes.com/specials-images/imageserve/61b6d5fd475a71fdc7dda795/The-5-Biggest-Internet-Of-Things--IoT--Trends-In-2022/960x0.jpg?format=jpg&width=960, accessed on 31 May 2023
[13]https://www.verdict.co.uk/future-of-iot-benefits-risks/, accessed on 31 May 2023
[14]https://www.fia.uk.com/news/history-of-iot.html, accessed on 31 May 2023
[15]https://toolsense.io/glossary/m2m/, accessed on 1 June 2023
[16]https://www.iiconsortium.org/, accessed on 1 June 2023

http://dx.doi.org/10.31364/SCIRJ/v11.i7.2023.P0723950

[17]https://openconnectivity.org/, accessed on 1 June 2023
[18]Paul Sawers (19 February 2016). "Microsoft, Intel, Samsung, & others launch IoT standards group: Open Connectivity Foundation"
[19]https://www.mdpi.com/2227-9091/9/11/192, accessed on 1 June 2023
[20]https://www.qualcomm.com/5g/what-is-5g, accessed on 1 June 2023
[21]https://www.weforum.org/focus/fourth-industrial-revolution, accessed on 1 June 2023
[22] Ibid
[23] https://link.springer.com/chapter/10.1007/978-3-030-82786-1_11, accessed on 31 May 2023
[24]Lee, I., and K. Lee., The internet of things (IoT): Applications, investments, and challenges for enterprises, Business Horizons, 58 (4): 431–440, 2015
[25]Haghi, M., K. Thurow, and R. Stoll. 2017. Wearable devices in medical internet of things: scientific research and commercially available devices, Healthcare Informatics Research, 23 (1): 4
[26]Motti, V.G., and K. Caine. 2015. Users' privacy concerns about wearables. In Financial Cryptography and Data Security, 231–244. Berlin: Springer
[27] https://www.bbva.ch/en/news/advantages-and-disadvantages-of-smart-cities/, accessed on 31 May 2023
[28]https://currentaffairs.adda247.com/smart-cities-mission-get-june-2023-deadline/,accessed on 31 May 2023
[29]Naeini, P.E., S. Bhagavatula, H. Habib, M. Degeling, L. Bauer, L.F. Cranor, and N. Sadeh. 2017. Privacy expectations and preferences in an iot world. In Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017
[30]Zheng, S., N. Apthorpe, M. Chetty, and N. Feamster. 2018. User perceptions of smart home iot privacy, Proceedings of the ACM on Human-Computer Interaction 2 (CSCW): 200:1–200:20
[31]Lee, H. and A. Kobsa. 2016. Understanding user privacy in internet of things environments. In 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), 407–412. Piscataway: IEEE
[32]https://waterfm.com/georgia-city-moves-forward-with-extensive-water-loss-control-program/,accessed on 31 May 2023
[33]https://waterfm.com/georgia-city-moves-forward-with-extensive-water-loss-control-program/,accessed on 31 May 2023
[34]Bloom, C., J. Tan, J. Ramjohn, L. Bauer. 2017. Self-driving cars and data collection: Privacy perceptions of networked autonomous vehicles. In Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017), Santa Clara, CA, 357–375. San Francisco Bay: USENIX Association
[35] https://medium.com/@baumhedlund/what-you-need-to-know-about-driverless-cars-and-privacy-8720d46e8877, accessed on 31 May 2023
[36]https://www.researchgate.net/figure/IoT-Application-Domains-1_fig4_316277950, accessed on 31 May 2023
[37]https://www.sciencedirect.com/journal/internet-of-things/about/call-for-papers#artificial-intelligence-of-things-in-education, accessed on 31 May 2023
[38]https://journalppw.com/index.php/jpsp/article/view/2585,accessed on 31 May 2023
[39] http://it-in-industry.org/downloads/it-in-industry_Copyright_Form.pdf, accessed on 31 May 2023
[40]https://www.ibm.com/topics/artificial-intelligence, accessed on 31 May 2023
[41]https://ovic.vic.gov.au/privacy/resources-for-organisations/internet-of-things-and-privacy-issues-and-challenges/,
[42]https://www.cloudflare.com/learning/cloud/what-is-the-cloud/, accessed on 31 May 2023
[43] https://www.clark.edu/academics/programs/science-technology-and-engineering/network-tech/index.php#, accessed on 31 May 2023
[44]https://iot.telenor.com/technologies/connectivity/5g/, accessed on 31 May 2023
[45] https://pdfs.semanticscholar.org/c82b/071173279ec5501bc104cae3e3081b520be2.pdf , accessed on 31 May 2023
[46]Rocco Di Taranto et al, 'Location-aware Communications for 5G Networks' (2014) 31(6) IEEE Signal Processing Magazine 201, accessed on 31 May 2023
[47]https://www.researchgate.net/profile/Ali-Semerci-2/publication/334173076.pdf, accessed on 31 May 2023
[48] https://www.sciencedirect.com/science/article/pii/S1877050919304752, accessed on 31 May 2023
[49] https://ieeexplore.ieee.org/abstract/document/7868439, accessed on 31 May 2023
[50]https://ieeexplore.ieee.org/abstract/document/8972389,accessed on 31 May 2023
[51]https://www.bcg.com/publications/2018/four-ways-banks-can-radically-reduce-costs.aspx, accessed on 31 May 2023
[52]https://ieeexplore.ieee.org/abstract/document/8493126, accessed on 31 May 2023
[53] https://link.springer.com/article/10.1140/epjqt/s40507-022-00143-0, accessed on 31 May 2023
[54]Prof. Ahmed Banafa, "Secure and Smart IoT Using Blockchain and AI"
[55]https://www.bbvaopenmind.com/en/technology/digital-world/quantum-computing-trends/, accessed on 31 May 2023
[56]https://www.antino.com/blog/top-9-iot-trends/,accessed on 31 May 2023
[57]https://www.gsma.com/mobileeconomy/wp-content/uploads/2018/02/The-Mobile-Economy-Global-2018.pdf
[58] https://ieeexplore.ieee.org/abstract/document/8234580, accessed on 31 May 2023
[59]Taeihagh, Araz; Lim, Hazel Si Min, "Governing autonomous vehicles: emerging responses for safety, liability, privacy, cybersecurity, and industry risks", Transport Reviews, 39 (1), 2 January 2019

http://dx.doi.org/10.31364/SCIRJ/v11.i7.2023.P0723950

[60]https://link.springer.com/book/10.1007/978-3-319-90403-0,accessed on 31 May 2023
[61]https://aws.amazon.com/what-is/digital-twin/,accessed on 31 May 2023
[62] Prof. Ahmed Banafa, "Blockchain Technology and Applications"
[63] https://ieeexplore.ieee.org/abstract/document/9083958, accessed on 31 May 2023
[64] https://www.fierceelectronics.com/electronics/fundamentals-what-edge-device, accessed on 31 May 2023
[65] https://www.epsu.org/sites/default/files/article/files/GDPR_FINAL_EPSU.pdf, accessed on 31 May 2023
[66]Wünderlich N.V., F.V. Wangenheim, M.J. Bitner, High tech and high touch: a framework for understanding user attitudes and behaviors related to smart interactive services, Journal of Service Research, 16 (1) (2013
[67]https://www.bbvaopenmind.com/en/technology/digital-world/, accessed on 31 May 2023
[68] https://ieeexplore.ieee.org/abstract/document/9277862,accessed on 31 May 2023
[69]https://www.bbvaopenmind.com/en/technology/digital-world/trends-iot-2023/,accessed on 31 May 2023
[70]https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/inspired/smart-cities,
[71]https://www.antino.com/blog/top-9-iot-trends/#IoT-Security-1,
[72]https://www.antino.com/blog/top-9-iot-trends/#Metaverse-1, accessed on 31 May 2023
[73] Khurana,Ajeet (25 November 2019). "Did You Know That There Are 4 Types of Ecommerce?", The Balance Small Business, Dotdash, Archived from the original on 22 January 2021, accessed on 31 May 2023
[74]https://priceonomics.com/the-iot-data-explosion-how-big-is-the-iot-data/, accessed on 31 May 2023
[75]https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/, accessed on 31 May 2023
[76]https://etzq49yfnmd.exactdn.com/wp-content/uploads/2022/03/image4-11.png?strip=all&lossy=1&resize=640%2C480&ssl=1,accessed on 31 May 2023
[77]https://etzq49yfnmd.exactdn.com/wp-content/uploads/2022/03/image6-4.png?strip=all&lossy=1&resize=640%2C480&ssl=1,accessed on 31 May 2023
[78]https://etzq49yfnmd.exactdn.com/wp-content/uploads/2022/03/image5-10.png?strip=all&lossy=1&resize=640%2C566&ssl=1, accessed on 31 May 2023
[79]https://www.techtarget.com/iotagenda/tip/Top-8-IoT-applications-and-examples-in-business,accessed on 31 May 2023
[80]https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3906607, accessed on 31 May 2023
[81]https://ieeexplore.ieee.org/abstract/document/9319251, accessed on 31 May 2023
[82] https://ieeexplore.ieee.org/abstract/document/7452560, accessed on 31 May 2023
[83]https://ieeexplore.ieee.org/abstract/document/8108501, accessed on 31 May 2023
[84]https://ieeexplore.ieee.org/abstract/document/7945515, accessed on 31 May 2023
[85]https://ieeexplore.ieee.org/abstract/document/8326498, accessed on 31 May 2023
[86] https://www.ccdcoe.org/uploads/2019/03/CCDCOE-Huawei-2019-03-28-FINAL.pdf, accessed on 31 May 2023
[87]https://ieeexplore.ieee.org/abstract/document/8732436, accessed on 31 May 2023
[88]https://ieeexplore.ieee.org/abstract/document/6879315, accessed on 31 May 2023
[89] https://www.theseus.fi/bitstream/handle/10024/749993/Giao_Phung_S.pdf?sequence=2, accessed on 31 May 2023
[90]https://digitalrepository.unm.edu/ece_etds/450/, accessed on 31 May 2023
[91]https://ieeexplore.ieee.org/abstract/document/7589556, accessed on 31 May 2023
[92]https://h9e3r9w2.rocketcdn.me/wp/wp-content/uploads/2018/08/Number-of-global-device-connections-2015-2025-Number-of-IoT-Devices.png, accessed on 31 May 2023
[93]https://h9e3r9w2.rocketcdn.me/wp/wp-content/uploads/2018/08/Number-of-IoT-devices-worldwide-2015-2025-Aug-2018-min.png, accessed on 31 May 2023
[94] Op Cit
[95]https://h9e3r9w2.rocketcdn.me/wp/wp-content/uploads/2018/08/Global-IoT-Market-Forecast-2017-2025.png, accessed on 31 May 2023
[96]https://priceonomics.com/the-iot-data-explosion-how-big-is-the-iot-data/, accessed on 31 May 2023
[97]Structured authoring for AR-based communication to enhance efficiency in remote diagnosis for complex equipment, Advanced Engineering Informatics, 2020,
[98]F. Lamberti, F. Manuri, A. Sanna, G. Paravati, P. Pezzolla, Challenges, Opportunities, and Future Trends of Emerging Techniques for Augmented Reality-Based Maintenance, IEEE Trans. Emerg. Top. Comput., 2 (4), 2015
[99] A. Sanna, F. Manuri, F. Lamberti, S. Member, G. Paravati, and P. Pezzolla, "Using Handheld Devices to Support Augmented Reality-based Maintenance and Assembly Tasks," IEEE Int. Conf. Consum. Electron. Using, pp. 178-179, 2015
[100]https://etzq49yfnmd.exactdn.com/wp-content/uploads/2022/03/image1-15.png?strip=all&lossy=1&resize=640%2C480&ssl=1, accessed on 31 May 2023
[101]https://www.cigionline.org/articles/emerging-internet-things/, accessed on 31 May 2023
[102]Bertino, E., and N. Islam. 2017. Botnets and internet of things security, *Computer* 50 (2): 76–79
[103]https://portal.facebook.com/privacy, accessed on 31 May 2023

http://dx.doi.org/10.31364/SCIRJ/v11.i7.2023.P0723950

[104]https://www.businessinsider.com/how-to-stop-google-home-from-listening-to-me, accessed on 31 May 2023
[105] https://www.businessinsider.com.au/tracking-employees-with-productivity-sensors-2013-3?r=US&IR=T, accessed on 31 May 2023
[106]https://www.researchgate.net/figure/Domains-of-IoT-research-challenges-and-much-more-But-still-there-are-some-research_fig2_323949379, accessed on 01 June 2023
[107]https://www.techtarget.com/iotagenda/blog/IoT-Agenda/Addressing-the-fundamental-challenges-to-IoT-data-management, accessed on 01 June 2023
[108]https://www.sciencedirect.com/science/article/pii/S2212827116309830, accessed on 01 June 2023
[109]https://www.manufacturingtomorrow.com/tag/iot, accessed on 01 June 2023
[110]https://www.techtarget.com/iotagenda/tip/IoT-integration-challenges-require-strategy-vendor-support, accessed on 01 June 2023
[111]https://www.cisco.com/c/dam/en_us/services/downloads/cms-white-paper.pdf, accessed on 01 June 2023
[112]https://solutionsreview.com/data-management/idc-data-creation-to-reach-163-zettabytes-by-2025/, accessed on 01 June 2023
[113]https://www.networkworld.com/article/3323063/cisco-predicts-nearly-5-zettabytes-of-ip-traffic-per-year-by-2022.html, accessed on 02 June 2023
[114]https://www.networkworld.com/article/3325397/idc-expect-175-zettabytes-of-data-worldwide-by-2025.html, accessed on 02 June 2023
[115] M. Hincapié, A. Caponio, H. Rios, and E. González Mendívil, "An introduction to Augmented Reality with applications in aeronautical maintenance," Int. Conf. Transparent Opt. Networks
[116]https://www.forescout.com/security-disclosure/, accessed on 02 June 2023
[117]https://www.techtarget.com/iotagenda/blog/IoT-Agenda/Addressing-the-fundamental-challenges-to-IoT-data-management, accessed on 02 June 2023
[118]https://www.researchgate.net/publication/221518517_Privacy_risks_emerging_from_the_adoption_of_innocuous_wearable_sensors_in_the_mobile_environment, accessed on 02 June 2023
[119]https://www.researchgate.net/publication/2985118_An_Introduction_to_Multisensor_Data_Fusion, accessed on 31 May 2023
[120]Nashreen Nesa and Indrajit Banerjee, 'IoT-based sensor data fusion for occupancy sensing using Dempster–Shafer evidence theory for smart buildings' (2017) 4(5) IEEE Internet of Things Journal , 2017
[121]https://www.usenix.org/system/files/conference/soups2017/soups2017-naeini.pdf, accessed on 02 June 2023
[122] https://thenextweb.com/artificial-intelligence/2018/10/15/amazons-new-patent-will-allow-alexa-to-detect-your-illness/, accessed on 02 June 2023
[123]https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id:%22legislation/billhome/r4335%22,
[124]: http://scholarship.kentlaw.iit.edu/cgi/viewcontent.cgi?article=3780&context=cklawreview, accessed on 31 May 2023
[125]Miro Enev et al, 'Televisions, Video Privacy, and Powerline Electromagnetic Interference' (2011) Proceedings of the 18th ACM Conference on Computer and Communications Security 537
[126]United States National Institute of Standards and Technology, 'Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid' (2010)
[127] https://www.sciencedirect.com/science/article/pii/S0740624X16300818, accessed on 31 May 2023
[128]Michel Foucault, 'Discipline and Punish' (1975); Ivan Manokha, 'Surveillance, Panopticism, and Self-Discipline in the Digital Age' (2018) 16(2) Surveillance & Society 219
[129]https://www.aaai.org/ocs/index.php/ICWSM/ICWSM13/paper/viewFile/6093/6350, accessed on 31 May 2023
[130]Ben Marder et al, 'The extended "chilling" effect of Facebook: The cold reality of ubiquitous social networking' (2016) 60 Computers in Human Behavior 582, 2016
[131]https://scholar.law.colorado.edu/cgi/viewcontent.cgi?article=2222&context=articles, accessed on 31 May 2023
[132]Andria Cheng, 'New York Proves Amazon Go Works, And An Even Bigger Rollout Is Only A Matter Of Time' (26 June 2019) Forbes
[133] https://one.oecd.org/document/DAF/COMP(2018)13/en/pdf, accessed on 31 May 2023
[134] https://www.aclu.org/blog/speakeasy/invasion-data-snatchers-big-data-and-internet-things-means-surveillance-everything, accessed on 31 May 2023
[135]The Effects of Physical Coherence Factors on Presence in Extended Reality (XR), International Journal of Human Computer Studies,2023
[136]Does imagination compensate for the need for touch in 360-virtual shopping?International Journal of Information Management,2023
[137]An Introduction to the Special Issue "Virtual Reality in Marketing": Definition, Theory and Practice**,** Journal of Business Research, Volume 100, 2019
[138]K. Rose, S. Eldridge, L. Chapin, The internet of things: An overview, understanding the issues and challenges of a more., 2018
[139]A survey of industrial augmented reality**,** Computers & Industrial Engineering, Volume 139, 2020
[140]G. Fortino, M. Ganzha, C. Palau, M. Paprzycki, Interoperability in the internet of things, 2016
[141]https://www.techtarget.com/iotagenda/Ultimate-IoT-implementation-guide-for-businesses, accessed on 31 May 2023

http://dx.doi.org/10.31364/SCIRJ/v11.i7.2023.P0723950

[142]https://crypto.com/university/blockchain-and-ai, accessed on 31 May 2023
[143]https://www.ibm.com/topics/blockchain-ai, accessed on 31 May 2023
[144]https://www.ibm.com/cloud/blog/cloud-at-the-edge, accessed on 31 May 2023
[145]https://www.wirecube.com/cases/high-volume-iot-data-processing/, accessed on 31 May 2023
[146]El-Sayed H., Edge of things: The big picture on the integration of edge, IoT and the cloud in a distributed computing environment, IEEE Access, 2018
[147]Setola, R.; Luiijf, E.; Theocharidou, M. Critical infrastructures, protection and resilience. In Managing the Complexity of Critical Infrastructures; Springer: Berlin/Heidelberg, Germany, 2016
[148]Sreenu, G.; Durai, M.S. Intelligent video surveillance: A review through deep learning techniques for crowd analysis. J. Big Data 2019
[149]Meredydd Williams et al, 'The perfect storm: The privacy paradox and the Internet-of-Things' (2016) 11th International Conference on Availability, Reliability and Security 644, available at: https://kar.kent.ac.uk/67485/1/ARES2016-author-final.pdf, accessed on 31 May 2023
[150] https://firstmonday.org/ojs/index.php/fm/article/view/3086/2589, accessed on 31 May 2023
[151]Katie Boeckl et al, 'Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks' (2018) National Institute of Standards and Technology
[152] GSMA, 'Protecting Privacy and Data in the Internet of Things' (2019), available at: https://www.gsma.com/iot/wp-content/uploads/2019/02/Protecting-Privacy-big-data-report-gsma.pdf, accessed on 31 May 2023

[153] Michael J. Covington and Rush Carskadden, 'Threat Implications of the Internet of Things' (2013) 5th International Conference on Cyber Conflict 1, available at: https://ccdcoe.org/uploads/2018/10/1_d1r1s6_covington.pdf, accessed on 31 May 2023
[154]https://www.imperva.com/blog/malware-analysis-mirai-ddos-botnet/, accessed on 31 May 2023
[155] Meredydd Williams et al, 'The perfect storm: The privacy paradox and the Internet-of-Things' (2016) 11th International Conference on Availability, Reliability and Security 644, available at: https://kar.kent.ac.uk/67485/1/ARES2016-author-final.pdf, accessed on 31 May 2023
[156]Sandra Spickard Prettyman et al, 'Privacy and security in the brave new world: The use of multiple mental models' (2015) International Conference on Human Aspects of Information Security, Privacy, and Trust 260
[157]: https://www.infoblox.com/company/news-events/press-releases/infoblox-research-finds-explosion-of-personal-and-iot-devices-on-enterprise-networks-introduces-immense-security-risk/, accessed on 31 May 2023
[158]https://www.businessinsider.com.au/hackers-stole-a-casinos-database-through-a-thermometer-in-the-lobby-fish-tank-2018-4, accessed on 31 May 2023
[159]https://www.ftc.gov/system/files/documents/cases/150902nomitechcmpt.pdf, accessed on 31 May 2023
[160]Yu Tianlong et al, 'Handling a trillion (unfixable) flaws on a billion devices: Rethinking network security for the Internet-of-Things' (2015) Proceedings of the 14th ACM Workshop on Hot Topics in Networks 5, available at: https://www.cs.cmu.edu/~srini/papers/2015.Yu.hotnets.pdf,accessed on 31 May 2023
[161] https://www.oaic.gov.au/updates/news-and-media/privacy-commissioners-reveal-the-hidden-risks-of-the-internet-of-things/, accessed on 31 May 2023
[162]https://www.ipaustralia.gov.au/sites/default/files/ip_australia_and_the_future_of_intellectual_property.pdf,accessed on 31 May 2023
[163]https://www.researchgate.net/publication/226218872_Identities_in_the_Future_Internet_of_Things,accessed on 31 May 2023
[164]https://www.franziroesner.com/pdf/geeng-smarthomes-chi19.pdf,accessed on 31 May 2023
[165] https://ieeexplore.ieee.org/abstract/document/8471687, accessed on 31 May 2023
[166] https://ieeexplore.ieee.org/abstract/document/7796149, accessed on 31 May 2023
[167] P. Lynggaard, "Artificial intelligence and internet of things in a "smart home" context: A distributed system architecture," PhD Dissertation, Aalborg University Copenhagen, 2013
[168] S. D. T. Kelly, N. K. Suryadevara, and S. C. Mukhopadhyay, "Towards the implementation of IoT for environmental condition monitoring in homes," IEEE Sensors Journal, vol. 13, no. 10, October 2013
169A.S. Elmaghraby et al., Cyber security challenges in smart cities, Safety, security and privacy, Journal of Advanced Research, 2014
[170]M.M. Rathore et al., Urban planning and building smart cities based on the internet of things using big data analytics, Computer Networks, 2016
[171] https://link.springer.com/chapter/10.1007/978-3-030-57328-7_12, accessed on 31 May 2023
[172] https://ieeexplore.ieee.org/abstract/document/8769560, accessed on 30 May 2023
[173] https://ieeexplore.ieee.org/abstract/document/8386824, accessed on 30 May 2023
[174]https://core.ac.uk/download/pdf/145044628.pdf, accessed on 31 May 2023
[175]https://ieeexplore.ieee.org/abstract/document/7789475, accessed on 31 May 2023

http://dx.doi.org/10.31364/SCIRJ/v11.i7.2023.P0723950

[176]M. Abomhara et al., Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks, Journal of Cyber Security and Mobility, 2015
[177]https://scholarworks.rit.edu/theses/782/, accessed on 31 May 2023
[178]https://www.forbes.com/sites/bernardmarr/2021/12/13/the-5-biggest-internet-of-things-iot-trends-in-2022/?sh=6935f9865aba, accessed on 31 May 2023
[179]https://www.mdpi.com/2624-831X/4/2/9, accessed on 31 May 2023
[180]https://www.mdpi.com/2624-831X/4/2/9,accessed on 31 May 2023
[181]Thomasian, N.M.; Adashi, E.Y. Cybersecurity in the internet of medical things. Health Policy Technol. 2021
[182]Valanarasu, M.R. Smart and secure IoT and AI integration framework for hospital environment. J. ISMAC 2019
[183]Karthick, R.; Ramkumar, R.; Akram, M.; Kumar, M.V. Overcome the challenges in bio-medical instruments using IOT—A review. Mater. Today Proc. 2021
[184] Ibid
[185]Al-Husainy, M.A.F.; Al-Shargabi, B.; Aljawarneh, S. Lightweight cryptography system for IoT devices using DNA. Comput. Electr. Eng. 2021
[186]Mueller, S. Facing the 2020 pandemic: What does cyberbiosecurity want us to know to safeguard the future? Biosaf. Health 2021
[187]Amiri, A.; Shekarchizadeh, M.; Esfahani, A.R.S.; Masoud, G.H. Bio-Cyber Threats and Crimes, the Challenges of the Fourth Industrial Revolution. Bioethics 2021
[188]Yadav, J.; Sangwan, S., Dynamic Offloading Framework in Fog Computing, Int. J. Eng. Trends Techno, 2022
[189]https://link.springer.com/chapter/10.1007/978-3-030-82786-1_11, accessed on 30 May 2023
[190] https://ieeexplore.ieee.org/abstract/document/9437171, accessed on 30 May 2023
[191]https://www.trendmicro.com/vinfo/us/security/definition/industrial-internet-of-things-iiot, accessed on 31 May 2023
[192]Taneja, M.; Davy, A. Resource aware placement of data analytics platform in fog computing, Procedia Comput. Sci, 2016
[193]'The persuasion effects of virtual reality (VR) and augmented reality (AR) video advertisements: A conceptual review', 2023, Journal of Business Research
[194]https://www.ibm.com/topics/what-is-a-digital-twin, accessed on 31 May 2023
[195] Mainelli, T. (2017). Worldwide augmented and virtual reality hardware forecast update, 2017
[196]M. Gulati, V. Anand, S.K. Salaria, N. Jain, S. Gupta, Computerized implant-dentistry: advances toward automation, J Indian Soc Periodontol- 1, 2015
[197]https://www.sciencedirect.com/science/article/pii/S1607551X1730815X, accessed on 31 May 2023
[198]Abasi-amefon, O.A.; Matulevičius, R.; Tõnisson, R. Security Risk Estimation and Management in Autonomous Driving Vehicles. In Proceedings of the International Conference on Advanced Information Systems Engineering, Melbourne, VIC, Australia, 28 June–2 July 2021
[199]J.H. Kietzmann *et al.*, Disruptions, decisions, and destinations: Enter the age of 3-D printing and additive manufacturing, Business Horizons, 2015
[200]Zuiderwijk, A.; Chen, Y.C.; Salem, F. Implications of the use of artificial intelligence in public governance: A systematic literature review and a research agenda, Gov. Inf. Q., 2021
[201]Iorga, M.; Goren, N.; Feldman, L.; Barton, R.; Martin, M.; Mahmoudi, C. Fog Computing Conceptual Model, Natl. Inst. Stand. Technol. Spec. Pub., 2018
[202]Sun, Y.; Song, H.; Jara, A.J.; Bie, R. Internet of Things and Big Data Analytics for Smart and Connected Communities, IEEE Access, 2016
[203]Shafiq, M.; Gu, Z.; Cheikhrouhou, O.; Alhakami, W.; Hamam, H., The Rise of Internet of Things: Review and Open Research Issues Related to Detection and Prevention of IoT-Based Security Attacks, Wirel. Commun. Mob. Comput., 2022
[204]Bonomi, F.; Milito, R.; Zhu, J.; Addepalli, S. Fog computing and its role in the internet of things. In Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing, Helsinki, Finland, 17 August 2012
[205]Alsuhli, G.; Khattab, A. A Fog-based IoT Platform for Smart Buildings. In Proceedings of the 2019 International Conference on Innovative Trends in Computer Engineering (ITCE), Aswan, Egypt, 2–4 February 2019
[206]Sadatacharapandi, T.P.; Padmavathi, S. Survey on Service Placement, Provisioning, and Composition for Fog-Based IoT Systems, Int. J. Cloud Appl. Comput., 2022
[207]Zhai, Z.; Xiang, K.; Zhao, L.; Cheng, B.; Qian, J. IoT-RECSM-Resource-Constrained Smart Service Migration Framework for IoT Edge Computing Environment, Sensors, 2020

About Author

http://dx.doi.org/10.31364/SCIRJ/v11.i7.2023.P0723950

Khandakar Akhter Hossain, PhD is a professor/researcher/Examiner at NAME of BUET. Email: khandokarhossain1969@gmail.com

http://dx.doi.org/10.31364/SCIRJ/v11.i7.2023.P0723950