Fall 2022

IoT: The Revolutionary Tech And Its Challenges In The Modern Technological Landscape

Suhaib Riyasat Ali

IOT: THE REVOLUTIONARY TECH AND ITS CHALLENGES IN THE MODERN TECHNOLOGICAL LANDSCAPE.

By

Suhaib Riyasat Ali
B.E., IT., Osmania University, 2019

THESIS

Submitted in partial fulfillment of the requirements

For the Degree of Master of Science,
With a Major in Information Technology

Governors State University
University Park, IL 60484

2022

Table of Contents

Abstract

The Internet of Things is a new paradigm that has transformed the conventional approach to technology. The Internet of Things is responsible for such developments as the smart city, home automation, prevention of pollution, energy efficiency, and industrial automation. In order to improve technology by means of the IoT, a significant amount of important research studies and analyses have been carried out. In spite of this, there continue to be a number of roadblocks that need to be resolved before the Internet of Things can live up to its full promise. These difficulties and challenges need to be evaluated from a variety of perspectives regarding the Internet of Things, including challenges and issues. The paper provides a comprehensive discussion from both a technical and a social point of view. The paper explores a variety of IoT difficulties and essential concerns, as well as architectural considerations and significant application fields.

IoT: The revolutionary tech and its challenges in the modern technological landscape

Introduction

The term "internet of things" refers to the business processes and applications of sensed data, information, and content that are created from a globally networked environment by means of connected devices that already exist in the architecture of the internet (Karale, 2021). The number of gadgets that are linked to the internet grows by the hundreds every single day. Because of the exponential increase in the number of devices that are linked to the Internet and the widespread use of Internet of Things (IoT) technology across all business sectors, thorough research and development of technical standards has become necessary. The success of the Internet of Things is primarily reliant on the development of global standards that are interoperable both within and across application domains. For instance, in order to design business solutions that are both cost-effective and allow collaboration across multiple applications, a common language (vocabulary) and a standard reference architecture are required as prerequisites. These architectures encompass a broad variety of subject areas. The primary purpose of this review is to provide a comprehensive discussion from both a technical and a social point of view (Nižetić et al., 2020). The paper explores a variety of IoT difficulties and essential concerns, as well as architectural considerations and significant application fields. Additionally, the article sheds light on previously published works and demonstrates how those works have contributed to various parts of the Internet of Things.

Literature Review

The word 'internet' is being expanded thanks to associated technological developments such as mobile networks, sensor networks, and the like, which are all part of the Internet of Things. The "Internet" connects everything, and all of these "things" may interact with one another via this network. These sorts of systems have the potential to be very flexible and scalable, but they also run the danger of having security issues. It seems that this technology will not be able to be realistically applied in the near future since there are numerous concerns over its widespread implementation, and because it does not provide suitable remedies for the newly given dangers (Atlam & Wills, 2020). The participation of Internet of Things–based systems in many facets of human life, as well as the myriad of technologies involved in the movement of data between embedded devices, rendered it complicated and gave birth to a number of concerns and obstacles. These problems provide a challenge for the creators of IoT in today's highly sophisticated society of smart technology. Challenges and the need for more sophisticated Internet of Things systems are rising in tandem with the advancement of technology. Therefore, developers working on the Internet of Things need to anticipate new problems and work to find solutions for such problems (Panchiwala & Shah, 2020).

The Internet of Things is fraught with several dangers, including cyberattacks, hazards, and vulnerabilities, which make privacy and data protection among its most pressing concerns and difficult problems to solve. Insufficient authorization and authentication, insecure software, firmware, and web interfaces, and inadequate transport layer encryption are the problems that give rise to concerns about privacy at the device level. When it comes to developing trust in Internet of Things systems, concerns of security and privacy are highly crucial characteristics that need to be

taken into consideration. In order to forestall security breaches and assaults, the Internet of Things architecture has to include security procedures at each of its levels (Patel, Vyas & Pandya, 2019).

Interoperability is another aspect to consider. Interoperability refers to the degree to which various Internet of Things devices and systems are able to successfully exchange information with one another. This information sharing does not depend on the already installed software or hardware in any way. The problem of interoperability is caused by the diverse character of the many technologies and solutions that are employed in the development of the Internet of Things (IoT) (Zalewski, 2019). The ethics, the legislation, and the regulatory rights provide another challenge for IoT developers. There are some laws and regulations in place to keep standards and moral values intact and to stop individuals from acting in a way that goes against them. The sole difference between ethics, which are the standards that people believe in, and laws, which are particular limits chosen by the government, is that ethics are standards that people believe in while laws are certain restrictions imposed by the government (Karale, 2021). Another crucial component of the Internet of Things is its quality of service, or QoS. The quality of service (QoS) is a metric that may be used to assess the quality, efficiency, and performance of Internet of Things (IoT) devices, systems, and architecture (Zalewski, 2019).

Architecture of IoT in Business settings

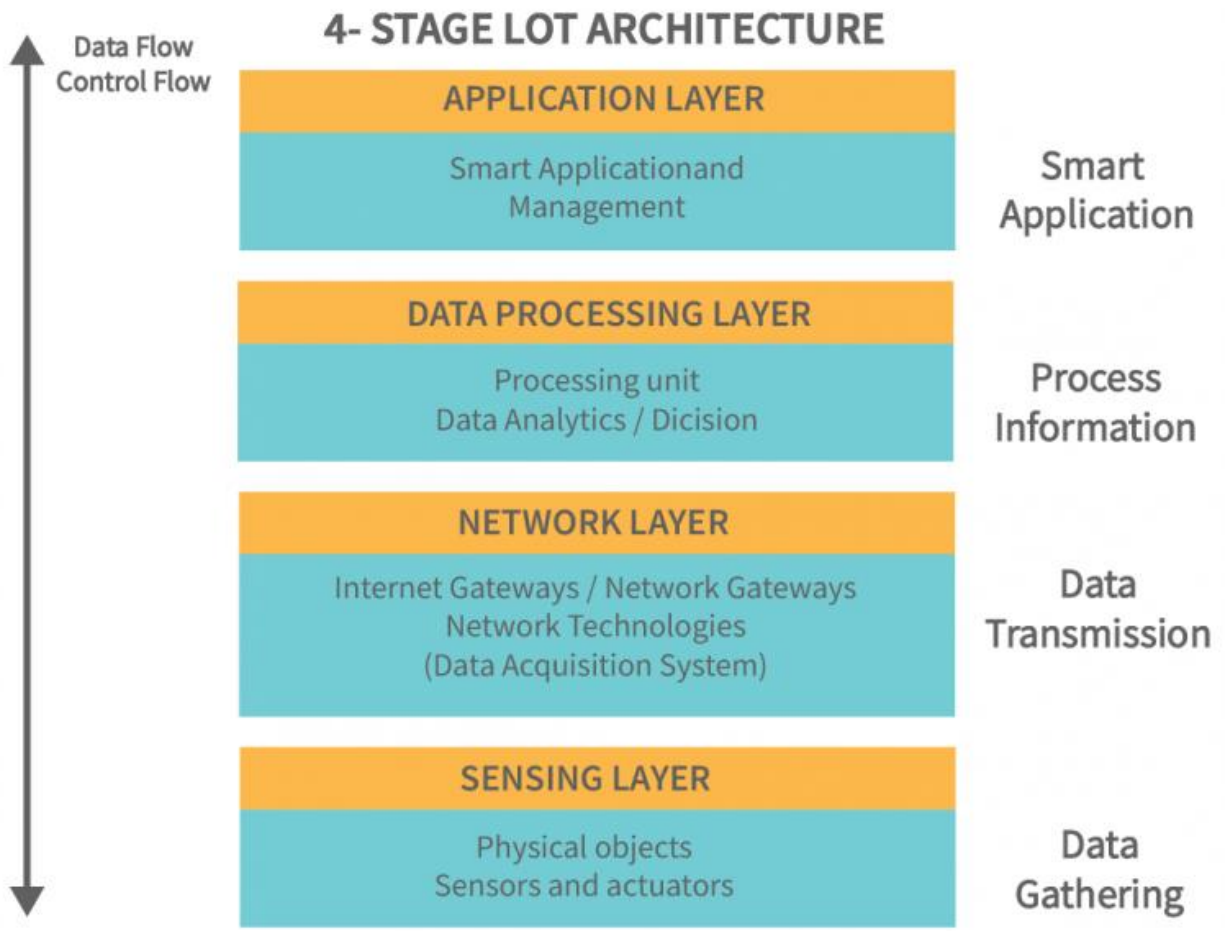
The Internet of Things, also known as IoT architecture, refers to the intricate configuration of components that are employed in IoT network infrastructure. Cloud services, sensors, actuators, protocols, and layers are all components that fall under this category. In most cases, it is partitioned

into layers, which gives administrators the opportunity to examine, monitor, and generally maintain the system's integrity by ensuring that it is not compromised (Khanna & Kaur, 2020) . The architecture of the internet of things consists of a four-step process that includes the flow of data from devices that are connected to sensors, to a network, and then eventually toward the cloud for the sake of processing, analysis, and storage. It is anticipated that the Internet of Things will continue growing as a result of the substantial amount of work being carried out in terms of research and development (Perera et al., 2013). This is due to the spike in the adoption of IoT across a variety of industries.

On the other hand, from a purely technological standpoint, the architectural design of the internet of things is composed of five essential layers that define all of the functionality of IoT systems. The perception layer, the network layer, the middleware layer, the application layer, and the business layer make up these layers. A perception layer is present at the foundation of the internet of things architecture (Abdullah, Kaur, & Biswas, 2020). This layer is composed of many chips, sensors, barcodes, and other physical things that are linked to one another through a network.

The information that is gathered by these components is then sent up to the network layer, which is the primary role of these elements. The information is sent to the system for data processing from the perception layer through the network layer, which acts as a transmission channel for the information. This information may be sent through any wired or wireless method available, such as a link to the internet or even a Bluetooth device (Patel, Vyas & Pandya, 2019).

The middleware layer is the next step up in the stacking order. The primary responsibility of this layer is to analyze the data that has been sent down from the network level and to arrive at conclusions and recommendations based on the findings of ubiquitous computing. After that, the application layer makes use of this processed information in order to perform global device management (Assiri & Almagwashi, 2018). There exists a business layer at the very base of the architecture, and it is responsible for controlling the Internet of Things as a whole, together with all of its services and applications. The information and data that have been sent down from the application level are visualized and used by the business layer, which then plans future objectives and strategies based on this information (Perera et al., 2013).



Layers in IoT Architecture in Normal Settings

The first layer in this situation is the one that deals with perception or sensing. The "things" or endpoint devices that act as a bridge between the digital and physical worlds are what make up the initial layer of any Internet of Things (IoT) system. The term "perception" refers to the physical layer of the network, which is composed of actuators and sensors that are able to collect, accept, and analyze data that is sent across the network. Both wireless and cable connections may be used to link actuators and sensors together in a system. The design does not place any restrictions on the components' potential uses or where they may be located (Jabraeil Jamali et al., 2020).

The network layer makes up the second layer. These layers provide a summary of how the data is transported from one part of the program to another. This layer comprises Data Acquiring Systems as well as gateways to the Internet and other networks. The functions of data aggregation and data conversion are carried out by the system. It is essential to both communicate and process the information that has been gathered by the sensor devices. This is the responsibility of the network layer. It enables these gadgets to communicate with the other computers, connected devices, and network equipment to interact with them (Zalewski, 2019). In addition to that, it is in charge of all of the devices' data transfers.

The processing layer makes up the third layer. It is regarded as the central processing unit of every IoT ecosystem. Before being delivered to the data center, data is often examined, preprocessed, and stored in this location. In the data center, software programs that both observe and manage the

information as well as plan for further actions may then access the data. Edge computing and analytics come into play at this point in the narrative (Abdullah, Kaur, & Biswas, 2020).

The application layer is the last one in this particular scenario. During this stage, the user engagement takes place as the system provides the user with application-specific services. A good illustration of this would be an application for a smart home in which users could switch on a coffee maker by touching a key in an app or a display that displayed the current condition of the various components of the system (Nižetić et al., 2020).

Functional blocks in the IoT architecture

In addition to layered frameworks, the Internet of Things consists of a number of functional blocks that provide support for a variety of IoT activities. These activities include various techniques, authentication and identity, control and administration. There are a number of critical functional blocks that are responsible for the processing, as well as the operations, connection difficulties, data monitoring, and storage management (Jabraeil Jamali et al., 2020).. Together, all of these different functional pieces make up an effective Internet of Things system, which is essential for reaching one's full potential. Even though there are a number of reference designs that have been offered along with the technical requirements, they are still a very long way from the standard platform that is appropriate for the internet of things on a global scale. As a result, it is still necessary to create an appropriate architecture that is capable of satisfying the requirements of the global IoT. Because it enables connection between IoT servers and devices relevant to a variety of applications, gateways play a vital part in the communication of the internet of things (Cristea, Feraru, & Paduraru, 2022).

In a heterogeneous setting, the most important design considerations for an effective Internet of Things architecture are modularity, scalability, interoperability, and openness. The Internet of Things architecture has to be developed with the goal of satisfying the criteria of cross-domain interactions, complex multifactorial integration with the possibility for easy and scalable administration features, user-friendly apps, and big data analytics & storage (Abdullah, Kaur, & Biswas, 2020). In addition to this, the architecture should have the capacity to increase the functionality, as well as add additional sophistication and automation to the IoT devices that are part of the system (Vorakulpipat, et al., 2018).

In addition, a whole new obstacle presents itself in the form of the ever-increasing volume of huge data that is produced by the connectivity between IoT devices and sensors (Khanna & Kaur, 2020). As a result, for an Internet of Things system to be able to cope with huge volumes of streaming data, an efficient design is necessary. Cloud computing and fog computing/edge computing are two prominent designs for internet of things systems. These architectures facilitate the monitoring, management, and processing of huge amounts of information in IoT systems (Soldatos, 2016).

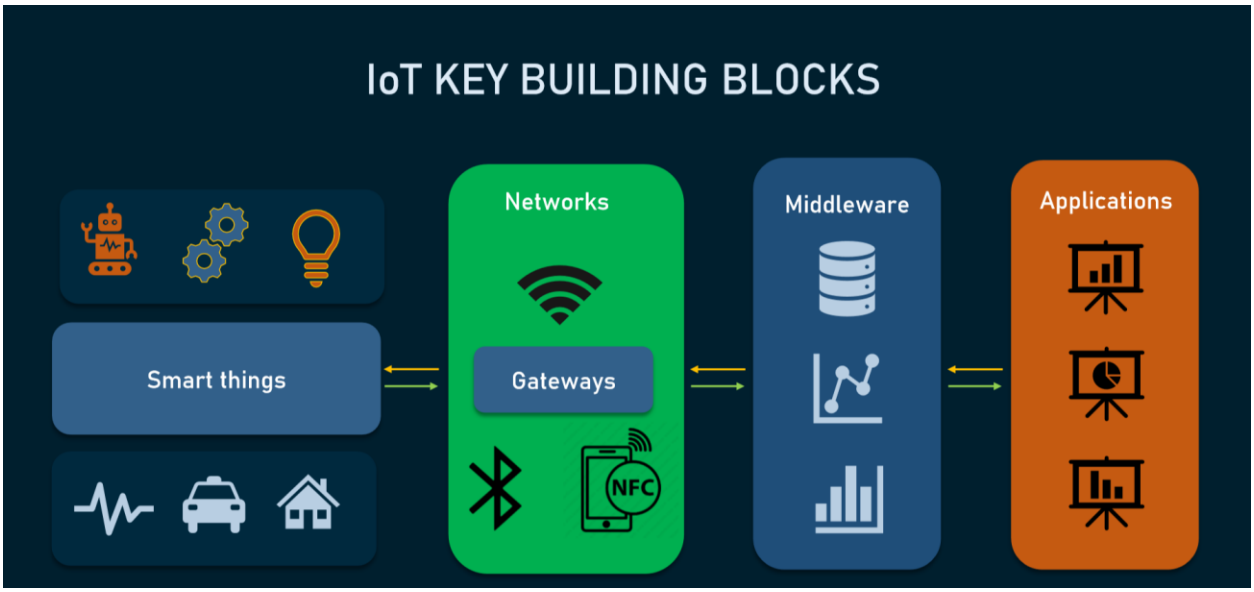


Figure 2: *Modern IoT architecture*

Applications of IoT

Iot applications in General Activities

The rising presence of Internet of Things powered devices and technologies has brought about a significant shift in the way humans go about their typical day-to-day activities. One of the developments brought about by the Internet of Things is the idea of "smart home" systems and appliances. These systems and appliances include internet-connected gadgets, home automation systems, and dependable energy management systems. In addition, one of the most significant developments brought about by IoT is the Smart Health Sensing system. It integrates many pieces of tiny, intelligent equipment and technologies to aid in the maintenance of a person's health

(Goyal et al., 2018). The various health problems and fitness levels, as well as the number of calories burnt at the fitness facility, can all be checked and monitored using these gadgets, which may be utilized either inside or outdoors. In addition to that, it is being utilized in hospitals and trauma centers to monitor the critical health situations that patients are experiencing. As a result, it has reshaped the whole landscape of the medical industry by providing it with access to sophisticated technologies and cutting-edge tools. In addition, researchers and developers working in this field are actively interested in improving the quality of life for those who are handicapped or in the senior age group (Kodali, Soratkal & Boppana, 2016).

The Internet of Things has delivered a remarkable performance in this domain and has opened the door to a fresh path for the everyday lives of individuals in these situations. The majority of people are taking use of these tools and technologies because they are extremely economical in terms of the amount of money required to produce them and because they are readily accessible within a price range that is considered to be reasonable. They are able to lead a regular life now because of the internet of things (Saha, Mandal & Sinha, 2017). Transportation is an additional crucial component of our everyday lives. The Internet of Things has enabled some new technological developments that make it more effective, pleasant, and dependable. Intelligent sensors and drone-like machines are currently in use to regulate the flow of traffic at a variety of signalized junctions located across major cities. In addition, automobiles are being sold in markets with pre-installed sensor devices that are able to detect the impending presence of significant traffic congestion on a map and may provide an alternate route that has less traffic congestion as a solution to the problem. As a result, the Internet of Things has a lot of potential applications in many different fields of life

& technology (Dey, 2019). Therefore, it is fair to assert that the IoT has a great deal of potential both for the development of new technologies and for the benefit of people everywhere.

IoT in Trade Market

The Internet of things has shown both its relevance and its possibilities in the industrial and economic development of an area that is still in the process of evolving. Additionally, it is being called a revolutionary move as in trade and stock market markets at the moment. However, ensuring the safety of one's information and data is a significant worry that is also extremely desired (Le & Tran, 2020). This is a significant obstacle that must be overcome. The Internet, which is responsible for the majority of security breaches and cyberattacks, has provided several entry points for cybercriminals, which has led to the insecurity of data and information. Nevertheless, this configuration of a wide range of components and systems is devoted to providing the best available solutions for dealing with concerns pertaining to the security of information and data. As a result, safety should be the primary priority with regard to the Internet of Things in business and the economy. However, recent improvements in the industry point to some promising trends in terms of improved safety (Schermuly et al, 2019).

IoT in Agricultural and Industrial sector

It is anticipated that the current population of the planet will almost double over the course of the next three decades. Agriculture plays a crucial part in our lives. It demands significant changes in the way humans approach agriculture if species are going to be able to feed such a large population (Talavera et al., 2017). Therefore, there is a need to integrate agriculture and technology in order to make improvements in a manner that is both effective and efficient in terms of increasing productivity. Technology based on greenhouses is one of the potential techniques that may be used in this regard. It offers a means of exerting control over the environmental elements in order to boost the level of output (Sushanth & Sujatha, 2018). The manual control of such a system, on the other hand, is less effective, necessitates the expenditure of physical labor and expense, and leads to decreased productivity and energy waste. In addition, the use of intelligent devices and sensors makes it simpler to manage the temperature within the tank and track the process, which ultimately leads to a reduction in energy consumption as well as an increase in output quality. In addition to this, one of the other advantages that comes with the deployment of IoT is the digitalization of many sectors. It has been delivering solutions that are changing the game in terms of industrial digitization, supply chain management, quality control, logistics (Farooq et al., 2019).

IoT in Automotive Industry

The use of the internet of things is now undergoing a revolution in the automobile sector in the present times. One of the most important applications is the development of autonomous vehicles, which has caused a sea shift in the way that the automobile industry operates. Engineers have developed automobiles that can drive themselves in an effort to minimize the risk of accidents

caused by human mistakes and to make driving more secure. Tesla, Audi, Google, and Mercedes-Benz are just a few of the corporations across the globe who are developing autonomous driving technology for their automobiles. Deep Learning, Data Science, Artificial Intelligence, and the Internet of Things are just a few of the technologies that are used by these self-driving platform systems. These high-tech gadgets have been programmed in such a manner that they contribute to the development of an automated process for vehicles that drive themselves (Rahim et al., 2021).

Devices such as speed controllers, cameras, temperature sensors, smart navigators, wireless connection, rain sensors, and proximity sensors are included in such systems. After the user inputs location and destination information into a platform for autonomous driving, the system will begin driving itself. After that, the navigator will assist in locating the location and will attempt to identify the quickest route possible. After that, AI-based systems get the data from the IoT-based cameras, which assist in obtaining pictures of the surrounding environment and transmit them on to the machine learning powered systems. These systems do an analysis and visualization of the data collected from the surrounding area, and then adjust the behavior of the autonomous vehicles appropriately. In addition, there are speed controllers based on the internet of things that may assist in regulating the speed of these automobiles in accordance with the traffic (Kodali, Soratkal & Boppana, 2016). All of these examples demonstrate how the Internet of Things is revolutionizing the automobile sector.

Major issues and challenges of IoT

The participation of Internet of Things–based systems in many facets of human life, as well as the myriad of technologies involved in the movement of data between embedded devices, rendered it complicated and gave birth to a number of concerns and obstacles. These problems provide a problem for the developers of IoT in today's highly sophisticated society of smart technology (Patel, Vyas, & Pandya, 2019). Difficulties and the requirement for more sophisticated Internet of Things systems are rising in tandem with the advancement of technology.

The Internet of Things is fraught with several dangers, including cyberattacks, hazards, and vulnerabilities, which make privacy and data protection among its most pressing concerns and difficult problems to solve. Inadequate authorization and authentication, unsecured software and firmware, an insecure web interface, and inadequate transport layer encryption are the factors that give rise to concerns about the privacy of individual devices (Rao & Haq, 2018). When it comes to developing trust in Internet of Things systems, concerns of security and privacy are highly crucial characteristics that need to be taken into consideration. In order to forestall security breaches and assaults, the Internet of Things architecture has to include security procedures at each of its levels. For the purpose of protecting users' personal information and preserving their privacy inside IoT-based systems, a number of protocols have been designed, developed, and successfully implemented across all levels of communication channels (Vorakulpipat et al., 2018).

If, however, the IoT-powered system communicates with one another utilizing wireless technologies, then the system is opened up to a greater number of potential security vulnerabilities. As a result, the deployment of certain mechanisms to identify harmful behaviors and to facilitate

self-healing or recovery is recommended (Zalewski, 2019). Privacy, on the other hand, is a separate but equally significant problem that enables consumers to have a sense of safety and comfort when using Internet of Things technologies. Due to this reason, in order to create communication between trustworthy parties, it is necessary to keep the authentication & verification up via a secure network (Panchiwala & Shah, 2020).

Consequences of attacks on IoT powered systems

When it comes to the Internet of Things (IoT), the effects of cyber assaults might be far more detrimental to cope with. The Internet of Things has the extraordinary capacity to have an effect on both physical and the virtual systems simultaneously. Because they are easier to convert into tangible repercussions, cyberattacks against IoT ecosystems may have significantly more unanticipated outcomes than other types of cyberattacks. This is especially noticeable in the sector of industrial internet, where previous hacks have already shown cascading effects. IoT (Internet of Things) devices are already being used in the healthcare profession to remotely monitor patients' vital signs. These gadgets have proved to be of great assistance during the pandemic. Attacks on these devices might disclose confidential medical information and possibly put the patients' health and safety in jeopardy. In the context of the smart home, exposed gadgets might make it possible for hackers to watch the family, compromise security equipment such as security systems, and use devices against their owners (Radanliev et al., 2018). For instance, in one case the baby monitor. Also, a smart thermostat was hacked. These incidents show that it can pose a physical threat as well.

Interoperability Challenges

Interoperability refers to the degree to which various Internet of Things devices and systems are able to successfully exchange information with one another. This information sharing does not depend on the already installed software or hardware in any way. The problem of interoperability is caused by the diverse character of the many technologies and solutions that are employed in the development of the Internet of Things. Interoperability may be broken down into four different levels: the technical, semantic, syntactic, and organizational levels (Gonzalez-Usach et al., 2019).

Ethical and Legal Challenges

When it comes to the development of systems that are driven by the internet of things, this is also the primary problem. These concerns include ethical questions, legal concerns, and regulatory rights. There are some laws and regulations in place to keep the standards and moral values intact and to stop individuals from acting in a way that goes against them. The sole difference between ethics, which are the standards that people still believe in, and laws, which are particular limits chosen by the government, is that morality are values that individuals believe in while laws are certain restrictions imposed by the government. However, the purpose of ethics and laws alike is to uphold standards and ensure quality while discouraging individuals from engaging in criminal activity. The emergence of the Internet of Things has led to the resolution of a number of issues that arise in real life; yet, it has given birth to significant ethical and legal dilemmas (Karale, 2021). Resulatenly, the number of users of IoT devices support the government regulations and norms

with respect to data safeguard, privacy, and safety because of their lack of confidence in IoT devices.

Research Framework

The most important research approaches for this project are going to be developing a conceptual framework and conducting a review of the existing relevant literature. In a conceptual framework, extra concepts and empirical facts are gained from the relevant body of study, in addition to one or more formal theories that are incorporated (either in part or in their whole). The objective of this section is to illustrate the links between these ideas and to show how those connections relate to the subject of the investigation.

Future Research Agenda

In order to accomplish the goal of the study, the author of the article utilizes a review of the relevant previous literature. In order to carry out an objective evaluation, the article follows the ethical norms that are in place. In this analysis, we look at some of the potential problems that the Internet of Things (IoT) might face in the future. It intends to address the topic from a technical as well as a social point of view. Research may be conducted on the use of the Internet of Things (IoT) in a variety of business sectors and the worries that those sectors have about the protection of their data. In addition, concerns such as the expense of the infrastructure and the formulation of a system for regulation may also be attended to.

Conclusion

The Internet of Things (IoT) is a nascent technology that has captured the attention of a significant number of academics from all over the globe. There have been significant advances made toward incorporating this technology into our day-to-day lives. However, there are a number of important aspects to consider when resolving the security concerns of the internet of things, and these problems need more study to be handled. This study devotes a significant amount of time to investigating and reviewing various IoT security principles. The requirements and difficulties associated with implementing security measures in IoT have been examined and compiled under a variety of different areas. In this article, some problems and obstacles related to the Internet of Things (IoT) that software engineers will need to consider in order to create a better model are presented. In addition, significant application domains of the Internet of Things that are currently being worked on by IoT academics and developers are covered. Because the Internet of Things not only delivers services but also produces a massive volume of data. As a result, the significance of big data analytics is also covered in this article. Big data analytics may provide precise conclusions, which can then be used in the process of developing an enhanced IoT system.

References

Abdullah, A., Kaur, H., & Biswas, R. (2020). Universal Layers of IoT Architecture and Its Security Analysis. In *New Paradigm in Decision Science and Management* (pp. 293-302). Springer, Singapore.

Assiri, A., & Almagwashi, H. (2018, April). IoT security and privacy issues. In *2018 1st International Conference on Computer Applications & Information Security (ICCAIS)* (pp. 1-5). IEEE.

Atlam, H. F., & Wills, G. B. (2020). IoT security, privacy, safety and ethics. In *Digital twin technologies and smart cities* (pp. 123-149). Springer, Cham.

Cristea, R., Feraru, M., & Paduraru, C. (2022, May). Building blocks for IoT testing-a benchmark of IoT apps and a functional testing framework. In *2022 IEEE/ACM 4th International Workshop on Software Engineering Research and Practices for the IoT (SERP4IoT)* (pp. 25-32). IEEE.

Dey, S. (2019). Emerging Trends of IoT-Based Applications in Day-to-Day Life. *Internet of Things in Biomedical Engineering*, 235-257.

Farooq, M. S., Riaz, S., Abid, A., Abid, K., & Naeem, M. A. (2019). A Survey on the Role of IoT in Agriculture for the Implementation of Smart Farming. *Ieee Access*, *7*, 156237-156271.

Goyal, K. K., Garg, A., Rastogi, A., & Singhal, S. (2018). A literature survey on Internet of Things (IoT). *International Journal of Advanced Networking and Applications*, *9*(6), 3663-3668.

Gonzalez-Usach, R., Yacchirema, D., Julian, M., & Palau, C. E. (2019). Interoperability in IoT. In *Handbook of research on big data and the IoT* (pp. 149-173). IGI Global.

Gurunath, R., Agarwal, M., Nandi, A., & Samanta, D. (2018, August). An overview: security issue in IoT network. In *2018 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC) I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), 2018 2nd International Conference on* (pp. 104-107). IEEE.

Ijaz, S., Shah, M. A., Khan, A., & Ahmed, M. (2016). Smart cities: A survey on security concerns. *International Journal of Advanced Computer Science and Applications*, *7*(2).
Jabraeil Jamali, M. A., Bahrami, B., Heidari, A., Allahverdizadeh, P., & Norouzi, F. (2020). IoT architecture. *Towards the Internet of Things*, 9-31.

Karale, A. (2021). The challenges of IoT addressing security, ethics, privacy, and laws. *Internet of Things*, *15*, 100420.

Khanna, A., & Kaur, S. (2020). Internet of things (IoT), applications and challenges: a comprehensive review. *Wireless Personal Communications*, *114*(2), 1687-1762.

Kodali, R. K., Soratkal, S., & Boppana, L. (2016, April). IOT based control of appliances. In *2016 International Conference on Computing, Communication and Automation (ICCCA)* (pp. 1293-1297). IEEE.

Le, T. T. L., & Tran, N. H. (2020). IoT Monitoring Stock Price Forecasting by Using Machine Learning Techniques.

Nižetić, S., Šolić, P., González-de, D. L. D. I., & Patrono, L. (2020). Internet of Things (IoT): Opportunities, issues and challenges towards a smart and sustainable future. *Journal of Cleaner Production*, *274*,
122877.

Panchiwala, S., & Shah, M. (2020). A comprehensive study on critical security issues and challenges of the IoT world. *Journal of Data, Information and Management*, *2*(4), 257-278.

Patel, K., Vyas, S., & Pandya, V. (2019, June). IoT: leading challenges, issues and explication using latest technologies. In *2019 3rd International conference on electronics, communication and aerospace technology (ICECA)* (pp. 757-762). IEEE.

Perera, C., Zaslavsky, A., Compton, M., Christen, P., & Georgakopoulos, D. (2013, October). Semantic-driven configuration of internet of things middleware. In *2013 Ninth International Conference on Semantics, Knowledge and Grids* (pp. 66-73). IEEE.

Radanliev, P., De Roure, D. C., Nicolescu, R., Huth, M., Montalvo, R. M., Cannady, S., & Burnap, P. (2018). Future developments in cyber risk assessment for the internet of things. *Computers in industry*, *102*, 14-22.

Rahim, M. A., Rahman, M. A., Rahman, M. M., Asyhari, A. T., Bhuiyan, M. Z. A., & Ramasamy, D. (2021). Evolution of IoT-enabled connectivity and applications in automotive industry: A review. *Vehicular Communications*, *27*, 100285.

Rao, T. A., & Haq, E. U. (2018). Security challenges facing IoT layers and its protective measures. *International Journal of Computer Applications*, *179*(27), 31-35.

Saha, H. N., Mandal, A., & Sinha, A. (2017, January). Recent trends in the Internet of Things. In *2017 IEEE 7th annual computing and communication workshop and conference (CCWC)* (pp. 1-4). IEEE.

Schermuly, L., Schreieck, M., Wiesche, M., & Krcmar, H. (2019). Developing an industrial IoT platform–Trade-off between horizontal and vertical approaches.

Soldatos, J. (Ed.). (2016). *Building Blocks for IoT Analytics*. River Publishers.

Sushanth, G., & Sujatha, S. (2018, March). IOT based smart agriculture system. In 2018 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET) (pp. 1-4). IEEE.

Talavera, J. M., Tobón, L. E., Gómez, J. A., Culman, M. A., Aranda, J. M., Parra, D. T., ... & Garreta, L. E. (2017). Review of IoT applications in agro-industrial and environmental fields. *Computers and Electronics in Agriculture*, *142*, 283-297.

Vorakulpipat, C., Rattanalerdnusorn, E., Thaenkaew, P., & Hai, H. D. (2018, February). Recent challenges, trends, and concerns related to IoT security: An evolutionary study. In *2018 20th International Conference on Advanced Communication Technology (ICACT)* (pp. 405-410). IEEE.

Zalewski, J. (2019). IoT safety: state of the art. *IT Professional*, *21*(1), 16-20.