**TITLE:**

**THE APPLICATION OF BLOCKCHAIN TECHNOLOGY BASED ON DEEP LEARNING IN PROVIDING THE PRIVACY OF 5 G- AUTHORISED IOT FRAMEWORKS**

**Abstract**

**Chapter 1** This chapter contains the introduction and the background of the research work that has been performed for this paper. This chapter also contains the justification of the research work along with the aim, objectives, research questions and purpose of the research work.

**Chapter 2** The second chapter of the research work contains the literature review which elaborately highlights and discusses the purpose of the research project. It also consists of methodologies used for the accomplishment of this study. The various sources from where the data has been collected are mentioned which has been done using the mixed method of data collection.

**Chapter 3** This chapter of the paper contains the programming language of Python which has been taken into account for analysing the security enhancement of the 5 G-enabled IoT framework while applying the deep learning method for in-depth understanding.

**Chapter 4** This chapter contains part of the discussion of the research work done, which considerably talks about the intervention of the IoT as one of the main concerns for development. It also elaborately highlights the use of the Neural Network algorithm in the intelligent link area with the purpose of designing the enhancement of the security of the 5 G-based IoT.

**Chapter 5** Displayed in this chapter is the critical evaluation of this entire research study. It contains the summary of the addressed objectives set in the research work where the understanding of the paper is reflected back in accordance with the applicable future work in this domain.

**List of Abbreviations**

**Abbreviations Explanation**

DL Deep Learning

ML Machine Learning

IoT Internet of things

5G network 5th generation network

AI Artificial intelligence

GPS Global Positioning System

**Index**

[Chapter 1: Project](#_1fob9te) **6**

[1.1 Introduction](#_3znysh7) [6](#_3znysh7)

[1.2 Background](#_2et92p0) [6](#_2et92p0)

[1.3 Research Justification](#_tyjcwt) [7](#_tyjcwt)

[1.4 Aim](#_3dy6vkm) [7](#_3dy6vkm)

[1.5 Objectives](#_1t3h5sf) [7](#_1t3h5sf)

[1.6 Research Questions](#_4d34og8) [8](#_4d34og8)

[1.7 Research Rationale](#_2s8eyo1) [8](#_2s8eyo1)

[Chapter 2: The Research Process](#_17dp8vu) **8**

[2.1 Literature Review](#_3rdcrjn) [8](#_3rdcrjn)

[2.1.1 5 G-enabled IoT devices](#_26in1rg) [8](#_26in1rg)

[2.1.2 Blockchain-based industrial implementation in 5 G-enabled IoT](#_35nkun2) [10](#_35nkun2)

[2.1.2.1 Smart Home](#_1ksv4uv) [10](#_1ksv4uv)

[2.1.2.2 Smart City](#_2jxsxqh) [11](#_2jxsxqh)

[2.1.3 Shortcomings of Blockchain in IoT and its Contribution](#_3j2qqm3) [12](#_3j2qqm3)

[2.1.4 Challenges in deploying deep learning in 5 G-enabled IoT](#_4i7ojhp) [13](#_4i7ojhp)

[2.1.5 Deep learning and blockchain-empowered security framework for 5 G-enabled IoT](#_2xcytpi) [15](#_2xcytpi)

[2.2 Methodology](#_3whwml4) [16](#_3whwml4)

[2.2.1 Outline of the Research Method](#_2bn6wsx) [16](#_2bn6wsx)

[2.2.2 Research Philosophy](#_qsh70q) [16](#_qsh70q)

[2.2.3 Research Approach](#_1664s55) [17](#_1664s55)

[2.2.4 Research Design](#_3as4poj) [17](#_3as4poj)

[2.2.5 Population](#_3q5sasy) [18](#_3q5sasy)

[2.2.6 Data Collection Methods and Type](#_1pxezwc) [18](#_1pxezwc)

[2.2.7 Method of Data Analysis](#_49x2ik5) [18](#_49x2ik5)

[2.2.8 Sampling Techniques](#_25b2l0r) [18](#_25b2l0r)

[2.2.9 Validity and Reliability](#_3o7alnk) [19](#_3o7alnk)

[2.2.10 Ethical Consideration](#_23ckvvd) [19](#_23ckvvd)

[2.2.11 Research limitation](#_32hioqz) [20](#_32hioqz)

[2.3 Data Analysis](#_1hmsyys) [20](#_1hmsyys)

[**Chapter 3- Dissertation**](#_41mghml) **32**

[3.1 Introduction](#_2grqrue) [32](#_2grqrue)

[3.2 Arranging the materials and structuring the dissertation](#_vx1227) [34](#_vx1227)

[3.3 Summary](#_19c6y18) [34](#_19c6y18)

[**Chapter 4- Discussion**](#_3tbugp1) **35**

[4.1 Discussion](#_28h4qwu) [35](#_28h4qwu)

[4.2 Critical analysis](#_nmf14n) [36](#_nmf14n)

[**Chapter 5- Evaluation and Conclusions**](#_37m2jsg) **38**

[5.1 Critical Evaluation](#_1mrcu09) [38](#_1mrcu09)

[5.2 Summary of the Achievements](#_46r0co2) [38](#_46r0co2)

[5.3 Reflection](#_2lwamvv) [38](#_2lwamvv)

[5.4 Future Work](#_111kx3o) [38](#_111kx3o)

[Reference list](#_206ipza) **39**

**List of Figures**

[Figure 1: 5G Connection and Devices 10](#_lnxbz9)

[Figure 2:Blockchain for enhancing the security of IoT devices 11](#_44sinio)

[Figure 3: 5G in smart city 12](#_z337ya)

[Figure 4: Challenges of adopting Blockchain in IoT 13](#_1y810tw)

[Figure 5: Deep Learning and Blockchain-Empowered Security Framework for 5 G-based IoT 16](#_1ci93xb)

# Chapter 1: Project

## 1.1 Introduction

The considered research paper offers a comprehensive review of securing IoT devices to enhance security techniques for IoT deployed over Blockchain and 5G. Breakthroughs within technologies such as IoT are pushing humankind toward intelligent living. Blockchain and 5G have again escalated the authenticity of the IoT mechanisation to possess its implementation in numerous diversified realms such as innovative education, healthcare, integrated conveyance, and smart homes. Taking into account the disseminated use cases and the amount of exchanged data through IoT media poses the threats of privacy issues which have become a top priority in today's digital world. Modifying the Internet of Things extra strongly towards several extensive threats is a challenging task. The multifariousness of these technological instruments is a compelling modifier in searching for remedies in distinct aspects, which shows the advent of difficult privacy challenges.

The primary contribution of this research study is to effectively recognize the main components essential for developing a 5G-enabled IoT model to offer an insight and understanding of the concept. The research paper focuses on providing an overall understanding of the privacy and security challenges that are associated with the framework and also delivers insight and information about the technologies of deep learning and its role as an instrument, as well as its diverse approaches alongside the technology of Blockchain as well as its security patterns that are made use of to offer security to the stored data. This research study contributes to developing the concept of the adoption of this blockchain technology followed by a “deep learning method” to increase the privacy of the “5G-associated IoT framework”.

This segment of the paper hands out the introduction of this research study. This part shows an outline of the research realm or the research background. This introduction chapter determines and explains the research motivation and contribution and also discusses the study's aim, objectives and research questions.

## 1.2 Background

With this fast advancement of sensor detectors dependent on Communication or Information technology, IoT is considered to be the platform for imparting and exchanging information, and handling the services of innovative city applications like better recognition, monitoring, controlling and tracking (Sharma *et al.,* 2021). These sensor devices involving GPS, RFID, temperature, and many others are linked to everything via the Internet. Proliferating growth is observed regularly within the linked sensing IoT devices. The cross-domain amalgamation of IoT with emergent technologies such as Blockchain and 5G influences the lives of humankind. So surge in dependency on IoT entails concentrating on the technology's security and privacy concerns. Implementing security via authentication, encryption, communication security, and access control is vital and urgently necessary. These necessities can be served and nurtured by using deep learning and machine learning to recognize and acquire secure, intelligent systems (Singh *et al.,* 2021).

In today's digital world, 5G is a new leash and a turning point in the digital environment. Its highly secure connectivity or reliability is advantageous in every field, scaling from intelligent grids and self-operated vehicles to AI-associated healthcare or homes. The encounters of two encouraging prospective forces, IoT and 5G are comprehensive phenomena in various fields. Numerous researchers have learned the incorporation of Blockchain methods to maintain the privacy of modern cities. The objects of the material world are presented to the web world with the assistance of the “Internet of Things” (Almutairi, 2022). The IoT model is very different from other traditional software services solutions, so the deployment of security solutions requires it to be unique.

Deep learning is a leading technology and is also an approach of machine learning that is effectively made use of as an analytical instrument for analyzing vast amounts of data, further offering an understanding and insight into informative documents. Simultaneously, this Blockchain is an advancing distributed mechanisation that offers security for the data that is stored within it (Ahmed *et al.,* 2022). It also helps improve smart manufacturing and enables decentralization, authentication, decentralisation and digital reliability in a dispersed way (Sharma *et al.,* 2021). This paper focuses on the role played by these blockchain mechanisms followed by deep learning methods to improve the 5G-activated Internet of Things infrastructure security and proposes a mechanism to secure a 5G-activated IoT infrastructure.

## 1.3 Research justification

## 1.4 Aim

This research study aims to study the application of blockchain technology followed by deep learning adoption in refining the 5G-activated IoT framework security.

## 1.5 Objectives

* To identify the role of blockchain-based technology followed by deep learning.
* To figure out the significance of this 5 G-activated IoT framework.
* To examine all the challenges encountered by the 5 G-enabled IoT framework.
* To identify applications of Blockchain technology in security enhancement.
* To look into the role of ‘Blockchain technology" in improving 5G-activated IoT infrastructure security.

## 1.6 Research questions

1. How does the deep learning-based blockchain mechanism function?
2. How significant is the 5 G-enabled IoT framework for next-generation intelligent systems?
3. How does a deep learning-based blockchain mechanism operate in security enhancement?
4. How does incorporating blockchain technological function in facilitating the privacy of the 5G-activated IoT framework?
5. What security challenges are encountered by the 5G-activated IoT framework?

## 1.7 Research Rationale

The rationale behind conducting this review work is to critically evaluate the application of blockchain technology dependent on deep learning methods to improve the overall cyber privacy of 5G-enabled IoT frameworks. This research topic will assist in getting valuable insights regarding the effective use of DL-based Blockchain to fulfil security enhancement purposes. The implementation procedures of this Blockchain technology in 5G-activated modern homes and smart cities will also be understood. This will also help to determine the limitations of this blockchain mechanization and the barriers confronted during the incorporation of deep learning in 5G-enabled IoT so that effective strategies can be developed to deal with challenges and increase its overall efficiency. In these regards, some practical frameworks will also be proposed that can facilitate the implementation and use of Blockchain along with deep learning technology to mitigate the privacy threats in the 5G-activated IoT.

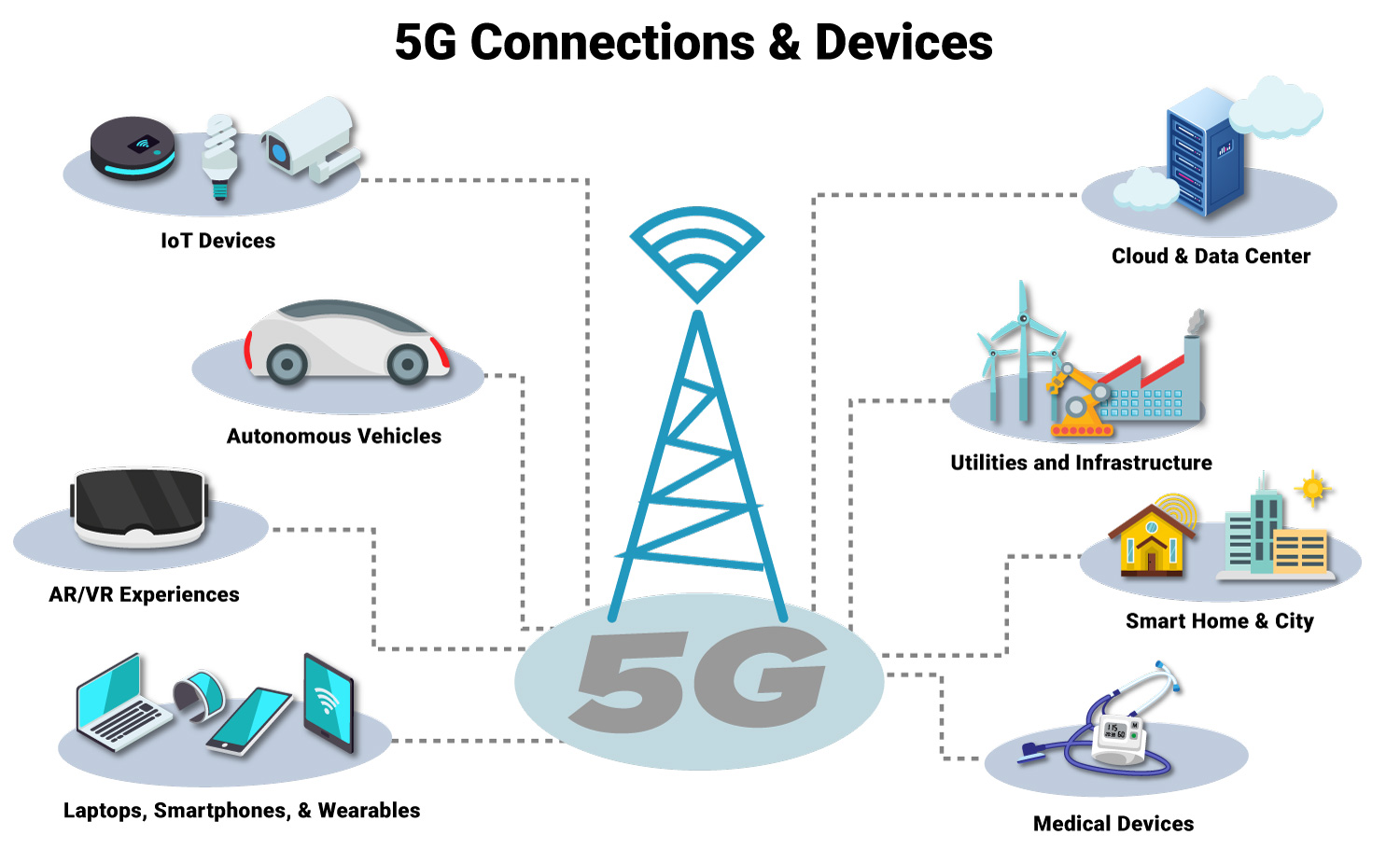
# Chapter 2: The Research Process

## 2.1 Literature review

### 2.1.1 5 G-enabled IoT devices

The author (Ahmed *et al.*, 2022) stated that the Internet of Things and its utilization in different industry sectors have been growing increasingly over the past few eras. In this research, the paper authors describe the 5G mobile communication-based system that primarily promotes the mobile-based network, which helps to interconnect with the individual, even control and interconnect the devices and machines. This includes self-driving, remote surgery, flying IoT drones, virtual reality, surveillance and security. The fifth generation introduced the development of performance and limitations of 4G. It helps for a good data transfer rate with high connection and low latency density. This 5G has connected twenty billion IoT devices that can connect to a worldwide network, producing massive amounts of data. The 5G IoT paradigm is merged with the 5G cellular network, artificial intelligence and IoT, which makes an intelligent IoT environment (Subba *et al.,* 2021). The 5 G-enabled IoT has various advantages in remote surgery because it provides a short time lag among a device pinging the network; with the help of the 5G network, surgeons can perform remote surgery. Also, it includes the self-driving car, transforming healthcare, virtual reality, surveillance and security, and flying IoT. This 5 G-enabled IoT is one of the best advantages provided by the 5 G-enabled IoT. This research study has shown that this technique is very useful for an autonomous vehicle that can sense its safety and surroundings with the help of negligible human involvement. This vehicle is also designed with many significant functionalities like odometers, inertial measuring units, GPS and radar systems (Subba *et al.,* 2021). This is one of the major things for any vehicle, and this helps to design the vehicle's navigation system.

On the other hand, it is involved in the artificial environment created for utilizing the software and many other concerned tools. This helps the software to feel the sound and sight. Flying IoT-based drones are also involved in controlling the airspace and are responsible for carrying out navigation services in different locations. With the help of 5G enabling IoT, analytics and surveillance are taking other applications that will be very fruitful with this modern connectivity system.



*Figure 1: 5G Connection and Devices*

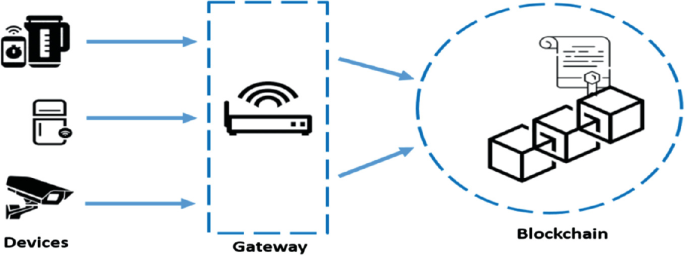
Citation: Mukherjee and Pradhan, 202

As per the authors (Mukherjee and Pradhan, 2021), the 5 G-enabled IoT plays a significant role, but on the other hand, this has various types of issues, like security and privacy. This technology plays a crucial role, and every single device is connected to the Internet. For this reason, privacy and security-related issues are raised. This type increases the risk taken towards enhancing the risk of leakage of sensitive information. The authors (Mukherjee and Pradhan, 2021) suggested that this is one of the important difficulties experienced by the IoT and the enhancement of the 5G also involves this area. If information is not tackled appropriately, confidential information may be disclosed to a third party. This also includes compatibility and complexity issues; this IoT consists of various networking and device protocols that are utilized to connect them. If a single mistake happens for any reason, then the entire programme is impacted. Significantly, the author stated that these 5G-enabled IoT devices are decreasing human labour drastically with task automation as these machines are replacing humans.

### 2.1.2 Blockchain-based industrial implementation in 5 G-enabled IoT

#### 2.1.2.1 Smart home

The technological enrichment for living is called the smart home. The primary goal of this is to provide a quality life for inhabitants. The authors (Xihua and Goyal, 2022) stated that these smart homes provide comfort, security and convenience to the house owner by supporting them to control the strings to their presence. It is happening with the help of smartphone devices as it describes that the smart home system is specifically coordinated with the machines to regulate any function based on utilizing the statics to serve uninterrupted actual-time service (Xihua and Goyal, 2022).



*Figure 2:Blockchain for enhancing the security of IoT devices*

Citation: Xihua and Goyal, 2022

The blockchain-based smart homes consist of three basic types of tiers, cloud storage, smart home and overlay; these are reviewed in this article. This overlay network helps focus on the distributed trust to eliminate POW and proposes an innovative home model. The Internet of Things devices are controlled centrally in the tier of modern homes.

#### 2.1.2.2 Smart city



*Figure 3: 5G in smart city*

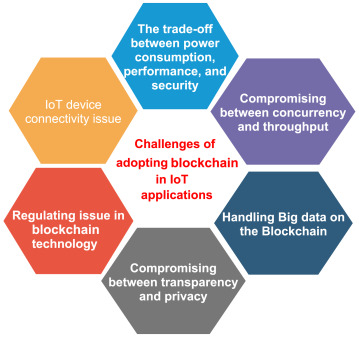
Citation: Mistry *et al.*, 2020

The research paper also shows the enhancing trend of individuals migrating to modern areas, linked with associated modernisation procedures. Smart cities provide their citizens with various major benefits; the smart city's infrastructure is associated with the IoT-enabled 5G systems. A smart city-state's significant element helps create a unique parking system. This system also collaborates with improving a traffic management system that helps reduce costs incurred by hiring relevant employees. The author (Mistry *et al.*, 2020) explains the algorithms that help to enhance the efficiency of cloud-based smart parking and that relate to IoT technology. The suggested triangular framework recognized the different features of smart cities from different types of perspectives of resources. The research paper has focused on the beneficial impact of IoT technologies.

As per the author (Mistry *et al.*, 2020), this IoT-based technology has a very bad impact on the environment, the IoT and internet appliances have essentially added the advancement in smart homes, and through this way, it reflects the enhancing assimilation and adoption of various new home applications. These technologies provide a modern level of comfort, privacy and convenience to the whole home setting. Although these facilities of smart homes might be flexible for environmental requirements, for this purpose, many privacy-related issues are faced. The author (Hewa *et al.,* 2020) stated that these intelligent IoT sensors, devices and appliances are responsible for enhancing the privacy risk. It also includes user experience-related issues and system transparency; smart cities also create major citizen issues. In this research paper, authors suggest that the growth of the sensors and the enhanced interlinked mutually dependent primarily siloes of any city's framework raised rightful concern. But, for any reason, if privacy standards remain unchanged, cybercriminals can shut down the entire city. Many issues are raised, such as housing, crowding, public education and crime. These issues impact the environment of living, and the security issues of public data are a major concern of these smart cities.

### 2.1.3 Shortcomings of Blockchain in IoT and its Contribution

According to Hewa *et al.* (2020), the authors have stated that integrating “IoT and Blockchain” has a lot to contribute in almost all the aspects of IoT when being implemented in different sectors. It has the potential to eradicate issues related to the security and privacy of IoT; however, the authors have argued that in the mass functionality of IoT with Blockchain, there can be certain shortcomings affecting the integration. The shortcomings can vary in nature and present in many different aspects.



*Figure 4: Challenges of adopting Blockchain in IoT*

Citation: Hewa *et al.,* 2020

The processing time and power, as per the argument presented by the authors, is that in the environment of Blockchain, there are computational resource-intensive operations which consist of verification of transactions and cryptographic operations (Hewa *et al.,* 2020). This, however, due to the IoT's nature of being resource-restricted, brings limitations in providing quality outcomes when raising the system's capability.

According to (Kumar and Mallick, 2018), throughput is one of the major challenges that significantly affects Blockchain in IoT. This challenge will likely appear repetitively when transaction amounts and sizes go up. The authors have stated that the occurrence of throughput can bring constraints in the cost along with the technical issues, which can increase the potential chances of passing the interoperability standards of IoT.

According to (Qatawneh *et al.,* 2020), other than the shortcomings of Blockchain in IoT, Blockchain massively contributes to the IoT. It can massively help build solid trust where the various associated stakeholders can trust the process in different dimensions towards achieving results safely. To manage and handle the vast data processed on a large scale in the IoT system, there is a need to raise the Internet's infrastructure. As per the authors (Kumar and Maliick, 2018), Blockchain can efficiently apply procedures to solve issues by the distributed networks where various aspects can function, such as DFS, ADC and Peer-to-Peer Networking (PPN). It can bring enhanced data. Blockchain has the potential to carry through three main functions, which are permitting the IoT systems to find a huge rate of connections as well as networked devices. The authors (Kumar and Maliick, 2018) have stated that Blockchain lets the systems of IoT track the process of transactions between the devices in coordination. It can also enhance the quality of privacy upon the reliability of IoT systems. Blockchain can be one of the remedies in eradicating the privacy issues of IoT as it removes the notion of a central server related to IoT and permits the data to flow with proper procedures in each process, such as mass transactions through distributed ledgers.

### 2.1.4 Challenges in deploying deep learning in 5 G-enabled IoT

Despite the excellent successes achieved through deploying deep learning in the 5G IoT, various challenges still exist. As (Hewa *et al.,* 2020), the authors have stated even though the utterly embedded procedure of deep learning has specific challenges, such are,

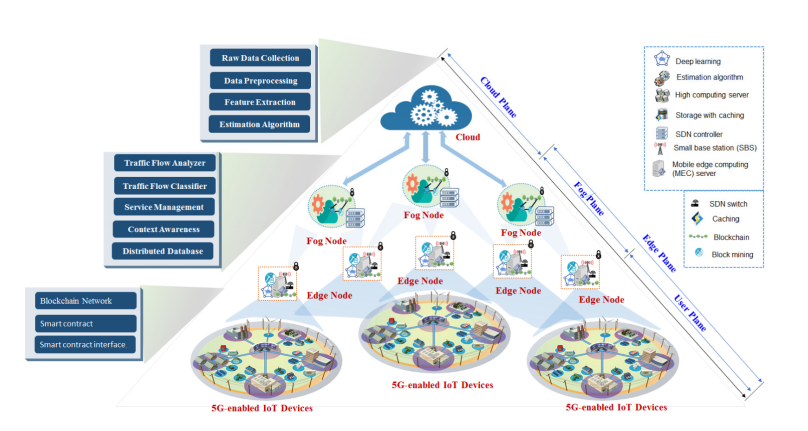
Privacy and security in the field of IoT The devices at the receiving end are, most of the time, lightweight handheld equipment with less power. According to (Jagannath *et al.,* 2022), In some IoT-driven applications, the devices are highly controlled by resources which is why the security and privacy state the chance of risk, as these have adequate security characteristics and features embedded into their structure for the functionalities. Hence, the authors have argued that with the deployment of deep learning in the 5 G-enabled IoT devices, the competition becomes extreme, compromising privacy and security aspects. For example, healthcare monitors, home sensors and similar devices containing locations are easy to meddle with.

Lack of control over the sharing of data, according to (Hewa *et al.,* 2020), in a 5 G-enabled IoT, the network consists of a huge rate of information that is accumulated from different enterprises. The collection, as well as extraction of ample data, enable the network to clash. It can often go out of control when there is an involvement of intermediate parties. Thus, it is perceived that the involvement of intermediate groups means equipment from vendors, the hardware of whom has the potential to form the network node, as well as all the network or providers of the services sharing a common physical network structure system, is what brings the complacent and the trouble of managing and auditing of the data based on who owns what, from where are the data and information extracted and processed.

Scalability, since IoT and the 5 G-enabled IoT devices are highly dependent on the Type of architecture that is mostly cloud-based for management and control. According to (Sodhro *et al.,* 2022), With the fast-increasing quantity of IoT devices, while deploying deep learning in a 5 G-enabled framework, the generating of huge amounts of data would be the forthcoming task for the centralized cloud servers to raise their capability to store while computing power. As per the authors, the cloud server from an edge node and series of networks can be called frontal, mid-haul, and backhaul. The major challenges occurred when a large number of 5 G-enabled IoT that are deploying deep learning in its functionalities to try to connect all to the cloud server, and the links connected with the networks of front haul, midhaul, and backhaul often crash, which the gateway nodes beside it become constricted to give out accurate results.

Controlling large IoT data from various network nodes can be tedious. According to (Sodhro *et al.,* 2022), the authors have argued the challenges that 5 G-enabled IoT devices possess in terms of flexibility. The 5 G-enabled IoT, upon deploying the algorithm of deep learning, considers the efficient recharging of IoT devices to be tiresome. The lack of flexibility becomes obvious in the framework of physical layer radio in the technology that can fulfil the requirement of IoT.

### 2.1.5 Deep learning and blockchain-empowered security framework for 5 G-enabled IoT



*Figure 5: Deep Learning and Blockchain-Empowered Security Framework for 5 G-based IoT*

Citation: Rathore *et al.,* 2021

The author (Rathore *et al.,* 2021) describes the perspective of this technology and the 5 G-activated IoT, where a wider outline of the 5 G-enabled IoT and Blockchain has been suggested. This technology primarily appeared as the next trouble-making technology, and the working capability of this Blockchain function was in the middle of the transformation. This also centralized the internet system of the client-server to a dispersed cryptographically protected network. Here this technique is suggested as the process of an immutable and distributed ledger that can record financial transactions. These blockchains mainly consist of a sequence of time-engraved blocks joined together with the utilization of cryptographic hashes. This helps the user to have a scattered P2P network; in this process, dishonest users interchange information with them. This process is completed without the necessity of any trusted intermediary.

The author (Sharma *et al*., 2021) demonstrates that various types of IoT applications like healthcare, virtual and smart transportation, along with “augmented reality” escapade primarily appear with the technology based on the fifth generation (5G). It helps to increase the user experience and QoS. Further “5G-enabled IoT” primarily help greater system capacity, distinct attributes, and energy saving; it includes lower latency and high data rate. In this research, the authors (Sharma *et al*., 2021) describe the 5 G-based IoT, which tends to ease the functioning of a large rate of devices and helps to develop satisfaction among users, the standard of experience and efficiency of services in IoT applications. The 5G has the ability to enable heterogeneous IoT service and flexible operation, and this 5 G-based IoT technology aids with upcoming technologies and also incorporates the orchestration of numerous multiple inputs and outputs, network function virtualization, ultra-dense networks and mobile edge computing. The authors (Hewa *et al.,* 2020) stated they investigated the development requirement and design for emerging services and networks in 5 G-based IoT. The growth of this system gives rise to privacy concerns and data security, such as the loss of sensitive data and breaches. The security method and conventional data analytics do not meet the 5H-enabled IoT requirements; it also includes the new characteristics of a low-security framework for the purpose of 5 G-enabled IoT and it influences DL competency for this blockchain and brilliant data analysis operations, which emerge across a few layers.

Modern technology powered the privacy framework for the 5 G-activated IoT, delivering security operation and intelligent data. The overall framework primarily shows the strength of Blockchain along with its various steps of the hierarchical framework, edge, user and fog (Sharma *et al*., 2021).

## 2.2 Methodology

### 2.2.1 Outline of the Research Method

The research work has followed a mixed research methodology in which both secondary and primary research methods are included. The secondary Method is helpful in extracting an abundance of data from trustable secondary sources like Google Scholar.

### 2.2.2 Research Philosophy

A positivist research philosophy has been acknowledged in this current dissertation to explain its findings in a precise manner. The positivist philosophy only adheres to factual knowledge from observation, including measurement of the collected data. It helps in interpreting the collected data in an objective way which demonstrates the fair conduction of the research work. The quantifiable observation regarding blockchain-based security to the 5 G-enabled IoT framework is accepted for this study. Using this positivist philosophy certified the research as independent of human interests. The philosophy uses external and independent evidence that carries forward the scientific sound of the study. In this current study, the reason behind selecting the positivist research philosophy as it specified science as its cornerstone. It is applied to test relevant hypotheses extracted from secondary and use a deduction approach to measure the core concept of it. It helps to simplify complex observations on blockchain technology in terms of IoT security to interpret it understandably so that everyone can learn from it. In addition, an interpretivism research philosophy is also associated with this research which includes social perspectives of blockchain-based IoT security solutions. These both have helped in answering all the research problems in an objective way without losing their scientific integrity.

### 2.2.4 Research design

The accurate identification of appropriate research design for this particular paper is also essential as the impactfulness and suitability of specific research rely on that. If an appropriate research design is not chosen, the research regarding “The application of blockchain technology followed by a deep learning procedure to upgrade the privacy of the 5G-activated IoT infrastructure" can not be conducted appropriately. For this particular paper, ***Sequential Explanatory Design*** has been chosen as the data regarding this research are collected in two particular phases, one is from past literature and studies. This research design helps researchers to collect, analyze and combine both qualitative and quantitative research methods in this single research and try to understand the challenges and devise a proper solution (Butler *et al.,* 2020). This particular design is beneficial for the research as it adds up multiple research methods and uses the acquired information to identify the best results for this research work.

### 2.2.6 Data Collection Methods and Type

A mixed method of data collection means "secondary data and technical data '' have been used in this fundamental research in order to find out The application of blockchain technology followed by deep learning techniques to develop the privacy of the 5G-activated IoT infrastructure in a detailed and understandable manner. The "secondary data" were obtained from the reliable scholarly database of Google Scholar, which discussed the key findings in the literature review part (Butler *et al.,* 2020).

### 2.2.7 Method of Data Analysis

To enhance the security measurements of the 5 G-enabled devices that are based on blockchain technology, deep learning technology has been used. In addition to deep learning technology, the classifier has been used in Neural Networks. In order to achieve enhanced privacy levels in the 5 G applications, based on blockchain technology, one data set has been imported that is known as 'df'. The online community for the data scientists along with machine learning devotees **‘Kaggle’,** the dataset has been imported for this file. Along with Kaggle. The .csv file that has been taken from Kaggle and its columns were mapped with the help of taking the dataset from GitHub.

### 2.2.9 Tools

In order to import the values in the source code, all the libraries that have been employed for enhancing the privacy levels of the 5 G applications of blockchain technology, are Keras **(**Conlin *et al.,* 2021**)**, NumPy, Pandas, Seaborn, Ski-Learn and Matplotlib where these are the libraries of this programming language. All these libraries of the Python programming language have been utilised in order to analyse the dataset that has been imported. Most developers use these libraries because all these libraries contain some modules that are built-ins so that it gets easier to access the input/output functionalities. Without the help of these built-in functionalities, using a Python programming language with ease could get tough for the programmers or the developers. Through these modules, the coders can explore the dataset in a clearer way which would give the dataset more statistical so that it could perform well in the various tests.

The **NumPy** library is an essential package of the Python programming language. It helps in working with the numerical values of the dataset. The arrays contained in the dataset to analyse the values and to give a proper outcome of enhanced privacy, this library has been used (Ziogas *et al.,* 2021).

The library **Pandas (**Vagizov *et al.,* 2021) has been used in order to represent the data set more cleanly. The functions of the Pandas are to analyse, clean, manipulate data and explore it. This library makes the work cleaner and more proper.

**Matplotlib (**Sial *et al.,* 2021**)** is an open-source programming library and free. Being an open-source library, the library can be used in the system by any developer. In order to visualize the data in a better manner, the way is to show them graphically. In order to show them in a graphical way, this library has been used.

**Seaborn (**Sial *et al.,* 2021**)** has been chosen to represent the output in a visualized manner. Along with that, it is able to handle the Pandas in a better way.

The Library **Keras (**Conlin *et al.,* 2021**)** has been chosen as this research work has been accomplished with the classifier Neural Network thus it provides the ease to work with this classifier to the developer.

The classifier that has been used in this research study of enhancing the privacy of the 5 G-enabled applications based on blockchain, is **Neural Network (**Sarker, I.H., 2021).

### 2.2.10 Methods

The methods that have been used in order to aim for the objective of the research are data exploration and data plotting. Neural Network is a method that is connected to the human brain in order to get the desired output. With the help of various connected modes to each other, it is performed. This classifier has been chosen to work in this platform as it has been seen earlier that by applying Neural Network with MORE, it has the ability to develop the security measurements and the accuracy of the process. Not only does it help with security but also increases the performance of the system and the runtime so that it gives proper output in a more flexible way.

**Data Exploration**

In the stage of data exploration the values that are to be checked in this section. For this IsNull () function has been done. This part is conducted in any research work, to check if there are any Null values, and then it will detect them.

**Data Plotting**

In order to represent the values in a graphical way matplotlib library of Python programming language has been used. As in the case of representing the values in a way so that the users can understand them easily, it is a better way to represent them in a graphical way.

### 2.2.11 Validity and reliability

Both the validity, as well as reliability, have been followed thoroughly during this research paper so that a trustworthy result can be concluded by the end of this research paper. From the detailed part of the literature review, the results are appropriate and valid (Pandey and Pandey, 2021). The sources of secondary data are valid as they offer a lot of understanding about The use of “blockchain technology” followed by deep learning methods to improve the privacy of the “5G-activated IoT infrastructure". Simultaneously, the primary study materials are identified to be valid as they offer the real-time response of 30 admin executives.

### 2.2.12 Ethical Considerations

The following are the ethical considerations for this dissertation.

* Collected sources of references and primary sources of data will be kept hidden to ensure privacy as well as consistency of the data, which will be evaluated further to perceive numerous aspects of the subject "The application of block-chain technology followed by deep learning procedure to develop the privacy of the 5G-activated IoT infrastructure".
* The complete research study is free from any kind of misconduct, and accurate and authentic findings will be expected from the whole discussion and the results in part (Pandey and Pandey, 2021).

### 2.2.13 Research limitation

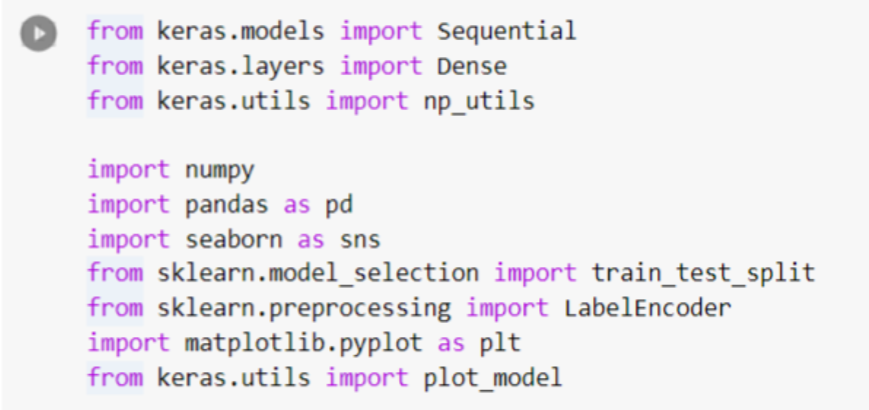
Every research paper is accountable for some limitations. In this particular research, the significant restrictions felt by the researcher were related to the availability of data and time limitations.

## 2.3 DataAnalysis

The prime goal of the research study is to analyse the security measurements in the applications based on blockchain and which frameworks are integrated with the (IoT). Further data analysis depends on data collection, processing, and modelling of the data and modification into the insights of the information so that it can support the critical analysis. Data analysis is performed in any research in order to retrieve various information from the research by testing and modifying it along with the frameworks that are 5 G oriented, which have been examined as per the future projections. In order to perform this research paper, deep learning technology has been used with the help of Neural Networks. The programming language that has been used to do this task is Python programming language to enhance the security of applications whose frameworks are IoT-based and the 5 G-enabled blockchain-based technologies. Through the benefits of ML algorithms, the reading of the dataset, pre-processing of the data, and analysis to exploit the data and visualize the data have been achieved. In order to get the collection of libraries rich the work can be done with proper assistance so that it gets easier to work with the input text.

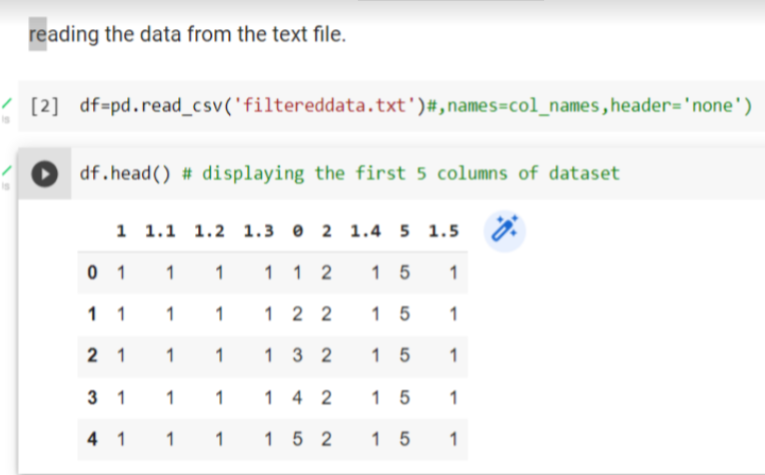
The dataset with which the research has been performed is imported from the popular community among the data scientists and the passionate persons of machine learning Kaggle. The dataset that has been collected or imported in this research paper, the entire pieces of information are based on the topic of 5 G-enabled frameworks based on the frameworks of IoT that can enhance the security of those applications. This project provides information based on various deep learning algorithms like different Neural Networks that are used in classification. Also the source GitHub, from there the dataset can be downloaded too. As per research, the neural network algorithm has better accuracy in classifying the security measurements, thus it has been utilised. This process of integrating all the data not only focuses on qualitative data analysis but also focuses on the quantitative process of analysing the data with a quantitative approach. The bits of help of applying deep learning technology in the search help provide data in a more statistical way. This whole section specifies the dataset to make sure of its validity. The research has used learning technology DL, in order to enhance the security measurements which integrates the technology artificial intelligence within the software in addition to that Jupiter, a live coding platform or Notebook for Python has been integrated as per work with deep learning.

**Importing Libraries:**



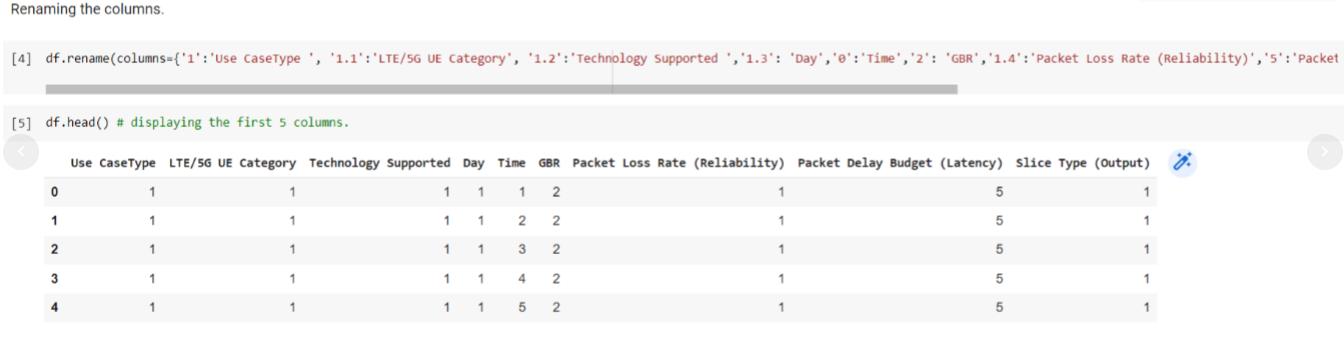
Keras, NumPy, Pandas, Seaborn, Scikit-Learn, Matplotlib, all these libraries of Python language have been imported into the source code of the research study. Keras is a library of the Python programming language that has been used in this dataset to implement the entire dataset through the benefits of the deep learning algorithm “Neural Network”. This library is used for making the neural network easy to handle. The NumPy library has been integrated into the source code to play with the numerical values in the dataset, as it simplifies the methodology of applying the functions inside the arrays. The library Pandas has been imported in the coding because it has the ability to provide the data analysis "ready to utilize" method for the tools of the data analysis along with the tools providing high performance. Besides, in order to split the whole data sets into diverse sub-parts to make the coding easier to handle the library Scikit-Learn has been used. One of the most important parts of any coding is to view the outcomes of the work, and in order to do that, the Seaborn library of Python programming language has been utilised in this dataset to represent the data of the enhanced security measurements. Along with that, the library Matplotlob would help in representing the data in the graphical preparation with the 2-dimensional model.

**Reading the Dataset**



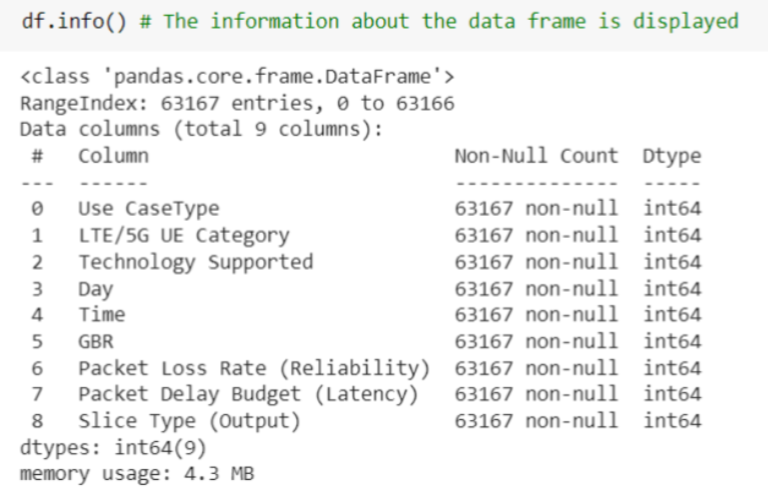
In this step, the dataset that has been used for enhancing the security measurements of the applications of 5 G enabled that have the technology related to IoT, has been read and the content has been stored in the 'df' data frame. The content has been checked with the help of the head() function in order to display the first 5 columns of the dataset.

**Rename the Column**



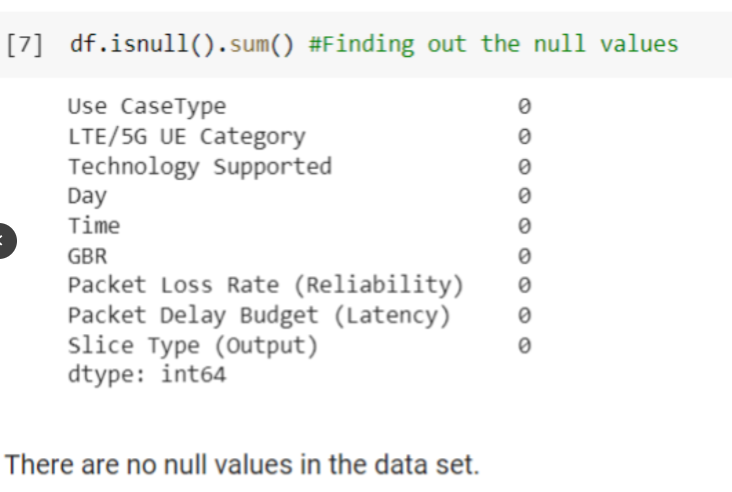
In this section with the help of the rename() function, the columns have been renamed and with the head() function it has been displayed.

**Information on the Dataset**

****

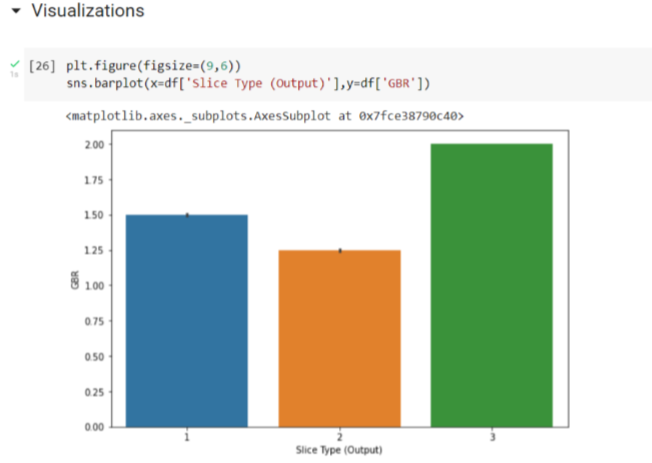
With the help of the info() function, the information of the dataset has been displayed in the above image.

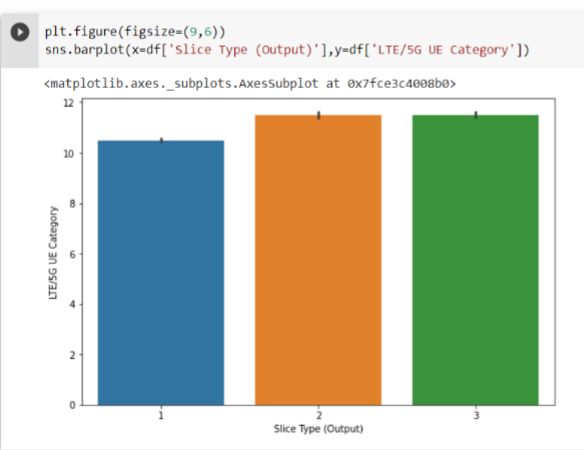
**Finding NULL Values**



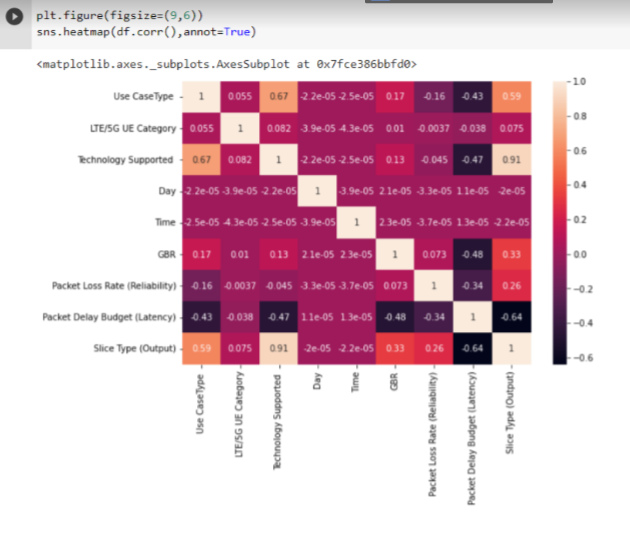
In this section with the help of the IsNull () function, all the NULL values are to be found and as a result, there are no NULL values in the taken dataset.

**Visualisation of the Dataset**



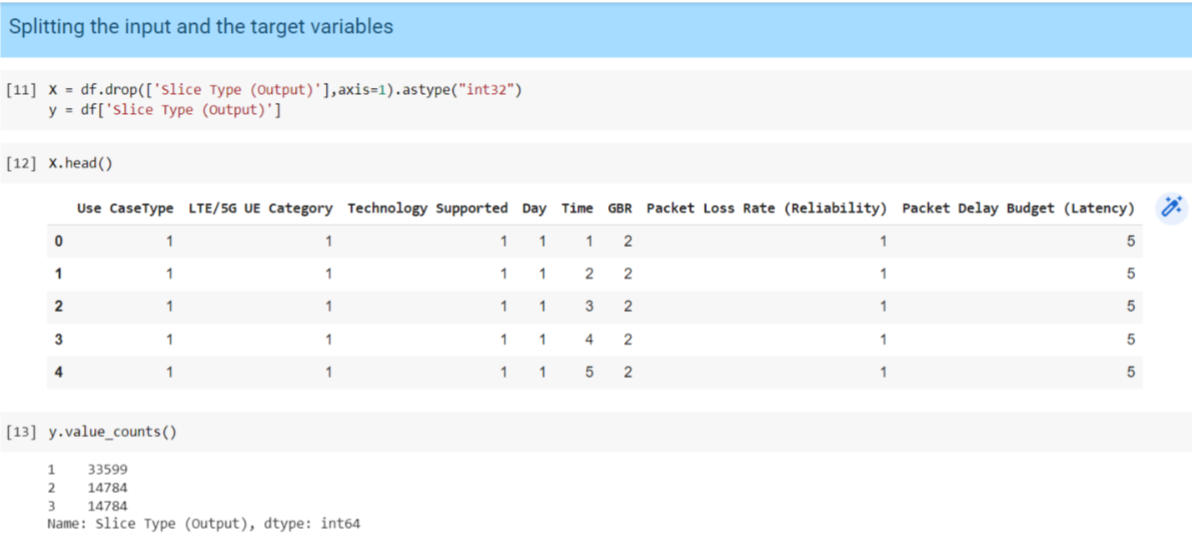


With the help of the seaborn as sns library of Python, the dataset has been visualised in the barplot way. Barplot has been chosen so that it would be understood in an easier way for the user.



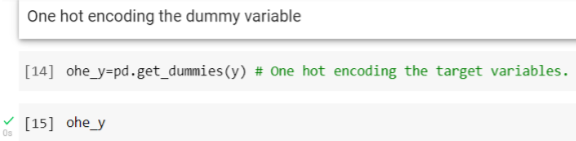
In the above image, for visual representation, matplotlib has been used. The output is represented as a heatmap. Here, the data that are true won't be affected by the heatmap.

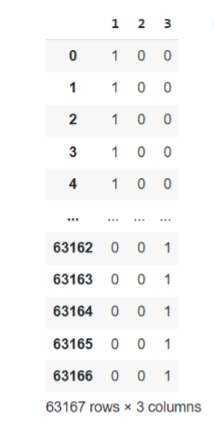
**Dropping the Column**



In the 'df' dataset, the values that contain integer type and 32-bit values, by applying the drop() function, in 'x' the files are being dropped.

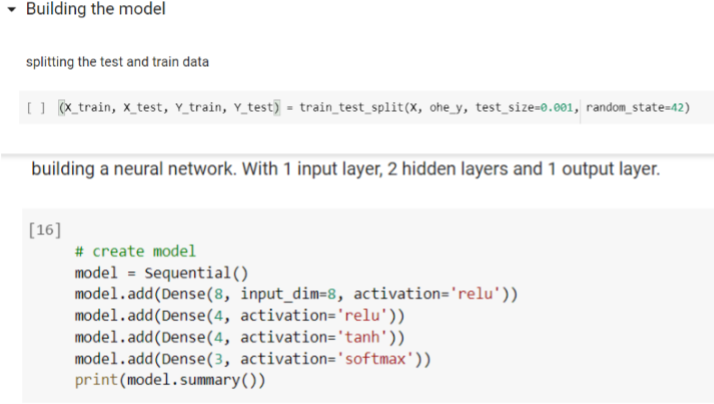
**Encoding the Dummy Variables**

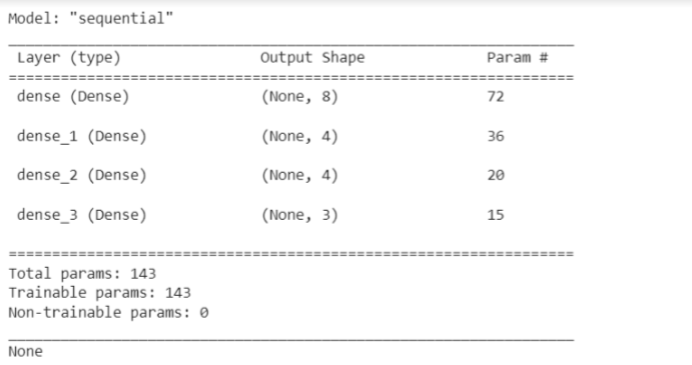




With the help of a dummy variable, with k-1, dummy encoding has been performed here.

**Checking the Parameters**



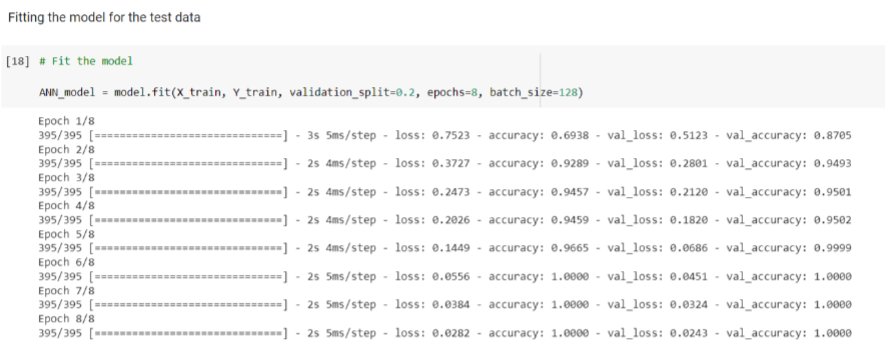


In the above section, with the summary() function, the layer, shape of the output and Parameter are checked and the output which has come shows that there is a total 143 number of Parameter, amongst which all 143 are trainable and thus there is need to perform the data pre-processing.

**Compilation**

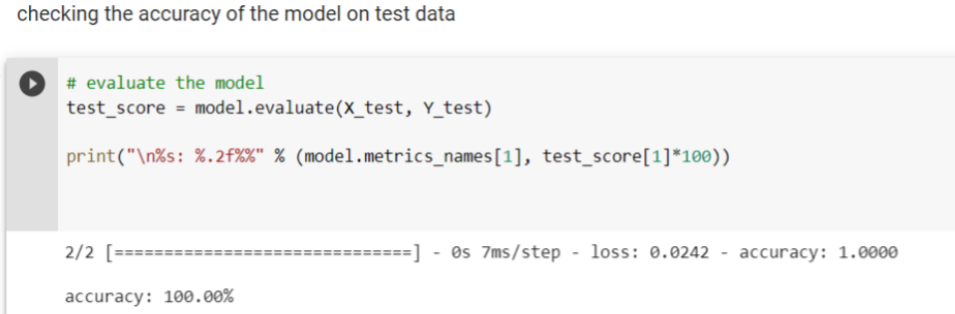


In this section, the dataset is compiled to check their accuracy.



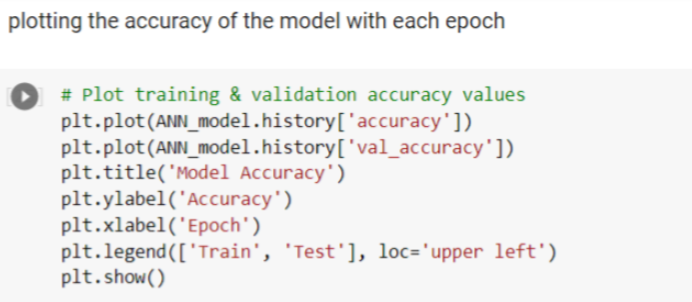
In this process, the Epoch is the iterations occurring with every step.

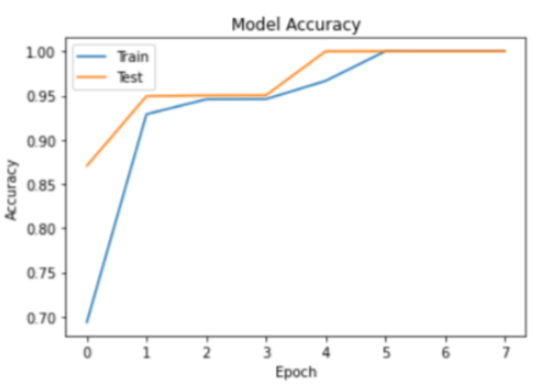
**Accuracy**



In this section, the accuracy is checked and the outcome has come in 100%. It has the most accuracy in enhancing security measures.

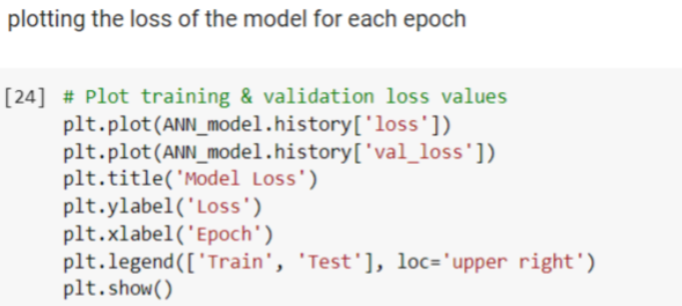
**Plotting the Accuracy with Epoch**

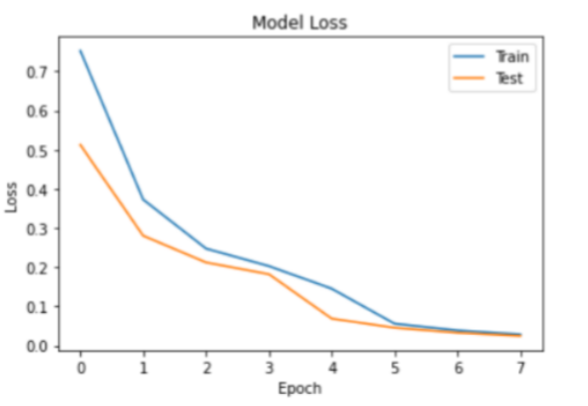




In the above section, the plotting is done with each Epoch where in the Accuracy axis, and in the Epoch axis, it can be seen that the graph has gone to the top.

**Plotting the Loss**





In the above section, the loss that the dataset has faced has been shown. The loss is very minimal as shown in the graph.

# Chapter 3- Dissertation

## 3.1 Introduction

The research work has been conducted by making use of varied software applications to interpret the data accumulated. In this dissertation, the focus has been given to evaluating the part of the “deep learning” based blockchain to upgrade the privacy of the 5th generation encouraged “IoT framework”. In this paper python programming language has been conducted along with mentioning different critical analyses to support the evaluation of deep learning-based technology for enhancing the 5th Generation encouraged “IoT framework". The use of Python libraries has also been considered in the data analysis method such as NumPy, pandas, seaborn, sklearn model, matplotlib and Keras. Different Python libraries have been enabled to conduct varied analytical aspects along with making use of the varied aspects of deep learning have been critically described in this specific dissertation work. An in-depth analysis has been conducted in this paper to recognize the process of enhancing the security of the 5 G-enabled IoT framework by throwing light on some effective deep learning algorithms.

## 3.2 Arranging the materials and structuring the dissertation

In this area, the focus has been given to making use of “deep learning learning” methods on the dataset for interpreting and detecting the security enforcement process. This algorithm of deep learning is regarded to be the practical algorithm used for the 5 G networks to be proactive and predictive which is vital for 5G networks to significantly function.

Considering the deep learning algorithm the focus has been given to making use of a “Neural network” which is a variety of “artificial neural networks” (ANN), utilized for enhancing the privacy of the 5 G-based IoT framework along with remarkable efficiency with the huge datasets. Even the use of “deep learning” incorporates the complex depiction of the information automatically.

The "neural network" is a kind of supervised machine learning technique that is formed to mimic the process by which the brain works (Wu *et al.,* 2021). One of the significant uses of a neural network is mainly in security enhancement and this specific detection, as well as prevention system “IDS/IPS” along with next-generation firewalls, have exceedingly utilized machine learning along the neutral network to support detecting anomalies while reducing the false positives.

The "neural networks" are mainly utilized by the deep learning algorithm in this specific research paper for recognising the role in enhancing security presented in the dataset. In the paper "5G & LTE wireless" a data set has been used which has been taken from the "Kaggle" which is normally regarded as the website from where datasets can be taken and utilised the Neural Network. The security-enhancing process completely relies on the Neural Network which is one of the best deep learning algorithms for security-related purposes. Moreover, the use of Neural networks has supported in effectively recognizing the traffic, minimizing the rate of false alerts and supporting the security team in identifying bad and good networking activities (Zhou *et al.,* 2020). This considerable deep learning algorithm has helped in minimizing the issues in IoT security while paving the process for implementing the 5 G-based IoT effectively.

## 3.3 Summary

In this part, the security enhancement of the 5 G-enabled IoT framework was analyzed, and the implementation method of the deep learning algorithm was processed critically. A different aspect of deep learning techniques has been used that has been acquired through "python programming". In order to begin the data analysis, opening the data set that has the potential to enhance security is vital. This research paper has made use of the 5G & LTE wireless dataset while using Neural Networks. The concepts behind using this algorithm were that it enables us to undertake the larger dataset and help in developing a system that can acquire learning from the samples to resolve security issues and make predictions. The use of matplotlib libraries has enabled us to present a clear visualization as graphical visualization is considered to be more effective in terms of understanding the data. The considered research topic has reflected the different algorithms of deep learning. Some vital procedures like "data preprocessing", "data visualization", "dataset loading" and certain specific tests on the provided dataset were vital methods for such research on the security enhancement of the "5 G-based IoT framework'. The use of deep learning algorithms along with "python programming" has been clearly illustrated which was highly vital to analyze the considered research topic. The "Neutral network" model is a kind of deep learning algorithm that has been used in the research paper and is associated with the model whose performance analysis has been considered in the work. Not only that but different analysts have also been listed in the research paper. The research paper has laid emphasis on conducting every aspect of the deep learning algorithm implementation method to ensure that the readers can have in-depth ideas about the role of deep learning in improving security.

# Chapter 4- Discussion

## 4.1 Discussion

In the highly technological environment, things are upgrading but this has also increased security concerns. The “Internet of Things” is a technique that is linked to interrelated nodes, mechanical and digital machines, computing devices and the individual who is equipped with the capability to transmit information over communication without making use of human-to-human or “human-to-computer” communication. Every node has been provided with distinctive identities. The intervention of the IoT is the main concern for the current development. In the intelligent link area, there has been the utilisation of the Neural network algorithm for designing the adaptive algorithm to enhance the security of the 5 G-based IoT. The use of python programs and neural networks have been used to enhance security. In order to enhance security, the multiple protection model has used the first boundary security isolation. In this work, the focus has been given to making use of the “python programming language” and “Neutral Network" to improve the security concern of the 5 G-enabled IoT devices. The consideration of deep learning algorithms is effective when used to enhance the privacy of the procedure as it provides a huge dataset base. This method has the potential to detect all sorts of malicious activity that impact the confidentiality, integrity and information communication system.

## 4.2 Critical analysis

With the help of deep learning, a Neutral network to enhance the security of the 5 G-based IoT framework has been focused on. In this work, the focus has been given to five aspects. In the process, the first thing that has to be done is to read the acquired data. A neutral network has been used and the 5G & LTE dataset has been acquired from the Kaggle community. After this data pre-processing has been used in which the focus has been given to modifying the dataset as per the need by eliminating unnecessary data (Ullah *et al.,* 2020). This has enabled us to ensure that all sorts of security concerns need to be mitigated by enhancing the privacy of the 5 G authorised IoT framework. After this, the focus has been given to making use of exploratory data analysis. Exploratory data analysis enabled us to make use of graphics and visualization for exploring and analyzing the considered data set. The goal here is exploring, investigating and learning. In the process, the focus has been given to finding all variables and recognizing them after this dataset has been cleaned. Even correlated variables have been identified while selecting significant statistical methods. This indicated that there are no null values in the data set. After this data visualization is done after acquiring the result. In order to observe the efficiency level of the model an evaluation has been done to recognize the data. In the process of model accuracy, the security process accuracy of the 5 G-enabled IoT framework has been measured. This accuracy test thus helped to understand the accuracy of the model in a more critical way.

**4.3 Awareness of solutions to technical challenges**

In the process of acquiring the data, it was observed that certain technical challenges have been encountered. For instance, at the time of finding the data set, there were issues faced at the time of detecting the dataset. There was no presence of the exact dataset needed for enhancing the security of the 5 G-based IoT framework. In context to this after acquiring the data set that is to some extent similar to the requirement has been extracted and customized. The next issue was encountered at the time of visualization. In order to understand the data segmentation has been done to ensure that the data acquired have some meaning and help in providing in-depth ideas. The data set has been segmented into two domains one “trend data set” and the other “test data set” (Ahmed *et al.,* 2020). The trend dataset helped to trend the model to be prepared thus helping in upgrading security. The test data set helps to test the overall model prepared. This segmenting process of the dataset has resulted in developing challenges. The encountered challenge has been then mitigated by making changes in the dataset ratio. The dataset segmentation has been done at the ratio of 80:20. 80 ratio was done in the trend dataset and 20 ratios were in the test data set. This enabled the dataset to acquire the highest accuracy level and thus helped in resolving the segmenting issues.

**4.4 Use of tools and techniques**

This research paper has made use of the deep learning algorithm and Python programming to enhance the security of the 5 G-based IoT framework. In the process of developing the model, the focus has been given to making use of the tools and techniques, classifiers and libraries. In the process, the Keras library has been used for developing the deep model and it goes well with the Neural network. Numpy has been used for numerical representation of the data such as linear algebra and other mathematical operations on the array. Pandas library has been used for data analysis (Singh *et al.* 2020). The consideration of Pandas has enabled us to process and explore huge datasets by considering interfaces identical to Pandas. Sklearn is the most effective and robust library used here as it enables to undertaking of a selection of more effective tools for machine learning as well as statistical modelling incorporating regression, clustering, classification as well and dimensionality reduction. The use of matplotlib has been done in the process of developing the model as it enables help in visualizing the extracted data by transforming in graphics representation to ensure that data evaluation can be done in a more effective way. In this research work, a Neutral Network has been used as a classifier.

**4.5 Linkage to Objectives**

The main research objective is to learn the significance of this 5 G-activated IoT framework and enhance its security by making use of the deep learning algorithm. IoT cross-domain amalgamation considering the emergent technologies such as 5G and blockchain tends to impact the lives of humans. Thus exceeding the resilience of IoT requires focusing on privacy and protection circumstances. Making use of privacy via authentication, necessitates, access control, encryption and communication security is considered to be the main requirement. It has been seen that the Neural network enabled the enhancement of the scalability, reliability and performance of the 5 G-based IoT framework (Almutairi, 2022). The recognized solution helps in the security of operation as well as helping the IoT connectivity protocols to interoperate.IDS is among the most effective types of security network technology that is being used to secure the network. In regard to the experimental outcome, the proposed architecture for security enhancement helps in recognizing malicious activity. The utilization of the Neural network helped in detecting the approach of the attack in an effective way.

# Chapter 5- Evaluation and Conclusions

## 5.1 Critical Evaluation

In the paper, a 5th generation power security method is suggested on which a smart link has reflected the algorithm and developed the model for protection by designing it using neural network algorithm and python programming language and the required libraries. The strong link reflects the algorithm is dependent on the “deep learning” method to propose the considerable data transmission rate among the 5th generation extranet host as well as the “Zero Trust” security platform. The neural network-based protection model is developed by making use of sufficient libraries as well as CBR methodology. The classifier. There has been consideration given to conducting experiments on validating the efficiency as well as the effectiveness of the proposed model. The libraries that have been used have supported improving the model privacy concern and this mainly involved pandas, NumPy, Seaborn, and Sklearn. However, it was observed that undertaking the development of a deep learning algorithm for a 5 G-based blockchain application was quite challenging. The size of the dataset along with the quality of the data was an area of concern. However, the consideration of the small datasets and the significant network of deep learning will help in overfitting and will help in transiting data. It will result in considerably performing in a low-key manner toward the varied validation datasets. It has also been encountered that the acquired huge dataset was considerably cumbersome but the concerns related to privacy are considered with accumulating data. Thus it has been detected that the use of the data by augmenting the available data can be helpful in further managing the issues associated with a security concern.

## 5.2 Summary of the Achievements

The study has depicted the scope of making use of deep learning as well as its varied model for detecting its role in the security enhancement of the 5 G-based IoT framework. It was found that the deep learning algorithm is among the most utilized algorithms in the 5th-generation wireless network. The neural network framework was able to detect the user equipment position in the 5th-generation network. It has been viewed till now that data learning applications can help in enhancing the security of the 5 G IoT model making the model more secure. Neural Network algorithms help in security by supporting intrusion detection and prevention models and providing next-generation firewalls. Neural networks are also regarded as ANNs that support boosting data security.

## 5.3 Reflection

After conducting the overall dissertation, I must have stated that I have considerably acquired the wisdom of making use of the deep learning algorithm in security enhancement for the 5 G-based IoT framework. I have detected that this research work has focused on the drawbacks as well as advantages of the Neural network algorithm. I have also stated that the overall format that is used by me in an effective way is also an effective way to depict the main idea of constructing this entire research work. Further, at the time of formulating this work, different models, diagrams, frameworks, methodology and analytical interpretations have been significantly utilized to evaluate the findings of the research effectively. Along with this, I have found that deep learning algorithms such as Neural Networks have played quite a considerable role in enhancing the security concerns of the 5 G-based IoT model. Not only this, but I have also detected the significant way, design, ethical consideration and testing process to be used in this research to ensure that the research result can be legitimate. Even though there has been a considerable scope that has been identified at the time of conducting the work.

## 5.4 Future work

In spite of the huge success acquired by making use of the deep learning classifier, an enormous dataset is a key element. The implementation of the “deep learning” algorithm in data analytics tends to extensively rely on the present datasets. Nevertheless, it is detected that at present there is no 5 G scale data presence publicly for benchmarking the deep learning and neural network in the 5 G. The directional accuracy mainly for the significant and well-stable 5G ecosystem is yet to identify optimacy. It is stated that traffic manners learning in training the learning space in actual time is reliant on underpinning learning. This needs to be extended by 6G. Further accumulating the system logs by considering the 5 G wireless interaction system tend to be critical due to privacy concern, and disturbance in the network along with the continuous repetition in the scenario. The live information in the 5G wireless mobile network acquires user information which is naturally confidential and not every user likes to expose the data to a third party. This concern indicates the future scope of the research work. The article can indeed be utilised by the upcoming researcher as the vital aspect and existing researchers can make use of it to significantly recognize the area that needs further development.

## 

# Reference list

Ahmed, I., Anisetti, M., Ahmad, A. and Jeon, G., 2022. A multi-layer deep learning approach for malware classification in 5G-enabled IIoT. IEEE Transactions on Industrial Informatics.

Ahmed, I., Anisetti, M., Ahmad, A. and Jeon, G., 2022. A multi-layer deep learning approach for malware classification in 5G-enabled IIoT. *IEEE Transactions on Industrial Informatics*.

Ahmed, I., Zhang, Y., Jeon, G., Lin, W., Khosravi, M.R. and Qi, L., 2022. A blockchain‐and artificial intelligence‐enabled smart IoT framework for sustainable city. *International Journal of Intelligent Systems*.

Almutairi, M.S., 2022. Deep learning-based solutions for 5G network and 5G-enabled Internet of vehicles: advances, meta-data analysis, and future direction. Mathematical Problems in Engineering, 2022.

Almutairi, M.S., 2022. Deep learning-based solutions for 5G network and 5G-enabled Internet of vehicles: advances, meta-data analysis, and future direction. *Mathematical Problems in Engineering*, *2022*.

Butler, C., Wilson, P., Abrahamson, V., Mikelyte, R., Gage, H., Williams, P., Brigden, C., Swash, B., Rees-Roberts, M., Silsbury, G. and Goodwin, M., 2022. Methodology. In Optimum models of hospice at home services for end-of-life care in England: a realist-informed mixed-methods evaluation. National Institute for Health and Care Research.

Conlin, R., Erickson, K., Abbate, J. and Kolemen, E., 2021. Keras2c: A library for converting Keras neural networks to real-time compatible C. Engineering Applications of Artificial Intelligence, 100, p.104182.

Hewa, T.M., Kalla, A., Nag, A., Ylianttila, M.E. and Liyanage, M., 2020, October. Blockchain for 5G and IoT: Opportunities and challenges. In *2020 IEEE Eighth International Conference on Communications and Networking (ComNet)* (pp. 1-8). IEEE.

Jagannath, J., Ramezanpour, K. and Jagannath, A., 2022, May. Digital Twin Virtualization with Machine Learning for IoT and Beyond 5G Networks: Research Directions for Security and Optimal Control. In *Proceedings of the 2022 ACM Workshop on Wireless Security and Machine Learning* (pp. 81-86).

Kumar, N.M. and Mallick, P.K., 2018. Blockchain technology for security issues and challenges in IoT. *Procedia Computer Science*, *132*, pp.1815-1823.

Mistry, I., Tanwar, S., Tyagi, S. and Kumar, N., 2020. Blockchain for 5G-enabled IoT for industrial automation: A systematic review, solutions, and challenges. *Mechanical systems and signal processing*, *135*, p.106382.

Mukherjee, P., Barik, R.K. and Pradhan, C., 2021. A comprehensive proposal for blockchain-oriented smart city. In *Security and Privacy Applications for Smart City Development* (pp. 55-87). Springer, Cham.

Pandey, P. and Pandey, M.M., 2021. Research methodology tools and techniques. Bridge Center.

Qatawneh, M., Almobaideen, W. and AbuAlghanam, O., 2020. Challenges of blockchain technology in context of the internet of things: A survey. *International Journal of Computer Applications*, *175*(16), pp.13-20.

Rathore, S., Park, J.H. and Chang, H., 2021. Deep learning and blockchain-empowered security framework for intelligent 5G-enabled IoT. IEEE Access, 9, pp.90075-90083.

Sarker, I.H., 2021. Deep cybersecurity: a comprehensive overview from neural network and deep learning perspective. SN Computer Science, 2(3), pp.1-16.

Sharma, P., Jain, S., Gupta, S. and Chamola, V., 2021. Role of machine learning and deep learning in securing 5G-driven industrial IoT applications. *Ad Hoc Networks*, *123*, p.102685.

Sharma, P., Jain, S., Gupta, S. and Chamola, V., 2021. Role of machine learning and deep learning in securing 5G-driven industrial IoT applications. *Ad Hoc Networks*, *123*, p.102685.

Sial, A.H., Rashdi, S.Y.S. and Khan, A.H., 2021. Comparative analysis of data visualization libraries Matplotlib and Seaborn in Python. International Journal, 10(1).

Singh, S.K., Azzaoui, A.E., Kim, T.W., Pan, Y. and Park, J.H., 2021. DeepBlockScheme: A deep learning-based blockchain driven scheme for secure smart city. *Hum.-Centric Comput. Inf. Sci*, *11*, p.12.

Singh, S.K., Salim, M.M., Cha, J., Pan, Y. and Park, J.H., 2020. Machine learning-based network sub-slicing framework in a sustainable 5g environment. *Sustainability*, *12*(15), p.6250.

Sodhro, A.H., Awad, A.I., van de Beek, J. and Nikolakopoulos, G., 2022. Intelligent authentication of 5G healthcare devices: A survey. *Internet of Things*, p.100610.

Subba Rao, V., Chandra Shekar Rao, V. and Venkat Ramulu, S., 2021. Secure Architecture for 5G Network Enabled Internet of Things (IoT). In Proceedings of the International Conference on Paradigms of Computing, Communication and Data Sciences (pp. 659-672). Springer, Singapore.

Trivedi, M., Kakkar, R., Gupta, R., Agrawal, S., Tanwar, S., Niculescu, V.C., Raboaca, M.S., Alqahtani, F., Saad, A. and Tolba, A., 2022. Blockchain and Deep Learning-Based Fault Detection Framework for Electric Vehicles. *Mathematics*, *10*(19), p.3626.‘

Ullah, Z., Al-Turjman, F., Mostarda, L. and Gagliardi, R., 2020. Applications of artificial intelligence and machine learning in smart cities. *Computer Communications*, *154*, pp.313-323.

Vagizov, M., Potapov, A., Konzhgoladze, K., Stepanov, S. and Martyn, I., 2021, October. Prepare and analyze taxation data using the Python Pandas library. In IOP Conference Series: Earth and Environmental Science (Vol. 876, No. 1, p. 012078). IOP Publishing.

Wu, Y., Wang, Z., Ma, Y. and Leung, V.C., 2021. Deep reinforcement learning for blockchain in industrial IoT: A survey. *Computer Networks*, *191*, p.108004.

Xihua, Z. and Goyal, S.B., 2022. Security and privacy challenges using IoT-blockchain technology in a smart city: critical analysis. *IJEER*, *10*(2), pp.190-195.

Zhou, S., Huang, H., Chen, W., Zhou, P., Zheng, Z. and Guo, S., 2020. Pirate: A blockchain-based secure framework of distributed machine learning in 5g networks. *IEEE Network*, *34*(6), pp.84-91.

Ziogas, A.N., Ben-Nun, T., Schneider, T. and Hoefler, T., 2021, June. NPBench: A benchmarking suite for high-performance NumPy. In Proceedings of the ACM International Conference on Supercomputing (pp. 63-74).