Czech University of Life Sciences Prague

Faculty of Economics and Management

Department of information engineering

Bachelor's Thesis

IoT Network Design and Cloud Networks

Kaushal Patel

Declaration

I declare that I have worked on my bachelor's thesis titled "IoT Network Design and Cloud Networks" by myself and that I have used only the sources mentioned at the end of the thesis. As the author of the bachelor's thesis, I declare that the thesis does not violate any copyrights.

in Prague on 15.3.2023 Signature

Acknowledgement

I would like to thank my thesis supervisor, Dr. Josef Pavlicek, for his great support and understanding in the completion of this thesis. His irreplaceable encouragement led me to this success.

I would like to express my sincere thanks to my faculty members and the Czech University of Life Sciences, Prague, for their support during my graduation.

I would like to finish by thanking my parents for their constant help, support, and love.

ABSTRACT

Incredible technological advancements in telecommunications technology and the internet have revolutionized the use of electronic devices in the present time. This spectacle presents wonderful opportunities for the use of IoT devices to make our lives better. Sensors and actuators are the backbones of IoT technology. IoT application developers have used the cloud as a universal computing resource and a backend for storage. IoT devices produce a massive volume of data and put significant pressure on the internet. Growing concern over the security aspects of IoT networks can diminish the progress and use of this marvelous technology in daily life applications. Privacy, safety, scalability, latency, bandwidth availability, and durability control are some of the major concerns. It is time to concentrate efforts to address these aspects in order to create a progressive environment for technology to prosper and benefit humankind. There is an ensuing need to develop an effective cloud-based IoT network design to mitigate the growing concerns. This thesis aims to investigate the various entities of network design, along with cloud computing networking systems, and suggest the best possible solution for enhancing the user experience. In this research, we have analyzed various issues regarding IoT network design and cloud networks. Research objectives were enlisted, followed by research methodology. This research is primarily based on qualitative research methodology and a profound literature review. Comparative studies and statistical analysis were performed using t-test formulation and analysis methods. Based on the derived results, recommendations were made to improve the cloud-based IoT networking design.

Keywords

IoT, Internet, cloud network, network design, sensors, actuators, cloud computing

ABSTRAKTNÍ

Neuvěřitelný technologický pokrok v oblasti telekomunikačních technologií a internetu způsobil revoluci v používání elektronických zařízení v současné době. Tato podívaná představuje skvělé příležitosti pro využití zařízení internetu věcí ke zlepšení našeho života. Senzory a akční členy jsou páteří technologie IoT. Vývojáři aplikací IoT využili cloud jako univerzální výpočetní rezervu a backend pro úložiště. Zařízení IoT produkují obrovské množství dat a vyvíjejí značný tlak na internet. Rostoucí obavy o bezpečnostní aspekty sítí IoT mohou snížit pokrok a používání této úžasné technologie v aplikacích každodenního života. Soukromí, bezpečnost, škálovatelnost, latence, dostupnost šířky pásma a kontrola trvanlivosti jsou některé z hlavních problémů. Je načase soustředit úsilí na řešení těchto aspektů, aby se vytvořilo progresivní prostředí, v němž technologie prosperuje a přináší prospěch lidstvu. Z toho plyne potřeba vyvinout efektivní návrh sítě IoT založený na cloudu, aby se zmírnily rostoucí obavy. Tato práce si klade za cíl prozkoumat různé entity návrhu sítě spolu se síťovými systémy cloud computingu a navrhnout nejlepší možné řešení pro zlepšení uživatelské zkušenosti. V tomto výzkumu jsme analyzovali různé problémy týkající se návrhu sítě IoT a cloudových sítí. Byly uvedeny výzkumné cíle a následně metodologie výzkumu. Tento výzkum je založen především na metodologii kvalitativního výzkumu a důkladném přehledu literatury. Srovnávací studie a statistické analýzy byly provedeny za použití t-testu formulace a analytických metod. Na základě odvozených výsledků byla vydána doporučení ke zlepšení návrhu sítě IoT na bázi cloudu.

Klíčová slova

IoT, Internet, Cloudová síť, Návrh sítě, senzory, akční členy, Cloud computing.

Table of Contents

Table of Figures

1.Introduction

The Internet of Things (IoT) is now one of the most significant and promising technical issues. By 2020, up to 50.4 billion linked devices are expected to be available. The IoT comprises things that can gather and exchange information every day, such as physical gadgets, buildings, and vehicles with embedded software, electronics, sensors, and network connections. An IoT network comprises physical devices that gather and transmit data from the surrounding environment through the Internet. The IoT may transfer the data across a network without any interactions between people. In many areas, like smart cities and intelligent houses, the IoT plays a crucial role. Two distinct kinds of devices, sensors and actuators, are included in the IoT network (Cui, 2016). The sensor is a device capable of detecting environmental changes. Various sensors, such as heat, moisture, pressure, motion, and thermal sensors, are accessible on the market. Actuators are employed based on the sensor data to execute a particular action. The IoT not only detects and analyses data but also enables different devices to operate based on data dynamics. IoT automation is based on sensor and actuator combinations. Therefore, we may conclude that the IoT's backbones are sensors and actuators.

The IoT provides a massive volume of big data, placing an enormous amount of pressure on the Internet. In managing data storage, cloud computing plays an important role. The strain on the Internet infrastructure may be reduced using cloud computing. Cloud computing simply implies that a centralised pool of computer resources accesses data and applications. Both cloud computing and IoT are complementary, and both help make daily activities more efficient. IoT produces a huge volume of data and offers storage and calculation of that data on the cloud. Cloud computing also gives software engineers better collaboration. Cloud computing enables the developer to store data readily accessible from a distant source.

The age of cloud computing has introduced many new methods in our everyday lives for using smart devices and objects, paving the path for the internet of things. This allows the employment of embedded technology, which allows it to communicate with the external world and exchange information through the internet effortlessly. Although the IoT cloud network has had a beneficial impact since its debut, the dangers involved, which are a barrier to the adoption of this technology, cannot be simply ruled out (Al Mtawa et al. 2018). In particular, security concerns in IoT cloud networks involve the security of communication and the privacy protection of end users. In this situation, a good user is always able to share the same network as a malicious user. A fraudulent user's traffic may cause a deterioration in other sensors'

performance and may also create incorrect invoicing concerning other virtual network nodes. The Cloud Services Provider (CSP) is important for traffic management and monitoring of different IoT nodes. Different challenges make traffic management difficult for CSP, such as the confidence of a user group that shouldn't be shared with CSP and IoT node mobility support for CSP, which makes it very difficult to manage traffic.

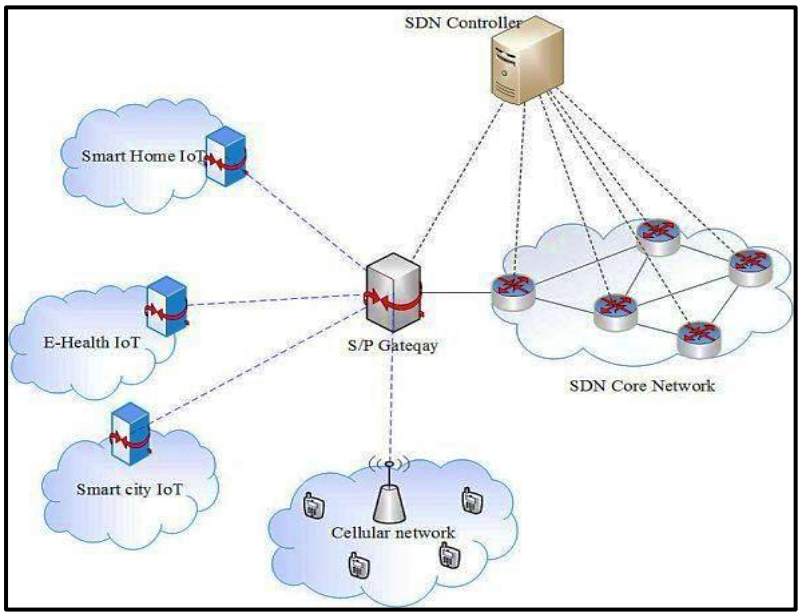

Figure 1:IoT Network Design (Source: Alkadi et al. 2020)

pt behind the work is to create secure communication with IoT nodes, located inside various groups of users in different virtual networks, between the cloud services provider. The cloud service provider and user groups communicate via a public channel. The CSP thus assigns the user groups' duties to each other. There may also be instances in which the IoT nodes located in one user group want to interact with the various IoT nodes situated in another user group inside another virtual network, which may be intercepted when they transmit via a public channel between the CSPs and user groups.

2. Research Objectives and Methodology

This section focuses on the research that the author did. The research was carried out in two ways: primarily using surveys and secondarily through analysing existing studies and literature. The next section addresses the study's goals, sample selection, research methods, quantitative research findings, quantitative analysis findings, a comparison of the theoretical and practical portions of the study, and a conclusion.

2.1 Research Thesis Objectives

The prime research aim of this thesis is to dig more deeply into the various entities of network design along with the cloud computing networking system. The research objectives are to identify the necessities to fulfil the aim of the research.

The different objectives of the research include:

- to research out the most effective designs of IoT and cloud networks.
- to find out the advantages and disadvantages of cloud-based IoT networks.
- to identify the method through which the IoT network design and cloud networks support each other.
- perform and implement the framework or system to improve the entire cloud computing and IoT network design.

2.2 Research Methodology

The research methodology deals with the method through which the execution of the process would be performed to get the desired result. Aiming toward this thesis and the topic, the primary research methodology that will be adopted is a profound analysis of a detailed literature review. The literature review will cover the entire framework of IoT network design as well as cloud computing. Through critical appraisal, the significant entities will be picked up to fulfil the objectives. Apart from that, secondary or desk research will be adopted. Existing data will be collected and summarised to improve overall research efficacy. Along with the literature review, several other research covers, research papers, and related materials released in research reports will be appraised. Public libraries, websites, and data from surveys that have already been completed may make such materials accessible. Benefits from different research institutes and help from the worldwide web will be taken to further improve.

One of the best ways of achieving large data and response from everyone is through surveys. The survey was carried out using google forms as it is one of the simplest and best solution when it comes to such things. The survey was aimed to collect around 100 responses, and in the end, 82 responses were achieved. The respondents were contacted through social media like WhatsApp, LinkedIn, Facebook, Instagram etc. The main aim was to reach people who were at least studying or working in the IT field, so that the most accurate result could be achieved.

The survey was designed in such a way that it started with asking basic questions of age and gender, to find the segment of respondents, and then it developed further into main questions related to the research. Questions were either in MCQ style, scale of 1-10 and yes/no questions.

This section focuses on the research that the author did. The research was carried out in two ways: primarily using surveys and secondarily through analysing existing studies and literature. The next section addresses the study's goals, sample selection, research methods, quantitative research findings, quantitative analysis findings, a comparison of the theoretical and practical portions of the study, and a conclusion.

3.Literature Review

IoT is among the most touted ideas in the computer industry nowadays. On a massive scale, cloud-based IoT systems may potentially surpass IoT. However, both of these have genuine uses and may become significant to your company. The basic interpretation of IoT is that it involves tangible Internet-related stuff. Sensors may measure and transmit your data over the internet, usually back to the distant "edge" server situated in the same region. Things on the internet may also take instructions received via the internet and act on them. The physical items that comprise the IoT can transmit assessments and obtain information most efficiently.

3.1 Choosing an IoT Cloud Platform

According to Huang et al. (2020), "the Internet" is not an endpoint but an interrelated set of data-transmitting networks. For the IoT, distant endpoints typically lie on a cloud server rather than within a private data centre on a single server. Running a server in the cloud enables all data to be placed in cloud storage and used by the machine to forecast the optimal water flow. It may be as advanced and flexible as the user's desires. Furthermore, operating in the cloud provides savings. The server does not need to stay connected for the remaining hour if sensor reports arrive once per hour. The input data will spin up to save data and then distribute its resources in a "serverless" cloud setup. After a delay, the addition and processing of fresh data are activated, and irrigation water flow is changed if necessary. The system will continue to function in our example of irrigation if the cloud server reaction time is one hour. Other techniques are much less lag-tolerant.

According to Javadpour et al. (2020), the cloud can also continuously transmit its data but cannot change its throttle, brakes, or steering on a remote server. This is one of the key teachings of an introduction to the course of controlling systems technology: Drill down the control feedback loops to the lowest level feasible. Yes, a remote monitor may alter the location or the plan of the road, but all time-conscious activities must be handled by the vehicle itself.

3.2 Essential Features of Cloud IoT Networks

A cloud IoT platform must monitor IoT endpoints and event streams, evaluate information locally and in the cloud, and allow the creation and deployment of applications. These are the most important functionalities for almost every IoT solution. The IoT platform requires access to cloud storage to allow cloud analysis and application development. A lot of data may be stored on industrial IoT devices and vehicles, even though, for long-term analytical reasons, it

may be filtered or aggregated. In terms of network and protocol conversions, industrial IoT may also present a problem (Faizullah et al., 2020). For Ethernet and TCP/IP, old-style industrial programmable controllers were not manufactured. The data from edge devices to the cloud platform is being transported to another piece of the jigsaw. Wired Ethernet or Wi-Fi are often available for interior applications. Any use of cellular data is widespread for external applications, including the farming category, which uses mobile M2M plans rather than cellular plans that are much more costly. This may be helped by managed IoT connection services. Some of these services mainly involve the management of SIM cards and associated data; wider IoT platforms also include cutting-edge devices and agents. Beware: Some established M2M services incorporate "IoT" without adding actual IoT capabilities to their branding.

3.3 Considerations for the IoT Platform

Users should first define their own needs and outline the monitoring, analysis, management, and application designs that may satisfy them rather than just switching to an appealing IoT cloud platform. Figure out the user interface, data, and design decisions before diving into the technology. Try to avoid the design of the particular device, its OS, gateway, border platform, networking, a protocol for connectivity, and cloud platform. Rather, first design generically. Figure out the most essential characteristics for your application and utilize this list to guide the choice of the platform.

It may be difficult to anticipate and easy to underestimate cloud-based IoT expenses. Part of the issue is the complexity of cloud pricing. Another issue is that cloud IoT solutions usually provide an initial discount (Mahajan & Kaur, 2021). You may be in for an unpleasant surprise when costs increase if you depend on the initial rate. Finally, the expense of data storage is easy to ignore, and a long-term plan to delete outdated and irretrievable data is difficult to execute.

Some suppliers provide strong, almost complete systems that may be readily adapted to any application. Other suppliers provide some of the parts users need, but they need to integrate and customise them considerably more, either internally or via consultants.

3.4 Differences between Fog and Edge Computing

Fog computing or even edge computing have nearly the same functionality and objectives that concentrate on the transfer of the data processing and analysis inside a local network closer to the actual source of its origin. Two technologies were specially developed to replace part of cloud computing and eliminate certain problems related to internet connectivity. Information analysis and processing processes may thus be performed more quickly and efficiently. The actual distinction between the two lies in the manner in which the processing takes place—how and where precisely. According to Abbasi et al. (2021), Edge data management operates directly on devices that are connected and tied, without transmitting data to IoT devices like sensors or cameras. Fog computing, however, results in data processing at a fog node or IoT gateway inside the LAN, thus being positioned remotely. The real aim for users is to establish a balance between the storage and transit of data between cloud computing and fog/edge computing, if necessary, to combine their benefits and characteristics.

3.5 Types of IoT Cloud Networks

A huge number of digitally driven technological developments, encompassing all aspects of our existence, offer new and unprecedented creative possibilities for improving quality of life and simplifying job performance. In the development of intelligent interactions between people and the surrounding entities and items, the Internet of Things (IoT) plays an incredibly vital role (Kayes et al. 2020). It is also of great significance when it comes to the acquisition, transmission, processing, and analysis of data from different sources, both for people and big businesses, whether from sensors, cameras, or other devices.

Since such systems gather data on a continuous basis, the total information volume is so enormous that particular tools and application services must be stored and used efficiently. Most businesses move to IoT cloud platforms to save costs, speed up production processes, and utilise the information collected from different devices.

Microsoft Azure IoT Hub

Microsoft is a renowned digital and IT developer and now provides its services in IoT marketing. The multi-industry requirements of a Microsoft Azure IoT hub, including remote monitoring, smart spaces, and previsualize maintenance, are being developed. It offers a high

data security level and excellent scalability, enabling you to select and pay for the precise services you now require, with different features and functionalities.

For every kind of company, Microsoft Azure is an excellent option. It may be utilised by both novices and professionals, despite the inherent complexity of IoT architecture. Sadly, Azure has to be professionally maintained, monitored, and corrected when transferring your company computer from your office to the cloud.

Google Cloud Platform

Google Cloud offers one of the most effective and scalable cloud computing platforms for IoT applications. Its primary aim is to make things quick and simple, to achieve the quickest input and output, and to offer dependable, secure, and large storage of data, which allows you to connect, store, and manage IoT data without any problems. Google's global fibre network and connectivity with other Google services will give you the edge. Google Cloud prices may vary depending on your specific company requirements and involve many variables, such as chosen data storage, network and operational use, and data recovery choices (Sadeeq et al., 2021). Google Cloud Platform offers excellent, easy-to-use capabilities and a large, multi-functional structure, but the bulk of the components are Google-based technology with a restricted range of languages.

IBM Bluemix

Bluemix is the cloud-based IoT platform for all kinds of applications with adjustable pricing and safety layers for developing, managing, monitoring, and operating. It also supports a DevOps system and open-source APIs, as well as several programming languages that provide both PaaS (Platform-as-a-Service) and IaaS platforms. With a PaaS, it may work with the apps in the cloud, as well as on-site settings, using the Cloud Foundry open-source IoT platform. During IaaS, businesses may utilise IT resources over the internet, including computer power, storage, and networking. It is quite difficult for a novice to gain an insight into the complicated architecture and interface.

Oracle IoT Architecture

Oracle is one of the finest cloud platforms, offering diverse features and supporting connections with Oracle and non-Oracle apps and IoT devices through a REST API for manufacturing and logistics operations. Oracle has a total rating of 4.4 as per Gartner's list of IoT platforms. The primary aim of the company is to enhance and improve the supply chain, customer experiences, and operational efficiency by utilising high-speed messages and endpoint management to help you reach the market as quickly as possible (Beitelspacher et al. 2020). Users may connect their device to the cloud by utilising the Oracle IoT cloud platform, conduct research in real-time, and integrate the obtained data with the applications or Web services of this business.

Cisco IoT Cloud Connect

To develop relationships with clients and partners, Cisco is one of the world's leaders in the field of IT services. Cisco IoT Cloud Connect is a mobile operator-based cloud-based software package that optimises and streamlines the network, security, and data management, as well as the IoT experience. The Cisco IoT cloud protects the control system against hacker assaults and human factor problems. It also allows various virtualized device deployment choices, coupled with in-hour visibility in real-time.

Alibaba IoT Architecture

It was thought that and named "the Chinese AWS," Alibaba is a fast-expanding business that forms a component of the Chinese eCommerce enterprise (Alibaba Group) with comparable structures and techniques. Alibaba IoT Platform provides all the key services like hosting, object storage, computer flexibility, relationship databases, big data analysis, artificial information, machine learning, and NoSQL databases, together with a range of flexible discount proposals for new customers. Alibaba is China's biggest supplier of clouds, but it also serves worldwide clients. It also offers tremendous possibilities for business seekers in the country.

SAP IoT Platform

SAP is a platform-as-a-service that offers seamless, multi-functional environments for developing, managing, monitoring, and operating cloud applications, including Cloud Foundry

and Neo. In recent years, it has become one of the top IoT cloud platforms with the latest technology to improve your company's productivity and optimise operational operations. This platform is built on SAP HANA, a database and application development platform especially intended to handle high-throughput data in real-time.

This SAP offers a broad range of capabilities for users, including several programming languages, DevOps, which serves the purpose of application development and user satisfaction, enables you to create customised user interactions, and much more (Shahryari et al. 2020). The SAP price is very costly and may be calculated to include up to three types of entities: medium-sized businesses, companies, and developers.

3.6 IoT and Cloud Networks' Most Efficient Designs

To enable businesses to obtain the full benefits from IoT infrastructure, cloud computing assists in storing and analysing this information. In this cooperation, the IoT solutions should link and enable communication between staff, people, processes, and cloud computing to provide a high degree of visibility. According to Vitunskaite et al. (2019), IoT is not limited to system connection functions, data collection, storage, and analysis alone. It helps to modernise operations via the connection of legacy devices and intelligent devices, machines with the Internet, and the reduction of barriers between IT and OT teams with a common view of the systems and data. Organizations do not need to install significant hardware, set up, and maintain IoT deployments using cloud computing. Cloud computing also allows companies without extra gear and infrastructure to scale up their infrastructure, depending on their requirements. This not only helps to accelerate the process of development but may also reduce development expenses. Because businesses just pay for utilised resources, they don't need to invest any money to buy, provide servers and other infrastructure.

3.7 Cloud Platform for Device Lifecycle Management

According to Ji et al. (2019), companies build cloud services (SaaS) apps and software that allow device registration, onboarding, remote device upgrades, and remote device diagnostics within a minimum timeframe with lower operating and maintenance expenses. In the IoT ecosystem, the cloud enables DevOps to enable businesses to remotely automate numerous operations. The problems with data security, control, and administration grow as more and more devices connect. Cloud services allow lifecycle management of IoT remote devices to play an important part in providing a 360-degree picture of device infrastructure. Some cloud

providers provide various IoT tools that make sure firmware and software are updated and installed easily (FOTA).

3.8 Enabling Cloud Platform Applications

Cloud allows portability and interoperability application development across various cloud configurations throughout the network. According to Zou et al. (2019), these are the advantages inter-cloud companies may profit from. Intercloud solutions include SDKs, on which companies may build their applications and software without worrying about the backend operations. For instance, Cisco offers an application enablement platform for application hosting, updating, and cloud deployment, whereby companies may operate and update programmes remotely. Businesses may transfer their apps to host applications and analyze or monitor data on key systems between the cloud and fog nodes.

Most cloud service providers concentrate on developing the cloud environment on OCF-based standards so that the majority of applications, appliances, and platforms enable machine-to-machine communication and device-to-device communication and are interoperable. Standardization by the Open Connectivity Foundation (OCF) ensures that devices may connect and communicate securely in any cloud environment that intraoperatively affects the world.

3.9 Types of IoT Solutions: Cloud Models

Three kinds of cloud computing models are frequently provided by the cloud service providers for various types of linked environments. Let's have a look:

Infrastructure as a Service

It provides companies with virtual servers and storage. Increasing critical data in the organisation leads to security vulnerabilities, and IaaS can help distribute the critical data in virtual or physical locations for security improvements (Saha et al. 2019). The organisation can also provide a computer, data storage, network connections, load balancers, and bandwidth for access to network components.

Platform as a Service

This allows businesses to develop software and apps using tools and libraries supplied by cloud service providers. It removes the fundamental needs of hardware and operating system

management and enables enterprises to concentrate more on the deployment and management of software or applications.

Software as a Service

It offers a whole programme or application operated by the cloud-based service provider alone. The user has to worry about the usage of the product and does not have to worry about the development and maintenance process that lies at its heart. Social networking networks and e-mail services are the best examples of SaaS applications. In addition, the providers of cloud services now provide IoT as a service (IoTaaS), which reduces efforts to build IoT software and hardware.

3.10 The advantages and disadvantages of these designs

The Internet of Things (IoT) is for the connecting of sensors, devices, and other items for the transmission and reception of data via the internet and other networks to transmit requests and instructions. Given this conventional definition and the decades since the IoT was developed, it is no wonder that the number of linked items has increased steadily. This has inevitably led to larger quantities of data being collected, which has made information processing and storage more complex in turn (Ren et al. 2019). Given the difficulties posed by the continuous growth of IoT—a trend that is anticipated to further amplify in the next 5G period—many organizations, in particular those with cloud-based IoT solutions, have resorted to cloud computing. Built on the concept of "rentable storage space," IoT solutions based on the cloud can adapt to the requirements of businesses in terms of integration, processing, scalability, and security.

3.11 Comparison of Conventional IoT Solutions Versus IoT Solutions Based on the Cloud

Cloud service providers have suggested solutions to their various business requirements for businesses. And as more companies move their workloads to the cloud to enjoy the advantages of the infrastructure, they may also extend their product features to further commercial possibilities. Companies that have previously used cloud services can provide more IoT-specific solutions with less expense than is usually necessary to enter the IoT market and without significantly changing the current product infrastructure. Sellers may also redefine some company elements to enhance them, such as addressing current security holes in the IoT

industry. Software-as-a-Service (SaaS) environments are ready to be developed, as are certification and authentication methods with API management resources available (Donassolo et al. 2019). Cloud providers may transfer their experience in cloud-based IoT advancements based on our study. The following table compares conventional IoT and cloud-based solutions' benefits and drawbacks across various business sectors, effectively showing their potential growth for companies.

3.12 Support for IoT Network Design and Cloud Networks

The Internet of Things (IoT) will continue to change both business and people's way of life. The backbone of this shift is cloud computing. Increased cloud usage has served as a springboard for numerous IoT applications and business models, enabling businesses to decrease market time and total ownership costs. Cloud computing offers businesses the capacity to store, administer, and scale applications and software as a service via a cloud platform (SaaS). A large quantity of data may be generated by IoT devices every second; Cisco predicts that by 2021, IoT will produce 847 zettabytes a year. IoT devices are often sensors that gather and transmit data for processing. In the IoT sector, before data is transferred to the cloud, actual sensors are virtualized. Although IoT devices may produce a lot of data, cloud computing opens the route to this data. This data helps developers to improve workflow, which may remotely store and access data so that projects can be implemented without delay.

Cloud computing allows for the fast and real-time storage and analysis of data, which allows firms to maximise their benefits. This is confirmed by an InformationWeek industry poll, in which 65% of respondents stated that it was one of the main reasons why a company moved into the cloud environment (Elmubarak et al. 2017). This results in "the capacity to fulfil business needs rapidly." Organizations don't need significant hardware deployed for cloud computing or network and infrastructure configuration and management. Cloud computing also allows companies to scale their infrastructure without having to put up new gear and infrastructure according to their requirements. This not only contributes to accelerating the process of development but may also reduce development expenses. Devices dependent on device connections are linked to the cloud in many ways. These include a cellular network, a satellite network, Wi-Fi networks, Low Power Wide Area Networks (LPWAN), and an Ethernet direct internet connection. Mobile connection is a great option for continuous data transmission between devices, apps, and the cloud.

Cellular systems for dependability, safety, and scalability have been developed. To provide great IoT coverage and quick time-to-market, cellular Internet of Things (CIoT) based on 3GPP standards uses existing infrastructure. Cellular IoT projects will comprise all of the devices, SIM cards, and administration platforms. CIoT gear always has SIM cards and can connect through 2G, 3G, or LTE networks, whichever cell tower is accessible across countries. As described in our earlier blog article, for example, 2G switch-off has begun in many areas of the globe.

The Internet and all-in-one computing created a new paradigm, the Internet of Things (IoT), through which many physical objects are linked to the Internet in trillions. These devices rely on several essential features to provide dependable communication in an IoT environment, including effective network optimization, architecture, protocols, security elements, and different services linked to distinct applications (Ibrahim et al. 2018). Today's IoT movement is seen as a future internet and includes billions of linked devices or things that utilise contemporary technology by stretching the world's boundaries to virtual and physical objects. IoT has had an important impact on the emerging market today during its dawning stage, with its use and application forecast for the next few years. It is predicted that by 2020, approximately 50 billion IoT-related products and gadgets will enable more and more IoT research and development activity to be carried out. In emergencies, IoT uses the internet as the technology to enable physical instruments or sensors to quantify, use the cloud for storing, and immediately trigger the alerting system. Consequently, by using various advanced technologies, including computer-based systems, artificial intelligence, integrated devices, multiple communication protocols and techniques, various services, and different Internet standards, the IoT is transforming current conventional devices into intelligent ones. By interconnecting different items and devices, IoT is intended to offer smarter services. In the IoT, traffic should be managed with a decentralised passion for applications like traffic management systems, where individual nodes share their traffic statistics and assist in planning traffic from each source, using data rates to prevent traffic jams. For example, fire detection, smoke detection, built-in health monitoring, and intrusion detection apps are designed for many IoT applications when the latency or jitter in the network is not optimal. The network should be sufficiently resilient in these applications to provide the data to the target system within a specified time frame, and optimal processing of these data should take place.

3.13 Considerations for Installation

Cloud environments provide enormous flexibility and are less concerned with physically connecting components. There is a smaller but more significant requirement for prior preparation. The initial criteria for installation include the following:

Elasticity and scalability

The number of sensors may be extremely high in an IoT design, and the related number might be much greater. In the case of linked vehicles with additional data like traffic and weather, this is further increased. For such data flows, IoT transformation and connectivity must provide scalable messages and scalable data transformation in the cloud. Elasticity is the capacity to provide and de-supply computer resources on-demand using cloud solutions as workloads change. Public clouds offer a clear benefit because bigger pools of resources are usually accessible (Yu et al. 2020). You will also profit from paying just for what you use. With greater bandwidth routes, private clouds and hardware can make a difference. The autoscale setup for the queue is not necessarily a one-off event; it is preferable to modify it as needed to prevent over- or undersubscription.

Bandwidth of Data

Big data must be optimised for public and private clouds. Large cloud data sets with rapid access are supported by fast and efficient data access processing components. This often implies that the processing of the data is moved, or vice versa. The physical location of data and processing may be easily disguised by cloud technologies. Tuning operations with little effect on deployed applications may be carried out continuously.

Supremacy of Data

The physical placement of the data may be controlled, although laws differ across countries. This applies in particular to PII and sensitive data such as health information and financial data. For instance, the European Union has strict rules for Europeans in terms of their PII. Consequently, any IoT cloud system must take care of the laws of data sovereignty and only store and process data at the places allowed by legislation that requires a cloud provider to give control over the storage and processing sites to a cloud service client.

Resilience

Resilience and tolerance of faults are extremely essential in IoT systems. At no time should IoT systems rely on one individual component and accept a single-component failure, such as a single IoT device. Components in the cloud provider may be robust via numerous program instances and cloud services linked to data replication and multi-storage redundancies.

Networks are also robust, e.g., with numerous routes and different network providers (Han et al. 2020). The whole network does not have a silver bullet but should be extremely robust and available. It is essential to guarantee that connection can promote resilience.

Computing and CPU

The availability of low-cost commodity manufacturers usually makes it very scalable for public, private, and hybrid cloud servers. These massively parallel systems are used by modern development environments like Hadoop, Spark, and I Python. Streams and high-speed analytics are emerging fields where cloud applications use stronger processing pools to provide in-motion data solutions in real-time. Hardware dedicated to hybrid and public areas may be developed and tested quickly before migration.

Volume of Data

In IoT systems, the data volume may reach a level with which conventional analysis tools and methods can no longer comply. So, it is extremely important to prepare carefully to store data in the public cloud, the private cloud, or conventional data centres. Data streaming in the event of weather or GPS mapping may lead to an enormous analytical data package. Every piece of data also loses its significance over time. The retention of data needs a little experiment unless regulatory or other rules explicitly apply (Haji & Ameen, 2021). Public clouds provide the freedom to store different quantities of data without prior preparation. In-house solutions for cloud storage may provide long-term storage costs when the volume is forecast.

Security

The difficulties of information governance and security grow as more data on individuals, financial transactions, and operational choices are gathered, processed, and kept. Cloud

computing is of great importance for data privacy and the management of devices and individuals. The cloud enables new compliance and monitoring technologies, which promote agile policy and compliance frameworks, to be deployed quicker.

Optimized supply

Optimized cloud supply may help you choose the appropriate product family for a certain set of user requirements.

3.14: Hybrid Cloud and IoT

A company regularly requires a mix of public cloud, private cloud, and locally connected hybrid cloud components. Hybrid cloud computing is a deployment paradigm that combines the usage of many cloud services across various deployment methods, especially in combination with the use of public cloud services and existing on-site systems. For additional information on hybrid cloud, see the CSCC Practical Guide for Hybrid Cloud Computing. The companies that adopt hybrid cloud solutions want flexibility and agility to provide new capabilities.

The Internet of Things is a vibrant and interesting field for information technology. In the next several years, several IoT systems will be established, encompassing many and diverse applications in various residential, commercial, industrial, health, and government settings (Deebak & Al-Turjman, 2020).

There are many different components in IoT systems, each with its own difficulties. Scale, speed, security, and privacy aspects are prevalent and need careful consideration in IoT systems.

3.15 The Advantages of Using a Cloud Platform in IoT

The IoT cloud platform brings together the IoT and cloud computing technology stacks to provide additional value for both consumer and enterprise applications. Indeed, the increasing use of cloud services has stimulated the growth of the Internet of Things across many corporate sectors, which allows for the extremely costly development of IoT on-site architecture. Putting your data in the cloud allows you to save money and has many other benefits. However, we need to examine two fundamental components that it relies on, an IoT and cloud computing platform, before we look at what makes an excellent IoT cloud solution.

The Internet of Things depends on IoT platforms for the supply, administration, and automation of intelligent devices inside a particular IoT infrastructure in a bid to bring physical subjects online and make them interact, cooperate, and behave intelligently without any human involvement. Every IoT environment is generally a mashup of technologies from different vendors that create a complex and naturally heterogeneous ecosystem that would remain fragmented, "stubborn," and eventually unable to function without a common foundation for integration (Huong et al., 2021). Thus, an IoT platform offers a meeting place for all of the linked devices and is used for data collection and handling throughout the network.

Cloud computing is available at the other end of the Things Cloud internet solution. Cloud computing is the newest technology to give consumers and business applications a new lease on IT services. One of the biggest benefits of clouding your IoT system is that it's easy to scale. In the event of sophisticated on-site network infrastructures, the expansion will need the acquisition of more hardware, more time, and more setup efforts to ensure appropriate operation (Zargar et al. 2021). On the other hand, adding more resources to a cloud-based Internet of Things system typically means renting another virtual server or more cloud space, which usually have the additional benefit of being deployed quickly. Furthermore, to restrict your storage needs or reduce the number of IoT devices, the IoT cloud services provide greater freedom.

It may be accessible from virtually anywhere in the globe because your data is saved and handled on cloud servers, which also implies it will not be linked by any infrastructure or network limitations. In IoT projects requiring real-time monitoring and control of linked devices, mobility is particularly essential. Although on-site data can only be translated inside the company's premises, a sophisticated internet cloud platform from Things will provide you with the capabilities to remotely and in real-time provide, manage, and upgrade your devices and sensors.

Security concerns, which since their creation have been an important worry for the IoT sector, may be hard to address. It's all a question of accountability in the cloud platform vs. on-site IoT infrastructure conflict. In the internal Internet of Things system, a large initial investment and higher risk for deployment may be a deterrent. Furthermore, the continuing expenditures on hardware and IT staff are at stake. Things seem better from the cloud's viewpoint. Significantly reduced start-up costs and a flexible pricing system based on current use entice IoT companies to migrate to the cloud (Sadeeq et al., 2021).

4. Architecture of The IoT Network

4.1 Building blocks of the IoT Network

Sensors

Sensors are the IoT devices' front ends, and their primary responsibility is to collect essential data from the environment and transmit it to the processing systems. Because they are the fundamental front-end interface in a vast network of other devices, they must be uniquely findable via their IP address. Sensors gather data in real-time and may either operate autonomously or be directed by the user.

Processors

Processors, like those found in computers and other electrical systems, serve as the IoT system's brain. Processors' primary responsibility is to convert raw data received by sensors into useful information. In a nutshell, it must add intelligence to the data. Processors are readily controlled by applications, and one of their most essential responsibilities is data security. They are in charge of data encryption and decryption.

Gateways

The primary function of gateways is to route processed data and send it to appropriate databases or network storage for suitable use. In other terms, a gateway facilitates data transmission. IoT systems need communication and network connections.

Applications

Another end of an IoT system is applications. Applications make appropriate use of all gathered data and offer users interfaces to interact with that data. These apps may be cloud-based programmes that are in charge of displaying the data gathered. Applications are user-controllable and serve as delivery points for certain services.

To summarise the components of the IoT, we may state that raw data collected by sensors is transmitted to embedded processors. Processors convert raw data into useful information, which is subsequently sent to distant cloud-based applications or database systems through

gateway device connections. It then moves to apps for appropriate application use as well as data analysis through big data.

4.2. The architecture of an IoT system

The architecture of an IoT system is divided into three levels. The number of layers and the deployment of IoT systems may vary depending on the requirements. These three levels may be used to describe IoT system architecture in general.

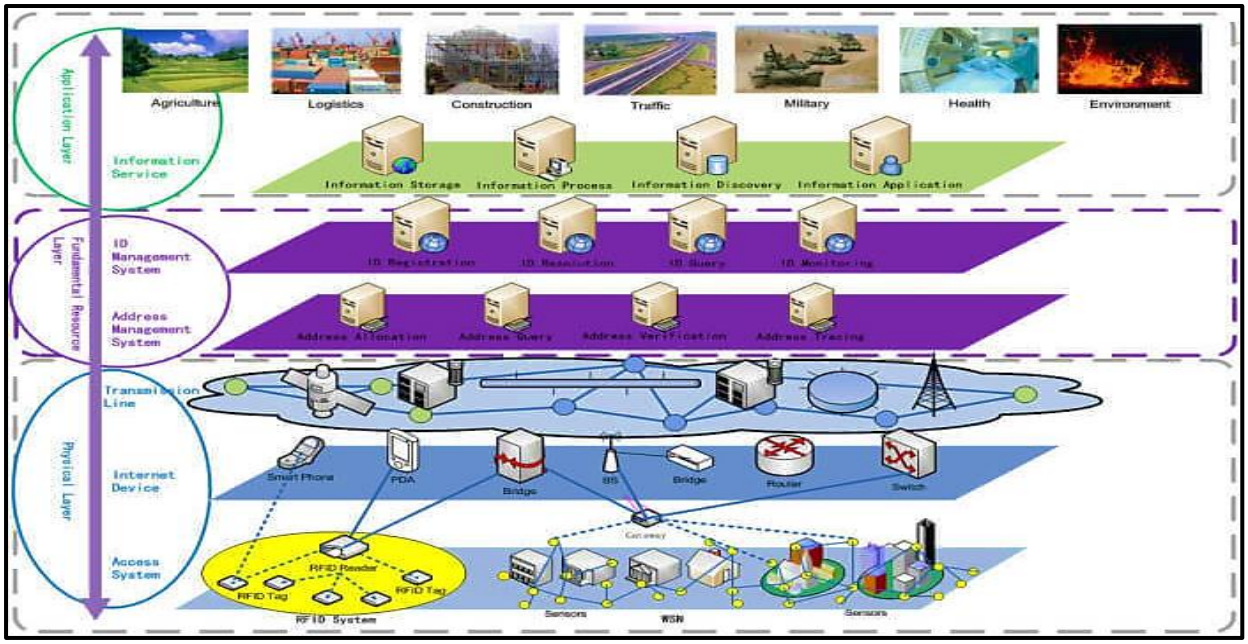

Figure 2:Layers of IoT network (Source: Mahajan et al., 2021)

The Physical Layer

The physical layer is made up of three types of devices. The first is an access system, which may include various sensors and RFID systems to gather raw data. The second category is Internet devices, which are mostly used for communication. Finally, transmission lines include all high-end communication equipment such as satellites, transmission hubs, and data networks. The primary function of the physical layer is to gather data and transmit it to appropriate cloud-based apps and database applications.

The primary resource layers

This layer is divided into two subsystems: the address management system and the IO management system. As previously stated, each item in the IoT ecosystem is uniquely

identifiable by its IP address. The address management system is a system that handles all of these devices in an IoT system. It handles all device address allocation, verification, and tracing. Another kind of system is the IO Management System, which controls all IO activities involving raw data. This system is made up of application and database servers that analyses the data. This system is in charge of IO registration, resolution, and monitoring.

The Application Layer

The application layer is the uppermost layer of the IoT architecture, and it is responsible for making efficient use of the data gathered. These apps mostly work with information to make it more meaningful. This layer offers Internet of Things (IoT) services. The application layer is in charge of information and data security. Certain circumstances require quick action. This layer aids in this process by extracting information, regulating data flow, and abstracting data.

4.3 The Basic Structure of an IoT Network

IoT allows physical things (IOT devices/objects) via a communication network to interact with things in the virtual realm, enabling them to share and exchange context-conscious information. As a consequence, every IoT system consists of physical, virtual, and communication systems. These three components are the main components of the IoT system. An IoT system is properly represented in the following block diagram.

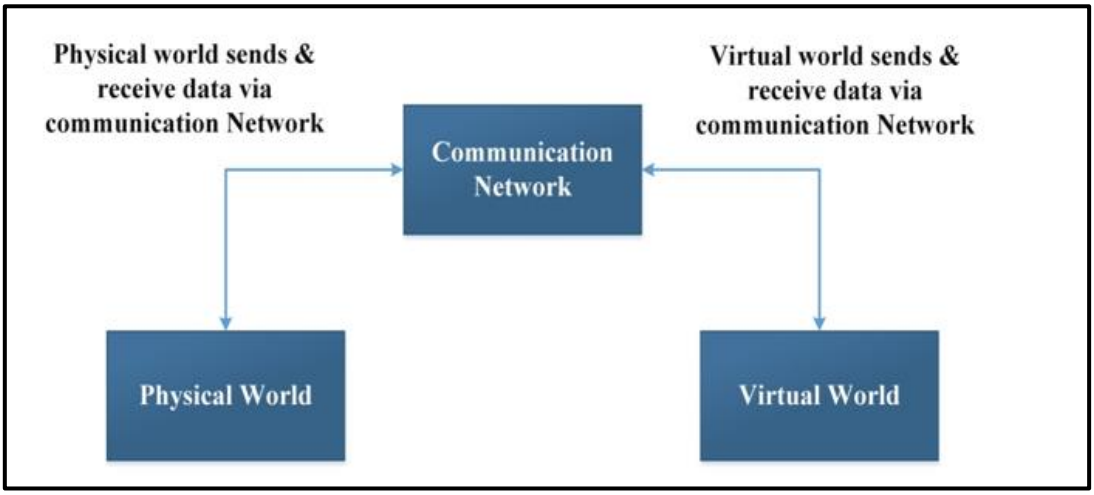

Figure 3:Basic structure of IoT network (Source: Nagaraj, 2021)

Things

It is any object that has a unique identity and is included in a communication network in the physical or information world. In nature, things may be physical as well as virtual. The physical items are often called "IoT" devices. IoT concepts vary from device concepts. The term "device" means a physical device that may interact through a network and be equipped with sensors, actuators, transformers, memory, and/or a controller, whereas "objects" may be both virtual and physical. Things like cloud service solutions may also be virtual. These virtual objects are independently exchanging and processing data through software programs, APIs, or application solutions.

Physical World

Real and virtual items may be present in an IoT system. In the IoT, a collection of items or devices is referred to as the "physical world." To build physical objects or devices, IOT boards are built around controllers or CPUs. IoT boards have a microcontroller or a CPU, are memory-restricted, and have one or more ports. They have generic input/output pins to connect to one or more sensors, actuators, or communication channels. This enables these physical devices to detect, collect, store, exchange, and analyze data, and operate one or more actuators to affect the real environment.

Virtual World

A virtual world is a collection of IoT systems for virtual things. Examples of virtual things include web, cloud, or mobile applications, APIs, or app platforms. With an IoT system, data recording, data extraction, and testing are very important for the virtual world or a collection of virtual items. Physical object data physics is shared with software applications, for which important insights or information needed for controlling actuators is stored, analyzed, and processed.

Communication Network

A link between a physical and a virtual world is provided by the Internet of Things. In theory, the IoT boards with sensors and actuators may communicate with online or cloud servers, as well as with each other; in practice, this is an extensive network or internet network. Each level

of communication offers several protocols for the secure and effective transfer of data. Data will be passed between the physical and virtual worlds with each data transmission, exchange, or insight.

4.4 The Architecture of the IoT System

Different businesses and service providers have unique methods of designing, implementing, and identifying IoT architecture. However, regardless of the implementation or business model, the basic design of an IoT system remains the same. To comprehend its basic architecture, a four-layer model of an IoT system is necessary.

.

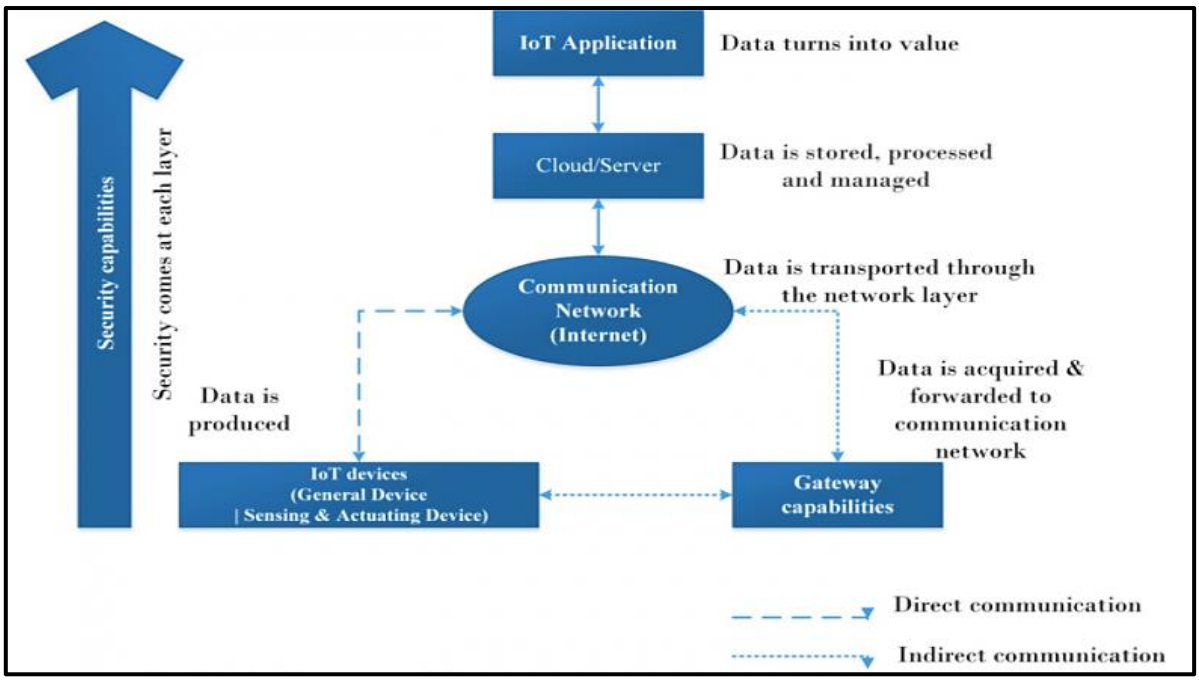

Figure 4:Direct and Indirect Communication of IoT Network (Source: Bernard, 2021)

An IoT system produces, transmits, analyzes, and transforms data into useful information. The figure below shows the basic architecture of an IoT system.

IoT devices: Any item or equipment fulfilling the following requirements shall be qualified as an IoT device if,

It is capable of communicating with and connecting to other devices on the internet. It must be equipped with hardware interfaces, firmware, or an operating system for communication with other devices or connection to an internet network.

Sensors and/or actuators must be included. Static or dynamic data may be collected from the physical environment via sensors. Information or data from a sensor should be sent to a server or cloud, or shared. In addition, the device may include actuators operating on or in reaction to the data or insights provided by the cloud or server.

A controller or processor must be included in the device for data collection, memory, and temporary storage, as well as firmware or an operating system for analyzing the data collected from the server or cloud.

Most IoT devices are built using traditional IoT boards. The most popular IOT boards include Arduino, Raspberry Pi, Banana Pi, etc. They have on-board microcontrollers or processors, digital and analogue GPIO pins, and several channels of communication. These devices may be joined together to build an IoT device with other boards, sensors, and actuators.

The combination of standard microcontrollers or CPUs with network interfaces, RF, or cell transceivers may also build IoT devices. Among the main microcontroller manufacturers are Texas Instruments (TI), ARM, Freescale, Intel, Microchip Technology, Atmel, and Broadcom.

IoT devices may usually be classified according to their hardware architecture and functions:

General Equipment

A generic device is an IOT application device that has embedded computing and communication capabilities. An all-around device may process data and communicate through wired or wireless interfaces with a communication network. These devices just collect data and insights from a cloud or server and then analyze or process them as necessary. Examples of general IoT devices include, for instance, web-controlled industrial equipment or home appliances.

Sensors and actuators

Sensors and actuators are equipped to interact with and affect the environment in which they operate. The sensors collect and transmit to the onboard controller and processor data about the physical factors of the actual environment, such as temperature, moisture, light intensity, energy, and density. The information is saved to the communications network by the controller or processor. It is received through several communication network tiers in the cloud or server. The cloud analyses data and gives important insights about drives.

4.5 Function of Gateways

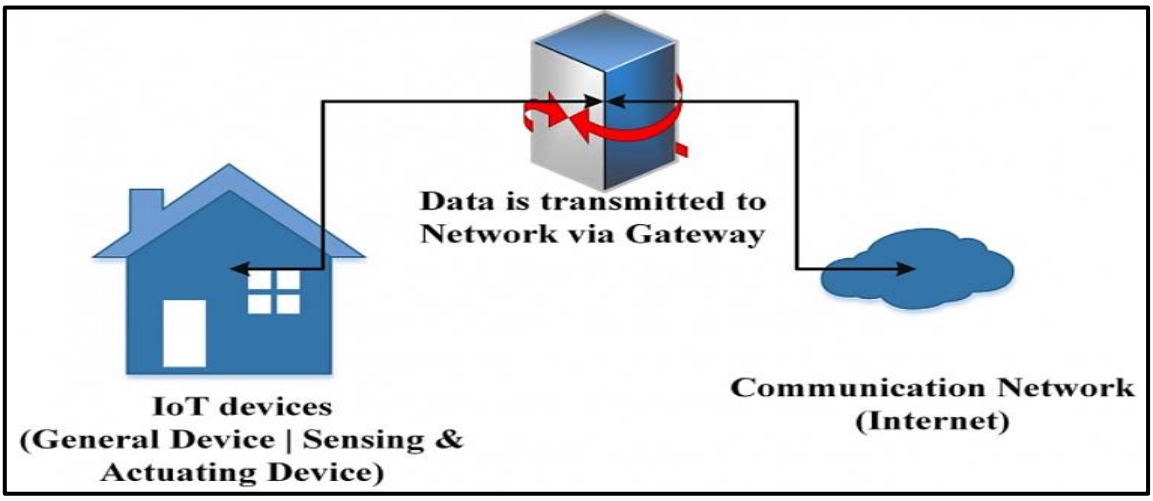

Figure 5:Direct and Indirect Communication of IoT network (Source: Javanmardi et al. 2021)

The IoT device may communicate through a gateway or without other devices. Conversion of protocols without gateways is impossible. Suppose that an IoT device may broadcast, receive, and interact with Zigbee via the Zigbee interface. The communication network for receiving and transmitting data may use the TCP/IP protocol. This scenario will need a gateway to convert data arriving from the device through the Zigbee protocol into TCP/IP data transmissions and cloud or server data transmissions into Zigbee protocols to be received by the IoT device via the TCP/IP protocol. Since the communication network and the IoT device onboard network are not identical, the gateway acts as a two-way connection between the two networks.

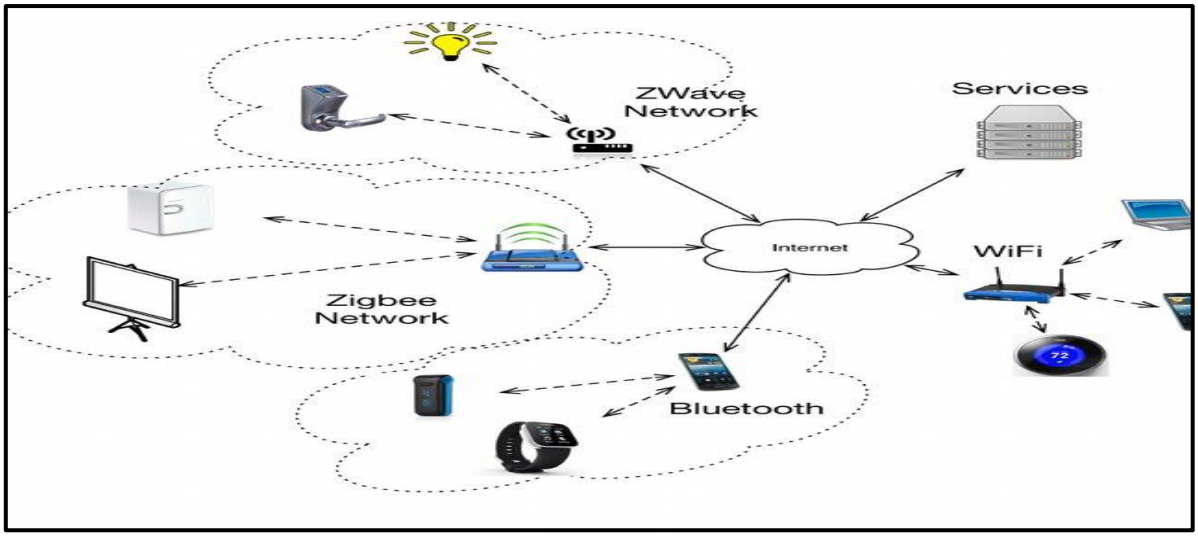

Figure 6:Zigbee Protocol of IoT network (Source: Saba et al. 2021)

In line with the device's protocol, the gateway collects and extracts sensor data according to the protocol under which it is operated and sends the data for transmission in the cloud or on the server to the communication network. Similarly, data, insights, or information are received and extracted from the cloud or server, then wrapped and formatted according to the on-device network protocol, and then sent from the cloud to the IoT device.

4.6 Gateway-Free Communication

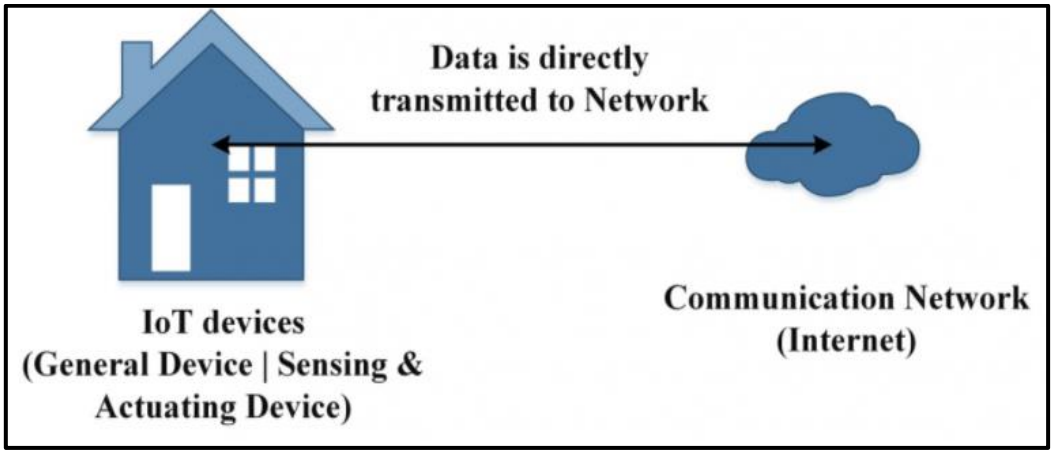

Figure 7:Gateway-Free Communication of IoT Network (Source: Lakhan et al. 2021)

n IoT unit may also link to the cloud or another IoT unit directly. This is the time to communicate and exchange data using the same protocol with the device and communication network, or devices engaging with one another. As a consequence, protocol conversion or a

gateway would not be necessary. IoT devices may contain a firmware or operating system in real-time for processing data, communicating, networking, managing data storage, and controlling actuator actions.

The characteristics of IoT services may be expressed in many ways. The interaction mechanism between IoT services and sensors is explored. However, the key components of IoT services are tagging, real-time awareness, and support in the decision-making process via deep analysis and data visualization. IoT not only connects sensor devices and produces the data for one goal but also focuses on the automation and optimization of existing processes. Understanding the value of the data requires searching the data using a semantic modelling method. As such, these basic automation models and resource optimization for every environmental setting have already been integrated into the planned IoT services, such as smart homes, smart cities, health monitoring, smart grids, and intelligent traffic systems.

4.7 The Process to Build the IoT Architecture in the Cloud

IoT cloud architecture refers to the many components that make up the cloud computing and data processing systems of each business. A robust cloud architecture helps facilitate data transfer through emerging IoT technologies.

To succeed, the cloud architecture has to be smooth, adaptable, and ready to take on new platforms and applications without friction. A step-by-step walkthrough of IoT cloud architecture is provided via the request "Powering Smart Cities with IoT and Early Time and Agile Database." Whether or not an IoT application operates with Big Data, it should know how and why IoT Cloud architecture should be flexible and how various levels of that architecture function together.

The cloud architecture for IoT must be agile.

The Internet of Things is used every day by most individuals. Connected devices provide, for example, digital signage, mobile purchasing choices, and even item monitoring in retail applications. This functionality is maintained by the IoT cloud architecture and provides them with the freedom to improve. The data platforms of an organisation must be very agile to further improve the data processing activities. The more agile a company is, the more new and better

technologies it can use. With the development of new software, a robust cloud architecture easily integrates these new programmes into its data optimization platform.

Layers of cloud architecture

Data travels across various levels in an efficient IoT cloud architecture. For analysis and understanding, each layer makes the data more and more functional. At each company, the cloud architecture looks different, yet much of the cloud architecture of every organisation resides in the reporting and processing layer, which includes:

Internal Aggregate or Cloud Sources Layer

This is the place where all the data is ready for processing. It may be made up of public SaaS, IoT, and other cloud-sourced information. This is the initial level of data processing inside the cloud architecture.

Ingestion Framework Layer

The ingestion architecture enables all unstructured, semi-structured, and structured information to flow into the reporting layer from cloud sources and other public platforms. It functions as the intermediary for the processing and reporting layer between the source data.

Reporting Layer

The reporting layer consists of various levels; however, there are distinct areas of data flow in most reporting layers.

Raw Zone: The raw area is a location where the raw data may simply fall into the reporting layer. This is the last step before the data is processed.

Usable Zone: This area is used to generate visibility and extract operational data using several kinds of mask learning.

Final Zone: The finishing zone is designed to provide insights from historical and real-time data. Data for analysis and decision-making is ready to be utilised in the final zone.

Outbound Layers

It offers outbound services, including APIs and controlled accesses, so that both internal and external parties may readily exchange information.

Practical part

5. Research

Sample selection

Section A: Respondents Demographic Details

The results from the questionnaire administration were as follows;

a. The response rates

Out of the 100 administered questionnaires, the responses collected were 82 in number. This meant that the response rate was 82 percent.

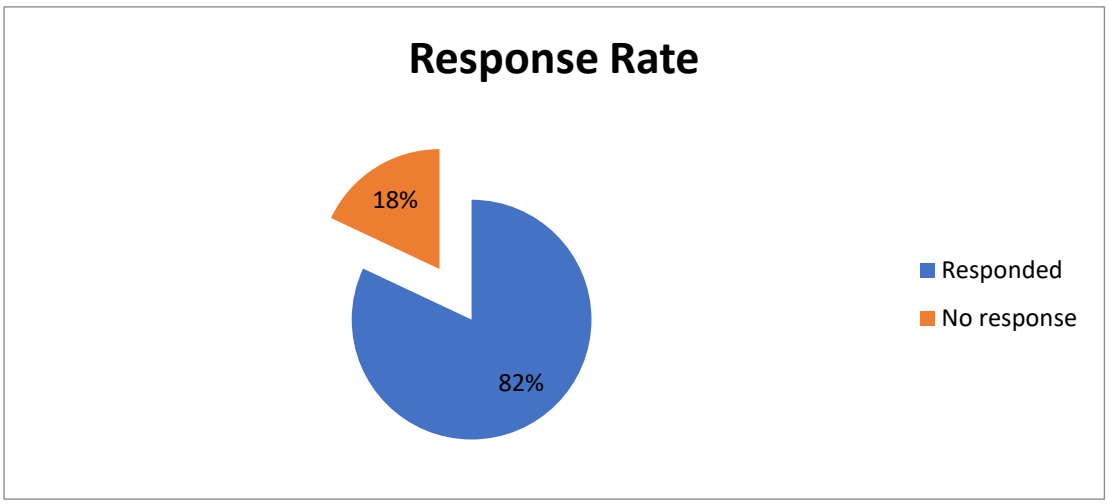

Figure 8:The response rate

b. Respondent's Details

The part for the respondents' details was not determining the actual reflection on the choice or importance of the IoT infrastructure.

i. Gender

Out of the 82 respondents 58 were male and 24 were female. This distribution does not indicate that the higher number of males were in consideration of the importance of IoTs but rather a mere demographic distribution of the respondents. It is never an indication of the role of gender in the outcome of the preferences of the IoT.

Male	Female
58	24

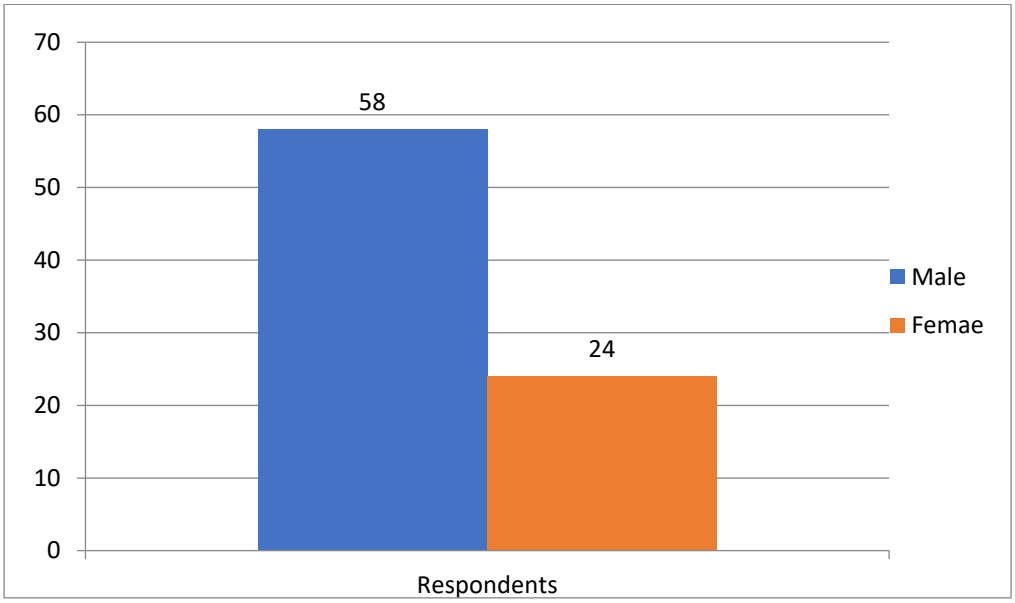

Figure 9:Respondent's Gender

ii. Respondents Age-group

Age group	Frequency
18-30	54
31-45	23
46 and above	5

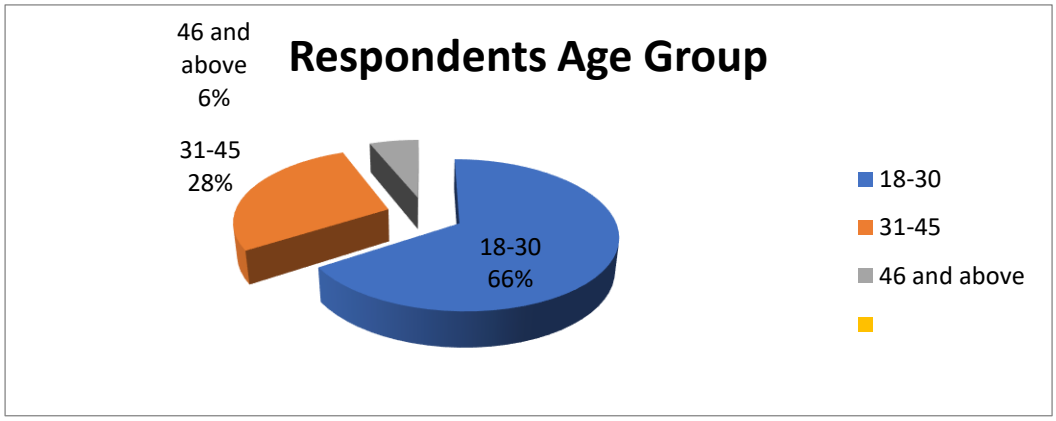

Figure 10:Respondents Age-group

iii. Education Level

Secondary School	18
Diploma & Bachelor's degree	52
Post Graduate Degree	12

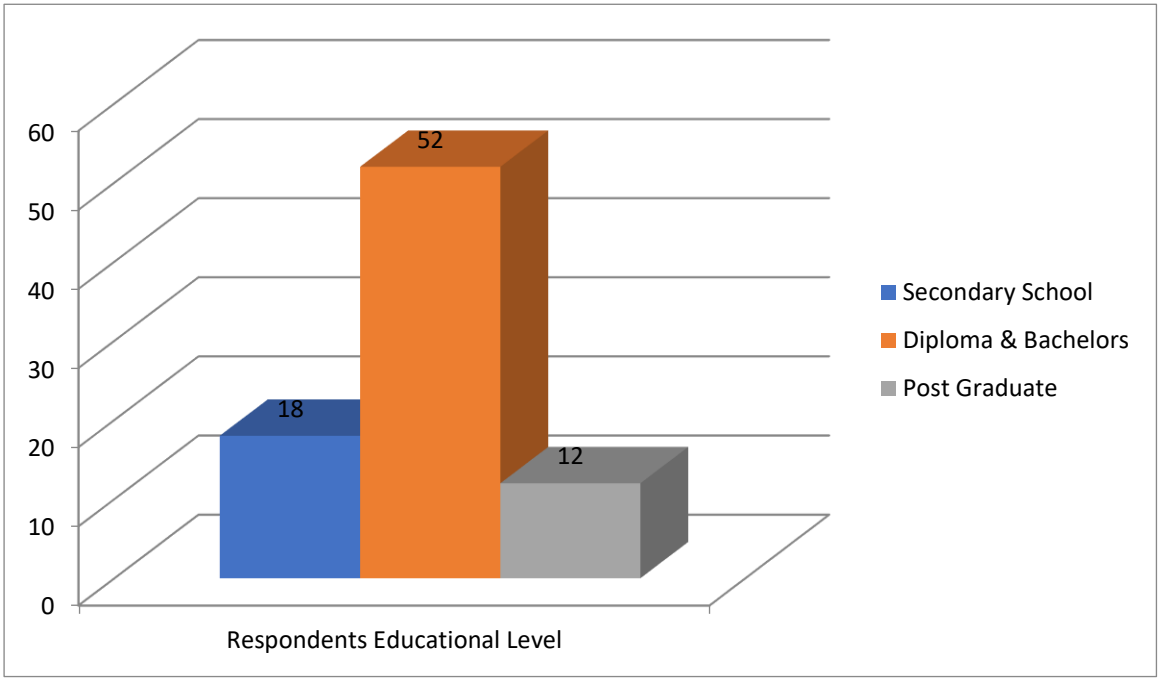

Figure 11: Respondents Education Level

The respondent education level could determine the level of understanding on the IOT devices. However, a tangible number of respondents were in a position to understand and use the IoT devices or technologies. This means that the understanding of the technology would be ideal for the individuals to express their preference of the IoT technologies and infrastructure.

iv. Expertise in IoT Technologies

Basic	10
Intermediate	39
Expert	25
Specialist	8

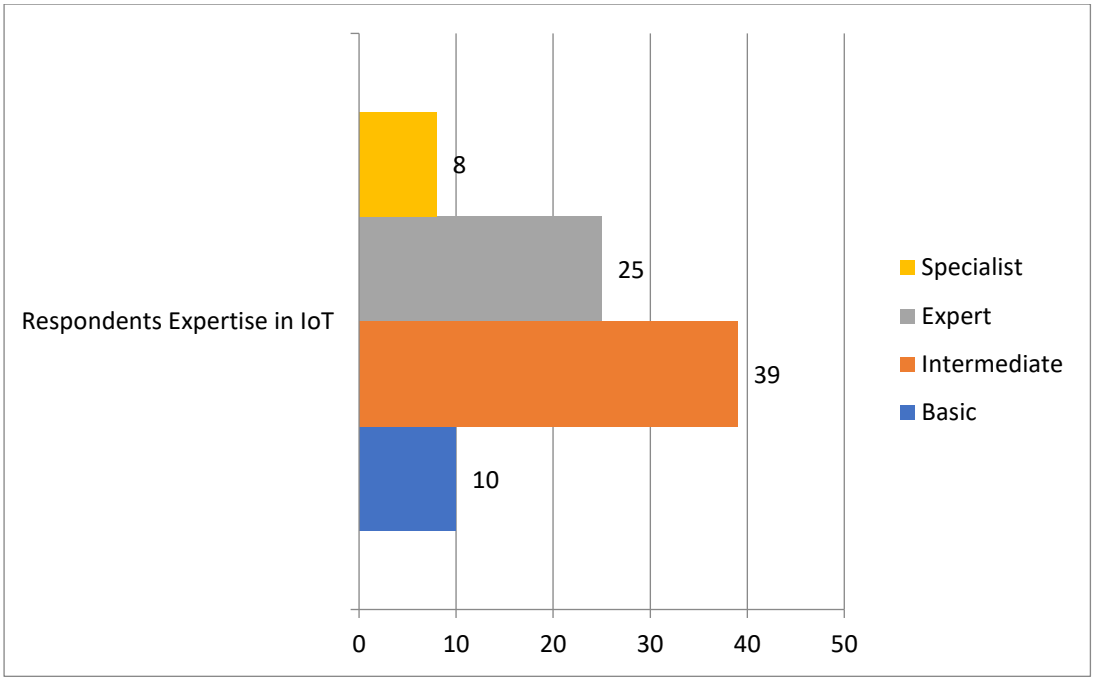

Figure 12: Respondents Expertise in IoT

The above figure indicates that the highest number of respondents could be considered as knowledgeable in the field of IoT. The higher numbers of responses were from individuals within the intermediate level and the expert levels of understanding the operations of IoT infrastructure. This meant that their responses could be used to interpret the considerations being sought for in the study.

Section B: awareness of IoT frameworks

Can you tell me about your awareness of the following IoT Frameworks? Indicate your rating.

v. Respondents Awareness of IoT Frameworks

Platform	Unfamiliar 1	2	3	4	5	6	7	8	9	Very familiar 10
Microsoft Azure IoT Hub	2	0	2	0	12	14	10	0	12	32
Google Cloud Platform	0	0	1	3	5	4	2	15	30	22
IBM Bluemix	1	2	8	1	22	10	25	0	1	12
Oracle IoT Architecture	1	5	7	10	18	13	9	0	2	14
Cisco IoT Cloud Connect	0	5	8	1	5	10	18	5	12	18

Alibaba IoT Architecture	1	1	3	0	5	4	12	10	15	30
SAP IoT Platform	3	4	15	13	22	13	2	0	0	8

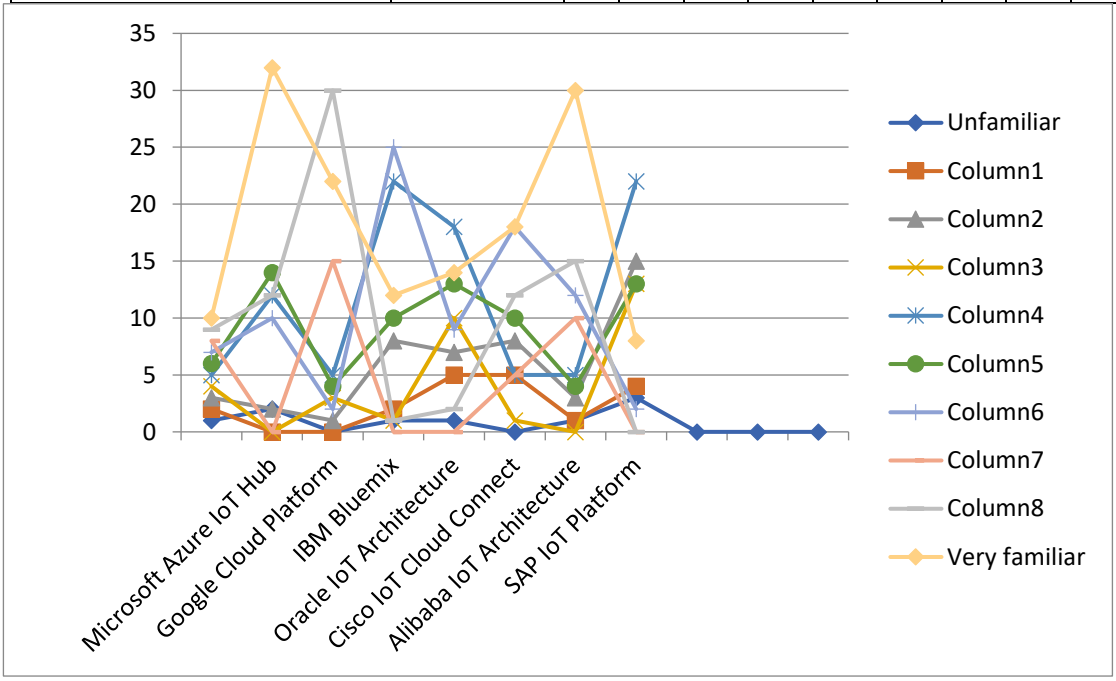

Figure 13: Awareness of IoT Frameworks

From the Data above, the highest respondents were knowledgeable of IoT platform under Microsoft Azure IoT Hub and Alibaba IoT Architecture. However, on the same survey, the highest number was less aware or unfamiliar with Cisco IoT and SAP IoT Platforms.

How would you rate your preference for the aforementioned IoT platforms?

vi. Preference for IoT platforms.

Platform	Not Preferred 1	2	3	4	Very Preferred 5
Microsoft Azure IoT Hub				10	53
Google Cloud Platform				48	13
IBM Bluemix			35	28	
Oracle IoT Architecture			22	38	12
Cisco IoT Cloud Connect				42	
Alibaba IoT Architecture				25	51
SAP IoT Platform			45	10	

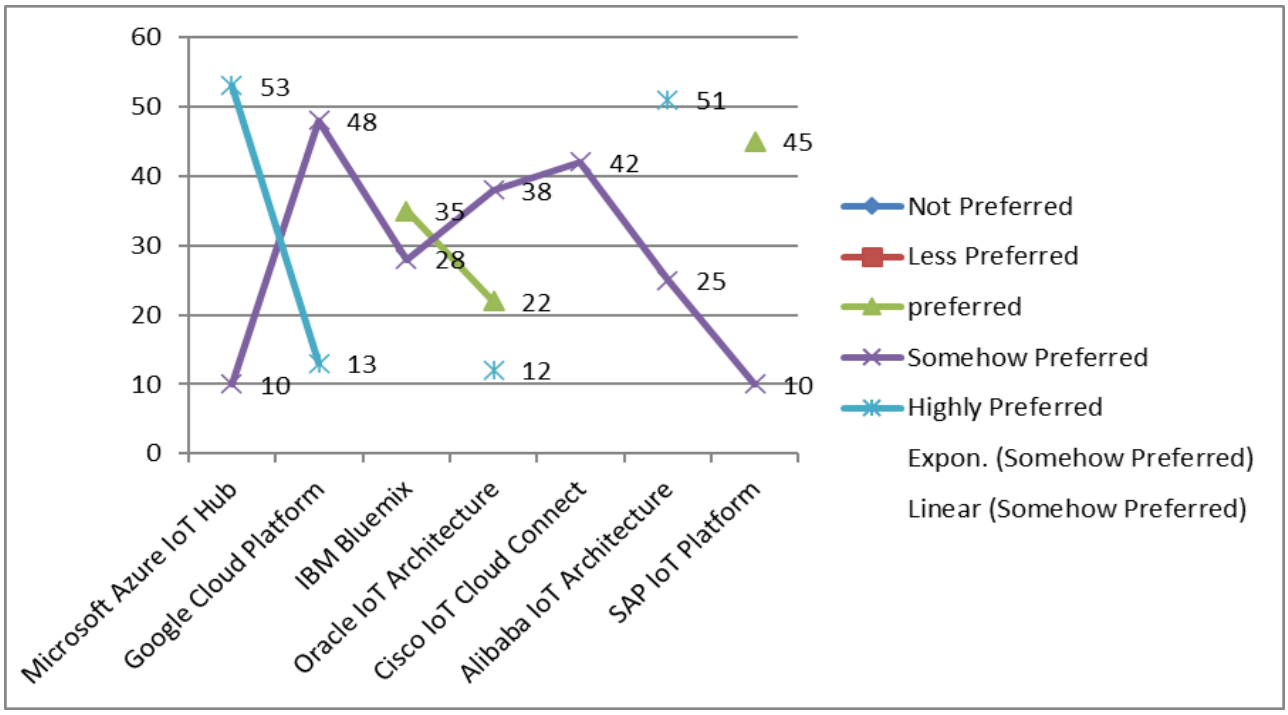

Figure 14: Preference for IoT platforms.

From the scatter chart above, the highest preferences were for Microsoft Azure and Alibaba IoT. This reflects on the usage aspects that perhaps the respondents would use the platforms for. This meant that the preference was potentially capable of ensuring that the platforms could be chosen based on utility.

What is your consideration on the effectiveness of the IoT Frameworks?

Platform	Not Effective 1	2	3	4	Very Effective 5
Microsoft Azure IoT Hub	0	0	10	24	48
Google Cloud Platform	0	0	8	21	53
IBM Bluemix	0	3	17	32	30
Oracle IoT Architecture	0	4	13	27	38
Cisco IoT Cloud Connect	0	0	7	33	42
Alibaba IoT Architecture	0	3	10	19	50
SAP IoT Platform	0	0	39	11	32

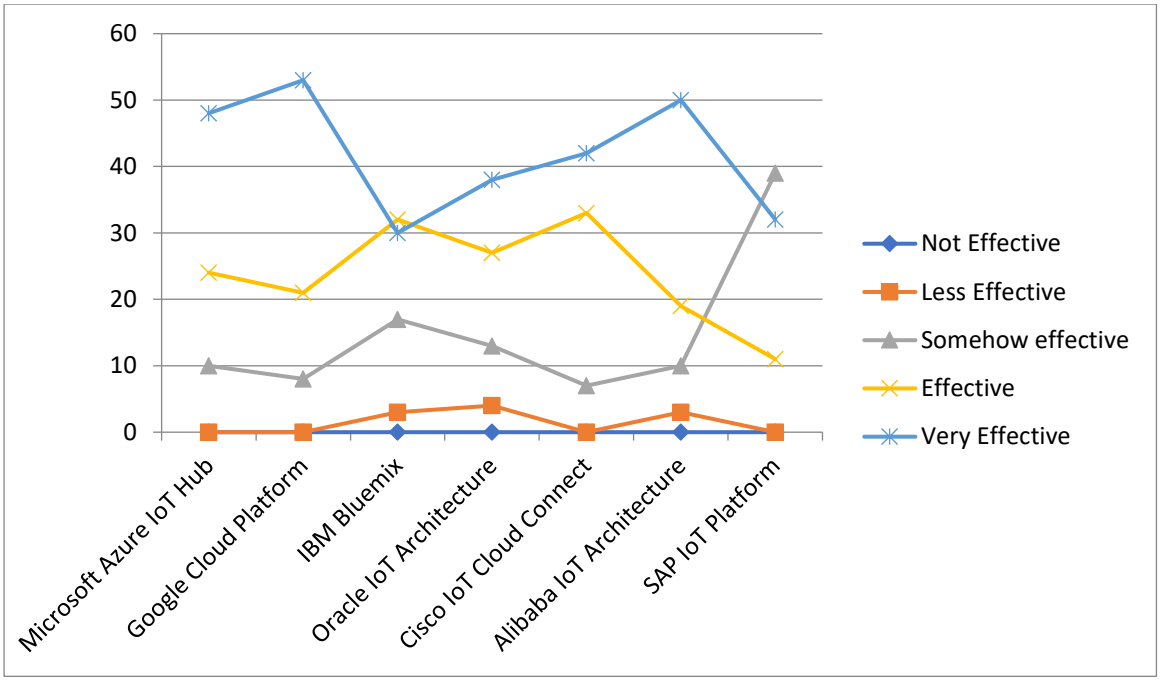

Figure 15: effectiveness of the IoT Frameworks

From the figure above, the respondents indicated that it is possible for Alibaba IoT, Microsoft Azure IoT, and Google Cloud to be highly effective to the category of respondents. This exhibits a preference for these three platforms and ensures that they meet the desired utility. Other platforms such as Cisco and IBM also rank high in closeness to being opinionated as effective. Figures for not effective were zero on all categories and this meant that the platforms were somehow operational on different categories that may not have been considered by the respondents.

Section C: Areas of Improvement for IoT Framework

	Yes	No	Neutral
IoT Frameworks as a service	72	8	4
IoT platforms as a platform	58	24	0
IoT computing as Technology	54	20	8
Home sensors	70	12	0

Transmission and reception networks	55	17	10
Security aspects	78	2	2
Privacy	80	2	0

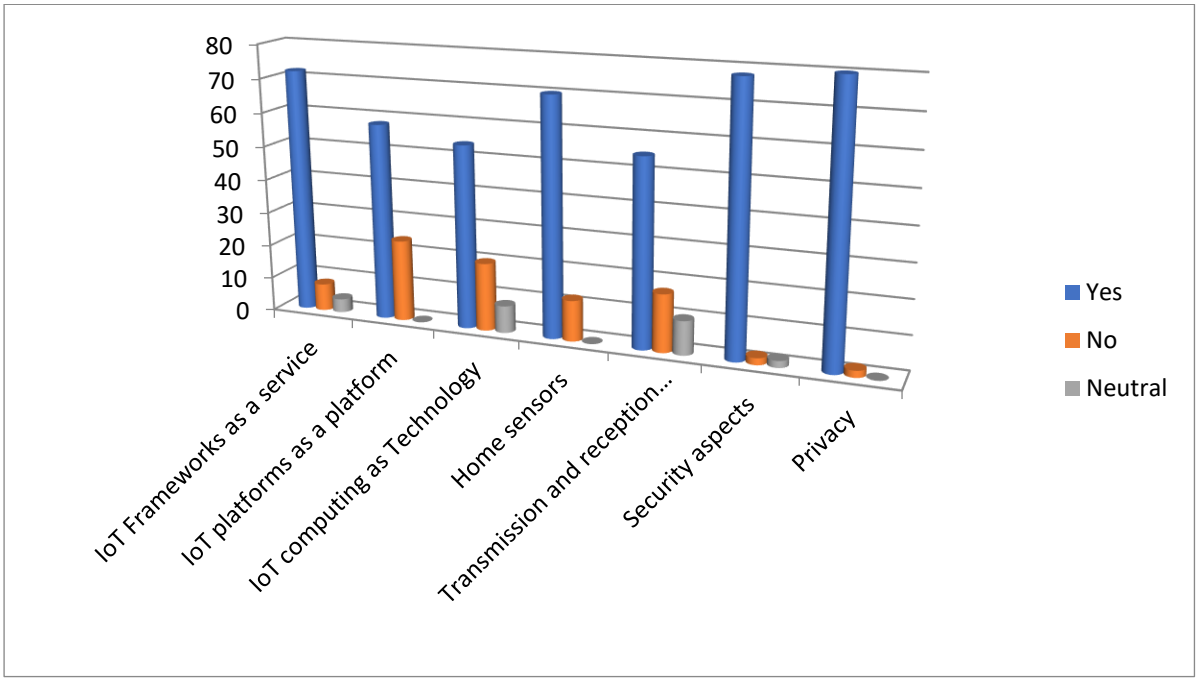

Figure 16: Areas of Improvement for IoT Framework

From the figure above, the respondents indicated a general request to have the IoT strategy improved in almost all aspect with the Privacy, Security, Home Sensors, and the IoT frameworks being the highest in consideration.

6. Results

This section in brief discusses the results of the primary and secondary research.

The general comments on what the respondents think is the most effective IOT network design and cloud platform. Some indicated that they would consider the amount of data being handled, the kind of users they are dealing with, and the newest inclusions in the IoT infrastructure. A number indicated that the changes in the frameworks and capacity of computing would determine their choice of IoT framework. However, there are a high number that argued that the brand had a role to play in the significance of the IoT framework with Microsoft Azure and IBM mentioned as some of the preferred brands in technology frameworks.

Respondents from the survey expressed concern over security by showing the need to have security concern addressed. Lin and the Royal College of Art, United Kingdom. (2022) note that due to the IoT devices capacity to deal with massive amounts of data, Machine Learning and Deep Learning (ML/DL) algorithms are currently being utilized for dealing with the factors for better device performance. However, complexity in any form should be taken into account for security reasons because security flaws and vulnerabilities can be concealed there (Qushtom et al., 2022). In order to reap the anticipated benefits, security professionals should assess whether the framework is overly complex and avoid workarounds that open up new attack vectors.

Based on the findings from the survey, it was apparent that the preference for the IoT framework was dependent on the security and privacy in the infrastructure. IoT networks are naturally and frequently unavoidably complex. IoT frameworks are beneficial because they produce a data model abstraction that is simpler to understand than applications' need to deal with a plethora of options for message exchange and disparate data definitions. Interoperability is enhanced by allowing applications to concentrate solely on the semantics of IoT node behaviour and interactions (Li et al., 2023). Efficiency enhancements can be implemented more uniformly by concealing the complexity of heterogeneous platform deployment, bridging, connection establishment, and gatewaying. Even though frameworks can make simple deployments more difficult, they scale as deployments grow, making the IoT system overall simpler.

6.1 Advantages of IoT and Cloud Networking

- It provides fast processing and information delivery, decreased latency, and improved dependability.
- It provides greater security by spreading processing, storage, and applications across many devices and data centres, making network failure harder.
- It provides a much cheaper path towards scalability and flexibility to enable businesses via a mix of IoT devices and edge data centres to increase the processing capacity.

6.2 Disadvantages of IoT and Cloud Networks

- More storage capacity is required.
- Due to large volumes of data, security problems in edge computing are significant.
- Only the data are analysed.
- Costs are extremely high for edge calculation.
- Advanced infrastructure is required.

6.3 How IOT Networks and Cloud Computing Supports the Network Design

Cloud computing and the Internet of Things (IoT) have undergone massive evolution and advancement. The features that the two fields display on incorporation through each other are impeccable. Both cloud computing and IoT respectively accompany very fine technologies, and consequently, many scholars, through their research findings, have intended and projected all probable implementations possessing in cognizance the amalgamation of cloud services and IoT. The Internet of Things (IoT) is on the receiving end after grasping its situation upon receiving plentiful sustenance from cloud services in relation to storage and computation capabilities. The two autonomous confrontations, cloud computing and the Internet of Things (IoT), are being perceived as growing independently. Nonetheless, grounded on the compensations curtailing through their incorporation, both will be perceived as unified in the forthcoming generation (Bernard, 2021). IoT has endangered operators in delivering new-fangled facilities in actual possession for a huge quantity of factual significance.

Since it is difficult for the Internet of Things (IoT) system to deal with the massive data dispensation efficiently, a cloud computing service is needed to deal with the operator's data

storage and dispensation matters. In this research study, cloud service unification with nodes is considered for incorporation since it is the most current development in cloud computation.

The cloud computing service consents the possessions of prevailing servers in data hubs with further appliances like smartphones as well as private computers. By means of the identical expertise on the IoT, source-inhibited sensor appliances can be directed toward sending and storing the extents in a fundamental position manageable through numerous additional appliances (Cui, 2016). Cloud storage services likewise make it possible to accomplish further analytics besides building erudite facilities exploiting the data from the sensors of the IoT appliances. Manifold cloud storage platform strategies, rules, contexts, and applications are being put forward for the Internet of Things (IoT). These resolutions are furthermore focused on "closed-trace" or connectivity-related difficulties and not on safety.

7. Discussion

The role of Cloud computing and IoT technology in homes has not been dwindling and is increasing with time. There are numerous advantages to considering an IoT platform investment for homes, business or general use. An IoT platform basically serves as a ready-made framework for your entire IoT infrastructure, bringing everything together and assisting you in beginning to reap the benefits as soon as possible (Barra et al., 2022). In evaluating the utility of the IoT frameworks, security issues are a recurring theme. The IoT framework node provides a security context in which an IP multicast address serves as the security endpoint. According to Yavuz and Brant (2022) data security ends at the network interface card or possibly in an operating system networking driver. This means that data is exposed before it reaches the enforcement point of the IoT framework, where it is decided which node it belongs to (Purbey & Khandelwal, 2022). They may have been designed with a wide range of privacy and security considerations in mind, but there are a few areas that are always problematic. IP addresses are used to identify endpoint nodes in IP networks, and routing logic is expressed in terms of IP addresses.

Choosing the right IoT framework can be considered a major decision with diverse factors to consider. As IoT framework node identifiers, network layer identifiers are insufficient. Nodes in IoT frameworks are logical and can have different node identifiers despite sharing the same IP address. When it comes to the Internet of Things (IoT), connectivity plays a crucial role because each project and organization has distinct connectivity requirements that will directly determine which IoT platform is most suitable. Different IoT platforms specialize in different technologies.

There may be differences in IoT usage because different frameworks intend to address distinct use cases and requirements. In other instances, features and capabilities appear to overlap significantly because they address similar requirements in different ways (Goel et al., 2022). This is unfortunate because it opens the door to potential conflicts. When used in isolated deployments, these differences may be unnoticeable, but when interoperability across multiple deployments is desired, they significantly increase complexity (Hassan et al., 2022).

The network layer is used for more than just uploading data for analysis. At the physical layer, it is also used to make communication between diverse IoT objects easier. As the number of objects grows, the network layer should be able to support scalability, device discovery, and context awareness. Importantly, it should also provide IoT devices with privacy and security.

The IoT devices' uploaded data can be thoroughly analysed to generate insights and assist in decision-making.

Other advantages of frameworks include the ability to represent multiple perspectives on the IoT system's manageability, resiliency, interoperability, security, safety, and usability.

8. Conclusion:

The main goal for this study was to evaluate the impact that Internet of Things had in establishment of resilient Cloud-based IoT networks. The Internet of Things (IoT) is regarded as one of the next disruptive technologies and has received a great deal of interest in recent years. IoT devices are small sensors or actuators connected to everyday items that may transmit sensor data and receive instructions. A lot of devices can strain an internet connection, necessitating intelligent devices to send data to servers rather than to central servers for processing. You can now access data from many parts of your network, be on the effectiveness of processes, respond faster to downtime, and anticipate when errors might occur. Using the Cloud with IoT devices enhances security because regular updates and immediate notification of infrastructure breaches are possible. Utilizing Large Information, IoT, and the Cloud together implies that one can have fruitful correspondence, association and transaction of information between gadgets, most really and effectively.

The study has noted that the effectiveness of networks has been largely dependent on the gadgets and capacities in the networks. The capacity includes the capabilities that enable Internet of Things (IoT) devices to interact with cloud services, other applications, and even other IoT devices are provided by cloud platforms. Users can centrally onboard, manage, monitor, and control IoT devices through these cloud platforms. IoT data can be stored and processed in one central location by utilizing the cloud. Plenty of research has been performed in the cloud to enable remote access and control of IoT device virtualization.

Another objective that was desirable in this study was to establish the means through which the IoT network designs are developed to ensure interconnectivity. This research has established that the IoT devices will, in the future, be accessible through their respective virtual objects. Like a physical device's network, the cyber world has to have a network of virtual things. We propose in this article the idea of creating a dynamic virtual network among linked IoT devices in the cloud environment. Cloud computing technology offers huge processing and internet storage capacity to overcome restricted IoT device capabilities. Sensors, actuators, operating systems, mobile devices, standalone applications, and analytical systems are all sources of IoT data. The primary concept is to offer a method to develop a virtual network of linked IoT devices in the cloud environment from a range of domains. The dynamic end-to-

end connectivity between IoT devices would enable resource sharing and fast growth in various applications across the virtualization layer.

In implementing a reliable Cloud-based IoT network, the first step is to assess the needs in the area where the network will be implemented. This is followed by defining the network gadgets that are needed to handle the network needs. Once the The designing must address every aspect of the network including security, capacity, and user-friendly attributes within the networks. As the number of IoT devices grows, the underlying cloud networks that allow and serve them must be updated. The cloud infrastructure has to be improved to handle the traffic. Each of the voices, videos, and data has unique transmission requirements and network requirements. The cloud infrastructure has to be improved to handle the traffic. Each of the voices, videos, and data has unique transmission requirements and network requirements. IoT traffic varies significantly, and thus separate network requirements must be taken into account when designing the network, they transport.

References

Abbasi, M., Mohammadi-Pasand, E., & Khosravi, M. R. (2021). Intelligent workload allocation in IoT–Fog–cloud architecture towards mobile edge computing. *Computer Communications*, *169*, 71-80.

Al Mtawa, Y., Haque, A., & Bitar, B. (2018, August). Does Internet of Things Disrupt Residential Bandwidth Consumption?. In 2018 IEEE 88th Vehicular Technology Conference (VTC-Fall) (pp. 1-5). IEEE.

Alkadi, O., Moustafa, N., Turnbull, B., & Choo, K. K. R. (2020). A deep blockchain framework-enabled collaborative intrusion detection for protecting IoT and cloud networks. *IEEE Internet of Things Journal*, *8*(12), 9463-9472.

Barra, S., Hossain, S., Pero, C., & Umer, S. (2022). A facial expression recognition approach for social IoT frameworks. *Big Data Research*, *30*(100353), 100353. https://doi.org/10.1016/j.bdr.2022.100353

Beitelspacher, S., Mubashir, M., Besher, K. M., & Ali, M. Z. (2020, April). Prioritizing health care data traffic in a congested IoT cloud network. In *2020 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)* (pp. 1-6). IEEE.

Bernard, Z. J. (2021). IoT with Cloud-Based Distributed Disease Diagnosis System using Deep Belief Networks. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *12*(10), 3240-3255.

Cui, X. (2016). The internet of things. In Ethical ripples of creativity and innovation (pp. 61-68). Palgrave Macmillan, London.

Deebak, B. D., & Al-Turjman, F. (2020). A novel community-based trust aware recommender system for big data cloud service networks. *Sustainable Cities and Society*, *61*, 102274.

Din, I. U., Asmat, H., & Guizani, M. (2019). A review of information-centric network-based internet of things: communication architectures, design issues, and research opportunities. Multimedia Tools and Applications, 78(21), 30241-30256.

Donassolo, B., Fajjari, I., Legrand, A., & Mertikopoulos, P. (2019, January). Fog based framework for IoT service orchestration. In 2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC) (pp. 1-2). IEEE.

Elmubarak, S. A., Yousif, A., & Bashir, M. B. (2017). Performance-based ranking model for cloud SaaS services. *International Journal of Information Technology and Computer Science*, *9*(1), 65-71.

Ezenwoke, A., Daramola, O., & Adigun, M. (2018). QoS-based ranking and selection of SaaS applications using heterogeneous similarity metrics. *Journal of Cloud Computing*, *7*(1), 15.

Faizullah, S., Khan, M. A., Alzahrani, A., & Khan, I. (2020, February). Permissioned blockchain-based security for SDN in IoT cloud networks. In *2019 International Conference on Advances in the Emerging Computing Technologies (AECT)* (pp. 1-6). IEEE.

Garg, S., Guo, S., Piuri, V., Choo, K. K. R., & Raman, B. (2020). Guest editorial special issue on edge-cloud interplay based on SDN and NFV for next-generation IoT applications. *IEEE Internet of Things Journal*, *7*(7), 5690-5694.

Ghobaei-Arani, M., Jabbehdari, S., & Pourmina, M. A. (2016). An autonomic approach for resource provisioning of cloud services. *Cluster Computing*, *19*(3), 1017-1036.

Goel, U., Mongia, K., Gupta, Q., Rajput, H., & Jha, V. (2022). Sparse mobile crowdsensing: Components and frameworks. *2022 IEEE World AI IoT Congress (AIIoT)*.

Haji, S. H., & Ameen, S. Y. (2021). Attack and anomaly detection in IoT networks using machine learning techniques: A review. *Asian Journal of Research in Computer Science*, 30-46.

Han, T., Muhammad, K., Hussain, T., Lloret, J., & Baik, S. W. (2020). An efficient deep learning framework for intelligent energy management in IoT networks. *IEEE Internet of Things Journal*, *8*(5), 3170-3179.

Hassan, M. A., Samara, G., & Fadda, M. A. (2022). IoT Forensic Frameworks (DFIF, IoTDOTS,FSAIoT): A Comprehensive Study. In *arXiv [cs.CR]*. http://arxiv.org/abs/2203.15705

Huang, J., Samplawski, C., Ganesan, D., Marlin, B., & Kwon, H. (2020, September). Clio: Enabling automatic compilation of deep learning pipelines across IoT and cloud. In *Proceedings of the 26th Annual International Conference on Mobile Computing and Networking* (pp. 1-12).

Huong, T. T., Bac, T. P., Long, D. M., Thang, B. D., Luong, T. D., & Binh, N. T. (2021, January). An Efficient Low Complexity Edge-Cloud Framework for Security in IoT Networks. In *2020 IEEE Eighth International Conference on Communications and Electronics (ICCE)* (pp. 533-539). IEEE.

Ibrahim, A. A., Varrette, S., & Bouvry, P. (2018, January). PRESENCE: toward a novel approach for performance evaluation of mobile cloud SaaS web services. In *2018 International Conference on Information Networking (ICOIN)* (pp. 50-55). IEEE.

Javadpour, A., Wang, G., & Rezaei, S. (2020). Resource management in a peer to peer cloud network for IoT. *Wireless Personal Communications*, *115*(3), 2471-2488.

Javanmardi, S., Shojafar, M., Mohammadi, R., Nazari, A., Persico, V., & Pescapè, A. (2021). FUPE: A security-driven task scheduling approach for SDN-based IoT–Fog networks. *Journal of Information Security and Applications*, *60*, 102853.

Ji, W., Xu, J., Qiao, H., Zhou, M., & Liang, B. (2019). Visual IoT: Enabling internet of things visualization in smart cities. IEEE Network, 33(2), 102-110.

Kayes, A. S. M., Kalaria, R., Sarker, I. H., Islam, M., Watters, P. A., Ng, A., ... & Kumara, I. (2020). A survey of context-aware access control mechanisms for cloud and fog networks: Taxonomy and open research issues. *Sensors*, *20*(9), 2464.

Lakhan, A., Mastoi, Q. U. A., Elhoseny, M., Memon, M. S., & Mohammed, M. A. (2021). Deep neural network-based application partitioning and scheduling for hospitals and medical enterprises using IoT assisted mobile fog cloud. *Enterprise Information Systems*, 1-23.

Li, S., Zhao, S., Gope, P., & Da Xu, L. (2023). Data privacy enhancing in the IoT user/device behavior analytics. *ACM Transactions on Sensor Networks*, *19*(2), 1–13. https://doi.org/10.1145/3534648

Lin, Z., & Royal College of Art, United Kingdom. (2022). Designing experiences for IoT products: A case study testing existing UX frameworks. *Proceedings of DRS*.

Mahajan, P., & Kaur, P. D. (2021). Three-tier IoT-edge-cloud (3T-IEC) architectural paradigm for real-time event recommendation in event-based social networks. *Journal of Ambient Intelligence and Humanized Computing*, *12*(1), 1363-1386.

Nagaraj, A. (2021). *Introduction to Sensors in IoT and Cloud Computing Applications*. Bentham Science Publishers.

Puliafito, C., Mingozzi, E., & Anastasi, G. (2017, May). Fog computing for the internet of mobile things: issues and challenges. In 2017 IEEE International Conference on Smart Computing (SMARTCOMP) (pp. 1-6). IEEE.

Purbey, S., & Khandelwal, B. (2022). Analyzing frameworks for IoT data storage, representation and analysis: A statistical perspective. In *Lecture Notes in Networks and Systems* (pp. 472–488). Springer International Publishing.

Qushtom, H., Mišić, J., Mišić, V. B., & Chang, X. (2022). A high performance two-layer consensus architecture for blockchain-based IoT systems. *Peer-to-Peer Networking and Applications*, *15*(5), 2444–2456. https://doi.org/10.1007/s12083-022-01363-y

Rashid, A., & Chaturvedi, A. (2019). Cloud computing characteristics and services: a brief review. *International Journal of Computer Sciences and Engineering*, *7*(2), 421-426.

Ren, J., Zhang, D., He, S., Zhang, Y., & Li, T. (2019). A survey on end-edge-cloud orchestrated network computing paradigms: transparent computing, mobile edge computing, fog computing, and cloudlet. ACM Computing Surveys (CSUR), 52(6), 1-36.

Saba, U. K., ul Islam, S., Ijaz, H., Rodrigues, J. J., Gani, A., & Munir, K. (2021). Planning Fog networks for time-critical IoT requests. *Computer Communications*, *172*, 75-83.

Sadeeq, M. M., Abdulkareem, N. M., Zeebaree, S. R., Ahmed, D. M., Sami, A. S., & Zebari, R. R. (2021). IoT and Cloud computing issues, challenges and opportunities: A review. *Qubahan Academic Journal*, *1*(2), 1-7.

Saha, R., Kumar, G., Rai, M. K., Thomas, R., & Lim, S. J. (2019). Privacy Ensured ${e} $-healthcare for fog-enhanced IoT based applications. IEEE Access, 7, 44536-44543.

Saunders, M., (2012). *Research Methods for Business Students.* 6th Edition ed. s.l.:Pearson Education.

Shahryari, O. K., Pedram, H., Khajehvand, V., & TakhtFooladi, M. D. (2020). Energy-Efficient and delay-guaranteed computation offloading for fog-based IoT networks. *Computer Networks*, *182*, 107511.

Vitunskaite, M., He, Y., Brandstetter, T., & Janicke, H. (2019). Smart cities and cybersecurity: Are we there yet? A comparative study on the role of standards, third party risk management and security ownership. Computers & Security, 83, 313-331.

Yavuz, T., & Brant, C. (2022). Security analysis of IoT frameworks using static taint analysis. *Proceedings of the Twelveth ACM Conference on Data and Application Security and Privacy*.

Yu, M., Liu, A., Xiong, N. N., & Wang, T. (2020). An intelligent game-based offloading scheme for maximizing benefits of IoT-edge-cloud ecosystems. *IEEE Internet of Things Journal*.

Zargar, S., Shahidinejad, A., & Ghobaei-Arani, M. (2021). A lightweight authentication protocol for IoT-based cloud environment. *International Journal of Communication Systems*, *34*(11), e4849.

Zou, Z., Jin, Y., Nevalainen, P., Huan, Y., Heikkonen, J., & Westerlund, T. (2019, March). Edge and fog computing enabled AI for IoT-an an overview. In 2019 IEEE International Conference on Artificial Intelligence Circuits and Systems (AICAS) (pp. 51-56). IEEE.

Appendix

First Name Only:_____

Please circle any one option:

1. Gender
    - Male
    - Female

2. Age-group
    - 18-30
    - 31-45
    - 46 and above

3. Education Level
    - Secondary School
    - Diploma & Bachelor's degree
    - Post Graduate Degree

4. Expertise in IoT Technologies
    - Basic
    - Intermediate
    - Expert
    - Specialist

SECTION B: AWARENESS OF IOT FRAMEWORKS

Can you tell me about your awareness of the following IoT Frameworks? Indicate your rating.

Platform	Unfamiliar 1	2	3	4	5	6	7	8	9	Very familiar 10
Microsoft Azure IoT Hub										
Google Cloud Platform										
IBM Bluemix										
Oracle IoT Architecture										
Cisco IoT Cloud Connect										
Alibaba IoT Architecture										
SAP IoT Platform										

How would you rate your preference for the aforementioned IoT platforms?

Platform	Not Preferred 1	2	3	4	Very Preferred 5
Microsoft Azure IoT Hub					
Google Cloud Platform					
IBM Bluemix					
Oracle IoT Architecture					
Cisco IoT Cloud Connect					
Alibaba IoT Architecture					
SAP IoT Platform					

What is your consideration on the effectiveness of the IoT Frameworks?

Platform	Not Effective 1	2	3	4	Very Effective 5
Microsoft Azure IoT Hub					
Google Cloud Platform					
IBM Bluemix					
Oracle IoT Architecture					
Cisco IoT Cloud Connect					
Alibaba IoT Architecture					
SAP IoT Platform					

SECTION C: Recommendations on Software Enhancement

What would you desire to be addressed in the future of IoT integrations?

	Yes	No
IoT Frameworks as a service		
IoT platforms as a platform		
IoT computing as Technology		
Home sensors		
Transmission and reception networks		
Security aspects		
Privacy		