Tampere University

Oliver Liombe Molua

# SECURITY AND PRIVACY ASPECTS OF CLOUD, EDGE, AND FOG PARADIGMS

## A Systematic Literature Review

Master of Science Thesis
Faculty of Information Technology
and Communication Sciences.
Examiner: Prof. Jari Nurmi
Supervisor: Dr. Aleksandr Ometov
December 2021

# ABSTRACT

Oliver Liombe Molua: Security and Privacy Aspects of Cloud, Edge, and Fog Paradigms
Master of Science Thesis
Tampere University
Information Technology
December 2021

Information security and privacy is one aspect of the information technology sector that currently attracts a lot of research interest. From Cloud computing to Edge computing and then Fog computing, all forming a unique ecosystem but with different architectures, networks, storage, and other capabilities. The heterogeneity of this ecosystem also comes with certain issues, particularly security and privacy challenges. Therefore, this thesis is research-oriented and mainly focused on Systematic Literature Review (SLR) of other research papers based on security and privacy in Cloud, Edge, Fog paradigms. The thesis aims at identifying similarities, differences, attacks, and countermeasures in the various paradigms mentioned.

We performed an SLR to choose articles centered specifically on security and privacy in Cloud, Edge, and Fog paradigms, using modified PRISMA-2009 guidelines. The research articles were released between 2005 and 2021 within the recognized academic databases, some other articles were selected which were published before 2005. We selected 77 studies after carefully examining the issued works to assist in responding to the established research questions (RQs). Several databases were used as the main libraries of information for the systematic literature review. The generated criteria for inclusion/exclusion were applied in the selection process of works of literature. A modified version of the PRISMA-2009 checklist to suit the objective was used as the defined methodology.

The systematic literature review outcome pointed out several security and privacy challenges. The presented results outlined some important similarities and differences in Cloud, Edge, and Fog computing paradigms. Some other threats and vulnerabilities were found relating to the individual paradigms. The SLR outcome also reveals that the heterogeneity of such an ecosystem does have issues and poses a great setback in the deployment of security and privacy mechanisms to counter security attacks and privacy leakages. Different deployment techniques were found in the review studies as ways to mitigate and enhance security and privacy shortcomings. Other discoveries relating to the strengthening of information confidentiality, integrity, and availability were seen in the systematic literature reviews envisioning the future research pathways to be performed.

Keywords: Cloud paradigm, Edge paradigm, Fog paradigm, Information Security, Privacy, systematic literature review, vulnerabilities, attacks, countermeasures

# PREFACE

I was privileged to learn a lot about information security and data privacy in computing paradigms and cybersecurity industry in particular during this thesis. This thesis has now provided me with a clear road map in pursing my dream career in Ethical Hacking and Cybersecurity.

I am hugely indebted to my Supervisor, Dr. Aleksandr Ometov for his valuable and enormous assistance in my Master's thesis, not leaving out my always responsive Examiner Prof. Jari Nurmi, a real mentor. Although it has not been all roses for me, I would like to immensely appreciate the benevolent and academic selflessness from all the wonderful lecturers at the former Tampere University of Technology (TUT) now part of Tampere Universities (TUNI), who dedicatedly contributed to my success, directly and indirectly.

I would like to dedicate this thesis to my big mum, Mama Mary Namondo Liombe (1930 - 2020) of blessed memory, who passed away during my thesis project.

Finally, I wish to extend a million gratitude to my family and loved ones, especially to my daughter Favour Dana Liombe Molua (Ukraine), and my sweet mum Mama Pauline Limunga Liombe, for all their immeasurable supports along this extraordinary academic path.

Tampere, 1st December 2021

Oliver Liombe Molua

# CONTENTS

# LIST OF SYMBOLS AND ABBREVIATIONS

| | |
|---|---|
| AI | Artificial Intelligence |
| AP | Access Point |
| APT | Advanced Persistent Threats |
| AR | Augmented Reality |
| BS | Base Station |
| CC | Cloud Computing |
| CSA | Cloud Security Alliance |
| CSP | Cloud Service Provider |
| DDoS | Distributed Denial of Service |
| DoS | Denial of Service |
| EC | Edge Computing |
| EDL | Edge Device Layer |
| FC | Fog Computing |
| FN | Fog Nodes |
| GUI | Graphic User Interface |
| IaaS | Infrastructure as a Service |
| ICT | Information and Communication Technology |
| IDS | Intrusion Detection System |
| IoE | Internet of Everything |
| IoT | Internet of Things |
| IT | Information Technology |
| MDT | Modified Decoy Technique |
| MITM | Man in the Middle |
| ML | Machine Learning |
| PaaS | Platform as a Service |
| QA | Quality Assessment |
| QoS | Quality of Service |

| | |
|---|---|
| RQ | Research Question |
| SaaS | Software as a Service |
| SDN | Software Defined Network |
| SLA | Service Level Agreement |
| SLR | Systematic Literature Review |
| SSL | Secure Socket Layer |
| Staas | Storage as a Service |
| TAU | Tampere University |
| TCB | Trusted Computing Base |
| TIP | Threat Intelligence Platform |
| TPM | Trusted Platform Model |
| TUNI | Tampere Universities |
| VM | Virtual Machine |

# 1 INTRODUCTION

## 1.1 Review Objectives

The continuous growth in technology, especially with the massive migration to Cloud, Edge, and Fog paradigm coupled with the extensive integration of Internet of Things (IoT) technologies in homes and work environments, creates great concern for security and privacy. Weak security and privacy implementation mean potential threats from attackers. These threats can be security attacks or privacy leakages.

This thesis is research-oriented, and its primary objective is focused on the systematic literature review of other research papers based on security and privacy in Cloud, Edge, and Fog paradigms. An overview is taken on the challenges and countermeasures involved. The thesis also aims at identifying similarities, differences, attacks, and countermeasures in Cloud, Edge, and Fog paradigms. This will help develop proposals for possible future improvements in the facet of security and privacy.

## 1.2 Overview and Analysis of Paradigms

We will be examining the general overview of three different Paradigms: Cloud, Edge, and Fog Paradigms. This will focus on security and privacy aspects. From a layman's perspective, one may think that Cloud, Edge, and Fog are strongly or almost the same paradigms, but we will carefully present some similarities and differences for these paradigms. For clarity and consistency, each paradigm is carefully discussed separately concisely. The reason for discussing each of these paradigms is to have an overview that will guide our understanding of the research goal for this thesis, which is primarily the information security and privacy aspects for each paradigm.

The goal of having a huge capacity for storage with efficient scalability has recently been the driving force for different companies, organizations, and small firms to switch to Cloud, Edge, and Fog Paradigms. Interestingly, the aspect of security and other issues regarding privacy, in particular, becomes a matter of concern when Cloud providers holding large amounts of data and essential applications share it with customers [1]. As a result of these concerns, security and privacy issues arise to present major problems in Cloud, Edge, and Fog paradigms. Currently, the biggest attention in each computing model is about protecting the privacy of users (essential data) from unauthorized groups or individuals gaining access and hindering attacks. Moreover, the keeping of data integrity intact and also maintaining it is a very vital aspect. This research takes an approach to review the security and privacy aspect in Cloud, Edge, and Fog paradigms [2].

The rapid and ever-increasing need for Cloud, Edge, and Fog Computing is a great challenge when it comes to protecting personal information (privacy) and other important data [3]. Cloud customers possess legitimacy to their individual information and data (in other words, users should have the right as to how, when, and to the certain defined range that persons can gain access to their personal information) [4]. Importantly, five different features relating to security and privacy aspects are raised here in any order: integrity, accountability, confidentiality, availability, and the preservation of privacy [4, 5, 6]. This thesis focuses on how security in Cloud, Edge, and Fog Computing systems is provided and how users' privacy is protected from attackers. Essentially, the vision here is to render a holistic management style for personal data at the global centers hosting Edge, Fog, and Cloud. It is noteworthy that clients' data confidentiality must be preserved, which is only possible by acquiring access control and monitoring devices. **Figure** 3.1 shows that acting in place of customers (data proprietor), a Trusted Third Party can gain access to stored data in the cloud to control information. Customers could also be provided with special tools to facilitate the monitoring and accessibility with control over their data [7].

## 1.3 Review Methodology

Recently, there has been a sharp, universal shift from traditional operations in organizations to embracing innovations such as Cloud Computing and other paradigms. These different paradigms, such as Cloud, Edge, and Fog Computing, have many academic studies and reviews from students and researchers. It is greatly difficult or if not very challenging for different Information and Communication Technology (ICT) engineers, researchers, and students to generally match up with the ever-growing pace of new journals, literature, and article reviews. One important area concerning the various paradigms is the security and privacy aspect, which we shall systematically review based on PRISMA guidelines. This review is essential because it provides the opportunity to see into gaps of other journals after carefully examining them, thereby making room for improvement with proposed solutions. This is considered a more efficient way of getting a “baseline” on what was right and what wasn't right [8].

Moving forward, it is of opt-most importance that we take a glimpse at the overall idea of a Systematic Literature Review (SLR). Firstly, we shall be answering the question, what is SLR by defining it. According to Denyer David and Tranfield David, **"Systematic review is a specific methodology that locates existing studies, selects and evaluates contributions, analyses and synthesizes data, and reports the evidence in such a way that allows reasonably clear conclusions to be reached about what is and is not known"** [9].

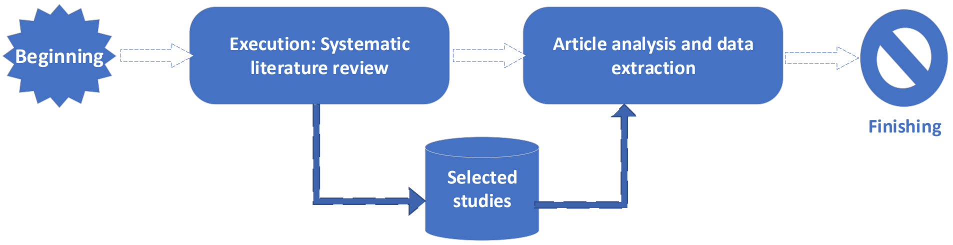

Beginning
Execution: Systematic literature review
Article analysis and data extraction
Finishing
Selected studies

***Figure 1.1.*** *Summarised methodological research process [10]*

The research methodology in **section A** is considered to perform a systematic literature review, as per the guidelines suggested in the PRISMA statement [11]. Initially, identifying appropriate keywords and other related synonyms was the first step. These keywords do assist in generating search expressions. A concise and adequate breakdown and analysis of the literature were carried out, and the following keywords gave a much-needed search expression: Cloud computing, Edge computing, Fog computing, security, privacy, Internet of Things (IoT). Details on the search expression is presented in **section A.3**

Keywords used for performing the search are selected and range from 2010 – 2021 scale, using the most popular ICT sector databases for research works, such as IEEE, Web of Science, Science Direct, SpringerLink, Scopus, and a few others. We put together some potentially essential journals (January 2021), not considering pre-prints, duplicates, and grey literature. Later on, we decided to analyze the titles, abstracts, and keywords of the various academic publications to figure out specific journals, articles, and other important papers related to security and privacy in Cloud, Edge, and Fog paradigms.

Some exclusion criteria were set to narrow down the search outcomes during the first screening stage from the paper's titles and abstracts.

- Not related to security and privacy in Cloud, Edge, and Fog computing.
- Not in English.
- Works with no technical content.
- Full text not available.

After successfully applying the above-refined process, we significantly reduced the number of potentially essential papers to 447. Also, after a critical analysis of the chosen literature based on their citations and references, and inclusion of 77 papers were added, which these were made to be included in the main body and discussion of this particular systematic literature review on security and privacy aspects in Cloud, Edge, and Fog paradigms.

(“cloud computing*” OR “edge computing*” OR “fog computing”) AND (Security*) AND (edge OR cloud OR Fog OR approximate OR iot OR “Internet of Things” OR security OR privacy)

Not related to cloud/edge/fog computing security; Pure survey and review articles; Works with no technical content; Full text not available. After a successful application of the above-refined process, we significantly reduced the several potentially essential papers. Also, after a critical analysis of the chosen literature based on their citations and references and inclusion of 77 papers were added, which these were made to be included in the main body and discussion of this particular systematic literature review on security and privacy aspects in Cloud, Edge, and Fog paradigms.

## 1.4 Selection of Study

During the review, an overall of 77 papers were chosen. A selected number of 447 articles were achieved from the search in the various databases. 61 duplicates were found and were taken off the list. The headings of the various articles, their abstracts, and important words of the retained 386 papers were screened, and 187 papers were dismissed since they unmatched the basic requirements. The number of papers left was 199, and their whole content were thoroughly analyzed. 122 papers were still rejected since they also did not match some other demanded criteria, while a complete number of 77 papers were subsequently added to the literature review process. After examining the reference lists, no additional papers were found qualified to be included in the review steps.

**Figure 1.2** depicts a summary of the entire steps using a PRISMA flow chart.

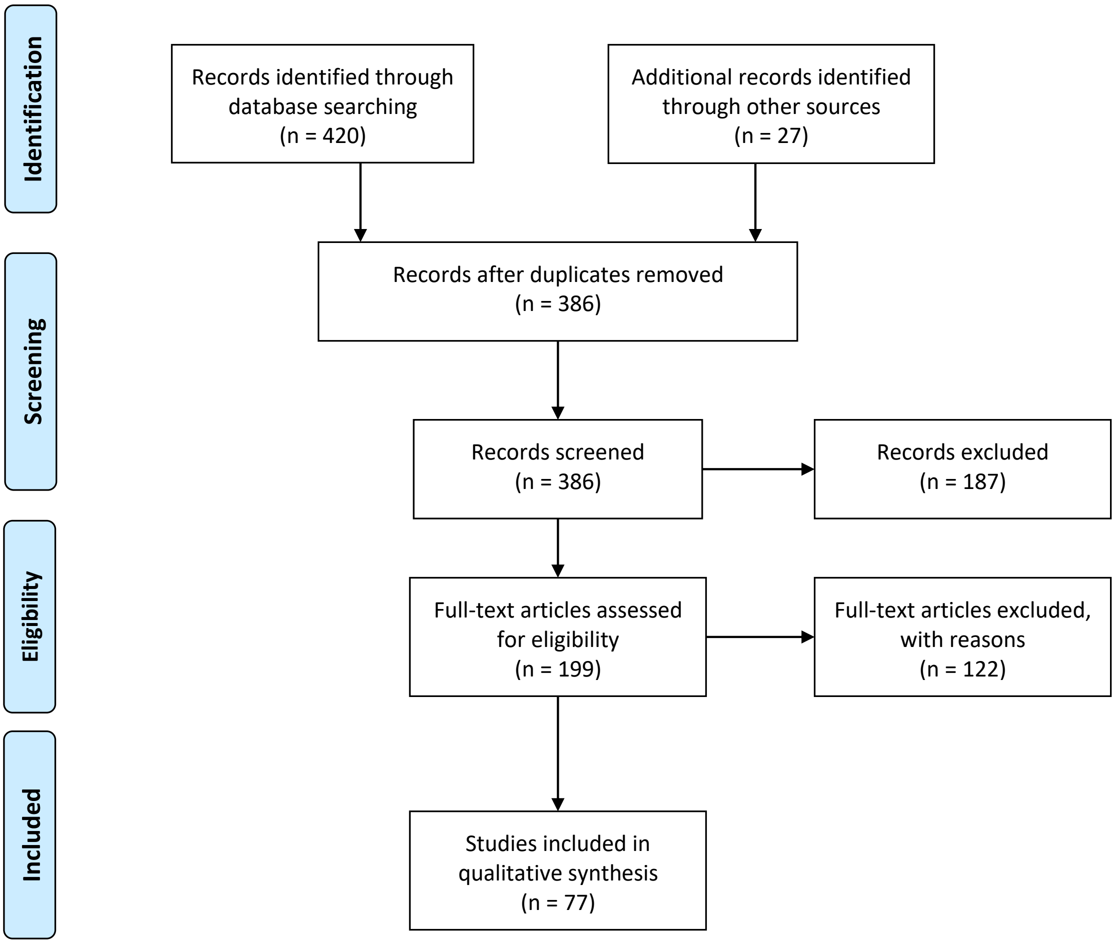

Identification
Screening
Eligibility
Included
Records identified through database searching (n = 420)
Additional records identified through other sources (n = 27)
Records after duplicates removed (n = 386)
Records screened (n = 386)
Records excluded (n = 187)
Full-text articles assessed for eligibility (n = 199)
Full-text articles excluded, with reasons (n = 122)
Studies included in qualitative synthesis (n = 77)

***Figure 1.2.*** *Studies selection summary.*

# 2 OVERVIEW OF CLOUD, EDGE, AND FOG PARADIGMS

## 2.1 CLOUD PARADIGMS

The growth and expansion of many company's infrastructures have come from evolving technologies and innovations. Cloud computing is seen as the unique solution to provide applications for enterprises. Cloud computing uses different components such as hardware and software to render services, especially over the Internet. The possibility of accessing various files and using provided applications from technological devices with Internet access is made easy by cloud computing. Over several servers, the execution of Cloud computing applications is carried out, and developers require clarity on this vital information, particularly when offered as a service by the provider.

### 2.1.1 Definition

Several persons and institutions have attempted to define cloud computing in their understandings and views. Cloud computing is considered an almost new model for enterprises in today's technological facet, though it is rapidly and widely gaining extensive growth, especially within the corporate world. The National Institute of Standards and Technology (NIST) is the most reliable organ, widely considered a near and precise definition for cloud computing. Based on NIST definition as seen below:

**"cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction"** [12].

Different models particularly characterize cloud computing. These models are five in number as widely regarded: on-demand self-service, broad network access, multi-tenancy and resource pooling, rapid elasticity, and scalability. Let's attempt to explain each of the mentioned characteristics.

- On-demand self-service:

More cloud computing resources can be provided as required by manufacturers and different enterprises while avoiding interactions with humans involving service providers. This may refer to database instances, storage space, virtual machines, and many others.

Having access to corporate cloud accounts is essential as it helps corporations to virtualize the various services, cloud usages and mainly to supply and non-supply of services as demanded [13].

- Broad network access:

  Accessing capabilities via established channels across the network advances the use of heterogeneous thick and thin customer devices—for example, workstations, tablets, laptops, and mobile phones [14].

- Resource Pooling:

  Computing resources from the provider are grouped using a particular multi-tenant model to serve various clients. The unseen and non-virtual resources are carefully allocated and reallocated according to the customer's needs. Usually, customers are seen not to understand or have access to the spot-on position or area provided. However, location specification can be established at an advanced state of situation or abstraction. An example here is a data center, country, and state. There are various examples of resources such as network bandwidth, processing, memory, and storage [15].

- Scalability: The growth of a client marketplace or business is made possible due to the tremendous ability to create specific cloud resources, enabling improvement or reduction of the business. Sometimes, changes might occur on the user's need for cloud computing, which will be given immediately by the platform or system. With the cost of management involved in the data center of cloud computing, customers are not expected to incur some financial burden and do not have to make future payments in Information Technology sectors, mindful of owned enterprise as much as possible by you [16].

- Measured Service:

  The resource use is keenly observed, regulated, and feedback is given to established billing based on usage (e.g., accounts of frequent customers, bandwidth, processing, and storage). The proper reporting of essential used services can be done transparently if the utilized resources are adequately looked into, controlled and account is given [17].

### 2.1.2 Architecture

In recent days, we see that big, medium, and small enterprises utilize cloud computing technology to save or store vital data in the Cloud, enabling them to access this stored information from any part of the world via connecting to the Internet. Service-oriented and event-driven architectures are the main combination that makes up the cloud computing architecture. The two important parts dividing the cloud computing architecture are Front End (FE) and Back End (BE) [18].

**Figure 2.1** depicts the architectural view of cloud computing.

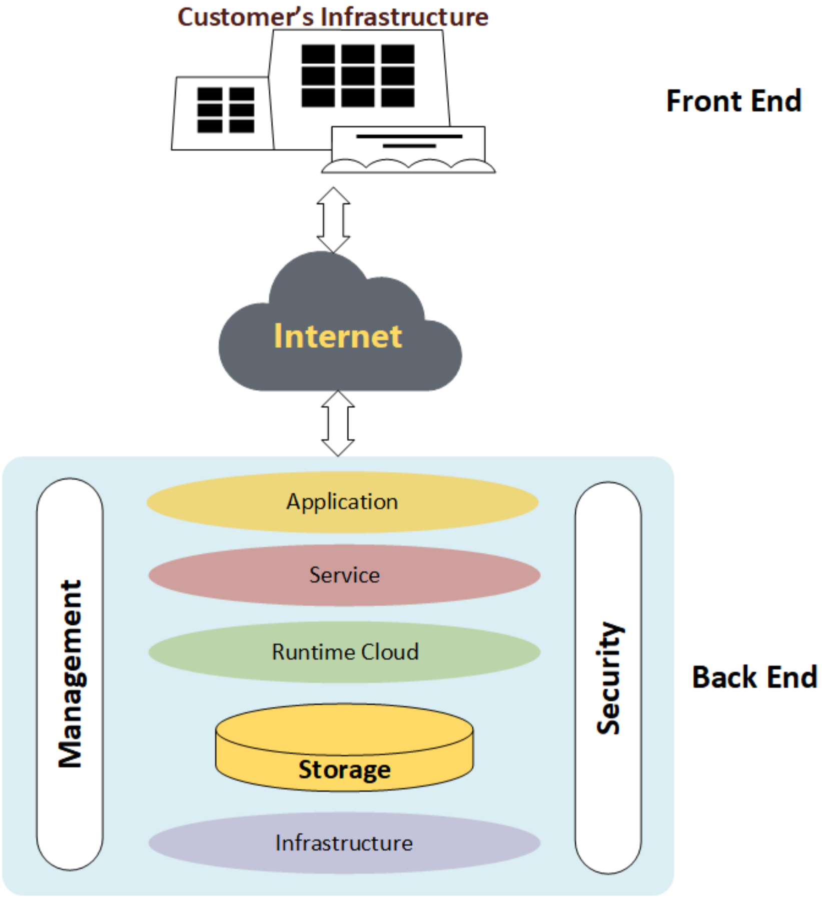


***Figure 2.1.*** *Cloud Computing Architecture [19]*

#### Features of Cloud Computing Architecture

As seen in **Figure 2.1**, various components make up the Cloud computing architecture. In this section, we take a brief look at each of the architecture's different features. Also, we can see that a network connects both front and back ends via the Internet.

1. **Front End**

   The customers constitute the front end. To gain access to the Cloud environment, the front end must have customer-side applications and other interfaces, such as web servers (may comprise Internet Explorer, Google Chrome, etc.), mobile gadgets, and tablets [18].

2. **Back End (Storage, Servers)**

   Companies providing services, also known as service providers, use this back end. Cloud services involve different resources, and the known service provider is managing these resources. Some of the management activities here may include handling a great amount of stored data, implementing new models, servers, control of traffic mechanism, virtual machines, and most importantly, security [18].

3. **Customer's Infrastructure**

   Interacting with the Cloud requires Graphic User Interface (GUI), and this is being provided by customer infrastructure found at the front end [20].

4. **Internet**

   There must be a medium linking both features for the front and back end to function smoothly. Here, the Internet plays the linking role.

5. **Application**

   Application services of Cloud or "Software as a Service" render services by delivering software via the Internet, thus, enabling support and maintenance in a simplified manner. This is possible because the client's personal computer is needless to install and operate the application on it [21].

6. **Service**

   Service plays a vital role, and it is considered an important part of the cloud structure. In the architecture, it is known as a utility provider. Accessing a specific service is made possible by a cloud service. It coordinates and oversees which kind of service you reach for based on customers' demands. The three different types of services provided by cloud computing are Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). Details about the various services are shown in **Figure 2.3** below [21].

7. **Cloud Run-time**

   Services are running in cloud runtime. It acts as a Cloud operating system thereby, providing virtualization platforms to all users while enabling several runtimes to function simultaneously within a single server. The hypervisor is another name runtime referred to. Some examples of Hypervisors are software like Oracle VM (x86), Oracle Virtual Box, and VMWare Fusion. Its primary goal is to coordinate the resources by dividing and distributing them accordingly [22].

8. **Storage**

Storage also refers to storage as a Service (STaaS), enabling cloud applications to operate limitlessly from their restricted servers. With that, customers can save their information remotely and access them whenever they wish globally. There are various standard demands established to be met by Cloud storage to protect customers' information and data. Other typical requirements are performance, reliability, replication, data consistency, and maximum availability. Unfortunately, no single cloud system has established all of the above requirements due to differences in nature. Besides, storage is one of the essential requirements because of the massive storage space and data management it provides in the Cloud [23].

9. **Management**

   Certain tasks are being allocated certain resources by management software. For sure, serious problems can arise from poor management, and it is for this reason, management software is highly important to assist in offering optimum performances in a cloud platform. Some managed components are storage, infrastructure, security, application, service, and cloud runtime. Some security matters at the back-end are also handled seamlessly. There is dynamic interfacing between the front-end and the back-end when there is proper management [24].

10. **Security**

    Traditionally, clients' information was locally saved on their personal computers, but with the arrival of Cloud Computing, a designated data center is established to keep information. Since end-users have to give out sensitive personal data, there is a great concern about protecting users' privacy. For this reason, we see how integrated, and essential security is in the back-end of cloud infrastructure. There are possibilities of emerging threats, such as cybercriminals who can use visualized designs to perform attacks, security is adequately offered to secure files copyrights, systems, infrastructure, and cloud resources to customers. In all, customer privacy and data protection with integrity are the most and number one service provided by cloud service providers [21].

### 2.1.3 Cloud Scenario

The growing rate of digitization and the coming of Cloud Computing, with its great benefits, has influenced many institutions to shift towards Cloud services. Computer technology has come a long way with numerous advantages, such as electronic learning, fondly known as E-learning. Here, it is hard to witness person-to-person interaction in most circumstances. However, a widely popular expression describes E-learning as content with specific instructions or a learning opportunity made available online via internet technologies [25]. A typical example here is the SISU and Moodle platforms by Tampere University.

In the past, Universities relied on their IT services for all the IT-related works by students, staff, and other employees, which most often was challenging as seen in **Figure 2.2**. Solutions were sometimes hardly affordable or very costly.

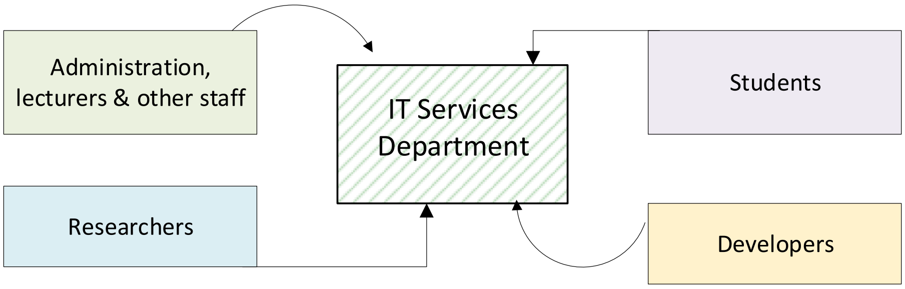


***Figure 2.2.*** *University Traditional IT Scenario [26]*

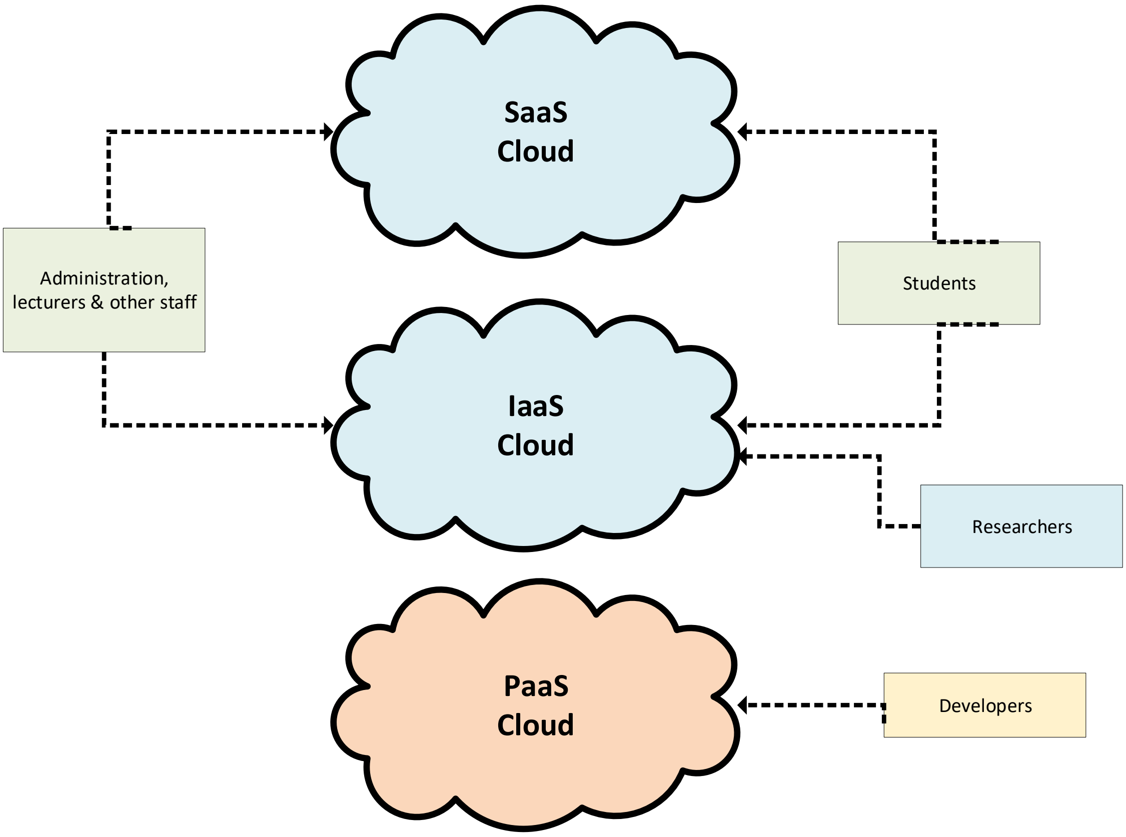


***Figure 2.3.*** *University Modern Cloud Scenario [26]*

E-learning is defined in [27] as “all materials delivered through the internet connection, audio streams, videotapes, CD’s, interactive TVs, adding to this mobile and wireless technologies.” Other academic journals explain the essential part played by services rendered via E-learning in the teaching field and the great role of Cloud Computing in current distance learning difficulties [28].

University students and administrations are capable of accessing online materials via Web applications within the University campuses and also at home for individual assignments, thanks to the infrastructure of Cloud Computing seen in **Figure 2.3**. Today, we all acknowledge the immeasurable advancements that virtualization brought to the educational sector, which is greatly noted and established. Cloud Computing which allows for the making of several networks for customers and easy configuration of servers while meeting the required demands for different specifications, gives an easy to manage the system. In general, Cloud Computing has greatly enhanced Higher Education learning, for example, University lectures with the help of E-learning and massively offers possible solutions to long-aged traditional classroom learning [27].

### 2.1.4 Cloud Computing Services

In the cloud paradigm, in terms of provided services, there are several different types we can look into. Here, narrowing it down to the most vital ones will help us concisely understand. While we all know how huge cloud computing services are enormous, there are classified under a variety of categories. Three main cloud computing services we shall be looking into are as follows:

1. **Software as a Service**

   SaaS is classified as public cloud computing. The browser is considered the main platform for delivering cloud applications using internet service. It is widely believed today that Microsoft's Office 365 and Google's G Suit are the primary enterprise applications for SaaS; regarding business applications involving ERP suits that are gotten from SAP and Oracle, they have embraced the SaaS design. Significantly, clients are provided an environment to grow with huge choices where they can initiate or create their customization and improvements [29].

2. **Infrastructure as a service**

   "IaaS" is an abbreviation for the term widely known as Infrastructure-as-a-Service.

   According to International Business Machines Corporation (IBM), cloud education, IaaS "is a form of cloud computing that delivers fundamental compute, network, and storage resources to consumers on-demand, over the Internet, and on a pay-as-you-go basis" [30].

3. **Platform as a service**

   Based on search Cloud computing (online 2020), "Platform as a service is a cloud computing model where a third-party provider delivers hardware and software tools to users over the Internet [31]." Often, developing applications requires these needed tools. The building owned by the PaaS supplier turns to accommodate both the software and hardware. For this reason, new applications are created or executed, thereby allowing developers not to bother with the in-house installation of software and hardware applications [32].

### 2.1.5 Benefits of Cloud Computing

1. **Cost-effectiveness**

   It can create cost reduction by lowering or increasing the rate at which software or hardware devices consume compared to other computing paradigms. In certain scenarios, it can be automatically performed [33].

   Choosing to switch to cloud computing might lower expenses in maintaining equipment and managing the entire system. It will be wise enough to acquire cloud computing services providing establishment instead of buying costly models and devices for your business. Some very important points why the cost of running your business may be reduced as seen below [34]:

   - Your contract usually includes updating your systems and access to new software and hardware when available.
   - Wages paid to some staff specialist is avoided.
   - Possible lowered cost due to energy utilization.
   - Delay in time is significantly decreased.

2. **Scalability**

   Business execution and storage demands can be increased or decreased rapidly to meet your condition, permitting flexibility and demands to evolve. It is quite reasonable to deploy Cloud, which helps in allowing you more free time to operate your enterprise. Things are made easier by your cloud service supplier, who takes care of the various application upgrades, so you don't have to bother buying and installing costly upgrades [35]. Here, you pay only for user services, and this gives you the flexibility to manage your finances adequately, thereby avoiding unnecessary spending [36].

3. **Sustainability**

   Global campaign for a green environment is the talk of the time worldwide. Businesses have been tasked with doing much better because putting thrash bins in office areas and other strategic corners is insufficient. Adequate sustainability demands remedies that tackle wastefulness in various categories in an organization. A minimum carbon footprint can be achieved by migrating to a cloud system, which is highly regarded as being more friendly to the environment.

   Designs of cloud structures proactively support environmental friendliness, enhance virtual activities while limiting hardware and material products, and greatly reduce paper thrash. Workers can perform their duty from different locations without necessarily commuting to the office goes a long way to decreasing emissions relating to road activities. Data presented by a report from Pike Research indicates that between 2010 to 2020, there will be a 31 percent drop in energy usage from the data center, based on the hosting of cloud computing, which also includes varieties in virtual data [37].

4. **Effective Collaboration:**

   Communication and data sharing are important aspects of every modern business setup. This is made possible by using a cloud system, which effectively collaborates in a cloud milieu. Different members taking part in a particular project from various geographic locations can access the same file using cloud computing, such as workers, procurement management team, and other parties concerned. There is the possibility to select a special model of cloud computing that facilitates record sharing with other administrators such as an adviser (e.g., a faster and reliable medium in which accounting report records can be shared between financial personnel) [38].

5. **Accessibility and Higher Security:**

   Security fears are always at the pivot of many business organs when aiming at migrating to cloud infrastructures. Basically, how is someone able to know that files, data, and other programs are secured on-site if they are being accessed from different locations remotely? What restricts an internet criminal from performing the same remote task? Mainly, one of a full-time duties in the Cloud is to keenly observe security, which is very important and effectively better than the usual in-doors system, in which an enterprise does share its activities between numerous concerns in IT, as security is top of the worries. Data encryption is often considered a safe way to transfer data within a network and preserve it in a database. Information is more protected, and less access can be made possible from cyber fraudsters when data is encrypted. Cloud users differ in their security demands. This means that Cloud computing services render various security levels as per the customer's need [39].

6. **Automatic Updates Possibility:**

   Service fees are often not charged separately to get updates automatically and may come as a package for IT demands. Company's systems are frequently updated with the most current technological innovations, which are done based on different service providers of cloud computing. Generally, the latest versions of up-to-date software, the processing capability of computer and also servers' upgrades [40].

## 2.2 EDGE PARADIGMS

A few years back, offices hosted servers with edge computing. No one thought of it in such a manner. The result was all that mattered and not how it worked. Later on, Cloud was introduced, and everything was different. Devices such as computers have been placed hundreds of meters and milliseconds apart. In certain offices, their applications were quite fine with the latency. However, with the rapid increase of 5G, IoT, and the constant quest for internet speed, an innovative form of computing has been born, known as edge computing. This type of computing is not only popping up like any normal technology by the day.

The word “cloudlets” describes small nodes of edge-located computing ends. As a new aspect or computing paradigm, edge computing helps position important compute and save resources at the Internet Edge, close to various office and home appliances such as mobile devices, IoT devices, clients, and clients sensors. There has been fast growth in industrial and research investment in Edge computing in recent years. The pivot for Edge computing is the physical availability and closeness, which end-to-end latency is influenced by this essential point of cloudlets, with bandwidth achievable economically, trust creation, and ability to survive [41].

### 2.2.1 Definition

Communication between a customer and a server site is improved due to a reduction in long distances brought about by the edge computation of the network. According to Cloudflare (online), "Edge computing is a networking philosophy focused on bringing computing as close to the source of data as possible to reduce latency and bandwidth use. In simpler terms, Edge computing means running fewer processes in the Cloud and moving those processes to local places, such as on a user’s computer, an IoT device, or an edge server" [42].

Some other attempted definitions of edge computing are as follows: Stlpartners (Online), "edge compute is a physical compute infrastructure that is positioned on the spectrum between the device and the hyper-scale Cloud, supporting various applications. Edge computing brings processing capabilities closer to the end-user/device/source of data which eliminates the journey to the cloud data center and reduces latency" [43].

### 2.2.2 Architecture

There are several cases in which architectural designs are specifically intended for, considering their work plan and setting up the infrastructure is based on its need.

Considered a current paradigm, edge computing takes services and applications from

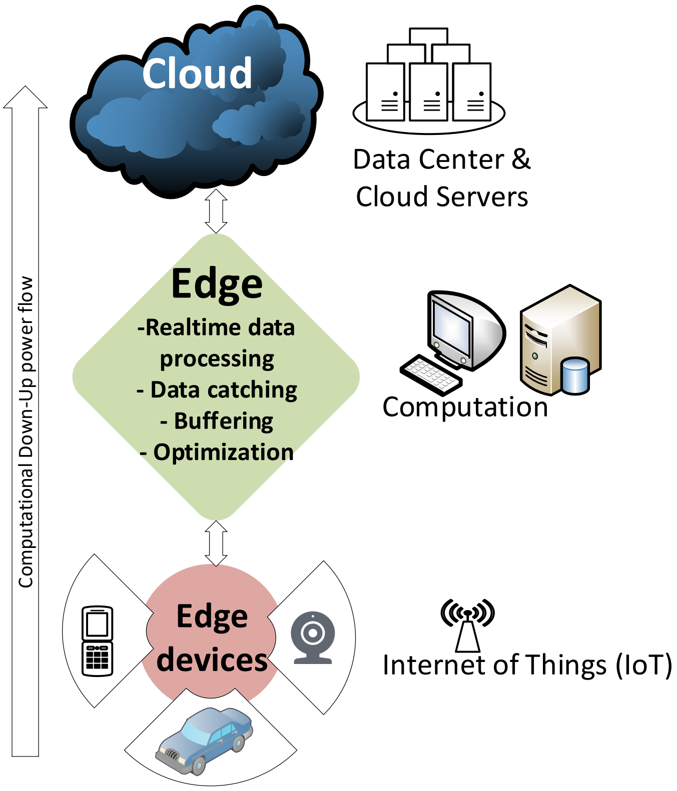


***Figure 2.4.*** *Edge Computing Architecture*

the Cloud, which is known to be centralized to the nearest sides to the main source and offers power to process data. It provides added links, linking the Cloud and the end-user devices, as shown in **Figure 2.4**. One of the best ways to solve or reduce cloud computing issues is to make sure there is an increase in edge nodes in a particular location. Increasing the Edge nodes will also help in decreasing the count of devices attributed to a sole Cloud [44].

**Figure 2.4** shows the interaction of various edge devices to the Fog nodes and later to cloud data centers. Some such Edge devices are tracker bands for fitness and medical uses, smart televisions, and smartphones. Edge devices and the Cloud are linked up by Fog nodes connecting the links. Between different gadgets or personal items, Edge devices act as interfaces attaching these devices to the cloud [45].

A typical Edge Computing architecture comprises three important nodes: the Cloud, local Edge, and the device edge. These are further explained as follows:

- **Cloud (Data Center)**

  Cloud is fully responsible for the hosting of data structures and cloud servers. Both the data centers and the cloud servers have specific functions which they do carry-out. These functions can be broken down as follows:

  **Data Center:** Great quantity of generated data from edge servers and data centers are being stored here.

**Cloud Server:** Involves in the integration of various duties removed (offloaded) from edge storage, and importantly with the maximum standardized authentication, authorization, and computation. The most exceptionally outstanding data center and cloud servers are made of very powerful machine clusters [46].

- **Local Edge (Computation)**

  Local Edge involves a well-defined structure having several sublayers made up of different edge servers with a down-to-up power flow in computation depicted in **Figure 2.4**. Both Access Points (AP) and wireless base stations are edge servers situated at the sublayer considered to be the lowest. These are particularly installed to get data during communication from various edge devices, returning a control flow using several wireless interfaces [47].

  Base Stations (BS) send data to the edge servers found in the sublayer (upper) after receiving data from edge devices. Here, the upper sublayer is particularly concerned with operating the work of computation. Very fundamental analysis and computation are done after getting data forwarded from base stations. At a recent edge server, the computational restriction is placed such that, if the difficulty in a given work surpasses it, the work is offloaded and sent to the upper sublayers with adequate computation abilities. A chain of flow control is then concluded by these servers with passing back to the access points, and finally, in the end, send them to edge devices [46].

- **Edge Device (Smartphones / Health Monitoring)**

  Sensing, actuating, and controlling are some of the main activities carried out by edge devices. Edge devices are described as electronic devices with a low-standard and established Edge device layer (EDL). Every edge device consists of a micro-controller (MCUs) that logically control the devices. Each of these MCUs is considered a little computer operating on one integrated circuit. Firmware helps provide the device with control through the low-standard programmed interface in the MCUs. The MUCs solely cover all operations, while the controlling, computing, sensing, and other functions are coded in the firewall. Both mobile devices and IoT devices can widely be classified as edge devices. Few device examples of the IoT are health monitoring, smart home devices, and smart warehouse [46].

### 2.2.3 Edge Scenario

#### Augmented Reality and Cloud Gaming

A global number of participatory video performance or players, also known as gamers, is rapidly increasing annually, with a prediction in growing in video players of about 2.73 billion, forecasted by 2021 [48], projecting a global business which surpasses 50USD billion [49]. Due to this, applications were made with innovations capable of bringing together physical actuality with data generated from computers [50], popularly referred to as applications of augmented reality. However, the application types have resisted expansion because of processing disadvantages, recent network, and storage. Internet of a recently adopted infrastructure has shown a great lack of readiness to facilitate Augmented Reality (AR) due to high latency because of vast distance from the infrastructure geographically, not leaving out bandwidth shortages from the network. By adopting and implementing the Edge, we can alleviate the situation effortlessly. The established network design will help reduce the distance from which data can travel. A shorter travel distance of data will go a long way to provide a wonderful and more experience in Reality gaming with better interactiveness (decreased lag time and latency) [49].

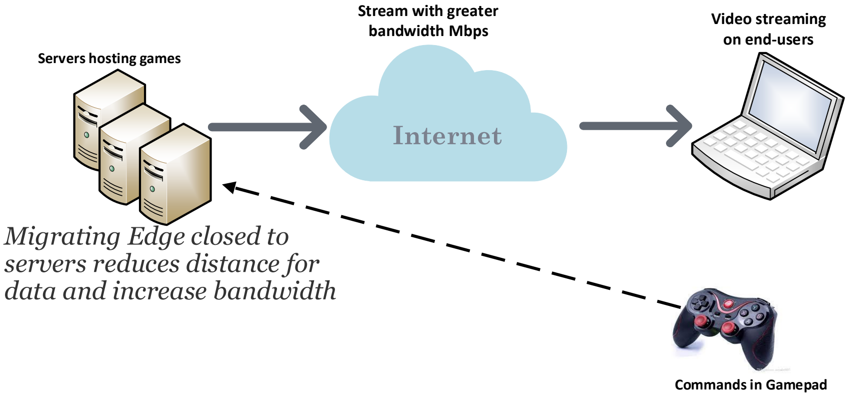

Stream with greater bandwidth Mbps
Video streaming on end-users
Servers hosting games
Internet
Migrating Edge closed to servers reduces distance for data and increase bandwidth
Commands in Gamepad

***Figure 2.5.*** *Edge Scenario-Cloud gaming*
[51]

### 2.2.4 Characteristics of Edge Computing

- **Proximity**

  They are positioned at the Edge of the network. Storage and shared computation are provided at the network edge [52]. There are two approaches to the proximity between the Edge and user's equipment: physical and logical proximity. Physical proximity refers to the exact distance between the top segment of data computation and user equipment. Logical proximity refers to the count of hops at the middle of the Edge computing segment and the users' equipment. There are potential occurrences of congestion because of the lengthy route caused by the count of hops, leading to more latency issues [53]. To avoid queuing that can result in delay, logical proximity needs to limit such events at the back-haul of the computing network systems [54, 55].

- **Collaboration occurs between Cloud-Edge**

  Despite the shortcomings of the normal cloud paradigm innovations to match up with great demands, given lower energy level, real-time, particularly security and privacy aspects, the edge paradigm is not considered a substitute for the Cloud paradigm. Edge and Cloud paradigms are known to assist each other in a cordial manner in several situations. Some network areas where the Cloud and Edge paradigms cooperate include driverless cars, industrial Internet, smart towns, and houses. Importantly, Edge and Cloud paradigm collaboration offers many chances for reduced latency in robust software like in driverless cars, network assets of companies, and information analysis on the IoT [56].

- **Access Mode**

  Operates through supported capabilities from several actors. Bluetooth, ZigBee, Wi-Fi, and some more, are various technologies that create connectivity by linking endpoint equipment and nodes of the Edge computing layer [57]. There is great importance for access modalities as it establishes the endpoint equipment bandwidth availability, the connection scope, and the various device type assistance rendered [54].

### 2.2.5 Benefits of Edge Computing

- **Reduced Latency:**

  Data processing becomes more and less essential when it takes a lengthy time. Looking at examples like in autonomous cars, time is of massive importance because, within some seconds, the required and collected data becomes worthless. We must note that the slightest of milliseconds counts on a rush traffic highway. This also highlights that; milliseconds are extremely valuable during manufacturing in smart factories where robots and other intelligence machines are used to closely observe the various production processes and ensure consistency in data usage. The Cloud does not have enough time to fulfill a back and forth data round trip on several occasions. Rapid call for data analysis is usually a result of dangerous occurrences and disappointment in devices. Latency is easily reduced or perhaps discarded when data analysis is positioned at the Edge where it is made, depicting a quicker response time. With this, data is essential, valuable, and usable. The general organization's total traffic capacity can be reduced by Edge computing, whereby applications and different services are enhanced by an increased level of performance for the entire company [58].

- **Enhanced Data Security:**

  The introduction of uncountable Edge appliances worldwide indicates that all of such appliances are important targets and gateway for cybercriminals and other risks in the security domain. Devices are often scattered in various locations, and handling many such devices is frightening in terms of security. Looking at it keenly, such a model has been challenging when discussing the IoT method due to its centralized design and cloud-focused management systems. We may all say that substantial clients are correct for inquiring about the level of security with Edge or how secured Edge is? Every organization is often concerned about possible attacks on their data and how to keep Edge's workloads best safe. Is it possible to detect and minimize or rather stop further damage from a device? How can Edge nodes be handled regarding rogue? Clients are willing to know what are the special cautions laid down or perhaps current rules and policies to apply during operations within the Edge [59].

  For efficiency and better coordination, everywhere that edge computing is considered the main actor in that network, it must have a centralized approach to enable every device to have the ability to undergo frequent updates and that adequate security standards are observed. It is also important to notice and engage against security threats by constantly monitoring the system using encryption, artificial intelligence (AI), and patching. Notably, the sole responsibility for security steps does not belong to the customers or end-users but the service providers.

- **Decreased Bandwidth:**

  The use of bandwidth and resources for the server are reduced with the assistance of edge computing. There is a finite and huge cost in terms of money from resources of Cloud and bandwidth. Prediction by Statista states that, by 2025, global installation of Internet of Things devices in households and offices such as printers, smart surveillance, thermostats, and alarms, will be rated beyond 75 billion. The smooth functionality of these devices mainly depends on Edge, which therefore means, reasonable number of computations will migrate to the edge [60].

- **Cost reduction in Data Transmission**

  A central server that mostly regulates the different actions to be engaged at is unnecessary since Edge computing facilitates data collection. This assists in decreasing the expenses for running the storage facilities where information is held [61]. More request for IoT means expanded networks. The cost of needed operations will increase due to the increasing size of the ever-growing network systems. It is for this reason that edge computing is attracting more customers and organizations. Regarding other available paradigms, edge computing is considered effective, highly secured, and flexible in scalability, reducing the cost to a bigger extent of security and longer processing time. The entire network, storage, and operating expenses are greatly lowered by edge processing [62].

- **Increased Availability**

  Connectivity is very important with vital systems. It is known that value systems are expected to function, despite the absence of connectivity. Looking at the current flow in communication depicts many pivotal views of failure. These views of failure involve the business's main network, many hops over the many network nodes with issues in security along the path of the network, and different others. Considering Edge, communication is primarily between the customer/client and the equipment (local edge node), which ends up creating an increase as a result in the availability of the various systems [63].

## 2.3 FOG PARADIGMS

Access gateway or set-top-boxes are end devices that can accommodate fog computing services. The new paradigm infrastructure permits applications to operate nearby to observe activities easily and huge data, resonating from individuals, processes, or items. The creation of automated feedback is driving value due to the fog computing concept [64]. Customers benefit from Fog and Cloud services, such as storage, computation, application services, and data provision. In general, it is possible to separate Cloud from Fog. Fog is closer to clients in terms of proximity, mobile assistance for mobility, and dense locational sharing [65].

At the Edge of the network regarding Cloud computing, Fog computing is considered an extension or advancement of cloud computing. Cloud computing ideally focuses mostly on a central system for computing, and it occurs on the upper section of the layer. Fog computing is responsible for reducing the load at the edge layer, particularly at the entrance points and for resource-constrained devices [66].

The term 'Fog Computing' and 'Edge Computing' refers to the hosting and performing duties from the network end by Fog devices instead of having a centralized cloud platform. This means putting certain processes, intelligence, and resources to the Cloud's Edge rather than deriving utilization and storage in the Cloud. Fog computing is rated as the future huge player when it comes to the Internet of Everything (IoE) [67] and its' subgroup of the Internet of Wearable Things [68].

According to David Linthicum, the chief cloud strategy consultant and an important contributor to several tech publications, he states that “Fog computing, a term created by Cisco, also refers to extending computing to the network’s Edge. Cisco introduced its fog computing in January 2014 as a way to bring cloud computing capabilities to the Edge of the network” [69].

The deployment of Fog computing systems and the main concerns are the demands involved in the Fog computing paradigm. This explains why devices belonging to the Fog sphere are heterogeneous, thereby raising the question of the ability for Fog computing to overcome the newly created adversaries of managing resources and problem-solving in this heterogeneous setup? Therefore, investigation for related areas like simulations, resource management, deployment matters, services, and tolerating fault is a very simple requirements [70].

### 2.3.1 Definition

The link between the cloud-to-thing devices is made available by Fog computing. Communication, storage, control, decision-making, and computing close to the Edge of the network are specially chosen by Fog architecture. Here, data is created to solve the shortcomings in the present infrastructure to access critical missions and use cases such as data density. OpenFog consortium defines Fog computing as **"a horizontal, system-level architecture that distributes computing, storage, control, and networking functions closer to the users along a cloud-to-thing continuum"** [71]. There are different approaches when it comes to defining Fog computing paradigm. Some other few definitions can be seen as follows:

"Fog computing is a term for an alternative to cloud computing that puts a substantial amount of storage, communication, control, configuration, measurement, and management at the edge of a network, rather than establishing channels for the centralized cloud storage and utilization, which extends the traditional cloud computing paradigm to the network edge [72]."

### 2.3.2 Architecture

Architecture is a standard for every paradigm. Due to deployments and adoption for the market, Fog computing architecture must consist of standards. Until recently, there is no definite architecture with given criteria. Despite so, many research articles and journals have managed to develop their versions of Fog computing architecture. In this section, an attempted explanation is detailed in an understanding manner, which describes the different components which make up the general architecture in **Figure 2.6**

Over the past years, one of the most treated research themes has been Fog computing and the challenge to precisely define its architectural design. Generally, most of the

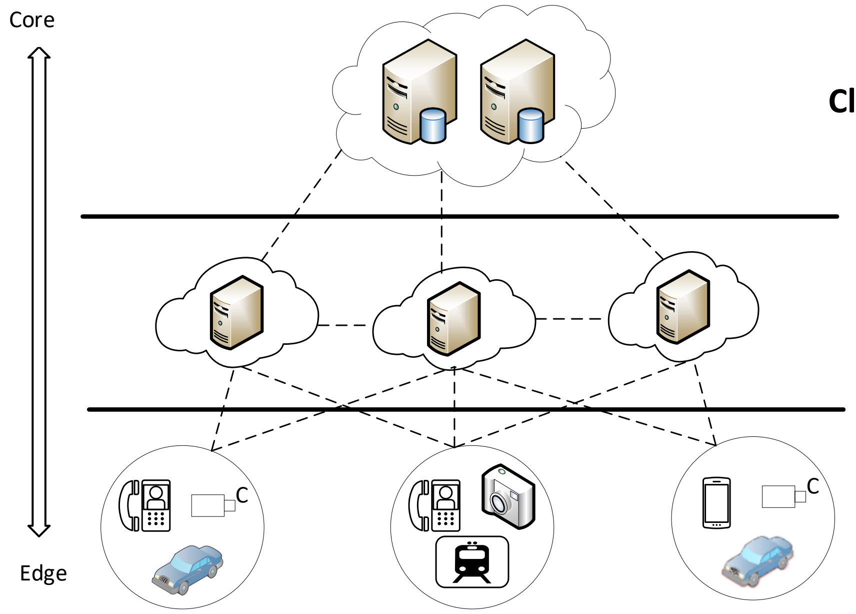


*Figure 2.6. Fog Computing Architecture [73]*

research projects performed on Fog computing had mostly been represented as a three-layer model in its architecture [74]. Besides, there is a detailed N-layer reference architecture [75], established by the OpenFog Consortium, being regarded as an improvement to the three-layer model. However, we will be looking at a three-layer architecture. Below is a depiction of Fog architecture.

**Figure 2.6** importantly portrays the three-layer architecture of Fog computing. Fog computing is considered a non-trivial addition regarding Cloud computing based on Cloud-to-Things setup. Infect it displays a middle layer (also known as Fog layer), closing the distance between IoT devices and Cloud infrastructure. The three layers involved, Cloud, Fog, and IoT, which made up the architecture, are explained below [76].

- **Cloud Layer**

  At this layer, the centralized cloud infrastructure is its main composition. It renders several services with the availability of many servers, which offers high computational and storage capacity. Away from the usual Cloud computing architecture and looking in the Fog architecture, many provided services and computation could greatly be migrated to the Fog layer from the Cloud. Migrating from Cloud to Fog layer essentially means reducing the load burden on Cloud and thereby the efficiency is significantly increased [73].

- **Fog Layer**

  The Fog layer's middle section is considered an essential layer within the Fog computing architecture. All devices known to perform intermediate computing are located in this layer. Like in the Cloud, the Fog layer also uses local virtualization technologies. On the other hand, taking into consideration the available resources, it will be more adequate to implement virtualization with container-based [70]. It should also be remembered that Fog nodes are large in numbers found in this layer. Based on OpenFog Consortium, Fog node is referred to as “the physical and logical network element that implements Fog computing services” [77]. Fog nodes have the capability of performing computation, transmission, and also storing data temporarily and are located in between the Cloud and end-user devices (IoT) [73].

- **IoT Layer**

  Physical and logical software are properly arranged to create and plan an important network, including network components and hardware. For example, an IoT network. There are various decisions one will have to make when considering a Fog computing architecture, such as; availability of data bandwidth with their amount of consumption, arrangement of topology, how the Fog nodes are positioned, and the usage and management of Fog nodes [26].

### 2.3.3 Fog Scenario

#### Streaming Video

Fog environments are known for their properly organized manner to transmit data packets relating to video operations, influenced by the ability and flexibility of the Fog paradigm for reduced latency provisioning, place recognition, and mobility with data analytic based on real-time operations. A similar work [78] shows how application to observe a video of structural hierarchy with the demand for three-stage, reacts on detecting motion via smart or digital cameras and later carried out a process to detect and recognize faces while using fog technology accompanied by a Cloud instance process to collect data for identification. According to Magurawalage et al. [79] expression to aqua computing is an outcome from water cycle inspiration that can be performed in either or both Cloud and Fog processing vicinity. The suggested modeled application comprises clones found at the Edge, which will function in different situations when streaming video on users' devices, acting as a buffer zone.

Fog services are highly useful when it comes to supporting on-demand streaming of video [80], such as improved communication when it comes to real-time video packet analysis in security cameras, done through a structured, virtually designed desktop system. One of the essential gains for deploying fog computing is to enhance the streaming of video, in another research [81] where specific requirements are identified for fog paradigm deployment organized in an orderly manner of Cloud computing to assist Edge node as an intelligent network.

### 2.3.4 Characteristics

The essential pushes for the eminent migration from Cloud computing to Fogging or Fog computing are caused by load from computations and bringing Cloud computing close to Edge. Several characteristics are defined Fog computing by the tremendous applications with varieties and IoT design services [82].

#### Heterogeneity

Storage, computational, and networking are rendered by Fog computing, a virtually inclined structure. It provides services between centralized Cloud and different devices found at the Edge, such as end-user applications. The heterogeneity of Fog computing servers comprises shared locations with hierarchically structured blocks.

#### Distribution by Geography

Fog computing models consist of extensively shared deployments in actuality to offer a Quality of Service (QoS) regarding mobile and non-mobile user appliances [83]. The nodes and sensors of the Fog computing are geographically shared in the case of various stage environments. For instance, monitoring different aspects such as chemical vats, health care systems, STLS sensors, and climate is important.

#### Cognition

The ability to effectively react to the primary goal and objective can be called cognition. Customers' requirements are better alerted by analytics a Fog-focused data gateway, which helps give a good position to understand where to make a transmission, storage possibilities, and the control operations along the whole process from Cloud to the Internet of Things continuum. Customers turn to enjoy the best experience due to applications' closeness to users' devices and creating a better precise and reactiveness of clients' need relation [84].

#### React-Time Monitoring

The interactiveness based on real-time varies. It is vital for applications with fog features, such as monitoring oil drills assisted by fog-edge appliances, traffic observation systems for real-time transmission, and applications for monitoring electricity sharing. The utmost ability to enable the processing in real-time is involved with Fog applications because the QoS is guaranteed instead of processing in batch.

#### Mobility Support

Mobility support is a pivotal fog computational strong feature which can facilitate straight communication between mobile items making use of Software Defined Network (SDN) standard rules that rearrange main identification from the place identifier with a distributed indexing style [85].

#### Interoperability

To acquire a higher probability or maximum assured support ranging across vast services, for example, getting the opt most performances when analyzing data and making anticipated decisions in real-time processing and streaming of data, the components of Fog computing are much more expected to pose the capabilities to inter-operate in diverse platforms.

### 2.3.5 Benefits of Fog Computing

Core capabilities of Fog are distributed with various advantages offered and benefited by many organizations, applications, and developers. Usually, the benefits related to Fog computing are most often given as CEAL [86, 87], although we know that one vital advantage of them is Security and abbreviated as SCALE [88] which represents: Security, Cognition, Agility, Latency, and Efficiency.

- **Security**

  Despite some particular security drawbacks encountered by Fog Computing, it can still render specific advantages. It is known that there are fewer openings for eavesdropping, especially when the distance in which data have to travel or be transmitted is shortened. Verification of Identity is made stronger when authentication issues are taken into consideration based on location [89].

- **Cognition**

  Clients' demands are better met by sharing unique computing, storage capacity, communicating, and controlling Cloud-to-IoTs from built applications. All these are made possible due to the great understanding and cognition of Fog Computing [73].

- **Agility**

  For any innovation to be established and adopted, it takes so much time and can be expensive as well, and because of this, there is a slow development of modern services. The coming of Fog has offered quick, innovative, and achievable scaling as a marketing open place, providing the opportunity for different persons and little groups to utilize available developmental tools (SDKs and APIs) and the rendering of recent services from increased Internet of Things [73].

- **Latency**

Storage is positioned near end-users or customers, supported by Fog Computing which also supports data processing. Based on this, it is known that Fog infrastructure squarely matches the demands for applications in time-sensitivity and also in real-time processing [89].

- **Efficiency**

There are improved general activities and smoothness amongst Cloud systems and IoT devices due to the integrated manner of Fog's designed structure. This Fog model assists in bringing together various computing systems facilitates communication between them, implement control, and provides storage capacities [73].

Different papers also talked about the various features and benefits of the Fog paradigm. However, we agree that the established benefits mentioned here are the main ideas that generated other characteristics.

## 2.4 Differences And Similarities: Cloud, Fog And Edge Paradigms

The main goal of Fog and Edge paradigms are similar in some areas, unlike Cloud Computing. They both render capabilities of the Cloud paradigm right to the network edge. They can offer customers low latency in services and make sure that highly practical applications that are delayed have a saved bandwidth in the network [90].

It is not often easy to differentiate and compare Cloud, Edge, and Fog Computing simultaneously. This section tries to differentiate and look into some similar features between the computing paradigms. The differences and similarities of the various paradigms is summarized as represented in **Table 2.1**.

| **Attributes** | **Cloud Computing** | **Edge Computing** | **Fog Computing** |
|---|---|---|---|
| Architecture | Centralised | Distributed | Distributed |
| Response in Real-Time | Lesser | High | Higher |
| Provided Services | Universal services | Often utilizes mobile networks | Vital for particular domain and distributed |
| Security/Privacy | Undefined | Devices involves limited security | Point-to-point |
| Energy Consumption | High | Low | Lower |
| Identifying location | No | Yes | Yes |
| Main Providers | Amazon and Google | Cellular network organs | Cisco IOx |
| Mobility | Inadequate | Offered with limited support | Supported |
| Interaction in Real-Time | Available | Available | Available |
| Latency | High | Low | Low |
| Bandwidth Cost | High | Low | Low |
| Storage capacity and Computation | Strong | Very limited | Weak |
| Scalability | Average | High | High |
| Overall usage | Computation distribution for huge data (Google MapReduce), Apps virtualization, Storage of data scalability | Control of traffic, surveillance and caching of various videos | CCTV surveillance, imaging of subsurface in actual-time, Internet of Things(IoT), Smart town, autonomous vehicles. |

***Table 2.1.*** *Comparison on different computing paradigms [91]*

## 2.5 Conclusion

To address security and privacy in Cloud, Edge, and Fog paradigms, we needed to have an overview of each of these indicated paradigms, respectively. This section described some fundamental features that constitute each of the said paradigms, making them unique in their ways. We looked into the different architectures, how these paradigms are characterized and how beneficial they are to the industries, and addressed some scenarios in which they are applied. From all these, we could deduce the differences and similarities for Cloud, Edge, and Fog paradigms.

Cloud being a centralized architecture and an IoT promoter, have several shortcomings such as high latency, location sensibility, and computation, just to name a few. Researchers then suggested upgraded technologies known as Edge and Fog paradigms to lessen the burden on Cloud systems and resolve the issues indicated. Ultimately, we see that those two paradigms have helped decrease the large quantity of data sent to the Cloud.

Finally, the Edge paradigm is advantageous over the Cloud paradigm, especially regarding security and privacy. However, the Fog paradigm consisting of Fog nodes is most regarded as an outstanding architecture uniquely created so that IoT appliances are rendered improved services and support. In **chapter 3**, we shall see some security and privacy analysis relating to Cloud, Edge, and Fog paradigms, respectively.

# 3 ANALYSIS OF SECURITY AND PRIVACY IN CLOUD, EDGE, AND FOG PARADIGMS

After taking a thorough look into each paradigm overview in **chapter 2**, this chapter deals with the analysis of the different paradigms in regards to their security and privacy.

The goal of having a huge capacity for storage with efficient scalability has recently been the driving force for different companies, organizations, and even small firms to switch to cloud, Edge, and Fog paradigm. Primarily, Cloud providers dealing with customers large and sensitive data handles the aspect of security and privacy with extreme care, using the best reliable mechanisms to store and protect these data. It is noteworthy that clients' data confidentiality must be preserved, which is only possible by acquiring access control and monitoring devices. It is established in **Figure** 3.1, that acting in place of customers (data proprietor), a Trusted Third Party can gain access to stored data in the Cloud to control information. Customers could also be provided with special tools to facilitate the monitoring and accessibility with control over their data [7].

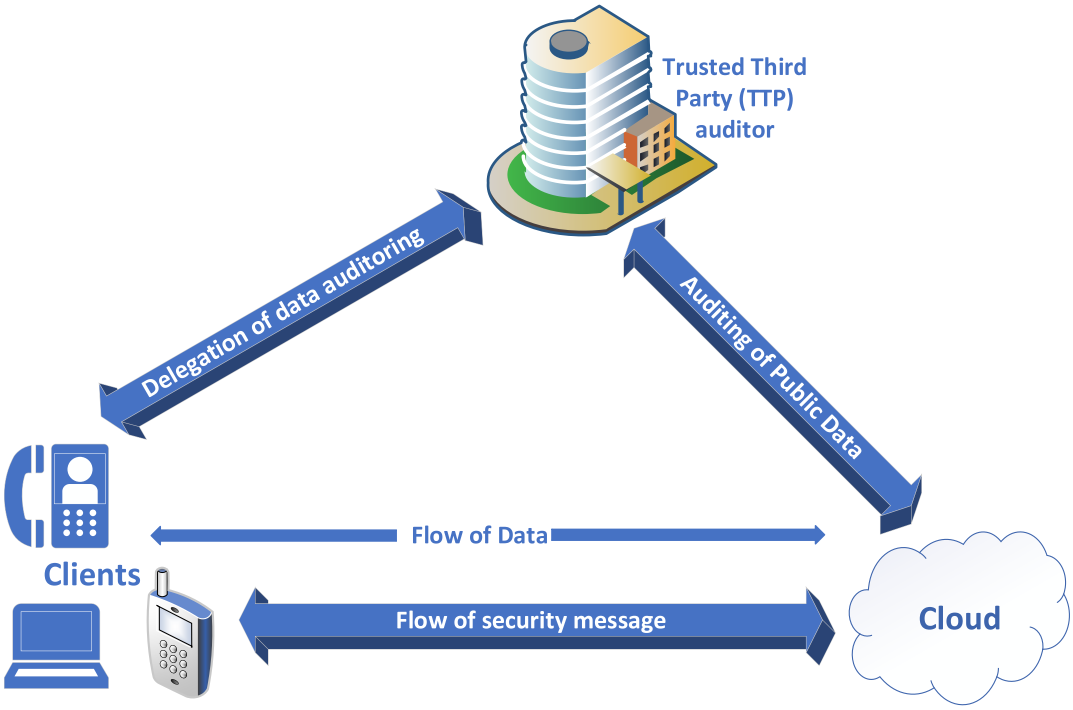


***Figure 3.1.*** *Basic Data Storage design for Cloud [92].*

Looking at **Figure** 3.1, the third party makes the duty of users simple, as they represent the clients in performing the task. The third-party carries out several defined responsibilities, but the major aim is to ensure adequate data information being acquired by the customer being forwarded from cloud services providers. Some other purpose in which the third party is being utilized is for authenticating, encrypting, and decrypting reasons involving other basic work relating to security demands. Despite the importance of the Trusted Third Party model, it still poses various challenges. Focus is placed more on inspecting data instead of concentrating on the security aspect in the Cloud. It also does not entail protecting the privacy of information and thereby exerting huge pressure on customers since the customer performs encryption and decryption with increased load. The provider side of cloud services, carry out no encryption and decryption duty [93].

## 3.1 Definition of Security and Privacy - related Terms

Security and privacy are known to have a symbiotic relationship and a close reflection of one another. In ICT, many academicians and organizations see the two terms as closely related. The influence of digitalization has tremendously shaped our daily activities [64]. Big companies now deal with various computing paradigms, involving huge computation and processing of large data. Thus, transmitting these data from one source to another makes it vulnerable and therefore requires protection. This protection is commonly known as security and privacy. In this section, we will define security, privacy, threats, countermeasures, security mechanism, see some differences and possible similarities between security and privacy [94].

### 3.1.1 Information Security

Information security is defined as the act of protecting essential information from exposure by implementing strict standards or mechanisms to restrict or deny unauthorized access, thereby ensuring data confidentiality, integrity, and availability.

The information is mostly in digital format and requires absolute security from attackers. The presence of security is not a complete assurance for no breaching of data, and therefore calls for enhanced security procedures to assist in stopping internet criminals from gaining free access. **Figure 3.2** depicts major aims of security which are to assure confidentiality, portray integrity and maintain the availability of data [95].

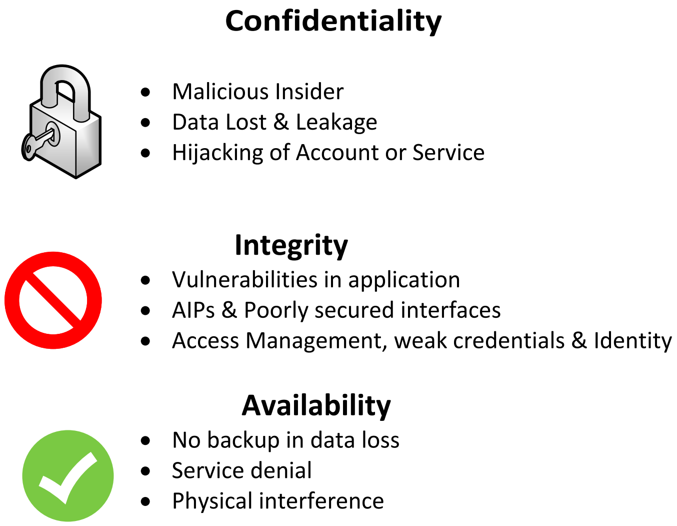

Confidentiality
Malicious Insider
Data Lost & Leakage
Hijacking of Account or Service
Integrity
Vulnerabilities in application
AIPs & Poorly secured interfaces
Access Management, weak credentials & Identity
Availability
No backup in data loss
Service denial
Physical interference

***Figure 3.2.*** *Main Security Expectations [96]*

### Security mechanism

“Security mechanism is a defensive framework used for securing the computing resources, services, information, and sensitive data. They are narrated in terms of safeguards and countermeasures to increase the security of the cloud” [97].

## 3.1.2 Information Privacy

Privacy refers to the privilege owned by individuals having control over their essential information. Another article defines privacy as “the ability of an entity to control what information it reveals about itself to the cloud (or to the cloud SP), and the ability to control who can access that information” [98]. Privacy can also be interpreted as the secrecy of personal information. One big issue about various computing domains is privacy since there is a transfer of private and important data from users’ devices to the servers. Institutions handling people’s information are highly expected to comply with a nation’s legal regulations regarding standard protection of privacy. The main privacy concerns are data privacy, identity privacy, and location privacy [99].

## 3.1.3 Vulnerability, threats, Attacks, and Countermeasures

### Threats

Threat refers to "a potential breach of security that could exploit a device or asset’s weakness. Accidental, environmental (natural disaster), human error, or human failure may be the cause of the threat" [97].

| Attacks | Threats |
|---|---|
| • It is a willful action | • It can be done willfully or unwillingly |
| • Harmful intension | • It might be or not be for any harmful intension |
| • The aim is to inflict damage | • Certain actions might cause real damage |
| • High risk of potentially accessing data and destroying it | • Risk to change or destroy data is considered low |
| • Can quickly be recognized unlike threats | • Hard to easily detect |
| • Vulnerability management is not enough to block it | • It can be blocked using vulnerability management |

***Table 3.1.*** *Different Attacks and threats [97]*

### Vulnerability

For an attacker to gain access to a system, there must be a loophole, which can be described as vulnerability. In other words, it is a passage allowing attackers to get to their destination [100].

### Attacks

An attack is an unlawful act perpetrated by accessing a network to reach classified information or to cause defects for various purposes. It can occur through DDoS attacks, phishing, malware, node breaching, jamming, etc. The perpetrator can be someone from within the organization or an external person [101].

### Countermeasures

Countermeasures can be defined as several algorithms, security proceedings, security tools, and skills assembled to protect the system and sensitive data from attacks by some persons. Before carrying out any countermeasures, experts must have vivid knowledge by analyzing the attacks and the defense standard to be applied [102].

**Table 3.3** shows several types of threats identified in the area of security and privacy.

## 3.1.4 Similarities / Differences Between Security and Privacy

Fog paradigm and mobile Cloud are the major systems in privacy protection that studies are focused on. Thus, it has greatly gained research attention on protecting customers' privacy because of the cross-connectivity in the edge paradigm. **Table 3.3** shows some differences in security and privacy with a separate list of similarities.

| Security | Privacy |
|---|---|
| Man-in-the middle Attack | Data Privacy Leakage |
| Impersonation Attack | Identity Privacy Leakage |
| Denial-of-Service (DoS) Attack | Location Privacy Leakage |
| Collusion Attack | Usage Privacy Leakage |
| Jamming Attack | Other Information Leakage |
| Spam Attack | – |

***Table 3.2.*** *Forms of Security and Privacy issues [103]*

| Security | Privacy |
|---|---|
| Main challenge are attacks | Main challenge is Leakage |
| Concentrates on various collected information resources from companies | Concentrates on private information like account credentials, banking information, names, and social security digits |
| Offers protection to digital information and other data types | Offer protection to classified information belonging to users and institutions |
| Information resources display confidentiality, integrity, and availability designed by security principles | Individual's private information is preserved during processing |
| Refers to safeguarding information from attackers or intruders | Refers to the capability to safeguard private information |
| It can be attained in the absence of privacy | It is unattainable in the absence of security |

***Table 3.3.*** *Differences between Security and Privacy*

### Similarities

- Both security and privacy aim to provide QoS to individuals and organizations.
- Their main objective is the protection of sensitive information.
- Both implement restricted access of information to unauthorized persons.
- They both faces vulnerabilities and threats such as attacks and leakages.
- Both uses standard protocols to apply security and privacy countermeasures.
- They also involve legal regulations and government legislation

## 3.2 Cloud Computing Paradigm

For a brief revisiting on cloud computing, cloud service vendors have the capability to provision and provide their services worldwide and on request by granting access to systems of distributed computing resources [104]. Multi-tenancy, scalability, and flexibility are all been supported by this model. Based on cloud architecture, clients can gain cloud access from any corner of the globe with their supported gadgets [105]. Cloud computing has experienced exponential advancement over the years. The coming of cloud computing brought great advantages, especially in cost reduction in devices, enhanced cooperation, and more flexibility. Since the initial periods of cloud computing, many were reluctant to migrate to it due to issues relating to security. Many establishments dealing with very sensitive data never deemed it necessary or safe to move to the Cloud for fear of exposing their important information to an unauthorized individual or group of persons. Presently, many previous doubters have reluctantly embraced cloud computing because of its huge gains in using it. Despite the massive choices by organizations to migrate to the Cloud, the biggest concern remains that of security [106].

Information security and data privacy are the primary interest of every company and different firms using cloud computing services. It is of interest to these organs because storing their classified digital volume of data with a cloud provider is something to think twice [107]. The accepted system or model such as SaaS, PaaS, IaaS plays an important role since the information and usable applications for businesses can often be supervised and controlled via the cloud providers' infrastructure. Clients may void partial or absolute control. Wholly, a multi-tenant system, is mostly used in storing customers' information. Concerning this system, information security and data privacy raise more problems than the local computing setup. Since customers cannot observe and monitor their essential data on cloud-designed models, this creates a reduced sense of confidence. Security and privacy techniques utilize various approaches to understand its challenges in the view of cloud computing, and it differs from the existing study relating to modest computing systems [107, 108]. It is advised that institutions or companies such as big, medium, and small firms must set up certain cloud system specifics before moving to the Cloud. For this reason, it is so imperative to create modalities that do not solely see and analyze only the needs for security and privacy but do as well offers some level of guarantee that these needs should attain. Although local information technology-designed models have so far gotten this idea [109], however, services relating to the Cloud were not rendered proofs of a structure that meets that goal. Several research projects exist on security and privacy challenges, especially in trust, encryption, and control of access gain. However, most of these literature's are systematically organized [110, 111, 112]. Hence, it is important to systematically review the most present-day research outcomes obtained from different cloud computing companies to promote and protect the privacy of users [113].

It is seen that there exist weak scalability and a lack of functional protective framework in most of the available mechanisms used in protecting data privacy. On the whole, it is assumed that cloud computing's recent study area and its advancement are yet to accelerate, and there is the absence of an adequate research structure put in place. The massive hindrance here is gaining the most available security and data preservation during the updating of data dynamically [114, 115, 116].

### 3.2.1 Considerations For Security And Privacy in Cloud Paradigm

The majority of today's network and the idea of storing data is greatly inclined to technologies relating to cloud computing. One of the exceptional demands nowadays is for the Cloud to see that services are always made available consistently, reliability is upheld, and data is supplied. As earlier mentioned, one of the prime reasons organizations or individuals are reluctant to embrace the quick movement to the cloud model is the huge concern for information and privacy safety. Some acknowledged issues tying to security and privacy in cloud computing are confidentiality, data security, phishing, multi-tenancy, and others [117]. This section looks into the various threats aligned with security and privacy within the cloud computing system and suggests some modalities for threat mitigation at some point in this research work.

Cloud computing users adopt different distributed cloud models based on their specific needs, and because of this, the cloud security and privacy threats differ according to the infrastructure hosted in the Cloud. According to the Cloud Security Alliance (SCA), major regular threats are information leakages, Denial of Service (DoS) Attack, Advanced Persistent Threats (APT) Attack [118].

Adequate Cloud infrastructural security largely depends on the established protective technologies with many layers. This brings about the importance of adapting an Intrusion Detection System (IDS) specifically trace suspicious threats intelligently and potential attacks over a network. Furthermore, to carry out network status analysis in which the various events witnessed can be separated. Resources and services of Cloud CIA are said to encounter different types of threats originating from either insider or outside intruders [119].

### 3.2.2 Cloud Data Security

Data security is an essential aspect that plays a significant role in handling Cloud devices and keeps them running. This may involve protection and restoration guides for data and centers for Cloud services. Data involved in transmissions or transfers must always be protected. There is a huge problem the Cloud sector is encountering, which is that of cloud security. For this reason, there is a necessity for simple but robust mechanisms that offers a smooth method of learning about cloud service capabilities before deployment and those that align with Cloud security features during the establishing stage. The presence of Cloud service providers and Cloud customers also plays a role in the deployment plan since both parties must meet up certain data security requirements [120]. When a company happens to see potential expansion and is not capable of acting fast and professionally, issues like service level negotiation, information traffic, and most especially data security will arise [121]. It is important for Cloud service suppliers to properly protect data stored in the Cloud by customers to reduce or eliminates security shortcomings. Techniques used in encrypting data must be very strong to guarantee better data security and particularly implement authentication mechanisms that monitor other information access. Access control through data encryption should be established so that only the rightful selected employees can reach the data.

### 3.2.3 Cloud Data Privacy

The public Cloud faces more privacy threats, although these threats are very different based on their cloud model variants. Some of the concern of the danger here is a proliferation of information, malicious usage from an unauthorized person and incapability to control by clients [122]. Clients' sensitive documents stored in the Cloud can be reached by attackers using the file's hash codes, with the help of a mechanism used in duplicating information [123]. Based on [124], risks about privacy are regarded from several angles, such as access control, cloud systems, customers, and stored information. Knowing data privacy and other relating privacy principles will enormously assist in dealing with the known threat concerns. One vital setback holding some organizations to move to the Cloud is the fear of losing classified data through information leakage [125].

Most often, people's privacy is breach either knowingly or unknowingly. Accessing a person's private data without their knowledge or authorization is strongly considered invading one's privacy. Different trends can occur, such as open disclosure, privacy attack, data violation, and other means of attacks. Privacy leakage can be very damaging, but privacy issues can be better managed with the points mentioned below.

- **Trust**

  Disclosing data of individuals or organizations is considered a breach of privacy. Trust plays a very pivotal role in decreasing or eliminating fear [126]. There are various trust standards every customer can agree to, but in general, their concern is to see minimal or zero breaches of privacy at a reasonable scale [127].

- **Access Control**

  At times there could arise some confusion in terms of who, what, and when? We well know that cloud systems do present massive issues, such that an unauthorized person or group of individuals can get access if not properly addressed. An effective way of addressing this is by answering the above question [128]:

  **- Who**? The privileged persons to access certain data and who not to.

  **- What**? Some detailed data are not made accessible to every worker. So what specific files are permitted for who?

  **- When**? Some data are needed for a period of time, and that period must strictly be controlled when that information has been accessed. These can be made functional by establishing management policies, checks on multi-domain, and providing strong management keys.

- **Encryption**

  Encryption of data needs to be sufficiently strong to protect the privacy of client's files. Weak encryption of data poses a serious challenge to cloud privacy [128].

| Systems | Issues | Threats | CSA score |
|---|---|---|---|
| **Deployment** | Data residuals and information motility<br>Resource pooling and cloning<br>Multi-tenancy sharing<br>Data not encrypted<br>Authentication / Identity Management | Capability of cloud provider<br>Ensuring data processes on others | Not enough access control<br>Danger of malicious insiders |
| **Service** | Loss of data/leakage<br>Malicious Attacks<br>Man in the middle Attacks<br>Service hijacking<br>Virtualisation | Compliance in rules and regulations<br>Cloud security breach | Service denial<br>Misuse of cloud service |
| **Network** | Injection Attack on SQL<br>Browser security<br>Sniffer Attacks<br>DNS Attacks<br>Flooding Attacks<br>Partial deletion of data | Attack from some clients<br>Security failure from cloud provider | Vulnerabilities in sharing technology<br>Information loss/leakage |
| **Application** | Distributed denial of service(DDoS) Attacks<br>Hypervisor security worries<br>CAPTCHA breaking | Data confidentiality and protection<br>Issue in Availability and Reliability | Hijacking of service traffic or Account<br>Information breaches |

***Table 3.4.*** *Cloud systems with various challenges [129]*

## 3.3 Edge Computing Paradigm

This section will focus on the main aspects of Edge Computing since most of the details had been given previously in the Cloud Computing Security and Privacy section. Cloud Computing is the pioneering paradigm but later lost its status, which brought about the introduction of Edge Computing to continue the demanding activities of cloud Services. Two attempts will be approached to have a clear understanding of all these: Cloud paradigm drop and Edge paradigm shift later in this section.

### 3.3.1 Considerations For Security And Privacy in Edge Paradigm

- **Cloud Paradigm Limitations**

  From the inception of CC, data processing has to be one of the most advanced areas. Cloud servers are often centrally set up on a versatile range, and it also has to deal with a huge amount of data handling. Rendering cloud services on a global scale means covering very long distances, which means latency will affect the QoS and feedback time of clients' applications. Moreover, the growing use of enhanced technological devices highly impacts the duration of computation, insufficient analytical strength, and unlimited storage space. Due to the congested state of data over the Internet network, things became bad, and cloud computing drop could no longer support these ever-growing demands [130, 131].

- **Edge Paradigm Shift** Since Cloud computing performance dropped greatly, a significant paradigm shift to a higher version is EC. The rise in Edge Computing came about due to its new abilities such as scalability, response time, closeness to resources, reduced expenses to operate, and most importantly, security and privacy aspects. Edge Computing is observed as an innovation because it can carry applications with its new technological capabilities in shared computing while also performing information processing right at the point of need, without wanting the Cloud for data to be transported there. Users feel good when data are processed close to them, thereby improving their time to respond. This is made possible thanks to the computation that is directly carried out at the nodes of distributed equipment's [132].

5G network is here and strongly taking over many areas and operations of our daily activities [133, 134]. Edge computing is undeniably the pivot of all these changes. Edge Computing is a part of the 5G network, making it very vital in terms of driverless vehicles on how they interact with each other. Edge Computing shows a relationship with heterogeneous equipment and several networks that are cross-connected. The interconnectivity of these Edge supporting technologies exposes it to the most concerning aspect of any device, technology, network, and above all, organizations, which is safety. The threats involve here cannot be taken for granted, and this now led us to the subject matter, which is security and privacy in Edge Computing. With computation at the node of Edge devices, other security circumstances will show up and still requires continuous research work for improvements [135].

The arrival of Edge computing does not necessarily imply that cloud computing is not in service anymore. Businesses, applications, and networks are seen to have a greater boost when Edge and Cloud computing function in alliance to support each other in an

| | **Cloud Computing (CC)** | **Edge Computing (EC)** |
|---|---|---|
| Application State | Worldwide | Regional |
| Pressure on Network bandwidth | Huge | Reduced |
| Mode of operation | Processing is centralised in big scale | Little scale intelligent analysis |
| Response-time | Slow | Fast |

***Table 3.5.*** *Basic difference between Cloud and Edge Paradigm [136]*

advance and organized manner. Any substantial analytical result from extensive analysis from the Edge node still needs cloud computing for a better-summarized analysis. Therefore, the improvement of intelligent IoT pieces of equipment still largely depends on cloud computing that continues to perform a vital role [136].

Data security and privacy protection in Edge Computing attract much research interest. Data from the Edge Computing network private and sensitive information that requires absolute data privacy protection. The chances for imminent threats and attacks are very likely because of the distributed design of the Edge computing system, even though the processing of information at the nodes offers some security and privacy protection. The presence of Edge Computing smart devices also exposes vulnerabilities such as security issues and dangerous malware. The structure of Edge Computing cannot adequately support the mechanisms for securing and protecting information. This, therefore, implies that the complexity of this edge node at the network leaves the data very expose and hard to secure. There are four identified existing setbacks witnessed in Edge Computing paradigm [136].

Despite the growing nature of Edge Computing technologies, its security and privacy development remain a continuous process and tells why there exist not so many research findings. Researchers and other academicians globally have been putting every effort in performing relevant research work to develop countermeasures to better the security and privacy of Edge systems. Different simple mobile Edge Computing was used for carrying out security checks, presentation of an overall security and protection scheme with proposals from the research work done. The Edge security findings do present a relevant citation from a theoretical approach. As mentioned previously, the existing known issues in this thesis work relating to Edge computing information security and privacy are partitioned in four separate parts and any order [137]; Access Control, Identity Authentication, Information Security and Privacy Protection. Based on the focused theme of this thesis work, "Security and Privacy Aspects," we are going to maintain the focus area. That been said, we shall be looking more into only Information security and data protection.

### 3.3.2 Edge Data Security

Information Integrity, confidentiality, and attack detection are the common goal and reasons for data security. It helps in designing an edge-computing system that is secured. Issues such as information breach and information loss are resolved by outsourcing information under control, non-fixed storage, and sharing responsibility. Data duties are allowed to be carried out securely by customers. We can rarely find research works on Edge Computing security and privacy since many academicians do mostly focus on cloud paradigms [138], or perhaps fog paradigm [139]. The major aim of information security in Edge systems is to securely move data and ease the heavy load by creating a shared model with a great smooth system. As a result, very acceptable shared information security and lightweight designs are realized.

A key responsibility in safeguarding customer's secrets and upholding the confidence involved, especially at the edge network, should be rendered. An example is a digitalized house constructed with many IoT devices, which can be a prime target due to its huge quantity of personal data produced. Here, the biggest challenge is making sure customers' data are very safe. Before computation at the cloud server, a suggestion is first to take away any sensitive information. Therefore, a more regarded approach to protect the privacy of customers and gaining their confidence is to make sure that data processing occurs at the Edge network or node of the house [140].

- **Confidentiality**

  The confidentiality of data is an important factor in Edge computing [141]. In the case of mobile clients intending to use the services of mobile applications, confidentiality is always taken seriously, and for this reason, some clients find it difficult to decide whether to use it. In [142], some shortcomings relating to Edge computing confidentiality were presented. Also, there is a very high risk posed by the providers of services gaining unpermitted passage to classified information. This is seen to possibly occur during transmission of data in a distributed or unsecured network which is later stored and processed in the Edge distributed network. Data security has constantly been breached and violated very often, and resolving this issue, is a big plus for confidentiality since it is a challenging aspect [99]. Good enough, restricting access today to project confidentiality is achievable due to some newly created mechanisms [143].

- **Detecting Attacks**

  Edge systems can operate smoothly with the assistance of edge nodes where the edge applications are located to offer maximum standard services. This is done to make sure that the entire edge system is free from abnormalities or threats. The edge node consists of a considerable harsh surrounding with an inadequate security guarantee, making the edge nodes exposed to threats. The performance of an edge system can massively be hindered when the threats from one edge node are mismanaged and might subsequently extend to another edge node. Thus, finding a quick solution can be hard because of the weight of the threat that spreads across the edge nodes. Also, added costs would be incurred to find the baseline reason for the problem, and even recovery might take a while [144]. Therefore, regular checks must be performed to detect any previous potential or imminent attacks.

- **Integrity**

  The integrity of information is considered vulnerable during the transmission process, making it a matter of concern regarding security in Edge Computing. Customer information can easily be breached cause of outsourcing data to the Edge computing servers. To avoid any unwanted access to these data and possibly alter information, service providers execute the availability and integrity required to check. The systems can also undergo these checks to ensure data integrity [99].

### 3.3.3 Edge Data Privacy

In Edge Computing, accessing the system does not reflect trust. Averagely accepted systems are used to store customers' important data, resulting in some critical privacy leakage. Some clients' data stored are personal information, location data, and data identity. The focus areas to be discussed herein any order includes privacy, identity, and location privacy safeguarding [136].

Edge computing always raises so much concern in stark contrast to other existing computing models regarding protecting information. This is because the challenges such as leakages relating to Edge data privacy are daunting. An Edge information center, services, infrastructure suppliers, and even certain clients make them the potential weak link or at least establishments you cannot fully trust with such interwoven computing networks. In regards to this, the act of keeping safe the private information of clients is an obligation that requires very close attention [99].

- **Data Privacy**

  At the nodes of Edge systems, huge data of clients are retrieved from applications and other users' pieces of equipment. This collected information is then processed and analyzed. Despite the trustworthiness of the edge computing nodes, they can still display some level of vulnerability. Classified information such as medical data of an individual must be top secrecy. Therefore, information privacy protection is very important to avoid leakage at the nodes of Edge Computing [145].

- **Identity Privacy**

Compared to other cloud systems, especially mobile Cloud, Edge models still lack adequate research attention in protecting the identity of customers well. Identity privacy protection is a major concern for several organizations and even individual customers. The third-party identity-designed model is said to still pose vulnerability [146].

- **Location Privacy**

  Several software and services from Worldwide Web are available that render functional capabilities based on location. For a client to gain access when they want to use the services in Edge computing, that client must surrender their location as required by the service supplier. One of the particularly concerning fear is that of breaching data location through possible leaks. Different researchers gave some solution schemes on how to deal with issues on data leakage. A dynamic distribution in location privacy protection was presented in a mobile model of social internet platforms. This model can sort out visitors with low trust levels within a certain range of social interactions. It performs this by dividing customers' data location(unidentifiable) and personalities in individual storage systems. This separation enables the service provider to hide the data about customers' location safely. The importance of this model is that, even if an attacker manages to breach one of the storage facilities, for example, data location, it will not pose a major threat since the identity of the client is not leaked or exposed [147].

## 3.4 Fog Computing Paradigm

Many businesses have transformed massively, especially with the fast growth in large data usage, due to the presence of cloud computing [148]. Meanwhile, the quest for private services also began to grow hugely. A great amount of well-centralized systems is offered by cloud computing platform [149, 150], although with some shortcomings. Clouds and their endpoints show certain unwanted long and irregular delays and time-conscious services to some [151]. There is a pertinent high risk in a situation whereby there is a breakdown in the information building and between network interconnected systems. One potential breach here is possible privacy exposure. To mitigate this challenge, the Fog computing [152] model was introduced, and it assisted Cloud-Edge in improving computation, security, and privacy, which is now the leading and most recommended computing service.

Fog computing system utilizes Edge devices which vary from Cloud computing model. The devices are considered local pieces of equipment ranging from gateways, routers, switches, and others or professional installation of traditional servers [153]. Furthermore, with the recent cry for huge emission reduction, Fog computing is highly viewed as a smart green platform with sustainability and great security benefits. A good amount of fog nodes seen as renewable constitute the Fog computing system. The geographical placing of these Fog nodes (FN) can be spread throughout several locations. A great level of pressure exerted in the information center during computation is vastly decreased due to the different Fog nodes working independently but together in harmony through a well-calculated formula. Fog can separate or sifter client's messages at the central layer found at the middle of the endpoint and cloud [154]. Messages deemed essential by Fog are then transmitted, thereby lightening the burden on the information center. With this strategy on a division of work, it significantly enhances the quality and brings down expenses [155].

There are many studies done within the sphere of Cloud security and data privacy [156]. In great demand to deal with the ever-growing IoT issues, Fog computing was highly considered, as we shall see in the next sub-heading.

### 3.4.1 Considerations For Security And Privacy in Fog Paradigm

Fog computing was established as the most viable approach because of its ability to cross-connect every digital equipment, wireless endpoints, and home device. This interconnectivity does pose vital security and privacy violations such as disclosing clients' data location, leaking classified documents, and stealing private accounts. First considered by Cisco, Fog computing was brought to expand the cloud activities to the system's Edge. The consideration of Fog computing surfaces as an option to local Cloud offering huge assistance in terms of QoS, latency, and location distribution [157]. Services such as networking, storage, and most importantly, computing between the customer and information center are rendered by Fog computing hugely considered a virtualized system [158].

Edge and Fog computing are terminologies frequently mentioned within the facet of scholars and Companies. Regarding intelligence, computing capability, and data processing, Edge and Fog paradigms have differences despite their viewed similarity. Computation amenities are transferred towards sources holding the information, which is the major Edge computing goal [159]. Examples of these sources are wireless pieces of equipment, actuators, and sensors. According to the Edge system, every single unit in the Edge computing functions independently to see that information is not forwarded to the Cloud. Instead, it is locally handled. On the other hand, transferring to Cloud or processing the data from various information origins is always a decision made by Fog computing nodes, taking into account its assets. Fog computing can expand some Cloud services that are not assisted in Edge structure, such as IaaS, SaaS, and PaaS. Edge computing is completely Edge inclined but can be supported by Fog computing while at the Edge of the network, expansion of communication assets and computation are performed [160].

### 3.4.2 Fog Data Security

Issues arising from network systems are imminent, and vital data security measures should be put in place while establishing a fog infrastructure. Some attacks usually threaten private and government entities since they function in Cloud, Edge, and Fog computing. To offer a level of protection to the structure, a TIP is important to be developed [161]. Data security is the most prioritized aspect in the industrial sector, especially as information must be safeguarded. Intelligent equipment and sensor devices are deployed to reduce threats and security attacks extensively. The feature about heterogeneity and geographical sharing impacts the implementation of cloud security frameworks into Fog computing systems [162]. Some of the considered security challenges are confidentiality, authentication, availability, and information privacy. These mentioned frameworks assist in creating and monitoring accesses to persons and organizations.

Considering the medical field, we see that patients' health history involves classified information and the Fog architecture has several nodes that might present some vulnerabilities. These vulnerabilities can be unpermitted access to information when stored or at the time of transfer, untrustworthy insiders, and during system distribution of information. Fog system by means of cable or wireless network consistently receives information transferred from sensors of medical devices. Tampering with patients' personal data, integrity, and device availability is obvious and can occur when communication systems and sensors are targeted. Some through channels as DoS can easily be perpetrated with ease due to the vulnerabilities found in wireless networks. On the other hand, the absence of proper frameworks to control access to the Fog nodes that process important information can compromise information through leakage because of account theft, unpermitted access, and possibly some unsafe passage. The mentioned problems can be mitigated through thorough analysis and stringent rules and regulations to establish standard control mechanisms such as personal systems, selective (limited) encryption, and reciprocated authentication [163].

### 3.4.3 Fog Data Privacy

Protecting the privacy of individuals and enterprises is often a primary concern encountered by the Fog paradigm, especially with the Fog nodes positioned near the individuals and facilitates the gathering of vital information sometimes relating to geographical location, identity, social security numbers, and many. One great challenge is that it is quite hard to keep centralized monitoring due to the distributed nature of Fog nodes. During transmission, attackers can easily gain access to steal essential information when the Fog nodes are not well secured. More practical studies are needed to understand privacy problems better and innovate current solutions to preserve data privacy [164]. Privacy leakage often happens, even though end-users are never in accordance to release their personal information. There are some main areas of clients' privacy: data privacy, location privacy, identity privacy, and usage privacy [165].

## 3.5 Conclusion

In **chapter 3**, we performed an in-depth analysis of security and privacy for Cloud, Edge, and Fog paradigms. We looked at some of the related terms on security and privacy while defining them for example, vulnerability, threat, attacks, and countermeasures. The key challenges on security and privacy witnessed by these paradigms are security attacks and privacy leakage. While analysing data security and privacy for each of these mentioned paradigms, several differences and similarities were derived at in **chapter 2**, which presented reasons for each paradigm's considerations based on their benefits. Some issues encountered by Cloud, Edge, and Fog paradigms in regard to data security and privacy, shall be dwell on in **chapter 4**. Importantly, some attacks and their corresponding countermeasures are presented as well.

# 4 SECURITY AND PRIVACY ISSUES - SUGGESTED SOLUTIONS

## 4.1 Information Security And Privacy Challenges

### 4.1.1 Cloud Paradigm Challenges

Data loss, privacy leakage, multi-tenancy, unpermitted access to management platforms, Internet protocol, injection attacks are some of the main challenges faced in cloud computing [166, 167]. Such challenges turn to make room for potential attacks, letting access control to cybercriminals, granting access to unauthorized services, thereby disclosing several classified data, if not all.

Cloud computing faces enormous threats when involved with these vulnerabilities and thus affects business too, either directly or indirectly. One of the most reliable ways to repel threats and attacks is to identify any one of them found and analyze the behavior to have a proper understanding. This section explains the different cloud computing issues [168].

**Multi-tenancy**

Multi-tenancy is used in providing services to different customers and organizations with a particular software operating on the SaaS provider's servers within the architectural design. Every user company can utilize an application that is virtually designed in dividing data and configuring it virtually with the help of specially designed software. In this SaaS model, there is a high risk of vulnerability because clients turn to work with applications of multi-tenancy manufactured by CSP. The maximum security of customer's data is the direct responsibility of the cloud provider since sensitive information such as financial and individual data are hosted in their cloud system [107].

Managing resources and scheduling work are some methods used by cloud providers [169], but hardware potential is fully attained through virtualization by cloud providers. Sandboxed setups refer to Virtual Machines (VM), which means they are completely separate from one another. Hardware sharing with my clients is considered safe according to this mindset. On the other hand, cybercriminals (hackers) can gain access to the host when the sandboxed system is having security setbacks [170]. The virtualization software is strongly recommended since it is capable of showing recent vulnerabilities in cloud security, such as retrieving data by targeting a VM on one machine through attacks through cross-Virtual Machine side channel [171].

#### Integrity of Data

Security attention is greatly put on data integrity in the Cloud, which means any reply to a data request sent must be from someone with an access privilege. Establishing a general basic data integrity standard is important, though it is not still in place [172]. Trust is one of those many values that clients are expected to demonstrate in the computing facet. Today, a lot of firms or institutions encounter the issue of trust, and this hugely impacts the handling of their data [173].

#### Unauthorised Access

One of the most vulnerable aspects of cloud computing is getting unauthorized access to management platforms and resources. Users are so much exposed to this due to the shared technologies often involved in cloud services. An acceptable way of mitigating the security solution of such a scenario is by introducing access control. This helps in securing the client's personal information and its domain for privacy [174]. It is worth noting that cybercriminals can simply have unauthorized access to cloud service systems because of a single-style authentication model and also not very strong authentication mechanisms been used [97].

#### Data loss and Leakage

The low cost of cloud services is one reason customers turn to migrate to the Cloud, and it is warned that customers should pay attention to their important information since various multifarious aspects can easily breach the security of their data. There is an increased chance of data leakage or loss due to high traffic and usage of the Cloud. The vulnerabilities and threats in cloud service are undeniable, posing a great security threat to businesses and institutions. Significantly, it can be frustrating when you cannot retrieve and restore data after accidentally deleting files from the Cloud due to a lack of a backup system [97].

#### Malicious Insider

Every organization has different rules and regulations regarding recruitment policies and information available to employees. However, some employees have higher status, which guarantees them the privilege of accessing certain essential data within the company. Based on CSA, they proposed the implementation of transparency in the general data security and management activities standard, outlining notification procedures during security failures, while using Service Level Agreement (SLA) as a demand for human resource, and finally establishing and exercising strict rules in the management of supply chain [97].

In [175], it is far easier for a person with malicious ideas to work for a CSP since no one is seen as a suspect. This individual can quickly be involved in malicious events, especially if they have unhindered access to sensitive information, especially if the CSP cannot strictly monitor its workers.

### Identity Theft

Victims or organizations can suffer heavy impact due to weak passwords due to phishing attacks by some attackers who turn to disguise as authentic persons to steal the different important data of their victims. The sole reason for identity theft is to gain access to sensitive digital resources of individuals and companies by any malicious means. Every protected communication within the cloud system happens with access control, and this is made possible by using an encryption key [176].

### Man-in-the Middle Attack

During the flow of data from one end to another or between different systems, cybercriminals can easily take advantage and gain access, thereby having control of classified data. This can easily occur when the Secure Socket Layer (SSL) is insecure due to inadequate configuration. Specifically, in cloud systems, hackers can attack the communication within the information centers. Efficient SSL configuration and data analysis among accepted entities can go a long way to significantly lower the threat pose by middle man attacker [177].

### Denial of Service (DoS) Attack

DoS attacks targets such as institutions and various companies by limiting or stopping them from accessing needed data. This creates a scenario where actual users partially or lack service availability. Whenever the right persons using the cloud services try to reach the data server to access information, access is denied. This happens because the attacker uses a method in which he constantly congests the server of a precise resource through request flooding, and the targeted server will then be unable to reply to a legitimate access request. There exist several ways this attack can be performed, for example, by way of SQL injection attack, bandwidth wastage, and also by way of incorrectly using model resources [178].

During a DoS attack, several individual machines or sources are responsible for the heavy flooding demands. Attempting to restrict or counteract a particular intruder is impossible to halt the entire attack scenario. This action presents a complex view whereby it is very difficult to differentiate between malicious traffic and valid traffic. The primary aim here for the attacker is to send wrong requests to the destination devices to stop the activities of their resources. This is usually carried out by overloading the machine with more packet size than the recommended size of a message in an IPv4 network [179].

#### Phishing Attack

This is one of the most common attacks in which the criminal turns to impersonate and deceive their victims by leading them to fake or malicious links. The presence of the Cloud makes it flexible for hackers also to hide their cloud hosting of numerous accounts of different clients that uses cloud services utilizing phishing activities. There are two kinds of threat divisions in which phishing can be grouped. Primary, Irresponsible attitude whereby a cyber-criminal can also make full use of cloud services to host a site for a phishing attack simply. Secondary, Cloud computing services and their many accounts can be hijack [180].

### 4.1.2 Edge Paradigm Challenges

The Edge paradigm is considered to offer huge benefits to edge customers such as storage, data processing, just to name a few. However, despite these many gains, unlike the Cloud paradigm, Edge computing is still faced with big security and privacy challenges, which we are going to explore in this segment below.

#### Data Injection

When a machine is vulnerable, an attacker can push harmful information into it to share negative information. The act of injecting dangerous data by a malicious attacker into a device is known as poisoning. Data can be faked, then used to create fraudulent messages to render the nodes of the target compromised, and it is called an external forgery, for example, in a modern digital industrial production line where the adversary happens to give false machine readings, thereby causing severe functional changes with the bad aim to harm the devices [135].

#### Eavesdropping

In this scenario, an attacker can mask itself and secondarily observes network traffic during transmission and capture data illegally. It is quite hard to point out this type of attack because the attacker happens to hide inside the platform [181].

### Privacy Leakage

The absence of strict access control to the node of Edge can easily lead to data privacy being tempered with. However, the attack strength is very little. The information generated from devices situated at Edge proximity is stored and processed in the Edge data building. Customers classified these Edge data buildings can leak information since the content is known [182].

### Distributed Denial of Service (DDoS)

The Edge paradigm suffers immensely from DDoS attacks. Attackers usually take advantage of network protocol vulnerabilities to launch attacks on Edge nodes, causing network damage and restricting resource access and provision of services. Attackers carry out these attacks by loading the server with a huge amount of data packets to shut down the channel by jamming the server's bandwidth. Another option is where the Cloud data server or the Edge systems are being flooded with data packets to massively take out resources [135].

### Permission and Access Control

Unauthorized access is a major challenge as well in the Edge paradigm. It is important to know an individual or employee before authorizing them to access any sensitive information in the system. It can be achieved by establishing access control protocols. Connectivity between several pieces of equipment and other services can be considered secured when access control measures and permission are implemented [183].

## 4.1.3 Fog Paradigm Challenges

Cloud paradigm has countermeasures for its security and privacy threats. Notwithstanding, these countermeasures may not apply to the Fog paradigm due to the active presence at the network edge of Fog entities. The immediate vicinity where Fog entities operate will confront various threats which may not constitute a good functioning Cloud. The security solutions in the Fog paradigm are improving and increasing well. However, most of the published literature on Fog computing security and privacy does not provide insights with an extensive assessment of the various issues. Importantly, we deliberate on some security and privacy challenges encountered in the Fog paradigm.

### Trust Issue

Looking into cloud systems and Fog systems, it is a bit different when analyzing the aspect of trust. Fog systems face trust design challenges due to the reciprocal demand for trust and the distributed nature of their network. Cloud computing platforms are different since it already consists of pre-designed security models that match the industrial security requirements granting customers and enterprises some measurement of trust within the cloud system. However, this is not so with Fog computing networks which are more exposed and liable to security and privacy attacks. Even though the same security mechanism can be deployed to every Fog node that makes up the Fog computing network, the distributed design also makes it quite challenging to resolve the trust problem [184].

#### Malware Attacks

Infecting the Fog computing system with a malware attack is regarded as a very high-level challenge in the network. It is carried out to steal sensitive data, breach confidential information, and can even go further to refuse service with the help of a virus, spyware, Trojan horse, or Ransomware. To assist Fog computing applications in mitigating these malicious attacks, authentic defense mechanisms for virus or worm detection and advanced anti-malware must be introduced [185].

#### Computation – Data Processing

Fog nodes often receive data collected from end-user equipment, processed, sent to the Cloud system, or end-user pieces of equipment get forwarded information transmitted from the Cloud. After the various processes, the data sent from end-users to Cloud systems and the data sent from Fog nodes to Cloud are different in size and nature. Another challenge here is that several providers have these Fog nodes making it hard to be trusted due to the many security and privacy shortcomings arising after processing of data [186].

#### Node Attack

Here, the attacker engages physically by targeting to capture the vulnerable nodes. There are moments where the attacker can decide to alter the whole node, cause defects on the hardware, or steal sensitive information from the Fog nodes by digitally sending messages and also causing sensor nodes distortion of classified data. Such attacks can have damaging effects on the nodes of the Fog network, and observing these node sensors will help identify issues and deploys some node capturing defense of algorithmic cryptography [185].

#### Man in the Middle Attack

In this situation, the attacker takes charge of a vulnerable node during data transmission between separate Fog nodes. The hostile equipment performs at the center of the nodes through eavesdropping, thereby extracting data stored and forward it during communication from the two authentic types of equipment. The two pieces of equipment cannot notice the presence of an eavesdropper and therefore determine that only two of them are connected and communicating. The severity of this attack is that it can potentially violate confidentiality, creates a loss of integrity, and unauthorized privacy access in Fog networks [185].

### Privacy Preservation

There is a huge concern as customers using CSP, the IoT, and wireless systems face data leaks of personal information. It is not easy to preserve this privacy in the Fog network due to the closeness of Fog nodes to the customers' environment. It can also facilitate gathering plenty of vital information such as identity, location, and utility usages. Privacy leakage can also occur when communication between Fog nodes becomes more frequent [165].

## 4.2 Suggested Solutions For Security and Privacy

### 4.2.1 Cloud Solutions

Cloud computing consists of several factors and thus brings about the importance of security in its various architectures. The differences in cloud systems mean different security and privacy attention to be applied. Here, we attempted some of the countermeasures in regards to cloud infrastructures as shown below [187].

**Security from Services**

- Making sure the network is well segmented
- Regular network monitoring
- Make use of firewalls
- Request must be established before authorization is granted.
- An added Operating System acting layer such as TCB can be introduced. It collects files in a secured manner.
- Policies for access control should be encapsulated
- Proper security for emails against malware and spams
- Provision for data backup should the system break down.
- Data encryption for customers.
- Amenities for data recovery.

### 4.2.2 Edge Solutions

Despite the plenty of advantages presented by Edge computing, the security and privacy aspect has always been of much concern. Based on the challenges exhibited, some countermeasures were proposed, such as blockchain. Other solutions are listed below [188].

- Data must be encrypted appropriately and with strong authentication to grant access.
- Decoy scheme for customer profiling, also known as User Behaviour Profiling (UBP). The overall attitude of the customer is closely watched.
- Network security standards should be the same with every Edge computing node.

- Use a specialized monitor to observe hardware performance with algorithms of lightweight cryptography.
- The constant use of detection means, such as IDS. This assists in drawing the attention of a user whenever an intruder is detected.
- An interactive platform should be developed where customers can keep track and see all activities.

### 4.2.3 Fog Solutions

Some suggested countermeasures to Fog computing [163].

- Trusted Platform Module (TRM): In this scenario, the Cloud and Edge share an extra main key, but the Cloud is given access only to information which the key is used in encryption.
- Modified decoy technique (MDT): It is a scheme where attackers are rendered with duplicated data and masked nodes which are not real. It is done by redesigning the decoy technique from its original form. As the attackers gain access to these false data, their identity details are exposed and retrieved, such as their Mac address.
- Data encryption.
- Monitoring of network through the use of Virtual Machine (VM).
- Use of Decoy technique relating to UBP.

## 4.3 Attacks and Countermeasures

In subsection 3.1.3, we briefly explained attacks and countermeasures in order to aid our understanding when dealing with this topic. We must know that vulnerabilities, threats, or security attacks can appear differently, and there exists no specific way of solving the various security issues. Thus, to safeguard whether a Cloud, Edge, or Fog computing system, several designed models must be considered. This will help create a joint force of many reliable layer defense models [96].

### 4.3.1 Security and Privacy Attack Comparisons in Cloud, Edge and Fog paradigms

**Table 4.1** presents a detailed comparison of Cloud, Edge, and Fog paradigms based on a designated OSI model layer. The table contains layers such as application, virtualization, transport, network, and abstraction layer which consist of the physical and MAC layers. Each of these layers are given brief descriptions on the role they play in the OSI model. Different attack examples were found that are common to the three involved paradigms, associated to the various layers. Each of these identified security attacks and privacy leakages are matched to a specific proposed countermeasure. In some situations, same countermeasure of a particular paradigm can be applicable to the other. However, due to the complexity of these paradigms or their ecosystem, this deployment of a single countermeasure is challenging.

As of now, end-devices don't involve any established security measures. For this reason, during data transmission security vulnerabilities are likely present. There is some vulnerability research underway to get an understanding on difference ways an end-device or layer can face attack. It is of significance that vulnerability research projects must be done extensively and in in-depth when studying attacks and its aspects [189]. At each layer, we can deduce that security vulnerabilities are safeguarded differently. This definitely attains the basic security demands like, confidentiality, authenticity, integrity and not the least, availability. In stopping leakages on data to illegitimate persons, cryptography is suggested for data confidentiality. Although cryptography turns to offer better data confidentiality, it does need additional computation power, thereby causing latency. Users and End-devices have a close proximity to each other. Fog nodes are known to poses some level of reach to data of individuals and especially the location where the data is generated. Data processed in Fog nodes are very significant security wise, due to its sensitivity more than data in Cloud servers being processed, and requires enhanced protection.

| Layer | Brief description | Attack Examples | Specifics of paradigm/main proposed countermeasures | | |
|---|---|---|---|---|---|
| | | | Cloud | Edge | Fog |
| Application | Data inclined applications faces attacks and if breached, unpermitted access on websites is reached. Malwares are of different forms e.g., Trojan horse and virus. An illegal software used to access legitimate information. Attacks HTTP [190]. | HTTP Flood | Application monitoring is highly recommended. Web Application Firewalls (WAF), Antivirus, privacy protection management [191] | Filtering mechanisms and intrusion detection systems [46] | HTTP-Redirect scheme [192] |
| | | SQL Injection | SQL injection detection using adaptive deep learning [193] | Modifying circuits thereby "minimizing information leakage, by intentionally adding random noise or delay to the data, implementing a constant execution path code and balancing Hamming weights" [194] | ,SQL injection detection utilizing Elastic-pooling [195] |
| | | Malwares | Use of Antivirus Softwares [191] | Signature-based and behaviour-based detection [196] | Mirai botnet detector [192] |
| Virtualization | "It is defined as a pool of virtualized computer resources". Virtualisation offers better usage of hardware assets with an the opportunity for additional services avoiding extra costs for infrastructures. Customers are provided with virtual storage [197] | Hypervisor | Strong configurations, Always update host operating system (OS) | Computational Auditing | Robust Authentication scheme |
| | | Data leakage | Encrypt stored data/use secured transmission medium e.g SSL/TLS, Virtual Firewall [198] | Homomorphic Encryption [199] | Isolation of user's data, Access control strictly based on positions [185]. |
| | | VM-Based | Anti-viruses, anti-spyware to monitor illegal events in guest Operating System (OS) [200] | Identity and Authentication scheme such as Identity-Based Encryption (IBE) [199] | Intrusion detection and prevention mechanism use for anomaly detection, behavioural assessment and machine learning approach in classifying attacks [192] |
| Transport | "Provides a total end-to-end solution for reliable communications". The two main protocols are TCP and UDP. The smooth performance in communication strongly depends on TCP/IP between user and server [201]. | TCP Flood | Firewalls, SYN Cache [202] | SYN cookies [203] | Firewalls [204] |
| | | UDP Flood | Graphene design for secure communication [205] | Response rate for UDP packets should be reduced [204] | Response rate for UDP packets same as in Edge, should be reduced [204] |
| | | Session hijacking | AES-GCM symmetric encryption [205] | User light-weight authentication algorithm [203] | Encrypting communication using two-ways/multi-purpose authentication [163] |
| Network | The routing of data packets across different networks from a source to an end node, is performed by the network layer [206]. | DoS attack | Intrusion Detection System (IDS) [207], Access Security | Network Authentication mechanisms | Deploy routing security and observing the behaviour of nodes [208] |
| | | MITM | Data Encryption [191] | Time stamps/Encryption Algorithm [194] | Use of Authentication schemes [185] |
| | | Spoofing attacks | Identity Authentication [191] | Secure trust schemes [74] | Secured identification and Strong authentication [74] |
| PHY/MAC | The physical layer simply depicts the manner how equipments are physically hooked up to a cabled or cableless network system and are able to be sorted for physical addressing with the help of a designated MAC address. [209] | Eavesdropping | Encryption, Cryptography [210] | Data Encryption using asymmetric AES scheme [211] | Protection of identity by use of Identity Based Cryptography (IBC) [212] |
| | | Tampering | Detection of behavioural pattern | Observe manner of behaviour [210] | Multicast authentication as a Public Key Infrastructure (PKI) [213] |
| | | Replay attack | Dynamic identity-based authentication model [214] | Authentication mechanisms [215] | Key generation approach [215] |

***Table 4.1.*** *Attack specifics of paradigms and suggested countermeasures*

## 4.4 Conclusion

This chapter has executed detailed security and privacy analysis of Cloud, Edge, and Fog paradigms. We also looked into the different reasons why these paradigms were considered while analyzing their challenges as well. Importantly, some attacks faced by each paradigm were also observed, and to establish an adequate defense mechanism against these attacks, it is imperative to set up specific security corresponding countermeasures for each attack. Beware that certain system demands and limitations should be considered when deploying security mechanisms to counter attacks.

Cloud, Edge, and Fog paradigms consists of applications, resources, and massive quantity of End-devices within a given centralized or decentralized area, existing together and inter-communicating. Therefore, the huge potential for vulnerabilities in security and privacy does exist. One good way of screening systems for possible vulnerabilities is by auditing security standards.

Vulnerabilities in any system, might expressly grant attackers partial or full access to cause severe harm. If a data is breached, it can expose critical information of individuals or organizations. An attack can cause serious malfunctioning of an entire network and creates disruptions. We found that, be it threats, attacks, or vulnerabilities of the examined paradigms whether joint and/or apart, the main target is to gain access to sensitive data. Importantly, we also found that, each of these vulnerabilities can be properly discovered with the right tools and approaches. Despite the persistent search for vulnerabilities in systems by attackers (hackers/cybercriminals), there are up-to-date sophisticated countermeasures to mitigate such threats, be it from within or external. Most essentially, each vulnerability has a specific mechanism to counter its threats and attacks. Besides, another important aspect found is that, the vulnerabilities turns to undermine the security and privacy of the related paradigms,thereby exposing them (data) to potential security attacks and privacy leakages.

Next, in **chapter 5**, we shall be discussing the shortcomings, conclusions and future research pathways of this research work.

# 5 DISCUSSION

## 5.1 Shortcomings

Based on this systematic literature review, included evidence display Search Strategy as a challenging area. Another difficult area in this SLR is data extraction involving inclusion and exclusion aspects, with difficulties figuring out important synonyms and secondary words. Another issue encountered was keeping and handling the acquired outcomes properly at the search level. The exportation of references by databases has various supported styles, as well as some to be exported are not supported. Dealing with a massive number of saved acquired evidence manually is tiring and time-consuming. It will greatly assist researchers when several databases can be made available with a simple search platform that also organizes citations. Modern and substantial tools are needed to generalize systematic literature review data adequately. The research was furthered by conducting an alternative search by closely analyzing included sources to widen the search scheme. A comprehensive review is executed once the data extraction from sub-searches is done. It is worth noting that some papers were limited in precise information on results and models. We often noticed that models or methods did not have sufficient explanation. These pose a challenge in sorting out some of the papers' research models, especially in retrieving information in the desired way.

## 5.2 Conclusions and Future Research Pathways

The essential aim of this thesis was to execute a comprehensive article review on Cloud, Edge, and Fog paradigms, respectively, with a special focus on identifying similarities, differences, attacks, and countermeasures based on security and privacy aspects.

One big challenge in most SLR is gathering every single paper relating to the field of work, but desirably representing these papers is far more vital than showcasing a huge amount of documents. We developed search queries in a methodological pattern to obtain a good review, and several databases were queried for studies. A possible 447 important papers were gotten from the start search queries and were slashed down to 77 selected papers employing a Systematic scheme consisting of various stages. For the sole goal of this work, different papers were read extensively and critically analyzed. We moved further to deliberate the existing security and privacy challenges, vulnerabilities, threats, attacks, and some specifics of the main suggested countermeasures.

In terms of thesis structuring, **Chapter 1**, introduces the approach methodology, while **Chapter 2**, gave an overview of Cloud, Edge, and Fog paradigms, focusing on their different architecture, network, processing, and storage capabilities. **Chapter 3**, made a detailed analysis of the three mentioned paradigms based on their security and privacy aspects. **Chapter 4**, presented a more extensive review on security and privacy issues, with suggested solutions. **Table 4.1** shows several attacks with proposed countermeasures of Cloud, Edge, and Fog paradigms. According to the Open System Interconnection(OSI) model, the attacks were classified based on layers, briefly describing each of these layers involved.

Cloud, Edge, and Fog paradigms create a substantial heterogeneous quantity of data capable of being managed on a centralized or distributed system. Looking at the discussions presented in this work, we deduced that the security and privacy issues on the heterogeneity of this ecosystem are a significant challenge. Data transfer from one end to another creates many security and privacy vulnerabilities, even though some of these weaknesses can be detected quickly. Solutions can not be swiftly deployed to user devices simply because of the complexity of the ecosystem. However, IDS mechanisms are largely significant for different paradigms, as some are considered effective in countering DoS/DDoS attacks (Zero-day-attack). In certain scenarios, gateway devices are introduced to provide higher processing power if needed by IDS mechanisms.

Security and privacy are considered primary drawbacks, limiting several institutions and organizations to adopt Cloud technology. These paradigms face different security and privacy threats, but the most outstanding are DoS/DDoS attacks, as mentioned earlier. For instance, Cloud customers can suffer heavily if Cloud services and resources are breached for a moment by attackers. CC encounters high latency and high costs in communication and data storage. These issues are present because of the centralized nature of the Cloud and its geographical distance from end-devices that produces data. To resolve these shortcomings in the cloud, Edge Computing was introduced as a CC extension.

Between the Cloud and the user-device platform is situated the Edge platform. We found that Edge network to end-device platform experiences much more latency reduction than Cloud platform to end-devices. This feature is very relevant to the Edge paradigm. Reaching the end-device platform, there is a rapid drop in security when migrating from the Cloud platform to the Edge platform due to the Edge network being decentralized (distributed) in nature. Also, observing the migration of data to end-devices from Cloud platform via Edge network, the storage capacity sharply reduces. There is also a rapid decrease in real-time as data moves from end-devices via the Edge platform to the Cloud platform. For longer storage needs, a Cloud platform is utilized. Storage or processing of data from the end-devices occurs in the Edge platform. Despite the emerging of Edge Computing, vulnerabilities and threats still exist, and this, therefore, calls for strict measures with enhanced security and privacy techniques. Fog paradigm was considered to ameliorate Cloud and Edge paradigms.

Like the Edge paradigm, the Fog paradigm is also known to be an extension of the Cloud paradigm extending to the Edge network while rendering services such as computation, networking, data storage, and others close to the end-devices rather than moving data to the Cloud platform. However, the introduction of the Fog paradigm is seen to improve the infrastructural network to match the demands of large data quantity while enhancing the processing strength efficiently. Fog paradigm can ameliorate issues like mobility, complexity in a distribution environment, location identity, real-time response, and security and privacy aspects. The fog paradigm does not depend on the Cloud data center but instead relies on end-devices to store and process its data. Broader availability of node access gives some level of flexibility to the applications. Like the Fog paradigm, the Edge paradigm also permits the handling of computation at the network edge, which is very near where data is generated. What makes the Fog paradigm different from the Edge paradigm is its ability for Fog nodes to interconnect, while the Edge paradigm operates with separate Edge nodes.

Confidentiality, Integrity, and Availability are the three most significant security and privacy expectations. The transfer and storage of data must be confidential, with integrity, and made available. Confidentiality grants data access only to individuals and organizations that own these data. During the transfer of data within the different user layers, the main network, storing and processing data in Cloud, Edge, or Fog paradigm, its access is strongly restricted. Encrypting data is a way of achieving confidentiality. Data correctness and consistency is a model of integrity which avoids information being tampered with or modified. Some mechanisms can be used for verifying sent and received data integrity. Only authorized persons are granted access to available data. Thus, availability determines that data must be available anywhere at any time based on established policies. To attain these expectations, various instruments, patterns, methodologies, and mechanisms such as cryptography, encryption, authentication, and others are deployed to the multiple platforms (layers) when data is being transferred and stored.

Cloud, Edge, and Fog paradigms exhibit the same view of providing QoS to customers, but they all have a separate set of features that makes them differ from one another, as we have explained in this work. However, the Fog paradigm is designated the most effective and reliable system to better handle the security and privacy challenges encountered.

Even though the Fog paradigm can offer better security and privacy services to end-devices in general, some features of the Fog paradigm like decentralization, constraints of resources, homogeneity, and virtualized systems are vulnerable to security and privacy challenges in comparison to the Cloud paradigm, which is centralized. Due to the absence of standardization regarding countermeasures deployment, highly effective security and privacy mitigation in the Cloud paradigm cannot be implemented straight to the Fog paradigm because of the named features above. Therefore, Fog systems do need innovative countermeasures to address these challenges. Future research should also be on new techniques and mechanisms that can fit Fog paradigm features and possibly cross-platform countermeasure tools. Hence, they should be suggestions for effective and efficient solutions.

# REFERENCES

[1] Mäkitalo, N., Ometov, A., Kannisto, J., Andreev, S., Koucheryavy, Y. and Mikkonen, T. Safe, secure executions at the network edge: coordinating cloud, edge, and fog computing. *IEEE Software* 35.1 (2017), 30–37.

[2] Alhroob, A. and Samawi, V. W. Privacy in Cloud Computing: Intelligent Approach (Research Poster). *2018 International Conference on High Performance Computing Simulation (HPCS)*. 2018, 1063–1065. DOI: 10.1109/HPCS.2018.00170.

[3] Ometov, A., Chukhno, O., Chukhno, N., Nurmi, J. and Lohan, E. S. When wearable technology meets computing in future networks: a road ahead. *Proceedings of the 18th ACM International Conference on Computing Frontiers*. 2021, 185–190.

[4] Guilloteau, S. and Venkatesen, M. Privacy in cloud computing-itu-t technology watch report march 2012. *International Telecommunication Union: Geneva, Switzerland* (2013).

[5] Cook, A., Robinson, M., Ferrag, M. A., Maglaras, L. A., He, Y., Jones, K. and Janicke, H. Internet of cloud: Security and privacy issues. *Cloud Computing for Optimization: Foundations, Applications, and Challenges*. Springer, 2018, 271–301.

[6] Xiao, Z. and Xiao, Y. Security and Privacy in Cloud Computing, IEEE Communications Surveys & Tutorials, Vol. 15. (2013).

[7] Pearson, S. and Casassa-Mont, M. Sticky policies: An approach for managing privacy across multiple parties. *Computer* 44.9 (2011), 60–68.

[8] Riaz, S. and Muhammad, J. An evaluation of public cloud adoption for higher education: A case study from Pakistan. *2015 International Symposium on Mathematical Sciences and Computing Research (iSMSC)*. 2015, 208–213. DOI: 10.1109/ISMSC.2015.7594054.

[9] Denyer, D. and Tranfield, D. Producing a systematic review. (2009).

[10] Romero, M., Guédria, W., Panetto, H. and Barafort, B. Towards a characterisation of smart systems: A systematic literature review. *Computers in industry* 120 (2020), 103224.

[11] *PRISMA Guidelines. PRISMA Statement*. 2021. URL: http://www.prisma-statement.org/ (visited on 2021).

[12] *Definition of Cloud Computing. Cloud computing*. 2020. URL: https://www.nist.gov/publications/nist-definition-cloud-computing (visited on 2020).

[13] *Five characteristics of cloud computing. Cloud computing*. 2020. URL: https://www.controleng.com/articles/five-characteristics-of-cloud-computing/ (visited on 2020).

[14] *Application Management in the Cloud. Managing Applications for Cloud, Mobile, IoT and eBusiness*. 2020. URL: ⟨http://www.sciencedirect.com/science/article/pii/B9780128040188000048⟩ (visited on 2020).

[15] *Cloud computing: Assessing the risks.[Skillsoft version]*. 2020. URL: ⟨https://masterworkshop.skillport.com/skillportfe/main.action?assetid=47045⟩ (visited on 2020).

[16] Tang, J. G. The Research on Cloud Computing Security Model and Countermeasures. *Applied Mechanics and Materials* 511-512 (Feb. 2014). Copyright - Copyright Trans Tech Publications Ltd. Feb 2014; Last updated - 2018-10-06, 1196–1200.

[17] *National Institute of Standards and Technology Special Publication 800-145 7 pages (September 2011). Measured Service*. 2020. URL: ⟨https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf⟩ (visited on 2020).

[18] Jadeja, Y. and Modi, K. Cloud computing - concepts, architecture and challenges. *2012 International Conference on Computing, Electronics and Electrical Technologies (ICCEET)*. 2012, 877–880.

[19] *Cloud Computing. Cloud Computing architecture*. 2020. URL: ⟨https://www.tutorialspoint.com/cloud_computing/cloud_computing_architecture.htm⟩ (visited on 2020).

[20] Odun-Ayo, I., Ananya, M., Agono, F. and Goddy-Worlu, R. Cloud Computing Architecture: A Critical Analysis. *2018 18th International Conference on Computational Science and Applications (ICCSA)*. 2018, 1–7.

[21] Mathur, P. and Nishchal, N. Cloud computing: New challenge to the entire computer industry. *2010 First International Conference On Parallel, Distributed and Grid Computing (PDGC 2010)*. 2010, 223–228.

[22] *Cloud Computing Architecture. Cloud Run-time*. 2020. URL: https://www.toolbox.com/tech/cloud/articles/what-is-cloud-computing-architecture-front-end-back-end-explained/ (visited on 2020).

[23] Divya, K. and Jeyalatha, S. Key technologies in cloud computing. *2012 International Conference on Cloud Computing Technologies, Applications and Management (ICCCTAM)*. 2012, 196–199.

[24] Sarathy, V., Narayan, P. and Mikkilineni, R. Next Generation Cloud Computing Architecture: Enabling Real-Time Dynamism for Shared Distributed Physical Infrastructure. *2010 19th IEEE International Workshops on Enabling Technologies: Infrastructures for Collaborative Enterprises*. 2010, 48–53.

[25] Ong, C.-S., Lai, J.-Y. and Wang, Y.-S. Factors affecting engineers' acceptance of asynchronous e-learning systems in high-tech companies. *Information & management* 41.6 (2004), 795–804.

[26] Singh, S. P., Nayyar, A., Kumar, R. and Sharma, A. Fog computing: from architecture to edge computing and big data processing. *The Journal of Supercomputing* (Nov. 2018). DOI: 10.1007/s11227-018-2701-2.

[27] Watfa, M. Cloud computing and E-learning: Potential pitfalls and benefits. *2016 Sixth International Conference on Innovative Computing Technology (INTECH)*. 2016, 140–144. DOI: 10.1109/INTECH.2016.7845128.

[28] Alabbadi, M. M. Cloud computing for education and learning: Education and learning as a service (ELaaS). *2011 14th International conference on interactive collaborative learning*. IEEE. 2011, 589–594.

[29] *Cloud computing definitions for each type. Software as a Service - SaaS*. 2020. URL: https://www.infoworld.com/article/2683784/what-is-cloud-computing.html) (visited on 2020).

[30] *IBM Cloud Learn Hub. Infrastructure as a Service - IaaS*. 2020. URL: https://www.ibm.com/cloud/learn/iaas (visited on 2020).

[31] *PaaS and Development Tools. PaaS*. 2020. URL: (https://searchcloudcomputing.techtarget.com/definition/Platform-as-a-Service-PaaS) (visited on 2020).

[32] *Platform as a Service. PaaS*. 2020. URL: (https://searchcloudcomputing.techtarget.com/definition/Platform-as-a-Service-PaaS) (visited on 2020).

[33] Nuria, L. R. "Cloud computing" in library automation: benefits and drawbacks. *The Bottom Line* 25.3 (2012). Copyright - Copyright Emerald Group Publishing Limited 2012; Last updated - 2019-12-20; CODEN - BOLIEO, 110–114.

[34] *Business Queensland. Benefits Of Cloud Computing*. 2020. URL: (https://www.business.qld.gov.au/running-business/it/cloud-computing/benefits) (visited on 2020).

[35] *Platform as a Service. Scalability*. 2020. URL: (https://www.business.qld.gov.au/running-business/it/cloud-computing/benefits) (visited on 2020).

[36] Nuria, L. R. "Cloud computing" in library automation: benefits and drawbacks. *The Bottom Line* 25.3 (2012). Copyright - Copyright Emerald Group Publishing Limited 2012; Last updated - 2019-12-20; CODEN - BOLIEO, 110–114.

[37] *Benefits of cloud computing*. 2020. URL: (https://www.salesforce.com/products/platform/best-practices/benefits-of-cloud-computing/) (visited on 2020).

[38] *Benefits of cloud computing. Collaboration Efficiency*. 2020. URL: ⟨https://www.business.qld.gov.au/running-business/it/cloud-computing/benefits⟩ (visited on 2020).

[39] *Benefits of cloud computing. Security*. URL: ⟨https://www.salesforce.com/products/platform/best-practices/benefits-of-cloud-computing/⟩ (visited on 2020).

[40] *Benefits of cloud computing. Access to Automatic Updates*. 2020. URL: ⟨https://www.business.qld.gov.au/running-business/it/cloud-computing/benefits⟩ (visited on 2020).

[41] Satyanarayanan, M. Edge Computing. *Computer* 50.10 (2017), 36–38.

[42] *Edge Computing Learning Objectives. What is edge computing?* 2020. URL: ⟨https://www.cloudflare.com/en-gb/learning/serverless/glossary/what-is-edge-computing/⟩ (visited on 2020).

[43] *Edge computing – what is edge computing? Edge computing definition: key terms in edge computing defined*. 2020. URL: ⟨https://stlpartners.com/edge-computing/what-is-edge-computing/⟩ (visited on 2020).

[44] Gezer, V., Um, J. and Ruskowski, M. An extensible edge computing architecture: Definition, requirements and enablers. *Proceedings of the UBICOMM* (2017).

[45] Mukherjee, M., Matam, R., Shu, L., Maglaras, L., Ferrag, M. A., Choudhury, N. and Kumar, V. Security and privacy in fog computing: Challenges. *IEEE Access* 5 (2017), 19293–19304.

[46] Xiao, Y., Jia, Y., Liu, C., Cheng, X., Yu, J. and Lv, W. Edge Computing Security: State of the Art and Challenges. *Proceedings of the IEEE* 107.8 (2019), 1608–1631.

[47] Stepanov, N., Alekseeva, D., Ometov, A. and Lohan, E. S. Applying Machine Learning to LTE Traffic Prediction: Comparison of Bagging, Random Forest, and SVM. *2020 12th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*. IEEE. 2020, 119–123.

[48] Statista. Number of active video gamers worldwide from 2014 to 2021 (in millions). (2018).

[49] Pottie-Sherman, Y. and Lynch, N. Gaming on the edge: Mobile labour and global talent in Atlantic Canada's video game industry. *The Canadian Geographer/Le Géographe canadien* 63.3 (2019), 425–439.

[50] Olshannikova, E., Ometov, A. and Koucheryavy, Y. Towards big data visualization for augmented reality. *Proc. of IEEE 16th Conference on Business Informatics*. Vol. 2. IEEE. 2014, 33–37.

[51] *Edge Computing Use Case Examples. Entertainment-Cloud Gaming*. 2020. URL: https://stlpartners.com/edge-computing/edge-computing-market-trends/ (visited on 2020).

[52] Tang, W., Zhao, X., Rafique, W. and Dou, W. A Blockchain-Based Offloading Approach in Fog Computing Environment. *2018 IEEE Intl Conf on Parallel Distributed Processing with Applications, Ubiquitous Computing Communications, Big Data Cloud Computing, Social Computing Networking, Sustainable Computing Communications (ISPA/IUCC/BDCloud/SocialCom/SustainCom)*. 2018, 308–315. DOI: `10.1109/BDCloud.2018.00056`.

[53] Ometov, A., Moltchanov, D., Komarov, M., Volvenko, S. V. and Koucheryavy, Y. Packet level performance assessment of mmWave backhauling technology for 3GPP NR Systems. *IEEE Access* 7 (2019), 9860–9871.

[54] Dolui, K. and Datta, S. K. Comparison of edge computing implementations: Fog computing, cloudlet and mobile edge computing. *2017 Global Internet of Things Summit (GIoTS)*. 2017, 1–6. DOI: `10.1109/GIOTS.2017.8016213`.

[55] Pokorny, J., Ometov, A., Pascual, P., Baquero, C., Masek, P., Pyattaev, A., Garcia, A., Castillo, C., Andreev, S., Hosek, J. et al. Concept design and performance evaluation of UAV-based backhaul link with antenna steering. *Journal of Communications and Networks* 20.5 (2018), 473–483.

[56] Jiang, C., Cheng, X., Gao, H., Zhou, X. and Wan, J. Toward Computation Offloading in Edge Computing: A Survey. *IEEE Access* 7 (2019), 131543–131558. DOI: `10.1109/ACCESS.2019.2938660`.

[57] Ometov, A. Short-range communications within emerging wireless networks and architectures: A survey. *14th Conference of Open Innovation Association FRUCT*. IEEE. 2013, 83–89.

[58] *WEI Tech Exchange. Top 5 Benefits Of Edge Computing*. 2020. URL: `⟨https://blog.wei.com/top-5-benefits-of-edge-computing⟩` (visited on 2020).

[59] *Security at the Edge. Cloud, Security*. 2020. URL: `⟨https://www.ibm.com/cloud/blog/security-at-the-edge⟩` (visited on 2020).

[60] *Edge computing. what are the benefits of edge computing?* 2020. URL: `⟨https://www.cloudflare.com/en-gb/learning/serverless/glossary/what-is-edge-computing/⟩` (visited on 2020).

[61] *Benefits of Edge Computing for Business. Lowered Operational Costs*. 2020. URL: `⟨https://innovationatwork.ieee.org/benefits-of-edge-computing-for-business/⟩` (visited on 2020).

[62] *The Benefits of Edge Computing. Cost Effectiveness*. 2020. URL: `⟨https://www.bbconsult.co.uk/blog/edge-computing⟩` (visited on 2020).

[63] *Edge computing architecture and use cases. Core benefits*. 2020. URL: `⟨https://www.lfedge.org/2020/03/05/edge-computing-architecture-and-use-cases/⟩` (visited on 2020).

[64] Mäkitalo, N., Aaltonen, T., Raatikainen, M., Ometov, A., Andreev, S., Koucheryavy, Y. and Mikkonen, T. Action-oriented programming model: Collective executions and interactions in the Fog. *Journal of Systems and Software* 157 (2019), 110391.

[65] Stojmenovic, I., Wen, S., Huang, X. and Luan, H. An overview of Fog computing and its security issues. *Concurrency and Computation: Practice and Experience* 28.10 (), 2991–3005. DOI: 10.1002/cpe.3485. eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1002/cpe.3485. URL: https://onlinelibrary.wiley.com/doi/abs/10.1002/cpe.3485.

[66] Ometov, A., Shubina, V., Klus, L., Skibińska, J., Saafi, S., Pascacio, P., Flueratoru, L., Gaibor, D. Q., Chukhno, N., Chukhno, O. et al. A survey on wearable technology: History, state-of-the-art and current challenges. *Computer Networks* 193 (2021), 108074.

[67] Mahmood, Z. and Ramachandran, M. Fog Computing: Concepts, Principles and Related Paradigms. *Fog Computing*. Springer International Publishing, 2018, 3–21. DOI: 10.1007/978-3-319-94890-4_1. URL: https://doi.org/10.1007%2F978-3-319-94890-4_1.

[68] Qaim, W. B., Ometov, A., Molinaro, A., Lener, I., Campolo, C., Lohan, E. S. and Nurmi, J. Towards energy efficiency in the Internet of Wearable Things: A systematic review. *IEEE Access* 8 (2020), 175412–175435.

[69] *Edge computing vs. fog computing: Definitions and enterprise uses. Definitions and enterprise uses*. 2020. URL: ⟨https://www.cisco.com/c/en/us/solutions/enterprise-networks/edge-computing.html?dtid=osscdc000283⟩ (visited on 2020).

[70] Naha, R. K., Garg, S., Georgakopoulos, D., Jayaraman, P. P., Gao, L., Xiang, Y. and Ranjan, R. Fog Computing: Survey of Trends, Architectures, Requirements, and Research Directions. *IEEE Access* 6 (2018), 47980–48009.

[71] IEEE Standard for Adoption of OpenFog Reference Architecture for Fog Computing. *IEEE Std 1934-2018* (2018), 1–176.

[72] Peng, M., Yan, S., Zhang, K. and Wang, C. Fog-computing-based radio access networks: issues and challenges. *IEEE Network* 30.4 (2016), 46–53.

[73] De Donno, M., Tange, K. and Dragoni, N. Foundations and Evolution of Modern Computing Paradigms: Cloud, IoT, Edge, and Fog. *IEEE Access* 7 (2019), 150936–150948. DOI: 10.1109/ACCESS.2019.2947652.

[74] Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H. and Zhao, W. A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. *IEEE Internet of Things Journal* 4.5 (2017), 1125–1142.

[75] Consortium, O. et al. OpenFog reference architecture for fog computing. *Architecture Working Group* (2017), 1–162.

[76] Hu, P., Dhelim, S., Ning, H. and Qiu, T. Survey on fog computing: architecture, key technologies, applications and open issues. *Journal of network and computer applications* 98 (2017), 27–42.

[77] Group, O. C. A. W. et al. Openfog architecture overview. *White Paper OPFWP001* 216 (2016), 35.

[78] Hong, K., Lillethun, D., Ramachandran, U., Ottenwälder, B. and Koldehofe, B. Mobile Fog: A Programming Model for Large-Scale Applications on the Internet of Things. New York, NY, USA: Association for Computing Machinery, 2013. ISBN: 9781450321808. DOI: 10.1145/2491266.2491270. URL: https://doi.org/10.1145/2491266.2491270.

[79] Magurawalage, C. M. S., Yang, K. and Wang, K. Aqua Computing: Coupling Computing and Communications. *CoRR* abs/1510.07250 (2015). arXiv: 1510.07250. URL: http://arxiv.org/abs/1510.07250.

[80] Zhu, X., Chan, D. S., Hu, H., Prabhu, M. S., Ganesan, E. and Bonomi, F. IMPROVING VIDEO PERFORMANCE WITH EDGE SERVERS IN THE FOG COMPUTING ARCHITECTURE. *Intel Technology Journal* 19.1 (2015).

[81] Foerster, J., Ott, D., Oyman, O., Liao, Y., Somayazulu, S., Zhu, X., Chan, D. S. and Neisinger, C. TOWARDS REALIZING VIDEO AWARE WIRELESS NETWORKS. *Intel Technology Journal* 19.1 (2015).

[82] *"Fog Computing: An Overview of Big IoT Data Analytics". Wireless Communications and Mobile Computing*. 2020. URL: ⟨https://www.hindawi.com/journals/wcmc/2018/7157192/#references⟩ (visited on 2020).

[83] Bonomi, F., Milito, R., Zhu, J. and Addepalli, S. Fog Computing and Its Role in the Internet of Things. New York, NY, USA: Association for Computing Machinery, 2012. ISBN: 9781450315197. DOI: 10.1145/2342509.2342513. URL: https://doi.org/10.1145/2342509.2342513.

[84] Chiang, M. and Zhang, T. Fog and IoT: An Overview of Research Opportunities. *IEEE Internet of Things Journal* 3.6 (2016), 854–864.

[85] Zhu, J., Chan, D. S., Prabhu, M. S., Natarajan, P., Hu, H. and Bonomi, F. Improving Web Sites Performance Using Edge Servers in Fog Computing Architecture. *2013 IEEE Seventh International Symposium on Service-Oriented System Engineering*. 2013, 320–323.

[86] Chiang, M. and Zhang, T. Fog and IoT: An overview of research opportunities. *IEEE Internet of Things Journal* 3.6 (2016), 854–864.

[87] Chiang, M., Balasubramanian, B. and Bonomi, F. *Fog for 5G and IoT*. Vol. 288. Wiley Online Library, 2017.

[88] Chiang, M., Ha, S., Risso, F., Zhang, T. and Chih-Lin, I. Clarifying fog computing and networking: 10 questions and answers. *IEEE Communications Magazine* 55.4 (2017), 18–20.

[89] Chiang, M., Ha, S., Risso, F., Zhang, T. and Chih-Lin, I. Clarifying Fog Computing and Networking: 10 Questions and Answers. *IEEE Communications Magazine* 55.4 (2017), 18–20. DOI: 10.1109/MCOM.2017.7901470.

[90] Khan, S. U. The curious case of distributed systems and continuous computing. *IT Professional* 18.2 (2016), 4–7.

[91] *Wireless Communications and Mobile Computing. Key featured difference between fog and cloud.* 2020. URL: https://www.hindawi.com/journals/wcmc/2018/7157192/tab1/ (visited on 2020).

[92] Wang, C., Chow, S. S. M., Wang, Q., Ren, K. and Lou, W. Privacy-Preserving Public Auditing for Secure Cloud Storage. *IEEE Transactions on Computers* 62.2 (2013), 362–375. DOI: 10.1109/TC.2011.245.

[93] Thamizhselvan, M., Raghuraman, R., Gershon Manoj, S. and Victer Paul, P. A novel security model for cloud using trusted third party encryption. *2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)*. 2015, 1–5. DOI: 10.1109/ICIIECS.2015.7193199.

[94] Zar, J. Privacy and Security As Assets: Beyond Risk Thinking to Profitable Payback. *IEEE GLOBECOM 2008 - 2008 IEEE Global Telecommunications Conference*. 2008, 1–6. DOI: 10.1109/GLOCOM.2008.ECP.1060.

[95] Hurlburt, G. F., Miller, K. W., Voas, J. M. and Day, J. M. Privacy and/or Security: Take Your Pick. *IT Professional* 11.4 (2009), 52–55. DOI: 10.1109/MITP.2009.81.

[96] Alkadi, O., Moustafa, N. and Turnbull, B. A Review of Intrusion Detection and Blockchain Applications in the Cloud: Approaches, Challenges and Solutions. *IEEE Access* 8 (2020), 104893–104917. DOI: 10.1109/ACCESS.2020.2999715.

[97] Patel, A., Shah, N., Ramoliya, D. and Nayak, A. A detailed review of Cloud Security: Issues, Threats Attacks. *2020 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA)*. 2020, 758–764. DOI: 10.1109/ICECA49313.2020.9297572.

[98] Ranchal, R., Bhargava, B., Othmane, L. B., Lilien, L., Kim, A., Kang, M. and Linderman, M. Protection of Identity Information in Cloud Computing without Trusted Third Party. *2010 29th IEEE Symposium on Reliable Distributed Systems*. 2010, 368–372. DOI: 10.1109/SRDS.2010.57.

[99] Zhang, J., Chen, B., Zhao, Y., Cheng, X. and Hu, F. Data Security and Privacy-Preserving in Edge Computing Paradigm: Survey and Open Issues. *IEEE Access* 6 (2018), 18209–18237. DOI: 10.1109/ACCESS.2018.2820162.

[100] Sinha, P., Rai, A. k. and Bhushan, B. Information Security threats and attacks with conceivable counteraction. *2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT)*. Vol. 1. 2019, 1208–1213. DOI: 10.1109/ICICICT46008.2019.8993384.

[101] Hossain, M. M., Fotouhi, M. and Hasan, R. Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things. *2015 IEEE World Congress on Services*. 2015, 21–28. DOI: 10.1109/SERVICES.2015.12.

[102] Khanam, S., Ahmedy, I. B., Idna Idris, M. Y., Jaward, M. H. and Bin Md Sabri, A. Q. A Survey of Security Challenges, Attacks Taxonomy and Advanced Coun-

termeasures in the Internet of Things. *IEEE Access* 8 (2020), 219709–219743. DOI: 10.1109/ACCESS.2020.3037359.

[103] Aljumah, A. and Ahanger, T. A. Fog computing and security issues: A review. *2018 7th International Conference on Computers Communications and Control (ICCCC)*. 2018, 237–239. DOI: 10.1109/ICCCC.2018.8390464.

[104] Jouini, M. and Rabai, L. B. A. A security framework for secure cloud computing environments. *Cloud security: Concepts, methodologies, tools, and applications*. IGI Global, 2019, 249–263.

[105] Sharma, A., Keshwani, B. and Dadheech, P. Authentication issues and techniques in cloud computing security: a review. *Proceedings of International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM), Amity University Rajasthan, Jaipur-India*. 2019.

[106] Paxton, N. C. Cloud Security: A Review of Current Issues and Proposed Solutions. *2016 IEEE 2nd International Conference on Collaboration and Internet Computing (CIC)*. 2016, 452–455. DOI: 10.1109/CIC.2016.066.

[107] Kalloniatis, C., Mouratidis, H., Vassilis, M., Islam, S., Gritzalis, S. and Kavakli, E. Towards the design of secure and privacy-oriented information systems in the cloud: Identifying the major concepts. *Computer Standards & Interfaces* 36.4 (2014), 759–775.

[108] Pearson, S. and Benameur, A. Privacy, security and trust issues arising from cloud computing. *2010 IEEE Second International Conference on Cloud Computing Technology and Science*. IEEE. 2010, 693–702.

[109] Ouedraogo, M., Khadraoui, D., De Rémont, B., Dubois, E. and Mouratidis, H. Deployment of a security assurance monitoring framework for telecommunication service infrastructures on a VoIP service. *2008 New Technologies, Mobility and Security*. IEEE. 2008, 1–5.

[110] Stevenson, D. and Pasek, J. Privacy concern, trust, and desire for content personalization. TPRC. 2015.

[111] Aluvalu, R. and Muddana, L. A survey on access control models in cloud computing. *Emerging ICT for Bridging the Future-Proceedings of the 49th Annual Convention of the Computer Society of India (CSI) Volume 1*. Springer. 2015, 653–664.

[112] Cai, F., Zhu, N., He, J., Mu, P., Li, W. and Yu, Y. Survey of access control models and technologies for cloud computing. *Cluster Computing* 22.3 (2019), 6111–6122.

[113] Takabi, H. Privacy aware access control for data sharing in cloud computing environments. *Proceedings of the 2nd international workshop on Security in cloud computing*. 2014, 27–34.

[114] PRASAD, S. N. and AMBICA, M. Privacy Preserving Policy Based Content Sharing in Public Clouds. (2015).

[115] Weiyu, J., Zhan, W., Limin, L. and Neng, G. Towards efficient update of access control policy for cryptographic cloud storage. *China Communications* 12.12 (2015), 43–52.

[116] Li, J., Zhang, Y., Chen, X. and Xiang, Y. Secure attribute-based data sharing for resource-limited users in cloud computing. *Computers & Security* 72 (2018), 1–12.

[117] Lee, K. Security threats in cloud computing environments. *International journal of security and its applications* 6.4 (2012), 25–32.

[118] Alliance, C. *The Treacherous Twelve-Cloud Computing Top Threats in 2016*. 2016.

[119] Modi, C., Patel, D., Borisaniya, B., Patel, H., Patel, A. and Rajarajan, M. A survey of intrusion detection techniques in cloud. *Journal of network and computer applications* 36.1 (2013), 42–57.

[120] Chang, V. and Ramachandran, M. Towards Achieving Data Security with the Cloud Computing Adoption Framework. *IEEE Transactions on Services Computing* 9.1 (2016), 138–151. DOI: 10.1109/TSC.2015.2491281.

[121] Fox, A., Griffith, R., Joseph, A., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I. et al. Above the clouds: A berkeley view of cloud computing. *Dept. Electrical Eng. and Comput. Sciences, University of California, Berkeley, Rep. UCB/EECS* 28.13 (2009), 2009.

[122] Pearson, S. and Benameur, A. Privacy, security and trust issues arising from cloud computing. *2010 IEEE Second International Conference on Cloud Computing Technology and Science*. IEEE. 2010, 693–702.

[123] Mulazzani, M., Schrittwieser, S., Leithner, M., Huber, M. and Weippl, E. Dark clouds on the horizon: Using cloud storage as attack vector and online slack space. (2011).

[124] Di Vimercati, S. D. C., Foresti, S., Jajodia, S., Paraboschi, S. and Samarati, P. Over-encryption: Management of access control evolution on outsourced data. *Proceedings of the 33rd international conference on Very large data bases*. 2007, 123–134.

[125] Mills, A. Protecting your data: Cloud Security Alliance. *CIO* Jul/Aug 2012 (2012).

[126] Tyagi, A. K., Niladhuri, S. and Priya, R. Never trust anyone: Trust-privacy trade-offs in vehicular ad-hoc networks. *Journal of Advances in Mathematics and Computer Science* (2016), 1–23.

[127] Rusk, J.-D. Trust and decision making in the privacy paradox?: *Proceedings of the Southern Association for Information Systems Conference*. 2014.

[128] Sun, P. J. Privacy Protection and Data Security in Cloud Computing: A Survey, Challenges, and Solutions. *IEEE Access* 7 (2019), 147420–147452. DOI: 10.1109/ACCESS.2019.2946185.

[129] Saxena, T. and Chourey, V. A survey paper on cloud security issues and challenges. *2014 Conference on IT in Business, Industry and Government (CSIBIG)*. 2014, 1–5. DOI: 10.1109/CSIBIG.2014.7056957.

[130] França, R. P., Iano, Y., Monteiro, A. C. B. and Arthur, R. Lower memory consumption for data transmission in smart cloud environments with CBEDE methodology. *Smart Systems Design, Applications, and Challenges*. IGI Global, 2020, 216–237.

[131] França, R. P., Iano, Y., Monteiro, A. C. B. and Arthur, R. Intelligent applications of WSN in the World: a technological and literary background. *Handbook of Wireless Sensor Networks: Issues and Challenges in Current Scenario's*. Springer, 2020, 13–34.

[132] Ai, Y., Peng, M. and Zhang, K. Edge computing technologies for Internet of Things: a primer. *Digital Communications and Networks* 4.2 (2018), 77–86.

[133] Markova, E., Gudkova, I., Ometov, A., Dzantiev, I., Andreev, S., Koucheryavy, Y. and Samouylov, K. Flexible spectrum management in a smart city within licensed shared access framework. *IEEE Access* 5 (2017), 22252–22261.

[134] Moltchanov, D., Ometov, A., Andreev, S. and Koucheryavy, Y. Upper bound on capacity of 5G mmWave cellular with multi-connectivity capabilities. *Electronics Letters* 54.11 (2018), 724–726.

[135] Roman, R., Lopez, J. and Mambo, M. Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges. *Future Generation Computer Systems* 78 (2018), 680–698.

[136] Cao, K., Liu, Y., Meng, G. and Sun, Q. An Overview on Edge Computing Research. *IEEE Access* 8 (2020), 85714–85728. DOI: 10.1109/ACCESS.2021.2991734.

[137] Roman, R., Lopez, J. and Mambo, M. Mobile edge computing: a survey and analysis of security threats and challenges. *Elsevier Future Gen. Computer Systems* (2016).

[138] Zissis, D. and Lekkas, D. Addressing cloud computing security issues. *Future Generation computer systems* 28.3 (2012), 583–592.

[139] Stojmenovic, I. and Wen, S. The fog computing paradigm: Scenarios and security issues. *2014 federated conference on computer science and information systems*. IEEE. 2014, 1–8.

[140] Bhat, S. A., Sofi, I. B. and Chi, C. .-.-Y. Edge Computing and Its Convergence With Blockchain in 5G and Beyond: Security, Challenges, and Opportunities. *IEEE Access* 8 (2020), 205340–205373. DOI: 10.1109/ACCESS.2020.3037108.

[141] Khan, A. N., Ali, M., Khan, A. u. R., Khan, F. G., Khan, I. A., Jadoon, W., Shamshirband, S. and Chronopoulos, A. T. A comparative study and workload distribution model for re-encryption schemes in a mobile cloud computing environment. *International Journal of Communication Systems* 30.16 (2017), e3308.

[142] Du, M., Wang, K., Chen, Y., Wang, X. and Sun, Y. Big data privacy preserving in multi-access edge computing for heterogeneous Internet of Things. *IEEE Communications Magazine* 56.8 (2018), 62–67.

[143] Hou, Y., Garg, S., Hui, L., Jayakody, D. N. K., Jin, R. and Hossain, M. S. A data security enhanced access control mechanism in mobile edge computing. *IEEE Access* 8 (2020), 136119–136130.

[144] Zeyu, H., Geming, X., Zhaohang, W. and Sen, Y. Survey on Edge Computing Security. *2020 International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE)*. 2020, 96–105. DOI: 10.1109/ICBAIE49996.2020.00027.

[145] Liu, D., Yan, Z., Ding, W. and Atiquzzaman, M. A Survey on Secure Data Analytics in Edge Computing. *IEEE Internet of Things Journal* 6.3 (2019), 4946–4967. DOI: 10.1109/JIOT.2019.2897619.

[146] Khalil, I., Khreishah, A. and Azeem, M. Consolidated Identity Management System for secure mobile cloud computing. *Computer Networks* 65 (2014), 99–110.

[147] Wei, W., Xu, F. and Li, Q. MobiShare: Flexible privacy-preserving location sharing in mobile online social networks. *2012 Proceedings IEEE INFOCOM*. 2012, 2616–2620. DOI: 10.1109/INFCOM.2012.6195664.

[148] Li, R., Liu, A. X., Wang, A. L. and Bruhadeshwar, B. Fast and scalable range query processing with strong privacy protection for cloud computing. *IEEE/ACM Transactions On Networking* 24.4 (2015), 2305–2318.

[149] Wang, K., Du, M., Yang, D., Zhu, C., Shen, J. and Zhang, Y. *Game-theory-based active defense for intrusion detection in cyber-physical embedded systems*. 2016.

[150] Shi, W., Zhang, L., Wu, C., Li, Z. and Lau, F. C. An online auction framework for dynamic resource provisioning in cloud computing. *ACM SIGMETRICS Performance Evaluation Review* 42.1 (2014), 71–83.

[151] Ma, F., Luo, X. and Litvinov, E. Cloud computing for power system simulations at ISO New England—Experiences and challenges. *IEEE Transactions on Smart Grid* 7.6 (2016), 2596–2603.

[152] Chen, X., Jiao, L., Li, W. and Fu, X. Efficient multi-user computation offloading for mobile-edge cloud computing. *IEEE/ACM Transactions on Networking* 24.5 (2015), 2795–2808.

[153] Chen, S., Irving, S. and Peng, L. Operational cost optimization for cloud computing data centers using renewable energy. *IEEE Systems Journal* 10.4 (2015), 1447–1458.

[154] Zeng, D., Gu, L., Guo, S., Cheng, Z. and Yu, S. Joint optimization of task scheduling and image placement in fog computing supported software-defined embedded system. *IEEE Transactions on Computers* 65.12 (2016), 3702–3712.

[155] Wang, K., Yuan, L., Miyazaki, T., Zeng, D., Guo, S. and Sun, Y. Strategic antieavesdropping game for physical layer security in wireless cooperative networks. *IEEE Transactions on Vehicular Technology* 66.10 (2017), 9448–9457.

[156] Rimal, B. P. and Maier, M. Workflow scheduling in multi-tenant cloud computing environments. *IEEE Transactions on parallel and distributed systems* 28.1 (2016), 290–304.

[157] Bonomi, F., Milito, R., Zhu, J. and Addepalli, S. Fog computing and its role in the internet of things. *Proceedings of the first edition of the MCC workshop on Mobile cloud computing*. 2012, 13–16.

[158] Aazam, M. and Huh, E.-N. Fog computing: The cloud-iot\/ioe middleware paradigm. *IEEE Potentials* 35.3 (2016), 40–44.

[159] Cao, J., Zhang, Q. and Shi, W. Challenges and opportunities in edge computing. *Edge Computing: A Primer*. Springer, 2018, 59–70.

[160] Mahmud, R., Kotagiri, R. and Buyya, R. Fog computing: A taxonomy, survey and future directions. *Internet of everything*. Springer, 2018, 103–130.

[161] El-Sayed, H., Sankar, S., Prasad, M., Puthal, D., Gupta, A., Mohanty, M. and Lin, C.-T. Edge of things: The big picture on the integration of edge, IoT and the cloud in a distributed computing environment. *IEEE Access* 6 (2017), 1706–1717.

[162] Aljumah, A. and Ahanger, T. A. Fog computing and security issues: A review. *2018 7th international conference on computers communications and control (ICCCC)*. IEEE. 2018, 237–239.

[163] Khan, S., Parkinson, S. and Qin, Y. Fog computing security: a review of current applications and security solutions. English. *Journal of Cloud Computing* 6.1 (Aug. 2017). Copyright - Journal of Cloud Computing is a copyright of Springer, 2017; Last updated - 2019-10-23, 1–22. URL: https://libproxy.tuni.fi/login?url=https://www-proquest-com.libproxy.tuni.fi/scholarly-journals/fog-computing-security-review-current/docview/1953281318/se-2?accountid=14242.

[164] Atlam, H. F., Walters, R. J. and Wills, G. B. Fog Computing and the Internet of Things: A Review. English. *Big Data and Cognitive Computing* 2 (June 2018). URL: https://libproxy.tuni.fi/login?url=https://www-proquest-com.libproxy.tuni.fi/scholarly-journals/fog-computing-internet-things-review/docview/2124676199/se-2?accountid=14242.

[165] Ni, J., Zhang, K., Lin, X. and Shen, X. Securing Fog Computing for Internet of Things Applications: Challenges and Solutions. *IEEE Communications Surveys Tutorials* 20.1 (2018), 601–628. DOI: 10.1109/COMST.2017.2762345.

[166] Modi, C., Patel, D., Borisaniya, B., Patel, A. and Rajarajan, M. A survey on security issues and solutions at different layers of Cloud computing. *The journal of supercomputing* 63.2 (2013), 561–592.

[167] Khorshed, M. T., Ali, A. S. and Wasimi, S. A. A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing. *Future Generation computer systems* 28.6 (2012), 833–851.

[168] Nenvani, G. and Gupta, H. A survey on attack detection on cloud using supervised learning techniques. *2016 Symposium on Colossal Data Analysis and Networking (CDAN)*. IEEE. 2016, 1–5.

[169] Ciurana, E. *Developing with google app engine*. Apress, 2009.

[170] Kortchinsky, K. Cloudburst: A VMware guest to host escape story. *Black Hat USA* 19 (2009).

[171] Ristenpart, T., Tromer, E., Shacham, H. and Savage, S. Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. *Proceedings of the 16th ACM conference on Computer and communications security*. 2009, 199–212.

[172] Naccache, D. and Stern, J. A new public key cryptosystem based on higher residues. *Proceedings of the 5th ACM Conference on Computer and Communications Security*. 1998, 59–66.

[173] Hay, B., Nance, K. and Bishop, M. Storm clouds rising: security challenges for IaaS cloud computing. *2011 44th Hawaii International Conference on System Sciences*. IEEE. 2011, 1–7.

[174] Almtrf, A., Alagrash, Y. and Zohdy, M. Framework modeling for User privacy in cloud computing. *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*. IEEE. 2019, 0819–0826.

[175] Wrenn, B. and CISSP, I. Unisys secure cloud addressing the top threats of cloud computing. *white paper* (2010).

[176] Grabosky, P. Organized cybercrime and national security. *Cybercrime Risks and Responses*. Springer, 2015, 67–80.

[177] Freier, A., Karlton, P. and Kocher, P. Netscape Communications. (2011).

[178] Chonka, A., Xiang, Y., Zhou, W. and Bonti, A. Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks. *Journal of Network and Computer Applications* 34.4 (2011), 1097–1107.

[179] Mittal, R. and kazim, A. Ananlysis of DDoS Attacks In Cloud. *2020 International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE)*. 2020, 19–23. DOI: 10.1109/ICSTCEE49637.2020.9277476.

[180] Amara, N., Zhiqui, H. and Ali, A. Cloud Computing Security Threats and Attacks with Their Mitigation Techniques. *2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*. 2017, 244–251. DOI: 10.1109/CyberC.2017.37.

[181] He, D., Chan, S. and Guizani, M. Security in the Internet of Things Supported by Mobile Edge Computing. *IEEE Communications Magazine* 56.8 (2018), 56–61. DOI: 10.1109/MCOM.2018.1701132.

[182] Yi, S., Qin, Z. and Li, Q. Security and privacy issues of fog computing: A survey. *International conference on wireless algorithms, systems, and applications*. Springer. 2015, 685–695.

[183] Abomhara, M. and Køien, G. M. Security and privacy in the Internet of Things: Current status and open issues. *2014 International Conference on Privacy and Security in Mobile Systems (PRISMS)*. 2014, 1–8. DOI: `10.1109/PRISMS.2014.6970594`.

[184] Mukherjee, M., Matam, R., Shu, L., Maglaras, L., Ferrag, M. A., Choudhury, N. and Kumar, V. Security and Privacy in Fog Computing: Challenges. *IEEE Access* 5 (2017), 19293–19304. DOI: `10.1109/ACCESS.2021.2749422`.

[185] Veerraju, T. and Kumar, K. K. A survey on fog computing: research challenges in security and privacy issues. *International Journal of Engineering & Technology* 7.2.7 (2018), 335–340.

[186] Guan, Y., Shao, J., Wei, G. and Xie, M. Data security and privacy in fog computing. *IEEE Network* 32.5 (2018), 106–111.

[187] Hussein, N. H. and Khalid, A. A survey of cloud computing security challenges and solutions. *International Journal of Computer Science and Information Security* 14.1 (2016), 52.

[188] Parikh, S., Dave, D., Patel, R. and Doshi, N. Security and privacy issues in cloud, fog and edge computing. *Procedia Computer Science* 160 (2019), 734–739.

[189] Davis, B. D., Mason, J. C. and Anwar, M. Vulnerability Studies and Security Postures of IoT Devices: A Smart Home Case Study. *IEEE Internet of Things Journal* 7.10 (2020), 10102–10110. DOI: `10.1109/JIOT.2020.2983983`.

[190] Li, Y., Li, D., Cui, W. and Zhang, R. Research based on OSI model. *2011 IEEE 3rd International Conference on Communication Software and Networks* (2011), 554–557.

[191] Ara, A., Al-Rodhaan, M., Tian, Y. and Al-Dhelaan, A. A secure service provisioning framework for cyber physical cloud computing systems. *arXiv preprint arXiv:1611.00374* (2015).

[192] Krishnan, P., Duttagupta, S. and Achuthan, K. SDN/NFV security framework for fog-to-things computing infrastructure. *Software: Practice and Experience* 50 (2020), 757–800.

[193] Li, Q., Li, W., Wang, J. and Cheng, M. A SQL Injection Detection Method Based on Adaptive Deep Forest. *IEEE Access* 7 (2019), 145385–145394. DOI: `10.1109/ACCESS.2019.2944951`.

[194] Alwarafy, A., Al-Thelaya, K. A., Abdallah, M., Schneider, J. and Hamdi, M. A Survey on Security and Privacy Issues in Edge-Computing-Assisted Internet of Things. *IEEE Internet of Things Journal* 8.6 (2021), 4004–4022. DOI: `10.1109/JIOT.2020.3015432`.

[195] Xie, X., Ren, C., Fu, Y., Xu, J. and Guo, J. SQL Injection Detection for Web Applications Based on Elastic-Pooling CNN. *IEEE Access* 7 (2019), 151475–151481. DOI: 10.1109/ACCESS.2019.2947527.

[196] Soni, N., Malekian, R. and Thakur, A. Edge Computing in Transportation: Security Issues and Challenges. *ArXiv* abs/2012.11206 (2020).

[197] Turel, Y. and Kotowski, R. Cloud Computing Virtualization and Cyber Attacks: Evidence Centralization. *Civil-Comp Proceedings* 107 (2015).

[198] Almutairy, N. M. and Al-Shqeerat, K. H. A Survey on Security Challenges of Virtualization Technology in Cloud Computing. *International Journal of Computer Science & Information Technology (IJCSIT) Vol* 11 (2019).

[199] Tao, Z., Xia, Q., Hao, Z., Li, C., Ma, L., Yi, S. and Li, Q. A Survey of Virtual Machine Management in Edge Computing. *Proceedings of the IEEE* 107.8 (2019), 1482–1499. DOI: 10.1109/JPROC.2019.2927919.

[200] Kazim, M. and Zhu, S. Y. Virtualization security in cloud computing. *Guide to Security Assurance for Cloud Computing*. Springer, 2015, 51–63.

[201] Alotaibi, A. M., Alrashidi, B. F., Naz, S. and Parveen, Z. Security issues in Protocols of TCP/IP Model at Layers Level. English. *International Journal of Computer Networks and Communications Security* 5.5 (May 2017). Copyright - Copyright Dorma Trading, Est. Publishing Manager May 2017; Last updated - 2017-06-29, 96–104. URL: https://libproxy.tuni.fi/login?url=https://www-proquest-com.libproxy.tuni.fi/scholarly-journals/security-issues-protocols-tcp-ip-model-at-layers/docview/1914454958/se-2?accountid=14242.

[202] Kumarasamy, S. and Gowrishankar, A. An Active Defense Mechanism for TCP SYN flooding attacks. *ArXiv* abs/1201.2103 (2012).

[203] Butun, I., Österberg, P. and Song, H. Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures. *IEEE Communications Surveys Tutorials* 22.1 (2020), 616–644. DOI: 10.1109/COMST.2019.2953364.

[204] Sinha, P., Jha, V. K., Rai, A. K. and Bhushan, B. Security vulnerabilities, attacks and countermeasures in wireless sensor networks at various layers of OSI reference model: A survey. *2017 International Conference on Signal Processing and Communication (ICSPC)*. 2017, 288–293. DOI: 10.1109/CSPC.2017.8305855.

[205] Faisal, A. and Zulkernine, M. A secure architecture for TCP/UDP-based cloud communications. *International Journal of Information Security* 20.2 (2021), 161–179.

[206] Radhakrishnan, R., Edmonson, W. W., Afghah, F., Rodriguez-Osorio, R. M., Pinto, F. and Burleigh, S. C. Survey of Inter-Satellite Communication for Small Satellite Systems: Physical Layer to Network Layer View. *IEEE Communications Surveys Tutorials* 18.4 (2016), 2442–2473. DOI: 10.1109/COMST.2016.2564990.

[207] Younis, O. H., Essa, S. E. and Ayman, E.-S. A survey on security attacks/defenses in mobile ad-hoc networks. *Commun Appl Electron* 6 (2017), 1–9.

[208] Le, A., Loo, J., Lasebae, A., Vinel, A., Chen, Y. and Chai, M. The Impact of Rank Attack on Network Topology of Routing Protocol for Low-Power and Lossy Networks. *IEEE Sensors Journal* 13.10 (2013), 3685–3692. DOI: 10.1109/JSEN.2013.2266399.

[209] Dimic, G., Sidiropoulos, N. and Zhang, R. Medium access control - physical cross-layer design. *IEEE Signal Processing Magazine* 21.5 (2004), 40–50. DOI: 10.1109/MSP.2004.1328087.

[210] Pan, F., Pang, Z., Luvisotto, M., Xiao, M. and Wen, H. Physical-Layer Security for Industrial Wireless Control Systems: Basics and Future Directions. *IEEE Industrial Electronics Magazine* 12.4 (2018), 18–27. DOI: 10.1109/MIE.2018.2874385.

[211] Yahuza, M., Idris, M. Y. I. B., Wahab, A. W. B. A., Ho, A. T. S., Khan, S., Musa, S. N. B. and Taha, A. Z. B. Systematic Review on Security and Privacy Requirements in Edge Computing: State of the Art and Future Research Opportunities. *IEEE Access* 8 (2020), 76541–76567. DOI: 10.1109/ACCESS.2020.2989456.

[212] Echeverrıa, S., Klinedinst, D., Williams, K. and Lewis, G. A. Establishing trusted identities in disconnected edge environments. *2016 IEEE/ACM Symposium on Edge Computing (SEC)*. IEEE. 2016, 51–63.

[213] Stojmenovic, I. and Wen, S. The Fog computing paradigm: Scenarios and security issues. *2014 Federated Conference on Computer Science and Information Systems*. 2014, 1–8. DOI: 10.15439/2014F503.

[214] Li, C.-T., Lee, C.-C. and Weng, C.-Y. A Dynamic Identity-Based User Authentication Scheme for Remote Login Systems. *Sec. and Commun. Netw.* 8.18 (Dec. 2015), 3372–3382. ISSN: 1939-0114. DOI: 10.1002/sec.1264. URL: https://doi.org/10.1002/sec.1264.

[215] Wang, D., Bai, B., Lei, K., Zhao, W., Yang, Y. and Han, Z. Enhancing Information Security via Physical Layer Approaches in Heterogeneous IoT With Multiple Access Mobile Edge Computing in Smart City. *IEEE Access* 7 (2019), 54508–54521. DOI: 10.1109/ACCESS.2019.2913438.

[216] Miswar, Suhardi and Kurniawan, N. B. A Systematic Literature Review on Survey Data Collection System. *2018 International Conference on Information Technology Systems and Innovation (ICITSI)*. 2018, 177–181. DOI: 10.1109/ICITSI.2018.8696036.

[217] Beyea, S. C. and Nicoll, L. H. Ten questions that will get you through any research report. *AORN journal* 65.5 (1997), 978–980.

[218] Gaberson, K. B. What's the answer? What's the question?: *AORN journal* 66.1 (1997), 148–151.

[219] Richardson, W. S., Wilson, M. C., Nishikawa, J., Hayward, R. S. et al. The well-built clinical question: a key to evidence-based decisions. *Acp j club* 123.3 (1995), A12–A13.

[220] Setiyoko, A., Sensuse, D. I. and Noprisson, H. A systematic literature review of environmental management information system (EMIS) development: Research trends, datasets, and methods. *2017 International Conference on Information Technology Systems and Innovation (ICITSI)*. 2017, 20–25. DOI: 10.1109/ICITSI.2017.8267912.

[221] Qasem, Y. A. M., Abdullah, R., Jusoh, Y. Y., Atan, R. and Asadi, S. Cloud Computing Adoption in Higher Education Institutions: A Systematic Review. *IEEE Access* 7 (2019), 63722–63744. DOI: 10.1109/ACCESS.2019.2916234.

[222] *Systematic Reviews: Search Strategy. Developing a Search Strategy*. 2021. URL: ⟨https://libguides.csu.edu.au/review/Search_Strategies⟩ (visited on 2021).

[223] Zhou, Z., Zhi, Q., Morisaki, S. and Yamamoto, S. A Systematic Literature Review on Enterprise Architecture Visualization Methodologies. *IEEE Access* 8 (2020), 96404–96427. DOI: 10.1109/ACCESS.2020.2995850.

[224] *Systematic Reviews: Search Strategy. PICO as a Search Strategy*. 2021. URL: ⟨https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6148624/⟩ (visited on 2021).

[225] Kitchenham, B. and Charters, S. Guidelines for performing systematic literature reviews in software engineering. (2007).

[226] Okoli, C. A guide to conducting a standalone systematic literature review. *Communications of the Association for Information Systems* 37.1 (2015), 43.

[227] Kitchenham, B. and Charters, S. *Guidelines for performing Systematic Literature Reviews in Software Engineering*. 2007.

[228] Yu, J. .-.-Y., Kim, Y. and Kim, Y. .-.-G. Intelligent Video Data Security: A Survey and Open Challenges. *IEEE Access* 9 (2021), 26948–26967. DOI: 10.1109/ACCESS.2021.3057605.

[229] Haneem, F., Ali, R., Kama, N. and Basri, S. Descriptive analysis and text analysis in Systematic Literature Review: A review of Master Data Management. *2017 International Conference on Research and Innovation in Information Systems (ICRIIS)*. 2017, 1–6. DOI: 10.1109/ICRIIS.2017.8002473.

[230] Alouffi, B., Hasnain, M., Alharbi, A., Alosaimi, W., Alyami, H. and Ayaz, M. A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies. *IEEE Access* 9 (2021), 57792–57807. DOI: 10.1109/ACCESS.2021.3073203.

[231] Keele, S. et al. *Guidelines for performing systematic literature reviews in software engineering*. Tech. rep. Citeseer, 2007.

[232] Wen, J., Li, S., Lin, Z., Hu, Y. and Huang, C. Systematic literature review of machine learning based software development effort estimation models. *Information and Software Technology* 54.1 (2012), 41–59.

# A METHODOLOGY: SYSTEMATIC LITERATURE REVIEW

## A.1 Criteria For Eligibility

Understanding and knowing about eligibility criteria makes it an important and easy to uphold the comprehensive, applicable, and validity of a literature review. Authors of reviews are expected to indicate and be specific in presenting the different eligibility criteria been utilized in reviews. The eligibility criteria involve different phases in the methodology of literature reviews in this thesis work and guarantee the unbiased and systematic selection of various studies, thereby playing a vital role in developing a search strategy as expected. Obtaining a substantial and meaningful result, the thesis approached the survey on diverse released literature obtained via a renowned database for academic journals, such as Scopus, ScienceDirect, IEEE Xplore, SpringerLink, and Google Scholar [216].

The first thing in the mind of any reader is to figure out the systematic review question, which will often ask, what the research question is all about? [217] [218]. Most essentially, the basic rule is that there must be a direct reflection of the research question to the research topic. Sometimes, it is also encouraged that if the research question can not reflect the topic, it should be mentioned in the abstract section accompanied by the text. Constructing the question is something that has to be in a simplified form, whereby readers can easily comprehend and re-construct in their different vocabularies [217] [218]. It must be noted that the PICO principle was established in the year 1995 and is now a universally acceptable format used in formulating research questions [219].

| **PICO CATEGORY** | **Important Notes** |
|---|---|
| Participants | Cloud, Edge and Fog Computing providers/customers. |
| Intervention | Security and Privacy |
| Comparison | Similarities and Differences |
| Outcome | Protection of applications, infrastructures and data from threats |

***Table A.1.*** *PICO Summary [220]*

The eligibility criteria performed here are based on studies relating to Cloud, Edge, and

Fog Paradigms, focusing on Security and Privacy. Peer-reviewed journals were primarily considered, and related articles were randomly chosen without a specific year of publication, at least dating back 10 – 15 years, mainly in the English language, and was carried out in an academic research setup, involving participants as providers and customers in Cloud Computing sector, with Security and Privacy studied as an intervention without any comparison. The main purpose of the intervention was to gain a comprehensive outcome of enhancing security measures and privacy management policies in organizations.

The main target of this thesis is to acquire a deeper understanding of research papers relating to security and privacy in Cloud, Edge, and Fog paradigms. In the light of gaining a wholistic insight of the study area, we had to define the thesis topic by importantly constructing four vital systematic literature review (SLR) research questions (RQ). The research questions aim to facilitate segmenting and good comprehension of the studies existing within this subject matter. This will also enhance the recognition of different limitations and other research pathways ahead. Below are the four generated research questions:

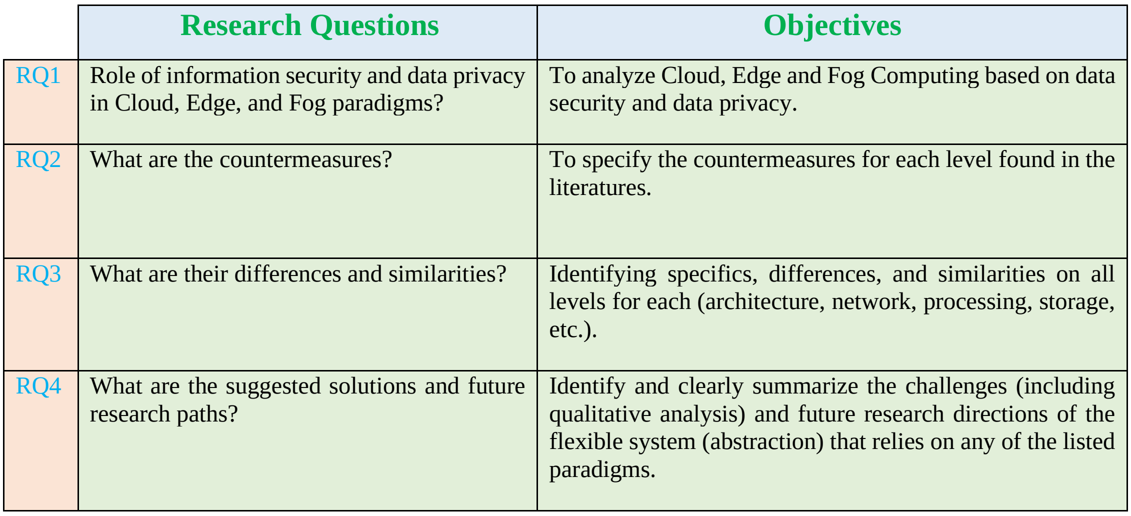
**RQ1**: What is the role of information security and privacy in the Cloud, Edge, and Fog paradigm?

**RQ2**: What are the attacks and countermeasures involved?

**RQ3**: What are their differences and similarities?

**RQ4**: What are the suggested solutions and future research paths?

**Figure A.1** shows related objectives to the defined research questions, which further gives us a well-guided approach in our SLR process. RQs, provide a path to engage, while the objectives pilot the entire research process with specific studies base on the research theme.



| | Research Questions | Objectives |
|---|---|---|
| RQ1 | Role of information security and data privacy in Cloud, Edge, and Fog paradigms? | To analyze Cloud, Edge and Fog Computing based on data security and data privacy. |
| RQ2 | What are the countermeasures? | To specify the countermeasures for each level found in the literatures. |
| RQ3 | What are their differences and similarities? | Identifying specifics, differences, and similarities on all levels for each (architecture, network, processing, storage, etc.). |
| RQ4 | What are the suggested solutions and future research paths? | Identify and clearly summarize the challenges (including qualitative analysis) and future research directions of the flexible system (abstraction) that relies on any of the listed paradigms. |

***Figure A.1.*** *Research questions with related objectives*

## A.2 Data Sources

Knowing and understanding, especially what area or databases to search for journals and articles, is a good path towards achieving a smooth, systematic review success. Every study has its specific databases to locate the essential journals needed. Different electronic databases were searched to figure out the various studies specifically, while also reference lists of journals were systematically scanned, and experts like my supervisor in the field of Cloud Computing were consulted. There was a limit stated for language, and non-English papers were not considered.

**Figure A.2** shows several databases were used as searches were done in platforms such as Andor (Tampere University Library's discovery service), IEEE Xplore (2015 - Present), Scopus (2015 - Present), Web of Science (2015 - Present), Springer (2015 - Present), ScienceDirect (2015 - Present), and other sources such as ResearchGate and Google Scholar (2015 - Present). On the other hand, few related articles with important materials reflecting the thesis title were hand-searched.

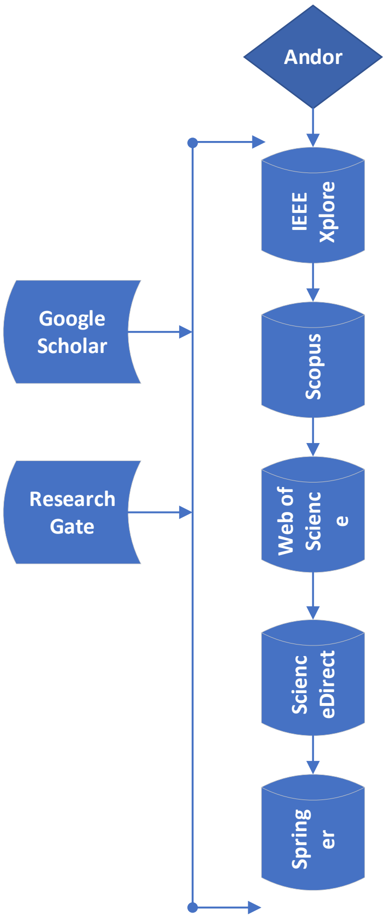


***Figure A.2.*** *Information Sources Used*
[221]

## A.3 Search Strategy

Conducting a systematic literature review takes a huge amount of time. To adequately manage and use lesser time during search with databases, the research must be well structured and consistent. It is always advised to keep a proper track of search history as searching advances and is narrowed down to get the most relevant materials. A good search approach can generate relevant results, especially when keywords, titles, authors, and filters are appropriately applied [222].

The different databases used in performing this extensive but essential review search include Scopus, Web of Science, IEEE Xplore, ScienceDirect, ProQuest, Ebsco, Springer, and ResearchGate. The selected sources were chosen because of their huge importance and are widely considered as the most relevant academic databases within the facet of engineering, particularly software and information technology engineering [223]. Some grey literature was also searched in Google Scholar. All these were done right up to February 1, 2021. Generally, the quality of the various articles or journals searched was the main goal for a good outcome primarily, while the reduced duration for searching the literature during search progress was the secondary obtained result. These outcomes were also made possible due to using a PICO guide acting as a tool model for a search strategy, unlike an unguided search process [224].

Respective search keywords used to find essential academic articles are theme, abstract, and index phrase. However, some steps were applied to formulate the key search words as presented below:

1. The research questions assisted in creating keywords.
2. Main terms were viewed in potential articles and necessary books.
3. Synonyms for key terms are identified with secondary spellings.
4. We made use of the Boolean operation OR to include synonyms and secondary spellings.
5. To combine several key terms, we use the Boolean AND.

“Cloud Computing” or “Edge Computing” or “Fog Computing” or “Security and Privacy” or “Security” or “Privacy.” The inclusion criteria used in choosing the research papers were done individually by reading through several academic articles and journals. All the criteria met by the various research studies were validated for selection in this systematic literature review [223].

A collection of pre-defined definitions and approaches were established to come up with the search words [225] [226]. After that, they were used to create the following search strings for the studies: Use of the Boolean operator "OR" to include secondary words or spellings, and the use of the Boolean operator "AND" to enable that all the combination of search terms are cloud computing OR edge computing OR fog computing OR security OR privacy. The keywords for the research were all derived from the title of the thesis. Cloud computing, Edge computing, Fog computing, security, and privacy are the keywords in question. Different search strings were formulated for different search engines, but the main search terms used in IEEE Xplore, is as follow: ("All Metadata":Cloud computing) AND ("All Metadata":edge computing) AND ("All Metadata":fog computing) AND ("All Metadata":security) AND ("All Metadata":privacy) [221]. Some complete search expressions were generated as seen below:

("cloud computing*" OR "edge computing*" OR "fog computing") AND (Security*) AND (edge OR cloud OR fog OR approximate OR IoT OR "Internet of Things" OR security OR privacy)

1. “Cloud Computing” AND “Security and Privacy” OR “Cloud Computing” AND “Security”

OR “Cloud Computing” AND “Privacy”

2. “Edge Computing” AND “Security and Privacy” OR “Edge Computing” AND “Security” OR “Edge Computing” AND “Privacy”

3. “Fog Computing” AND “Security and Privacy” OR “Fog Computing” AND “Security” OR “Fog Computing” AND “Privacy”

Zotero software system (https://www.zotero.org/) was utilized to save and deal with identified studies from the search outcome. We were able to retain **X** essential articles gotten from the search steps in **Figure A.3**. **Figure X** details the number of literature studies found, included, excluded, and the final number maintained.

## A.4 Study Selection

After completing the systematic literature review planning stage, it is then time to proceed to the important aspect of the study, which is the selection part that deals with a comprehensive screening of the various academic articles. The screening process is considered very decisive because it has to do with paper reduction, or in other words, to narrow down the number of acquired articles to be processed and examined. The main goal here is to achieve or select the most relevant articles worthy for the intended purpose of the study [227].

**Figure A.3** depicts the reason for study selection criteria which is aimed to look for primary studies that show clear proof about the research issue. Selection criteria are determined during the protocol specification to minimize the risk of bias, but they may be readjusted as the search process goes on. The research question acts as a guide to the inclusion and exclusion criteria, which is well supervised, thereby making sure, there is adequate understanding in interpretation and correct classification of studies [225].

**Table A.2** shows a generated inclusion and exclusion criteria, as it is well outlined with the use of special selection. The study selection was performed by scanning through the topics, abstracts, publication year, and full content.

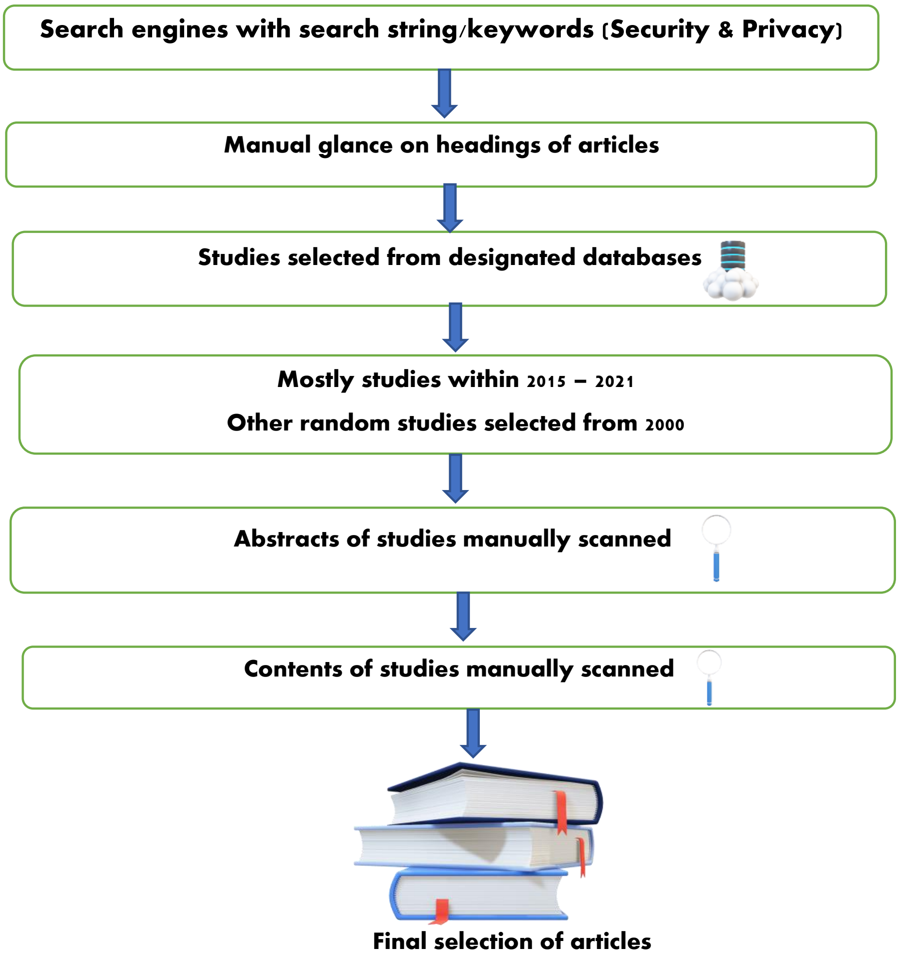

Search engines with search string/keywords (Security & Privacy)
Manual glance on headings of articles
Studies selected from designated databases
Mostly studies within 2015 – 2021
Other random studies selected from 2000
Abstracts of studies manually scanned
Contents of studies manually scanned
Final selection of articles

***Figure A.3.*** *Study Selection [228]*

| **Inclusion Criteria** | **Exclusion Criteria** |
|---|---|
| - A paper is regarded fit for inclusion as a journal, survey, or conference article to acquire an important highest standard. | - Papers not dwelling on security and privacy in Cloud, Edge, and Fog paradigm are excluded. |
| Published articles between 2010 and April 2021 are considered for inclusion to involve the most recent techniques used to address security and privacy issues in the various mentioned paradigms. | - Exclusion is considered for papers not available online or reachable on different digital databases. |
| - Only English articles were considered | - Non-English papers were excluded as well. |

***Table A.2.*** *Inclusion and exclusion outlines*

## A.5 Quality Assessment of Study

The extracted quantitative information of meta-analysis is the primary assessment baseline applied by the chosen articles with quality assessment (QA), considered a vital approach for information synthesis. In this review, the extracted data were achieved from several academic databases, and the quantity of information is quite less, which makes meta-analysis not appropriate here. As a matter of this, the quality assessment outcome was never utilized to measure the extracted information. However, the research outcomes were carefully interpreted, and the level of evidence was noted. These were made possible through coordination by using quality assessment.

Three basic quality assessment conditions were formulated to measure the essential papers' strength, authenticity, and vitality. **Table A.3** shows the formulated questions. There are three choices of responses relating to individual questions: Yes, Partially, or Not. Scoring the various responses, we got: Yes=2, Partially=1, and Not=0. To achieve a quality assessment mark for any research performed, we sum the quality mark of the responses to the quality assessment demands.

| **Category** | **Conditions** |
|---|---|
| QA1 | The prime target of the article is security and privacy |
| QA2 | Goals are visibly expressed |
| QA3 | Literatures are main research or primary papers |

***Table A.3.*** *Quality Assessment conditions [229]*

## A.6 Data Extraction

Primarily, the aim of data extraction is for defining and carrying out information extraction step-by-steps to keep the information gotten through the initial research and minimize some bias. Furthermore, the extracted information extracted can then be synthesized to provide a good response to the research or thesis questions. Generally, it is very important to perform information extraction and analysis, which helps to offer answers to specific research demands. In answering the research demands, vital information was thoroughly recorded from the X studies to meet the inclusion requirement. The documented aspects are as seen: Authors, title, publishing year, journal, surveys, conferences, nature of article, security and privacy considerations, their differences and similarities, the level of the technological approach been used, attacks, and their countermeasures. Moreover, the presence of weaknesses in the security and privacy of Cloud, Edge, and Fog paradigms renders an identified future research pathway.

## A.7 Data Synthesis

"Data synthesis is aimed to aggregate the evidence from chosen studies to answer the research questions [230]." One set of proof can pose a little force of evidence, but the totality of them severally can create a strengthened view (41). The retrieved data in this thesis involves both qualitative information (comparisons, attacks, and countermeasures of the various paradigms). In most cases, researchers will engage various approaches to synthesize the retrieved information concerning several types of review questions. However, in this case, the synthesis approach used is expressed as seen below.

Because of information relating to RQs, an approach known as the reciprocal translation was used in qualitative information synthesis and is known to be a meta-ethnography strategy. According to Kitchenham and Charters, "when studies are about similar things and researchers are attempting to provide an additive summary, synthesis can be achieved by 'translating' each case into each of the other cases" [231]. Based on this study, a two-way translation model is introduced when security and privacy in Cloud, Edge, and Fog paradigms are extracted from several identical papers. This security and privacy will be interpreted as a combined explanation of security and privacy. For example, considering that we managed to sort out three various, but unified explanations based on security in Cloud, Edge, and Fog paradigms from three papers: (1) protects the system, (2) can easily identify threats, and (3) response time to threats are good. Looking at the listed points, we can use the reciprocal translation by harmonizing the stated three explanations into a single phrase, "quick in protecting against threats" [232].