

**CLOUD, EDGE AND FOG COMPUTING
SYSTEMS: SECURITY AND PRIVACY ISSUES**

**A THESIS SUBMITTED TO THE INSTITUTE OF
GRADUATE STUDIES
OF
NEAR EAST UNIVERSITY**

By

MAJED SALEH ABDULQAWI

**In Partial Fulfilment of the Requirements for
the Degree of Master of Science
in
Computer Information Systems**

NICOSIA, 2021

MAJED SALEH ABDULQAWI

**CLOUD, EDGE AND FOG COMPUTING SYSTEMS:
SECURITY AND PRIVACY ISSUES**

SECURITY AND PRIVACY ISSUES

2021

NEU

**CLOUD, EDGE AND FOG COMPUTING
SYSTEMS: SECURITY AND PRIVACY ISSUES**

**A THESIS SUBMITTED TO THE INSTITUTE OF
GRADUATE STUDIES
OF
NEAR EAST UNIVERSITY**

By

MAJED SALEH ABDULQAWI

**In Partial Fulfilment of the Requirements for
the Degree of Master of Science
in
Computer Information Systems**

NICOSIA, 2021

**MAJED SALEH ABDULQAWI: CLOUD, EDGE AND FOG COMPUTING
SYSTEMS: SECURITY AND PRIVACY ISSUES**

Approval of Director of Institute of Graduate Studies

PROF. DR. KEMAL HÜSNÜ CAN

**We certify that this thesis is satisfactory for the award of the degree of Master
of Science in Computer Information Systems**

Examining Committee in Charge:



Prof. Dr. Nadire Çavus

Committee Chairperson, Department of
Computer Information Systems, NEU



Assoc. Prof. Dr. Boran Şekeroğlu

Department of Information Systems
Engineering, NEU




Assist. Prof. Dr. Sahar Ebadinezhad

Supervisor, Department of Computer
Information Systems, NEU

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last name: Majed Saleh Abdulqawi

Signature: 

Date:01/07/2021

ACKNOWLEDGEMENTS

I would like to express my special appreciation and thanks to my advisor Assist. Prof. Dr. Sahar Ebadinezhad who has been a tremendous mentor for me.

I would also like to thank Head of my Department of Computer Information Systems, Prof. Dr. Nadire Cavus, for encouraging my research and for allowing me to grow as a research scientist. Your advice on both this research as well as on my career has been invaluable.

I will like to specially appreciate my family; my parents and my siblings; most especially my brother Dr. Ahmed for everything they continue to do to support me. Their love is immeasurable.

ABSTRACT

Cloud computing is an internet-based computing in which users pay for applications, storage, platform, computers, other services and networking on a pay-as-you-go basis from distributed shared servers. This study aimed to review the security challenges associated with the fog, edge and cloud computing systems.

This study is a qualitative research and systematic review that was done based on secondary resources in order to determine the security issues of the computing systems. Data for this study was obtained from secondary sources like journals, articles or from research databases. The newest security concerns for the Cloud system were discovered in this study as mis-configuration. Mis-configuration ranked as the top challenge in the Cloud Security Study, with more than 60% of businesses reporting it as their top concern. The possible solutions proffered by literature are two new IoT-layered models: basic and extended features with confidentiality, authentication and layer-recognition elements; Trusted Cloud Computing Platform (TCCP) which serves as a suite of technologies to address the issue of an un-trusted execution environment was also introduced to solve the security issues of the cloud system. The insecurities of data can be managed as edge and fog computing could supplant conventional cloud computing as far as possible in the future.

Keywords: Cloud, Edge, Fog, Security, IoT

ÖZ

Bulut bilişimi, dağıtımli ortak sunuculardan kullanıcıların uygulamaları, depolamayı, platformu, bilgisayarları, diğler hizmetler ve ađ oluřumunu anında ödeme yöntemiyle kullandıkları internet temelli bir bilişim aracıdır. Bu çalıřma sis, sınır ve bulut bilişimi sistemlerindeki güvenlik sorunlarını incelemeyi amaçlamaktadır.

Bu çalıřma bilişim sistemlerinin güvenlik hatalarını belirleyebilmek için ikincil kaynaklar üzerinde yapılmıř olan nitel bir arařtırma ve sistematik bir incelemedir. Bu çalıřma için gerekli olan veriler; dergiler, makaleler veya arařtırma veri tabanları gibi ikincil kaynaklardan elde edilmiřtir. Bu çalıřmada Bulut sistemleri için en yeni güvenlik endiřesinin hatalı yapılandırma olduđu keřfedilmiřtir. İřletmelerin %60'ından fazlasının en önemli endiřeleri olarak belirttiđi hatalı yapılandırma, Bulut Güvenliđi Çalıřmasında en önemli güvenlik sorunu olarak listelenmiřtir. Literatür tarafından sunulan olası çözümler iki yeni IoT-katmanlı modeldir: Gizliliđe, kimlik dođrulamaya ve katman tanımaya sahip temel ve geniřletilmiř özellikler ve güvensiz bir yönetim ortamı sorununu çözmek için bir güvenlik paketi görevi gören Güvenilir Bulut Bileşimi Platformu da (TCCP) Bulut sisteminin güvenlik sorunlarını çözmek üzere sunulmuřtur. Sınır ve sis bilişimin gelecekte konvansiyonel bulut bilişimin yerini mümkün olduđunca almasıyla veri güvensizlikleri kontrol edilebilir hale gelecektir.

Anahtar Kelimeler: Bulut, Kenar, Sis, Güvenlik, IoT

TABLE OF CONTENTS

ACKNOWLEDGEMENTS	i
ABSTRACT	ii
ÖZ	iii
TABLE OF CONTENTS	iv
LIST OF TABLES	vi
LIST OF FIGURES	vii
CHAPTER 1: INTRODUCTION	
1.1 Motivation.....	3
1.2 Problem Statement	3
1.3 Research Contribution	4
1.4 Organization of Thesis.....	4
CHAPTER 2: LITERATURE REVIEW	
2.1 Fog Computing	5
2.2 Edge Computing	8
2.3. Cloud Computing	11
CHAPTER 3: METHODOLOGY	
3.1 Data Collection	19
3.2 Data Analysis	19
3.3 Data Extraction and Mapping Studies.....	22
CHAPTER 4: RESULTS AND ANALYSIS	
4.1 Quality Evaluation	24
4.2 Results.....	24
4.3 Analysis.....	35
4.4 Research Gap	36

4.5 Graphical Representation of the Major Security Concerns of Cloud, Fog and Edge Computing Systems.....	38
CHAPTER 5: CONCLUSION AND FUTURE WORK	
5.1 Conclusion.....	39
5.2 Recommendations and Suggestions.....	41
REFERENCES	42
APPENDICES	50
APPENDIX 1: Similarity Report	51
APPENDIX 2: Ethical Approval Document.....	52

LIST OF TABLES

Table 3.1: Databases used for the systematic mapping study.....	21
Table 4.1: Results of study selection procedure.....	25
Table 4.2: Nominated studies for RQ1.....	26
Table 4.3: Security concerns of computing systems in IoT.....	27
Table 4.4: Nominated studies for RQ2.....	29
Table 4.5: Nominated studies for RQ3.....	31
Table 4.6: Nominated studies for RQ4.....	34
Table 4.7: Quality evaluation for the nominated studies.....	35

LIST OF FIGURES

Figure 2.1: Distributed data processing in fog-computing environment.....	6
Figure 2.2: Fog computing architecture.....	7
Figure 2.3: Cloud Computing	12
Figure 2.4: Cloud storage data security threats	18
Figure 3.1: Procedure of the systematic mapping.....	22
Figure 4.1: Security issues and solution for fog and cloud computing systems.....	38
Figure 4.2: Security issues and solution for edge computing system.....	38
Figure 4.3: Security issues and solutions for IoT computing systems (cloud, fog, edge).....	38

ABBREVIATIONS AND SYMBOLS

AWS:	Amazon Web Services
IT:	Information Technology
COVID:	Corona Virus Disease
CoAP:	Constrained Application Protocol
MQTT:	MQ Telemetry Transport
SDN:	Software Defined Network
IoT:	Internet of Things
MCC:	Mobile cloud computing
CDNs:	Content delivery networks
DoS:	Distributed Denial-of-service
IaaS:	Infrastructure-as-a-service
PaaS:	Platform-as-a-service
SaaS:	Software-as-a-service
DNA:	Deoxyribonucleic Acid
LAN:	Local Area Network
PACs:	Programmable Automation Controllers
TDOS:	Temporary Denial of Service
TCCP:	Trusted Cloud Computing Platform

CHAPTER 1

INTRODUCTION

Cloud is comparable to the Internet, and cloud computing consists of cloud graphics which formerly were utilized for the purpose of illustrating the networks of telecommunications and depicting the internet after (De Filippi & McCarthy, 2012). A web-based system of computing is referred to as cloud computing. This computing system ensures that customers are able to 'pay by pay-as-you-go' from the servers that are shared while distributing them. Applications, machines and storage are also shared among other web services. Cloud infrastructure is a paradigm for making available customizable computers such networks, servers, store, software, and services on demand and may be delivered rapidly and without maintenance or service provider participation. The cloud computing paradigm provides all information that the digitized system has to give. Without prior know-how on the management of the resources required, users are able to access services via the "Internet Cloud." Users may then fully focus more on their primary business operations instead of exhausting their time with the management of their business processes. The ideal cloud computing platform makes an efficient utilization of resources; it is flexible and highly available and accessible.

The work is done remotely from everywhere, and this technique has been in use with some of the major business companies for years, but the real benefit or value came in March 2020, when workers all over the world were required to stay at home because it was the only way to prevent the epidemic from spreading. The pandemic changed all aspects of life at any stage, and the culture of business was no different, but cloud-based companies and capabilities were able to maintain this dramatic transformation in the workplace when they had the remote working approach in effect. Not only a few but several firms began to exploit the advantages of cloud adoption in this pandemic, and the majority of the companies began to realize that cloud capabilities are a workaround. The pandemic of Covid-19 has forced government officials to close schools and universities, forcing students to

learn at home through virtual means. Ferri et al. (2020) stated that in the aftermath of the pandemic, educators have allowed virtual solutions for teachers and students by introducing virtual solutions such as Microsoft Teams, which not only offers video-enabled remote classrooms but also a forum for studying and sharing documents and assignments according to age ranges. Teachers will build a stronger bond with their students using these platforms. It is an easy way to take online classes from anywhere, and videos can be used to revisit the material learned in a live online class if necessary.

The cloud allows one to visualize data from wherever and helps the user to avoid having to be in the same location with the data storage unit which normally is a requirement in conventional computer set-up. The hardware that contains your data through the cloud will not be needed to be at the same physical location. The users' cloud provider however, might own and maintain the hardware and software needed to run your home or business apps. This is of huge advantage to small businesses and firms who are lagging in terms of storage and hardware as compared to the bigger firms. When small businesses save their data in the cloud, it allows them to also save money, likewise helping them to avoid the risks of acquiring and maintaining memory devices. Clouds can be according to one's needs and can also be subscribed to accordingly. Cloud can be utilized as public service for example in educational institutions, it can also be utilized for private use at home or for a private company. More classification is depicted below.

- a) Cloud which is public- This can be used by any subscriber that has an Internet connection and cloud connections.
- b) Cloud which is private – This can be used by a single company or organization created with the access of the cloud system only available to the user.
- c) Collaborative cloud – A cloud which is utilized by two or more cloud-based enterprises.
- d) Cloud which is Hybrid – This can be used by the public, firms and groups of firms. A minimum number of two clouds are combined in this.

1.1 Motivation

The buzz of the Information Technology (IT) sector nowadays is cloud computing and, in the cloud, computer resources such as the software, storage, and even infrastructure may be accessed on demand. Jiménez- Martínez (2013) mentioned that Cloud computing has been around for decades but with the existence, there has been technological advancement to one that is now of millions of dollars. A highly competitive cloud computing system supply industry was established by the flood of new technologies and analysts believe that cloud will continue to be sought after in companies as years go by. There are significant economies of cost and greater productivity opportunities and it will be hard to overlook the influence of IT outsourcing on third parties with the demand on the market will be quite strong, with huge profits. Cloud computing systems allow for work to be done from home and with the COVID situation in the world, working remotely is an essential part people's life nowadays. The cloud computing systems have been known for the insecurities that the systems are vulnerable to such as; data loss, lack of privacy (Kaur & Kaushal, 2012). It is important that the effective measures are put in place to tackle these security concerns to enable the global population to be able to make safe and appropriate use of the computing systems. Hence, the aim of this study to review the security challenges associated with the fog, edge and cloud computing systems.

1.2 Problem Statement

Ferri et al. (2020) stated that since the world was struck by the Covid-19 pandemic, many industries have migrated to the cloud or are preparing to do so vigorously. There are a number of reasons why cloud computing is an irresistible technology that provides the only way to access IT applications and systems. It has emerged as a new critical driver for Enterprise Organizations seeking to transform into Digital Organizations (Dibbern & Hirschheim, 2020). Remote working is also a normal occurrence in all IT firms, with facilities available at all times. Cloud networking has supplanted traditional data warehousing and distribution platforms. Data storage in the cloud, on the other hand, comes with its own range of problems and security issues. Furthermore, Shi et al. (2016) said as the amount of data provided

by each computer grows, the conventional cloud computing approach is no longer successful in dealing with issues such as high latency, bandwidth constraints, and resource constraints. Zhang et al. (2019) stated that, modern technological paradigms such as edge and fog computing have been proposed to address the former's problems at or near the computer. All of these paradigms bring computation and memory management closer to the device. However, no system is flawless, beyond its benefits and given the security concerns on data loss, concerns with data confidentiality/privacy (Kaur & Kaushal, 2012). This study will review the security concerns of Cloud, Edge and Fog computing systems while proffering the possible solutions to them.

1.3 Research Contribution

This research will contribute to creating awareness about the security concerns of the computing systems. There have been some researches on the various security concerns of the cloud computing systems but few researches have talked about the edge and fog computing systems in terms of their security issues. This research enhances the investigation with possible solutions being proffered and as well pave way for more research to be done regarding them.

1.4 Organization of Thesis

Chapter 1: This is the introductory chapter of the research and it entails some background information on cloud computing especially during this pandemic time, the statement of problem of the research and the contribution of this research.

Chapter 2: This is the literature review where the extensive explanation is done regarding cloud computing, edge computing and fog computing.

Chapter 3: This is the chapter that comprises of the research methods for the study investigation.

Chapter 4: The analysis of the data collected from secondary sources is done in this chapter

Chapter 5: This is the concluding chapter of the study.

CHAPTER 2

LITERATURE REVIEW

Cloud, fog, and edge computing are more than buzzwords; understanding what they mean is critical when designing and executing an organization's infrastructure needs. This requires, of course, the critical application of database technologies. Casino et al. (2019) explained that data from IoT and sensing instruments is sent to remote cloud data centers for research (fusion, storage, and processing). As there are many features attributed to cloud, fog and edge computing that can be explored such as application and security. This research will focus on the components of each of the computing systems, the challenges faced in terms of security and privacy issues and as well proffering solutions to these problems.

2.1 Fog computing

Fog computing is seen as one of the most promising paradigms in computing lately, which performs the task of extending cloud computing to the network's edge (Mukherjee, et al., 2017). Therefore, the desire to reduce the distance at which data travels over the network, gave birth to edge computing, hence, data is handled at the cloud edge. Mushunuri et al. (2017) furthermore explained that edge computing is characterized by closeness to zone geographical distribution, end users, and high support for flexibility and value addition to IoT customer services

Fog computing is usually an enabler of computing services and applications for numerous devices connected directly at the network edges. The devices of fog are typically in a form of a set-top-boxes, road side units, access points, cellular base stations and end devices (Zhu, et al., 2013). The technology was presented and developed by the year 2012 hasten and secure the connectivity from center of the data and the devices end, in order to ensure user's privacy and safety on the network (Rahman & Chuah, 2018).

2.1.1 Characteristics of Fog

Fog computing is characterized by data processing components, which run in a decentralized edge and cloud devices. It enables the design and management of networking, computing and storing facilities between end devices and data-centers.

Also, it is considered as a supporting technology for user’s agility, interface heterogeneity and resources, and decentralized data analytics, in order to ensure low latency in broadly decentralized applications (Dastjerdi & Buyya, 2016). These are clearly explained in Figure 2.1.

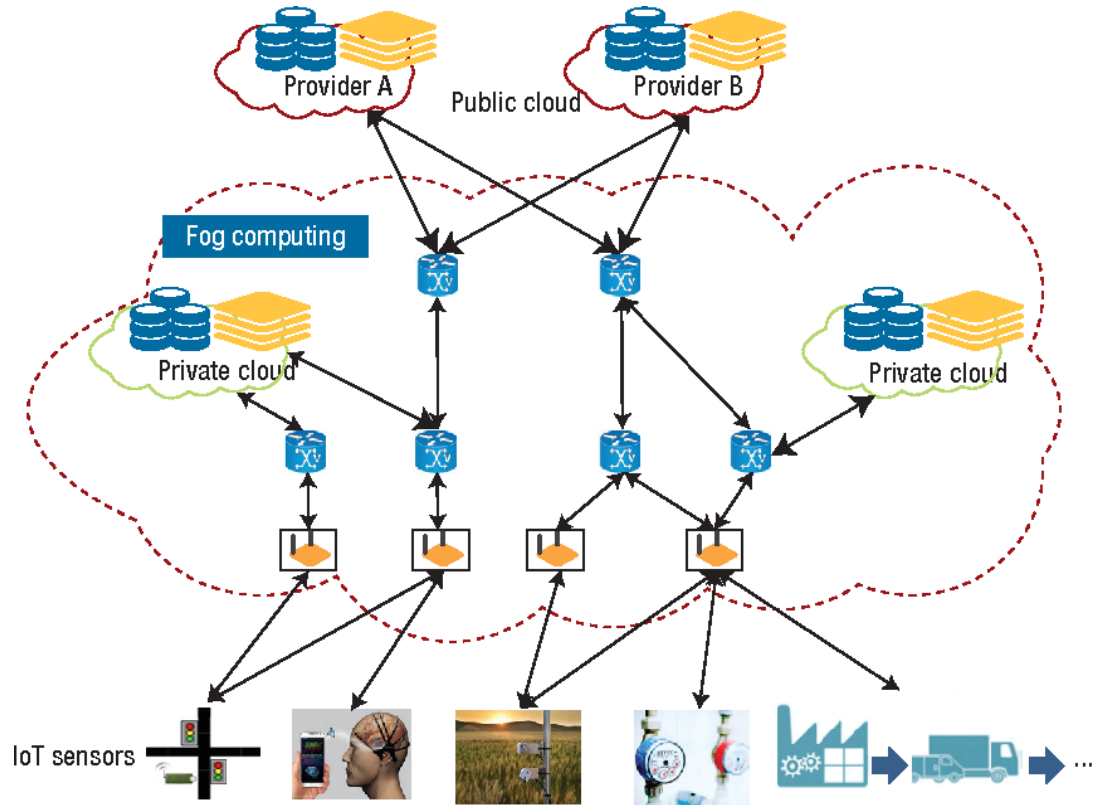


Figure 2.1:Distributed data processing in fog-computing environment
(Dastjerdi & Buyya, 2016)

2.1.2 Components of Fog

The systems of fog are animatedly used and discovered APIs in forming composite functionalities. The information resources from the monitoring services are used by the components at the management layer resources in pursuing the state of availability of cloud, fog and the network’s resources, aimed at identifying the most suitable applicants to carry out the processing of the subsequent received task (Dastjerdi & Buyya, 2016).

With the use of multi-tenant applications, the management component of resources will certainly give priority on the tasks of various contributing programs or users.

Therefore, the resources of cloud and edge establish communication by employing the standards of machine-2-machine like constrained application protocol (CoAP), formerly MQ Telemetry Transport (MQTT) and SDN (software defined network). Al-Fuqaha et al (2015) said the protocols employed go a long way to help in margining the mixed networks in fog computing. These are also fully detailed in Figure 2.2.

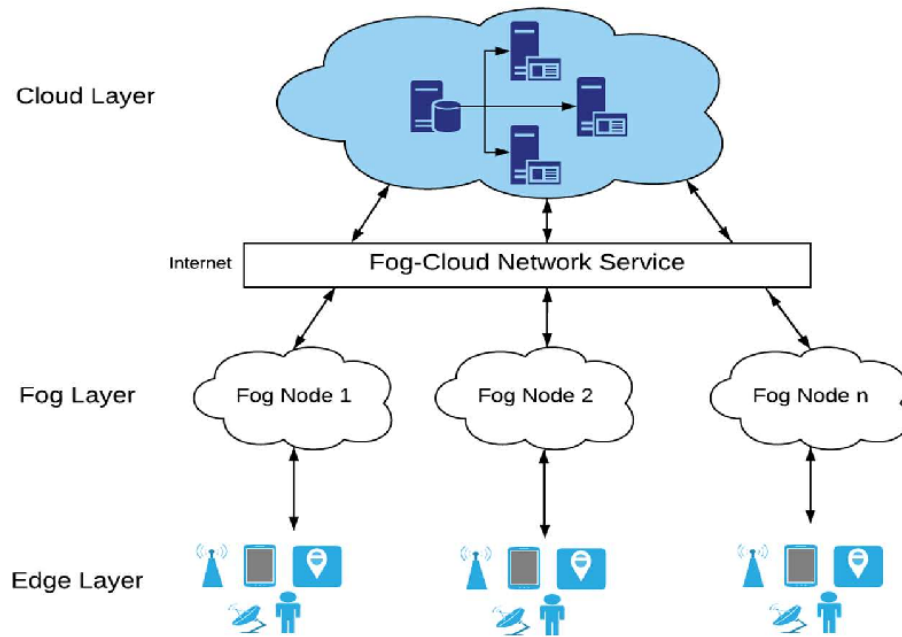


Figure 2.2:Fog computing architecture (Neware & Shrawankar, 2020)

2.1.3 Fog-Computing Software Systems

Fog computing has four majorly known software systems that are used in building the fog application and environment namely:

- Cisco IOx: it enables management of resources and enhances services of machine-2-machine within the environment of fog computing.
- Cisco Data in Motion (DMo): It's a software which enables the management of data plus analysis within the network edge, which by extension is made into systems provided by Cisco and its co-partners.

- Local Grid's: it enables dependable communication of machine-2-machine between data processing and devices without profiting through the cloud.
- Cisco ParStream: It enables IoT analytics in the platform of fog.

2.1.4 Fog Computing Existing Issues and Recommended Solutions

Fog computing, also known as fogging, is a cloud architecture that uses an intermediary layer between the data source and the cloud, analogous to edge computing. It is achieved at fog nodes that gather data from different edge devices in fog computing.

Some privacy and security issues of fog computing by Parikh et al. (2019)include;

1. Network Visibility is Restricted
2. Ineffective threat prevention practices

Some of the solutions that will be proffered by this research to solve these issues include;

- a) Data encryption
- b) Monitor for virtual machines

The existing issues and concerns attributed to Fog, Cloud and Edge computing will be explored in detail in this research study across the chapters.

2.2 Edge computing

The production of data at the network edge is increasing, hence, the need to process data at the very network edges is necessary. Services such as cloudlet, datacenter and fog computing were presented to the community, in that, data created at the edge of the network is always insufficient to be processed by cloud. Shi et al. (2016) explained that the desire to reduce the distance at which data travels over the network, gave birth to edge computing. Thus, edge computing is therefore characterized by closeness to zone geographical distribution, end users, and high support for flexibility and value addition to IoT customer services.

Edge computing is seen as an enabling that allows data computations to be carried out at the network edge, downstream data in-line with cloud services and upstream

data which goes with the services of IoT. Satyanarayanan et al. (2009) mentioned that edge computing is defined as the network resources and computing beside any route between the data-centers of cloud and data source. For instance, the edge of a smart phone exists between the edge of a cloud and the body centric communication. Similarly, the edges in a smart home, exist between the edge of home appliances and the cloud.

The main foundation of edge computing is actually the computing that happens within the surrounding data sources.

2.2.1 Mobile edge computing

The concept of Mobile cloud computing (MCC) shares some features with mobile edge computing. The most significant aspect that exists within MCC is that the power of the computing is situated only somewhere within the cloud, which produces the latency transmission, where it serves as a deterrent for mass services (Mäkinen, 2015).

At the moment the mobile edge computing novel and industrially driven, researches have shown the offloading of the computation for VoLTE for the utilization of servers, aimed at reducing the power consumption (Mäkinen, 2015).

2.2.2 Emergence of edge computing

The origin of root computing is traced back to the mid-1990s; this happens when Akamai presented a content delivery network (CDNs) aimed at increasing the speed of Web performance. Hence, the CDNs employ the usage of nodes within the proximity of edge to cache web content and pre-fetch. The nodes of the edge are used for the customization of content in performing, like adding relevant-location, advertisement. Satyanarayanan et al. (2009) explained that though CDNs are more relevant for video content, but edge computing extends and generalizes the relevance of the CDNs in the leverage of cloud computing infrastructure.

Bonomi et al. (2012) introduced fog computing to denote decentralization of the cloud infrastructure. This is driven from the scalability of IoT infrastructure, rather than the interactive performance of mobile applications. In addition, the study

predicts the stretching of fog nodes hierarchy of several levels from IoT to cloud edge devices.

2.2.3 Why proximity of the edge computing matters

The importance of the nearness as days keep pushing is becoming undoubtedly very clear. Therefore, the unified connectivity presented by the internet has definitely attracted the users to disregard the physical proximity. Thus, the physical proximity directly affects the latency of end-to-end, the band width of viable economy, trust establishment and survivability. The importance of the proximity is as follow:

- Highly responsive service of the cloud
- The edge analytics via scalability
- Enforcement of primary-policy
- Masking of cloud outages

2.2.4. The benefits of edge computing

The key relevance of edge computing is to place the computing closer (proximity) to the sources of the data. By doing that, the benefits of edge computing cannot be compared with the old-style computing paradigm of cloud-based. Yi et al.(2015) have it that, by adapting the modern edge, from cloud to edge the response time is significantly reduced from 900 to 169 M/S.

Ha et al. (2014) mentioned how the response time is reduced when cloud outlets are used in offloading computing tasks for the wearable cognitive assistance. The results of the findings indicate that, the response lies between 80-200MS of time also, the consumption of energy can also be put down by 30-40%.

2.2.5 Edge Computing Existing Issues and Recommended Solutions

The data provided by smart devices or sensors is stored in the system itself or closer to the device in an edge computing paradigm, rather than being submitted to the cloud. Hamdan et al. (2020) mentioned that it is preferable to conventional cloud computing because it allows for real-time data processing with no latency.

Some of the security concerns attributed to Edge computing according to Parikh et al.(2019)are that:

1. To steal user data, a malicious user will mask their identity and control the network.
2. DoS (distributed denial-of-service) attacks
3. A data tampering attack, in which a hacker alters data sent during conversation or data stored on a computer.

The following solutions are some that are proffered to tackle the challenges faced in security and privacy in Edge computing.

1. Have the same degree of protection to all edge nodes as the network.
2. The user would be provided with continuous network control and visibility with an integrated interface.
3. Data encryption and access authorization

2.3. Cloud computing

According to Mushunur et al. (2017), due to the explosion of internet of things (IoT), problems such as computational capacities on sensing devices became very low, limited memory and storage capacities and huge gap between execution and response (latency).

However, these problems can be overcome by employing cloud computing. This is because it offers scalable hardware resources on demand for storing and computing data. In the account of Mushunur et al. (2017), this minimizes the computational load on network devices and increases their battery lifetime.

Cloud computing is seen as a model which enables a continuous demand of access to network aims at sharing turns of computing resources that are configurable like server, networks, storage etc. which are worthy to be provided fast and equally released with less effort of management or even the interaction of service provider (Mell & Grance, 2009).Cloud computing with regards to IT has rapidly grown in terms of various services. There are three categories of cloud computing.

- Private cloud: is an infrastructure of a cloud used purposely for the service and management within an organization.
- Public cloud: is an infrastructure of a cloud, designed purposely to service participants and members, which is an open system meant for public use.
- Hybrid cloud: is an infrastructure of a cloud between a public cloud and private cloud. Which is mostly managed by the host organization.

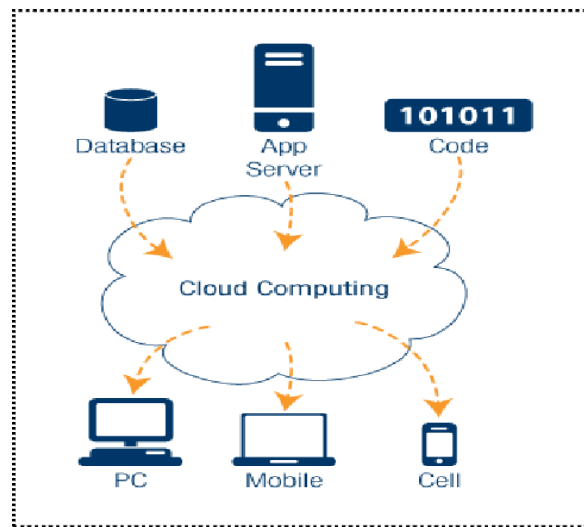


Figure 2.3: Cloud Computing(Trivedi & Suthar, 2013)

2.3.1 Overview of cloud computing: Cloud Service Models

Based on the theory of virtualization and SOA, all other things within the environment of a cloud are seen as a device such as hardware as-a-service, database-as-a-service etc. Therefore, all other services of cloud are categories into three main classes:

- IaaS (Infrastructure-as-a-service) clouds: these provide all the services related to hardware like storage, firewalls, network etc. and other resources of computing. Therefore, it has ever growing control over cloud infrastructure. Alhamad et al.(2010)stated that the services of IaaS are always rooted from PaaS and SaaS clouds.
- PaaS (Platform-as-a-service) clouds: it provides a platform that enables for users for the development of their desired application via programming tools that's predefined, settings and PaaS providers that are supported. Thus, a PaaS user can

essentially use the PaaS remote cloud as a locally configured computer without managing any of the settings of hardware.

- SaaS (software-as-a-service) clouds: it provides the users with the applications developed in line with the infrastructure of cloud and its platforms. These applications are accessed by the users using different interfaces, which are mostly and commonly developed using web –based applications within the environment of a cloud.

2.3.2 Cloud-based Real-time Collaboration Service

In order to provide coloration of cloud-based services in real-time, which are integrated through means of communication. Jeong et al.(2013)said the services are connected to the concerned staff in the course of task processing in real-time without much delay, to allow decision making in real-time.

2.3.3 Review on Cloud Data Security

In a cloud storage environment, Atiewi et al. (2020) abstracted an IOT based multi-factor authentication and lightweight cryptography encryption scheme. IoT devices are divided into two categories: sensitive data and non-sensitive data. To maintain high confidentiality, confidential data is broken into two sections, each of which is encrypted using different encryption algorithms (RC6, Fiestel) and stored on private cloud storage. When non-sensitive data is stored in the public cloud, it is encrypted using a single algorithm (AES). The trusted authority ensures multifactor authentication. Using IP addresses, passwords, and biometrics to identify users.

Shahid et al. (2020)proposed a modern data protection system with less complexity, based on a distributed storage concept that divides data into sensitive and non-sensitive parts. The data designated as usual is encrypted separately and saved in a single server, but the confidential data is designated as a dual component and is encrypted separately and stored in a separate cloud. The suggested strategy protects against the following attacks: linked main attacks, man-in-the-middle attacks, and contamination attacks.Chang et al. (2020) developed a cancelable multi-biometric solution by combining a fuzzy extractor with a novel bitwise encryption scheme to

produce cancelable biometric models. The biometric template safety scheme is defined by irreversibility, renewability, and precise biometric scene recognition. In the retained template, the scheme that protects against additional noise by using bit errors is implemented.

Wang & Su (2019) proposed a new encryption method for audio which dispenses reliability state high. Preliminary value that presents in chaotic controlled by hash value on the audio and then making unpredictable chaotic trajectory, DNA coding is used to mystify and scatter the data (audio). Encryption scheme is used for single and dual format audio.

The 2D chaotic structure suggested by Zheng & Liu (2020) is a combination of sine maps and logistic maps. The sine map is the product of combining two unstable maps. Now, a new encryption scheme for dynamic DNA encoding and decoding has been developed. The security tests accomplished with this algorithm are key critical, histogram, and correlation analysis. For an image cryptographic algorithm, Zhang & Li (2020) used a neuron-like scheme, masking operation, and flipping operation. The neuron-like learning scheme is used to find a catchy scattered scheme and run the plaintext-based image encryption algorithm. To control image information, the mechanism receives input and weights from the neuron via the feedback action. Finally, the encryption algorithm used to disperse the image data results in a high level of protection and adaptability. The hash value was improved and used in the plain image during encryption, making it impossible for intruders to use a special plain-image attack. Simple picture correlated DNA order progress is more reliant on hashed data in DNA encoding and decoding schemes. Poon & Miri (2017) used Bloom filters based on word quest in their abstracted methodology. It adopts versatility through the use of n-gram filters. It enables phrase search to run indefinitely without the need for an initial progression of conjunctive keyword-based searches to find user files.

Chen et al. (2019) explained that any critical information on the mode of transfer may be intruded by an identified attacker and to solve a problem by encrypting data before sending it to a cloud storage service. Hidden transmit mode and multi

authority factor is planned to secure the hidden encryption password. First, the user breaks a secret password, which encrypts sensitive files into trivial bits, and then the user conceals the hidden password parts using their own key and biometrics. Pammu et al. (2019) also suggested a multi-core processor matrix transition, focusing on authentication and concurrent encryption. It helps to allow high efficiency, understanding and stable AES construction in the chain mode. The new password is introduced to secure those who choose to use a symmetric key algorithm for the development of the negative, encrypted password from a password to hashing, hashing and password and it is assumed that the strategy is safe from the assault of the search Table.

To stop anonymity, Lin (2019) addresses user pre-authentication and post-authentication. The administrator of this scheme assists the user in creating a pseudo persona that is known to the user. By registering as a pseudo identity administrator in cloud servers, it is possible to check the user's authentication of the requesting client. This method is very effective in locating the illicit customer. This security feature allows for fast error detection and password updates when offline. Song et al. (2019) developed a novel key substitution encryption algorithm that uses an advancing key to update the starting keys, implements a simple picture, and develops another substitution scheme that encrypts various categories of pictures. It aids in overcoming the low security and computing costs of using single round encryption alone, as well as the proposed replacement approach based on s-boxes for various image encryption categories.

The algorithm proposed by Zhang et al. (2019) used image hashed data to improve parameterized value of chaotic maps by a frequentative advancing feature of matrix, which increases the correlation of key with original image. The DNA coding and decoding process is processed to generate some kind of order by chen's chaotic structure for some order encryption. Finally, they solve counter statistical attacks, noise attacks and crop robustness, vulnerability to the plaintext, and differential attacks.

Guo et al. (2016) proposed a new encryption concept and its implementation, such as distance-driven encryption for internal result encryption, which is appropriate in terms of private key and cipher text size. Here is where the current encryption concept comes into play. In the encryption process, a biometric scanned private key is used to generate an encrypted cipher, and in the key generation phase, another biometric scanned private key is used to decipher an encrypted key. When the algorithm notices the two biometric transits are exactly the same.

The most efficient multiple verification transaction suggested by Niet al. (2014) would rely on the distribution along with the parallel mechanism. They have a timid protocol, and any active adversary will get into cloud storage. During the auditing process, the auditor can detect randomly changed cloud data. Role dependent encryption is a system suggested by Zhou et al. (2013) that incorporates cryptographic principles, with role-based access control (RBE). They offer a secure RBE-based cloud storage environment that allows a company to store documents on public storage while saving sensitive information on private cloud storage.

A devised a multifactor authentication-based user-dependent data backup scheme was created by Liu et al. (2016). The user has a symmetrical key and has split it into three actions. Remove the key at last. To access the files, you can easily rebuild the key by combining user share in your smart card, pen drive, notebook, and so on. The login and biometrics for the recovery process are missed or damaged on a laptop and smart card. Zhang et al. (2017) proposed a scheme to function or strengthen batch validation in conjunction with a data dynamic operation procedure, and in the proposed system audition is at most necessary to test message validity code tag for validation. It is supported by several validation works, and in the auditor side this approach ensures that the main encryption keys are protected while the AES algorithm is executed on open-source devices and depends on the key relay S-box extension. S-boxes act as a key extension, and they are extended on all round keys. S-boxes are used to protect from well-known white-box threats.

Liuet al.(2016)addressed the use of two-factor authentication to protect data in a volatile cloud storage environment. Here, encrypted data is sent from sender to receiver through the cloud, but the decryption process is handled by two keys: the first is private, and the second is public. The 3 layers of DES, suggested by Tang et al. (2018)along with its network coding, focus on the partial main updating tasks carried out in low complexity and which improve the adaptability of the various cyber environments. Asymmetric cryptography necessitates a significant volume of computing and storage, according to Howe et al.(2016). The elliptic curve cryptography is used to reduce power consumption, improve computer speed, and ensure safe communication, especially when the message is encoded in an elliptic curve.

Nguyen &Turitsyn(2015) suggested a new statistical “robust stability” criterion to judge small-signed stability of operating points. It helps to ensure the reliability of the operating point mathematically at every few load links. RSA is effective in confirming the solidity of its capacity without specifying several load responses. The excluded user is permitted to obtain an unapproved file, and the attack algorithm desires to convert cipher-text existing-version to older-version in order to trick the cloud storage provider into obtaining sufficient cipher test updated keys. These bugs will be essentially avoided in the DAC-MACS system, and cryptographic keys will be used to authenticate procedures within institutions broadcasting, improving transfer security. They investigated the feasible relation between energy consumption and runtime phase and eventually concluded that the ECC algorithm used less energy than the RSA algorithm. Mitchell (2016)opposed the van oorstch-wiener attack, which employs a range of keys to generate both ciphertext and plaintext sets. They argue that an 80-bit security key is preferable to a 56-bit security key. The primary adjustment at frequent intervals tends to reduce the effect of active threats, but it does not eliminate the risk of victory.

2.3.4 Cloud Computing Existing Issues and Recommended Solutions

Considering its many capabilities, the cloud's stability remains one of its most critical prospects. Each cloud infrastructure has its own set of privacy and security

issues. In the account of Butpheng et al.(2020)the security staff examines the architecture for bugs and possible attacks to hack it for cloud security and safety.

Some of the security issues faced in cloud computing according to Parikh et al.(2019)include:

1. Unauthorized access to classified information.
2. A malicious person in the system steals data from the system.

Some solutions for these security issues include;

1. Keep watch on the network.
2. The installation of firewalls.

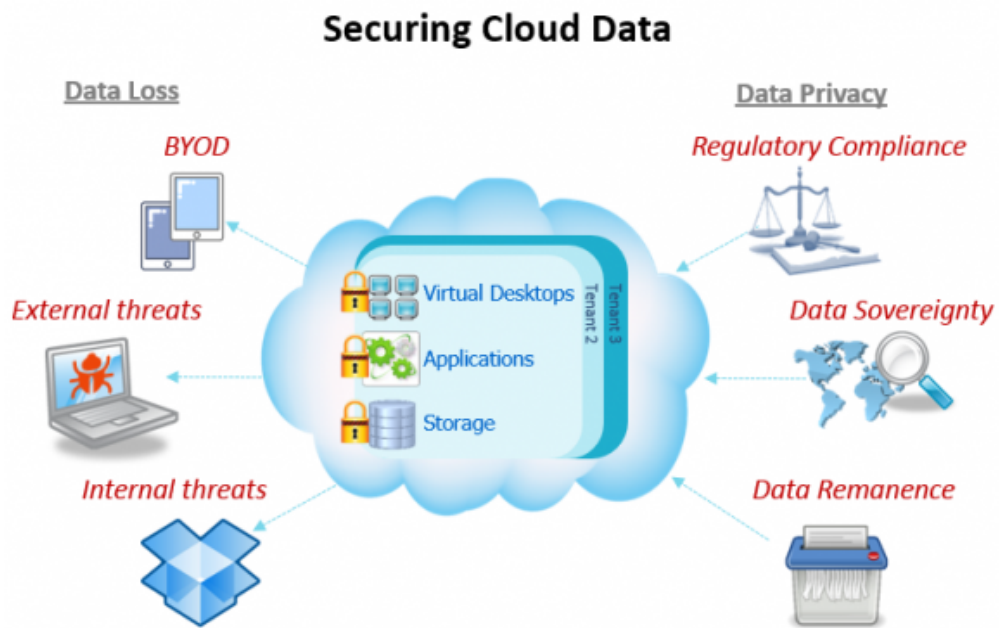


Figure 2.4:Cloud storage data security threats(Umapathy & Kalpana, 2020)

CHAPTER 3

METHODOLOGY

The introduction of technology such as IoT and 5G ushered in a modern technological era known as cloud computing. Cloud networking has supplanted traditional data warehousing and distribution platforms. Data storage in the cloud, on the other hand, comes with its own range of problems and security issues. Edge and fog computing are two new technological paradigms proposed to address the former's issues pertaining to the computing system. These systems make a provision for the management of computation as well memory/storage management that are related to the computer. Despite their benefits, no technology is flawless, which is why it's critical to look at the security problems that concern edge, fog, and cloud computing.

3.1 Data Collection

Data for this study is gathered from articles and conferences based on research reliable databases such as Springer, IEEE, Science direct, Scopus and ACM digital library. This research is conducted based on the range of 2010 to 2021 in order to seek for the recent challenges and solutions. The important keywords that were searched were “security in cloud computing”, “security in fog computing”, security in edge computing”, “issues and challenges” in this context and the “existing solutions” so far.

3.2 Data Analysis

For this systematic review, the author ensured the careful planning and allocation of tasks at each stage of the study. Narrative analysis is done based on the data that obtained from related sources. The systematic mapping study is a valuable tool for both academics and specialists equally. A mapping study specifies a graphical demonstration of domain of work in a certain regulation. Systematic mapping study encompasses repeating a process for inferring and expounding accessible resources, in line with a study objective. This important process includes describing the research question and defining the review scope as it shown in Section 3.2.3. Next is selection the articles to choose the significant ones and key wording the abstract

of the articles, with the aim of forming a categorization system. Finally, the last step focuses on exploiting the data, which eventually leads to generating the systematic map. At each phase of the procedure there was a result which was filtered for enhancing overall outcome of this systematic map.

3.2.1 Definition of Research Questions

The aim of a systematic map is to deliver more understanding into the quantity and type of work being conducted in a particular discipline. It may also be necessary to know the places where such work was published. This challenge said in distinguishing the suitable research questions to use for this research. The following questions will be answered in this study.

RQ 1) What related researches have been conducted (what was their evaluation and novelty on the computing systems)?

RQ 2) What is the orientation of previous studies on the security issues in terms of Data Privacy/Confidentiality and Data Loss/Leakage?

RQ 3) Which of these computing systems has been identified by literature to have the most security concern?

RQ 4) What are the solutions that have been proposed by researchers with consideration of the identified security issues?

3.2.2 Conduct of Research for Primary Studies

In order to collecting papers for this research, five main digital libraries were utilized on the basis of their impact factor of conferences and journal publication. Table 3.1 includes the digital libraries and their related uniform resource locator (URL).

Table 3.1: Databases used for the systematic mapping study.

Digital Databases	URL
ACM	Portal.acm.org
IEEE	ieeexplore.ieee.org
SCOPUS	www.scopus.com
SPRINGER	www.springerlink.com
SCIENCE DIRECT	www.sciencedirect.com

The searches were executed on the digital database, which contains applying the intended search string above on document metadata to assure the incorporation of important articles. For this study, findings from relevant databases relating to cloud computing and computer science were utilized, and an overall of 39 papers were applicable to be included out of a fundamental containing of 508 papers. This study covered the period 2010 – 2021.

3.2.3 Screening of Papers for Inclusion and Exclusion

The significance of selection benchmarks is recognizing and including all papers related to this research. This was a fundamental feature of the study. It was vital usage the inclusion and exclusion conditions for eliminating unrelated articles in regards to cloud, fog, and edge/security. In addition, the criteria were applied in eliminating all resources not offering solutions to the research question. Generally, some abstracts state only one perspective of the study concentration without additional details which are excluded from the selection. Moreover, prefaces, panel discussions, presentation slides, tutorials and summaries are excluded in this research. It was relevant to contemplate articles that not only had the focal concentration but also offers some secondary details. The central emphasis of this research was finding solutions for security issues in terms of Data Privacy/Confidentiality and Data Loss/Leakages it relates to cloud, fog, and computing.

3.2.4 Keywording of Abstracts

Keyword of abstracts is an essential procedure in any systematic mapping and used for designing the categorization system of the analysis and encompasses the subsequent phases as indicated in Figure 3.1.

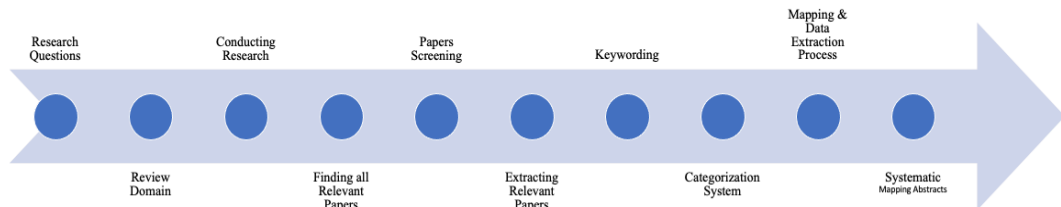


Figure 3.1: Procedure of the systematic mapping.

Using key wording in reducing the compulsory period to design a categorization system was applied for security issues in cloud, fog, and computing. Moreover, key wording guaranteed that only the substantial studies were contemplated in the layout of the research. The abstracts were reviewed for extracting hypotheses and keywords linking to the attention of this study. Thus, the combination of keywords from several publications are utilized in order to provide adequate knowledge about the research contribution. This was ultimately applied in specifying the evidences or classifications of the study.

Finally, a cluster of keywords were utilized in this study to specify the classifications and the ultimate systematic mapping. In this research, three classifications facts concentrated on topics which are entirely aspect of the study title, the sorts of contributions in terms orthometric, process and method; research styles like validation and evaluation.

3.3 Data Extraction and Mapping Studies

Related articles were arranged into a categorization scheme at the key wording step. This next stage permitted data extraction from the initial studies. Data extraction technique formed the main character of the categorization system. The process for data extraction was attained on Microsoft Excel tables. The Excel tables comprised from the several sets of the categorization system. The publications frequency in all class was obtained to diverse tables and was merged into a table either contenting the topic/contribution category or the topic/research category. The

analysis was attentive on displaying the occurrences of articles on the basis of the entries from diverse Excel tables. The substance was recognizing security concerns and issues that relates to cloud, fog and edge computing were specified more importance in this research. Therefore, gaps determination is enabled that eased to detect sphere for further study. Based on the outcome obtained from the Excel tables, helped organizing the articles frequency.

CHAPTER 4

RESULTS & ANALYSIS

4.1 Quality Evaluation

To assess studies the following questions are defined:

QE1) Does study match with presence of the concentration of research in security for Cloud Computing?

QE2) Does study report illustrate how to face securely unpredicted risks and motivate proper counter action to reply to latest threats?

QE3) Is it feasible to prevent indicating all the demeanor in advance for Adaptive and Autonomous Security?

QE4) Does suitable security develop a precedence for establishments contracting with a cloud computing provider?

QE5) Does study offer assurance to the users of cloud computing security?

The weights of assessment are: Y (Yes) = 1, P (Partially) = 0.5 and N (No) = 0 or Unknown while information is not clearly specified. This research is assessed every article and if there is no agreement in scoring, it is reviewed sufficient for reaching agreement.

4.2 Results

The results of our selection technique are illustrated in Tables 4.1 where searching results in all databases are specified, except, some of the researches were redundant in more than one online database. Therefore, concluding number of unique studies nominated for this study review which was notable after removal of redundant articles.

Table 4.1: Results of study selection procedure.

Database	Search results	Nominated studies
IEEE Xplore	130	10
Scopus	270	12
ACM	45	4
Springer	57	11
Science direct	6	2
Total	508	39
Redundancy		22
Final Nominated studies		17

RQ 1) What related research has been conducted (what was their evaluation and novelty on the computing systems)?

Fog computing and edge computing are used interchangeably, according to Parikh et al.(2019), since they all require an intermediate stage of computation and storage. The Local Area Network (LAN) serves as a portal in fog computing. On the other hand, the edge environment is where smart technological devices are employed for computing purposes. An example of the devices includes; Programmable Automation Controllers (PACs). There is research that can be performed to reduce latency and bandwidth requirements much more without jeopardizing the system's protection. Since setting up the machine with all of the specifications, it should be able to operate on its own.

Yi et al.(2015) carried out research stating that the fog computing system is still young and requires much more research, more improvements and enhancements for its security concerns. The research also mentioned that fog has been chosen as the IoT's framework and given that fog is an extension of cloud computing, the system is given an inheritance of cloud's protection and its concern for security. While some issues can be overcome using existing methods, others pose new challenges due to fog computing peculiar features, such as the heterogeneity of fog nodes and fog networks, and the need for mobility assistance. The prevalence of wireless in

the fog system has made it a realization that tackling security of the network is paramount.

Francis & Madhiajagan (2017) explained that fog computing allows users to run cloud operations at places near to their point of interest. To run tasks, it uses existing networks and routers in neighboring areas, much like the internet. These technologies are compared to clone cloud and digital off-loading processes that are already in use. Clone clouds are divided into various forms of augmentation techniques, restricting the amount of cloud services that can be used. Recent cloud approaches are appropriate for users with minimal access challenges, and clone clouds are appropriate for making the most of cloud services. Table 4.2 shows some related research on cloud computing.

Table 4.2: Nominated studies for RQ1.

ID	Author(s)	Year	Research Title	Orientation
N1	Yi et al	(2015)	A review on fog computing security and privacy concerns	The fog computing technology is still in its early stages, and it would take a lot of testing, upgrades, and updates to address security issues.
N2	Mohan, N., &Kangasha rju	(2016)	Edge-Fog Cloud: Internet of Things Computers distributed cloud	Fog is a cloud storage extension; the framework inherits the cloud's encryption and privacy. There are usually a large number of smart sensors on the Internet that capture environmental information and share it with a cloud provider. A number of architectural abstractions, including Fog and Edge, were suggested to locate any processing close to the sensors and far from the central cloud servers.
N3	Francis &Madhiajagan	(2017)	Cloud Execution Mechanisms Compared: Fog, Edge, and Clone Cloud Computing	Fog Computing enables users to perform cloud operations in locations near their focus. Clone clouds are divided into different types of increase techniques which limit the number of cloud services available. Recent cloud techniques are suitable for users with limited connectivity problems and clone clouds make use of cloud resources.
N4	Parikhet al	(2019)	Cloud, fog and edge networking security and privacy concerns.	The Local Area Network (LAN) is a portal in fog computing, in which intelligent computational instruments are used to compute the condition.
N5	Mijuskovic et al..	(2021)	Resource Management Techniques for Cloud/Fog and Edge Computing: An Evaluation Framework and Classification	The direct processing of IoT applications in the cloud, particularly in time sensitive applications, is not the most effective solution for each IoT scenario. The use of fog and edges is a promising solution, addressing the problem of handling the wide bandwidth required for end devices. These paradigms require the processing of vast volumes of data produced in the cloud instead of near the data sources. Cloud-based IoT environments include resource management, which usually focuses on resource sharing, working charge balance, resource provision, task schedule and QoS to increase performance.

RQ 2) What is the orientation of previous studies on the security issues in terms of Data Privacy/Confidentiality and Data Loss/Leakage?

Tawalbeh et al. (2020) explained that despite the fact that IoT implementations expect good security support, protecting IoT devices is difficult for a variety of reasons and extreme resource limitations and poor security architecture are two of the most common sources of security issues in today's IoT applications. Current security protocols necessitate a high degree of processing capacity and memory space on the computer in order to operate and have varieties of security threats which are depicted in the Table 4.3 (Sen, 2015).

Table 4.3: Security issues of cloud, edge and fog computing

Security Threat	Description
Data Confidentiality	
The Insider User Threats: <ul style="list-style-type: none"> • Malicious Cloud platform consumer • Malicious Cloud client user • Malicious Third-party supporter of the cloud vendor or consumer organizations 	Because each of the distribution models will require many internal users, the risk of insiders gaining access to consumer data stored in the cloud is greater: <ul style="list-style-type: none"> • Administrators and customers of cloud services (SaaS) • Application developers and test environment administrators may use PaaS to build and maintain their test environments. • Consultants that have IaaS (independent as a service) platforms
External intruder risks: <ul style="list-style-type: none"> • Remote software assault on cloud infrastructure • Remote software attack on cloud systems • Remote hardware attack on the cloud • Remote software and hardware attack on endpoint software and hardware of cloud user organizations • Social engineering of cloud vendor and cloud consumer users 	However, all forms of cloud distribution models are compromised by external attackers in private clouds, in particular where user endpoints may be attacked. The vulnerability from external attackers could be more applied to public Internet clouds. Cloud vendors of major data stores with credit card records, confidential information and intellectual property or critical government would be vulnerable to community attack, with considerable funding, trying to collect data. This involves the possibility of assault by computers, social technology and supply chains by specialized attackers.
The leakage of data: <ul style="list-style-type: none"> • Failure of multidisciplinary security access privileges • Cloud records and backups failure of electronic and physical conveying networks 	Many future rival organizations using the same cloud provider could be at risk of systemic data leakage through human error or defective hardware which could lead to information compromised.

Integrity	
<ul style="list-style-type: none"> The separation of data • Security perimeter improperly specified • Failure to correctly configure virtual machines and hypervisors 	The integrity of data in complex cloud storage environments like SaaS that is designed to share customers' computer resources could threaten data integrity if system resources are effectively separated.
<ul style="list-style-type: none"> The access granted to Users: • Poor identity and processes for access control 	Weak access management protocols may lead to a variety of threats, such as disgruntled ex-employees of cloud vendor companies having remote access to manage consumer cloud resources and causing intentional harm to their data sources.
<ul style="list-style-type: none"> Data quality: • Incorporation of defective device or infrastructure elements 	As cloud services host many customers' data, the threat of data quality effect has grown. Another cloud user's need for a defective or mis-configured feature could jeopardize the privacy of data for other cloud users sharing infrastructure.

According to Alzoubi et al.(2021) edge computing, in which cloud processing is decentralized and located at or near data-generating nodes, poses similar problems, the least of which is edge protection, or the study of edge computing's cyber-security vulnerabilities and countermeasures. There is some trepidation around successfully protecting edge computing devices, with more than 60% of IT teams seeing the architecture as a challenge to their organizations. Their biggest cause for concern is data protection in edge, fog and cloud computing. For edge computing, it is generally regarded as a protected computing model as long as good safety policies are implemented around the network (Yu, et al., 2017). Considering its many features, the cloud's protection remains one of the most critical concerns. Each cloud infrastructure has its own set of privacy and security considerations.

Sun et al. (2011) identified core stability, safety, and confidence challenges in the current cloud storage world, assisting users in recognizing the visible and intangible risks associated with its use. The authors claim the three major possible challenges to cloud storage are protection, privacy and confidentiality. Protection is critical in the digital era of the long-awaited view of computing as a commodity. The four subcategories are protection systems, cloud device tracking, customer confidentiality and preventing the illegal activities of malicious persons and service hijacking (Saxena, et al., 2020). Data protection is critical when storing private or confidential data in the cloud. Authentication and access control strategies are used to protect data security. The improving reliability and trustworthiness of the cloud

storage problems such as user authentication and access protection can be solved. Users don't trust cloud servers and cloud storage vendors have virtually no problems avoiding possible insider attacks, so storing sensitive data directly in cloud storage is very dangerous.

Lin et al. (2017) gave an overview of the Internet of Things, including supporting technology, IoT architectures, and privacy and security concerns. In terms of implementations, they looked at combining IoT with fog/edge computing. They did not, however, survey IoT implementations. Table 4.4 shows the security challenges.

Table 4.4: Nominated studies for RQ2.

ID	Author (s)	Year	Research Title	Security Issues
N6	Sun et al.	(2011)	Cloud computing surveys and analysis of security, privacy and trust concerns	The authors argue that data protection, anonymity and confidentiality are three main challenges for cloud storage.
N7	Sen	(2015)	Cloud computing security and privacy problems. Concepts, methodologies, tools and implementations of cloud technologies.	Challenges when necessitating Current security for high degree of processing capacity and memory space.
N8	Yu et al.	(2017)	An Internet of Things edge computer survey	IoT's edge computing architecture, performance goals, offloading systems and challenges to security and privacy and the related edge computing steps.
N9	Tawalbeh et al.	(2020)	Confidentiality and safety: challenges and solutions	IoT devices-associated security bugs. Risks to hurt end-users can be by having unwanted access to confidential personal information, allowing device attacks, causing personal security risks.
N10	Alzoubi et al.	(2021)	Internet of Thing applications: state-of-the-art computing security and privacy: Fog	Fog computing faces a lot of stability and privacy problems. The limits of Fog's computer capabilities present these problems. Fog computing will provide IoT devices more local security services as a whole, but new security and privacy problems in relation to centralized cloud computing are the features of Fog computing such as homogeneity, distributing, space limits, and the remote operating system. Due to the above characteristics, privacy and security solutions which in Cloud computing are successful cannot be directly applied to Fog computing

RQ 3) Which of these computing systems has been identified by literature to have the most security concern?

Liu (2020) mentioned that in recent years, edge computing, which allows data to be stored and processed at the network's edge, has emerged as a promising technology when the right and effective security practices are put in place. The unique aspects of edge computing, such as information interpretation, real-time computing, and parallel processing, have created a slew of new concerns in the areas of data security and privacy safety, which are also central issues in other popular computing paradigms such as cloud computing, mobile cloud computing, and fog computing. Recent advancement in the fields of information and edge computing is not also investigated and the architecture of IoT networks presents many security issues, including security and user account authentication. Any of the security problems that concern IoT networks are addressed by edge computing technologies.

AlMendah & Alzahrani (2021) mentioned that edge computing is a stand-alone pattern made up of a large number of heterogeneous devices that bind to the grid and perform some computation tasks, such as store and operation. Any initiative that is dependent on a leasing program will also assist in the providing of services where a person leases a system and receives motivators for resumption. Fog computing is a form of cloud computing that expands cloud models by bringing services and resources from backbone networks to the end network. In the terminal network, it is a virtual computing machine that offers storing and network operation. Sen (2015) stated that threats to cloud-based information assets can differ depending on the cloud delivery frameworks used by cloud user organizations. Cloud storage is vulnerable to a number of different forms of security attacks. Table 4.5 illustrates the least security concern in the literature.

Table 4.5: Nominated studies for RQ3.

ID	Author(s)	Year	Research Title	Summary
N11	Inam ul Haq	(2013)	The security issues that cloud computing faces	Cloud computing is a computer model in which computational services including software, hardware, and data are distributed as a service over the internet through a web browser or a light-weight desktop computer. This programming paradigm eliminates the need to maintain computational infrastructure on a local level, lowering the cost of valuable resources. Different security challenges, such as Temporary Denial of Service (TDOS) attacks, user identity theft, session hijacking issues, and flickering attacks, have an effect on a unique cloud.
N12	Liu	(2020)	Internet-of-things secure and secure computing	Study provides an edge computing architecture to solve the existing multi-tenancy edge systems' security and safety issues. This architecture focuses on a wide range of IoT devices, including both rich and efficient border processors such as ARM Cortex-A processors and bare-metal IoT devices with only microcontrollers, such as ARM Cortex-M processors. This framework focuses on a large number of sensors and actuators. The second section of this dissertation focuses on the data use from the sensors by stopping applications from retrieving unexpected information from the sensory data, which could contribute to the leakage of users' privacy.
N13	AlMendah, O. M., &Alzahrani	(2021)	Security Challenges, Demands, Known Threats, and Vulnerabilities in Cloud and Edge Computing	Edge cloud computing is described by increasing bandwidth, reducing latency, and providing real-time access to scheme data that can be used by several systems. Edge computing can be more useful in the real world for certain uses, such as video platforms, autonomous vehicles, and smart homes. Edge cloud computing can help minimize cloud reliance while still increasing data processing speed.

RQ 4) What are the solutions that have been proposed by researchers with consideration of the identified security issues?

Parikh et al.(2019) revealed that IoT network management is regarded as a significant problem because it improves stability and device stability while also making network maintenance easier. The Internet of Things (IoT) is a space that is

constantly evolving and there is a need to transition away from conventional computing techniques and into modern, more efficient techniques as data and data-generating devices develop. Fog and edge computing have started to take the place of traditional cloud computing for transmitting data from IoT computers. However, with a plethora of data on the way, there is the need to develop new computing methods while keeping the reliability and safety of user data in mind first. Edge and fog computing could supplant conventional cloud computing as far as possible in the future and there is research that can be performed to reduce latency and bandwidth requirements much more without jeopardizing the system's protection.

Tawalbeh et al. (2020) proposed two new IoT-layered models: basic and extended with confidentiality, authentication and layer-recognition elements. The proposed cloud/edge support IoT architecture has been reviewed and implemented and the IoT nodes created by the Amazon Web Service (AWS) are seen in the lower layer as virtual machines with the middle level (Edge) of the AWS server-enabled IoT ecosystem and the AWS Greengrass Edge environment in AWS used in order to strengthen the top layer, which is the cloud, using Raspberry Pi4 hardware kit. These layers were outfitted with a security policy and critical management sessions to ensure the security of users' data and facilitate data transfer between the layers of the proposed Cloud/Edge driven IoT model; security certificates were also added.

Tawalbeh et al. (2020) said a hybrid security architecture is a promising solution to combating security and privacy risks, as well as being able to adapt to advancements in new networking technologies and multiple system deployment scenarios as a result of the artificial intelligence. The edge computing system offers a new location for developing and deploying innovative and robust security technologies for IoT applications and through offloading security defense from end devices to the edge layer, these architectures aim to meet the majority of end-device security needs. Protection issues created by resource limitations at the IoT device layer can be mitigated by placing security protocols at a trusted edge layer.

To achieve data protection for guest virtual machines, Jiménez- Martínez (2013) suggested using the Trusted Cloud Computing Platform (TCCP). The Trusted

Computing Group (TCG) created TCCP as a suite of technologies to address the issue of an untrusted execution environment. TCCP ensures that virtual machine execution does not spill any information and that data is kept private. TCCP does this by enclosing VM execution inside a protected perimeter and blocking entry to a hosting VM's memory by a CSP user with root privileges. TCCP usually uses a Trusted Platform Module (TPM), which contains technologies such as a remote attestation, sealed storage and authenticated booting, which is integrated into motherboards.

As the network becomes overloaded, DoS attacks on a Fog platform, whether from end-users or external networks, will impede legal service use and since all contact is wireless, it is vulnerable to impersonation, message replay, and message manipulation. Since human life is at stake, protection from these attacks is critical. Implementing good authentication, encrypted email, key management program, doing routine auditing, and implementing a private network and stable routing are the most common ways to eliminate such problems. Stable data aggregation is important during the data encryption process and before sending data to Fog nodes to avoid data leakage and reduce transmission overhead on Fog nodes. To be processed, IoT devices send data to the closest Fog nodes, the data is split into sections and sent to multiple Fog nodes). The processed data is then merged from various nodes, putting the data's integrity at risk, particularly if any nodes were malicious. In this regard, as described by Trivedi et al.(2020) a lightweight dynamic, and distributed secure data storage system can be designed based on several convenient encryption methods. To reduce the complexity of the cryptographic algorithm, a mixture of edge data centers and cloud data centers can be used. Table 4.6 offers some solution for security concerns of the computing systems.

Table 4.6: Nominated studies for RQ4.

ID	Author(s)	Year	Research Title	Solutions to Security Issues
N14	Jiménez	(2013)	Issues of privacy and secrecy in cloud computing constructions	Trusted Cloud Computing Platform (TCCP). TCCP ensures that virtual machine execution does not spill any information and that data is kept private.
N15	Parikh	(2019)	Cloud, fog, and edge computing security and privacy concerns.	IoT network management by developing new computing paradigms.
N16	Tawalbeh	(2020)	Privacy and defense in the Internet of Things: Challenges and Solutions	Two new IoT-layered models: basic and extended with confidentiality, authentication and layer-recognition elements. Hybrid security architecture is a promising solution to combating security and privacy risks, as well as being able to adapt to advancements in new networking technologies and multiple system deployment scenarios.
N17	Trivedi	(2020)	Data Sharing and Care at the Edge	A lightweight, dynamic, and distributed secure data storage system can be designed based on several convenient encryption methods.

Some of the nominated articles deliberating security concern in broad-spectrum or only the Cloud Computing; unfortunately, those studies do not provide remarkable knowledge to our research. Therefore, our decision was to eliminate them from sphere of our research. Evaluation of each study from the literature apply by means of criteria that explained in Section 3.2.3. Moreover, the criteria's scores for each of nominated studies are indicated in Table 4.7.

Table 4.7: Quality evaluation for the nominated studies.

Source	QE1	QE2	QE3	QE4	QE5
N1	Y	P	Y	N	P
N2	Y	P	P	N	Y
N3	P	P	Y	Y	Y
N4	Y	Y	Y	Y	Y
N5	Y	Y	P	Y	P
N6	Y	Y	Y	P	Y

N7	Y	Y	Y	P	Y
N8	Y	Y	Y	Y	P
N9	Y	P	P	P	Y
N10	Y	Y	Y	Y	Y
N11	Y	Y	P	Y	Y
N12	Y	Y	Y	Y	Y
N13	Y	Y	Y	Y	Y
N14	P	P	Y	Y	Y
N15	Y	P	Y	Y	Y
N16	Y	P	P	Y	Y
N17	P	P	P	Y	Y
Average	0.91	0.76	0.82	0.79	0.91

4.3 Analysis

In this study, after answering the research questions on the security concerns of cloud, edge and fog computing systems; it was discovered that majority of the research done on the IoT computing systems have been conducted on Cloud. The evaluation of the research on the computing systems which are fog and edge computing, are used interchangeably; the fog computing system is still new and requires much more research and more improvements. Fog Computing enables users to perform cloud operations in locations near their focus. The use of fog and edges is a promising solution, addressing the problem of handling the wide bandwidth required for end devices. Cloud is the foundational system for Internet of things (IoT).

The second research question which depicts the orientation of previous studies on the security issues in terms of Data Privacy/Confidentiality and Data Loss/Leakage was answered and revealed that there is great awareness of how data protection is the highest priority of fog, edge and cloud systems. Companies with cloud architectures have also been found to be of great fear of data leakage/ vulnerability while using the system as more than 50% of the studies reviewed mentioned that several companies have complained about the insecurities of data confidentiality and data leakage surrounding the cloud system. For fog computing systems, it has

been discovered that as much as it is an extension of the cloud system, it is unfortunate that the system inherits the challenges of the cloud system and research is still being conducted on how to enhance the system. Edge computing on the other hand has been mentioned to only require the appropriate policies to be put in place for prevention of data insecurities. It is important to mention that the review of the related research revealed that all the systems have potential security concerns as none of the systems is perfect.

Due to the need for improvement for fog computing, edge computing systems have been identified by literature to have the most security concerns as there is room for the system to be used given that safe practices are being done. Edge computing might be the one with the least security concern presently but there has been uproar about how these 'safe practices' are not very affordable. However, as long as they are effectively done, insecurities of data can be managed as edge and fog computing could supplant conventional cloud computing as far as possible in the future. Some solutions were proposed for solving data confidentiality/data loss/data leakage concerns of edge, fog and cloud computing. The solutions that have opined include; the effective IoT network management by developing new computing paradigms; two new IoT-layered models; a hybrid security architecture is a promising solution; a dynamic, and distributed secure data storage system with multiple encryption methods.

4.4 Research Gap

Cloud computing means transforming, implementing across whole enterprises, managing new connections, entering into partnerships with cloud services vendors, learning more about data stockpiling and backup management, and knowledge of how providers protect the data, to an easier, more flexible and stable variant of the conventional client-server infrastructure. Edge computing, in which cloud computation is decentralized and installed at or near data-generating computers, poses similar security problems, and fog, as a cloud computing extension, inherits these challenges.

This research focused more on the security concerns of cloud, fog and edge computing systems by reviewing previous research on data confidentiality/privacy and data leakage/loss. It was discovered in the course of this study that most of the investigation done on computing systems and their security issues were done on cloud systems. Edge and fog were not very much focused on as they are believed to still be of infancy stage. However, the edge system is able to confront security concerns as long as there are safe practices being put in place. Sufficient and recent research has not been done on fog and edge computing systems.

As years pass by, change is inevitable, new things happen and that is why the newly discovered security concerns of these computing systems should be investigated without disregarding the security issues that were discovered in the earlier years. As of 2021, the newest security concern for the Cloud system has been pointed out to be mis-configuration which ranked as the top challenge in the Cloud Security Study, with more than 60% of businesses reporting it as their top concern (up from 62 percent from the previous year). Mis-configuration occurs when a cloud-related device, tool, or asset is not correctly installed, putting the system at risk and exposing it to a possible attack or data leak. Other Updated security issues include; Unauthorized access (58 percent), unstable interfaces (52 percent), and account hijacking were the next most common threats (50 percent). The cloud, as strong and creative as it is, is also dynamic and ever-changing. This poses many problems and loopholes in terms of defense.

It was also observed that the research done to evaluate the three computing systems up till date is very few. Most research focuses on evaluating one or two systems of the three. Few researchers such as Parikh et al.(2019) have examined the fog, edge and cloud computing systems at once. In summary, there is need for more research on fog and edge computing and need for the evaluation of three of them at once; this will create more avenues to tackle the security issues of the three givens that the cloud system is the foundational computing system of IoT.

4.5 Graphical Representation of the Major Security Concerns of Cloud, Fog and Edge Computing Systems

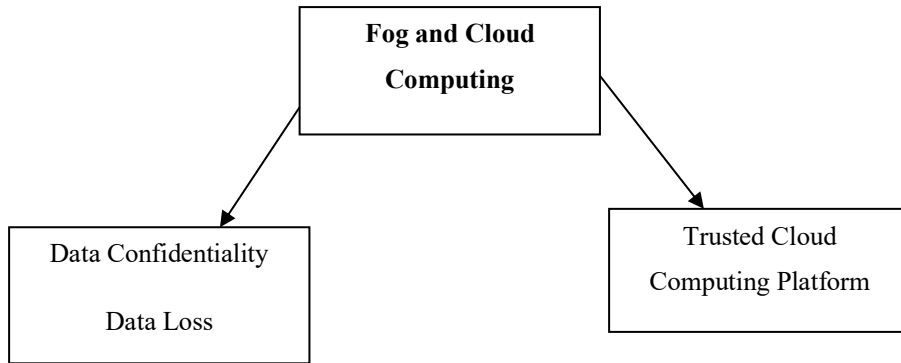


Figure 4.1: Security issues and solution for fog and cloud computing systems

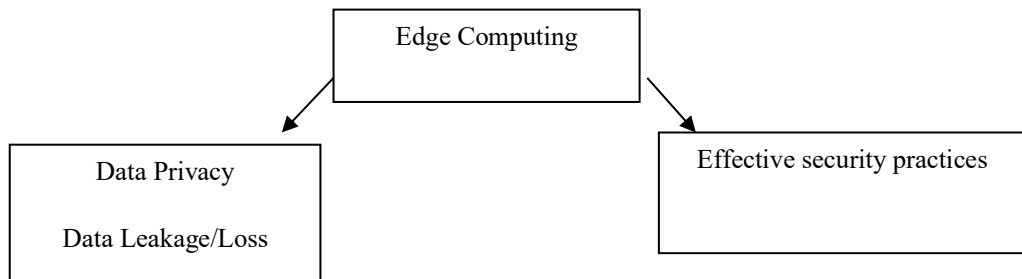


Figure 4.2: Security issues and solution for edge computing system

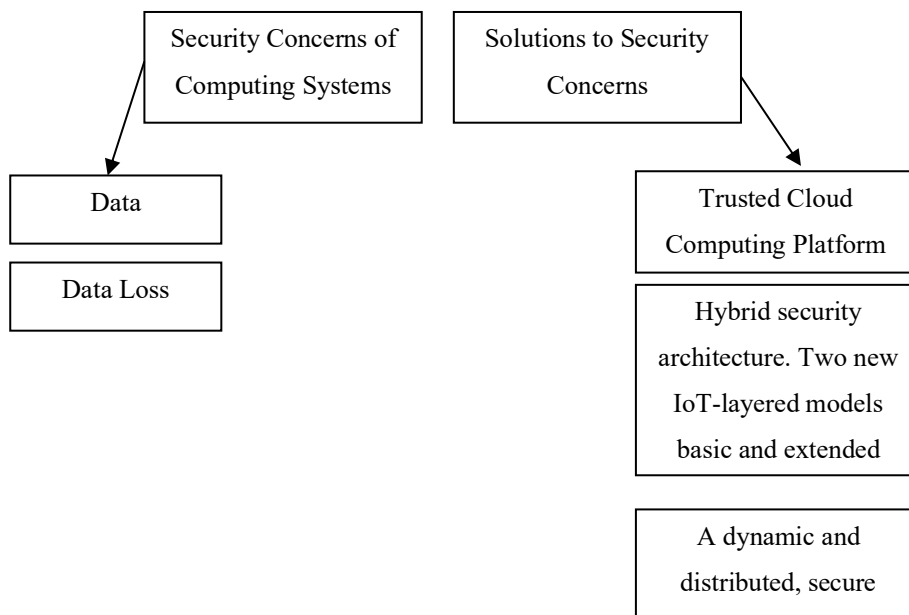


Figure 4.3: Security issues and solutions for IoT computing systems (cloud, fog, edge)

CHAPTER 5

CONCLUSION AND FUTURE WORK

5.1 Conclusion

Cloud infrastructure is seen as a model that is able to make provision of access to the network as demanded for computing resources that have been configured which includes servers and storage with the consideration that it can be quickly provisioned and released without too much effort taken for the maintenance. The cloud computing model comprises the various information that the computing system is capable of providing for the user of which the users have the access to these services via the internet cloud with no need for technological know-how. Cloud computing systems allow for work to be done from home and with the COVID situation in the world, working remotely is an essential part of people's life nowadays. The cloud computing systems have been known for the insecurities that the systems are vulnerable to such as; data loss, lack of privacy. There are several features attributed to cloud, fog and edge computing that can be explored such as application and security. This study focused on reviewing the security concerns while also proffering possible solutions to the issues.

Fog computing is seen as one of the most promising paradigms in computing lately, which performs the task of extending cloud computing to the network's edge. Therefore, the desire to reduce the distance at which data travels over the network, gave birth to edge computing, hence, data is handled at the cloud edge. Edge computing on the other hand, is seen as an enabling that allows data computations to be carried out at the network edge, downstream data in-line with cloud services and upstream data which goes with the services of IoT. Therefore, edge computing is defined as the network resources and computing beside any route between the data-centers of cloud and data source. It was revealed in this study that edge and fog computing are two new technological paradigms proposed to address the former's issues pertaining to the computing system. These systems make a provision for the management of computation as well as memory/storage management that are related to the computer. The investigation done in this study

showed that despite the fact that IoT implementations expect good security support, protecting IoT devices is difficult for a variety of reasons and extreme resource limitations and poor security architecture are two of the most common sources of security issues in today's IoT applications. It was also discovered that data protection, anonymity and confidentiality are three main challenges for cloud storage. Another examination revealed IoT's edge computing architecture, performance goals, offloading systems and challenges to security and privacy and the related edge computing steps while fog was discovered to still face a lot of stability and privacy problems. The limits of Fog's computer capabilities present these problems.

To solve these security concerns propositions were made. Two new IoT-layered models: were proposed basic and extended with confidentiality, authentication and layer-recognition elements. Hybrid security architecture is a promising solution to combating security and privacy risks, as well as being able to adapt to advancements in new networking technologies and multiple system deployment scenarios as a result of artificial intelligence. The Trusted Computing Group (TCG) created TCCP as a suite of technologies to address the issue of an untrusted execution environment. A lightweight, dynamic, and distributed secure data storage system which can be designed based on several convenient encryption methods of which in order to reduce the complexity of the cryptographic algorithm, a mixture of edge data centers and cloud data centers can be used; was also proffered as a solution.

More literature should be considered and more research questions should be deliberated for assessing of this study which are the limitation of this study.

Due to the need for improvement for fog computing, edge computing systems have been identified by literature to have the most security concerns as there are room for the system to be used given that safe practices are being done. Edge computing might be the one with the least security concern presently but there has been uproar about how these 'safe practices' are not very affordable. However, as long as they are effectively done, insecurities of data can be managed as edge and fog

computing could supplant conventional cloud computing as far as possible in the future.

5.2 Recommendations and Suggestions

It was discovered in the course of this study that most of the investigation on computing systems and their security issues were done on cloud systems. Edge and fog were not very much focused on as they are believed to still be of infancy stage. However, the edge system is able to confront security concerns as long as there are safe practices being put in place. Sufficient and recent research has not been done on fog and edge computing systems. There is a need for more investigation and exploration on fog and edge computing systems.

REFERENCES

- Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhar, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE communications surveys & tutorials*, *17*(4), 2347-2376. <https://doi.org/10.1109/COMST.2015.2444095>
- Alhamad, M., Dillon, T., & Chang, E. (2010, September). Sla-based trust model for cloud computing. In *2010, 13th international conference on network-based information systems*, pp. 321-324. <https://doi.org/10.1109/NBiS.2010.67>
- AlMendah, O., & Alzahrani, S. (2021). Cloud and Edge Computing Security Challenges, Demands, Known Threats, and Vulnerabilities. *Academic Journal of Research and Scientific Publishing*, *2*(21), 156-175. ISSN: 2706-6495. Accessed online. <https://www.ajrsp.com/en/Archive/issue21>.
- Alzoubi, Y. I., Osmanaj, V. H., Jaradat, A., & Al-Ahmad, A. (2021). Fog computing security and privacy for the Internet of Thing applications: State-of-the-art. *Security and Privacy*, *4*(2), 145. <https://doi.org/10.1002/spy2.145>
- Atiewi, S., Al-Rahayfeh, A., Almiani, M., Yussof, S., Alfandi, O., Abugabah, A., & Jararweh, Y. (2020). Scalable and secure big data IoT system based on multifactor authentication and lightweight cryptography. *IEEE Access*(8), 113498-113511. <https://doi.org/10.1109/ACCESS.2020.3002815>
- Bonomi, F., Milito, R., Zhu, J., & Addepalli, S. (2012, August). Fog computing and its role in the internet of things. In *Proceedings of the first edition of the MCC workshop on Mobile cloud computing*. 13-16. <https://doi.org/10.1145/2342509.2342513>
- Butpheng, C., Yeh, K. H., & Xiong, H. (2020). Security and privacy in IoT-cloud-based e-health systems: A comprehensive review. *Symmetry*, *12*(7), 1191. <https://doi.org/10.3390/sym12071191>
- Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: current status, classification and open

issues. *Telematics and informatics*, 36, 55-81.
<https://doi.org/10.1016/j.tele.2018.11.006>

Chang, D., Garg, S., Hasan, M., & Mishra, S. (2020). Cancelable multi-biometric approach using fuzzy extractor and novel bit-wise encryption. *IEEE Transactions on Information Forensics and Security*(15), 3152-3167.
<https://doi.org/10.1109/TIFS.2020.2983250>

Dastjerdi, A. V., & Buyya, R. (2016). Fog computing: Helping the Internet of Things realize its potential. *in computer*, 49(8), 112-116.
<https://doi.org/10.1109/MC.2016.245>

De Filippi, P., & McCarthy, S. (2012). Cloud computing: Centralization and data sovereignty. *European Journal of Law and Technology*, 3(2). HAL Id: hal-00746065 <https://hal.archives-ouvertes.fr/hal-00746065>.

Dibbern, J., & Hirschheim, R. (2020). Introduction: Riding the waves of outsourcing change in the era of digital transformation. In Information Systems Outsourcing. *In Information Systems Outsourcing*, pp. 1-20.
https://doi.org/10.1007/978-3-030-45819-5_1

Ferri, F., Grifoni, P., & Guzzo, T. (2020). Online learning and emergency remote teaching. *Opportunities and challenges in emergency situations. Societies*, 10(4), p. 86.<https://doi.org/10.3390/soc10040086>

Francis, T., & Madhiajagan, M. (2017). A Comparison of Cloud Execution Mechanisms: Fog, Edge and Clone Cloud Computing. *Proceeding of the Electrical Engineering Computer Science and Informatics*, 4(1), 446-450.
<https://doi.org/10.11591/ijece.v8i6.pp4646-4653>

Guo, F., Susilo, W., & Y, M. (2016, Feb). "Distance-Based Encryption: How to Embed Fuzziness in Biometric-Based Encryption". *in IEEE Transactions on Information Forensics and Security*, 11(2), 247-257.
<https://doi.org/10.1109/TIFS.2015.2489179>.

Ha, K., Chen, Z., Hu, W., Richter, W., Pillai, P., & Satyanarayanan, M. (2014, June). Towards wearable cognitive assistance. *In Proceedings of the 12th*

annual international conference on Mobile systems, applications, and services, pp. 68-81. doi:<https://doi.org/10.1145/2594368.2594383>

Hamdan, S., Ayyash, M., & Almajali, S. (2020). Edge-Computing Architectures for Internet of Things Applications: A Survey. *Sensors*, 20(22), 6441. doi:<https://doi.org/10.3390/s20226441>

Howe, J., Khalid, A., Rafferty, C., Regazzoni, F., & O'Neill, M. (2016). On practical discrete Gaussian samplers for lattice-based cryptography. *IEEE Transactions on Computers*, 322-334. doi:<https://doi.org/10.1109/TC.2016.2642962>

Inam ul Haq, M. (2013). .The major security challenges to cloud computing. *Journal of Engineering Science and Technology*, 3(3), 3478-3483. Accessed online.<https://www.diva-portal.org/smash/get/diva2:1309139/FULLTEXT01.pdf>. 2013MASI03.

Jeong, S., Jeong, H., Kim, H., & Yoe, H. (2013). Cloud computing based livestock monitoring and disease forecasting system. *International Journal of Smart Home*, 7(6), 313-320. <https://doi.org/10.14257/IJSH.2013.7.6.30>

Jiménez Martínez, D. (2013). *Privacy and confidentiality issues in cloud computing architectures* (Master's thesis, Universitat Politècnica de Catalunya). <https://upcommons.upc.edu/bitstream/handle/2099.1/20816/thesis-david.jimenez-martinez-1.pdf>

Kaur, P. J., & Kaushal, S. (2012, July). Security concerns in cloud computing. *In international conference on high performance architecture and grid computing*, pp. 103-112 https://doi.org/10.1007/978-3-642-22577-2_14.

Lin, H. Y., H. Y. (2019). Traceable anonymous authentication and key exchange protocol for privacy-aware cloud environments. *IEEE Systems Journal*, 13(2), 1608-1617. <https://doi.org/10.1109/JSYST.2018.2828022>.

Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W. (2017). A survey on internet of things: Architecture, enabling technologies, security and privacy,

and applications. *IEEE Internet of Things Journal*, 4(5), 1125-1142.
<https://doi.org/10.1109/JIOT.2017.2683200>

Liu, J. K., Liang, K., Susilo, W., Liu, J., & Xiang, Y. (2016). Two-factor data security protection mechanism for cloud storage system. *IEEE Transactions on Computers*, 65(6), 1992-2004. <https://doi.org/10.1109/TC.2015.2462840>

Liu, R. (2020). *Secure and Safe Edge Computing for the Internet-of-Things (Doctoral dissertation, UCLA)* ProQuest ID: Liu_ucla_0031D_19148. Merritt ID: ark:/13030/m51g5zwn. Retrieved from <https://escholarship.org/uc/item/9mm449dt>.

Mäkinen, O. (2015, September). Streaming at the edge: Local service concepts utilizing mobile edge computing. In 2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies., (pp. 1-6). doi:<https://doi.org/10.1109/NGMAST.2015.35>

Mell, P., & Grance, T. (2009). Draft NIST working definition of cloud computing. Referenced on June. 15(32), p. 2. <https://doi.org/10.6028/NIST.SP.800-145>

Mijuskovic, A., Chiumento, A., Bemthuis, R., Aldea, A., & Havinga, P. (2021). Resource Management Techniques for Cloud/Fog and Edge Computing: An Evaluation Framework and Classification. *Sensors*, 21(5), 1832. <https://doi.org/10.3390/s21051832>

Mitchell, C. J. (2016, Nov). "On the Security of 2-Key Triple DES". in *IEEE Transactions on Information*, 62(11), 6260-6267. <https://doi.org/10.1109/TIT.2016.2611003>.

Mohan, N., & Kangasharju, J. (2016, Nov 1-6). Edge-Fog cloud: A distributed cloud for Internet of Things computations. In 2016 Cloudification of the Internet of Things (CIoT). *IEEE*. <https://doi.org/10.1109/CIOT.2016.7872914>

Mukherjee, M., Matam, R., Shu, L., Maglaras, L., Ferrag, M. A., Choudhury, N., & Kumar, V. (2017). Security and privacy in fog computing: Challenges.

IEEE Access(5), 19293-19304.
<https://doi.org/10.1109/ACCESS.2017.2749422>

Mushunuri, V., Kattapur, A., Rath, H. K., & Simha, A. (2017, May). Resource optimization in fog enabled IoT deployments. In 2017 Second International Conference on Fog and Mobile Edge Computing (FMEC)., (pp. 6-13).
<https://doi.org/10.1109/FMEC.2017.7946400>

Neware, R., & Shrawankar, U. (2020). Fog computing architecture, applications and security issues. *International Journal of Fog Computing (IJFC)*., 3(1), 75-105. <https://doi.org/10.4018/IJFC.2020010105>.

Nguyen, H. D., & Turitsyn, K. (2015). Robust stability assessment in the presence of load dynamics uncertainty. *IEEE Transactions on Power Systems*, 31(2), 1579-1594. <https://doi.org/10.1109/TPWRS.2015.2423293>.

Ni, J., Yu, Y., Mu, Y., & Xia, Q. (2014). "On the Security of an Efficient Dynamic Auditing Protocol". in *IEEE Transactions on Parallel and Distributed Systems*, 25(10), 2760-2761. <https://doi.org/10.1109/TPDS.2013.199>.

Pammu, A. A., Ho, W. G., Lwin, N. Z., Chong, K. S., & Gwee, B. H. (2019, April 18). A High Throughput and Secure Authentication-Encryption AES-CCM Algorithm on Asynchronous Multicore Processor. *IEEE Transactions on Information Forensics and Security*, 14(4), 1023-1036. <https://doi.org/10.1109/TIFS.2018.2869344>.

Parikh, S., Dave, D., Patel, R., & Doshi, N. (2019). Security and privacy issues in cloud, fog and edge computing. *Procedia Computer Science*. (160), 734-739. <https://doi.org/10.1016/j.procs.2019.11.018>

Poon, H. T., & Miri, A. (2017). Fast phrase search for encrypted cloud storage. *IEEE Transactions on Cloud Computing*, 7(4), 1002-1012. <https://doi.org/10.1109/TCC.2017.2709316>

Rahman, G., & Chuah, C. W. (2018). Fog computing, applications, security and challenges, review. *International Journal of Engineering & Technology*, 7(3), pp. 1615-1621. <https://doi.org/10.14419/ijet.v7i3.12612>

- Satyanarayanan, M., Bahl, P., Caceres, R., & Davies, N. (2009). The case for vm-based cloudlets in mobile computing. *IEEE pervasive Computing*, 8(4), 14-23. <https://doi.org/10.1109/MPRV.2009.82>.
- Saxena, N., Hayes, E., Bertino, E., Ojo, P., Choo, K. R., & Burnap, P. (2020). Impact and key challenges of insider threats on organizations and critical businesses. *Electronics*, 9(9), 1460. <https://doi.org/10.3390/electronics9091460>
- Sen, J. (2015). *Security and privacy issues in cloud computing*. In *Cloud technology: concepts, methodologies, tools, and applications*. IGI global. <https://doi.org/10.4018/978-1-4666-4514-1.ch001>
- Shahid, F., Ashraf, H., Ghani, Ghayyur, S. A., Shamshirband, S., & Salwana, E. (2020). PSDS–Proficient Security Over Distributed Storage: A Method for Data Transmission in Cloud. *IEEE Access*(8), 118285-118298. <https://doi.org/10.1109/ACCESS.2020.3004433>
- Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2016). Edge computing: Vision and challenges. *IEEE internet of things journal*, 3(5), 637-646. <https://doi.org/10.1109/JIOT.2016.2579198>.
- Song, Y., Zhu, Z., Zhang, W., Yu, H., & Zhao, Y. (2019). Efficient and secure image encryption algorithm using a novel key-substitution architecture. *IEEE Access*, 7, 84386-84400. <https://doi.org/10.1109/ACCESS.2019.2923018>
- Sun, D., Chang, G., Sun, L., & Wang, X. (2011). Surveying and analyzing security, privacy and trust issues in cloud computing environments. *Procedia Engineering*,(15), pp. 2852-2856. <https://doi.org/10.1016/j.proeng.2011.08.537>
- Tang, H., Sun, Q. T., Yang, X., & Long, K. (2018). A network coding and DES based dynamic encryption scheme for moving target defense. *IEEE Access*, 6, 26059-26068. <https://doi.org/10.1109/ACCESS.2018.2832854>

- Tawalbeh, L. A., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT Privacy and security: Challenges and solutions. *Applied Sciences*, 10(12), 4102. <https://doi.org/10.3390/app10124102>
- Trivedi, A., Wang, L., Bal, H., & Iosup, A. (2020). Sharing and Caring of Data at the Edge. In *3rd {USENIX} Workshop on Hot Topics in Edge Computing (HotEdge 20)*. Accessed online. <https://www.usenix.org/conference/hotedge20/presentation/trivedi>.
- Trivedi, M., & Suthar, V. (2013). Cloud Computing: A Feasible Platform for ICT Enabled Health Science Libraries in India. *International Journal of User-Driven Healthcare (IJUDH)*, 3(2), 69-77. <https://doi.org/10.4018/ijudh.2013040108>
- Umapathy, B., & Kalpana, D. (2020). Survey on cryptographic algorithm for data security in cloud storage environment. *European Journal of Molecular & Clinical Medicine*, 7(9), 1602-1620.
- Wang, X., & Su, Y. (2019). An audio encryption algorithm based on DNA coding and chaotic system. *IEEE Access*(8), 9260-9270. <https://doi.org/10.1109/ACCESS.2019.2963329>
- Yi, S., Qin, Z., & Li, Q. (2015). Security and privacy issues of fog computing: A survey. In C. Springer (Ed.), (pp. 685-695). https://doi.org/10.1007/978-3-319-21837-3_67
- Yu, W., Liang, F., He, X., Hatcher, W., W, G., & Lu, C. (2017). A survey on the edge computing for the Internet of Things. *IEEE access*(6), 6900-6919. <https://doi.org/10.1109/ACCESS.2017.2778504>
- Zhang, Q., Han, J., & Ye, Y. (2019). Image encryption algorithm based on image hashing improved chaotic mapping and DNA coding. *IET Image Processing*. 13(14), 2905-2915. <https://doi.org/10.1049/iet-ipr.2019.0667>
- Zhang, Y. X., Zhang, Y., Xu, C., Li, H., & Liang, X. (2017). Cryptographic public verification of data integrity for cloud storage systems. *IEEE Cloud*

Computing, 3(6), 44-

52. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7742226>

Zheng, J., & Liu, L. (2020). Novel image encryption by combining dynamic DNA sequence encryption and the improved 2D logistic sine map. *IET Image Processing*, 14(11), 2310-2320. <https://doi.org/10.1049/iet-ipr.2019.1340>

Zhu, J., Chan, D. S., Prabhu, M. S., Natarajan, P., Hu, H., & Bonomi, F. (2013, March). Improving web sites performance using edge servers in fog computing architecture. In 2013 IEEE Seventh International Symposium on Service-Oriented System Engineering. 320-323. <https://doi.org/10.1109/SOSE.2013.73>

APPENDICES

APPENDIX 1

SIMILARITY REPORT

Sahar Ebadinezhad | User Info | Messages | Instructor | English | Community | Help | Log

turnitin

Assignments | Students | Grade Book | Libraries | Calendar | Discussion | Preferences

NOW VIEWING: HOME > PAPER CHECKING > MAJED SALEH ABDULQAWI

About this page
This is your assignment inbox. To view a paper, select the paper's title. To view a Similarity Report, select the paper's Similarity Report icon in the similarity column. A ghosted icon indicates that the Similarity Report has not yet been generated.

Majed Saleh Abdulqawi
INBOX | NOW VIEWING: NEW PAPERS ▾

Submit File		Online Grading Report Edit assignment settings Email non-submitters									
<input type="checkbox"/>	AUTHOR	TITLE	FILE	RESPONSE	GRADE	SIMILARITY	PAPER ID	DATE			
<input type="checkbox"/>	Majed Saleh Abdulqaw...	ABSTRACT		--	--	0%	1610527731	22-Jun-2021			
<input type="checkbox"/>	Majed Saleh Abdulqaw...	INTRODUCTION		--	--	0%	1610525028	22-Jun-2021			
<input type="checkbox"/>	Majed Saleh Abdulqaw...	RESEARCH FINDINGS		--	--	0%	1610526834	22-Jun-2021			
<input type="checkbox"/>	Majed Saleh Abdulqaw...	LITERATURE REVIEW		--	--	1%	1610525667	22-Jun-2021			
<input type="checkbox"/>	Majed Saleh Abdulqaw...	CONCLUSION		--	--	1%	1610527323	22-Jun-2021			
<input type="checkbox"/>	Majed Saleh Abdulqaw...	ALL-THESIS		--	--	5%	1610530075	22-Jun-2021			
<input type="checkbox"/>	Majed Saleh Abdulqaw...	RESEARCH METHOD		--	--	11%	1610528427	22-Jun-2021			

Majed Saleh Abdulqawi

Assist. Prof. Dr. Sahar Ebadinezhad

APPENDIX 2

ETHICAL APPROVAL DOCUMENT



ETHICAL APPROVAL DOCUMENT

Date: 01/ 07/ 2021

To The Institute of Graduate Studies

For the thesis project entitled as “CLOUD, EDGE AND FOG COMPUTING SYSTEMS: SECURITY AND PRIVACY ISSUES” the researchers declares that they did not collect any data from human/animal or any other subjects. Therefore, this project does not need to go through the ethics committee evaluation.

Title: **Assist. Prof. Dr.**

Name Surname: **Sahar Ebadinezhad**

Signature: 

Role in the Research Project: **Supervisor**