University of South-Eastern Norway

USN School of Business

Department of Business, Marketing and Law

–

Master's Thesis

Study programme: Management Information Systems

**Spring 2022**

Iliana Mogilevskaia

# Security and privacy challenges in edge computing

University of South-Eastern Norway
USN School of Business
Department of Economics, Marketing and Law
PO Box 235
NO-3603 Kongsberg, Norway

http://www.usn.no



This thesis is worth 30 study points

# Acknowledgments

I would like to express my sincerely gratitude to my supervisor Assoc. Prof. Rania El-Gazzar. Her support and guidance during the work on this thesis have helped a lot, and her comments were invaluable.

# Abstract

This thesis study security and privacy challenges of edge computing concept. First, concepts and definitions of edge computing and other technologies are reviewed. Then, possible application areas, where utilisation of edge technology has positive perspectives. Next, potential challenges, based on comparison with other technologies like cloud computing, are introduced. Then, this paper presents the research method along with data collection and analysis. In this part, formerly suggested categories are updated based on findings from the sample of articles. Additionally, deeper description of each category is present. In the discussion part, gups in the research of this topic are identified and possible future directions are proposed. Relations between categories are shown.

# Contents

# Table of Figures



# Table of Tables

# 1 Introduction

Cloud computing is a trend which for the last 20 years was heavily used by businesses for processing a huge amount of data, cloud allows to perform complex calculations on a remote server instead of local computers. However, with an exponential growth of smart devices which can generate data, cloud centres face some problems with bandwidth, data privacy and security, response time and latency (Hagan et al., 2019). Internet of Things (IoT) has entered different spheres of domain areas, smart houses, intelligent vehicles, health industry, and other industries. According to Costello (2021), the number of IoT devices doubles every five years and by the year 2029, Gartner expects more than 15 billion IoT devices will be used by industries. Growing number of IoT devices creates a need for real-time processing, data privacy, and need for automated decision-making (Patel et al., 2021). Edge computing is a new paradigm that has emerged to offload some processing to the local devices end resolve the above-mentioned issues with cloud technology and IoT (Cao et al., 2020).

Edge computing concept was introduced in 2016; it is relatively new and there are many challenges that need to be addressed, especially about security and data privacy (Cao et al., 2020). Edge computing has decentralised architecture, and it needs to connect with a large number of heterogenous technologies (Parikh et al., 2019). Additionally, users' high demands for privacy create many challenges for edge computing security (Parikh et al., 2019). According to report by Stratus Technologies (2019), professionals from different industries are positive about integrating edge computing; more than 60% responders are having plans to implement this technology. As shown in Figure 1, there are different barriers that prevent certain businesses to start using edge computing, from lack of education on when and how to use the technology (46%) to security concerns (37%) and lack of budget (33%). Numbers show that many businesses are interested in advantages of implementing edge computing. However, even if there is an existing infrastructure, there are some concerns with a proper utilization of edge nodes and a lack of trained personnel.

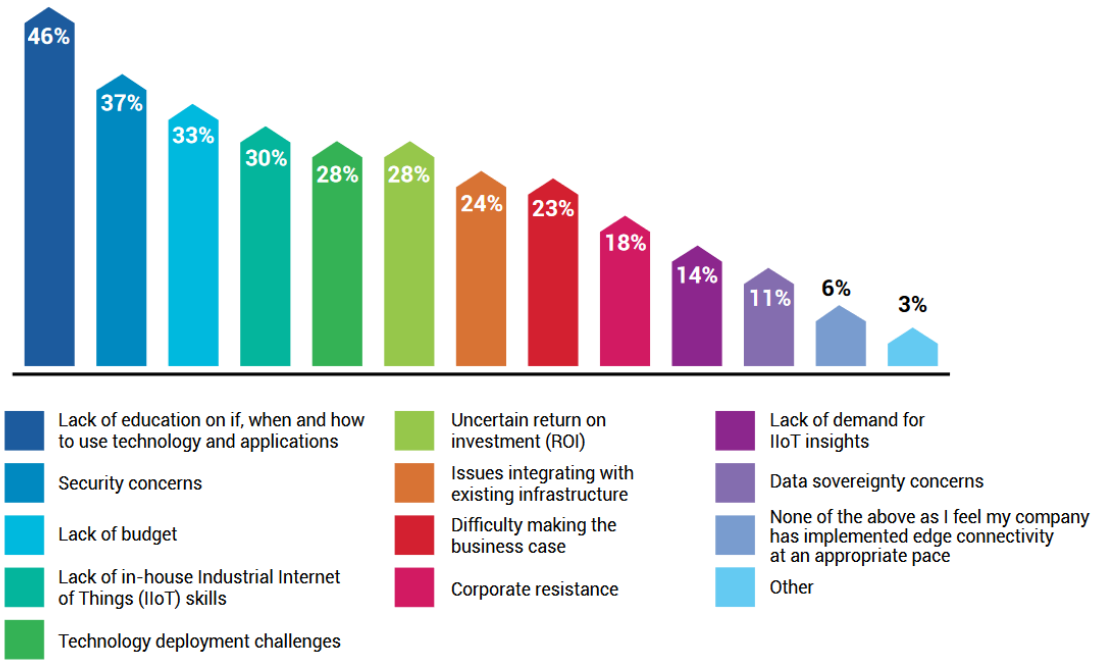


*Figure 1 The barriers to edge computing deployments. Adapted from (Stratus Technologies, 2019, September). Edge Computing Trend Report.* [https://lp.stratus.com/wp-content/uploads/stratus-edge-computing-trend-report-americas.pdf](https://lp.stratus.com/wp-content/uploads/stratus-edge-computing-trend-report-americas.pdf)

There is a great interest in edge technology among researchers, however, very few studies have addressed security and privacy. Furthermore, there are few systematic literature reviews addressing requirements of edge computing security and privacy. The aim of this thesis is to perform a mapping study on categories of security and privacy challenges in the edge computing implementation. The main goal of this systematic mapping study is to classify existing research and provide direction for future references.

RQ

*What are the categories of security and privacy challenges in edge computing and what are the relationships between these categories?*

# 2 Background

Not all smart hardware works through the cloud; the computing infrastructure is constantly changing along with the development of technology. Data can be stored, read, analysed, and sent to the control centre using peripheral devices (Cao et al., 2020).

## 2.1 Concepts and definitions

Cloud paradigm is a model for providing computing and network resources, as well as data storage on demand through the Internet (Parikh et al., 2019). The peculiarity of this model is that resources can be received with payment upon their use (Parikh et al., 2019). Cloud computing involves two participants (Parikh et al., 2019). Provider builds a data centre, places servers and data storage systems there, lays network equipment and deploys software that manages the IT resources and correctly distributes them among users (Parikh et al., 2019). The user, the client company - signs an agreement with the provider and requests a certain pool of resources from him: any number of processors, amount of memory for storage, Internet channel bandwidth, number of IP addresses (Parikh et al., 2019). These services accelerate innovation, increase resource flexibility, and deliver cost savings through high scalability (Parikh et al., 2019). However, the growing number of IoT and advances in 5G and AI, make traditional cloud computing performance inefficient because of bandwidth limitations, high latency, and data privacy and security; these new demands require new models and technologies (Mukherjee et al., 2020).

The core concepts of edge computing are easy to understand. There are three layers: a cloud layer, an edge layer, and devices layer (Alwarafy et al., 2021). The cloud layer is responsible for big data and long-term analytics, and storage (Alwarafy et al., 2021). The edge layer provides edge nodes, which can provide real-time processing of data required by applications, temporarily store the data, while ensuring that these devices are physically close to the source of data (Cao et al., 2020). The devices layer consists of every device embedded with sensors, actuators, etc. This layer generates data (Alwarafy et al., 2021). Edge nodes are located between user and the cloud, which means sensitive data can be processed within local network and a close proximity can shorten delays of data processing (Alwakeel, 2021). Advances in 5G and Artificial Intelligence (AI) allow edge devices to shift to machine-to-machine communication (M2M), meaning edge nodes can process and analyse raw data of IoT devices. (Patel et al., 2021)

Fog computing is another paradigm to partially offload data processing from the cloud centre. Fog computing is a technology where storage and processing of data are kept within the local network between the end-devices and the data centre (Alwakeel, 2021). Fog nodes, unlike cloud, are closer to users and play the role of a filter of data. Fog nodes can use processing power of the fog resources or send data to the cloud (Alwakeel, 2021).

*Table 1 Fog and edge computing features*

| Fog computing | Edge computing |
|---|---|
| Offload bandwidth | |
| Low latency | |
| Decentralised architecture | |
| Real-time processing | |
| Heterogeneous nature | |
| Fog nodes collect data from end devices and process it or send it to the cloud | Edge computing processes data in the devices that collect it |

As shown in Table 1, fog and edge computing have a lot of common features, however they should not be mistaken with each other. The main difference between two paradigms is their location, additionally fog computing cannot operate without a cloud, fog nodes form an extensive layer to the cloud. Edge, on the other hand can be standalone technology. (Alwakeel, 2021)

Edge computing is a main technology that allows to use the computing power of the devices on the edge of network (Ali et al., 2021). Mobile edge computing or multi access edge computing (MEC) is a next generation of technology, it brings computing capacity directly to the network's infrastructure (Ali et al., 2021). Research papers use the abbreviation MEC interchangeably for both mobile edge computing and multi access edge computing. MEC is more mobile than edge technology and lowers latency more than its' antecedent (Ali et al., 2021). Edge computing brings processing of the data closer to the edge, MEC brings processing directly to the edge of the network (Ali et al., 2021).

Mobile computing means wireless communication and its applications is a common technology referring to numerous devices that support access to transmitted data such as voice, video, and text anytime and anywhere through a radio access network (RAN), including mobile communications, mobile hardware, and mobile software (Garg et al., 2021). This means that MEC

services or applications do not require additional equipment, it can be installed at the base station (Garg et al., 2021). MEC characterised by low latency, real-time processing, high-efficiency, and user context and network status awareness (Ali et al., 2021). MEC is a collocation of edge devices and mobile network infrastructure which brings mobility to the Edge computing (Garg et al., 2021).

## 2.2 Application areas

Information is a strategically important source of decision-making, especially for enterprises (IMARC Group, 2022). IoT devices transmit a huge amount of unstructured data (IMARC Group, 2022). It is not enough to send it to a corporate data centre and expect high-quality information for further analysis by top management (IMARC Group, 2022). The transmission channel may simply not withstand a large amount of IoT data (Patel et al., 2021). To avoid this, enterprises are shifting the concentration of their IT resources closer to where data is generated (Patel et al., 2021). To do this, local switching facilities are introduced, and the need to send all or part of the data to the main cloud data centre is eliminated (Patel et al., 2021).

The gradual transfer of computing power to the edge of the network is associated with the desire of companies to increase the performance of applications and services, as well as reduce operating costs and ensure infrastructure reliability (IMARC Group, 2022). Edge nodes located close to users allows to lessen the computation load on cloud centres, which leads to reduced network bandwidth and lower latency (Zhang et al., 2018).

Edge technology is driving the adoption of 5G in enterprises and is a platform for a variety of scenarios which can benefit from having a massively distributed cloud environment connected to low latency 5G networks (Patel et al., 2021). This enables automation, new innovations and new business models using data and the cloud (Hagan et al., 2019). IoT sensors collect a huge amount of environment data that is essential for industries. According to Stratus Technologies (2019) most of the users desire autonomous device failure detection and advanced process control.

There are several applications of edge computing in real world:

Industry 4.0 – Use different technologies like cloud computing, edge computing, IoT, and AI to revolutionise the way of manufacturing and distribution of products (Sittón-Candanedo et al.,

2019). The main achievement of Industry 4.0 is predictive maintenance which can forecast and optimise maintenance plans (Cao et al., 2020).

Smart Energy – The use of innovative technologies to improve the operation of energy sector (Sittón-Candanedo et al., 2019). Implementation of IoT devices together with edge nodes and other technologies like AI or machine learning help to provide reliable services and reduce the cost (Sittón-Candanedo et al., 2019).

Smart city – is a system of interconnected smart devices like IoT, which helps to manage internal city processes and makes the life of residents more comfortable and safer (Sittón-Candanedo et al., 2019).

MEC is in initial stages of development but there are some pilot tries to use it on existing infrastructure:

Augmented and virtual reality (AR/VR) – AR and VR mobile applications and games require a good bandwidth and fast transmission (Ali et al., 2021). MEC provides content cashing and low latency, which can improve quality of service (Ali et al., 2021).

Location-based services (LBS) – LBS uses mobile geolocation data to provide information and entertainment (Tian et al., 2020). The ability of modern smartphones and other mobile devices allows to display maps of various kinds with high resolution (Tian et al., 2020). Applications can provide various directories, navigators, check-in services, which are local search services for objects of the service sector, such as the nearest cash machines, currency exchange offices, gas stations and others (Tian et al., 2020). MEC is used to connect user to other devices, shared bicycle/vehicle services (Tian et al., 2020).

Vehicular ad hoc network (VANET)- Self-driving or AI-integrated cars and other vehicles need a huge amount of data from their environment to work properly in real time (Singh et al., 2022). MEC servers which do not have a specific location are a perfect solution for fast moving vehicles (Singh et al., 2022).

Video analytics – Applications which show, live-stream or analyse video content especially HD videos are challenging for the data transmission through networks, MEC helps to offload traffic (Ali et al., 2021).

## 2.3 Security and privacy challenges

Over the years security of Cloud computing has improved, there are solid solutions to ensure that data will be safe in the cloud centre and during transmission to the user (Zeyu et al., 2020). There are multiple known types of threats and ways to attack data servers or data during communication process, and there are existing countermeasures and preventive techniques (Zeyu et al., 2020). Edge devices are vulnerable to plenty known cyber threats, the best way to find ensure safety of data is to apply existing methods and frameworks (Zeyu et al., 2020).

Edge computing introduces some new challenges (Zeyu et al., 2020). There are certain areas of concern:

- Decentralised architecture of edge computing makes it an easy target for attacks; presence of one vulnerable device can compromise the whole network (Singh et al., 2022). Location in proximity of the end devices means that personal data of users is processed and organised on edge nodes, which are exposed to threats (Hagan et al., 2019). Heterogeneity of devices, protocols, and data providers introduce complexity and demands creation of multi-layered security schemes (Singh et al., 2022).
- Environment of edge computing is changing, devices might come and go, perpetrator can easily be bland in (Mukherjee et al., 2020). Another concern is obsolete devices, with hundreds or thousands of gadgets, it is possible that some of them may be connected as active devices (Singh et al., 2022).
- Hardware – edge nodes are small that means memory and processing resources are limited, existing security frameworks, especially encryption, are demanding and can't be installed on these devices (Alwakeel, 2021). Another problem lies with the design of edge devices, manufactures focus on the demands of consumers which are scalability and a quick response time (Hagan et al., 2019). Designers tend to overlook the security of the device in favour of the fulfilment of the demands (Singh et al., 2022). Physical protection of edge nodes is another challenge that needs to be addressed (Zeyu et al., 2020).
- Resource management – decentralised architecture and heterogenous environment of edge computing create risks with communication, processing, and storage (Alwarafy et al., 2021). Sources are shared among edge devices which rises a concern; with a growing number of

devices there will be more request messages and that may lead to overheat or a potential DDoS attack (Singh et al., 2022).

Data privacy has become a big concern among users (Tian et al., 2020). Personal data like geolocation or device characteristics are transmitted and processed on edge node, end devices need to be anonymous, plus sensitive information about edge node itself need to be protected (Losavio, 2020). Data privacy can be ensured using encryption schemes, but edge nodes require researchers to come up with some novel lightweight solutions (Alwarafy et al., 2021). Anonymity of end devices as they connect and disconnect to/from the network need an authentication scheme that is lightweight and fast (Parikh et al., 2019).

Security and privacy of data are very important areas of concern because data plays crucial role in businesses and holds sensitive information about users (Losavio, 2020). There are many research papers addressing security and privacy of edge computing, these studies mainly focus on attacks and countermeasures. There are few papers that focus on security and privacy challenges, but those challenges are diverse and not synthesized in an organised manner.

# 3 Method

This thesis uses mapping review to classify available literature. Prior screening was performed to find if there are similar works; Yahuza et al. (2020) presented a systematic literature review of security and privacy requirements in edge computing and Sittón-Candanedo et al. (2019) employed systematic mapping review to study the implementation of edge computing in Smart Energy. There is no existing mapping study for security and privacy challenges in edge computing.

The literature search plan was developed. The main steps of the plan are shown in figure 2.

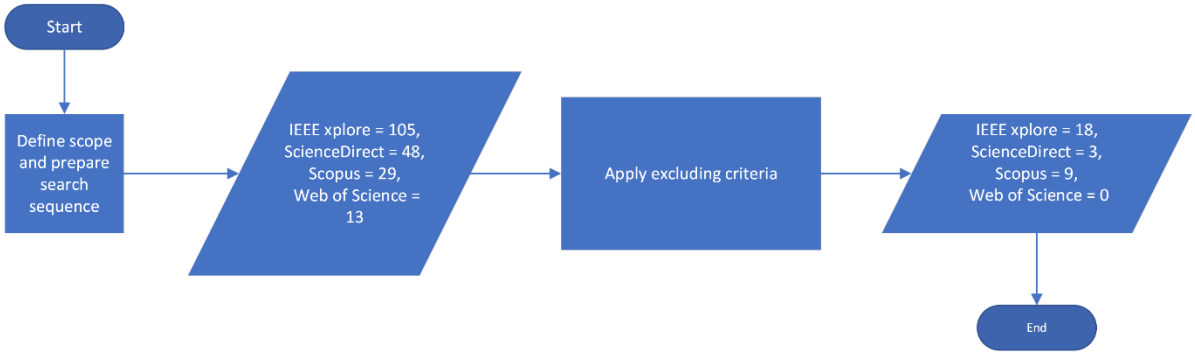


*Figure 2 Search plan*

Reliable online databases with a focus on computer science were identified: IEEE xplore, ScienceDirect, Scopus, and Web of Science. The word sequence for searching the papers is:

- (“edge computing" AND "security and privacy " OR "edge computing" AND "security challenges" OR "edge computing" AND "privacy challenges")

The advanced search option is used to achieve better results. Databases have different parameters available for searching IEEE xplore and Web of science performs inquires using paper title while ScienceDirect and Scopus search through title, abstract, and keywords. The years of publication are from 2017 till 2022. The language of paper is English. The type of publication limited to articles and conference papers. The total number of studies found is 195.

Titles and abstracts are scanned to make sure papers are within the scope of this thesis and exclusion criteria are applied.

1. Inclusive criteria>

1.1. Publication years 2017-January 2022

1.2. Language: English

2. Exclusive criteria>

2.1. Full text of the article is not accessible

2.2. Type of publication is a book or a book chapter

2.3. Article is not addressing security and privacy challenges in edge computing

34 articles and conference papers fulfilled inclusive criteria. Studies are reviewed again to remove duplicates; the number of articles is 24. Database IEEE xplore contains the most publications, the rest databases had many duplicate studies. Additionally, backward, and forward search is performed, and 6 articles identified that are relevant to the research question (Watson & Webster, 2002).

## 3.1 Data analysis

All articles have been read and some related data is extracted to help to answer the research question. Information like year of publication, publisher, research method, and proposed frameworks is noted. Based on the review findings, illustrated in Figure 3 the bigger number of publications is during 2020 and 2021. This can be explained by the influence of the Covid pandemic and a raised demand for bandwidth and speed for distant communication, as millions of people switched to working and studying from home. Figure 4 shows that conference papers make up only 27% of studies, however there might be some other publications in different databases.

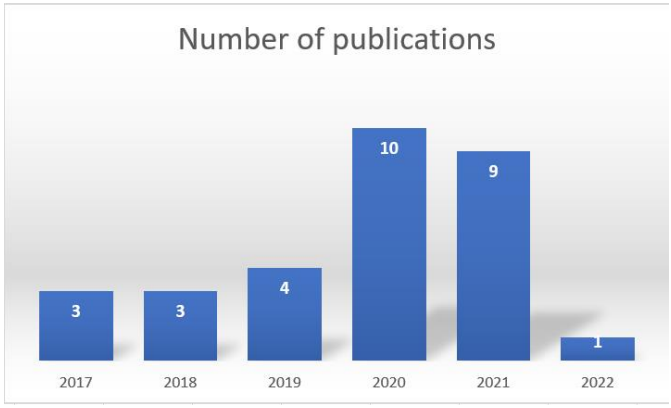


*Figure 3 Number of publications*

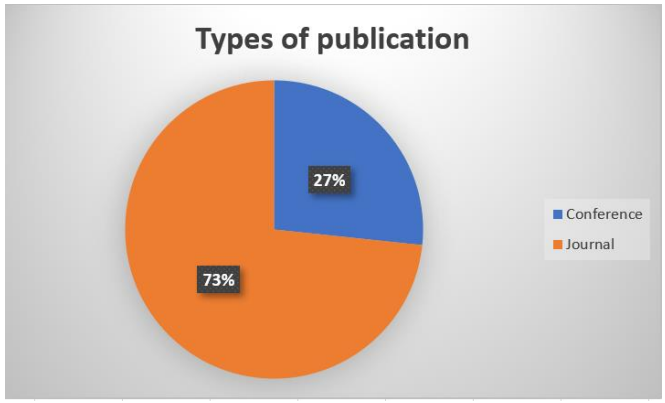


*Figure 4 Outlet*

Figure 5 illustrates research methods used by authors. Majority of the papers used qualitative method, 21 narrative literature review and 1 article used systematic review approach. There are 8 studies that propose and test new security frameworks. The number of experimental studies introducing new frameworks and models is small and require more attention.

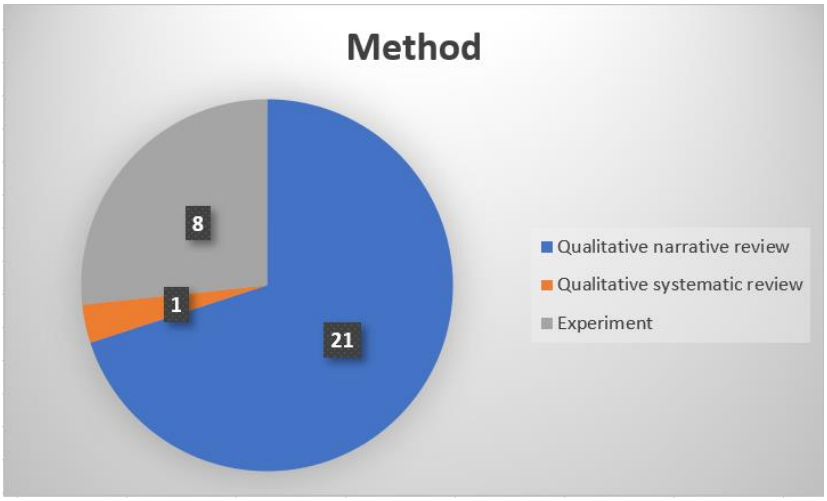


*Figure 5 Methods*

Edge computing is a new technology which offers a vast horizon of possibilities especially its ability to integrate with other emerging technologies. Most of the established and verified technologies for communication or security are not suitable for edge devices or architecture. There is a need to implement and test other ideas. Table 2 shows which technologies are used by authors to create new schemes to enhance the edge nodes performance and security, additionally to ensure security

and privacy of communication within the network. Several papers offer the solutions for an efficient management of the network resources.

*Table 2 Proposed frameworks*

| Paper | Technology | Proposed framework |
|---|---|---|
| Mukherjee et al., 2020 | AI, Deep learning | An intuitive framework implemented across different layers of the cloud-edge computing architecture to counter possible adversary attacks on data communication, authentication, privacy, and anonymity |
| Hagan et al., 2019 | Software | System Security Manager is a micro-architectural security mechanism that continuously monitor data processing and play a role in detection and prevention activity |
| Garg et al., 2021 | Deep learning<br>Blockchain | SecEdge-Learn Architecture uses deep learning to monitor data flow to the appearance of anomalies. Moreover, authors use blockchain to securely store data |
| Singh et al., 2021 | Software-defined perimeter (SDP) | SDP framework for MEC to precent DDoS attacks and monitor traffic. |
| Sicari et al., 2017 | Sticky policy | Sticky policy approach is proposed as a strategy for efficiently managing the access to IoT resources within an existing distributed middleware architecture |

| Paper | Technology | Proposed framework |
|---|---|---|
| Patel et al., 2021 | Network slicing | Based on the priority services, the processes of computation and storage of data are migrated from one device to another to ensure higher availability of the application, device, and network information and physical resources |
| Rahman et al., 2017 | Fog computing terminals (FCTs) | Middle layer of FCTs is acting as a proxy between the user end and cloud infrastructure |
| Zhang et al., 2020 | Blockchain | Framework that preserves data privacy in edge computing by combining blockchain, distributed data storage and trusted execution environment (TEE). |

Experimental papers propose the use of Artificial Intelligence (AI) and Blockchain to enforce security of the network. Mukherjee et al., (2020) suggest using deep learning and AI to have an Intelligent Edge Computing. Three layers: cloud, edge, and end user, will provide traffic and devices data to be analysed using deep learning techniques and to create data sets. These data sets are used by AI application to classify and ascertain the normal traffic flaw within the network. After sufficient training artificial intelligent application can predict and react to changes in devices operation or traffic and prevent attacks.

In their paper, Garg et al., (2021) provide a SecEdge-Learn architecture that uses deep learning techniques to ensure secure MEC environment. The SecEdge-Learn architecture consists of three layers, Internet core, MEC servers, and mobile devices. In order to ensure security of the network, authors propose three steps. Data collection is the first step, data about different features of MEC environment is acquired and classified. In second stage, prepared sets are analysed, and possible attack vectors are identified. The last step is to use blockchain techniques to safely distribute the

knowledge between devices. Another paper by Zhang et al., (2020) uses blockchain to safely distribute and store data among edge devices to ensure privacy.

Study by Hagan et al., (2019) propose a software security manager to be integrated into edge devices architecture. Described manager will monitor the devices performance for anomalies and can make decisions to shut down the device if any anomaly detected in its behaviour, which would halt any possible harm to other network devices.

There are three works introduce frameworks for network architecture. Singh et al., (2021) propose the combination of MEC and software defined perimeter, to add security layer to communication between devices. SDP is based on zero trust model, security model that would identify users, their devices, and their role before granting access to secure systems. In mobile environment like MEC authentication and authorisation are weaknesses. MEC-SDP combines device authentication, identity-based access, and dynamically created network connectivity.

Network slicing allows to create multiple virtualized and isolated logical networks on a physical network. Each isolated network can have different purposes. Patel et al., (2021) propose using network slicing on 5G enabled MEC. There are two instances of using network slicing in this paper. The first is between layers: cloud, edge, and transport layers. The second is based on communication services: secure information slice, interaction slice, and high bandwidth slice. Accessibility to network resources depends on the priority of needed communication.

Rahman et al., (2017) use additional security layer that consists of fog computing terminal which takes on a role of a proxy between a cloud and users.

Paper by Sicari et al., (2017) is the only study to introduce regulations. According to Sicari et al., (2017) access and use of user data is regulated by Sticky Policy. The concept of Sticky policy is to attach security and privacy policies directly to data, which ensure access by authorized only by devices.

## 3.2 Classification of challenges

Surface for security and privacy challenges is broad, to design proper schemes and techniques it is helpful to group possible challenges into categories as shown in figure 6.

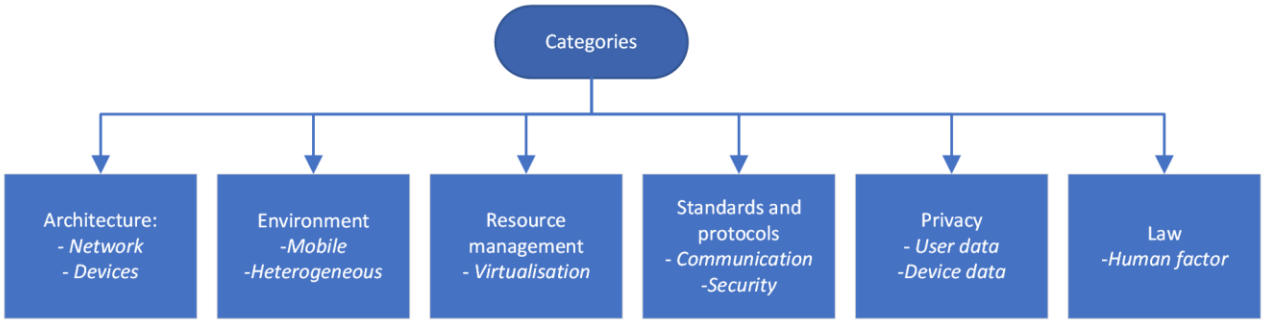


*Figure 6 Categories of challenges*

Figure 7 shows summary of numbers of research papers in each category.

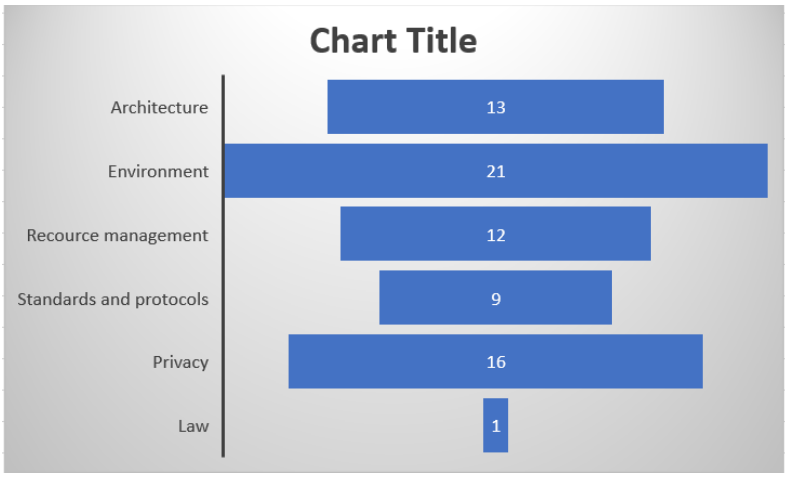


*Figure 7 Numbers of articles in each category*

Category architecture encompasses challenges in creating efficient and secure edge network, additionally, it involves challenges in designing edge nodes with sufficient but at the same time light weight security infrastructure.

Edge computing/ MEC environment is the most discussed category. Environment is mobile with a big number of user devices which may connect and disconnect, which leads to the need of proper authentication and authorisation techniques. Many user devices will make it hard to monitor the state of all connected machines, some of them might become obsolete. Edge paradigm brings together a lot of different providers and manufacturers who employ different hardware, software, and protocols. This heterogeneous nature creates many vectors for attacks.

Resource management is another important category. Edge concept offers offloading computation with limited hardware resources, that means that often computation is performed by several edge

devices. Assigning resources to the important tasks first, and continuous monitoring of processes create the need for new mechanisms of resource management.

Every new technology should be regulated by authorised companies, which work on creating and maintaining standards and protocols for implementing those technologies.

Law category rises concern of integration edge paradigm into different aspects of everyday life and the complicated relationship between edge technologies and public safety. This category of challenges was mentioned only by one paper.

Table 3 shows which categories mentioned in every article.

*Table 3 Categories of challenges*

| Paper | Architecture | Environment | Resource management | Standards and protocols | Privacy | Law |
|---|---|---|---|---|---|---|
| Zeyu et al., 2020 | × | × | | × | | |
| Mukherjee et al., 2020 | | × | × | | × | |
| Zhang et al., 2018 | | × | | | | |
| Cao et al., 2020 | | × | | | × | |
| Alwakeel, 2021 | | × | | × | × | |
| Alwarafy et al., 2021 | | × | × | × | × | |

| Paper | Architecture | Environment | Resource management | Standards and protocols | Privacy | Law |
|---|---|---|---|---|---|---|
| Tian et al., 2020 | | | | | × | |
| Ali et al., 2021 | × | × | | | × | |
| Singh et al., 2022 | | × | | | | |
| Hagan et al., 2019 | | × | | × | | |
| Liu et al., 2019 | | | | × | × | |
| Garg et al., 2021 | × | × | | | | |
| Anusuya et al., 2021 | | × | | | × | |
| Singh et al., 2021 | | × | | | × | |
| Ranaweera et al., 2019 | | × | × | × | | |
| Sicari et al., 2017 | × | × | × | | | |
| Goyal et al., 2020 | | × | × | | × | |

| Paper | Architecture | Environment | Resource management | Standards and protocols | Privacy | Law |
|---|---|---|---|---|---|---|
| Ranaweera et al., 2021 | × | × | × | × | × | |
| Yahuza et al., 2020 | | × | × | | | |
| Patel et al., 2021 | × | | | × | | |
| Parikh et al., 2019 | × | | | | × | |
| Losavio, 2020 | | | | | × | × |
| Bhat et al., 2020 | | | | × | × | |
| Yu et al., 2018 | × | × | × | | | |
| Singh et al., 2022 | × | × | × | | | |
| Rahman et al., 2017 | × | × | | | | |
| Shirazi et al., 2017 | × | | × | | × | |

| Paper | Architecture | Environment | Resource management | Standards and protocols | Privacy | Law |
|---|---|---|---|---|---|---|
| Zhang et al., 2020 | | | | | × | |
| Roman et al., 2018 | × | | × | | | |
| Khan et al., 2020 | × | × | × | | | |

### 3.2.1 Architecture

In this category studies found to be addressing network architecture and device architecture.

Regarding the network architecture, usually edge computing architecture consists of three layers (Zeyu et al., 2020). The three layers are: a cloud or central data centre, edge devices and an end devices layer (Zeyu et al., 2020). Edge layer consists of micro clouds, microdata centres, separate servers, taken out from the central data centre to the periphery, closer to the data sources (Rahman et al., 2017). Data is collected at the edge of the network, if the device that collects it has its own intelligence, it undergoes primary processing there, if not, it is sent to the edge layer equipment. It processes the data and makes decisions based on it (Rahman et al., 2017). Some data raw or aggregated is sent cloud for storage (Rahman et al., 2017).

Unlike the cloud architecture where all processes are done by a cloud server, there multiple edge servers without any control centre (Ali et al., 2021). Decentralisation has some advantages and disadvantages. One of the purposes of implementing edge model is to offload computation to cloud by distributing data processing among edge nodes, which is possible because of decentralisation (Ali et al., 2021). Another positive point is the improvement of network security, some types of attacks like DoS or DDoS will not hinder performance of the whole network. Properly managed and monitored network can stay safe and continue working even if one of the devices is attacked.

Attacked devices will be shut down and connections to other devices will be cut, preventing adversary of taking control of the network. (Shirazi et al., 2017)

On the downside, decentralised architecture makes edge network a lucrative target for the inside attack (Ali et al., 2021). The information flow can also be controlled by an internal attacker who has sufficient access rights to replace the information (Ali et al., 2021). Resources of the network might be used for malicious purposes (Ali et al., 2021). A separate concern is, all edge systems can be applied to existing underlying infrastructures such as centralized cloud service and mobile network (Yu et al., 2018). These underlying infrastructures are managed by third party providers such as mobile network operators, which causes concern about privacy of user data (Yu et al., 2018).

Another important aspect is device architecture. Edge servers or edge nodes are compact devices designed to be placed closer to end users. Small size of devices limits computing resources of the device, which means that resources to manage security of the gadget are very limited (Ranaweera et al., 2021). IoT devices, mobile devices, and sensors that make up end devices layer have the same problem. Additionally, demand for smart gadgets is high, to stay competitive in the market manufacturers may prioritise speed and number of produced devices, instead of paying attention to devices architecture and security. Vulnerability of the edge nodes and end devices creates the possibility to tamper them. Knowing the location of the edge server, which are placed close to users, both internal and external attackers can gain access to it and steal or change user information. (Ranaweera et al., 2021; Singh et al., 2022; Patel et al., 2021)

### 3.2.2 Environment

Category “Environment” is the most mentioned and discussed in the papers.

Devices and resources from various providers and manufacturers, create a unique heterogenous nature of edge computing (Alwarafy et al., 2021). In principle, with a proper planning an edge computing model can be implemented on already existing infrastructure (Alwarafy et al., 2021). This quality of EC makes it flexible in deployment (Mukherjee et al., 2020). On the other hand, heterogeneity creates security and privacy concerns, because of assortment of standards and protocols (Rahman et al., 2017). This rises the need of new data propagation management between multiple heterogenous devices (Mukherjee et al., 2020).

Data privacy is ensured by encryption mechanisms, but due to architecture of edge and user devices, existing encryption schemes are too cumbersome for limited processing resources (Cao et al., 2020). Furthermore, encrypted user data needs to be processed on edge nodes, which is a difficult process.

Another essential quality of EC is the ability to support the mobility of applications (Cao et al., 2020). Geographical distribution of edge nodes into domains allows users to use application without delays and use the real-time data (Cao et al., 2020; Alwakeel, 2021). However, this characteristic causes many challenges (Cao et al., 2020). Firstly, mobility of the gadgets makes monitoring of devices very hard, it means there might be some obsolete devices, which are critical vulnerability in the network (Singh et al., 2022). Secondly, authentication should happen in each trusted domain where many functional agents, services and infrastructures coexist. Authentication schemes between multiple domains needs to be fast and lightweight. Thirdly, when user connects to a new domain, resource management is difficult (Cao et al., 2020). Finally, mobile, and constantly changing environment makes it easier for perpetrators to bland in and stay unnoticed (Goyal et al., 2020).

### 3.2.3 Resource management

This category touches upon the importance of proper management of the network resources. Efficient resource management at the edge network will enable the use and analysis of big amounts of data and deliver real-time online services (Roman et al., 2018).

Processing of big volumes of data requires fine grained resource management. Some applications need real-time processing, these tasks need to be prioritised and have access to needed computing or storing resources (Goyal et al., 2020). Unique environment of edge networks makes this task challenging.

Edge nodes utilise virtualisation of resources to be able to accommodate high computation demand (Ranaweera et al., 2019). Special Virtualisation Infrastructure Manager (VIM) is responsible for assigning computation resources to the applications (Shirazi et al., 2017). However, virtualisation technique is still a grey zone, with unknown vulnerabilities (Ranaweera et al., 2021).

### 3.2.4 Standards and protocols

Challenges under this category mostly relate to communication protocols. European Telecommunication Standards Institute (ETSI) is responsible for the development of MEC standard simultaneously they also work on 5G standards (Ranaweera et al., 2021).

In relation to communication protocols, heterogenous environment creates difficulties due to many end devices using various communicating protocols (Alwakeel, 2021; Alwarafy et al., 2021). Interconnections between edge nodes are mostly use air channels or short-range channels (Bluetooth or Zigbee, etc.) due to proximity of machines to each other (Ranaweera et al., 2021).

Decentralised architecture together with various communication protocols causes problems related to data privacy, data from one application may be divided and processed on different edge nodes (Liu et al., 2019). This leads to problems to verify integrity of data (Liu et al., 2019). Privacy regulations for edge paradigm are the topic of a future (Ranaweera et al., 2021). Currently General Data Protection Regulation (GDPR) has enforced regulation for securing data and preserving the privacy of people using IoT applications (Ranaweera et al., 2021).

Europe applies GDPR law to protect personal data, which is challenging in some cases, like vehicular networks where vehicles while moving might change network providers or country where different data protection laws are applied. Ortiz et al., (2020) propose the use of virtual layer of edge network to ensure the privacy of data and to make the process of changing between providers or country regulations easier. An on-board unit (OBU) usually need to acquire legislation compliant data, while sharing sensitive data over the network. This task can be assigned to a virtual OBU using edge node.

Papers study some new light weight encryption to ensure the security of communication channels (Alwarafy et al., 2021; Patel et al., 2021).

Category of security standards and protocols is scarcer. The main concern is to ensure the same level of implementation of security standards on all edge nodes, to prevent devices from becoming a vulnerability (Alwakeel, 2021). In the study Patel et al., 2021, discuss that due to limited processing capabilities of the edge devices, there is a need in new lightweight security protocols.

### 3.2.5 Privacy

This section describes the importance of user personal data and devices data, both subcategories are crucial for ensuring privacy.

Data analysis happens in three steps, data collection from end devices, data processing in edge nodes, and storage either in cloud server or edge nodes (Anusuya et al., 2021). Sensitive data about user like location or devices specifications can be targeted at any stages of analysis (Anusuya et al., 2021; Ali et al., 2021). To ensure security of private data creation of regulation in relation to legal responsibilities is imperative (Bhat et al., 2020).

Another important aspect is edge devices data during communication between edge nodes some sensitive data about devices is exchanged (Liu et al., 2019). If this data can be accessed by attacker, he can tamper with devices configurations or create a fake node (Goyal et al., 2020).

### 3.2.6 Law

One paper addressed the lack of study about relation between edge computing and legislation. Losavio (2020) talks about possibility of getting personal data and using it for harming the user.

Environment of edge computing involves many parties, the proper regulations and responsibilities need to exist in case some mistake in configuration or use can lead to accident (Losavio, 2020). Human factor is a serious cause of problems with technologies.

## 3.3 Limitations

Data collection and analysis for this thesis has some limitations. The purpose of this research is to investigate security and privacy challenges, it means that article that mention challenges were collected.

# 4 Discussion and future research directions

Potential of edge computing is promising, and the number of academic publications is high. Studies are tackling different aspects of this technology from developing applications to reviewing possible features and challenges of security and privacy. This thesis discusses categories of challenges to security and privacy and inter relations between them. Table 4 shows comparison between the sample of articles chosen and this work.

*Table 4 Topics covered by articles in the sample for this thesis*

| Topics covered by articles | This thesis |
|---|---|
| Challenges for implementing edge paradigm<br><br>Countermeasures against threats<br><br>New technologies that compatible with edge paradigm<br><br>Possible attacks(/vectors)<br><br>Security and privacy challenges<br><br>Security and privacy requirements | Security and privacy challenges categorised<br><br>Relationships between categories found |

Existing literature laid profound foundation regarding security and privacy challenges of edge computing. There is a considerable gap in number of empirical and conceptual studies. There are eight empirical studies and all of them are experimental. Remaining 22 papers are literature reviews, most of them are narrative and only one used systematic review approach. Yahuza et al., (2020) research security and privacy requirements and state of the art techniques used to counter security threats.

Studies review different challenges of security and privacy. However, some categories are addressed less. Environment is the most discussed category. All the papers mentioned that heterogeneity of edge network is a serious challenge to security and privacy. Variety of edge device,

network providers noted to riser a concern over users' privacy. Authors say there is a need to create new ways to regulate this kind of environment. Open issue here to consider is the creation of a new complex security scheme suitable for edge networks.

Feature of environment like mobility creates challenges mostly in authorisation and authentication. Quick and light applications to administer incoming and outgoing devices, the access to resources, and interconnections between edge nodes. Future research needs to pay more attention to designing and testing authentication technique. Both mobility and heterogeneity need to be taken into account, another important factor is the time. Edge computing supports many applications that rely on real-time data and fast computing, for example in VANET, cars need constant updates on the environment around. When car leaves one edge network and joins another authentication process must be fast without delays.

Privacy is a serious challenge to any kind of emerging technology. Unique environment of edge networks poses a serious concern towards users' data privacy. When data is transmitted to an edge node user loses control over it. To ensure anonymity, integrity, and security of data, a lightweight encryption that can be used on devices with low computing power is the main challenge addressed by studies. Another serious concern is the use of LBS which allows to track real-time location. Some papers propose a solution by using blockchain to secure data privacy.

Connection between edge nodes is essential to guarantee a proper operation of the network. However, edge devices' data that being exchange between nodes is a lucrative target for attacks because it will allow to pinpoint location and get an access to the device. Users' data privacy is a popular topic for researchers; however, edge nodes' data has less coverage. Protecting data of edge nodes that being exchanged between devices is crucial. Edge devices are vulnerable to many attacks, designing security and privacy schemes to ensure that edge node won't be tampered will make networks more reliable and trustworthy.

Architecture of edge devices needs to be addressed. Manufacturers and designers need to pay more attention to the security of devices, existing solutions are not suitable for compact devices with low processing power. Experimental study by Hagan et al., (2019) suggest a software to manage the security of the edge node.

Most of the experimental studies propose some solutions to secure a network architecture, by implementing some existing techniques. There is a disparity in research efforts, edge devices' architecture should be studied more. Future research directions might address the need to safeguard the edge devices' design. Failures in the operation of the edge node because of some manufacturing flaw will influence the work of the whole network. Availability of the node is essential to prevent any delays and interruptions in the traffic of the network. Another direction is to add security layer to micro architecture.

Under category of resource management, the need to a fine grain access control is the main challenge. To ensure that only authorized devices can access resources of edge nodes there is a need to create new control mechanisms suitable for edge devices. Some papers analyse virtualisation and that it is a vulnerability of the edge node. Virtualisation is an important component in managing the resources of a node. Security of virtualisation technique needs to be studied deeper. Future research might investigate how to optimise the use of virtual platforms in edge computing networks.

Standards and protocols mentioned by some papers. Only two papers study this topic. Edge computing is an emerging technology, a proper communication and security regulations are essential. Existing connection and security standards and protocols are unsuitable to apply to edge devices with limited resources. GDPR published regulations concerning IoT devices, given that IoT devices are closely related to edge networks, connection between GDPR and edge computing require more research. This category calls for attention of researchers. Future research should focus on connection between various providers using different standards. Regarding security standards, mobility of the users and edge devices needs be studied. User can join, leave, or migrate to another edge network. Lightweight security scheme needs to consider users' devices not only edge nodes.

Relationship between law and edge technology is mentioned by only one paper. Losavio (2020) pointed the lack of attention directed towards this category. Nonetheless, this paper focuses on United States and the situation with local legal system and fog/edge computing. The need to study relation between administration and edge computing is imperative. Future research direction may be within one country or cover several.

## 4.1 Relationships between categories

Additionally, to being multi-layered each category influences another one and is affected back. Figure 8 shows interconnections between six categories. Even if there is no direct connection, indirect affiliation through another category exists. For example, heterogenous **environment** has direct relation to variety of **standards and protocols** which causes challenges with **privacy.** Figure 8 illustrates that relations are bilateral.

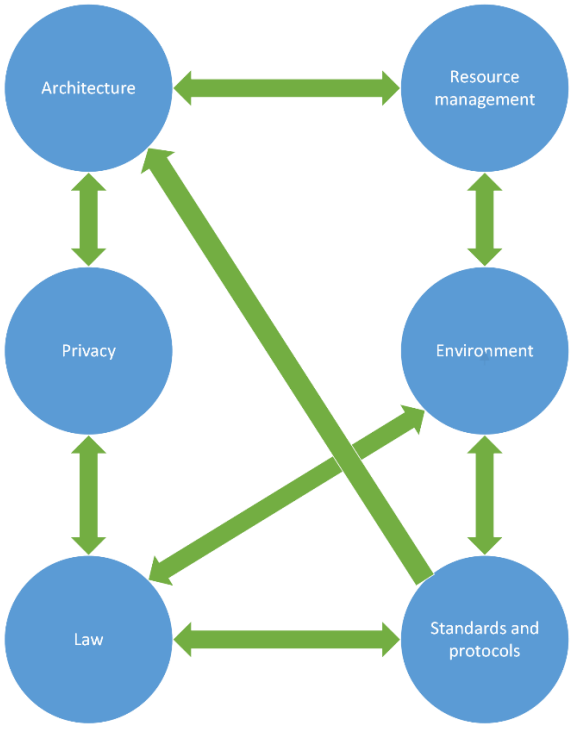


*Figure 8 Relation between categories*

**Network architecture** has direct connection with **privacy** challenges and the need to design new security **standards and protocols.** Edge **device architecture** subcategory directly related to **resource management**, restricted processing resources require very reliable technique to ensure that **resources** are distributed efficiently, and only authorised users can access them. Through **standards and protocols, and privacy** categories there is a relation to **law** category.

Subcategory **heterogeneous environment** has direct connection to variety of **standards and protocols** used by different providers and manufacturers. **Mobility of the environment** directly links to the need of fine-grained **resource management** methods, that can maintain proper authentication of many joining and leaving end devices. Another indirect relation between

environment and law, shows the need to have legal regulations specifically for unique edge computing environment.

Resource management directly influenced by decentralised architecture and by limited hardware capabilities of edge nodes, as well as by mobility of environment.

Privacy of users' data linked to law and standards and protocols categories. There is a need for legal organisations to publish regulations like communication and security standards to guarantee users' privacy. Decentralised architecture directly linked to privacy of edge devices. Decentralisation means edge nodes need to communicate between them. Safety of edge devices relies on safe intercommunication.

Standard and protocols closely related to law and privacy. Every country needs to address users' privacy when using edge networks. Regulations about design of edge devices and requirements to ensure its' security and to protect devices' data. Finally, direct link with the need of standards for network architecture.

Law category relates to standards and protocols, and environment, in relation to administer in case of some accident happens as a result of human factor. In case some misconfiguration or other mistake, who is going to take responsibility in heterogenous environment with many parties.

Security scheme for edge computing requires to be light-weight and complex, considering all possible interrelations between various components, user devices, edge nodes, connection channels, and cloud servers. This scheme needs to manage very large number of devices.

Edge computing differs from cloud computing in architecture and environment. Future research should focus on relations between categories, many unknown challenges unique to edge computing concept will come with time.

# 5 Conclusion

Security is fundamental requirement to a successful edge deployment. Edge nodes are currently the weakest link in network security. The best way to achieve reliable locking is through secure hardware and introduction of new security mechanisms. Key aspects of edge computing include low latency, the ability to perform real-time processing of big data, mobility, and flexibility.

On the other hand, there are many security and privacy challenges that need academic attention. Pre-configuration of platforms and devices requires partnerships between hardware, software, consultants, integrators, and IT service providers. Such partnership should be accompanied by common standards, technological integrations, design tools and control systems. Design of new encryption and authentication mechanisms suitable for edge devices with law processing power.

The analysis of articles found that most of experimental work addresses network architecture. There are visible gaps in the existing research.

# References


Ali, B., Gregory, M. A., & Li, S. (2021). Multi-Access Edge Computing Architecture, Data Security and Privacy: A Review. *IEEE Access*, *9*, 18706–18721. https://doi.org/10.1109/access.2021.3053233

Alwakeel, A. M. (2021). An Overview of Fog Computing and Edge Computing Security and Privacy Issues. *Sensors*, *21*(24), 8226. https://doi.org/10.3390/s21248226

Alwarafy, A., Al-Thelaya, K. A., Abdallah, M., Schneider, J., & Hamdi, M. (2021). A Survey on Security and Privacy Issues in Edge-Computing-Assisted Internet of Things. *IEEE Internet of Things Journal*, *8*(6), 4004–4022. https://doi.org/10.1109/jiot.2020.3015432

Anusuya, R., Renuka, D. K., & Kumar, L. A. (2021). Review on Challenges of Secure Data Analytics in Edge Computing. 2021 International Conference on Computer Communication and Informatics (ICCCI). https://doi.org/10.1109/iccci50826.2021.9402559

Bhat, S. A., Sofi, I. B., & Chi, C. Y. (2020). Edge Computing and Its Convergence With Blockchain in 5G and Beyond: Security, Challenges, and Opportunities. *IEEE Access*, *8*, 205340–205373. https://doi.org/10.1109/access.2020.3037108

Cao, K., Liu, Y., Meng, G., & Sun, Q. (2020). An Overview on Edge Computing Research. *IEEE Access*, *8*, 85714–85728. https://doi.org/10.1109/access.2020.2991734

Costello, K. (2021, February 11). *Predicts 2021: Cloud and Edge Infrastructure Cloud Infrastructure Edge*. Gartner. https://www.gartner.com/smarterwithgartner/gartner-predicts-the-future-of-cloud-and-edge-infrastructure

Garg, S., Kaur, K., Kaddoum, G., Garigipati, P., & Aujla, G. S. (2021). Security in IoT-Driven Mobile Edge Computing: New Paradigms, Challenges, and Opportunities. *IEEE Network*, *35*(5), 298–305. https://doi.org/10.1109/mnet.211.2000526

Goyal, S., Sharma, N., Kaushik, I., Bhushan, B., & Kumar, A. (2020). Precedence & Issues of IoT based on Edge Computing. 2020 IEEE 9th International Conference on Communication Systems and Network Technologies (CSNT). https://doi.org/10.1109/csnt48778.2020.9115789

Hagan, M., Siddiqui, F., & Sezer, S. (2019, August). Enhancing Security and Privacy of Next-Generation Edge Computing Technologies. *2019 17th International Conference on Privacy, Security and Trust (PST)*. https://doi.org/10.1109/pst47121.2019.8949052

IMARC Group. (2022, February). *Edge Computing Market: Industry Trends, Share, Size, Growth, Opportunity and Forecast 2021–2026*. https://www.imarcgroup.com/edge-computing-market

Khan, R., Kumar, P., Jayakody, D. N. K., & Liyanage, M. (2020). A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements, and Future Directions. IEEE Communications Surveys & Tutorials, 22(1), 196–248. https://doi.org/10.1109/comst.2019.2933899

Liu, D., Yan, Z., Ding, W., & Atiquzzaman, M. (2019). A Survey on Secure Data Analytics in Edge Computing. *IEEE Internet of Things Journal*, *6*(3), 4946–4967. https://doi.org/10.1109/jiot.2019.2897619

Losavio, M. (2020). Fog Computing, Edge Computing and a return to privacy and personal autonomy. *Procedia Computer Science*, *171*, 1750–1759. https://doi.org/10.1016/j.procs.2020.04.188

Mukherjee, M., Matam, R., Mavromoustakis, C. X., Jiang, H., Mastorakis, G., & Guo, M. (2020). Intelligent Edge Computing: Security and Privacy Challenges. *IEEE Communications Magazine*, *58*(9), 26–31. https://doi.org/10.1109/mcom.001.2000297

Ortiz, J., Fernandez, P. J., Sanchez-Iborra, R., Bernabe, J. B., Santa, J., & Skarmeta, A. (2020). Enforcing GDPR regulation to vehicular 5G communications using edge virtual counterparts. 2020 IEEE 3rd 5G World Forum (5GWF). https://doi.org/10.1109/5gwf49715.2020.9221248

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

Patel, Y., Rawal, B. S., Liu, Y., & Rahman, M. T. (2021). Security and Privacy Challenges in 5G-enabled Technology. *2021 8th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2021 7th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom)*. https://doi.org/10.1109/cscloud-edgecom52276.2021.00020

Rahman, A., Hassanain, E., & Hossain, M. S. (2017). Towards a Secure Mobile Edge Computing Framework for Hajj. IEEE Access, 5, 11768–11781. https://doi.org/10.1109/access.2017.2716782

Ranaweera, P., Jurcut, A. D., & Liyanage, M. (2019, October). Realizing Multi-Access Edge Computing Feasibility: Security Perspective. 2019 IEEE Conference on Standards for Communications and Networking (CSCN). https://doi.org/10.1109/cscn.2019.8931357

Ranaweera, P., Jurcut, A. D., & Liyanage, M. (2021). Survey on Multi-Access Edge Computing Security and Privacy. *IEEE Communications Surveys & Tutorials*, *23*(2), 1078–1124. https://doi.org/10.1109/comst.2021.3062546

Roman, R., Lopez, J., & Mambo, M. (2018). Mobile edge computing, Fog et al.: A survey and analysis of security threats and challenges. Future Generation Computer Systems, 78, 680–698. https://doi.org/10.1016/j.future.2016.11.009

Sicari, S., Rizzardi, A., Miorandi, D., & Coen-Porisini, A. (2017). Security towards the edge: Sticky policy enforcement for networked smart objects. *Information Systems*, *71*, 78–89. https://doi.org/10.1016/j.is.2017.07.006

Singh, A., Satapathy, S. C., Roy, A., & Gutub, A. (2022). AI-Based Mobile Edge Computing for IoT: Applications, Challenges, and Future Scope. *Arabian Journal for Science and Engineering*. https://doi.org/10.1007/s13369-021-06348-2

Singh, J., Bello, Y., Hussein, A. R., Erbad, A., & Mohamed, A. (2021). Hierarchical Security Paradigm for IoT Multiaccess Edge Computing. *IEEE Internet of Things Journal*, *8*(7), 5794–5805. https://doi.org/10.1109/jiot.2020.3033265

Singh, S., Sulthana, R., Shewale, T., Chamola, V., Benslimane, A., & Sikdar, B. (2022). Machine-Learning-Assisted Security and Privacy Provisioning for Edge Computing: A Survey. *IEEE Internet of Things Journal*, *9*(1), 236–260. https://doi.org/10.1109/jiot.2021.3098051

Shirazi, S. N., Gouglidis, A., Farshad, A., & Hutchison, D. (2017). The Extended Cloud: Review and Analysis of Mobile Edge Computing and Fog From a Security and Resilience Perspective. IEEE Journal on Selected Areas in Communications, 35(11), 2586–2595. https://doi.org/10.1109/jsac.2017.2760478

Sittón-Candanedo, I., Alonso, R. S., García, S., Gil, A. B., & Rodríguez-González, S. (2019). A Review on Edge Computing in Smart Energy by means of a Systematic Mapping Study. *Electronics*, *9*(1), 48. https://doi.org/10.3390/electronics9010048

Stratus Technologies. (2019, September). *Edge Computing Trend Report*. https://lp.stratus.com/wp-content/uploads/stratus-edge-computing-trend-report-americas.pdf

Tian, Z., Wang, Y., Sun, Y., & Qiu, J. (2020). Location Privacy Challenges in Mobile Edge Computing: Classification and Exploration. *IEEE Network*, *34*(2), 52–56. https://doi.org/10.1109/mnet.001.1900139

Watson, R. T., & Webster, J. (2002). Analyzing the Past to Prepare for the Future: Writing a Literature Review. *MIS Quarterly*, *26*(2), xiii. http://www.jstor.org/stable/4132319

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

Yu, W., Liang, F., He, X., Hatcher, W. G., Lu, C., Lin, J., & Yang, X. (2018). A Survey on the Edge Computing for the Internet of Things. IEEE Access, 6, 6900–6919. https://doi.org/10.1109/access.2017.2778504

Zeyu, H., Geming, X., Zhaohang, W., & Sen, Y. (2020). Survey on Edge Computing Security. *2020 International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE)*. https://doi.org/10.1109/icbaie49996.2020.00027

Zhang, D., & Fan, L. (2020). Cerberus: Privacy-Preserving Computation in Edge Computing. IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). https://doi.org/10.1109/infocomwkshps50562.2020.9162942

Zhang, J., Chen, B., Zhao, Y., Cheng, X., & Hu, F. (2018). Data Security and Privacy-Preserving in Edge Computing Paradigm: Survey and Open Issues. *IEEE Access*, *6*, 18209–18237. https://doi.org/10.1109/access.2018.2820162