Bachelor Degree Project

Edge Computing Security for IoT

- A Systematic Literature Review

Authors:
Albin Johnsson
Adam Nordling
Supervisor: Arslan Musaddiq
Examiner: Mauro Caporuscio
Semester: VT 2023
Subject: Computer Science

Abstract

This study conducts a systematic literature review (SLR) to explore the security threats, their mitigation strategies, and the roles of blockchain and 5G technologies in enhancing the security of IoT devices in edge computing environments. Utilizing digital libraries as resources, the review examines three research questions that delve into the common security threats for IoT devices in edge computing, the unique security issues for sensors, gateways, and actuators, and the advantages of integrating blockchain and 5G technologies into edge computing security for IoT systems. A total of 1667 articles in four digital libraries was identified through three distinct search strings aligned with the research questions where a selected sample comprising 82 primary articles was analyzed. The results reveal a wide variety of security threats, including Distributed Denial-of-Service (DDoS) and Denial-of-Service (DoS) attacks, Man-in-the-Middle (MITM) attacks, and malware injections, among others, with mitigation strategies spanning intrusion detection systems (IDS), firewalls, and cryptographic methods. Furthermore, it was found that the security issues unique to sensors, gateways, and actuators are mostly distinct, necessitating tailored countermeasures. The research also highlights the prospective advantages of integrating blockchain and 5G technologies into edge computing for IoT systems, emphasizing potential improvements in security, privacy, and trust. While analyzing the articles for the third research question it became evident that the advantages of implementing these technologies significantly outweigh the few disadvantages encountered. The conclusion of the study highlights the importance of a solid understanding of these security threats, mitigation strategies, and the advantages of integrating blockchain or 5G in edge computing for IoT.

Keywords: *Edge Computing, Internet of Things (IoT), Security Threats, Mitigation Strategies, Blockchain, 5G, Systematic Literature Review*

Preface

In this SLR titled "Edge Computing Security for IoT", we explore the challenges and solutions in securing edge computing systems within the Internet of Things (IoT) context. The aim is to provide valuable insights into potential threats, vulnerabilities, and mitigation strategies in this rapidly evolving field.

We would like to extend our heartfelt gratitude to our supervisor, Arslan Musaddiq, for his guidance and support throughout this research project.

Contents

1 Introduction

The rapid growth of the IoT in recent years has led to an increased demand for computing resources closer to the edge of the network [1]. Edge computing (EC) has emerged as a promising solution to address the challenges of latency, bandwidth, and data privacy in IoT [2]. However, ensuring the security of IoT devices and data at the edge presents unique security issues and threats.

In this bachelor thesis, we aim to conduct an SLR on EC security for IoT. Specifically, our goal is to identify the most common security threats faced by IoT devices in EC environments, the most effective strategies for mitigating each of these threats, and the unique security issues faced by different types of IoT devices (sensors, gateways, actuators) at the edge. We also compare the effectiveness of different mitigation strategies for each type of threat and different security approaches for each type of device.

Additionally, we'll look at how new technologies like blockchain and 5G may affect the security of EC for IoT and compare the potential advantages of integrating these technologies for security.

To achieve these objectives, we first explain our research methodology and search strategy for identifying relevant literature. We then conduct a systematic review of existing literature on EC security for IoT, focusing on the themes of threats and mitigation strategies, security issues for different types of IoT devices, and the advantages of blockchain and 5G integration.

1.1 Background

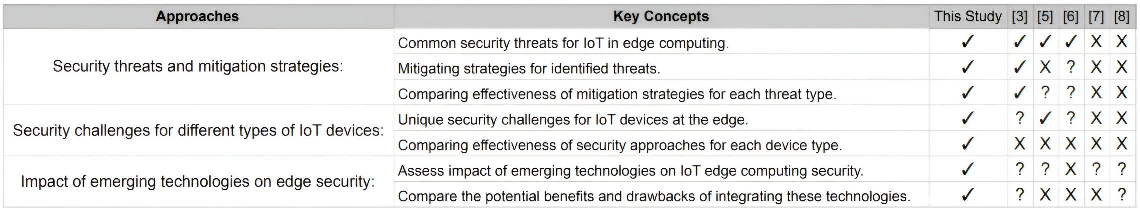
EC is an emerging computing technology that refers to a range of networks and devices located in close proximity to the user. The general idea of EC is to process data in close proximity to where it is being generated, this therefore enables processing at greater speeds as well as volumes. Thereby, IoT data can be gathered and processed at the edge, instead of sending the data center back to a data center or the cloud. This strategy enables rapid analysis and processing of data.

However, the implementation of EC in IoT also introduces numerous security issues and threats. These include, but are not limited to, DDoS attacks, DoS attacks, replay attacks, and many other attack scenarios [3].

As the security threats associated with EC in IoT continue to evolve, it is essential for users to consider how they can effectively manage and mitigate these threats. Current mitigation strategies include the use of IDS, firewalls, as well as authentication and authorization mechanisms, among others [4]. However, it is important to note that these strategies are not exhaustive and other measures may also need to be taken to ensure the security and reliability of EC security in IoT systems.

1.2 Related work

Table 1.1: Comparison Table



Approaches	Key Concepts	This Study	[3]	[5]	[6]	[7]	[8]
Security threats and mitigation strategies:	Common security threats for IoT in edge computing.	✓	✓	✓	✓	X	X
	Mitigating strategies for identified threats.	✓	✓	X	?	X	X
	Comparing effectiveness of mitigation strategies for each threat type.	✓	✓	?	?	X	X
Security challenges for different types of IoT devices:	Unique security challenges for IoT devices at the edge.	✓	?	✓	?	X	X
	Comparing effectiveness of security approaches for each device type.	✓	X	X	X	X	X
Impact of emerging technologies on edge security:	Assess impact of emerging technologies on IoT edge computing security.	✓	?	?	X	?	?
	Compare the potential benefits and drawbacks of integrating these technologies.	✓	?	X	X	X	?

✓	Completely answers the topic.
?	Partially answers the topic.
X	Does not answer the topic.

Table 1.1 presents a comparative table that pits our primary concepts with previous articles to offer an overview of the existing research and identify any gaps in knowledge. This process assists us in formulating research questions based on existing literature gaps and building upon the prior work of researchers.

The article by Vikas et al. explores security vulnerabilities in IoT and EC, reviewing numerous types of threats across diverse tiers of an IoT application, and delves into the exploration of potential countermeasures involving cutting-edge technologies such as blockchain and EC. The authors emphasize the possible advantages and disadvantages of integrating these technologies for security while also discussing the particular vulnerabilities of edge devices. They also outline unresolved problems and potential future study topics for improving IoT security. This comprehensive survey aims to aid the development and enhancement of security measures in IoT applications [3].

Ni et al. [5] explores the potential of mobile edge computing (MEC) to improve data analysis for IoT applications while maintaining data security and computational efficiency. The authors describe the overall architecture of MEC-assisted IoT and several promising applications, followed by an in-depth examination of security, privacy, and efficiency challenges in MEC. They discuss the trade-offs between security and efficiency in data usage and investigate research opportunities to tackle these issues, such as secure data aggregation, secure data deduplication, and secure computational offloading. The article points out several intriguing directions for future research into secure and efficient data analysis in MEC-assisted IoT, offering valuable insights for future articles in this field.

Shen et al. [6] delve into the security challenges and energy consumption trade-offs in edge-assisted IoT systems. With the emergence of 5G networks, EC has become a critical component in IoT architectures, providing lower latency, reduced energy consumption, and decreased network bandwidth usage. However, edge-assisted IoT faces numerous security issues due to the inherent vulnerabilities of edge nodes and the sensitive nature of collected data. Shen and colleagues discuss the architecture of edge-assisted IoT, its unique features, and its security threats. They also discuss the trade-offs between security and energy efficiency, using a case study of DDoS attacks and malware injection attacks to suggest a preliminary solution to address these conflicting demands. Using simulations, they prove the success of their proposed method and highlight remaining problems and possible future study areas for security and energy use in IoT systems assisted by EC.

In their article, Pan and Yang [7] examine the paradigm shift towards the IoT and the rise of EC, emphasizing the potential benefits and new cybersecurity challenges resulting from this shift. The article identifies five cybersecurity challenges and five emerging opportunities related to the convergence of cybersecurity, EC, IoT, and artificial intelligence (AI). The authors stress the potential for synergy between the "EC + IoT" platform and emerging blockchain and AI technologies, which could yield numerous benefits in various IoT application domains, such as smart homes, smart transportation, smart health, smart grids, and smart energy.

The article by Jazaeri et al. [8] centers on the integration of Software Defined Networking (SDN), EC, and IoT as a unified platform to tackle the challenges of IoT network management, security risks, and data processing. The article presents an SLR of 139 articles conducted between 2013 and 2021, analyzing 74 articles that focus on the use of EC and SDN in IoT environments. The authors discuss the benefits of combining SDN, EC, and IoT technologies and propose an SDN-EC-IoT platform optimized to use network resource virtualization for managing heterogeneous IoT devices. Additionally, the article highlights key challenges such as network bandwidth, latency, security, and data accumulation, while also providing future research directions and open issues related to standardization, implementation, techniques, and requirements in this domain.

As evident from our comparison table, the first article comprehensively addresses the topic of strategies and mitigation, while all other articles partially address the topics of our research questions. This indicates that there are knowledge gaps to be filled, which is the primary objective of this thesis. By examining and comparing the findings of these articles, our goal is to enhance the comprehension of security threats in EC for IoT. We also aim to identify the most effective strategies for mitigating these threats, address the unique security issues encountered by various types of IoT devices, and explore the advantages of integrating blockchain and 5G in EC security for IoT.

1.3 Problem formulation

The fields of EC and IoT are rapidly expanding, there is already a significant body of research available. However, this research does not provide a comprehensive understanding of how security threats in IoT can be mitigated within EC, nor does it consider emerging technologies such as Blockchain and 5G. Additionally, the current research does not offer a complete view of the distinct security issues posed by different edge-related IoT devices.

Therefore, our research questions are as follows:

RQ1	What are the most common security threats faced by IoT devices in edge computing, and what are the most effective strategies for mitigating these threats?
RQ2	What are the unique security issues or threats presented by sensors, gateways, and actuators in edge computing for IoT, and what are the most effective countermeasures for securing these types of devices?
RQ3	What are the advantages of integrating Blockchain and 5G technologies into edge computing security for IoT?

Due to their crucial role in EC, we decided to focus on sensors, gateways, and actuators as the primary IoT devices in our second research question. Similarly, in light of their increasing adoption and potential benefits for enhancing the security of IoT devices and facilitating their communication with both edge servers and cloud resources, we chose to explore Blockchain and 5G. These are emerging technologies that could significantly impact the security of EC in IoT systems

1.4 Motivation

The IoT has been growing rapidly over the years, with an increasing need for faster and more efficient data processing and handling [1]. In order to meet this demand, EC has been proposed as a solution to handle IoT data more rapidly [2]. EC involves processing and analyzing data closer to where it is generated, rather than sending it to a centralized cloud or data center. This approach allows for faster data processing and response times, as well as reducing the amount of data that needs to be sent over the network.

However, the expansion of IoT and EC also present security threats [9]. These threats include but are not limited to DDoS attacks, DoS attacks, replay attacks, and other types of cyberattacks. As more devices are connected to the internet, the potential attack surface area also increases, making it more challenging to secure the IoT ecosystem.

The purpose of this thesis is to inform readers and other interested parties about the current security threats associated with EC for IoT, as well as emerging technologies and mitigation strategies [2]. By drawing attention to these threats, the thesis aims to contribute to the development of secure and reliable EC solutions for IoT data handling and processing.

1.5 Scope/Limitation

As with any study, there are some limitations to consider. The scope of this SLR is to review existing literature related to EC security issues or threats in IoT environments, published between 2015 and 2023. The year 2015 has been chosen as a starting date since EC and IoT started to gain significant traction during this period. We focused our search on Scopus, IEEE Xplore, ACM DL, and Web of Science in order to ensure the level of quality of the primary articles used in this study. Guidelines suggested by Kitchenham [10, 11] had an impact on the selection of these digital libraries. While other sources were taken into consideration, due to time restrictions, we chose to concentrate on these four digital libraries because we thought they would offer a thorough foundation for our research.

First, our study specifically looks at security issues or threats in EC environments in IoT, and we do not examine security in other types of computing environments. We are also limited by the information available on emerging technologies like Blockchain and 5G, as these technologies are still new and may not have been studied extensively in the context of EC security for IoT.

Another limitation is that our findings are based on existing literature, and we are not collecting new data or conducting empirical analysis. This means that our results may not account for the most recent developments in EC security.

Finally, our study primarily focuses on security challenges and solutions for IoT devices at the edge, which are the subject of our first two research questions. However, our third research question deviates from this focus to explore all advantages related to security for EC in IoT. Even though our investigation does not delve into broader issues related to privacy, data ownership, and regulatory compliance within the context of the first two questions, we believe our research offers valuable insights into security threats and solutions for EC environments in IoT, serving as a potential starting point for future research.

1.6 Target group

The primary objective of this research project is to perform an extensive analysis of various attack scenarios and mitigation strategies in the context of EC within IoT. To achieve this goal, a comprehensive literature review has been conducted to identify the latest trends and developments in this field.

The study also explores the potential applications of emerging technologies in EC and IoT. This involves an assessment of the capabilities and limitations of these technologies, as well as their potential impact on IT security and risk mitigation strategies.

The thesis aims to provide a detailed overview of the emerging security threats within IoT in EC, as well as current mitigation strategies for these risks. By doing so, the study helps IT security professionals to better understand the latest threats and vulnerabilities in this area, and equip them with the knowledge and tools needed to effectively address them.

Moreover, this research provides valuable insights for IoT device manufacturers and network technicians, who are responsible for designing and implementing secure systems that can withstand potential cyberattacks. By highlighting the latest trends and developments in the field of EC within IoT, this study helps these stakeholders to stay ahead of the curve and develop more effective threat mitigation strategies.

Ultimately, the goal of this thesis is to contribute to the body of knowledge in the IT security community and provide a solid foundation for future research in this area.

1.7 Outline

The thesis is organized into several sections that each contribute to the overall understanding of the topic.

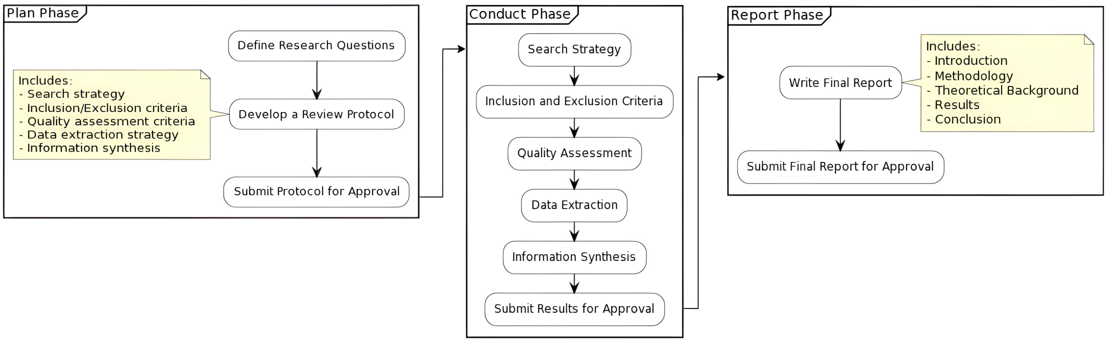
- **Section 2: Methodology**
  - This section introduces the SLR approach, followed by a description of the review process, including the five activities of the SLR.
  - Reliability and validity are also discussed in this section.
- **Section 3: Theoretical Background**
  - In this section, the background of EC, IoT, Blockchain, 5G, and related security aspects are discussed in detail.
- **Section 4: Results**
  - In this section, the information from the primary articles is presented and analyzed by answering each research question (e.g., RQ1, RQ2, and RQ3).
- **Section 5: Conclusion and Future Work**
  - This section provides a summary of the findings and potential avenues for future research in the area of EC security for IoT.

2 Method

In this thesis, we carry out an SLR by following the step-by-step guidelines for conducting an SLR in software engineering, as proposed by Kitchenham [10, 11]. After conducting a comprehensive review of existing literature on security in IoT EC, the SLR provides an in-depth analysis and summary of the findings. This analysis gives us a clear understanding of what's currently known, what's not yet known, and where future research could be focused. The subsequent sections delve into the systematic literature methodology, explore the review process, and address aspects of reliability, and validity.

2.1 Systematic literature approach

The systematic literature approach is about specifying the review process that has been followed in this thesis project which is shown in Figure 2.1 below. The review process which is from Kitchenham has the following phases: 1) Plan Phase, 2) Conduct Phase, and 3) Report Phase [10, 11].



Plan Phase
Define Research Questions
Develop a Review Protocol
Submit Protocol for Approval
Includes:
- Search strategy
- Inclusion/Exclusion criteria
- Quality assessment criteria
- Data extraction strategy
- Information synthesis
Conduct Phase
Search Strategy
Inclusion and Exclusion Criteria
Quality Assessment
Data Extraction
Information Synthesis
Submit Results for Approval
Report Phase
Write Final Report
Submit Final Report for Approval
Includes:
- Introduction
- Methodology
- Theoretical Background
- Results
- Conclusion

Figure 2.1: The systematic literature review process based on [10, 11].

Plan phase: In the planning phase, we identify the need for the SLR as has been shown in the earlier sections by going into the background and presenting the knowledge gaps of the current literature in our comparison table. Draft searches in various digital libraries have to be established and also plan the review protocol which conducts the SLR with five activities [10, 11].

Conduct phase: The conduct phase is executed after the planning phase and consists of these five activities that help organize and complete the literature review:

1. *Search strategy:* The search strategy involves identifying relevant keywords and constructing a search string that can be used to retrieve all relevant articles while minimizing irrelevant results. The relevant keywords are directly related to the research questions.

2. *Inclusion and exclusion criteria:* The inclusion and exclusion criteria are used to determine which articles to include or exclude from the review based on their characteristics. These criteria are applied to the titles and abstracts of the articles retrieved from the digital libraries to assess their relevance to the research question. Specifying the criteria is essential for efficiently filtering out non-relevant articles.

3. *Quality Assessment:* To ensure the reliability of the literature review's conclusions, it is essential to evaluate the methodological quality and validity of the chosen arti-

cles, which is achieved by assessing and documenting their quality of them using a quality assessment form.

4. *Data extraction:* To systematically collect and document relevant information from primary articles, data is collected and documented using a data items form.
5. *Information synthesis:* The information synthesis stage involves analyzing, integrating, and interpreting the extracted data to generate meaningful insights that address the research questions. This includes visualizing quantitative results in the form of charts and tables, explaining qualitative results with textual discussions, and separating quantitative results from qualitative results.

While the difficulty or time required for some of these activities may vary, it's crucial that each one is carefully carried out in order to guarantee an objective and thorough review of the available literature. The report phase is the next step after the conduct phase has been completed [10, 11].

Report phase: Following the conduct phase is the report phase, during which the results of the comprehensive literature review are presented and discussed. The review process and its results are presented in this phase in a manner that is clear, thorough, and transparent [10, 11].

2.2 Review process

This SLR is conducted through five activities. These are:

1. Search strategy
2. Inclusion and exclusion criteria
3. Quality assessment
4. Data extraction
5. Information synthesis

These steps are based on the Kitchenham guidelines for carrying out an SLR [10, 11].

2.2.1 Search strategy

The search strategy for this SLR is divided into three separate searches, with each focusing on a specific research question. Utilizing different keywords in the search string enables the discovery of more articles relevant to each question. The objective of these searches is to identify relevant articles that can be analyzed in the results section.

The search is restricted to four digital libraries: Scopus, IEEE Explore, ACM DL, and Web of Science, as recommended by [10]. The report encompasses articles published between 2015 and 2023. The reason for using 2015 as the initial year is because that is when EC was defined as a common computing paradigm and thereafter became more regularly used [12].

The search string used in Scopus is the Title, Abstract, and Keywords, while it is used in the full texts of the publications in IEEE Xplore, ACM DL, and Web of Science. The majority of IEEE and ACM publications are indexed in Scopus, therefore, by searching the Titles, Abstracts, and Keywords, it is possible to exclude less relevant articles. This is why searching in the Title, Abstract, and Keywords and not in full texts in Scopus is recommended.

Table 2.2 corresponds to the first research question, which explores the most common security threats faced by IoT devices in EC and the optimal mitigation techniques to address these threats:

Table 2.2: Research Question 1 Search String.

Digital Library	**Search String**
Scopus	TITLE-ABS-KEY(("edge computing") AND ("security") AND ("IoT" OR "Internet of Things") AND ("threats" OR "risks" OR "vulnerabilities") AND ("mitigation" OR "countermeasures"))
IEEE Xplore	("edge computing") AND ("security") AND ("IoT" OR "Internet of Things") AND ("threats" OR "risks" OR "vulnerabilities") AND ("mitigation" OR "countermeasures")
ACM DL	[All: "edge computing"] AND [All: "security"] AND [[All: "iot"] OR [All: "internet of things"]] AND [[All: "threats"] OR [All: "risks"] OR [All: "vulnerabilities"]] AND [[All: "mitigation"] OR [All: "countermeasures"]]
Web of Science	("edge computing") AND ("security") AND ("IoT" OR "Internet of Things") AND ("threats" OR "risks" OR "vulnerabilities") AND ("mitigation" OR "countermeasures")

Table 2.3 relates to the second research question, which explores the security issues or threats relating to sensors, gateways, and actuators in EC for IoT, as well as the best methods to secure each type of device:

Table 2.3: Research Question 2 Search String.

Digital Library	**Search String**
Scopus	TITLE-ABS-KEY(("edge computing") AND ("security") AND ("IoT" OR "Internet of Things") AND ("sensors" OR "gateways" OR "actuators") AND ("security issues" OR "threats" OR "vulnerabilities"))
IEEE Xplore	("edge computing") AND ("security") AND ("IoT" OR "Internet of Things") AND ("sensors" OR "gateways" OR "actuators") AND ("security issues" OR "threats" OR "vulnerabilities")
ACM DL	[All: "edge computing"] AND [All: "security"] AND [[All: "iot"] OR [All: "internet of things"]] AND [[All: "sensors"] OR [All: "gateways"] OR [All: "actuators"]] AND [[All: "security issues"] OR [All: "threats"] OR [All: "vulnerabilities"]]
Web of Science	("edge computing") AND ("security") AND ("IoT" OR "Internet of Things") AND ("sensors" OR "gateways" OR "actuators") AND ("security issues" OR "threats" OR "vulnerabilities")

Table 2.4 is associated with our third research question, which explores the potential benefits of integrating advanced technologies such as Blockchain and 5G into EC security for IoT. Initially, our research parameters were broader, including terms like "disadvantages" and "impact" in our search string. This decision was made to ensure a comprehensive review of the literature and to fully investigate the potential effects of these technologies on EC security for IoT. However, as our SLR progressed, we noticed a lack of significant findings related to the disadvantages or impacts of these technologies in the context of EC-IoT security. Consequently, we shifted our focus to exclusively concentrate on the 'advantages'. This transition is reflective of the dynamic nature of research, where the focus may evolve based on the findings. The narrowed focus on 'advantages' does not invalidate our original search string, but rather underscores the depth of our exploration into the literature on the subject.

Table 2.4: Research Question 3 Search String.

Digital Library	**Search String**
Scopus	TITLE-ABS-KEY ("edge computing") AND ("security") AND ("IoT" OR "Internet of Things") AND ("Blockchain" OR "5G") AND ("disadvantages" OR "advantages" OR "cons" OR "impact" OR "benefits" OR "drawbacks")
IEEE Xplore	("edge computing") AND ("security") AND ("IoT" OR "Internet of Things") AND ("Blockchain" OR "5G") AND ("disadvantages" OR "advantages" OR "cons" OR "impact" OR "benefits" OR "drawbacks")
ACM DL	[All: "edge computing"] AND [All: "security"] AND [[All: "iot"] OR [All: "internet of things"]] AND [[All: "blockchain"] OR [All: "5g"]] AND [[All: "disadvantages"] OR [All: "advantages"] OR [All: "cons"] OR [All: "impact"] OR [All: "benefits"] OR [All: "drawbacks"]]
Web of Science	("edge computing") AND ("security") AND ("IoT" OR "Internet of Things") AND ("Blockchain" OR "5G") AND ("disadvantages" OR "advantages" OR "cons" OR "impact" OR "benefits" OR "drawbacks")

2.2.2 Inclusion and exclusion criteria

Upon completion of the automated and manual search, the relevance of the articles must be evaluated. This is achieved by implementing inclusion and exclusion criteria to the articles' titles and abstracts. If it is not evident from the title or abstract whether the articles fulfill any of the inclusion or exclusion criteria, additional sections of the articles are examined. These criteria are derived from the research questions presented in Section 1.3.

Inclusion criteria: For an article to be included, it does not have to meet all the inclusion criteria. But since our research questions are divided into three search strings, we have different inclusion criteria for each research question. Therefore, the inclusion criteria can be expressed with the following operators: IC1, IC2, IC3, IC4, and IC5.

For RQ1, only include articles that meet IC1 or IC2:

- IC1: The article investigates common security threats faced by IoT devices in edge computing.

- IC2: The article investigates effective mitigation strategies for threats faced by IoT devices in edge computing.

For RQ2, only include articles that meet IC3 or IC4:

- IC3: The article investigates different security issues or threats for gateways, sensors, and actuators.

- IC4: The article investigates security countermeasures for gateways, sensors, and actuators.

For RQ3, only include articles that meet IC5:

- IC5: The article investigates potential advantages, impacts, or disadvantages of integration of Blockchain or 5G on the security of EC in IoT.

Exclusion criteria: For an article to be excluded, it matches any of the exclusion criteria. Therefore the exclusion criteria can be expressed with the following operators: EC1, EC2, and EC3.

- EC1: Articles of low quality: Articles that achieve a score of 1 or less than 1 whilst being assessed with the quality assessment score specified in Table 2.5 are thereby excluded from the SLR.

- EC2: Duplicate articles: As the digital libraries Scopus and Web of Science index articles from IEEE Xplore and ACM Digital Library, there is a risk of encountering duplicate articles during the search process. To address this concern, we utilized the Zotero software [13], which has a built-in feature that allows for the efficient detection and removal of duplicates, thus ensuring the uniqueness of our source material.

- EC3: Articles that are not written in English: These can be effectively filtered out using the language settings in both Scopus and Web of Science. Although IEEE Xplore and ACM Digital Library do host a small proportion of non-English content, the predominance of English language articles in these databases largely mitigates this concern.

2.2.3 Quality assessment

By making use of a quality assessment table, a quality check can be performed for each article. Gathering this data is crucial for the analysis and interpretation of the findings throughout the process of information synthesis. The quality assessment items, specified in Table 2.5, are based on the work of Kitchenham [10, 11] as well as [14].

Table 2.5: Quality assessment items.

Quality Assessment Item	**Quality Assessment Options**
QAI1	**Is a problem definition in the article?** (1) The article describes the problem and is addressed by the article. (0.5) The article defines general problems but does not address any. (0) The problem is not defined.
QAI2	**Is a research methodology described in the article?** (1) The article describes the steps of how the research is conducted. (0.5) The methodology is described partially. (0) The research methodology is not described.
QAI3	**Are there contributions and results discussed in the article?** (1) The article clearly details the contributions or results. (0.5) The results or contributions are discussed partially, or it is not clear what the results are. (0) Contributions or results are not discussed.
QAI4	**Does the article discuss or conclude the findings of the conducted research?** (1) The article draws a clear conclusion or has a discussion. (0.5) The article has a partial conclusion or discussion. (0) Conclusion or discussion are not specified.

If an article meets a quality assessment item (QAI) fully it is awarded 1 point, 0.5 points are awarded if the article partially addresses the issue, and 0 points when an article does not fulfill that item at all. Therefore, the maximum score for an article is 4 points.

2.2.4 Data extraction

The main goal of the data extraction form is to gather general and highly relevant data in relation to the research questions. This entails gathering information that is both broadly applicable and contributes to a deeper understanding, as well as specifics that are directly related to the research questions under consideration. To extract the data, a single data extraction form with different data extraction items (DEIs) for each research question is used. The form is based on the data extraction by Kitchenham [10, 11]. The data extraction form can be seen in Table 2.6.

Data extraction items DEI1 through DEI6 in the data extraction process aid in capturing basic information from the primary articles. This includes details such as the articles' year, title, authors, the digital library where the articles were found, and the type of publication. The publication type reveals if the article was published in a journal, as part of conference proceedings, within a book chapter, or in other formats. DEI6 makes use of the Quality Assessment Table 2.5 to ensure the included articles are of sufficient quality.

The remaining DEIs are specific to each research question. For RQ1, DEI7 and DEI8 focus on common security threats and effective mitigation strategies, respectively. For RQ2, DEI9 and DEI10 cover security issues for sensors, gateways, and actuators, as well as security countermeasures for these devices. Finally, for RQ3, DEI11 and DEI12 were designed to extract data on the advantages of integrating 5G and Blockchain, respectively, into EC Security for IoT. As our review found no significant disadvantages in the primary articles, we decided not to include a data extraction item for disadvantages.

Table 2.6: Data Extraction Form.

Item	Information to extract	Category
DEI1	Year	General
DEI2	Title	General
DEI3	Author	General
DEI4	Digital Library	General
DEI5	Publication Type	General
DEI6	Quality Assessment Score	RQ1, RQ2, RQ3
DEI7	Common Security Threats	RQ1
DEI8	Effective Mitigation Strategies	RQ1
DEI9	Issues for Sensors, Gateways, and Actuators	RQ2
DEI10	Countermeasures for Sensors, Gateways, and Actuators	RQ2
DEI11	Advantages of Blockchain Integration in EC-IoT Security	RQ3
DEI12	Advantages of 5G Integration in EC-IoT Security	RQ3

2.2.5 Information synthesis

The most common security threats faced by IoT devices in EC security include DDoS attacks, DoS attacks, malware injections, and MITM attacks. To mitigate these threats, effective strategies involve a combination of firewalls, cryptography, packet filters, pretesting, IDS, and firmware security (RQ1).

Different types of IoT devices, such as sensors, gateways, and actuators, present unique security issues/threats at the edge. Sensors, being resource-constrained, require lightweight security protocols, while gateways demand strong authentication and access control mechanisms. Actuators need to be protected against unauthorized commands and should employ real-time monitoring solutions. Tailoring security countermeasures to each device type is crucial for ensuring overall system security (RQ2).

Blockchain and 5G technologies offer significant advantages for EC security in the IoT. Blockchain enhances security through features like enhanced privacy, decentralized storage, data audibility, and trusted identity verification. It ensures data integrity, transparency, and authenticity while enabling decentralized storage and securing SDN-supported IoT networks. Additionally, 5G provides improved security, privacy, and device access management. It offers faster data transmission, increased network dependability, and customized network solutions. However, careful consideration of their potential disadvantages, such as energy use, scalability, integration issues, infrastructure costs, and cybersecurity risks, is essential when incorporating these technologies into EC settings (RQ3).

2.3 Reliability and validity

In order to ensure the reliability of our SLR, this thesis employs a strict and transparent methodology for selecting and analyzing the literature. The importance of reliability in a thesis can be attributed to the fact that if our work could be replicated by someone else under identical conditions, the results would be the same. If such replication is possible, the work can be regarded as reliable. The review process, which consists of the five activities that have been in-depth described in Section 2.2, is the primary factor in ensuring the reliability of the thesis work. If the replicate follows these five activities through the review process, reliability should be attained.

When it comes to validity, there are three different concerns: construct validity, internal validity, and external validity [15]. For construct validity, we made sure Section 3 fully outlined all the key terms and concepts associated with EC, IoT, Blockchain, 5G, and security. To make sure that our understanding corresponds to what is currently accepted in both academia and the industry, we used reputable sources [15].

For internal validity, we focused on drawing precise and dependable conclusions from the data we gathered. To do this, we conducted a thorough literature review using a systematic approach that is described in Section 2. To lessen any potential bias from the researcher, we selected specific search terms, established inclusion and exclusion criteria, and used quality assessment tools. This strategy ensures that our review is supported by a diverse and inclusive range of literature. We also acknowledged and discussed any potential factors and flaws in our methodology, recognizing their possible impact on our findings [15].

In terms of external validity, we considered the extent to which our findings could be generalized across various contexts. In Section 4, we examined how our results might be relevant to different IoT application domains, security challenges, and technological advancements. We openly acknowledged any limitations in the generalizability of our findings and proposed areas for future research to further investigate these limitations. Furthermore, to ensure our literature review represented the broader field, we conducted searches across multiple digital libraries (Scopus, Web of Science, IEEE Xplore, and ACM DL) and considered factors such as the publication years and geographical scope of the included articles [15].

3 Theoretical Background

This section builds upon Section 1.1, delving into the security paradigm of EC for IoT devices, alongside emerging mitigation strategies, common security threats, and effective security solutions.

3.1 Introduction to Edge Computing

Edge computing, as described by Shi and Dustdar [2], enables technologies to perform computation at the network edge, meaning that computation takes place close to the data source. For example, an edge device might be a smartphone that serves as a bridge between body sensors and the cloud. In EC, end devices fulfill dual roles: producing and consuming data. Moreover, these devices manage computing duties like processing, storing, caching, and load balancing for data transported to and from the cloud.

EC has emerged as a solution to the needs of IoT in contrast to traditional cloud computing, as described by Yu et al. [16]. By moving data processing closer to the end-user, its distributed design aids in balancing network traffic and reducing congestion in IoT networks. This results in faster communication between edge servers and end-users and quicker responses for real-time IoT applications compared to traditional cloud services.

It is important not to confuse EC with fog computing (FC). While both paradigms share similar goals and overlapping characteristics, the essential difference lies in the physical distance from the data source. EC takes place right on the devices attached to the sensors, or on a gateway device physically close to a sensor, whereas fog computing occurs further away [17]. FC focuses on a broader range of components, while EC mainly concentrates on the edge of the network, treating network edges as isolated computing platforms.

3.2 Introduction to Internet of Things

The IoT has emerged as a groundbreaking technology, transforming how we interact with the world around us [18]. The IoT refers to a network of physical objects interconnected through sensors, actuators, and communication interfaces [18]. These devices collect, exchange, and process data, enabling efficient communication and automation across a wide range of sectors, such as healthcare, agriculture, transportation, smart cities, and manufacturing [19].

The origins of IoT can be traced back to the late 20th century when the idea of connecting everyday objects to the Internet began to gain attention [20]. It was British technologist Kevin Ashton who, in 1999, first coined the term "Internet of Things" while working on radio-frequency identification (RFID) technology. Since then, IoT has evolved tremendously, fueled by advancements in wireless communication, miniaturization of electronic components, and widespread availability of the Internet [18, 19].

The IoT's growth can be attributed to the development of wireless communication protocols, such as Wi-Fi, Bluetooth, Zigbee, and LoRaWAN, which facilitate seamless data exchange between devices [19]. Furthermore, the increased availability of low-cost sensors and microcontrollers has accelerated the adoption of IoT, making it more accessible for various applications [21].

Within the context of EC, components like sensors, gateways, and actuators play vital roles in IoT systems. They work collaboratively to enable real-time data collection, processing, and control across various applications [22].

3.2.1 Sensors

In IoT systems, sensors are the main hardware components in charge of data collection [18]. They record data on various parameters, including pressure, temperature, humidity, and motion, subsequently transforming this data into electronic signals [18]. Simple temperature sensors, sophisticated cameras, and LiDAR systems are all examples of sensors. In EC IoT systems, sensors either process the data locally, reducing latency and bandwidth needs or send it to a nearby edge device for additional processing, enabling quicker decision-making and more effective use of network resources [22].

3.2.2 Gateways

Gateways serve as a bridge between edge devices like sensors and actuators and the cloud or other edge devices [21]. They gather, preprocess, and filter data from sensors before sending it for additional processing or storage [21]. Gateways also offer protocol translation services, enabling seamless data transfer between devices that use various communication standards [21]. In EC, gateways can also carry out data processing tasks, lightening the load on cloud infrastructure and enhancing system performance [22].

3.2.3 Actuators

Actuators execute physical actions based on decisions and data processing performed by the IoT system [18]. To regulate the environment or the operation of devices, they transform electronic signals back into mechanical or other forms of energy [18]. Actuators include things like motors, valves, and relays. In EC IoT systems, actuators receiving processed data from nearby edge devices or gateways facilitate real-time control and automation [22].

The foundation of IoT systems is formed by the interaction between sensors, gateways, and actuators, enabling smooth data transfer and command execution across the network. Maintaining the security of these systems and the data they process becomes more crucial as IoT grows and EC becomes more popular [22]. To safeguard the availability, integrity, and confidentiality of IoT systems, it is crucial to address the security issues relating to sensors, gateways, and actuators in EC environments [23].

3.3 Security in Edge Computing for IoT

EC has emerged as a revolutionary solution for processing the vast amounts of data generated by IoT devices [22]. By processing data closer to its source, EC reduces latency, saves bandwidth, and enhances the overall performance of IoT systems [22]. However, the distributed nature of EC, coupled with the diversity of IoT devices, brings about several security challenges that need to be addressed [23].

3.3.1 Threats

In EC for IoT, data security and privacy are major issues because it's crucial to safeguard sensitive information both during storage and transmission [23]. Due to their constrained capabilities and processing speed, maintaining the security of IoT devices can also be challenging. According to Fazeldehkordi and Grønli [9], these limitations increase the susceptibility of IoT devices to side-channel attacks, physical tampering, and malware injections [9]. Another crucial factor is network security because distributed and heterogeneous EC networks can be vulnerable to attacks like DDoS attacks, MITM attacks, and Routing Attacks [23]. It can be difficult to establish trust and enable authentication between IoT devices and edge nodes, particularly in dynamic, resource-constrained environments [9].

Distributed Denial of Service (DDoS) Attacks: The DDoS attack is one which involves overwhelming a target device, network, or service with a flood of traffic, rendering it inaccessible or inoperable. In EC for IoT devices, DDoS attacks can disrupt essential services or cause loss of critical data. Attackers may compromise a large number of IoT devices to create a botnet and launch coordinated DDoS attacks [9].

Denial of Service (DoS) Attacks: Similar to DDoS attacks, DoS attacks aim to overwhelm a single target, rendering it unable to function or respond. For IoT devices in EC, DoS attacks can cause service disruption, data loss, and compromised functionality. These attacks are often easier to execute than DDoS attacks, as they require fewer resources [9].

Man-In-The-Middle (MITM) Attack: The MITM attack involves an attacker intercepting and potentially altering communication between two parties without their knowledge. In EC for IoT devices, MITM attacks can lead to other risks such as data theft, unauthorized access, or injection of malicious payloads. Attackers may exploit weak encryption or poorly secured communication channels between IoT devices and edge servers [24].

Malicious/Code/Malware Injection: Attackers may inject malicious code or malware into IoT devices or EC infrastructure, compromising their integrity and potentially allowing unauthorized access or control. These attacks can lead to data theft, device malfunction, or unauthorized access to sensitive information [9].

Eavesdropping/Sniffing Attacks: In these attacks, an attacker intercepts and captures data transmitted between IoT devices and edge servers. They can result in data theft, loss of privacy, and unauthorized access to sensitive information. Weak encryption, poor authentication mechanisms, or insecure communication channels may make IoT devices in EC environments vulnerable to these attacks [9].

Replay or Freshness Attacks: In these attacks, an attacker captures and retransmits messages, often causing devices to process outdated or invalid commands. IoT devices in EC may be vulnerable to replay attacks due to inadequate encryption or poor implementation of message authentication mechanisms [9].

Physical Attacks/Tampering: Physical attack involves unauthorized access to, or tampering with, IoT devices or EC infrastructure. Attackers may modify hardware, steal data, or implant malicious components. These attacks pose a significant risk to EC security, as

IoT devices are often distributed in diverse and potentially unsecured environments [9].

Jamming Attacks: Jamming attacks involve the intentional disruption of wireless communication channels used by IoT devices in EC environments. Attackers may flood channels with noise or interfering signals, rendering devices unable to communicate with each other or edge servers. This can lead to service disruption, data loss, or isolation of affected devices [9].

Spoofing Attacks: These involve an attacker masquerading as a legitimate entity by falsifying data, such as IP addresses, MAC addresses, or device identities. In EC for IoT devices, spoofing attacks can lead to unauthorized access, data theft, or disruption of services. Attackers may exploit weak authentication mechanisms or poorly secured communication channels to carry out spoofing attacks [9].

Node Replication Attacks: In node replication attacks, adversaries create multiple copies of a legitimate node, also known as clones, and distribute them throughout the network. These replicated nodes can undermine the trust and security of the network by participating in communication, manipulating data, or launching other attacks. In EC and IoT environments, node replication attacks can compromise the integrity of data aggregation, cause the network to accept false information, or deplete resources by causing unnecessary traffic [9].

Side-Channel Attacks: These exploit information unintentionally leaked through various channels, including power consumption, electromagnetic radiation, or timing information. In EC for IoT devices, these attacks can lead to data theft or unauthorized access. Side-channel attacks may target the device's hardware, software, or communication channels [9].

3.3.2 Mitigation for Threats

This section explains the theoretical basis of mitigation strategies, their essential concepts and approaches, and their significance in controlling potential threats and repercussions across multiple domains are explored in the following section. Understanding the practical applications and ramifications of these tactics in realistic circumstances requires a solid foundation. Henceforth, a list of common mitigation strategies follows, to give the reader a practical understanding of said mitigation strategy. It should be noted that while there is a vast array of mitigation strategies, this list has been limited to the most commonly used and popular ones.

Intrusion Detection Systems (IDS): Serving as a digital watchdog, Intrusion Detection Systems (IDS) continuously monitor network operations and communication links to identify and report any suspicious activity indicative of potential security threats. By analyzing traffic patterns and user behavior, IDS can detect anomalies or signs of intrusion, such as unauthorized access, malware, or other cyberattacks. In EC and IoT environments, an effective IDS plays a crucial role in maintaining the security and integrity of the system by providing real-time alerts and facilitating rapid incident response [9].

Firewalls: Firewalls act as a barrier between trusted internal networks and untrusted external networks, such as the Internet, by monitoring and controlling incoming and outgoing network traffic. They enforce security policies by filtering and blocking potentially harmful data packets based on predefined rules. In EC and IoT environments, firewalls help protect devices and infrastructure from unauthorized access and cyberattacks [9].

Cryptography: Cryptography is the science of securing communication and data by using mathematical techniques to encrypt and decrypt information. It ensures confidentiality, integrity, and authentication in EC and IoT systems by protecting sensitive data from unauthorized access and tampering [9].

Packet Filters: Packet filters are a type of firewall that inspect and filter network traffic based on predefined rules, such as IP addresses, protocol types, or port numbers. They help protect EC and IoT environments by blocking malicious or unauthorized data packets from entering or leaving the network [9].

Packet Flow Analysis: Packet flow analysis is the process of examining and analyzing network traffic to detect anomalies, identify potential security threats, and monitor network performance. In EC and IoT environments, packet flow analysis helps maintain network security and integrity by providing insights into traffic patterns, detecting intrusions, and facilitating incident response [24].

Steganography: Steganography is the practice of hiding information within other data, such as images, audio files, or text documents. It can be used for both legitimate and malicious purposes in EC and IoT systems, such as secure communication or covert data exfiltration. Understanding steganography techniques can help in detecting hidden information and mitigating potential security risks [24].

Authentication Protocols: Authentication protocols are mechanisms used to verify the identity of users, devices, or systems in a network. They play a crucial role in maintaining the security of EC and IoT environments by ensuring that only authorized entities can access resources or perform actions on the network [9].

Pre-testing: Pre-testing refers to the process of evaluating and validating the security, functionality, and performance of EC and IoT devices or systems before deployment. By identifying and addressing potential vulnerabilities and weaknesses, pre-testing helps improve the overall security and reliability of the system [9].

Circuit Modification/Replacement: Circuit modification or replacement involves altering or replacing the electronic components of an IoT device or EC system to enhance its security or functionality. This can include adding hardware security features, implementing fault-tolerant designs, or upgrading outdated components. By making these changes, circuit modification or replacement can help improve the resilience and security of EC and IoT systems against various attacks, such as side-channel attacks, tampering, or hardware failures [9].

Firmware Security: This approach focuses on ensuring the integrity, authenticity, and confidentiality of the firmware – the software that controls the operation of IoT devices and EC systems. Secure firmware development and deployment practices, such as secure boot, firmware signing, and regular updates, can help protect these systems from malware, unauthorized access, and other security threats [9].

3.4 5G and Blockchain for IoT Edge Computing Security

This subsection aims to provide a balanced overview of how 5G and blockchain technologies contribute to enhancing security in IoT EC, discussing their advantages. We start by exploring the background of 5G, followed by its advantages in EC security for IoT [25]. We then discuss blockchain technology and its advantages for IoT EC security [25].

3.4.1 Blockchain

Blockchain is a distributed ledger technology (DLT) that enables secure and transparent data storage and sharing across multiple nodes. It utilizes cryptographic techniques to create a tamper-proof record of transactions, which is maintained by consensus among participating nodes [26]. Blockchain's decentralized nature, coupled with its inherent security features, makes it an attractive option for enhancing security in IoT EC [25]. Blockchain technology can be used to improve security in IoT EC in several ways:

Data Integrity and Authentication: Blockchain can be employed to securely store data generated by IoT devices, ensuring its integrity and providing a traceable record of its origin, enhancing the authenticity and provenance of the data [27].

Decentralized Trust: Blockchain's decentralized architecture eliminates the need for a central authority to validate transactions and manage trust, reducing the risk of single points of failure and increasing the resilience of the system against malicious attacks [28, 29].

Access Control and Privacy: Blockchain can be used to implement decentralized access control mechanisms for IoT devices, allowing for secure and fine-grained control over who can access and interact with the devices and their data [30].

3.4.2 5G

5G, or the fifth generation of mobile networks, is a technology that offers significant improvements over its predecessors in terms of speed, latency, capacity, and energy efficiency [31]. It is designed to support a wide range of applications and use cases, including the rapidly growing IoT ecosystem [32]. 5G's ultra-reliable low-latency communication (URLLC) feature and increased network slicing capabilities enable it to meet the stringent requirements of IoT devices and applications, allowing for more efficient and secure communication between devices and EC nodes [31]. 5G enhances EC security in IoT through several key features [25]:

Network Bandwidth: The increased network bandwidth in 5G technology enables the connection of a large number of IoT devices simultaneously, supporting the seamless communication, high-speed data transfer, and growth of various IoT applications across industries [33].

Low Latency: 5G networks provide ultra-low latency, which is crucial for real-time IoT applications that require immediate response and decision-making. Examples include autonomous vehicles, remote surgery, and industrial automation. Low latency ensures faster communication between devices and systems, improving the overall performance and reliability of IoT applications [34, 35].

Security and Privacy: IoT devices and their data are protected by sophisticated security mechanisms included in 5G protocols, such as end-to-end encryption, secure device authentication, and regular security upgrades. Additionally, the adoption of more robust privacy-preserving approaches, including federated learning and differential privacy, which help safeguard sensitive user data while enabling IoT devices to learn and develop their functionality, is supported by 5G technology [34].

In conclusion, 5G and blockchain technologies have the potential to enhance security in IoT EC [25]. By leveraging the unique features of these technologies and carefully considering their limitations, it is possible to create a more secure and resilient IoT ecosystem that can better address the challenges posed by the increasing scale and complexity of connected devices and applications [25, 32, 36]. However, it is essential to continuously evaluate and adapt these technologies to mitigate potential drawbacks and risks as they evolve, such as the challenges associated with integrating these technologies, ensuring their scalability, navigating potential regulatory issues, and establishing robust security protocols to prevent breaches.

4 Results

This section presents the results of the SLR in a sequential manner for each of the three research questions: RQ1, RQ2, and RQ3. For each research question, the following five steps are conducted and discussed: 1) Search strategy, 2) Inclusion and exclusion criteria, 3) Quality assessment, 4) Data extraction, and 5) Information synthesis.

The findings for each research question are shared and explored individually, with a distinct separation between the steps involved and their respective research question. This method allows us to present the results in a thorough and well-organized manner while keeping a clear emphasis on the unique goals of each research question.

4.1 Research Question 1: Review process findings

Figure 4.2 illustrates the distribution of articles obtained from various digital libraries using the search string for RQ1. A total of 255 articles were identified, with 44 sourced from Scopus, 23 from IEEE Xplore, 169 from ACM Digital Library, and 19 from Web of Science.

The significant difference in the number of articles found in each digital library can be attributed to several factors. The ACM Digital Library has a larger number of articles due to its extensive focus on computing and information technology, which are highly relevant to our research question. Additionally, ACM's broader coverage of conferences and workshops, as well as its more frequent updates, may contribute to the higher article count.

In contrast, Scopus has fewer articles because we only used the Title-Abstract-Keyword (TITLE-ABS-KEY) search field in this library. Scopus is a vast multidisciplinary database, and limiting the search to TITLE-ABS-KEY helped us focus on the most relevant articles without being overwhelmed by a large number of search results. The reduced article counts from IEEE Xplore and Web of Science may be due to their diverse range of disciplines or different indexing criteria, leading to a smaller number of articles directly related to our research question.

It is important to note that the quantity of articles retrieved from each digital library does not necessarily indicate the quality or relevance of the articles. As we proceed with the analysis, we apply inclusion and exclusion criteria and quality assessment to ensure that only the most relevant and high-quality articles are considered in our study.

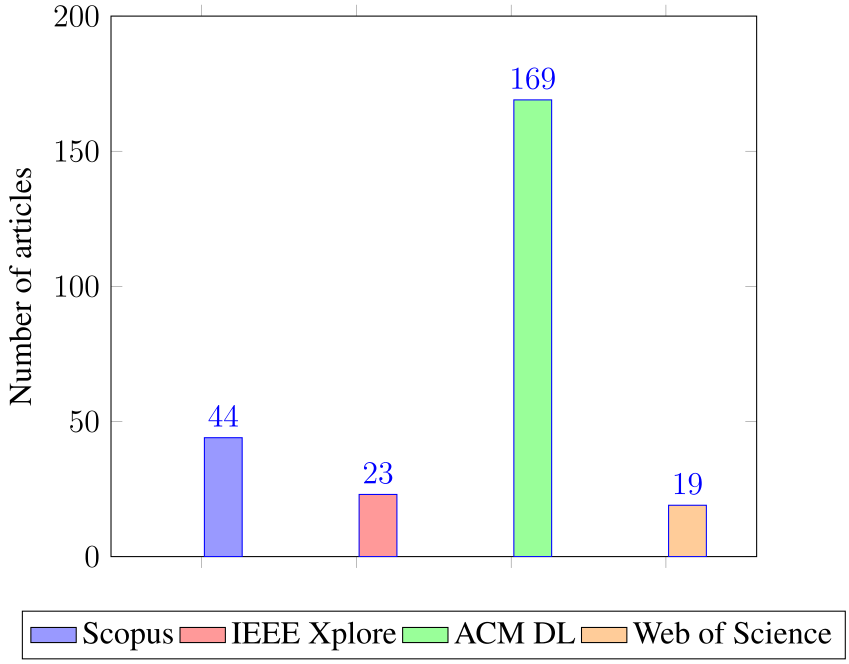


Figure 4.2: Bar chart of research sources for RQ1.

Figure 4.3 presents the results of implementing the search strategy and applying inclusion and exclusion criteria with the help of the Zotero software [13]. Initially, 255 articles were identified across the digital libraries (as shown in Figure 4.3). After excluding non-English articles, the total was reduced to 253 articles, with a loss of 2 articles. We imported these articles into Zotero, which helped identify and filter out articles not accessible through the Linnaeus University proxy. This removed another 67 articles, leaving 186 full-text articles. Zotero was then used to identify and remove duplicate articles, resulting in the removal of 28 articles and leaving 158 articles.

Then, we manually evaluated each article in Zotero for inclusion criteria IC1 and IC2, removing 126 articles and leaving 32 articles. After that, we performed a quality assessment and eliminated an additional 8 articles. This left us with 24 articles to use in the results.

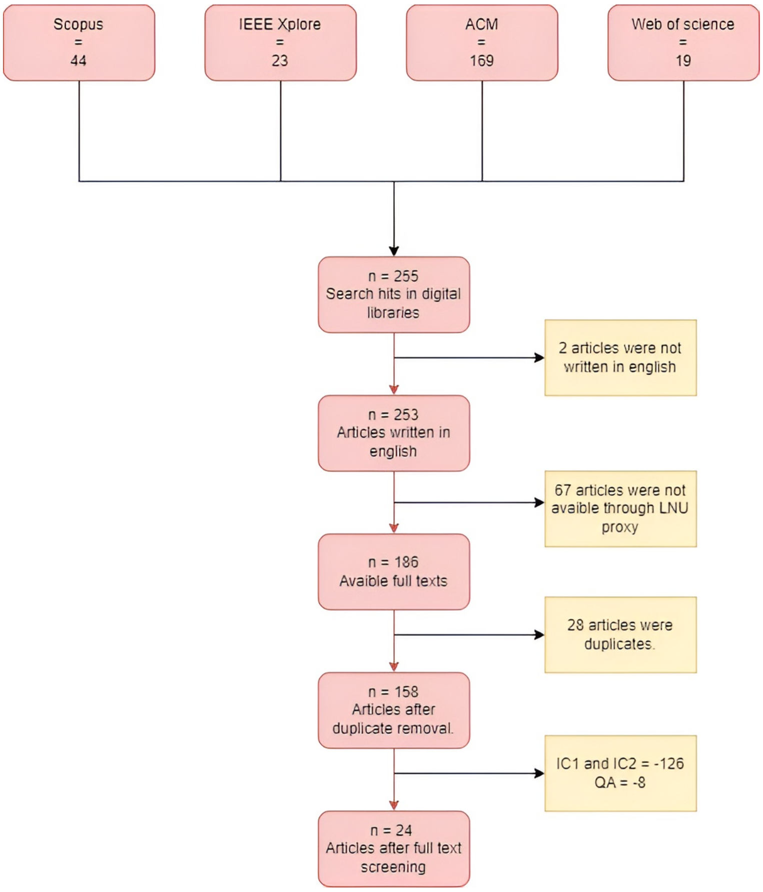

Scopus = 44
IEEE Xplore = 23
ACM = 169
Web of science = 19
n = 255 Search hits in digital libraries
2 articles were not written in english
n = 253 Articles written in english
67 articles were not avaible through LNU proxy
n = 186 Avaible full texts
28 articles were duplicates.
n = 158 Articles after duplicate removal.
IC1 and IC2 = -126 QA = -8
n = 24 Articles after full text screening

Figure 4.3: Results of the review process for RQ1

4.1.1 Most common security threats

To organize the articles and identify the most common security threats for the first part of the first research question, a reference mapping has been done for DEI7 as can be seen in Table 4.7. Here the reference mapping has taken all the security threats that have been given by each article, some having many while others having only a few. Then when all articles have been gone through, we can now see which security threats are the most common thanks to the reference mapping. There is a total of about 40 different security threats taken out of the 24 articles and the most common security threats are those with the most references by articles in ranking order. Those with four or more references on their mappings are included as one of the most common security threats and are explained thoroughly, and the rest of the security threats are shortly mentioned. Fazeldehkordi and Grønli [9] are one of the only articles that mention major security threats and those were DDoS, malware injection, and side-channel attacks, which we also had as our most common security threats.

If we rank it by order of threats who have the most references, Figure 4.4 shows the most common security threats in EC security for IoT devices. Here we can see that DDoS, DoS, and MITM attacks are the most prevalent, but also other attacks such as malware injection. This pie chart only shows the most common security threats, so only the security threats that had four references or more in the 24 primary articles. The reference mapping for the security threats can be seen in Table 4.7.

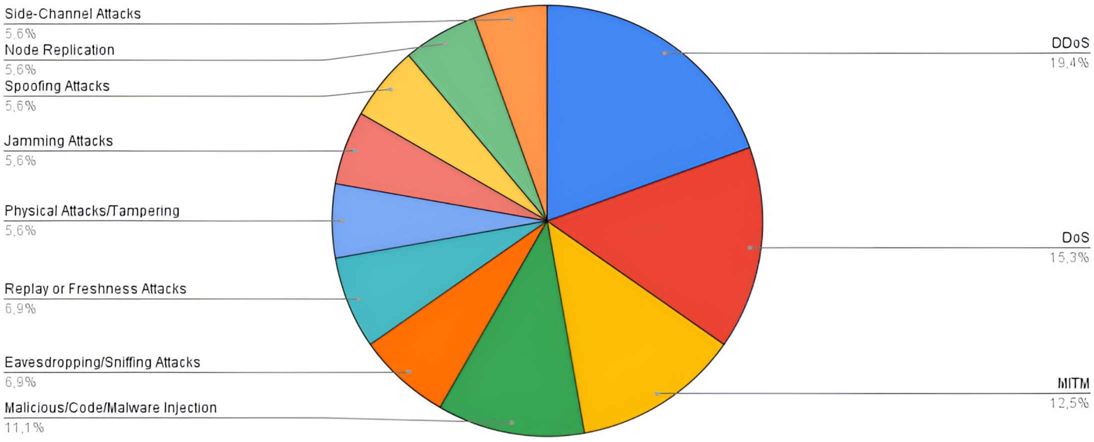


Figure 4.4: Pie chart showing the most common threats.

Table 4.7: DEI7 Reference Mapping.

Article ID (Reference)	Security Threats (DEI7)
[37] [38] [9] [39] [24] [40] [41] [42] [43] [44] [45] [46] [47] [48]	Distributed Denial of Service (DDoS) Attacks
[24] [49] [50] [51] [40] [52] [53] [42] [43] [54] [46] [47]	Denial of Service (DoS) Attacks
[24] [50] [51] [40] [42] [44] [54] [46] [47]	Man-In-The-Middle (MITM) Attack
[55] [9] [39] [24] [52] [45] [46] [47]	Malicious/Code/Malware Injection
[9] [39] [24] [54] [47]	Eavesdropping/Sniffing Attacks
[9] [39] [24] [51] [54]	Replay or Freshness Attacks
[9] [39] [54] [47]	Physical Attacks/Tampering
[9] [39] [24] [47]	Jamming Attacks
[24] [44] [54] [46]	Spoofing Attacks
[9] [39] [24] [47]	Node Replication
[55] [9] [45] [47]	Side-Channel Attacks
[55] [9] [39]	Integrity Attacks Against Machine Learning
[55] [9] [39]	Insufficient/Inessential Logging
[24] [54] [47]	Sybil Attack
[9] [39] [54]	Forgery Attacks
[9] [39] [47]	Unauthorized Control Access
[9] [40] [56]	Malware
[9] [56] [42]	Botnets
[55] [9]	Non-Standard Frameworks and Inadequate Testing
[9] [39]	Hardware Trojan
[9] [39]	Camouflage
[9] [39]	Corrupted or Malicious Edge Computing Nodes
[9] [45]	Authentication and Authorization Attacks
[9] [39]	Routing Information Attacks
[9] [40]	Ransomware
[9] [39]	Privacy Leakage
[24] [54]	Traffic Analysis
[24] [47]	Tag Cloning Attack
[54] [46]	Hijacking
[39]	Non-Network Side-Channel Attacks
[39]	Other Attacks (Different Framework Attacks)
[9]	Injecting Fraudulent Packets
[24]	Data Manipulation
[24]	Blackhole Attack
[24]	Sinkhole Attack
[50]	Rogue Gateway
[57]	AI Model Training Attacks
[57]	AI Model Interference Attacks
[57]	Attacks on Private Data
[58]	TCP SYN Scanning
[46]	DMA Assaults/Cold Boots Attacks
[47]	Node Capture Attack

4.1.2 Security threats and their mitigation discussion

Since there are numerous effective mitigation strategies for each threat, each of the security threats is displayed in a table (DEI8) along with any effective mitigation techniques that have been discovered.

Table 4.8: DEI8 Effective Mitigation Strategies - DDoS.

Security Threat	Effective Mitigation Strategies
DDoS Attacks	Packet filters, Firewalls, IDS, Cryptography [39, 9, 24] Packet flow analysis, Cryptanalysis [24] Large-scale security framework [37] SD-IoMT-Protector [41] π-Edge platform with NFV MANO IM [48] EDMOpti and EDMGame [38] KingFisher IDS (ML-based) [40], DTARS security system [42] DTARS in edge computing [43] SeArch IDS using SDN [44] Detect-and-filter, ML tools [45] SDN-NFV hardware technique [46] Mirai IoT Malware prevention [47]

Distributed Denial of Service (DDoS) Attacks was the security threat with the most articles referenced, as many articles primarily focused on specific countermeasures for DDoS attacks such as frameworks. For example, Zhou et al. [37] discussed DDoS attacks in different layers of the IoT architecture and proposed a security framework to countermeasure large-scale DDoS attacks [37].

Several other articles, like Sahoo and Puthal [41], also focused on DDoS attacks as their main security threat. They proposed an SDN-assisted two-phase detection framework called SD-IoMT-Protector to mitigate DDoS attacks.

Valantasis et al. [48] presented another DDoS-focused article. They demonstrated the effectiveness of their π-Edge platform through a DDoS attack scenario use case. The platform, designed for managing resources and services in distributed computing architectures, includes security analytics mechanisms based on a declarative NFV MANO Information Model (IM) to enhance Network Slices at the edge automatically.

He et al. [38] also explored DDoS attacks, proposing two edge DDoS mitigation (EDM) approaches, EDMOpti and EDMGame, as potential solutions to the problem formulated as a constraint optimization problem.

The articles by Alwarafy et al. [39] and Fazeldehkordi and Grønli [9] discussed various mitigation strategies for DDoS attacks, including packet filters, firewalls, securing firmware updates, IDS, and cryptographic schemes. Both articles, as well as Swamy and Kota [24], covered a wide range of security threats, with DDoS being just one of them.

Swamy and Kota [24] proposed mitigation techniques like analyzing packet flow information in the network and employing cryptanalysis and steganography techniques to prevent jamming messages in their DDoS-focused article.

Bernieri et al. [40] introduced KingFisher, a machine learning (ML)-based IDS framework, as a means of mitigating DDoS attacks.

Krishnan et al. [42] suggested the DTARS security system to protect IoT and 5G networks from DDoS and botnet attacks, boasting over 95% accuracy in real-time detection without disrupting normal network traffic. In another article, Krishnan et al. [43] introduced the DTARS framework for EC scenarios, using a cooperative security approach to combat complex DDoS attacks.

Nguyen et al. [44] presented SeArch, a collaborative and intelligent network-based IDS for cloud IoT networks that use SDN. SeArch's hierarchical IDS nodes quickly detect anomalies and mitigate threats, outperforming existing solutions.

Ansari et al. [45] discussed various attacks and challenges in EC security IoT, including DDoS attacks. They suggested using detect-and-filter techniques and ML tools to counter flooding attacks but acknowledged that zero-day attacks remain more challenging due to source code and firmware constraints.

Kolimbianakis and Kornaros [46] proposed a software-defined protection-oriented hardware technique to mitigate cybersecurity threats, including DDoS attacks, in IoT domains using SDN-NFV technologies. The approach supports physical isolation of memory compartments and hardware devices in modern Systems-on-Chip, enhancing IoT ecosystem security through innovative lightweight software-controlled hardware mechanisms.

Krishna et al. [47] presented a taxonomy of IoT threats, including DDoS attacks in the context of EC. The proposed mitigation here is a reference to a website discussing the Mirai IoT Malware, which can help prevent DDoS attacks.

Table 4.9: DEI8 Effective Mitigation Strategies - DoS.

Security Threat	Effective Mitigation Strategies
DoS Attacks	Packet flow analysis, cryptanalysis, steganography [24] Edge server deployment [50] General security frameworks [51] KingFisher Framework (ML-based IDS) [40] Tier-based reconfigurable security architecture [52] Resilient authentication, secure migration to edge computers [53] DTARS framework (cooperative security approach) [42, 43] Physical-Layer Security (PLS) (general mitigation) [54] Software-defined protection-oriented hardware technique [46]

Denial of Service (DoS) Attacks were the second-largest security threat, and in this article, several articles discussing DoS attacks in the context of IoT security are analyzed with a focus on the suggested mitigation techniques for these threats. Due to their similarities, some articles group DoS and DDoS attacks together and categorize them as such, which is important to note.

Swamy and Kota [24] is one such article that treats DoS and DDoS attacks together, suggesting that "analyzing the packet flow information in the network, cryptanalysis and steganography techniques can help prevent jamming messages" helps both DoS and DDoS attacks.

On the other hand, some articles specifically address DoS attacks. Shabaan et al. [49] discuss DoS attacks in the context of their CloudWoT reference model, but they do not mention any mitigation techniques. Zhang et al. [50] also explore DoS attacks, proposing the employment of servers at the edge as a mitigation strategy.

Several articles mention DoS attacks alongside other IoT security issues. Tawalbeh et al. [51] propose general security frameworks as a mitigation method, while Bernieri et al. [40] introduce the KingFisher Framework, an ML-based IDS framework. Charles and Mishra [52] recommend a tier-based reconfigurable security architecture for IoT systems that support encryption, authentication, and DoS attack detection with dynamic reconfiguration.

Kim et al. [53] discuss DoS attacks and propose a resilient authentication and authorization framework for IoT, utilizing secure migration to trusted edge computers to improve availability under DoS attacks or failures. Meanwhile, Krishnan et al. [42, 43] introduce the DTARS framework for IoT and 5G networks and EC scenarios. This cooperative security approach uses behavioral, flow monitoring, and traffic analysis algorithms to detect and respond to DDoS/DoS attacks in real time with more than 95% accuracy.

Michailidis et al. [54] explore the potential of using Unmanned Aerial Vehicles (UAVs) to enhance Mobile Edge Computing (MEC) in IoT networks, mentioning DoS attacks as a security threat. Although they do not specify a particular mitigation strategy for DoS attacks, they suggest general mitigation methods such as Physical-Layer Security (PLS) for secure information-theoretic transmissions.

Kolimbianakis and Kornaros [46] propose a software-defined protection-oriented hardware technique for mitigating cybersecurity threats, including DoS attacks, by supporting physical isolation of memory compartments and hardware devices in SoCs with innovative software-controlled hardware mechanisms.

Lastly, Krishna et al. [47] provide a taxonomy of IoT threats, including DoS attacks. They reference another article on DoS in sensor networks but do not specify any particular mitigation strategy.

Table 4.10: DEI8 Effective Mitigation Strategies - MITM.

Security Threat	Effective Mitigation Strategies
MITM Attack	Cryptographic algorithms & mutual authentication protocols [24] Dynamic credentials & PGP with PKI [50] General security frameworks [51] KingFisher Framework (ML-based IDS) [40] DTARS framework for SDN [42] SeArch (SDN-based IDS) [44] Physical-Layer Security (PLS) [54] Software-defined hardware isolation [46]

Man-in-the-middle (MITM) Attack were the third most common security threat. The articles that were discovered for the reference mapping on this security threat are examined here, along with any recommended mitigation techniques for an MITM attack.

Swamy and Kota [24] focus on EC-related attacks such as MITM in their IoT threats taxonomy article. They suggest using cryptographic algorithms and strong mutual authentication protocols to protect communication channels.

Zhang et al. [50] discuss various threats, including MITM attacks, proposing the use of dynamic credential generation based on mobile-cloud packet exchange and nonce participation. They also recommend the use of Pretty Good Privacy (PGP) based on Public Key Infrastructure (PKI) for secure mobile cloud computing.

Tawalbeh et al. [51] explore IoT privacy and security challenges, mentioning MITM attacks and proposing general security frameworks as a mitigation method.

Bernieri et al. [40] discuss the KingFisher framework, which addresses MITM attacks. They propose using the KingFisher Framework, an ML-based IDS.

Krishnan et al. [42] present the DTARS framework, noting that the SDN architecture paradigm is vulnerable to MITM or DoS attacks due to its control plane design. The framework aims to address these vulnerabilities.

Nguyen et al. [44] mention MITM attacks as one of the security threats and introduce SeArch, a collaborative and intelligent network-based IDS for cloud IoT networks using SDN. SeArch's hierarchical IDS nodes quickly detect anomalies and mitigate threats, outperforming existing solutions.

Michailidis et al. [54] investigate the use of Unmanned Aerial Vehicles (UAVs) to enhance Mobile Edge Computing (MEC) in IoT networks, identifying MITM attacks as a security threat. They suggest general mitigation methods, such as implementing Physical-Layer Security (PLS), which can prevent attackers from intercepting and manipulating data transmitted over the network, making MITM attacks more difficult.

Kolimbianakis and Kornaros [46] propose a software-defined protection-oriented hardware technique for mitigating cybersecurity threats, including MITM attacks. This technique supports the physical isolation of memory compartments and hardware devices in

SoCs with innovative software-controlled hardware mechanisms.

Krishna et al. [47] provide a taxonomy of IoT threats, including MITM attacks. They reference another article that discusses security threats in EDCs and CDCs by dividing the network structure into three layers: perception layer, network layer, and application layer but they do not specify any effective mitigation strategy.

Table 4.11: DEI8 Effective Mitigation Strategies - Injection.

Security Threat	Effective Mitigation Strategies
Malicious/Code/Malware Injection	Pre-testing [55], [9] Side-channel analysis, Trojan activation, circuit modification [39] Cryptographic algorithms, mutual authentication [24] Reconfigurable security architecture [52] Detect-and-filter with static analysis [45]

Malicious/Code/Malware Injection: was fourth in the list of common security threats, and here we analyze the references that either just mentioned the injections as a security threat or also had a mitigation strategy for them.

Mosenia and Jha [55] address IoT security concerns, specifically focusing on EC and mentioning malicious injection. They propose pre-testing as a mitigation strategy.

Fazeldehkordi and Grønli [9] discuss various security threats in EC security for IoT, including malicious and malware injections. They identify malware injection as one of the major security threats and also suggest pre-testing as a mitigation method.

Alwarafy et al. [39] mention malicious and malware injections as well, going further into countermeasures against malicious injection. They discuss three approaches: side-channel signal analysis, Trojan activation methods, and circuit modification or replacement.

Swamy and Kota [24] present a taxonomy of IoT threats, with a focus on EC-related attacks such as code injection. They recommend using cryptographic algorithms and strong mutual authentication protocols to protect communication channels.

Charles and Mishra [52] propose a tier-based reconfigurable security architecture for IoT systems that support encryption, authentication, and detection of denial-of-service (DoS) attacks with dynamic reconfiguration. This architecture helps with malware injection by incorporating encryption and dynamic reconfiguration for enhanced security.

Ansari et al. [45], who previously discussed DDoS and other security threats, suggest the same mitigation for malware injection attacks: a detect-and-filter technique. They mention that static analysis is typically used by defense mechanisms against injection attacks to identify malicious code and implement specific access control.

Kolimbianakis and Kornaros [46] address various IoT EC threats, including software attacks injecting invalid memory pointers, but do not specify any further details or mitigation strategies.

Krishna et al. [47] provide a taxonomy of IoT threats, including malicious data injection. They reference an article called "Statistical en-route filtering of injected false data in sensor networks," which does not specify any effective mitigation strategy for malicious injection.

Table 4.12: DEI8 Effective Mitigation Strategies - Eavesdropping/Sniffing.

Security Threat	Effective Mitigation Strategies
Eavesdropping/Sniffing Attacks	Cryptographic schemes [9], [39] Cryptographic algorithms & mutual authentication [24] Physical-Layer Security (PLS) [54]

Eavesdropping/Sniffing Attacks were identified as the fifth most common security threat. In this context, eavesdropping and sniffing attacks are considered synonymous, as most articles treat them as such. Five articles discuss this security threat, which we examine below.

Fazeldehkordi and Grønli [9] discuss eavesdropping/sniffing attacks, proposing cryptographic schemes as a mitigation strategy. Cryptographic schemes are methods and protocols used to secure communication and protect sensitive data from unauthorized access or manipulation by converting the original message or data into an unreadable form.

Alwarafy et al. [39], similar to [9], also recommend cryptographic schemes as a mitigation measure for eavesdropping/sniffing attacks.

Swamy and Kota [24] address eavesdropping attacks, suggesting that protecting communication channels using cryptographic algorithms and strong mutual authentication protocols can mitigate the threat.

Michailidis et al. [54] mention various security threats, including eavesdropping, but do not provide a specific mitigation strategy. Instead, they recommend the implementation of Physical-Layer Security (PLS) for secure information-theoretic transmissions as a general measure.

Krishna et al. [47] briefly discuss eavesdropping but do not offer a specific mitigation strategy. The article provides information about eavesdropping in sensor networks without suggesting any countermeasures.

Table 4.13: DEI8 Effective Mitigation Strategies - Replay/Freshness.

Security Threat	Effective Mitigation Strategies
Replay or Freshness Attacks	IDS and Cryptographic schemes [9] [39] Strong digital signatures & Cryptographic algorithms [24] Authentication & General security frameworks [51]

Replay or Freshness Attacks are the sixth most common security threats, with five articles reference-mapped to this category. Let's examine each article to see if they mention these attacks and propose any mitigation techniques.

Fazeldehkordi and Grønli [9] discuss Replay or Freshness Attacks and suggest the use of IDS and Cryptographic schemes as effective mitigation techniques. Alwarafy et al. [39] also mention Replay or Freshness Attacks but do not explicitly associate specific countermeasures with this attack type. However, their article extensively covers IDS and Cryptographic schemes.

Swamy and Kota [24] address replay or freshness attacks as well, proposing the use of strong digital signature techniques and cryptographic algorithms to secure the network.

Tawalbeh et al. [51] mention replay or freshness attacks, noting that authentication is used for mitigating Denial-of-Service (DoS) and replay attacks. They also discuss general security frameworks as potential mitigation approaches.

Michailidis et al. [54] mention replay attacks but do not provide specific mitigation strategies for this type of attack. Their article focuses on general strategies that are not directly applicable to replay or freshness attacks.

Table 4.14: DEI8 Effective Mitigation Strategies - Physical/Tampering.

Security Threat	Effective Mitigation Strategies
Physical/Tampering Attacks	Circuit modification or replacement [9] [39]

Physical/Tampering Attacks rank as the seventh most common security threat. In this section, we discuss the references that address these attacks and their proposed mitigation strategies.

Fazeldehkordi and Grønli [9] discuss physical/tampering attacks among other threats. They propose circuit modification or replacement as the best mitigation strategy, which includes physical tamper-prevention, minimizing information leakage, and embedding Physically Unclonable Functions (PUFs) for device authentication and Trojan detection. Alwarafy et al. [39], sharing similarities with [9], also suggest circuit modification or replacement as the optimal mitigation for physical/tampering attacks.

Michailidis et al. [54] mention physical/tampering attacks but do not provide a specific mitigation strategy. Furthermore, none of their general mitigation techniques seem particularly beneficial for addressing physical/tampering attacks.

Krishna et al. [47] identify physical/tampering attacks as a security threat, but do not offer any effective mitigation strategies for these attacks.

Table 4.15: DEI8 Effective Mitigation Strategies - Jamming.

Security Threat	Effective Mitigation Strategies
Jamming Attacks	Firewalls, firmware security, IDS, and cryptography [9] Firmware security, IDS, and cryptography [39] Packet flow analysis, cryptanalysis, and steganography [24] JAM: jammed-area mapping service for sensor networks [47]

Jamming Attacks is number eight in the list of common security threats, here we still have 4 articles that have come through the inclusion criteria and were reference mapped, let's analyze these ones by one and see if they are any good mitigation techniques for jamming attacks.

Fazeldehkordi and Grønli [9] of course have mentioned this security threat also and the best mitigation for jamming attacks according to them are actually four mitigation techniques; Firewalls, Securing firmware update, IDS and Cryptographic schemes. Alwarafy et al. [39] on the other hand does mention jamming attacks but does not specify the specific mitigation solution that matches jamming attacks and therefore we can't specify something, but we know they still mention securing firmware update, IDS, and cryptographic schemes but not firewalls, that's all we know.

Swamy and Kota [24] also mention jamming attacks, and here the proposed solution is analyzing the packet flow information in the network, cryptanalysis, and steganography techniques to prevent jamming attacks.

Krishna et al. [47] as usual mentions every attack including jamming attacks, but this time one proposed solution is JAM: a jammed-area mapping service for sensor networks. It is a proposed coping strategy of detecting and mapping jammed regions as a mitigation technique for jamming attacks. By mapping out the jammed regions, network applications can reason about the region as an entity and take necessary action to avoid those areas.

Table 4.16: DEI8 Effective Mitigation Strategies - Spoofing.

Security Threat	Effective Mitigation Strategies
Spoofing Attacks	Cryptographic algorithms & mutual authentication [24] SeArch (SDN-based IDS)s [44]

Spoofing Attacks is the ninth most common security threat, with four articles that have been reference mapped. The following analysis determines if they mention spoofing attacks and offer any effective mitigation techniques.

Swamy and Kota [24] categorize spoofing attacks alongside eavesdropping and MITM attacks. They recommend protecting communication channels using cryptographic algorithms and strong mutual authentication protocols as a mitigation technique.

Nguyen et al. [44] discuss spoofing attacks and propose the SeArch architecture, which uses lightweight, moderate, and compute-intensive ML algorithms for detecting network-related threats, including spoofing attacks.

Michailidis et al. [54] mention spoofing attacks, but their article only offers general mitigation strategies for non-specific attacks, which may not directly benefit spoofing attack defense.

Kolimbianakis and Kornaros [46] briefly touch on IP spoofing but do not provide any mitigation techniques for spoofing attacks.
Node Replication ranks as the tenth most common security threat, with four articles included in the reference mapping. The following analysis determines if these articles only mention node replication or if they also propose effective mitigation techniques.

Table 4.17: DEI8 Effective Mitigation Strategies - Node Replication.

Security Threat	Effective Mitigation Strategies
Node Replication	Implementing node revocation protocols [9] Node-revocation protocols [39] Lightweight algorithm with Clone Node Detection technique based on Cuckoo filtering, location information, watchdog nodes, and decentralized protocol based on random numbers (Nonce) [24] Sequential Probability Ratio Test [47]

Fazeldehkordi and Grønli. [9] discuss node replication and initially state that they do not have any solution for this issue. However, they briefly mention that implementing node revocation protocols can enable legitimate EC nodes to be revoked by node replicas.

Alwarafy et al. [39] also address node replication and similarly suggest that node replicas can revoke legitimate EC nodes by implementing node-revocation protocols.

Swamy and Kota [24] mention node replication as the first attack in their security threats. Their mitigation recommendations include using a lightweight algorithm with a Clone Node Detection technique based on Cuckoo filtering, employing location information and watchdog nodes to identify replicated nodes, and utilizing a decentralized protocol based on random numbers (Nonce) for detecting replicated nodes when two nodes meet and exchange information.

Krishna et al. [47] discuss node replication and refer to an article that recommends mitigating this type of attack in mobile sensor networks by using the Sequential Probability Ratio Test.

Table 4.18: DEI8 Effective Mitigation Strategies - Side-Channel.

Security Threat	Effective Mitigation Strategies
Side-Channel Attacks	Circuit modification or replacement [55] [9] Kill/sleep command [55] Isolation [55] Blocking [55] Differential privacy and k-anonymity data perturbation [45]

Side-Channel Attacks, ranking as the eleventh most common security threat, have been reference mapped in four articles. The following analysis explores whether these articles discuss side-channel attacks and offer any effective mitigation techniques.

Mosenia and Jha [55] address side-channel attacks and propose several mitigation techniques, including circuit/design modification, kill/sleep command, isolation, and blocking.

Fazeldehkordi and Grønli [9] discuss side-channel attacks among other threats, and their preferred mitigation approach is circuit modification or replacement.

Ansari et al. [45] also discuss side-channel attacks and suggest using differential privacy and k-anonymity data perturbation to mitigate side-channel attacks. Further study is required because these methods are also susceptible to such attacks.

Krishna et al. [47] also examine various threats, including side-channel attacks. However, for mitigation, they only reference an article on the introduction to side-channel attacks, which does not explicitly mention any specific mitigation techniques. Instead, the article emphasizes the importance of properly evaluating countermeasures to ensure security while maintaining implementation efficiency.

4.1.3 Overview of non-common security threats

While our systematic review has thoroughly discussed the most common threats, it's important to also recognize other significant security threats that didn't meet the common criteria which is to have four or more references in the reference mapping. Although these threats might not be mentioned as frequently, they still present considerable threats to the security of IoT systems in EC environments.

Some of these additional security threats include integrity attacks against ML [55, 9, 39], insufficient/inessential logging [55, 9, 39], Sybil attacks [24, 54, 47], forgery attacks [9, 39, 54], unauthorized control access [9, 39, 47], malware [9, 40, 56], botnets [9, 56, 42], non-standard frameworks and inadequate testing [55, 9], hardware trojans [9, 39], camouflage [9, 39], corrupted or malicious edge computing nodes [9, 39], authentication and authorization attacks [9, 45], routing information attacks [9, 39], ransomware [9, 40], privacy leakage [9, 39], traffic analysis [24, 54], tag cloning attacks [24, 47], hijacking [54, 46], non-network side-channel attacks [39], different framework attacks [39], injecting fraudulent packets [9], data manipulation [24], blackhole attacks [24], sinkhole attacks [24], rogue gateways [50], AI model training attacks [57], AI model interference attacks [57], attacks on private data [57], TCP SYN scanning [58], DMA assaults/cold boot attacks [46], and node capture attacks [47]. All of these non-common security threats can be seen in Figure 4.5.

In conclusion, the wide spectrum of security threats mentioned above target various system parts and characteristics, including data integrity, network functionality, privacy, confidentiality, system architecture, AI algorithms, and specific vulnerabilities. These dangers take advantage of flaws in communication protocols, hardware, software, and authentication processes, causing serious problems for system security. Understanding these threats' characteristics help researchers and practitioners create more effective security safeguards and countermeasures to safeguard sensitive data and preserve system functionality, ultimately improving the overall resilience of systems in the face of changing cyberthreats.

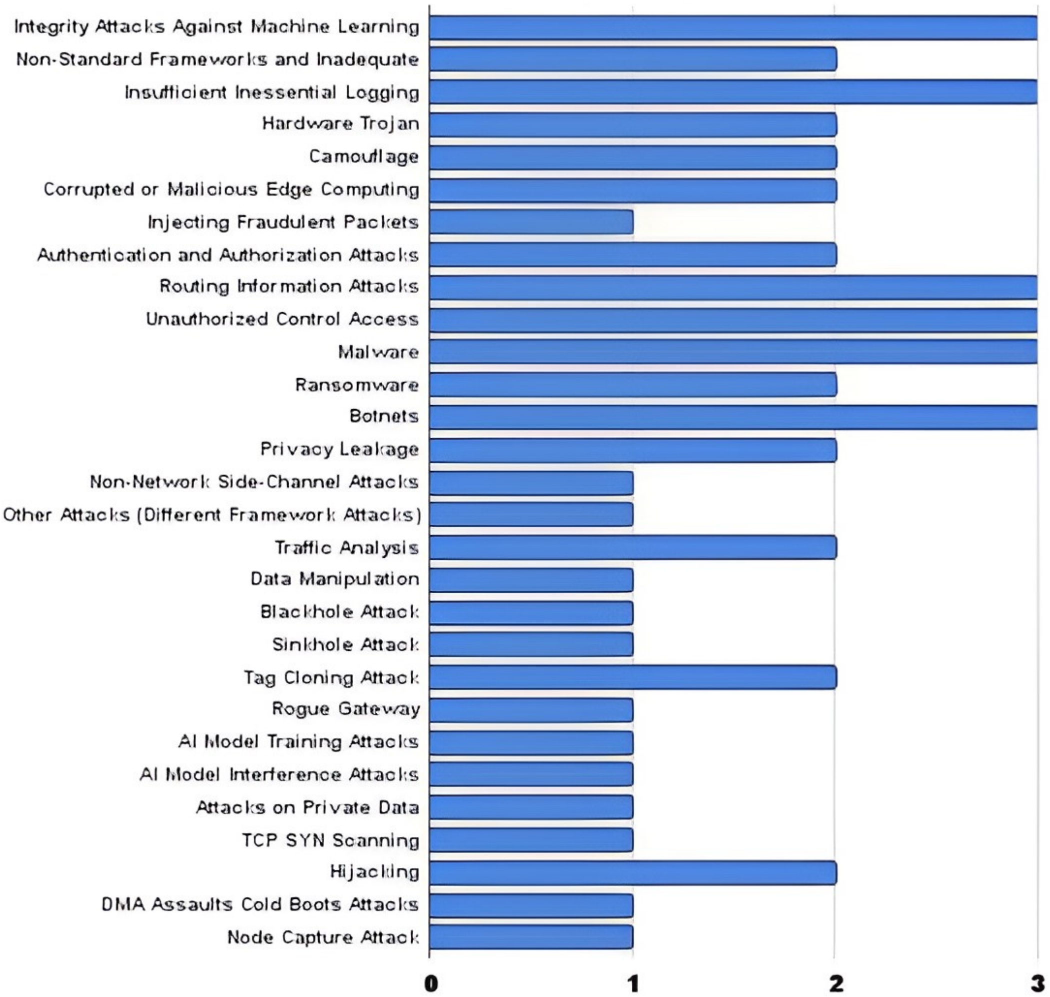


Figure 4.5: Staple chart showing the non-common threats.

4.2 Research Question 2: Review process findings

Figure 4.6 illustrates the distribution of articles obtained from various digital libraries using the search string for RQ2. A total of 534 articles were identified, with 99 sourced from Scopus, 58 from IEEE Xplore, 335 from ACM Digital Library, and 42 from Web of Science.

As in Section 4.1, the variation in the number of articles found in each digital library for this research question can be attributed to differences in focus, coverage, and search strategies. We followed the same methodology in selecting the most relevant and high-quality articles by applying the inclusion and exclusion criteria and our quality assessment.

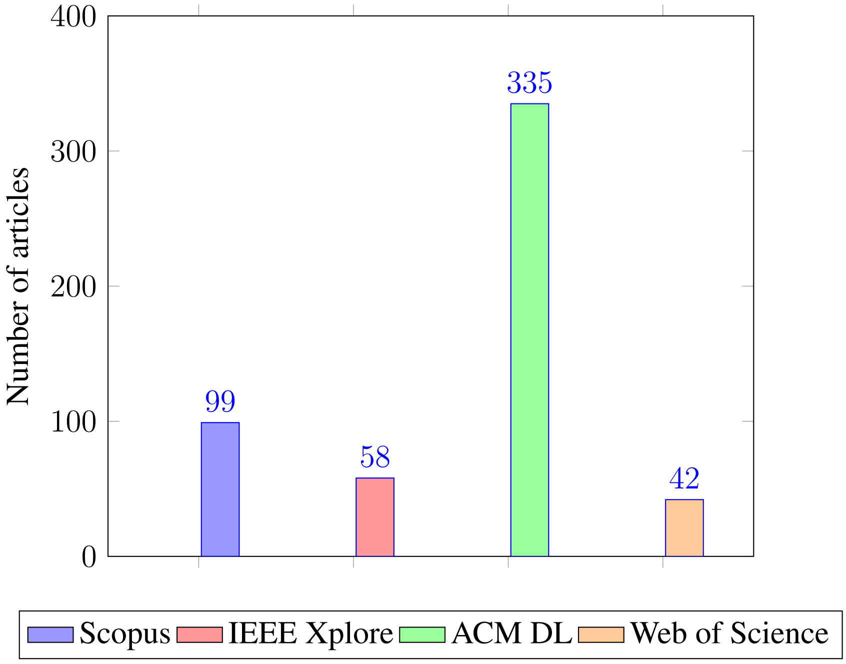


Figure 4.6: Bar chart of research sources for RQ2.

Figure 4.7 presents the results of implementing the search strategy and applying inclusion and exclusion criteria with the help of the Zotero software [13]. Initially, 534 articles were identified across the digital libraries (as shown in Figure 4.7). After excluding non-English articles, the total was reduced to 533 articles, with a loss of 1 article. We imported these articles into Zotero, which helped identify and filter out articles not accessible through the Linnaeus University proxy. This removed another 94 articles, leaving 439 full-text articles. Zotero was then used to identify and remove duplicate articles, resulting in the removal of 62 articles and leaving 377 articles. Then, we manually evaluated each article in Zotero for inclusion criteria IC1 and IC2, removing 347 articles and leaving 30 articles. After that, we performed a quality assessment and eliminated an additional 3 articles. This left us with 27 articles to use in the results.

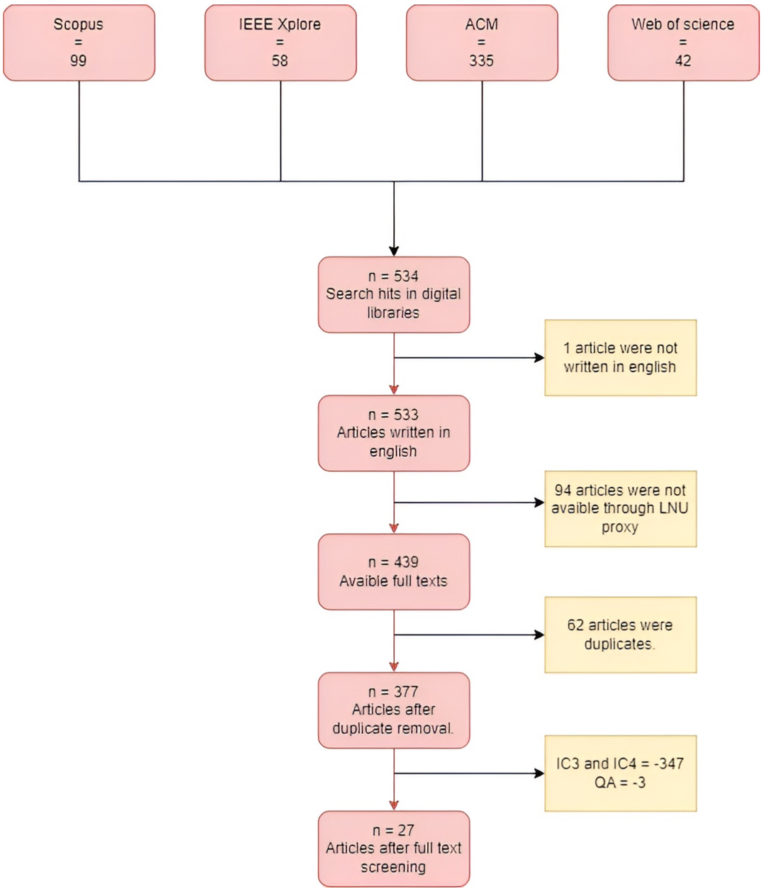

Scopus = 99
IEEE Xplore = 58
ACM = 335
Web of science = 42
n = 534 Search hits in digital libraries
1 article were not written in english
n = 533 Articles written in english
94 articles were not avaible through LNU proxy
n = 439 Avaible full texts
62 articles were duplicates.
n = 377 Articles after duplicate removal.
IC3 and IC4 = -347 QA = -3
n = 27 Articles after full text screening

Figure 4.7: Results of the review process for RQ2.

4.2.1 Unique security issues in sensors, gateways, and actuators

In order to organize the articles and effectively identify the unique issues or threats faced by sensors, gateways, and actuators, a reference mapping has been conducted for categorizing the security issues (DEI9) for the IoT devices, as depicted in Table 4.19. This approach enabled us to consider the issues or threats presented by each edge device in a comprehensive manner. The reference mapping involved analyzing all issues or threats presented in the selected articles, with some articles outlining multiple threats and others focusing on just a few.

For a number of reasons, the mapping of different threats or issues to the three components—sensors, gateways, and actuators—was done independently. First of all, it was impractical to include all of the threats in a single reference mapping due to their sheer number. Also, the majority of these threats are unique. At a later time, we create a reference mapping for each security issue and its proposed countermeasure, which makes it more focused and successful by individually assessing and addressing each component's security issues.

Based on the data provided in the articles, we determined during the reference mapping process which threats or issues applied to which IoT device. Which device the threat was most relevant for was always stated in the article posing the threat. By making it simpler to understand how the references have been mapped, this method of reference mapping is advantageous to authors and readers alike.

Upon analyzing 27 articles for RQ2, we identified 73 unique security issues. Table 4.19 shows the reference mapping, illustrating that some articles discuss multiple threats for the same IoT device. One issue is shared by [59] and [60], resulting in a total of 74 issues in the reference mapping. Among these, 14 were related to sensors, 33 to gateways, and 27 to actuators, as depicted in Figure 4.8.

Table 4.19: DEI9 Security Issues Divided Into IoT Edge Devices.

Article ID (Reference)	IoT Edge Devices
[61] [62] [16] [16] [63] [63] [64] [65] [65] [66] [67] [67] [59] [60]	Sensors
[61] [68] [68] [68] [16] [16] [63] [69] [70] [71] [72] [72] [72] [72] [73] [74] [74] [75] [65] [76] [77] [66] [78] [78] [79] [79] [59] [59] [59] [80] [81] [81] [81]	Gateways
[16] [69] [69] [70] [82] [82] [64] [64] [64] [73] [73] [75] [75] [83] [83] [83] [76] [76] [76] [77] [66] [59] [60] [60] [60] [80] [80]	Actuators

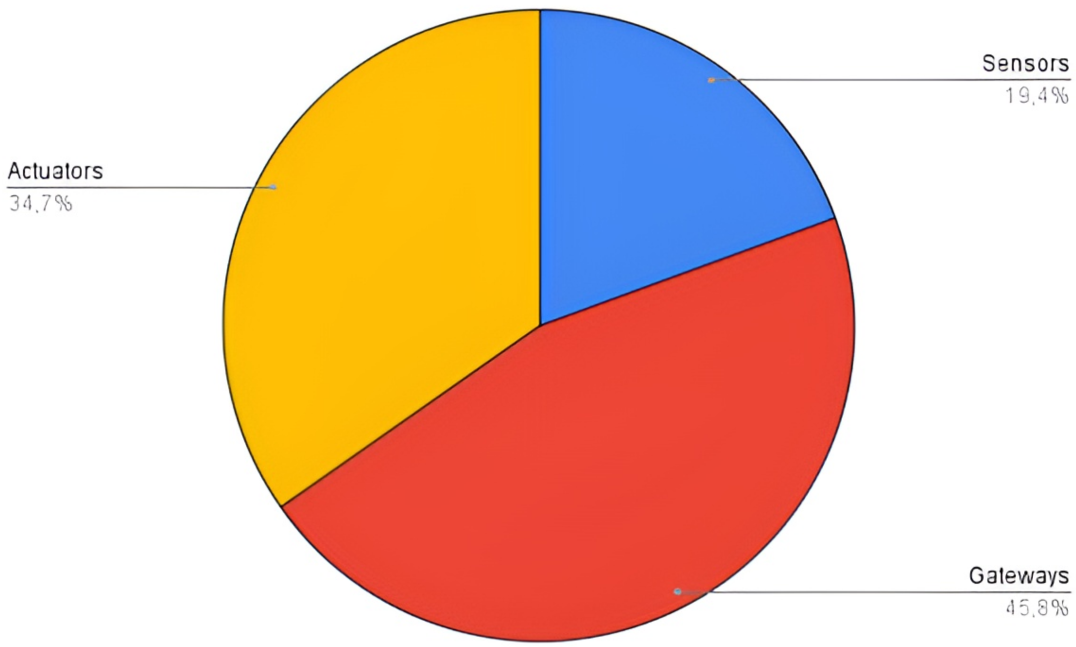


Figure 4.8: Pie chart showing the security issues divided into the edge devices.

4.2.2 Security issues and their countermeasures

In the upcoming sections, we delve into the specific security issues and threats faced by each IoT device category: Sensors, Gateways, and Actuators. Building upon the reference mapping conducted earlier, we provide an in-depth analysis of the unique issues within each component, while also discussing the proposed countermeasures to address these vulnerabilities.

4.2.3 Sensors

When it comes to sensors, it has a total of 14 security issues from our 27 primary articles as can be seen in Table 4.20. These issues in its corresponding article usually always give a countermeasure, and sometimes it even gives multiple. Some articles such as [59] and [60] are very similar and have the same security issue and countermeasure for their issue. Not many articles have the same security issues, even if some can seem the same, especially if one speaks about integrity and confidentiality as a whole since that's a broad topic.

Table 4.20: DEI9 Security Issues & DEI10 Countermeasures - Sensors.

IoT Device	**Security Issue**	**Countermeasures**
Sensors	Performance disparities [61]	SWDR [61]
	Limited resources [62]	CIA Cryptography [62]
	Integrity [16]	Digital signatures & Message authentication code [16]
	Confidentiality [16]	Encryption algorithms & Key management [16]
	Protect edge nodes [63]	Lightweight Algorithms & Protocols [63]
	Ensuring data veracity, value, homogeneity [63]	Data validation & filtering mechanisms [63]
	Secure data trade (P2P) [64]	EdgeBoT (Blockchain + Smart contracts) [64]
	Mass production security negligence [65]	Mode-based Hash Chain [65]
	Insufficient security measures [65]	Timestamps, mode-based hash chaining, zero-knowledge proof property, distributed database/blockchain, cryptography [65]
	Misleading/forged data gathering [66]	Trust evaluation model based on mobile edge nodes [66]
	Insufficient security in IoT devices in edge networks [67]	Intelligent intrusion detection system (IIDS) [67]
	Deployed IoT devices lack security support [67]	Authentication, encryption protocols, regularly update software & firmware, performing security audits [67]
	Security framework impractical for resource-constrained devices [59] [60]	Authentication & encryption protocols [59] [60]

Li et al. [61] brings up a problem called performance disparities in their article which refers to the differences in processing capabilities, power consumption, and data transmission rates among various sensor types. These disparities can lead to inefficiencies, delays, or bottlenecks in the IoT network, impacting the overall performance and responsiveness of the EC system. Their proposed mitigation strategy is called SWDR (Sliding Windows-based Data Reduction.

This method is a technique aimed at improving protocol performance by reducing data overhead and increasing efficiency in data transmission. By implementing SWDR, one can potentially address performance disparities in sensors within EC IoT, as it focuses on optimizing communication between devices and minimizing the latency and resource usage associated with data transmission. This, in turn, can lead to more balanced performance among sensors in the network.

Ometov et al. [62] brings up the problem of limited resources within resource-constrained edge devices, in this case, sensors. These limited resources can affect their ability to handle complex computations, maintain secure connections, and operate efficiently within the network. Their countermeasures are ensuring confidentiality, integrity, and availability through methods like cryptography.

These countermeasures are helpful for sensors with limited resources because they provide an added layer of security without consuming excessive resources. By using a lightweight security solution, resource-constrained sensors can still maintain their primary functions whilst ensuring their security in the edge network.

Yu et al. [16] brings up two problems, namely confidentiality, and integrity. The problem of confidentiality entails that sensors often collect sensitive information, which could be intercepted or tampered with by unauthorized parties during transmission or storage, leading to privacy breaches or unauthorized access to critical data. The problem of integrity entails that data generated by sensors can be manipulated or corrupted by attackers which can result in inaccurate or unreliable information. Their countermeasures are implementing encryption mechanisms and utilizing cryptographic techniques.

For confidentiality they propose that one implements encryption mechanisms to secure data during transmission and storage. Making use of strong encryption algorithms and key management. For integrity they propose that one utilizes cryptographic techniques such as digital signatures and message authentication codes, to verify the integrity of data sent and received within the edge network.

Junior and Kamienski [63] bring up the problem of protecting the distributed edge nodes and addressing their specific security requirements. For sensors, this means that they are often resource-constrained and distributed across various locations. This makes them more vulnerable to security threats such as data breaches, unauthorized access, and tampering. They propose to make use of lightweight security solutions.

The usage of lightweight security solutions provides adequate protection without consuming excessive resources on IoT devices, which is particularly beneficial for resource-constrained sensors. By adopting lightweight security algorithms and protocols, sensors can maintain their functionality while ensuring their data can communication remain secure.

Junior and Kamienski [63] also emphasize another issue concerning sensors, which is ensuring data veracity, value, and homogeneity across various formats and packet technologies. The data veracity mechanism plays a vital role in confirming and discarding outliers within a data set for a given context. Furthermore, it is responsible for detecting manipulated, corrupted, or fabricated data that may have been targeted by attacks or interference, thereby preserving the integrity of the data.

To address these security issues, the authors propose the implementation of data validation and filtering mechanisms that ensure data veracity, value, and homogeneity. These mechanisms not only help in detecting and removing inaccurate or inconsistent data but also contribute to maintaining a secure and reliable data flow in sensors deployed within IoT environments. By doing so, these techniques can effectively reduce the potential risks associated with compromised data and improve the overall performance and stability of IoT systems.

Nawas et al. [64] brings up the problem of vulnerability to cyberattacks due to P2P transactions and the need for secure data trade. This is a problem within sensors because they often communicate directly with each other (P2P transactions) to share data and perform tasks. This P2P communication can make sensors more vulnerable to cyberattacks as attackers might exploit weak security measures, intercept sensitive data, or manipulate sensor data during transmission. Their proposed solution is the usage of EdgeBoT.

The usage of EdgeBoT as a countermeasure for securing P2P data trade within sensors in edge networks leverages the immutability properties of blockchains and smart contracts to ensure data integrity and prevent unauthorized data manipulation during transmission. This secure environment helps protect sensor data from cyberattacks while enabling efficient and trustworthy data exchange among devices in the edge network.

Pardeshi et al. [65] brings up the problem of IoT devices' vulnerability due to mass production and ignoring basic security requirements. The reason this correlates to sensors is that mass-produced IoT devices often prioritize low-cost and rapid production over security measures. As a result, these sensors may lack basic security features or have outdated software, making them more susceptible to cyberattacks. In an EC environment, compromised sensors can put the entire network at risk. Their proposed countermeasure is implementing a mode-based hash chain for secure mutual authentication.

They also bring up the problem of insufficient security measures such as crackable passwords. The reason for this being a problem within sensors in edge networks is that they create a weak point in the network that can be exploited by attacks. Their proposed countermeasure for this to is Utilize techniques such as timestamps, mode-based hash chaining, zero-knowledge proof property, distributed database/blockchain, and cryptography for secure connections.

By implementing a mode-based hash chain for secure mutual authentication it can provide an additional layer of security by ensuring that only authenticated devices can communicate with each other, thus reducing the risk of cyberattacks on vulnerable sensors. Additionally, to counter the problem of insufficient security measures one can Utilize techniques such as timestamps, mode-based hash chaining, zero-knowledge proof property, distributed database/blockchain, and cryptography for secure connections. These techniques enhance the security of data communication and help prevent unauthorized access or tampering, thereby mitigating potential risks.

Wang et al. [66] brings up the problem of misleading or forged data gathering, this is a problem within sensors in edge networks because it can lead to incorrect or even malicious data being processed and acted upon. Thereby it could compromise the reliability, efficiency, and safety of the IoT system. Their proposed solution is making use of a trust evaluation model based on mobile edge nodes.

Making use of a trust evaluation model based on mobile edge nodes is beneficial in this case since it can help detect as well as resist malicious nodes, thus preventing the spread of misleading or forged data and ensuring the accuracy and reliability of data being processed within the IoT system.

Eskandari et al. [67] Brings up two problems, the first being limited security features in contemporary IoT devices which is a problem that arises when modern IoT sensors in EC networks lack built-in security measures which makes them more susceptible to security breaches, data manipulation, and unauthorized access. Their proposed countermeasure for this is the deployment of an IIDS like Passban.
The second problem is that millions of already deployed IoT devices lack hardware security support. This issue refers to the multitude of existing IoT Sensors in EC networks that were not designed with robust hardware security features. Their proposed countermeasures for this are implementing strong authentication and encryption protocols, regularly updating software and firmware, and performing security audits.

For the first problem, deploying an IIDS like Passban since it helps monitor traffic, detect potential security threats, and alert the system administrators to take appropriate countermeasures. For the second problem, implementing strong authentication and encryption protocols can help protect data communication and prevent unauthorized access to the devices. By also regularly updating software and firmware ensures that the devices stay up-to-date with the latest security patches and fixes, reducing the risk of exploitation due to known vulnerabilities and lastly by performing security audits can help identify potential security gaps and weaknesses in the deployed IoT devices, allowing for appropriate remediation measures to be taken.

Lastly Rauf et al. [59] and Butun et al. [60] bring up the same problem which is that resource-constrained devices cannot implement a fool-proof security framework. This means that sensors can be left vulnerable to various security threats such as unauthorized access, data breaches, and cyberattacks which may lead to compromising the security and privacy of the entire edge network. Both propose the same countermeasure for this problem, which is implementing strong authentication and encryption protocols.

Implementing strong authentication and encryption protocols for these resource-constrained sensors can protect sensitive data and ensure secure communication, reducing the risk of unauthorized access and data breaches. They also put a lot of weight in that is important to choose lightweight security protocols to not consume excessive resources on the devices.

4.2.4 Gateways

Regarding gateways, a total of 33 security issues have been identified from 27 primary articles, as illustrated in Figure 4.21 and Figure 4.22. Typically, the corresponding articles propose countermeasure strategies for each issue, with some even suggesting multiple approaches. Although some articles share similar security issues and countermeasures, most articles present unique security concerns. Some issues may appear to be the same, particularly when discussing broader topics like integrity and confidentiality, but they generally differ in their specific aspects.

The existence of two reference mappings is due to the inability to include all security issues and countermeasures for gateways on one reference mapping without drastically shortening the names; however, some of them are still shortened because some are very long; nonetheless, they are fully explained in detail below under the reference mapping. Table 4.21 displays the security issues and countermeasures for the first 11 articles; some of these articles have more than one security issue or countermeasure, so there are 20 total security countermeasures and issues listed. Table 4.22 displays the remaining security issues and countermeasures for a total of 9 articles which shows a total of 11 security issues for gateways.

Table 4.21: DEI9 Security Issues & DEI10 Countermeasures - Gateways (Part 1).

IoT Device	Security Issue	Countermeasures
Gateways	Advanced cyberattacks [61]	PacketVerifier (Framework) [61]
	Edge security [68]	Encryption, authentication, access control [68]
	Resource allocation [68]	Intelligent algorithms & models for distribution [68]
	Data fusion [68]	Advanced data processing methods[68]
	Access control [16]	Access control policies & 2FA authentication [16]
	Cybersecurity [16]	IDS & Firewalls at edge nodes [16]
	Managing devices and communication protocols [63]	Standardization & Security policies [63]
	Edge computing security [69]	Heterogeneous, lightweight & distributed security solutions [69]
	Safeguard threats to communication in the IoT ecosystem [70]	STCS (Smart Thing Control Service) [70]
	Zero-day attacks protection at the edge [71]	Distributed Anomaly Detection (DAD) system: [71]
	Zero-day attacks protection at the edge [71]	IoT-edge-cloud architecture [71]
	Securing edge gateways against cyberthreats & privacy leakage[72]	Edge intelligence assist gateway defense[72]
	Cyberthreat defense & identification at gateways [72]	Employing data-driven anomaly detection [72]
	Implementing emerging data-driven gateway defense [72]	Employing data-driven anomaly detection [72]
	Privacy-preserving data-driven learning [72]	Secure federated learning for privacy preservation [72]
	IoT cloud overload due to bandwidth, latency, and resource scarcity [73]	Edge computing paradigm for IoT resource extension [73]
	Complex security for diverse IoT/IIoT devices and protocols [74]	Edge-IIoTset dataset for ML-based intrusion detection [74]
	Identifying cyberattacks (DoS/DDoS...) [74]	Centralized and federated learning for IDS performance enhancement. [74]
	Identifying cyberattacks (DoS/DDoS...) [74]	Exploratory data analysis for improved threat detection [74]
	Optimal server placement in edge networks [75]	Research on optimal server placement in edge networks [75]

Table 4.22: DEI9 Security Issues & DEI10 Countermeasures - Gateways (Part 2).

IoT Device	Security Issue	Countermeasures
Gateways	Secure interconnection of devices in edge/fog computing [65]	Designing and deploying the HCFE protocol [65]
	Deploying IDS in resource-constrained and diverse IIoT environments [76]	Designing decentralized ID [76]
	Privacy and security in edge-based ML systems [77]	ML architectures for resource-constrained edge devices[77]
	Insecure communication [66]	Trust evaluation using mobile edge nodes [66]
	Decentralized architecture risks & Limited security features [78]	Authentication, encryption, updates, access controls, audits enhance edge network security [78]
	Adversarial attacks & Attack strength [79]	Authentication, encryption, updates, secure communication, access control, audits, risk assessments.[79]
	Privacy and network delays & Real-time application challenges & Increased attack surfaces [59]	IoT in MEC: authentication, encryption, updates, secure communication, innovative solutions, orchestration of multiple mechanisms[59]
	Vulnerabilities in perception systems [80]	IoT in MEC: authentication, encryption, updates, secure communication, new solutions, orchestration of multiple mechanisms [80]
	Edge gateways manage data flow between devices in edge networks [81]	TEE-assisted design & Gateway architecture for better security by isolating networking features & ARM TrustZone technology [81]
	Commodity OSes and services [81]	TEE-assisted design & Gateway architecture for better security by isolating networking features & ARM TrustZone technology [81]
	Recent CVEs [81]	TEE-assisted design & Gateway architecture for better security by isolating networking features & ARM TrustZone technology [81]

Li et al. [61] brings up a security issue on gateways and that is advanced cyberattacks. Advanced cyberattacks on gateways in EC IoT exploit vulnerabilities of low-performance and difficult-to-upgrade edge devices, compromising critical infrastructure. Such attacks, particularly advanced persistent threat (APT) attacks, use lateral movement strategies to gain long-term control over target systems, steal information, and cause damage across multiple networks.

To mitigate these threats, the article proposes PacketVerifier, a network verification framework designed to strengthen edge network security with minimal upgrades. PacketVerifier attaches verification information to packets, ensuring the integrity of data transmission between edge devices and edge gateways. The framework also introduces a new data processing structure called the sliding window double ring (SWDR) for parallel validation, improving the performance of strict sequential protocols. This approach effectively defends edge networks against advanced cyberattacks on gateways while maintaining compatibility with existing network topologies and establishing trustworthy transmission in a zero-trust environment.

Wang et al. [68] discuss three total issues and the first issue is edge security, which aims to protect data privacy and security on distributed and uncontrolled edge devices. They propose putting in place strong security measures like encryption, authentication, and access control to safeguard data in EC environments as a solution to this problem. Incorporating intrusion detection and prevention systems can also assist in locating and neutralizing potential threats, thereby enhancing edge security.

Wang et al. [68] second problem is resource allocation and is relevant for gateways managing multiple edge devices. This is about creating intelligent models and algorithms to intelligently allocate resources among edge devices, ensuring high-quality data processing without taxing individual devices. In order to address this problem, they suggest developing intelligent algorithms and models that can efficiently distribute resources among edge devices, achieving a balance between processing demands and device capabilities.

The third issue presented by Wang et al. [68] is data fusion, which deals with the use of advanced data processing methods to tackle the challenges of combining and analyzing data from various sources. This process aims to reduce delays and maintain data accuracy throughout the system. To mitigate the difficulties of combining and analyzing data from various sources, they advise using advanced data processing methods. These methods increase the overall system reliability and efficiency by minimizing delays while ensuring the accuracy of the data that has been aggregated.

Yu et al. [16] raises two issues in relation to gateways, the first of which is access control. Since gateways serve as the focal point of communication between edge devices and the larger network, this is relevant to them. Only authorized users and devices should be able to access the gateway in order to prevent unauthorized access and possible damage to sensitive data. Implementing a robust system with authentication mechanisms, such as having access control policies to restrict access to authorized users and devices only and also implementing two-factor authentication, is the countermeasure suggested here by Yu et al. [16].

The second issue raised by Yu et al. [16] is cybersecurity, which is essential for gateways given that they are potential targets for cyberattacks and privacy threats. The compromise of a gateway could also result in unauthorized access to data and even command over numerous edge devices, which would be detrimental to the system. The proposed countermeasure here is to deploy IDS and firewalls at the edge nodes to keep an eye on and defend the system against malicious activity. To maintain the network's security, they also advise conducting security audits, patching vulnerabilities, and updating security protocols frequently.

Junior and Kamienski [63] only discusses one security issue in terms of gateways and that is of managing heterogeneous devices and communication protocols. How this connects to gateways is that gateways are the key connection points for numerous edge devices, each using different communication protocols. Their role is to maintain a consistent level of security across these diverse connections, which can be quite challenging. Therefore Junior and Kamienski [63] proposes a countermeasure to develop standardization and security policies that accommodate the heterogeneity of devices and communication protocols and by doing this it can ensure a safer and more reliable IoT EC environment for gateways.

Wang et al. [69] also discusses EC security, similarly to [68]. Here, security is primarily discussed in terms of protecting distributed edge nodes and addressing their unique security needs. Their suggested solution to this problem is to develop and deploy security technologies that are heterogeneous, lightweight, and distributed due to the limitations and requirements of all different devices, such as gateways in the network. As a result, gateways function more reliably and securely overall. This benefits EC systems.

Endler et al. [70] discusses threats to communication between IoT system entities and how to protect this transmitted data between various IoT ecosystem components. This is relevant to gateways as they play a significant role in ensuring good data flow within the IoT ecosystem. The proposed solution to this is something called Smart Thing Control Service, which is about developing and deploying Smart Thing Control Service on the gateways which manages and secures them to make sure they keep their integrity and function. Maintaining the confidentiality, integrity, and availability of information in the IoT system makes the entire EC environment more secure.

Moustafa et al. [71] addresses the security protecting edge network against zero-day attacks, with a more focused approach on the new, previously unknown threats in edge networks with large numbers of IoT devices. These also are a threat to gateways since they are the point of connection between edge devices and the larger network infrastructure as we know them. The authors propose two different countermeasure techniques and the first is to suggest implementing a Distributed Anomaly Detection (DAD) system, specifically the Gaussian Mixture-based Correntropy model, to monitor and recognize zero-day attacks in real-time from edge networks. This helps to detect new and previously unknown threats, enhancing the security of edge networks, including gateways. For the second countermeasure approach, they advise creating and implementing a multi-layered IoT-edge-cloud architecture that shows how IoT, edge, and cloud components are connected to one another. This architecture not only increases security but also makes it possible for network gateways to detect anomalies effectively.

Xu et al. [72] addresses four key security issues related to gateways and the first of those talks about the difficulty in protecting edge gateways from malicious cyberthreats and privacy leaks. They suggest using edge intelligence to support gateway defense in cybersecurity to address this issue, utilizing the strength of intelligent algorithms to improve gateway protection.

Xu et al. [72] second security they discuss is identifying and addressing significant cyberthreats and gateway defense systems. This problem emphasizes the necessity of having a thorough understanding of potential weaknesses and practical defenses to secure gateways in the IoT ecosystem. And this security shares the same countermeasure with the third issue Xu et al. [72] discuss and that issue involves implementing emerging data-driven approaches for gateway defense. Both of these have the same countermeasure and that is to employ data-driven approaches for network anomaly detection and addressing cyberthreats. These approaches leverage data analysis to detect anomalies and strengthen the security of gateways.

And the last and fourth security issue Xu et al. [72] presents is the challenge of preserving privacy while utilizing data-driven learning models and propose mitigating this concern by exploring and applying secure federated learning, an approach that allows for decentralized learning and ensures sensitive data remains protected during the learning process.

Sehrawat et al. [73] tackle a security problem linked to gateways: the excessive strain and expense on IoT cloud owing to limitations in bandwidth, delay, and scarcity of resources. With IoT devices creating vast data quantities, the load on the IoT cloud intensifies, possibly affecting service quality and network efficiency.

To mitigate this concern, the authors propose utilizing EC paradigms to extend cloud storage capacity and computational resources close to IoT devices. By bringing processing capabilities closer to the source of data generation, EC helps reduce the volume of data transition over the cloud, alleviating the load and cost associated with bandwidth, latency, and resource scarcity. This approach not only enhances the efficiency of data processing but also contributes to improving overall network performance and security in the IoT EC environment, particularly in relation to gateways.

Ferrag et al. [74] discuss two issues in their article and the first revolves around handling a variety of IoT and IIoT devices and protocols, which can make security measures more challenging. The authors suggest using a large dataset called Edge-IIoTset to help alleviate this issue. This dataset includes a variety of IoT/IIoT devices and representative protocols, allowing for the development and assessment of ML-based IDS adapted for these various environments.

Addressing the second issue raised by Ferrag et al. [74], which involves recognizing and countering various types of attacks such as malware, MITM, DoS/DDoS, and information gathering, the authors recommend two countermeasures. Firstly, they advocate for the implementation of centralized and federated learning modes to improve the effectiveness and adaptability of IDS. Secondly, they advise using exploratory data analysis to find and extract relevant features for better detection of security threats. By employing these countermeasures, a more robust and effective security framework for gateways can be established.

Sulieman et al. [75] discuss the growing importance of EC in various applications, including IoT. They address the security issue of optimal server placement in edge networks, which is crucial in ensuring efficiency and security, especially in the context of gateways.

As a proposed countermeasure for the security issue related to server placement, they suggest conducting research on optimal server placement, taking into consideration efficiency, security, and communication requirements. This research helps in determining the best locations for servers to enhance the performance and security of the edge network infrastructure, which in turn contributes to improved security for IoT gateways.

Pardeshi et al. [65] raises the problem of securely interconnecting a large number of devices in EC environments. It is a challenge in gateways of edge networks due to the complex and diverse nature of these environments. This can make it difficult to establish secure communication channels and manage device authentication effectively, increasing the risk of unauthorized access, data breaches, and compromised network security.

They propose a countermeasure of designing and deploying the hash-chain fog/edge (HCFE) protocol. It is a beneficial solution for securely interconnecting a large number of devices in EC environments. The HCFE protocol offers a novel mutual authentication scheme and effective session key agreement, ensuring secure protocol communications and reducing the risk of unauthorized access and data breaches.

Hamouda et al. [76] raises the problem of deploying IDS in IIoT environments with resource constraints and varied architectures. It is a challenge for gateways in edge networks due to resource constraints and varied architectures. Limited processing capabilities and diverse network configurations can hinder the effective implementation and operation of IDS, potentially leaving the network vulnerable to attacks and unauthorized access.

They propose the designing of decentralized IDS. This approach provides generalized security across terminals, networks, and service platforms, allowing for effective intrusion detection even in resource-constrained and diverse IIoT environments, and enhancing overall system protection.

Murshed et al. [77] raises the problem of ensuring the privacy and security of user data in edge-based ML systems. It is a challenge in gateways of EC networks because these systems often require extensive access to sensitive information for training and inference. This makes the data vulnerable to potential breaches, unauthorized access, or misuse, which can compromise user privacy and overall system security.

They propose a countermeasure which is utilizing ML architectures specifically designed for resource-constrained EC devices. These architectures typically offer more secure and efficient processing, reducing the risk of data breaches and unauthorized access, while also improving the overall performance of the system.

Wang et al. [66] raises the problem of insecure communication. Insecure communication in gateways of EC networks poses a problem as it increases the risk of sensitive data being intercepted or tampered with during transmission. This can lead to unauthorized access, data breaches, and compromised network security, negatively impacting the overall system's performance and reliability.

They propose a countermeasure in the form of using a trust evaluation model based on mobile edge nodes. By detecting and resisting malicious nodes, this approach helps to maintain secure communication channels, reducing the risk of unauthorized access and potential data breaches.

Angel et al. [78] raises two problems. Decentralized architecture risks: In edge networks, the decentralized distributed architecture can lead to increased security breaches and data loss risks, as potential vulnerabilities may exist in multiple nodes, making it harder to monitor and secure the entire system effectively. Limited security features: Edge devices, due to their constrained processing capabilities, may lack advanced security features. This limitation makes them more susceptible to attacks and compromises, potentially affecting the entire network's security.

They propose a vast range of countermeasures. Addressing the challenges posed by decentralized architectures and limited security features in edge networks involves implementing a combination of security measures. Strong authentication and encryption protocols can protect data and ensure that only authorized users access the system. Regular software and firmware updates help keep the network up-to-date against emerging threats. Secure communication channels, along with access control mechanisms, can prevent unauthorized access and potential breaches. Deploying security solutions directly at the network edge enhances protection for resource-constrained edge devices. Regular security audits and risk assessments contribute to identifying and addressing vulnerabilities proactively, ensuring a robust security posture for gateways in edge networks.

Hatcher et al. [79] raises two problems. The first one is adversarial attacks, in gateways of edge networks, adversarial attacks can be characterized by the attackers' knowledge, goals, and intent. These attacks may target specific vulnerabilities in the system, aiming to disrupt services, steal sensitive information, or gain unauthorized access and control. The second raised problem is attack strength, the strength of attacks on edge network gateways can be measured by factors like frequency, intensity, and duration. Higher frequency or intensity attacks may cause significant damage, overwhelming the system defenses, while prolonged attacks can lead to long-term consequences, negatively affecting overall network performance and security.

They propose various countermeasures for each problem. To counter adversarial attacks and their varying strength in edge networks, a combination of security measures can be employed. Implementing strong authentication and encryption protocols ensures that only authorized users can access the network, and sensitive data remains secure during transmission. Regular software and firmware updates help to address potential vulnerabilities and keep the system up-to-date against emerging threats. Utilizing secure and trusted communication channels reduces the risk of unauthorized access and data interception. Implementing access control mechanisms further limits potential attackers' capabilities by restricting their access to critical systems and resources. Finally, conducting regular security audits and risk assessments helps organizations identify potential weaknesses and address them proactively, strengthening the overall security posture of the gateways in edge networks.

Rauf et al. [59] raises three problems. The first one is privacy and network delays, transferring data from IoT devices to cloud computing platforms can lead to privacy concerns due to the exposure of sensitive information during transmission. The second problem is real-time application challenges, real-time applications demand low latency and minimal jitter to function properly. Delays and jitters in edge networks can degrade the user experience, and even render some applications unusable. The third problem is increased attack surfaces, the growing complexity and interconnectedness of edge networks, IoT devices, and applications contribute to an increased attack surface.

The proposed countermeasures encompass a wide variety of strategies, including the adoption of robust authentication and encryption methods, consistent updates for software and firmware, utilization of secure and reliable communication channels, creation of innovative security solutions tailored for IoT applications in MEC, and the orchestration and integration of multiple security mechanisms. These comprehensive countermeasures aim to address the identified issues effectively.

He et al. [80] raises the problem of vulnerabilities in environment perception systems. This is a problem for gateways in edge networks as these systems are responsible for collecting and processing data from sensors and IoT devices. Compromised perception systems can lead to inaccurate or manipulated data, impacting decision-making, and potentially causing network disruption or security breaches.

They propose a vast range of countermeasures, from implementing strong authentication and encryption protocols, regularly updating software and firmware, making use of secure and trusted communication channels, developing new security solutions for IoT applications in MEC, and orchestrating and integrating diverse security mechanisms. All of these countermeasures are proposed to solve the raised problems

Schwarz [81] raises three problems in the sense of gateways. The first one is that edge gateways are critical components in EC networks, connecting various devices and managing data flow. Their central position and assumed security make them attractive targets for attackers, as compromising them can lead to significant network disruption. The second problem is commodity OSes and services, the use of common operating systems and auxiliary services on gateways increases the attack surface, as these components may have inherent vulnerabilities. This can undermine the perceived security of gateways and expose them to potential threats. The third problem is recent CVEs, new vulnerabilities like authentication bypass or remote code execution can enable attackers to gain full control over gateways and their security policies. Such exploits pose a major risk to the integrity and confidentiality of data services in EC networks.

The author proposes three countermeasures for the above-stated problems. The first one is TEE-assisted design, leveraging a Trusted Execution Environment (TEE) it can help to protect network paths and policies by providing a secure area to execute sensitive code and store data, enhancing gateway security. The second countermeasure, a new gateway architecture that implements an architecture that isolates core networking features from vulnerability auxiliary services and OSes can reduce the attack surface and improve the overall security of gateways in edge networks. The third countermeasure, ARM TrustZone utilizes ARM TrustZone technology that can protect the Network Interface Controller (NIC) and traffic processing from a fully-compromised gateway, as it creates a secure hardware partition for critical components, further strengthening security measures.

4.2.5 Actuators

In the case of actuators, 26 security issues have been identified from the 27 primary articles, as depicted in both Table 4.23 and Table 4.24. The corresponding articles usually provide a mitigation strategy for each issue and occasionally suggest multiple solutions. Some articles are quite similar and present the same security issue and mitigation strategy. Although not many articles share the same security concerns, some issues may appear similar, particularly when addressing broader subjects like integrity and confidentiality.

Similar to the situation with gateways, the need for two reference mappings in the actuators section arises from the challenge of incorporating all security issues and countermeasures into a single reference mapping without significantly shortening the names. Although some names are still abbreviated, they are explained in detail below under the reference mapping. Table 4.23 displays the first 16 security issues in actuators and their countermeasure and Table 4.24 displays the rest of the 10 security issues for actuators, where [80] has two security issues with the same countermeasure.

Table 4.23: DEI9 Security Issues & DEI10 Countermeasures - Actuators (Part 1).

IoT Device	Security Issue	Countermeasures
Actuators	Crucial data accessibility [16]	Designing resilient and fault-tolerant edge computing architectures [16]
	Security threats from within IIoT sensor-cloud [69]	Fine-grained trust evaluation [69]
	Ensuring trustworthiness and reliability in IIoT services [69]	Trust-based service selection [69]
	Threats to IoT system entities [70]	Implementing classic security for smart things [70]
	High demands on computing and storage resources [82]	Distributed secure edge computing architecture [82]
	Trust issues with centralized servers [82]	EdgeX framework with Hyperledger Fabric [82]
	Ensuring secure and private data ownership and management [64]	Hybrid edge-cloud computing architecture [64]
	Secure storage and sharing of encryption keys among devices [64]	ECIES, CKD, and ECDSA [64]
	Resilience against attacks on resource-constrained edge devices [64]	Double authentication [64]
	Security and privacy risks in Edge Computing for IoT [73]	R&D for innovative edge computing solutions [73]
	Issues caused by expanded service requirements [73]	Standard security practices [73]
	Data security in edge networks [75]	Development and implementation of data security measures [75]
	Balancing hybrid edge-cloud computing [75]	Investigating solutions [75]
	Security requirements and attacks [83]	Taxonomy of intrusion detection schemes for WSN and IoT-based communication environments [83]
	Complex architectures and vulnerability [83]	Selecting intrusion detection schemes based on key factors for specific scenarios [83]
	Designing security protocols [83]	Research challenges for WSN and IoT: effective intrusion detection and protocols. [83]

Table 4.24: DEI9 Security Issues & DEI10 Countermeasures - Actuators (Part 2).

IoT Device	Security Issue	Countermeasures
Actuators	Management of distributed IDS agents in decentralized systems [76]	Managing the distributed IDS agents [76]
	Behavior analysis-based IDS for IIoT applications [76]	Behavior analysis-based IDS [76]
	Privacy, resource exploitation and adversarial attacks in ML/DL-based IDS [76]	Addressing challenges in ML and DL-based IDS-solution [76]
	Securing ML models and data on edge devices [77]	Continuous update and monitoring of edge-based ML systems [77]
	Malicious attacks [66]	Performing security audits and regular software/firmware updates [66]
	Privacy and delay issues with IoT-to-cloud data transfer [59] [60]	Edge placement of IoT devices reduces latency and enhances privacy [59] [60]
	Network delays in real-time decision applications [60]	Develop new security solutions & Risk-based trust management models [60]
	Malicious attacks on IoT/Edge harm privacy and finances [60]	Develop new security solutions & Risk-based trust management models [60]
	GPS spoofing for non-cooperative drone control & Integration and interoperability of diverse security mechanisms [80]	IoT in MEC: authentication, encryption, updates, secure communication, new solutions, and orchestration of multiple mechanisms [80]

Yu et al. [16] brings up the problem of that one has to make sure data is accessible when needed. The reason for this being a problem is that actuators rely on real-time data to perform their tasks. Any disruption or delay in data access can lead to malfunctions or inefficiencies in the system. Factors like network congestion, hardware failures, and cyberattacks can affect the availability of data making it difficult for actuators to execute their functions properly and causing potential issues in the IoT system. Their proposed countermeasure is designing resilient and fault-tolerant EC architectures.

By making use of a resilient and fault-tolerant EC architecture it helps to ensure that the actuators can continue to operate effectively even under challenging conditions whilst also contributing to the overall stability and performance of the IoT system.

Wang et al. [69] brings up two problems. The first problem is security threats originating from within the sensor cloud in IIoT networks. The reason for this being a problem within actuators is because they originate is because internal attacks originate from within the system, thereby making the harder to detect and prevent. These threats can compromise the security and functionality of actuators, leading to unauthorized access, manipulation, or disruption of operations, ultimately affecting the overall performance and reliability of the IoT system. Their proposed countermeasure is fine-grained trust evaluation i.e. assessing the trustworthiness of devices and services in the network to detect and prevent internal attacks. The second problem is ensuring the trustworthiness and reliability of services provided in the IIoT ecosystem. With numerous services available, it can be challenging to ensure that the chosen services meet the security and performance requirements needed for actuators to operate efficiently and securely in EC environments. Their proposed countermeasure for the second problem is service selection based on trust

By deploying a fine-grained trust evaluation for actuators in edge networks and assessing the trustworthiness of devices and services, it helps identify potentially malicious or compromised internal elements, mitigating the risk of internal attacks and improving the overall security of the system. For the second problem, by implementing a trust-based service selection method to improve the effectiveness and security of service selection, one can help improve the effectiveness and security of service selection by ensuring that only trustworthy and reliable services are chosen.

Endler et al. [70] brings up the problem of threats to the operation of IoT system entities. If an actuator were to become the target of a cyberattack, it can disrupt the proper function of the system, leading to potential damage, loss of control, or unauthorized access to sensitive data. Ensure the security of each component. Their proposed countermeasure is implementing and adapting classic security solutions for smart things.

By adapting classic security solutions to meet the specific requirements and constraints of IoT systems can help ensure the security of each component, in this actuators whilst maintaining overall network stability and safety. By tailoring security measures to the unique needs of IoT devices can effectively protect them against potential threats and vulnerabilities.

Xu et al. [82] brings up two problems. The first is high demands on computing and storage resources. Actuators in edge networks may experience latency and performance issues due to the high demands on computing and storage resources. This can hinder real-time processing and decision-making, affecting the overall efficiency and responsiveness of the system. Their proposed countermeasure is implementing a distributed secure EC architecture. The second problem is trust issues due to strong dependence on centralized servers. Actuators in edge networks rely on centralized servers for communication and decision-making, which can create trust issues. If a centralized server is compromised, it can affect the entire network which includes actuators. Their proposed countermeasure for this is integrating the EdgeX framework with Hyperledger Fabric.

For the first countermeasure, by implementing a distributed secure EC architecture that combines blockchain platforms and EC frameworks to address the high demands on computing and storage resources in traditional cloud-based IoT architectures. Using multiple data storages and blockchain agents can ensure reliable access, scalability, and secure transactions while eliminating the need for centralized servers, which ultimately improves the performance and security of actuators in edge networks. For the second countermeasure, integrating the EdgeX framework with Hyperledger for addressing trust issues due to strong dependence on centralized servers within actuators in EC. This combination enables loose-coupling EC service scenarios and ensures data integrity in the IoT environment.

Nawas et al. [64] presents three problems in their article. The first one is ensuring secure and private data ownership and management, this is a challenge for actuators within edge networks because they must securely process, store and manage data while maintaining privacy and ensuring that the data owner's rights are protected. The second problem is the need for secure storage and sharing of encryption keys among devices, in edge networks, actuators often need to securely share encryption keys with other devices for encrypted data communication. Ensuring the safety of these keys during storage and transmission can be challenging, especially when devices have limited resources. The third problem is resilience against attacks on resource-constrained edge devices, actuators in edge networks may have limited resources, making them more vulnerable to attacks. Ensuring the resilience of these devices and their ability to maintain secure operation despite resource constraints is a challenge in EC networks. Thereby, they also propose three countermeasures, the first one being hybrid edge-cloud computing architecture, the second one being ECIES, CKD, and ECDSA, and lastly double authentication,

The first countermeasure, hybrid edge-cloud computing architecture is a beneficial solution for actuators in ensuring secure and private data ownership and management, as it leverages smart gateways to run the blockchain. This approach provides scalability and adaptability, making it easier to manage data securely and maintain privacy. The second countermeasure, ECIES, CKD, and ECDSA are cryptographic techniques that help address the need for secure storage and sharing encryption keys among devices in sensors and actuators. ECIES and CDK ensure secure data storage, whilst ECDSA enables secure communication between devices, making it easier to safeguard encryption keys. The third countermeasure, double authentication is for devices that send requests frequently which enhances the resilience against attacks on resource-constrained edge devices. The additional layer of security helps protect sensors and actuators by requiring more stringent authentication making it harder for attackers to compromise the devices.

Sehrawat et al. [73] raises two problems with the first one being security and privacy risks associated with EC-assisted IoT, this essentially means that EC exposes IoT devices to security and privacy risks to a distributed architecture. Their proposed countermeasure for this is investing in research and development which helps create innovative solutions, enhancing EC performance, security, and efficiency.

The second problem is expanded service requirements causing issues, this means that increasingly complex IoT services strain actuators' resources, causing performance and efficiency issues. Securing these systems is challenging, necessitating scalable security solutions and optimized resource allocation. Their proposed countermeasure for this is to implement common countermeasures, by identifying and adopting standard security practices to strengthen EC architecture it is beneficial to mitigate potential risks and vulnerabilities.

Sulieman et al. [75] brings up two problems, the first one being data security in edge networks, ensuring data security in actuators within edge networks is a challenge, as data is processed closer to the originating source. This distributed processing increases the risk of data exposure and vulnerability to attacks, as there are more points of entry for malicious actors. Their proposed countermeasure for the first problem is the development and implementation of data security measures. The second problem is balancing hybrid edge-cloud computing, finding the right balance between edge and cloud computing in actuators within edge networks can be difficult. The goal is to leverage the benefits of both computing models, such as reduced latency and scalability, while minimizing the risks associated with data security and device management. Their proposed countermeasure for the second problem is further investigating hybrid edge-cloud computing solutions.

The first countermeasure, development, and implementation of data security measures helps address the unique challenges of securing data in distributed environments and helps protect actuators from potential threats. The second countermeasure, further investigation of hybrid edge-cloud computing solutions aims to optimize performance and security in various applications. This research can lead to more effective and efficient systems that take advantage of both edge and cloud computing whilst minimizing risks.

Pundir et al. [83] brings up three problems. The first one is security requirements and attacks: In edge networks, actuators face issues regarding security requirements and various attacks in Wireless Sensor Networks (WSN) and IoT-based communication environments, making it difficult to maintain data privacy and system integrity. The second problem is complex architectures and vulnerability: Integrating WSNs into IoT leads to complex architectures, increasing the vulnerability of actuators in edge networks to potential breaches, unauthorized access, and compromised security. The third problem is designing security protocols: Developing effective intrusion detection schemes and security protocols for WSN and IoT-based communication environments can be challenging for actuators in edge networks, given the diverse and resource-constrained nature of these systems.

They propose one countermeasure for each problem. The first problem's countermeasure is developing a taxonomy of existing intrusion detection schemes to help in understanding and categorizing the various techniques applicable to WSN and IoT-based communication environments. The second one is comparing and evaluating intrusion detection schemes based on detection rate, false positive rate, and applicability allows for selecting the most suitable techniques for specific scenarios. And lastly, the third one is identifying future research challenges and working on more effective intrusion detection schemes and security protocols to contribute to enhancing the overall security of WSN and IoT-based communication environments in edge networks.

Hamouda et al. [76] brings up three problems. The first one is the management of distributed IDS agents in decentralized systems, this problem arises due to the challenges of efficiently coordinating multiple IDS agents in a distributed edge network environment, making it difficult to accurately identify and respond to threats for actuators. The second problem is adapting behavior analysis-based IDS IIoT applications, which can be crucial for maintaining the security of actuators in edge networks. The third problem is addressing data privacy, resource exploitation, and adversarial attacks in ML and DL-based IDS solutions, this problem stems from the vulnerability of ML and deep learning-based IDS to data privacy breaches, resource exploitation, and adversarial attacks, which can compromise the security of actuators within edge networks.

The article proposes one countermeasure for each problem which now follows. The first countermeasure is for managing the distributed IDS agents. Developing methodologies to effectively manage and correlate results from distributed IDS agent nodes can streamline threat detection and response, improving security for actuators in edge networks. The second countermeasure is for adapting behavior analysis-based IDS. Enhancing self-adaptability and predictability of intrusions through behavior analysis-based IDS research can enable more tailored and efficient security measures for various IIoT applications, benefiting actuators in edge networks. The third countermeasure is for addressing challenges in ML and DL-based IDS-solution. Investigating and addressing data privacy, resource exploitation, and adversarial attack issues in ML and DL-based IDS solutions can strengthen their effectiveness, leading to more robust security for actuators in edge networks.

Murshed et al. [77] brings up the problem of Safeguarding ML models and data from potential attacks on edge devices. The reason for this being a problem for actuators in edge networks is that compromised models or data can lead to incorrect actuator behavior, affecting the overall functioning and reliability of the edge network. They propose a countermeasure which is to continuously update and monitor edge-based ML systems to address emerging security threats and vulnerabilities.

Continuously updating and monitoring edge-based ML systems to address emerging security threats and vulnerabilities is a solution for the problem in actuators in edge networks, as it helps maintain the integrity and performance of ML models on edge devices.

Wang et al. [66] raises the problem of malicious attacks. Malicious attacks are a problem for actuators within edge networks because they can exploit vulnerabilities, compromise device functionality, and potentially cause data breaches or service disruptions, undermining network security and reliability. Their proposed countermeasure for this is to regularly update software and firmware but also to perform security audits.

These two countermeasures, whilst being simple, are effective. By keeping software and firmware updated it helps to patch vulnerabilities and enhance device security. Performing security audits, which are periodic assessments of the system to identify weaknesses can help ensure proper security measures are in place.

Rauf et al. [54] and Butun et al. [60] raise the same problem which is that transfer of data from IoT to cloud computing can introduce privacy issues and network delays. This is a problem within actuators in edge networks because data transfer from IoT devices to the cloud can expose sensitive information to privacy risks and increase latency, impacting overall system performance and user experience. Their proposed solution for this problem is to locate all devices in the IoT system at the edge, as it brings data processing closer to the end devices, reducing latency and enhancing privacy by minimizing data transfer to distant cloud servers.

Butun et al. [60] raises two further problems. The first one is real-time decision applications and network delays. Actuators in edge networks must respond promptly in real-time applications, but network delays and jitters can impact their performance, leading to suboptimal or even dangerous outcomes in critical situations. The second problem is severe attacks on IoT devices and EC, malicious attacks targeting IoT devices, specifically actuators can cause harm to privacy and financial interest. They propose two countermeasures. The first countermeasure is to develop new security solutions, by enhancing IoT security one increases user trust and acceptability, ensuring safer and more reliable experiences. This countermeasure can be applied to the second problem. The second countermeasure is risk-based trust management models, these models help address security and privacy concerns by prioritizing risks and implementing appropriate countermeasures, this countermeasure can also be applied to the second problem.

He et al. [80] raises two problems, the first one is taking control of non-cooperative drones using GPS spoofing, this is a problem within actuators within edge networks. By manipulating GPS signals, the actuators, which control the drone's movements, would then execute undesired actions based on the compromised navigation data accidents. The second problem is the integration and interoperability of diverse security mechanisms, this can be a problem with actuators within edge networks because it can lead to potential gaps and inconsistencies in security coverage.

They propose a vast range of countermeasures, from implementing strong authentication and encryption protocols, regularly updating software and firmware, making use of secure and trusted communication channels, developing new security solutions for IoT applications in MEC, and orchestrating and integrating diverse security mechanisms. All of these countermeasures are proposed to solve the raised problems.

4.2.6 Summary on security issues and countermeasures

As shown in Table 4.20, the majority of security issues and their corresponding countermeasures for sensors are unique, with minimal overlap. Some articles, such as [16], discuss broader concepts like integrity and confidentiality, which can be applicable to other security issues. Moreover, [62] specifically mentions the CIA triad (Confidentiality, Integrity, and Availability) cryptography as its countermeasure, while [65] employs cryptography more generally as one of its countermeasures. Despite the differing scope, the shared use of cryptography in these cases contributes to the perception that these countermeasures are similar. Apart from these instances, sensor security issues and countermeasures are largely unique. The only articles presenting identical security issues and countermeasures for sensors are [59] and [60], due to their significant similarities.

Then we have the gateways as shown in Tables 4.21 and 4.22, the security issues and corresponding countermeasures presented are diverse and mostly distinct. Some articles such as [16] and [68], discuss broader concepts like access control, encryption, and authentication, which can be applicable to other security issues. Furthermore, solution like the PacketVerifier framework [61] and Smart Thing Control Service (STCS) [70] specifically address unique problems, emphasizing the varied nature of countermeasures.

In summary, the gateways section showcases a wide range of distinct security issues and countermeasures, with only a few overlaps in broader concepts such as access control, encryption, and authentication or ML-based solutions. This highlights the diverse and context-specific nature of the problems and solutions in gateway security.

Lastly, we examine the actuators, as presented in Tables 4.23 and 4.24, which also exhibit a wide range of unique security issues and countermeasures. However, certain articles, such as [66] and [60], discuss malicious attacks, with [60] placing greater emphasis on the detrimental impact on privacy and finances resulting from such attacks. The only articles focusing on the same security issue, privacy, and delay issues in IoT-to-cloud data transfer, are [59] and [60], which also share the same countermeasure. Apart from these instances, most security issues and countermeasures for actuators remain unique.

4.3 Research Question 3: Review process findings

Figure 4.9 illustrates the distribution of articles obtained from the different digital libraries using the RQ3 search string. A total of 878 articles were identified, with 176 sourced from Scopus, 85 from IEEE Xplore, 532 from ACM Digital Library, and 85 from Web of Science.

Similar to Section 4.1 and Section 4.2, the disparity in article counts across digital libraries for this research question is due to their diverse focus, coverage, and search strategies. We maintained consistency in our approach to our methodology by applying the inclusion and exclusion criteria and quality assessment to ensure the selection of the most relevant and high-quality articles.

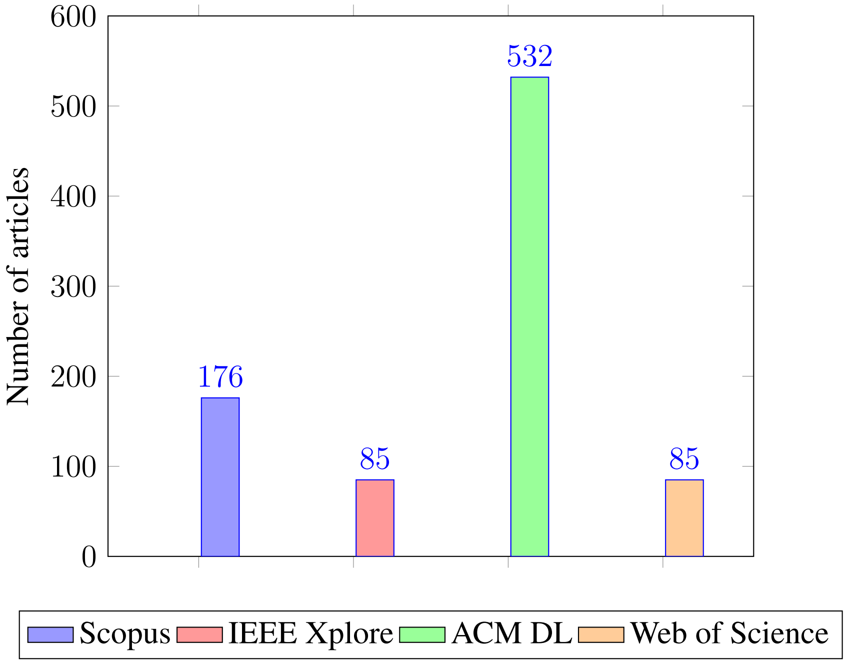
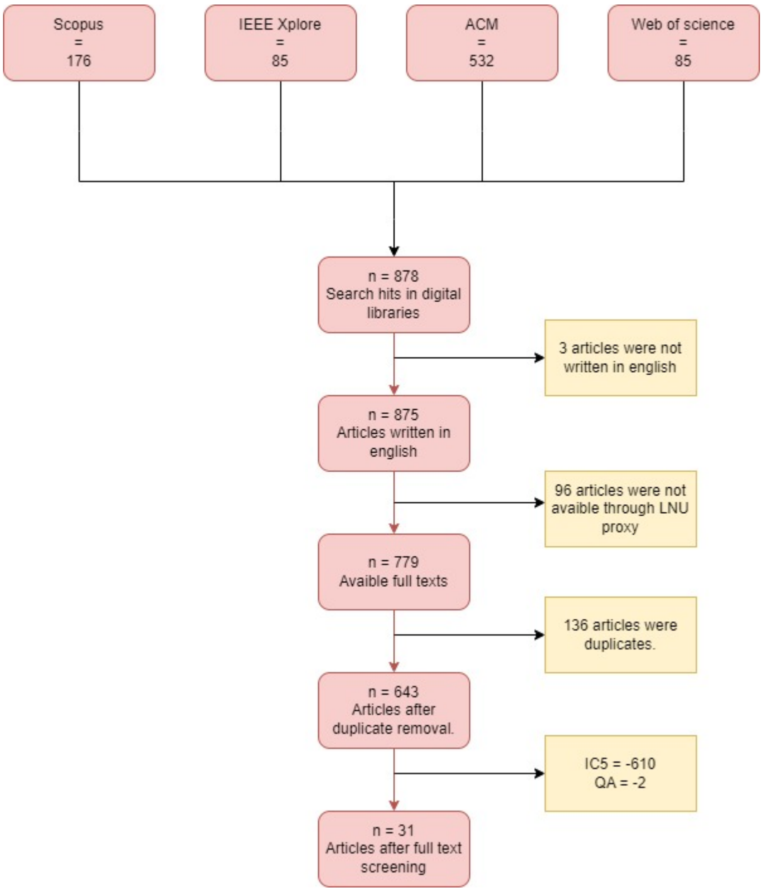


Figure 4.9: Bar chart of research sources for RQ3.

Figure 4.10 shows the results of performing the search strategy and applying inclusion and exclusion criteria. What is shown is the number of articles returned from each digital library when the search string for RQ3 was executed which gives us a total of 878 articles. After excluding articles that were not written in English we were left with 875 articles. After filtering out articles that were not available through the Linnaeus University proxy, another 96 articles were filtered out and we were left with 779 available full texts. Thereafter, the duplicates from each digital library were filtered out which was 136 articles which left us with 643 articles. Lastly, we applied IC5 and then quality assessed them which removed a total of 612 articles which left us with 31 articles which are included in the results.



Scopus = 176
IEEE Xplore = 85
ACM = 532
Web of science = 85
n = 878 Search hits in digital libraries
3 articles were not written in english
n = 875 Articles written in english
96 articles were not avaible through LNU proxy
n = 779 Avaible full texts
136 articles were duplicates.
n = 643 Articles after duplicate removal.
IC5 = -610 QA = -2
n = 31 Articles after full text screening

Figure 4.10: Results of the review process for RQ3.

4.3.1 Advantages by integrating Blockchain in EC-IoT security

In this sub-section, we delve into the security benefits of integrating Blockchain technology with EC in IoT systems. By analyzing the various advantages derived from incorporating Blockchain into IoT applications at the network edge, our goal is to provide a comprehensive understanding of this integration and pinpoint potential areas for future research and development.

All the advantages are outlined in Table 4.25. For clarity and in-depth comprehension, each advantage is discussed individually below the table, along with the respective articles mentioning it. These discussions detail how each advantage contributes to security, as explained in the referenced articles.

Table 4.25: DEI11 Advantages of Blockchain.

Article ID (Reference)	Advantages in Blockchain (DEI11)
[84] [85] [28] [86] [30] [87] [88] [7] [89] [90] [91] [29] [92] [27] [93] [94]	Enhanced security
[90] [58] [94]	Privacy
[28] [29]	Decentralization and Trust
[85]	Trusted identity verification
[85]	Localized cross-domain authentication
[87]	Improved privacy
[87]	Data auditability
[87]	Data ownership
[87]	Non-repudiation
[27]	Ensuring data integrity
[93]	Data transparency
[93]	Authenticity
[87]	Decentralized storage
[88]	False data detection
[95]	Securing SDN-supported, IoT Networks
[95]	Distributed Blockchain Systems
[30]	Permissioned Blockchain-based Access Control Scheme
[96]	Supply Chain Optimization and Security
[97]	Traceable, privacy-preserving, and tamper-resistant ledger

The advantage of EC security for IoT using blockchain integration that is most visible and has the most references is enhanced security. Several articles have arrived at the same conclusion (see, for example, Qi et al. [84] and Lv et al. [85]) which is that when integrating blockchain into edge networks security is enhanced. While articles like Qi et al. [84] present a more generalized way of improving security, their primary focus revolves around traffic classification which in its way enhances security. Whilst Wu et al. [86] has a more streamlined way of explaining how blockchain in edge networks can enhance security. By utilizing blockchain technology to counter collusion attacks and safeguard users' data. The tamper-proof nature of blockchain records ensures the integrity of the interactive information. As mentioned above, these explanations include but are not limited to the two articles mentioned in the explanation.

For trusted identity verification Lv et al. [85] raise a trusted identity-checking mechanism in blockchain-integrated edge networks, which enhances security by ensuring that only verified and legitimate participants can access and interact with the network. It establishes a reliable authentication process by cross-verifying identities against a trusted source. This prevents unauthorized access, data tampering, and other malicious activities, thereby increasing the overall security and trustworthiness of the network.

For localized cross-domain authentication Lv et al. [85] talks about how cross-domain authentication in blockchain-integrated edge networks enhances security by performing the authentication process at the network's edge. This improves efficiency and leverages the low latency of EC, allowing for faster and more secure authentication. Moreover, it minimizes the disclosure of detailed identity information, reducing the risk of data breaches and unauthorized access, thus improving overall security within the network.

For decentralization and trust Fernández-Caramés and Fraga-Lamas [28] and Zou et al. [29] talk about how integrating blockchain into edge networks enhances security and edge intelligence (EI) by providing decentralized and trusted information management. Blockchain's distributed nature promotes collaboration and transparency, addressing the challenges of decentralized management and security in EI. This integration benefits EI by improving computing power management, streamlining data administration, and optimizing models. Ultimately, it leads to a more secure, efficient, and intelligent EC environment.

For improved privacy Ajayi et al. [87] talks about a novel-blockchain-based EC architecture for IoT systems that improves privacy. Making use of data encryption and permissioned access control mechanisms ensures that only authorized parties can access and process sensitive information, which improves privacy for end-users. This is also applicable to data auditability. By making use of blockchain's transparent and tamper-proof nature it allows for easy tracking and verification of data transactions, enhancing trust and accountability. For data ownership, by letting users maintain control over their data, blockchain can enforce data provenance and user rights. For non-repudiation transactions recorded on the blockchain are immutable, ensuring that parties cannot deny their involvement in a transaction.

Song et al. [90], Alkhateeb et al. [91] and Fotia et al. [94] all bring up the matter of privacy in blockchain integrated edge networks. They all make separate points which could be summarized by saying that blockchain integration in edge networks can significantly improve data security, reliability, and user privacy, ultimately increasing trust in edge-based IoT systems.

For ensuring data integrity Ren et al. [27] explain how integrating blockchain with regeneration coding in EC creates a hybrid storage architecture that improves data security and reliability. This approach combines the benefits of edge network devices and cloud storage servers to optimize data storage. This combination of blockchain and regeneration coding offers a robust solution to maintain data integrity in blockchain-integrated networks, contributing to a more secure and reliable EC environment.

For data transparency Fernández-Caramés and Fraga-Lamas [93] tell the reader that blockchain integration enhances data transparency in edge networks by providing a tamper-proof, distributed ledger that records transactions, ensuring visibility and traceability for all network participants.

For authenticity Fernández-Caramés and Fraga-Lamas [93] tell the reader that blockchain enhances authenticity in edge networks by employing cryptographic techniques and consensus algorithms, ensuring that data and transactions are verified and validated by multiple nodes before being recorded.

Lv et al. [85] mention IoT device autonomy as an advantage of integrating blockchain, and IoT devices in the EC environment can control the generation, encrypted storage, registration, use, or cancellation of their identities, improving the overall security and autonomy of the devices.

Ajayi et al. [87] mention decentralized storage as one of the advantages of blockchain. This is because blockchain's distributed storage system enables data to be stored across multiple nodes in a decentralized network, eliminating the need for a single centralized storage entity. By using decentralized storage, blockchain can address concerns related to centralized data storage, data ownership, privacy, and data auditability in IoT systems, making it a viable solution for EC. The reason for this enhancing security is that by distributing data across many nodes, blockchain can enhance data security and redundancy.

Casado-Vara et al. [88] highlight data quality and accurate false data detection as key advantages of incorporating blockchain technology into IoT and EC systems for smart homes. They propose a novel architecture that introduces an EC layer and employs a cooperative game theory algorithm, which, when executed locally, significantly improves the data quality and accurately detects false data, therefore improving security by helping to detect alterations to data.

Hu et al. [95] emphasize the benefits of incorporating blockchain into EC by introducing an EC-based Blockchain as a Service (BaaS) solution that secures SDN-supported IoT networks. This solution employs an efficient, edge-distributed, blockchain system for the verification of inserted flows, effectively reducing the computational burden on IoT systems and highlighting the advantages of distributed blockchain systems, distributing data across multiple nodes in the blockchain enhances the security and resilience of the system.

Zhang et al. [30] discuss a permissioned blockchain-based access control scheme. By integrating blockchain into EC with a permissioned blockchain-based access control scheme for IoT offers several advantages for applications and use cases in integrated blockchain edge networks, such as fine-grained, dynamic access control, high throughput, low latency, and enhanced security by providing secure access controls.

Wang et al. [96] mentions supply chain optimization and security within blockchain-integrated edge networks. This approach offers supply chain optimization and security for various applications and use cases such as traceability, decentralization, security, automation and efficiency, and lastly, interoperability.

Li et al. [97] talks about traceable, privacy-preserving, and tamper-resistant ledgers. Traceable: Blockchain allows for accurate tracking and auditing of data transactions among decentralized intelligent network edges (DINES), end users, and supervisors, enhancing transparency and accountability. Privacy-preserving: Blockchain's cryptographic mechanisms protect sensitive data and ensure user privacy while sharing edge knowledge within the network. amper-resistant: Blockchain's immutable ledger and consensus algorithms prevent unauthorized data modifications, ensuring data integrity and security in edge networks.

4.3.2 Advantages by integrating 5G in EC-IoT security

In comparison to the blockchain integration seen in Section 4.3.1, the instances of advantages associated with 5G integration were fewer, appearing in only two articles. These articles identified three distinct advantages, which, while less numerous than those for blockchain, still provide significant insight into the potential benefits of 5G integration. The specifics of these advantages are presented in Table 4.26 and are discussed below it.

Table 4.26: DEI12 Advantages of 5G.

Article ID (Reference)	**Advantages in 5G (DEI12)**
[34]	Security
[34]	Privacy
[29]	Device Access Management

Zou et al. [29] address the issue of device access management. By incorporating 5G technology into edge networks, multiple IoT devices' access problems are ameliorated due to higher bandwidth and enhanced connectivity. This integration facilitates simultaneous data processing from a multitude of devices, thereby boosting the overall performance and efficiency of the network in a 5G environment. From a security standpoint, improved device access management reduces the risk of unauthorized access and potential cyberattacks, enhancing the security robustness of the entire IoT system.

Braeken and Liynage [34] highlight several advantages of 5G, including high availability, scalability, reduced backhaul bandwidth costs, low latency, local awareness, and, importantly, enhanced security and privacy. These attributes position 5G as an integral element for the future of EC. The improved data processing and real-time performance facilitated by 5G not only increase edge network capabilities but also strengthen security measures. This is because faster data processing and localized decision-making can help identify and mitigate potential security threats more quickly, leading to a more secure IoT ecosystem.

4.3.3 Summary on Blockchain and 5G integration

In the course of conducting this SLR, we focused on examining the advantages and potential disadvantages of integrating Blockchain and 5G technologies into EC for IoT systems. Interestingly, our primary articles did not highlight any notable disadvantages. Therefore, the results in this SLR center exclusively on the numerous advantages that emerged from the literature.

The incorporation of Blockchain technology into EC for IoT systems brings substantial improvements in terms of security. Blockchain's decentralized architecture ensures a high degree of trust [28, 29], and these are fundamental aspects in various applications. Notably, blockchain enables trusted identity verification and localized cross-domain authentication, further strengthening the security landscape [85].

Moreover, blockchain technology provides enhanced privacy [90, 58, 94], data auditability, and data ownership, as well as non-repudiation, all contributing to an improved security framework [87]. This technology also ensures data integrity [27] and fosters data transparency and authenticity [93].

Blockchain's capabilities extend to securing SDN-supported IoT Networks [95], and it supports a permissioned blockchain-based access control scheme, which is especially beneficial for supply chain optimization and security [30, 96]. Lastly, blockchain provides a traceable, privacy-preserving, and tamper-resistant ledger, crucial for maintaining system reliability [97].

On the other hand, the implementation of 5G technology in edge networks contributes significantly to the enhancement of system security and privacy [34]. Furthermore, 5G technology aids in efficient device access management, leading to more streamlined operations [29].

While the primary focus of this SLR is on the direct security advantages of integrating Blockchain and 5G technologies into EC for IoT systems, it's crucial to mention that numerous other advantages were identified in the literature. These include improvements in efficiency, scalability, and performance, among others. Although these benefits may not directly relate to security, they could indirectly contribute to a more secure and robust system by enhancing its overall performance and reliability. Future research could explore these indirect security implications in more detail.

5 Conclusion and Future Work

The increasing prevalence of IoT devices and the growing adoption of EC have amplified the need for robust security measures. The integration of Blockchain and 5G technologies presents promising opportunities for enhancing security within EC environments for IoT. This study explores three research questions to better understand the current landscape, challenges, and implications of security for IoT in EC environments. In particular, it focuses on the three most prevalent edge devices: sensors, gateways, and actuators, as well as the potential advantages of integrating Blockchain and 5G. The SLR aims to shed light on cutting-edge research and trends in EC security for IoT, serving as a valuable resource for researchers, practitioners, and stakeholders.

5.1 Summary and concluding remarks

This study carries out an SLR on the security of IoT devices in EC environments. Drawing from sources in digital libraries such as Scopus, IEEE Xplore, ACM DL, and Web of Science, published between 2015 and 2023, the study delves into the following research questions to provide comprehensive insights and analysis:

- **RQ1:** What are the most common security threats faced by IoT devices in edge computing, and what are the most effective strategies for mitigating these threats?
- **RQ2:** What are the unique security issues or threats presented by sensors, gateways, and actuators in edge computing for IoT, and what are the most effective countermeasures for securing these types of devices?
- **RQ3:** What are the advantages of integrating Blockchain and 5G technologies into edge computing security for IoT?

To answer the first research question, a total of 24 primary articles were analyzed, each presenting at least one security threat, with some discussing multiple threats. To determine the most common security threats, we assessed the reference mapping detailed in Section 4.1.1, identifying threats with over four references as the most common. As depicted in Figure 4.4, the most common security threats encountered by IoT devices in EC environments included DDoS attacks, DoS attacks, MITM attacks, Malicious Code/Malware injections, Eavesdropping/Sniffing attacks, Replay/Freshness attacks, Physical/Tampering attacks, Jamming attacks, Spoofing attacks, Node replication, and Side-channel attacks.

Various effective mitigation strategies were proposed for each risk, as outlined and discussed in Section 4.1.2. Many articles recommended using their own unique algorithms, protocols, frameworks, or specialized IDS based on ML or SDN to address the security threats discussed in their respective articles. In contrast, several articles frequently mentioned mitigation measures that were applicable to most security threats. These common strategies included IDS, firewalls, cryptography, packet filters, cryptanalysis, packet flow analysis, steganography, cryptographic algorithms, authentication protocols, pre-testing, circuit modification/replacement, and firmware security.

To answer the second research question, a total of 27 primary articles were analyzed, revealing that the unique issues or threats presented by sensors, gateways, and actuators in EC for IoT vary among the devices. Categorization was done for each security issue in all 27 primary articles, as discussed in Section 4.2.1, allowing for the identification of the specific security issues or threats faced by each device. The categorization was based on the article mentioning the relationship between the security issue and the device or presenting it in an obvious manner. Out of 74 total security issues identified, 73 were unique. As discussed in Section 4.2.6, while some security issues were somewhat similar, they focused on different aspects, approached the issue from different perspectives, and proposed distinct countermeasures.

The detailed analysis of each security issue and its proposed countermeasure can be found in Sections 4.2.3, 4.2.4, and 4.2.5. It is important to understand that solving these particular security problems is essential for enhancing the security of IoT devices, in particular sensors, gateways, and actuators, which considerably increase the general security and dependability of IoT systems. Researchers and practitioners can create more efficient and focused countermeasures by having a complete awareness of the wide spectrum of threats and vulnerabilities linked to these three devices.

In answering the third research question, we analyzed a total of 31 primary articles, illustrating the advantages of integrating Blockchain and 5G into EC security for IoT. Notably, no disadvantages were mentioned in these articles; thus, only the advantages were highlighted.

Section 4.3.1 presents the advantages of Blockchain integration, with a total of 19 advantages identified. While most articles primarily emphasized enhanced security, others mentioned additional advantages related to security. These included privacy, decentralization and trust, trusted identity verification, localized cross-domain authentication, improved privacy, data auditability, data ownership, non-repudiation, data integrity assurance, data transparency, authenticity, decentralized storage, false data detection, security of SDN-supported IoT networks, distributed blockchain systems, permissioned blockchain-based access control schemes, optimization and security of supply chains, as well as traceable, privacy-preserving and tamper-resistant ledgers.

Section 4.3.2 details the advantages of integrating 5G, which were fewer in comparison to those of Blockchain. With a total of 3 identified benefits, the advantages of 5G integration cover aspects such as security, privacy, and device access management.

5.2 Future work

This SLR has made significant progress in understanding the security threats faced by IoT devices in EC, the unique security issues presented by sensors, gateways, and actuators, as well as the advantages of integrating Blockchain and 5G technologies into EC security for IoT. However, the review has also exposed areas that require further exploration.

We identified a notable lack of research during the course of our SLR that particularly examines the potential disadvantages of incorporating Blockchain and 5G technologies into EC security for IoT systems. The vast bulk of the literature that is now available seems to focus on the benefits and possibilities of these technologies, frequently presenting a positive picture of greater security, improved scalability, and effective data management. However, like any other technology, Blockchain and 5G may also present certain challenges or drawbacks when integrated into EC. These could range from issues of latency, energy consumption, and data privacy, to more systemic challenges such as compatibility with existing infrastructure, cost of implementation, and the need for regulatory oversight. Therefore, there is a clear need for future work that investigates these aspects to provide a more balanced perspective on the use of Blockchain and 5G technologies.

The scope and effectiveness of an SLR heavily depend on the comprehensiveness of the employed search strategy. The search strings used in this review were designed to be broad enough to capture a wide range of relevant literature while remaining focused on the specific research questions at hand.

However, given more time, our search strategy could have been extended and refined to potentially uncover a greater number of studies and provide a more exhaustive review of the topic. In particular, the use of additional or alternative search terms and keywords could have brought to light studies that our initial search strings may have missed.

References

[1] Fortune Business. (2022) Internet of things (iot market size, share and covid 19 impact analysis. [Online]. Available: https://www.fortunebusinessinsights.com/industry-reports/internet-of-things-iot-market-100307

[2] W. Shi and S. Dustdar, "The promise of edge computing," *Computer*, vol. 49, no. 5, pp. 78–81, 2016.

[3] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on iot security: Application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82 721–82 743, 2019.

[4] K. Sha, T. A. Yang, W. Wei, and S. Davari, "A survey of edge computing-based designs for iot security," *Digital Communications and Networks*, vol. 6, no. 2, pp. 195–202, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2352864818303018

[5] J. Ni, X. Lin, and X. S. Shen, "Toward edge-assisted internet of things: From security and efficiency perspectives," *IEEE Network*, vol. 33, no. 2, pp. 50–57, 2019.

[6] S. Shen, K. Zhang, Y. Zhou, and S. Ci, "Security in edge-assisted internet of things: challenges and solutions," *Science China Information Sciences*, vol. 63, no. 12, Nov. 2020. [Online]. Available: https://doi.org/10.1007/s11432-019-2906-y

[7] J. Pan and Z. Yang, "Cybersecurity Challenges and Opportunities in the New "Edge Computing + IoT" World," in *Proceedings of the 2018 ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization*, ser. SDN-NFV Sec'18. New York, NY, USA: Association for Computing Machinery, Mar. 2018, pp. 29–32.

[8] S. S. Jazaeri, S. Jabbehdari, P. Asghari, and H. H. S. Javadi, "Edge computing in SDN-IoT networks: a systematic review of issues, challenges and solutions," *Cluster Computing*, vol. 24, no. 4, pp. 3187–3228, Jun. 2021. [Online]. Available: https://doi.org/10.1007/s10586-021-03311-6

[9] E. Fazeldehkordi and T.-M. Grønli, "A Survey of Security Architectures for Edge Computing-Based IoT," *IoT*, vol. 3, no. 3, pp. 332–365, Jun. 2022. [Online]. Available: https://www.mdpi.com/2624-831X/3/3/19

[10] B. Kitchenham and S. Charters, "Guidelines for performing systematic literature reviews in software engineering," vol. 2, 01 2007.

[11] B. Kitchenham, "Procedures for performing systematic reviews," *Keele, UK, Keele Univ.*, vol. 33, 08 2004.

[12] K. Arabi, "Trends, opportunities and challenges driving architecture and design of next generation mobile computing and iot devices," Aug 2022. [Online]. Available: https://www.mtl.mit.edu/events-seminars/seminars/trends-opportunities-and-challenges-driving-architecture-and-design-next

[13] Zotero, "Zotero: Your personal research assistant," https://www.zotero.org/, 2021.

[14] R. Dirnfeld, "Digital twins in railways," Ph.D. dissertation, 06 2022.

[15] Validity and reliability, [Online]. Available: https://coursepress.lnu.se/courses/thesis-projects/02-course-content/03-validity-and-reliability.

[16] W. Yu, F. Liang, X. He, W. G. Hatcher, C. Lu, J. Lin, and X. Yang, "A Survey on the Edge Computing for the Internet of Things," *IEEE Access*, vol. 6, pp. 6900–6919, 2018, conference Name: IEEE Access.

[17] M. Chiang, S. Ha, F. Risso, T. Zhang, and I. Chih-Lin, "Clarifying fog computing and networking: 10 questions and answers," *IEEE Communications Magazine*, vol. 55, no. 4, pp. 18–20, 2017.

[18] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[19] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (iot): A vision, architectural elements, and future directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645–1660, 2013.

[20] K. Ashton, "That 'internet of things' thing," RFID Journal, 2009.

[21] P. P. Ray, "A survey on internet of things architectures," *Journal of King Saud University - Computer and Information Sciences*, vol. 30, no. 3, pp. 291–319, 2016.

[22] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge computing: Vision and challenges," *IEEE Internet of Things Journal*, vol. 3, no. 5, pp. 637–646, 2016.

[23] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," *Computer Networks*, vol. 57, no. 10, pp. 2266–2279, 2013.

[24] S. Swamy and S. Kota, "An empirical study on system level aspects of Internet of Things (IoT)," *IEEE Access*, vol. 8, pp. 188 082–188 134, 2020.

[25] S. A. Bhat, I. B. Sofi, and C.-Y. Chi, "Edge computing and its convergence with blockchain in 5g and beyond: Security, challenges, and opportunities," *IEEE Access*, vol. 8, pp. 209 425–209 450, 2020.

[26] F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues," *Telematics and Informatics*, vol. 36, pp. 55–81, 2019.

[27] Y. Ren, Y. Leng, Y. Cheng, and J. Wang, "Secure data storage based on blockchain and coding in edge computing," *Mathematical Biosciences and Engineering*, vol. 16, no. 4, pp. 1874–1892, 2019.

[28] T. Fernández-Caramés and P. Fraga-Lamas, "A Review on the Use of Blockchain for the Internet of Things," *IEEE Access*, vol. 6, pp. 32 979–33 001, 2018.

[29] J. Zou, D. He, S. Zeadally, N. Kumar, H. Wang, and K. R. Choo, "Integrated Blockchain and Cloud Computing Systems: A Systematic Survey, Solutions, and Challenges," *ACM Computing Surveys*, vol. 54, no. 8, pp. 160:1–160:36, Oct. 2021.

[30] L. Zhang, B. Li, H. Fang, G. Zhang, and C. Liu, “An Internet of Things Access Control Scheme Based on Permissioned Blockchain and Edge Computing,” *Applied Sciences (Switzerland)*, vol. 13, no. 7, 2023.

[31] J. G. Andrews, S. Buzzi, W. Choi, S. V. Hanly, A. Lozano, A. C. K. Soong, and J. C. Zhang, “What will 5g be?” *IEEE Journal on selected areas in communications*, vol. 32, no. 6, pp. 1065–1082, 2014.

[32] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, “Internet of things: A survey on enabling technologies, protocols, and applications,” *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.

[33] J. Wang, J. Pan, F. Esposito, P. Calyam, Z. Yang, and P. Mohapatra, “Edge Cloud Offloading Algorithms: Issues, Methods, and Perspectives,” *ACM Computing Surveys*, vol. 52, no. 1, pp. 2:1–2:23, Feb. 2019.

[34] A. Braeken and M. Liyanage, “Highly efficient key agreement for remote patient monitoring in MEC-enabled 5G networks,” *Journal of Supercomputing*, vol. 77, no. 6, pp. 5562–5585, 2021.

[35] A. Narayanan, A. Sena, D. Gutierrez-Rojas, D. Melgarejo, H. Hussain, M. Ullah, S. Bayhan, and P. Nardelli, “Key Advances in Pervasive Edge Computing for Industrial Internet of Things in 5G and beyond,” *IEEE Access*, vol. 8, pp. 206 734–206 754, 2020.

[36] I. Makhdoom, M. Abolhasan, J. Lipman, R. P. Liu, and W. Ni, “Anatomy of threats to the internet of things,” *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1636–1675, 2019.

[37] H. Zhou, S. Pal, Z. Jadidi, and A. Jolfaei, “A Fog-Based Security Framework for Large-Scale Industrial Internet of Things Environments,” *IEEE Internet of Things Magazine*, vol. 6, no. 1, pp. 64–68, Mar. 2023, number: 1 Conference Name: IEEE Internet of Things Magazine.

[38] Q. He, C. Wang, G. Cui, B. Li, R. Zhou, Q. Zhou, Y. Xiang, H. Jin, and Y. Yang, “A Game-Theoretical Approach for Mitigating Edge DDoS Attack,” *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 4, pp. 2333–2348, Jul. 2022, number: 4 Conference Name: IEEE Transactions on Dependable and Secure Computing.

[39] A. Alwarafy, K. A. Al-Thelaya, M. Abdallah, J. Schneider, and M. Hamdi, “A Survey on Security and Privacy Issues in Edge-Computing-Assisted Internet of Things,” *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4004–4022, Mar. 2021, conference Name: IEEE Internet of Things Journal.

[40] G. Bernieri, M. Conti, and F. Turrin, “KingFisher: an Industrial Security Framework based on Variational Autoencoders,” in *Proceedings of the 1st Workshop on Machine Learning on Edge in Sensor Systems*, ser. SenSys-ML 2019. New York, NY, USA: Association for Computing Machinery, Nov. 2019, pp. 7–12. [Online]. Available: https://dl.acm.org/doi/10.1145/3362743.3362961

[41] K. S. Sahoo and D. Puthal, "SDN-Assisted DDoS Defense Framework for the Internet of Multimedia Things," *ACM Trans. Multimedia Comput. Commun. Appl.*, vol. 16, no. 3s, pp. 98:1–98:18, Dec. 2020. [Online]. Available: https://dl.acm.org/doi/10.1145/3394956

[42] P. Krishnan, S. Duttagupta, and K. Achuthan, "SDN/NFV security framework for fog-to-things computing infrastructure," *Software - Practice and Experience*, vol. 50, no. 5, pp. 757–800, 2020.

[43] ——, "SDNFV Based Threat Monitoring and Security Framework for Multi-Access Edge Computing Infrastructure," *Mobile Networks and Applications*, vol. 24, no. 6, pp. 1896–1923, 2019.

[44] T. G. Nguyen, T. V. Phan, B. T. Nguyen, C. So-In, Z. A. Baig, and S. Sanguanpong, "SeArch: A Collaborative and Intelligent NIDS Architecture for SDN-Based Cloud IoT Networks," *IEEE Access*, vol. 7, pp. 107 678–107 694, 2019, conference Name: IEEE Access.

[45] M. Ansari, S. Alsamhi, Y. Qiao, Y. Ye, and B. Lee, "Security of Distributed Intelligence in Edge Computing: Threats and Countermeasures," *Palgrave Studies in Digital Business and Enabling Technologies*, pp. 95–122, 2020.

[46] F.-G. Kolimbianakis and G. Kornaros, "Software-defined hardware-assisted isolation for trusted next-generation IoT systems," in *Proceedings of the 37th ACM/SIGAPP Symposium on Applied Computing*, ser. SAC '22. New York, NY, USA: Association for Computing Machinery, May 2022, pp. 139–146. [Online]. Available: https://dl.acm.org/doi/10.1145/3477314.3508378

[47] R. Krishna, A. Priyadarshini, A. Jha, B. Appasani, A. Srinivasulu, and N. Bizon, "State-of-the-art review on IoT threats and attacks: Taxonomy, challenges and solutions," *Sustainability (Switzerland)*, vol. 13, no. 16, 2021.

[48] A. Valantasis, N. Psaromanolakis, and V. Theodorou, "Zero-Touch Security Automation Mechanisms for Edge NFV: The π-Edge Approach," in *Proceedings of the 18th International Conference on Network and Service Management*, ser. CNSM '22. Laxenburg, AUT: International Federation for Information Processing, Jan. 2023, pp. 1–7.

[49] A. M. Shaaban, C. Schmittner, T. Gruber, A. B. Mohamed, G. Quirchmayr, and E. Schikuta, "CloudWoT - A Reference Model for Knowledge-based IoT Solutions," in *Proceedings of the 20th International Conference on Information Integration and Web-based Applications & Services*, ser. iiWAS2018. New York, NY, USA: Association for Computing Machinery, Nov. 2018, pp. 272–281. [Online]. Available: https://dl.acm.org/doi/10.1145/3282373.3282400

[50] J. Zhang, B. Chen, Y. Zhao, X. Cheng, and F. Hu, "Data Security and Privacy-Preserving in Edge Computing Paradigm: Survey and Open Issues," *IEEE Access*, vol. 6, pp. 18 209–18 237, 2018.

[51] L. Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider, "IoT privacy and security: Challenges and solutions," *Applied Sciences (Switzerland)*, vol. 10, no. 12, 2020.

[52] S. Charles and P. Mishra, "Reconfigurable Network-on-Chip Security Architecture," *ACM Trans. Des. Autom. Electron. Syst.*, vol. 25, no. 6, pp. 53:1–53:25, Aug. 2020. [Online]. Available: https://dl.acm.org/doi/10.1145/3406661

[53] H. Kim, E. Kang, D. Broman, and E. A. Lee, "Resilient Authentication and Authorization for the Internet of Things (IoT) Using Edge Computing," *ACM Trans. Internet Things*, vol. 1, no. 1, pp. 4:1–4:27, Mar. 2020. [Online]. Available: https://dl.acm.org/doi/10.1145/3375837

[54] E. Michailidis, K. Maliatsos, D. Skoutas, D. Vouyioukas, and C. Skianis, "Secure UAV-Aided Mobile Edge Computing for IoT: A Review," *IEEE Access*, vol. 10, pp. 86 353–86 383, 2022.

[55] A. Mosenia and N. Jha, "A comprehensive study of security of internet-of-things," *IEEE Transactions on Emerging Topics in Computing*, vol. 5, no. 4, pp. 586–602, 2017.

[56] A. Lekssays, G. Sirigu, B. Carminati, and E. Ferrari, "MalRec: A Blockchain-based Malware Recovery Framework for Internet of Things," in *Proceedings of the 17th International Conference on Availability, Reliability and Security*, ser. ARES '22. New York, NY, USA: Association for Computing Machinery, Aug. 2022, pp. 1–8. [Online]. Available: https://dl.acm.org/doi/10.1145/3538969.3544446

[57] C. Zhou, Q. Liu, and R. Zeng, "Novel defense schemes for artificial intelligence deployed in edge computing environment," *Wireless Communications and Mobile Computing*, vol. 2020, 2020.

[58] K. Cabaj, M. Gregorczyk, W. Mazurczyk, P. Nowakowski, and P. Żórawski, "SDN-based Mitigation of Scanning Attacks for the 5G Internet of Radio Light System," in *Proceedings of the 13th International Conference on Availability, Reliability and Security*, ser. ARES 2018. New York, NY, USA: Association for Computing Machinery, Aug. 2018, pp. 1–10. [Online]. Available: https://dl.acm.org/doi/10.1145/3230833.3233248

[59] A. Rauf, R. A. Shaikh, and A. Shah, "Security and privacy for IoT and fog computing paradigm," in *2018 15th Learning and Technology Conference (L&T)*, Feb. 2018, pp. 96–101.

[60] I. Butun, A. Sari, and P. Österberg, "Security Implications of Fog Computing on the Internet of Things," in *2019 IEEE International Conference on Consumer Electronics (ICCE)*, Jan. 2019, pp. 1–6, iSSN: 2158-4001.

[61] Z. Li, Y. Ding, H. Gao, B. Qu, Y. Wang, and J. Li, "A Highly Compatible Verification Framework with Minimal Upgrades to Secure An Existing Edge Network," *ACM Trans. Internet Technol.*, Mar. 2022, just Accepted. [Online]. Available: https://dl.acm.org/doi/10.1145/3511901

[62] A. Ometov, O. L. Molua, M. Komarov, and J. Nurmi, "A Survey of Security in Cloud, Edge, and Fog Computing," *Sensors*, vol. 22, no. 3, p. 927, Feb. 2022, number: 3 Place: Basel Publisher: Mdpi WOS:000757317400001. [Online]. Available: https://www.mdpi.com/1424-8220/22/3/927

[63] F. M. R. Junior and C. A. Kamienski, “A Survey on Trustworthiness for the Internet of Things,” *IEEE Access*, vol. 9, pp. 42 493–42 514, 2021, conference Name: IEEE Access.

[64] A. Nawaz, J. Pena Queralta, J. Guan, M. Awais, T. N. Gia, A. K. Bashir, H. Kan, and T. Westerlund, “Edge Computing to Secure IoT Data Ownership and Trade with the Ethereum Blockchain,” *Sensors*, vol. 20, no. 14, p. 3965, Jul. 2020, number: 14 Place: Basel Publisher: Mdpi WOS:000554692500001. [Online]. Available: https://www.mdpi.com/1424-8220/20/14/3965

[65] M. Pardeshi, R.-K. Sheu, and S.-M. Yuan, “Hash-Chain Fog/Edge: A Mode-Based Hash-Chain for Secured Mutual Authentication Protocol Using Zero-Knowledge Proofs in Fog/Edge,” *Sensors*, vol. 22, no. 2, 2022, number: 2. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85122884306&doi=10.3390%2fs22020607&partnerID=40&md5=6845ffec7c3fd73d521803e4ddc00aac

[66] T. Wang, P. Wang, S. Cai, X. Zheng, Y. Ma, W. Jia, and G. Wang, “Mobile edge-enabled trust evaluation for the Internet of Things,” *Inf. Fusion*, vol. 75, pp. 90–100, Nov. 2021, place: Amsterdam Publisher: Elsevier WOS:000671018300007. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S1566253521000737

[67] M. Eskandari, Z. H. Janjua, M. Vecchio, and F. Antonelli, “Passban IDS: An Intelligent Anomaly-Based Intrusion Detection System for IoT Edge Devices,” *IEEE Internet of Things Journal*, vol. 7, no. 8, pp. 6882–6897, Aug. 2020, number: 8 Conference Name: IEEE Internet of Things Journal.

[68] Y. Wang, H. Wang, S. Chen, and Y. Xia, “A Survey on Mainstream Dimensions of Edge Computing,” in *2021 the 5th International Conference on Information System and Data Mining*, ser. ICISDM 2021. New York, NY, USA: Association for Computing Machinery, Sep. 2021, pp. 46–54. [Online]. Available: https://dl.acm.org/doi/10.1145/3471287.3471295

[69] T. Wang, P. Wang, S. Cai, Y. Ma, A. Liu, and M. Xie, “A Unified Trustworthy Environment Establishment Based on Edge Computing in Industrial IoT,” *IEEE Transactions on Industrial Informatics*, vol. 16, no. 9, pp. 6083–6091, Sep. 2020, number: 9 Conference Name: IEEE Transactions on Industrial Informatics.

[70] M. Endler, A. Silva, and R. A. M. S. Cruz, “An approach for secure edge computing in the Internet of Things,” in *2017 1st Cyber Security in Networking Conference (CSNet)*, Oct. 2017, pp. 1–8.

[71] N. Moustafa, M. Keshk, K.-K. R. Choo, T. Lynar, S. Camtepe, and M. Whitty, “DAD: A Distributed Anomaly Detection system using ensemble one-class statistical learning in edge networks,” *Futur. Gener. Comp. Syst.*, vol. 118, pp. 240–251, May 2021, place: Amsterdam Publisher: Elsevier WOS:000620648600021. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0167739X21000212

[72] S. Xu, Y. Qian, and R. Q. Hu, “Edge Intelligence Assisted Gateway Defense in Cyber Security,” *IEEE Network*, vol. 34, no. 4, pp. 14–19, Jul. 2020, number: 4 Conference Name: IEEE Network.

[73] N. Sehrawat, S. Vashisht, and N. Kaur, "Edge-Computing Paradigm: Survey and Analysis on security Threads," in *2021 International Conference on Computing Sciences (ICCS)*, Dec. 2021, pp. 254–259.

[74] M. A. Ferrag, O. Friha, D. Hamouda, L. Maglaras, and H. Janicke, "Edge-IIoTset: A New Comprehensive Realistic Cyber Security Dataset of IoT and IIoT Applications for Centralized and Federated Learning," *IEEE Access*, vol. 10, pp. 40 281–40 306, 2022, conference Name: IEEE Access.

[75] N. A. Sulieman, L. Ricciardi Celsi, W. Li, A. Zomaya, and M. Villari, "Edge-Oriented Computing: A Survey on Research and Use Cases," *Energies*, vol. 15, no. 2, p. 452, Jan. 2022, number: 2 Place: Basel Publisher: Mdpi WOS:000758548800001. [Online]. Available: https://www.mdpi.com/1996-1073/15/2/452

[76] D. Hamouda, M. A. Ferrag, N. Benhamida, and H. Seridi, "Intrusion Detection Systems for Industrial Internet of Things: A Survey," in *2021 International Conference on Theoretical and Applicative Aspects of Computer Science (ICTAACS)*, Dec. 2021, pp. 1–8.

[77] M. G. S. Murshed, C. Murphy, D. Hou, N. Khan, G. Ananthanarayanan, and F. Hussain, "Machine Learning at the Network Edge: A Survey," *ACM Comput. Surv.*, vol. 54, no. 8, pp. 170:1–170:37, Oct. 2021, number: 8. [Online]. Available: https://dl.acm.org/doi/10.1145/3469029

[78] N. A. Angel, D. Ravindran, P. M. D. R. Vincent, K. Srinivasan, and Y.-C. Hu, "Recent Advances in Evolving Computing Paradigms: Cloud, Edge, and Fog Technologies," *Sensors*, vol. 22, no. 1, p. 196, Jan. 2022, number: 1 Place: Basel Publisher: Mdpi WOS:000757326100010. [Online]. Available: https://www.mdpi.com/1424-8220/22/1/196

[79] W. G. Hatcher, C. Qian, F. Liang, W. Liao, E. P. Blasch, and W. Yu, "Secure IoT Search Engine: Survey, Challenges Issues, Case Study, and Future Research Direction," *IEEE Internet of Things Journal*, vol. 9, no. 18, pp. 16 807–16 823, Sep. 2022, number: 18 Conference Name: IEEE Internet of Things Journal.

[80] D. He, S. Chan, and M. Guizani, "Security in the Internet of Things Supported by Mobile Edge Computing," *IEEE Communications Magazine*, vol. 56, no. 8, pp. 56–61, Aug. 2018, number: 8 Conference Name: IEEE Communications Magazine.

[81] F. Schwarz, "TrustedGateway: TEE-Assisted Routing and Firewall Enforcement Using ARM TrustZone," in *Proceedings of the 25th International Symposium on Research in Attacks, Intrusions and Defenses*, ser. RAID '22. New York, NY, USA: Association for Computing Machinery, Oct. 2022, pp. 56–71. [Online]. Available: https://dl.acm.org/doi/10.1145/3545948.3545961

[82] R. Xu, L. Hang, W. Jin, and D. Kim, "Distributed Secure Edge Computing Architecture Based on Blockchain for Real-Time Data Integrity in IoT Environments," *Actuators*, vol. 10, no. 8, p. 197, Aug. 2021, number: 8 Place: Basel Publisher: Mdpi WOS:000688637100001. [Online]. Available: https://www.mdpi.com/2076-0825/10/8/197

[83] S. Pundir, M. Wazid, D. P. Singh, A. K. Das, J. J. P. C. Rodrigues, and Y. Park, "Intrusion Detection Protocols in Wireless Sensor Networks Integrated to Internet of Things Deployment: Survey and Future Challenges," *IEEE Access*, vol. 8, pp. 3343–3363, 2020, conference Name: IEEE Access.

[84] H. Qi, J. Wang, W. Li, Y. Wang, and T. Qiu, "A Blockchain-Driven IIoT Traffic Classification Service for Edge Computing," *IEEE Internet of Things Journal*, vol. 8, no. 4, pp. 2124–2134, 15 Feb.15, 2021.

[85] P. Lv, Y. Wang, Y. Wang, C. Liu, Q. Zhou, and Z. Xu, "A highly reliable cross-domain identity authentication protocol based on blockchain in edge computing environment," in *2022 IEEE 25th International Conference on Computer Supported Cooperative Work in Design, CSCWD 2022*, 2022, pp. 1040–1046.

[86] Z. Wu, H. Huang, Y. Zhou, and C. Wu, "A secure and efficient data deduplication framework for the internet of things via edge computing and blockchain," *Connection Science*, vol. 34, no. 1, pp. 1999–2025, 2022.

[87] O. Ajayi, J. Rafferty, J. Santos, M. Garcia-Constantino, and Z. Cui, "BECA: A Blockchain-Based Edge Computing Architecture for Internet of Things Systems," *IoT*, vol. 2, no. 4, pp. 610–632, 2021.

[88] R. Casado-Vara, F. de la Prieta, J. Prieto, and J. M. Corchado, "Blockchain framework for IoT data quality via edge computing," in *Proceedings of the 1st Workshop on Blockchain-enabled Networked Sensor Systems*, ser. BlockSys'18. New York, NY, USA: Association for Computing Machinery, Nov. 2018, pp. 19–24.

[89] S. Bagchi, M.-B. Siddiqui, P. Wood, and H. Zhang, "Dependability in edge computing," *Communications of the ACM*, vol. 63, no. 1, pp. 58–66, Dec. 2019.

[90] J. Song, T. Gu, and P. Mohapatra, "How BlockChain Can Help Enhance the Security and Privacy in Edge Computing?" in *6th ACM/IEEE Symposium on Edge Computing, SEC 2021*, 2021, pp. 448–453.

[91] A. Alkhateeb, C. Catal, G. Kar, and A. Mishra, "Hybrid Blockchain Platforms for the Internet of Things (IoT): A Systematic Literature Review," *Sensors*, vol. 22, no. 4, 2022.

[92] X. Wang, X. Ren, C. Qiu, Z. Xiong, H. Yao, and V. Leung, "Integrating Edge Intelligence and Blockchain: What, Why, and How," *IEEE Communications Surveys and Tutorials*, vol. 24, no. 4, pp. 2193–2229, 2022.

[93] T. Fernández-Caramés and P. Fraga-Lamas, "Towards next generation teaching, learning, and context-aware applications for higher education: A review on blockchain, IoT, Fog and edge computing enabled smart campuses and universities," *Applied Sciences (Switzerland)*, vol. 9, no. 21, 2019.

[94] L. Fotia, F. Delicato, and G. Fortino, "Trust in Edge-based Internet of Things Architectures: State of the Art and Research Challenges," *ACM Computing Surveys*, vol. 55, no. 9, pp. 182:1–182:34, Jan. 2023.

[95] J. Hu, M. Reed, N. Thomos, M. F. AI-Naday, and K. Yang, "Securing SDN-Controlled IoT Networks Through Edge Blockchain," *IEEE Internet of Things Journal*, vol. 8, no. 4, pp. 2102–2115, 15 Feb.15, 2021.

[96] Z. Wang, J. Lu, M. Li, S. Yang, Y. Wang, and X. Cheng, "Edge Computing and Blockchain in Enterprise Performance and Venture Capital Management," *Computational Intelligence and Neuroscience*, vol. 2022, 2022.

[97] G. Li, M. Dong, L. Yang, K. Ota, J. Wu, and J. Li, "Preserving Edge Knowledge Sharing among IoT Services: A Blockchain-Based Approach," *IEEE Transactions on Emerging Topics in Computational Intelligence*, vol. 4, no. 5, pp. 653–665, 2020.

[98] H. Huang, W. Kong, S. Zhou, Z. Zheng, and S. Guo, "A Survey of State-of-the-Art on Blockchains: Theories, Modelings, and Tools," *ACM Computing Surveys*, vol. 54, no. 2, pp. 44:1–44:42, Mar. 2021.

[99] S. Taskou, M. Rasti, and P. Nardelli, "Blockchain Function Virtualization: A New Approach for Mobile Networks beyond 5G," *IEEE Network*, vol. 36, no. 6, pp. 134–141, 2022.

[100] B. Sellami, A. Hakiri, and S. Ben Yahia, "Deep Reinforcement Learning for energy-aware task offloading in join SDN-Blockchain 5G massive IoT edge network," *Future Generation Computer Systems*, vol. 137, pp. 363–379, 2022.

[101] R. Borgaonkar, I. Anne Tøndel, M. Zenebe Degefa, and M. Gilje Jaatun, "Improving smart grid security through 5G enabled IoT and edge computing," *Concurrency and Computation: Practice and Experience*, vol. 33, no. 18, 2021.

[102] N. Abbas, Y. Zhang, A. Taherkordi, and T. Skeie, "Mobile Edge Computing: A Survey," *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 450–465, 2018.

[103] P. Cruz, N. Achir, and A. C. Viana, "On the Edge of the Deployment: A Survey on Multi-access Edge Computing," *ACM Computing Surveys*, vol. 55, no. 5, pp. 99:1–99:34, Dec. 2022.

[104] A. Y. Ding and M. Janssen, "Opportunities for applications using 5G networks: Requirements, challenges, and outlook," in *Proceedings of the Seventh International Conference on Telecommunications and Remote Sensing*, ser. ICTRS '18. New York, NY, USA: Association for Computing Machinery, Oct. 2018, pp. 27–34.

[105] O. Devi, J. Webber, A. Mehbodniya, M. Chaitanya, P. Jawarkar, M. Soni, and S. Miah, "The Future Development Direction of Cloud-Associated Edge-Computing Security in the Era of 5G as Edge Intelligence," *Scientific Programming*, vol. 2022, 2022.

[106] R. Mishra, K. Joshi, and D. Gangodkar, "Wireless Communications Network and Mobile Computing using Blockchain in Distributed Internet of Things," in *Proceedings of the 2022 11th International Conference on System Modeling and Advancement in Research Trends, SMART 2022*, 2022, pp. 832–836.

A Data Item Extraction Table

Table 1.27: RQ1 - Primary article data items DEI1-6 (Part 1)

Article ID (Ref.)	**Year (DEI1)**	**Title (DEI2)**	**Author (DEI3)**	**Library (DEI4)**	**Publication Type (DEI5)**	**Quality Score (DI6)**
[55]	2017	A comprehensive study of security of internet-of-things	A. Mosenia, N.K. Jha	Scopus	Journal Article	3
[37]	2023	A Fog-Based Security Framework for Large-Scale Industrial Internet of Things Environments	H. Zhou et al.	IEEE Xplore	Journal Article	3.5
[38]	2022	A Game-Theoretical Approach for Mitigating Edge DDoS Attack	Q. He et al.	IEEE Xplore	Journal Article	2
[9]	2022	A Survey of Security Architectures for Edge Computing-Based IoT	E. Fazeldehkordi, T. Grønli	Web of Science	Journal Article	1.5
[39]	2021	A Survey on Security and Privacy Issues in Edge-Computing-Assisted Internet of Things	A. Alwarafy et al.	IEEE Xplore	Journal Article	2
[24]	2020	An empirical study on system level aspects of Internet of Things (IoT)	S. N. Swamy, S. R. Kota	Scopus	Journal Article	3
[49]	2018	CloudWoT - A Reference Model for Knowledge-based IoT Solutions	A. Shaaban et al.	ACM	Conference Paper	1.5
[50]	2018	Data Security and Privacy-Preserving in Edge Computing Paradigm: Survey and Open Issues	J. Zhang et al.	Scopus	Journal Article	2
[51]	2020	IoT privacy and security: Challenges and solutions	L. Tawalbeh et al.	Scopus	Journal Article	4

Table 1.28: RQ1 - Primary article data items DEI1-6 (Part 2)

Article ID (Ref.)	**Year (DEI1)**	**Title (DEI2)**	**Author (DEI3)**	**Library (DEI4)**	**Publication Type (DEI5)**	**Quality Score (DI6)**
[40]	2019	KingFisher: an Industrial Security Framework based on Variational Autoencoders	G. Bernieri, M. Conti, F. Turrin	ACM	Conference Paper	1.5
[56]	2022	MalRec: A Blockchain-based Malware Recovery Framework for Internet of Things	A. Lekssays et al.	ACM	Conference Paper	1.5
[57]	2020	Novel defense schemes for artificial intelligence deployed in edge computing environment	C. Zhou, Q. Liu, R. Zeng	Scopus	Journal Article	3.5
[52]	2020	Reconfigurable Network-on-Chip Security Architecture	S. Charles, P. Mishra	ACM	Journal Article	3.5
[53]	2020	Resilient Authentication and Authorization for the Internet of Things (IoT) Using Edge Computing	H. Kim et al.	ACM	Journal Article	4
[41]	2020	SDN-Assisted DDoS Defense Framework for the Internet of Multimedia Things	K. Sahoo, D. Puthal	ACM	Journal Article	3.5
[58]	2018	SDN-based Mitigation of Scanning Attacks for the 5G Internet of Radio Light System	K. Cabaj et al.	ACM	Conference Paper	1.5
[42]	2020	SDN/NFV security framework for fog-to-things computing infrastructure	P. Krishnan, S. Duttagupta, K. Achuthan	Scopus	Journal Article	1

Table 1.29: RQ1 - Primary article data items DEI1-6 (Part 3)

Article ID (Ref.)	Year (DEI1)	Title (DEI2)	Author (DEI3)	Library (DEI4)	Publication Type (DEI5)	Quality Score (DI6)
[43]	2019	SDNFV Based Threat Monitoring and Security Framework for Multi-Access Edge Computing Infrastructure	P. Krishnan, S. Duttagupta, K. Achuthan	Scopus	Journal Article	3
[44]	2019	SeArch: A Collaborative and Intelligent NIDS Architecture for SDN-Based Cloud IoT Networks	T. Nguyen et al.	IEEE Xplore	Journal Article	3.5
[54]	2022	Secure UAV-Aided Mobile Edge Computing for IoT: A Review	E.T. Michailidis et al.	Scopus	Journal Article	4
[45]	2020	Security of Distributed Intelligence in Edge Computing: Threats and Countermeasures	M.S. Ansari	Scopus	Journal Article Article	2
[46]	2022	Software-defined hardware-assisted isolation for trusted next-generation IoT systems	F. Kolimbianakis, G. Kornaros	ACM	Conference Paper	2
[47]	2021	State-of-the-art review on IoT threats and attacks: Taxonomy, challenges and solutions	R.R. Krishna	Scopus	Journal Article	3.5
[48]	2023	Zero-Touch Security Automation Mechanisms for Edge NFV: The Edge Approach	A. Valantasis, N. Psaromanolakis, V. Theodorou	ACM	Conference Paper	2

Table 1.30: RQ2 - Primary article data items DEI1-6 (Part 1)

Article ID (Ref.)	Year (DEI1)	Title (DEI2)	Author (DEI3)	Library (DEI4)	Publication Type (DEI5)	Quality Score (DI6)
[61]	2022	A Highly Compatible Verification Framework with Minimal Upgrades to Secure An Existing Edge Network	Z. Li et al.	ACM	Journal Article	2.5
[62]	2022	A Survey of Security in Cloud, Edge, and Fog Computing	A. Ometov et al.	Web of Science	Journal Article	2.5
[68]	2021	A Survey on Mainstream Dimensions of Edge Computing	Y. Wang et al.	ACM	Conference Paper	2
[16]	2018	A Survey on the Edge Computing for the Internet of Things	W. Yu et al.	IEEE Xplore	Journal Article	2.5
[63]	2021	A Survey on Trustworthiness for the Internet of Things	F. Junior, C. Kamienski	IEEE Xplore	Journal Article	2.5
[69]	2020	A Unified Trustworthy Environment Establishment Based on Edge Computing in Industrial IoT	T. Wang et al.	IEEE Xplore	Journal Article	1.5
[70]	2017	An approach for secure edge computing in the Internet of Things	M. Endler, A. Silva, R. Cruz	IEEE Xplore	Conference Paper	1.5
[71]	2021	DAD: A Distributed Anomaly Detection system using ensemble one-class statistical learning in edge networks	N. Moustafa et al.	Web of Science	Journal Article	3
[82]	2021	Distributed Secure Edge Computing Architecture Based on Blockchain for Real-Time Data Integrity in IoT Environments	R. Xu et al.	Web of Science	Journal Article	2

Table 1.31: RQ2 - Primary article data items DEI1-6 (Part 2)

Article ID (Ref.)	**Year (DEI1)**	**Title (DEI2)**	**Author (DEI3)**	**Library (DEI4)**	**Publication Type (DEI5)**	**Quality Score (DI6)**
[64]	2020	Edge Computing to Secure IoT Data Ownership and Trade with the Ethereum Blockchain	A. Nawas et al.	Web of Science	Journal Article	1.5
[72]	2020	Edge Intelligence Assisted Gateway Defense in Cyber Security	S. Xu, Y. Qian, R. Q. Hu	IEEE Xplore	Journal Article	2
[73]	2021	Edge-Computing Paradigm: Survey and Analysis on security Threads	N. Sehrawat, S. Vashisht, N. Kaur	IEEE Xplore	Conference Paper	1.5
[74]	2022	Edge-IIoTset: A New Comprehensive Realistic Cyber Security Dataset of IoT and IIoT Applications for Centralized and Federated Learning	M. Ferrag et al.	IEEE Xplore	Journal Article	3
[75]	2022	Edge-Oriented Computing: A Survey on Research and Use Cases	N. A. Sulieman et al.	Web of Science	Journal Article	4
[65]	2022	Hash-Chain Fog/Edge: A Mode-Based Hash-Chain for Secured Mutual Authentication Protocol Using Zero-Knowledge Proofs in Fog/Edge	M.S. Pardeshi, R.-K. Sheu, S.-M. Yuan	Scopus	Journal Article	3
[83]	2020	Intrusion Detection Protocols in Wireless Sensor Networks Integrated to Internet of Things Deployment: Survey and Future Challenges	S. Pundir et al.	IEEE Xplore	Journal Article	1
[76]	2021	Intrusion Detection Systems for Industrial Internet of Things: A Survey	D. Hamouda et al.	IEEE Xplore	Conference Paper	3

Table 1.32: RQ2 - Primary article data items DEI1-6 (Part 3)

Article ID (Ref.)	**Year (DEI1)**	**Title (DEI2)**	**Author (DEI3)**	**Library (DEI4)**	**Publication Type (DEI5)**	**Quality Score (DI6)**
[77]	2021	Machine Learning at the Network Edge: A Survey	M. G. S. Murshed et al.	ACM	Journal Article	1
[66]	2021	Mobile edge-enabled trust evaluation for the Internet of Things	T. Wang et al.	Web of Science	Journal Article	2
[67]	2020	Passban IDS: An Intelligent Anomaly-Based Intrusion Detection System for IoT Edge Devices	M. Eskandari et al.	IEEE Xplore	Journal Article	3
[78]	2022	Recent Advances in Evolving Computing Paradigms: Cloud, Edge, and Fog Technologies	N. A. Angel et al.	Web of Science	Journal Article	3
[79]	2022	Secure IoT Search Engine: Survey, Challenges Issues, Case Study, and Future Research Direction	W. Hatcher et al.	IEEE Xplore	Journal Article	3.5
[59]	2018	Security and privacy for IoT and fog computing paradigm	A. Rauf, R. A. Shaikh, A. Shah	IEEE Xplore	Conference Paper	1
[60]	2019	Security Implications of Fog Computing on the Internet of Things	I. Butun, A. Sari, P. Österberg	IEEE Xplore	Conference Paper	1.5
[80]	2018	Security in the Internet of Things Supported by Mobile Edge Computing	D. He, S. Chan, M. Guizani	IEEE Xplore	Journal Article	2.5
[81]	2020	TrustedGateway: TEE-Assisted Routing and Firewall Enforcement Using ARM TrustZone	F. Schwarz	ACM	Conference Paper	3

Table 1.33: RQ3 - Primary article data items DEI1-6 (Part 1)

Article ID (Ref.)	**Year (DEI1)**	**Title (DEI2)**	**Author (DEI3)**	**Library (DEI4)**	**Publication Type (DEI5)**	**Quality Score (DI6)**
[84]	2021	A Blockchain-Driven IIoT Traffic Classification Service for Edge Computing	H. Qi et al.	IEEE Xplore	Journal Article	1.5
[85]	2022	A highly reliable cross-domain identity authentication protocol based on blockchain in edge computing environment	P. Lv et al.	Scopus	Conference Paper	2
[28]	2018	A Review on the Use of Blockchain for the Internet of Things	T.M. Fernández-Caramés and P. Fraga-Lamas	Scopus	Journal Article	3.5
[86]	2022	A secure and efficient data deduplication framework for the internet of things via edge computing and blockchain	Z. Wu et al.	Scopus	Journal Article	4
[98]	2021	A Survey of State-of-the-Art on Blockchains: Theories, Modelings, and Tools	H. Huang et al.	ACM	Journal Article	2
[30]	2023	An Internet of Things Access Control Scheme Based on Permissioned Blockchain and Edge Computing	L. Zhang et al.	Scopus	Journal Article	2.5
[87]	2021	BECA: A Blockchain-Based Edge Computing Architecture for Internet of Things Systems	O.J. Ajayi et al.	Scopus	Journal Article	2

Table 1.34: RQ3 - Primary article data items DEI1-6 (Part 2)

Article ID (Ref.)	**Year (DEI1)**	**Title (DEI2)**	**Author (DEI3)**	**Library (DEI4)**	**Publication Type (DEI5)**	**Quality Score (DI6)**
[88]	2018	Blockchain framework for IoT data quality via edge computing	R. Casado-Vara et al.	ACM	Conference Paper	4
[99]	2022	Blockchain Function Virtualization: A New Approach for Mobile Networks beyond 5G	S.K. Taskou, M. Rasti, P.H.J. Nardelli	Scopus	Journal Article	3
[7]	2018	Cybersecurity Challenges and Opportunities in the New "Edge Computing + IoT" World	J. Pan, Z. Yang	ACM	Conference Paper	2
[100]	2022	Deep Reinforcement Learning for energy-aware task offloading in join SDN-Blockchain 5G massive IoT edge network	B. Sellami, A. Hakiri, S. Ben Yahia	Scopus	Journal Article	4
[89]	2019	Dependability in edge computing	S. Bagchi et al.	ACM	Journal Article	2.5
[33]	2019	Edge Cloud Offloading Algorithms: Issues, Methods, and Perspectives	J. Wang et al.	ACM	Journal Article	3.5
[96]	2022	Edge Computing and Blockchain in Enterprise Performance and Venture Capital Management	Z. Wang et al.	Scopus	Journal Article	3.5
[34]	2021	Highly efficient key agreement for remote patient monitoring in MEC-enabled 5G networks	A. Braeken, M. Liynage	Scopus	Journal Article	4
[90]	2021	How BlockChain Can Help Enhance the Security and Privacy in Edge Computing?	J. Song, T. Gu, P. Mohapatra	Scopus	Conference Paper	3.5

Table 1.35: RQ3 - Primary article data items DEI1-6 (Part 3)

Article ID (Ref.)	**Year (DEI1)**	**Title (DEI2)**	**Author (DEI3)**	**Library (DEI4)**	**Publication Type (DEI5)**	**Quality Score (DI6)**
[91]	2022	Hybrid Blockchain Platforms for the Internet of Things (IoT): A Systematic Literature Review	A. Alkhateeb et al.	Scopus	Journal Article	4
[101]	2021	Improving smart grid security through 5G enabled IoT and edge computing	R. Borgaonkar et al.	Scopus	Journal Article	3.5
[29]	2021	Integrated Blockchain and Cloud Computing Systems: A Systematic Survey, Solutions, and Challenges	J. Zou et al.	ACM	Journal Article	3.5
[92]	2022	Integrating Edge Intelligence and Blockchain: What, Why, and How	X. Wang et al.	Scopus	Journal Article	3.5
[35]	2020	Key Advances in Pervasive Edge Computing for Industrial Internet of Things in 5G and beyond	A. Narayanan et al.	Scopus	Journal Article	2.5
[102]	2018	Mobile Edge Computing: A Survey	N. Abbas et al.	Scopus	Journal Article	2
[103]	2022	On the Edge of the Deployment: A Survey on Multi-access Edge Computing	P. Cruz, N. Achir, A. C. Viana	ACM	Journal Article	2
[104]	2018	Opportunities for applications using 5G networks: requirements, challenges, and outlook	A. Y. Ding, M. Janssen	ACM	Conference Paper	3

Table 1.36: RQ3 - Primary article data items DEI1-6 (Part 4)

Article ID (Ref.)	**Year (DEI1)**	**Title (DEI2)**	**Author (DEI3)**	**Library (DEI4)**	**Publication Type (DEI5)**	**Quality Score (DI6)**
[97]	2020	Preserving Edge Knowledge Sharing among IoT Services: A Blockchain-Based Approach	G. Li et al.	Scopus	Journal Article	1.5
[27]	2019	Secure data storage based on blockchain and coding in edge computing	Y. Ren et al.	Scopus	Journal Article	1
[95]	2021	Securing SDN-Controlled IoT Networks Through Edge Blockchain	J. Hu et al.	IEEE Xplore	Journal Article	2
[105]	2022	The Future Development Direction of Cloud-Associated Edge-Computing Security in the Era of 5G as Edge Intelligence	O.R. Devi et al.	Scopus	Journal Article	3
[93]	2019	Towards next generation teaching, learning, and context-aware applications for higher education: A review on blockchain, IoT, Fog and edge computing enabled smart campuses and universities	T.M. Fernández-Caramés, P. Fraga-Lamas	Scopus	Journal Article	2.5
[94]	2023	Trust in Edge-based Internet of Things Architectures: State of the Art and Research Challenges	L. Fotia, F. Delicato, G. Fortino	ACM	Journal Article	1
[106]	2022	Wireless Communications Network and Mobile Computing using Blockchain in Distributed Internet of Things	R. Mishra, K. Joshi, D. Gangodkar	Scopus	Conference Paper	2