applied sciences

MDPI

Article

Combining Edge Computing-Assisted Internet of Things Security with Artificial Intelligence: Applications, Challenges, and Opportunities

Dulana Rupanetti [1,*] and Naima Kaabouch [1,2,*]

[1] School of Electrical Engineering & Computer Science, University of North Dakota, Grand Forks, ND 58202, USA

[2] Artificial Intelligence Research (AIR) Center, University of North Dakota, Grand Forks, ND 58202, USA

* Correspondence: dulana.rupanetti@und.edu (D.R.); naima.kaabouch@und.edu (N.K.)

Abstract: The integration of edge computing with IoT (EC-IoT) systems provides significant improvements in addressing security and privacy challenges in IoT networks. This paper examines the combination of EC-IoT and artificial intelligence (AI), highlighting practical strategies to improve data and network security. The published literature has suggested decentralized and reliable trust measurement mechanisms and security frameworks designed explicitly for IoT-enabled systems. Therefore, this paper reviews the latest attack models threatening EC-IoT systems and their impacts on IoT networks. It also examines AI-based methods to counter these security threats and evaluates their effectiveness in real-world scenarios. Finally, this survey aims to guide future research by stressing the need for scalable, adaptable, and robust security solutions to address evolving threats in EC-IoT environments, focusing on the integration of AI to enhance the privacy, security, and efficiency of IoT systems while tackling the challenges of scalability and resource limitations.

Keywords: edge computing; internet of things (IoT); artificial intelligence (AI); machine learning; deep learning; cybersecurity; trust measurement; data privacy

check for updates

Citation: Rupanetti, D.; Kaabouch, N. Combining Edge Computing-Assisted Internet of Things Security with Artificial Intelligence: Applications, Challenges, and Opportunities. *Appl. Sci.* **2024**, *14*, 7104. https://doi.org/10.3390/app14167104

Academic Editors: Carlos Enrique Palau Salvador and David Sarabia-Jacome

Received: 20 June 2024
Revised: 2 August 2024
Accepted: 8 August 2024
Published: 13 August 2024

1. Introduction

The internet of things (IoT) is a paradigm that refers to embedded computing devices interconnected within the existing internet infrastructure in a unique and identifiable way, enabling them to collect and exchange data without human intervention. This technology extends the internet's capabilities beyond traditional computing devices to a wide range of physical objects equipped with sensors and software, allowing them to communicate and interact with their environment. As the IoT evolves, it reshapes our interactions with the physical world through seamless connectivity and communication between objects, systems, and people. The vast potential for innovation and disruption across industries and sectors indicates a future where the digital and physical domains are intricately intertwined. Currently, the development of the IoT is rapidly advancing due to the integration of hardware and software, combining smart devices with sensing, processing, and communication capabilities [1]. This has led to a vast intelligent computing platform, connecting billions of devices to address real-world challenges [2].

Another rapidly growing sector in the IoT is its hardware capabilities. Proper hardware is essential for IoT systems, as initial design robustness is crucial for reliability. IoT chips are used in devices and facilitate network functionality, providing key features such as data sensing, wireless connectivity, data processing, energy efficiency, and security. IoT chips come in various types: processors, sensors, connectivity ICs, memory chips, and logic device chips. In AI-based IoT, essential chips include the system on chip (SoC), microcontroller units (MCUs), communication, and sensor chips. The SoC handles data processing, the MCU gathers data and executes commands, the communication chip manages data transmission, and the sensor chip detects external signals [3,4].

As an up-and-coming technology, the IoT can potentially revolutionize domains such as intelligent buildings, smart cities, healthcare, industries, and environmental monitoring [5]. The IoT has already been expanded to cover diverse applications, including smart grids, manufacturing processes, and product supply chains, demonstrating its integration into various aspects of society [6]. The future of IoT communication infrastructure is expected to sustain innovative applications in smart cities, smart grids, smart industries, and intelligent healthcare, emphasizing the potential of IoT technologies [7].

Figure 1 illustrates the current state of the IoT architecture. This IoT architecture integrates several critical components to effectively manage and utilize connected devices' data. At its core, "things"—objects equipped with sensors and actuators—collect and act on data. These objects can range from household appliances to industrial machinery, with sensors sometimes positioned remotely to monitor the surrounding environment. Data flows from these things to the cloud via gateways, which facilitate connectivity and preprocess and filter data to reduce the volume sent to the cloud while transmitting control commands from the cloud to the things. A cloud gateway further compresses these data and ensures secure transmission to IoT servers, adapting to different protocols as necessary. Within the cloud, a streaming data processor manages data transfer to a data lake and controls applications, ensuring there is no data loss or corruption. The data lake stores vast amounts of raw device data, which, when needed, are transferred to a big data warehouse, where they undergo further filtering and structuring for detailed analysis. Data analysts utilize this structured data to extract insights, identify trends, and improve system efficiency. Moreover, machine learning (ML) is employed to develop sophisticated models for control applications, which are regularly updated based on new data to enhance decision-making processes.

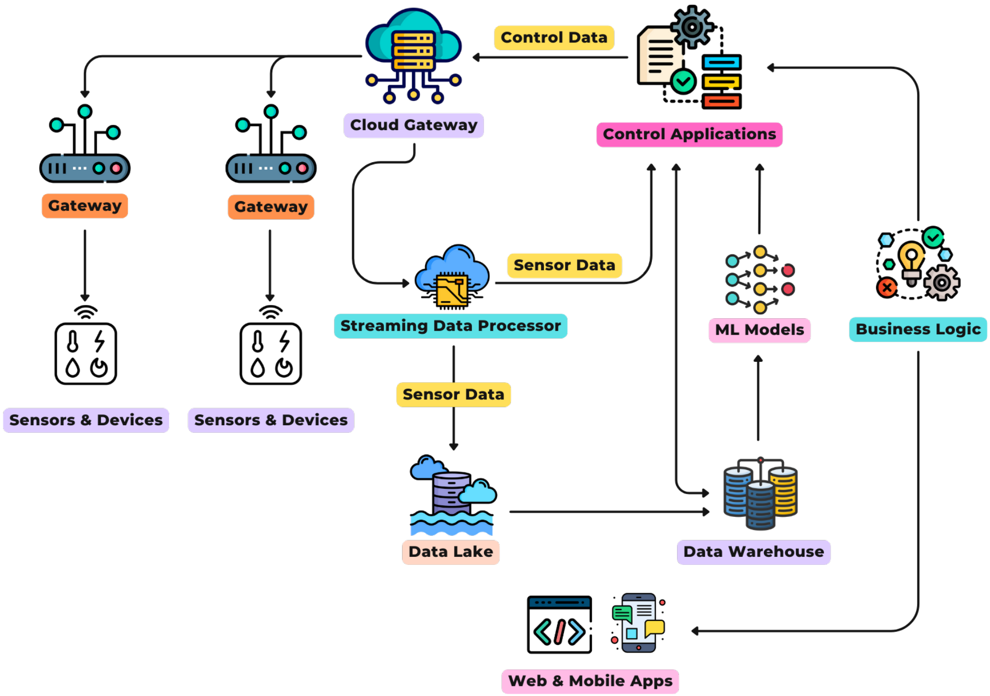

Figure 1. IoT architecture.

The IoT's ability to connect objects to the internet and enable autonomous decisions in smart environments highlights its significant impact [8]. This connectivity has introduced new paradigms, such as the internet of spatial things, focusing on everyday objects in the IoT era [9]. As the number of IoT devices continues to increase, they generate massive amounts of data, leading to concerns regarding data privacy and network costs in the current cloud-centric approach for extensive data analysis [10]. As the data transmission between cloud services and devices increase, service providers require the expansion of infrastructure, leading to system vulnerabilities for attacks.

EC-IoT has gained attention for enhancing IoT services by leveraging edge computing capabilities to help mitigate the growing data generation of these IoT networks. Edge computing processes data closer to end users, improving response times, reducing latency, and offloading computational tasks to edge nodes near IoT devices [11]. This integration has led to innovative strategies such as edge intelligence-aided IoT networks, which accelerate IoT services by deploying edge intelligence near IoT devices [12–15].

A key advantage of EC-IoT is providing location-aware services and optimizing resource allocation by offloading tasks from resource-limited IoT devices to powerful edge servers [16]. Edge computing also facilitates collaborative computing using a range of heterogeneous smart devices, enhancing overall IoT network efficiency [17]. This integration enables smart IoT devices at the edge of wireless networks to perform collaborative ML tasks using locally collected data, leading to the edge learning paradigm [18,19].

EC-IoT systems are designed to address security and privacy challenges in IoT networks. Researchers have proposed decentralized and reliable trust measurement mechanisms for EC-IoT to enhance data and network security [20]. Security frameworks have been developed to ensure secure communication and data processing in IoT-enabled healthcare systems [21,22].

Additionally, various approaches have been explored to improve EC-IoT services. These include IoT service slicing and task offloading for edge computing [23], IoT ecosystem modeling for design quality metrics [24], autonomic blockchain-based services for IoT device integration and payment [22], and service discovery approaches for IoT [25]. Further research into accountable anonymous access architectures for IoT networks [26], elastic IoT fog frameworks for AI services [27], and multi-perspective trust management frameworks for crowdsourced IoT services [27] could provide valuable insights into enhancing IoT services.

In this survey, we aim to provide a review of recent techniques related to the security of EC-IoT systems, specifically focusing on AI-based approaches. Due to growing concerns about the power and infrastructure needed to host large AI models on centralized servers, leading AI companies are moving towards smaller models that can run on microcontrollers or SoC-based systems. These systems can be placed closer to data-generating devices like IoT devices, making edge computing a strong candidate for such deployments. Therefore, it is imperative to begin researching improved security infrastructure for these EC-IoT systems to stay ahead of potential threats. This article aims to provide a detailed explanation of the current security concerns of EC-IoT and the countermeasures proposed in the literature.

In summary, this paper has the following contributions:

- Classification of current threats to EC-IoT systems.
- Analysis of the current countermeasures.
- Analysis of the AI-based countermeasures.
- Challenges in incorporating AI in protecting EC-IoT systems.

The survey is organized as follows. Section 2 discusses the related work on EC-IoT security. Section 3 explores edge computing and related paradigms. Section 4 explores the integration of edge computing with IoT, highlighting its advantages and applications. Section 5 categorizes and analyzes various attacks on edge-based IoT systems. Section 6 investigates AI-based countermeasures for these attacks, discussing different ML and deep learning (DL) techniques. Section 7 addresses the open challenges and future research opportunities in enhancing EC-IoT security. Finally, Section 8 presents the conclusions.

2. Related Work

While the research and development of edge and IoT system security is primarily in its early stages, numerous researchers have reviewed existing IoT security countermeasures in recent years to provide a roadmap for future work. Due to the diverse nature of IoT network hardware, intruders may create dynamic threats to take control of authorized communications or hardware devices. This section briefly examines the current state-of-the-art papers on IoT and edge security, highlighting recent attacks, threats, and countermeasures. A quick summary of these analyzed articles can be found in Table 1, including their focus, issues discussed, countermeasures described, and the future challenges provided.

The authors of [28] explored several critical issues related to IoT security within edge computing, such as resource constraints, insufficient security, high latency in cloud computing, and the complexity and heterogeneity of IoT devices. They underscored the importance of securing the edge layer, developing robust security solutions for edge devices, and ensuring secure communication between network components. The authors also emphasized the need for lightweight protocols and secure operating systems tailored for resource-constrained IoT devices.

A comprehensive survey on IoT security by the authors of [29] identified critical threats like privacy issues, authentication challenges, and information storage vulnerabilities. They categorized various physical, network, middleware, and gateway attacks. To address these challenges, the authors proposed scalable and adaptable security solutions leveraging technologies like blockchain, fog computing, and ML to enhance security and privacy while addressing scalability and resource constraints.

Focusing on secure healthcare data aggregation and transmission in IoT environments, the authors of [30] identified significant security and privacy concerns, such as data aggregation risks, transmission security, and data integrity issues. They suggested countermeasures, including data encryption, privacy preservation mechanisms, and robust authentication protocols. The potential of edge and fog computing to reduce latency and improve data processing efficiency was also highlighted, which is crucial for securely handling large volumes of healthcare data.

The application of ML and DL methods for IoT security was explored by the authors of [31], addressing the complexity and vulnerability of IoT systems. They discussed various attack surfaces and security threats, such as eavesdropping, DDoS attacks, and data tampering. The authors proposed leveraging supervised, unsupervised, and reinforcement learning techniques for anomaly detection and predictive analytics. Emphasizing the importance of scalable and adaptable ML/DL models, they aimed to handle the dynamic nature of IoT environments and ensure data privacy and security during processing.

The works reviewed in [32] integrated LoRa technology with edge computing to tackle IoT challenges. They highlighted the limitations of cloud-based computing, the need for low-power, long-range communication, and scalability issues. The proposed edge computing architecture aims to reduce latency by processing data locally. The discussion also included application-specific enhancements in smart cities, industrial IoT, and smart agriculture, stressing regulatory compliance and implementing security measures like AES-128 encryption as essential for ensuring data integrity and confidentiality.

Addressing secure data analytics in edge computing, the authors of [33] focused on the trade-offs between security and efficiency. They examined the trustworthiness of networked devices, usage privacy, and correctness of data computation as significant challenges. Proposing lightweight security mechanisms, effective trust management models, and privacy-preserving techniques, the authors aimed to ensure secure data analytics. They also emphasized the need for scalable security frameworks and the integration of ML to enhance security measures in edge computing environments.

The research conducted in [11] analyzed security and privacy issues in edge computing-assisted IoT. Highlighting new attack surfaces introduced by the distributed nature of edge computing, they noted vulnerabilities due to limited computational resources and data proximity to end-users. The authors suggested solutions, including scalable and lightweight security mechanisms, dynamic trust management systems, and standardization protocols to enhance security and privacy in EC-assisted IoT systems.

Exploring the potential of reinforcement learning (RL) for IoT security, the authors of [34] discussed various IoT security challenges, including diverse attack vectors and resource constraints. They highlighted RL's ability to adapt parameters and dynamically solve optimization problems with minimal information. They proposed RL-based security solutions that scale to handle many IoT devices and massive data volumes while addressing real-time adaptation and data privacy concerns.

The authors of [35] surveyed AI methods for securing IoT services in edge computing. Identifying the vulnerabilities of edge nodes, including their distributed layout, limited computational resources, and heterogeneous environments, they proposed integrating AI with blockchain to enhance IoT security. This integration addresses the high computation and communication costs and evolving threat adaptation, and it ensures efficient AI-based security schemes.

Examining DL-based security behavior in IoT environments, in ref. [36], the authors focused on security and privacy concerns due to limited resources and the ad hoc nature of IoT systems. They discussed the complexity of IoT systems and the need for advanced security methods. The authors proposed developing resource-efficient and adaptable DL models, handling heterogeneous data, and implementing lifelong learning to adapt to new security threats continuously.

The authors of [37] reviewed IoT security threats and applications, categorizing physical, software, network, and encryption attacks. They highlighted challenges like battery consumption, limited memory, and open-range operations. The authors suggested integrating fog computing, ML, edge computing, and blockchain technologies to enhance IoT security, emphasizing scalability, resource constraints, interoperability, and real-time adaptation.

Conducting a comprehensive survey on cybersecurity in IoT-based cloud computing, in ref. [38], the authors identified vital security concerns such as data breaches, data loss, unauthorized access, network vulnerabilities, and insider threats. They proposed countermeasures, including robust data encryption, multi-factor authentication, intrusion detection systems, and user education programs.

The research in ref. [39] surveyed security vulnerability analysis, discovery, detection, and mitigation in IoT devices. The authors discussed the IoT architecture, potential attack surfaces, and methodologies for identifying and detecting vulnerabilities. Mitigation strategies, such as side-channel signal analysis, policy-based mechanisms, secure firmware updates, and robust encryption methods, were reviewed.

Providing an extensive survey on security architectures for edge computing-based IoT systems, Fazeldehkordi and Gronli [19] addressed issues related to resource management, security and privacy, and advanced communication technologies such as 5G. They proposed future research directions focused on balancing security and efficiency, creating effective trust models, ensuring usage privacy, supporting mobility and scalability, designing lightweight security mechanisms, and ensuring verifiable computation.

The authors of [40] examined edge-computing architectures for IoT applications, emphasizing the importance of addressing the latency and bandwidth issues inherent in cloud-centric models. They discussed security and privacy concerns, scalability, interoperability, and data management challenges. The proposed solutions included lightweight encryption techniques, trust management frameworks, anomaly detection systems, edge analytics, and decentralized data storage.

In [41], the authors explored process automation in an IoT–Fog–Cloud ecosystem, highlighting challenges related to the high latency in cloud computing, big data management, real-time processing, and heterogeneity of devices. Their proposed solutions included enhancing fog layer resiliency, efficient big data processing, addressing heterogeneity, ensuring scalability, and improving interoperability. The authors emphasized the importance of automating functions within the ecosystem to enhance efficiency, reduce latency, and manage complex environments.

The authors of [42] surveyed cyberthreats and countermeasures in industrial IoT (IIoT) systems. They discussed vulnerabilities due to the complex integration of hardware and software and various types of cyberthreats such as phishing, ransomware, protocol attacks, supply chain attacks, and systems attacks. The paper suggested countermeasures, including phishing detection tools, next-generation firewalls, ML techniques, secure communication protocols, and blockchain-based solutions.

The authors of [43] identified the high data generation, limited computational power, and substantial energy demands of IoT devices as significant issues in examining the challenges and strategies for enhancing energy efficiency in IoT environments. The energy-intensive operations of edge, fog, and cloud computing exacerbate these challenges. To address these, they proposed energy-aware architectures—cluster-based, centralized, and distributed—and techniques like data compression, the use of low-power hardware, energy-aware scheduling, task offloading, and energy harvesting. The study further discussed future challenges such as scalability, adaptability, integration of renewable energy, and maintaining security and privacy without compromising cost and practical implementation.

Exploring the evolving security demands of systems of internet of things devices (SIoTD), the authors of [44] proposed adaptive, edge-based solutions to tackle these challenges. They identified complex security requirements, diverse and sophisticated cyberthreats, intermittent connectivity, significant data privacy concerns, latency issues, and the impracticality of centralized security measures as core challenges. To effectively address these issues, the authors advocated for shifting security processes closer to the data sources through edge-based processing, which reduces latency and enhances data privacy.

Discussing the critical need for robust security mechanisms and forensic capabilities within the expansive networks of the IoT, the authors of [45] identified significant challenges in protecting the decentralized and distributed entities such as devices, the data these devices generate, and the digital evidence arising from data interactions, which are often inadequately secured by traditional centralized security frameworks. The paper also explored the role of mobile edge computing (MEC) in bringing computing resources closer to IoT devices to minimize latency and enhance communication while highlighting the security vulnerabilities inherent in the decentralized MEC-enabled IoT systems, including physical access to devices and data tampering.

The surveys analyzed in our paper emphasize various AI approaches for detecting or countering cyberattacks in IoT environments. However, these studies often underscore persistent challenges related to scalability, resource constraints, and the dynamic nature of IoT systems. Our paper focuses on the specific paradigm of edge computing-assisted IoT (EC-IoT) incorporated with AI, highlighting its potential to enhance security measures in these environments. The key contributions of our review include the following:

- Exploring the emerging paradigm of EC-IoT: We explore how EC-IoT integrates AI to improve the efficiency and responsiveness of IoT systems.
- Discussing current threats and their effects on EC-IoT: We analyze the specific security challenges posed by integrating edge computing with IoT and the implications of these threats.
- Analyzing countermeasures in the current literature: We review existing solutions, particularly AI-based techniques, that address the security issues within EC-IoT frameworks.
- Proposing future directions to improve countermeasures for these threats: We suggest research avenues focused on developing scalable, efficient, and robust security solutions that can adapt to the evolving landscape of IoT threats and vulnerabilities.

Table 1. Related work on edge computing-assisted IoT security.

Article	Main Focus	Issues Discussed	Countermeasures/Solutions	Future Challenges
[43]	Energy efficiency	Network congestion, power limits	Energy-aware techniques	Scalability, renewable integration, ML enhancement
[44]	IoT security	Connectivity, privacy, latency	Edge processing, ML models	Hyperparameter tuning, complex topologies
[45]	Blockchain forensics	IoT security, MEC, blockchain	Blockchain integration	Scalability, delay optimization, mobility
[46]	Resource-limited IoT	Security vulnerabilities	IoT proxy, VPN, IPS	Anomaly detection, live traffic analysis
[42]	IIoT security	Cyberthreats	Phishing, ransomware, protocol attack countermeasures	Unconventional attack methods
[41]	IoT–fog–cloud	High latency, big data	Fog computing	Fog resiliency, big data management
[36]	Security analysis	IoT security, privacy	Deep learning	Efficiency, adaptability, heterogeneity
[39]	Vulnerability analysis	Attack surfaces	Firmware updates, secure boot	Device heterogeneity, lightweight security
[35]	AI for security	Edge node vulnerability	AI integration, blockchain	Computation costs, evolving threats
[34]	RL for IoT	Security challenges, RL	RL-based solutions	Scalability, resource constraints
[28]	Edge security	Resource constraints, edge vulnerability	Edge security architectures	Securing edge layer, data quality
[32]	LoRa edge integration	Cloud limits, low-power, long-range	Edge integration, regulatory compliance	Scalability, data privacy, standardization
[33]	Secure analytics	Security trade-offs, trust, privacy	Lightweight security, trust management	Advanced trust models, scalable frameworks
[29]	IoT security	IoT threats, attack types	Blockchain, fog computing, ML, edge computing	Scalability, resource constraints
[40]	Edge architectures	IoT edge architecture, challenges	Security, data management, scalability	Resource constraints, evolving threats
[31]	ML/DL methods	Complexity, vulnerability, attack surfaces	ML/DL techniques, anomaly detection	Scalability, data privacy, standardization
[38]	Cybersecurity	Data, network, service security	Data encryption, IDPS, secure software	Scalability, privacy concerns
[37]	IoT security	IoT threats, attack types	Fog computing, ML, edge, blockchain	Scalability, real-time adaptation
[30]	Secure aggregation	Security, privacy in healthcare IoT	Data encryption, secure aggregation	Device heterogeneity, dynamic trust
[11]	Edge security	Security, privacy risks, attacks	Secure updates, IDS, lightweight cryptography	Scalability, dynamic trust management
[19]	Security architectures	Resource management, privacy	Packet filters, firewalls, IDS	Balancing security, trust management

3. Edge Computing and Related Paradigms

This section examines the current technologies associated with edge computing and its related paradigms. We will also investigate how these technologies impact the IoT networks that edge computing capabilities assist. This discussion aims to clearly understand the technological landscape, including the advances and challenges faced in integrating edge computing with IoT systems.

3.1. Edge Computing

Edge computing is a computing paradigm that involves deploying computing resources at the edge of the network, closer to where the data are generated, processed, and consumed. This technique aims to reduce latency, ease traffic on the network, and meet the computational requirements of applications that demand low latencies [47]. It is considered an open platform that extends cloud computing capabilities by providing services close to users through IT infrastructure at the network edge [48]. Edge computing architecture involves placing tiny data centers at the network edge to enhance and extend cloud computing capabilities [49].

Edge computing utilizes advanced technologies such as deep learning to improve its applications. Researchers are increasingly exploring the intersection of deep learning and edge computing, as evidenced by existing surveys [50]. Moreover, edge computing is closely linked to other concepts such as fog computing, mobile edge computing (MEC), and mobile cloud computing (MCC), each with its own unique architectural features and areas of focus [29,51]. Security and privacy protection are crucial aspects of edge computing. Ensuring the security and privacy of computation and data management at the edge and in the cloud is a critical requirement [52]. Researchers have highlighted the importance of addressing security issues in supporting technologies for edge computing, including challenges and opportunities related to security and convergence with blockchain technologies [53].

3.2. Cloud Computing

Cloud computing has gained significant traction in recent years. It provides users with access to a shared pool of configurable computing resources over the internet, enabling ubiquitous, convenient, and on-demand network access to a wide range of services [54]. This model integrates various computing, storage, and software resources through distributed, utility, and parallel computing. Cloud computing has become widely adopted in academia and industry due to its ability to reduce computing and storage costs for users while enhancing ease of use.

One of the key features of cloud computing is its ability to provide remote computing resources to consumers and businesses, allowing them to leverage powerful computational capabilities without the need for extensive local infrastructure [55]. Cloud computing architectures typically involve centralized data centers that host and manage these resources, offering users scalability, flexibility, and cost-effectiveness [56]. By distributing cloud services over the internet, cloud computing enables users to access applications, store data, and perform computational tasks without being tied to specific physical locations.

Cloud computing has also paved the way for innovations in various domains, such as mobile edge computing, where cloud resources are extended to the edge of the network to provide services closer to mobile devices [57]. Additionally, cloud computing has been instrumental in developing collaborative computing systems that leverage local computing, edge cloud, and central cloud resources to optimize task offloading and resource allocation [58].

3.3. Fog Computing

Fog computing has emerged as a solution to address the challenges posed by traditional cloud computing models. It involves extending computing resources closer to the edge of the network, thereby reducing latency and improving efficiency [59]. This approach enables offloading storage, networking, and processing tasks to the edge, catering to the intensive computational demands and stringent latency requirements of modern applications [59]. By bringing computational servers closer to users, fog computing aims to minimize latency and enhance the quality of service for delay-sensitive applications [60]. Moreover, fog computing is instrumental in improving the accessibility of IoT resources by extending the data management capabilities of the cloud [61].

Like with any network-based paradigm, the security and privacy challenges associated with fog computing cannot be overlooked. As fog computing involves sharing data with the cloud for decision-making, there is an increased vulnerability regarding sensitive data sharing, necessitating robust security measures [62]. Researchers have highlighted the importance of addressing security and privacy concerns in fog computing to ensure the integrity and confidentiality of data [63]. Integrating fog computing with technologies like blockchain has been explored to enhance security and privacy-preserving mechanisms in fog-to-things environments [64]. Additionally, fog computing has been identified as a key technology in healthcare data aggregation and transmission in IoT, emphasizing the critical need for secure and efficient data handling in sensitive domains [30].

3.4. Mist Computing

Mist computing leverages the computing and storage capabilities of nodes, hubs, and gateways in the intermediate layers between Fog/Cloud and Edge. It is often implemented to optimize resources at the extreme edge, where static and mobile IoT devices act as thin servers and clients in fully distributed architectures [65]. Mist computing is often considered a subset of fog computing, operating on resource-constrained equipment like single-board computers. The concept of mist computing fills the need for specialized and dedicated nodes closer to end-users, especially with the adoption of fog computing, which emphasizes geographically dispersed, low-latency computational resources [53].

In practical applications, mist computing finds relevance in various domains. For instance, mist computing frameworks have been proposed to remotely monitor healthcare conditions like Parkinson’s disease [66]. Mist computing architectures have also been integrated into energy-efficient and high-security frameworks for IoT-enabled innovative environments [67]. Additionally, mist computing plays a role in improving the performance of cloud computing, as it brings resources closer to end-users, thereby enhancing overall system efficiency.

3.5. Cloudlet Computing

Cloudlet computing is a critical innovation within the edge computing spectrum. This concept revolves around deploying high-performance computing resources close to end-users, offering enhanced computational and storage services [68]. Imagined as miniature yet potent clusters, cloudlets are equipped with specialized computation and storage facilities. Strategically placed near user-centric locales like commercial buildings and shopping malls, they are engineered to support myriad functions such as data processing, computational offloading, and content caching [69]. These entities act as trusted and resource-dense nodes, optimally situated at the network’s edge to ensure seamless internet connectivity [70].

The essence of cloudlet computing lies in its ability to transcend the inherent limitations associated with traditional cloud computing frameworks, particularly the challenge of their high latency, which becomes acute in internet of things (IoT) applications [71]. Cloudlets are pivotal in empowering mobile devices, which often suffer from resource limitations, enabling them to offload heavy computational loads. This capability is indispensable for applications that demand prompt data processing [59]. Despite their ability to meet the burgeoning demand for computational resources, spurred by the exponential increase in connected devices, cloudlets must also navigate the potential for overburdening due to this rising demand [72].

3.6. Multi-Access Edge Computing (MEC)

Multi-access edge computing (MEC) is another paradigm that extends cloud computing capabilities to the edge of the network. The concept of MEC was introduced by the European Telecommunications Standards Institute (ETSI) Mobile Edge Computing Industry Specification Group (MEC iSG) to encompass the benefits of various access technologies such as 4G, 5G, Wi-Fi, and fixed access [73].

MEC is vital in optimizing mobile resources by hosting computationally intensive applications, processing extensive data locally before transmitting it to the cloud, and offering cloud computing capabilities within the radio access network (RAN) close to users citesanti2021. By leveraging computing, communication, and caching (3C) resources at the network edge, MEC is positioned as a critical enabler for next-generation networks. This architecture reduces latency, saves energy, and enhances the network's bandwidth efficiency [74].

MEC also enables the deployment of context-aware services and supports intelligent computation offloading, which is essential for handling the computational tasks of mobile devices by offloading them to MEC servers [75,76]. Integrating MEC with emerging technologies like 5G and the internet of things further enhances its capabilities, making it a critical component for applications such as mobile augmented reality (MAR) [77]. Additionally, MEC facilitates the implementation of AI-driven systems with UAV assistance in dynamic environments, addressing challenges through efficient resource utilization at the network edge [78].

4. Edge Computing-Based IoT

EC-IoT involves using edge computing paradigms such as fog computing, multi-access edge computing, and cloudlet to manage security-critical and time-sensitive data generated by IoT devices [19]. This strategy consists of deploying computing resources in close proximity to IoT devices for tasks such as data filtering, preprocessing, and aggregation.

The process is mainly conducted by designing the IoT layer sitting at the bottom of the architecture, while the resource providers are at the network edge. Edge computing optimizes IoT data processing [79]. In this architecture, IoT devices collect data from their environment, which is then processed locally on edge devices instead of being sent directly to distant cloud servers. This local processing capability allows for real-time data analysis and decision-making, which is critical in applications requiring immediate action such as autonomous driving, real-time health monitoring, and smart city infrastructure [80].

Similarly, edge computing-based IoT offers enhanced security features by limiting the amount of sensitive data transmitted over the network, thus reducing exposure to potential cyberthreats. It also supports more scalable deployments by distributing processing tasks across numerous edge devices, alleviating the load on central servers and reducing network congestion. One example would be facilitating vehicles' quick and accurate localization through IoT sensors and radar systems [81]. EC-IoT has a wide range of applications. While hidden in plain sight, these applications exist in extensive healthcare and urban applications, ensuring timely and accurate data processing [82] of these applications. In urban planning, the optimization of ecological landscape structures through EC-IoT has positively impacted biodiversity indices, highlighting the effectiveness of edge computing in diverse applications [83].

Figure 2 depicts the high-level three-layer architecture of the EC-IoT paradigm. The basic composition is the same as the conventional edge computing structure, with IoT devices being a part of the end-user subset of the edge computing layer. On the other hand, the edge computing layer does not exist for the standard IoT architecture. The things layer forms the foundation and comprises physical devices and sensors that collect environmental data. These can range from simple embedded systems to advanced industrial machinery, generating crucial operational data. Directly above this, the edge layer includes edge nodes and gateways that perform preliminary data processing tasks such as filtering, aggregation, and local analysis. This layer plays a pivotal role in reducing latency by handling data close to their origin, thus enabling quick local responses and minimizing the volume of data transmitted upwards. At the top, the cloud layer handles more complex processing tasks and storage needs that are less time-sensitive but require substantial computational resources. It manages advanced analytics, machine learning operations, and extensive data storage, providing centralized control over applications distributed across numerous edge devices. This structured approach ensures that each layer optimizes the processing and utility of the data in EC-IoT systems, enhancing overall efficiency and scalability.

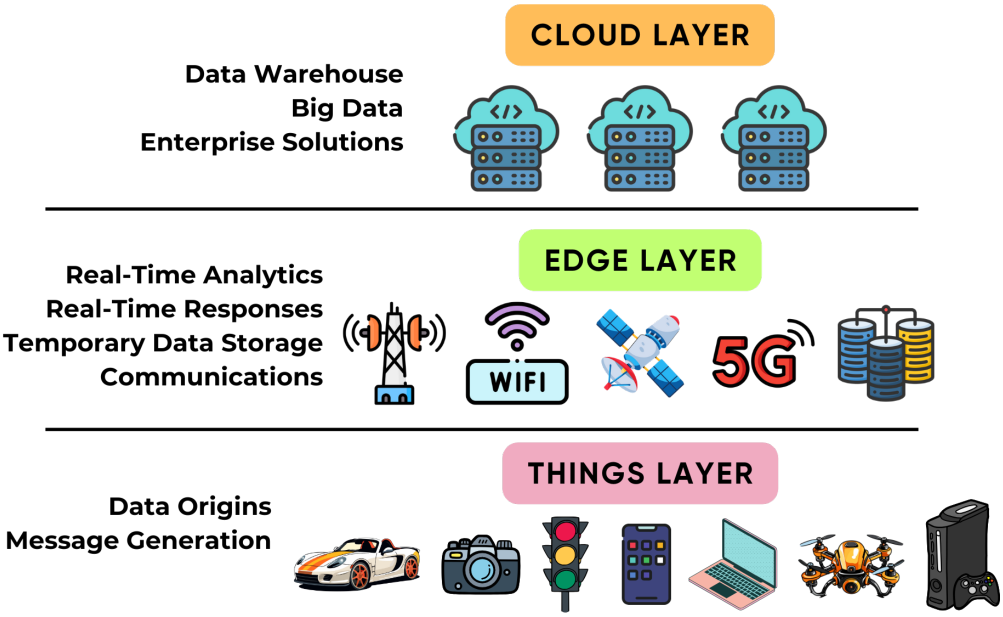

Figure 2. High-level depiction of edge computing combined with IoT.

4.1. Advantages of EC-IoT

AI-based security countermeasures enhance the protection of both EC-IoT and non-EC-based IoT systems, but their impacts vary significantly due to data processing and architecture differences. In EC-IoT systems, AI-driven security solutions operate at the edge, enabling real-time threat detection and response. This proximity to data generation points ensures the swift identification and elimination of potential attacks, reducing the window of vulnerability. Localized AI models also enhance data privacy by eliminating the need to move sensitive information to centralized servers, thereby lowering the risk of interception and unauthorized access. Conversely, AI-based security measures primarily function within centralized cloud environments in non-EC-based IoT systems. While this allows for deploying more sophisticated and resource-intensive AI models, it introduces higher threat detection and response latencies due to the time required to transmit data to and from the cloud. This centralized approach can also create a single point of failure, where a successful attack on the cloud infrastructure can compromise the entire IoT network. Given these differences, EC-IoT systems offer several advantages. The following are the main advantages that make EC-IoT stand out.

Reduced latency and improved bandwidth utilization: Edge computing processes data locally at the edge of the network, close to where they are generated. This proximity significantly cuts down the latency involved in sending data to a central server for processing. A primary advantage of this approach is the capability to perform tasks with a reduced latency, lower energy consumption, and more efficient use of network bandwidth [84]. This reduces the bandwidth requirements and alleviates congestion in network traffic, which is particularly important with the increasing number of IoT devices generating vast amounts of data [84].

Increased reliability and scalability: Edge computing enables devices to operate independently of the cloud, which increases the system's reliability. In scenarios where connectivity to a central server might be compromised or unavailable, edge devices can continue to function effectively, making decisions based on real-time data. Deploying edge computing devices across different locations is scalable, as it distributes the processing load. It allows for incremental additions without the need for significant infrastructure overhauls, which is ideal for scaling up IoT applications [13].

Context-aware computing and real-time data processing: Edge computing facilitates real-time data processing by eliminating the delays associated with transmitting data to remote servers, which is vital for applications that depend on instant data analysis and action. It enables edge devices to make decisions locally based on real-time environmental data, resulting in more context-sensitive and responsive computing solutions. This capability is particularly advantageous for sectors like smart city infrastructure and healthcare monitoring systems, where timely and relevant data are crucial [85,86].

4.2. AI in the Realm of EC-IoT

With current advancements in AI and the hardware that supports AI applications, EC-IoT has seen new technologies and concepts that improve and expand the current capabilities. A few of the major concepts that have been introduced with AI into EC-IoT systems are listed below:

Edge Intelligence (EI): EI represents a significant advancement in EC-IoT systems, where AI computations are performed locally on edge devices. This reduces the dependency on centralized cloud servers, thereby minimizing latency and bandwidth usage while enhancing real-time processing capabilities [42,87]. By enabling local AI processing, EI allows IoT devices to handle complex tasks independently, making systems more responsive and efficient [88].

Real-time data processing: Real-time data processing is a core benefit of integrating AI into EC-IoT systems. By processing data at the network edge, latency is significantly reduced, which is crucial for applications requiring immediate responses such as autonomous vehicles and industrial automation [42,89]. This decentralized approach also distributes AI tasks across edge devices, improving system robustness and scalability by avoiding single points of failure [87].

Enhanced security and privacy: Keeping data at the edge enhances security and privacy by reducing the risk of data breaches during transmission to central servers [42,87]. AI-based anomaly detection systems at the edge can monitor and detect unusual patterns or behaviors, providing early warnings for potential security threats, thus bolstering overall system security [89].

Advanced, scalable, and flexible AI architectures: AI on the edge supports advanced applications like real-time image and video processing, which are essential for smart surveillance, augmented reality, and natural language processing, enhancing real-time voice recognition and user interaction with IoT devices [89]. Integrating AI into EC-IoT systems introduces automation and intelligence, significantly enhancing the quality of service (QoS) and user experience [42]. This synergy enables smart and automated systems to deliver superior performance and reliability. Furthermore, federated learning in EC-IoT systems allows AI models to be trained across multiple edge devices without transferring data to a central server. This approach not only enhances data privacy and reduces transmission costs but also fosters secure and efficient AI deployment in IoT environments [88]. These advancements collectively drive the evolution of EC-IoT systems, making them more responsive, efficient, and secure.

5. Attacks on Edge-Based IoT

EC-IoT systems face a wide range of attack types, as depicted in Figure 3. While the current advancements in AI technology have significantly improved cybersecurity, they are particularly effective against specific categories of attacks. This paper focuses on analyzing AI-based solutions to defend against the following types of attacks. We aim to demonstrate

AI's practical applications and benefits in enhancing edge network security by narrowing our focus to the following list of specific threats;

- Network-level attacks
- Application-level attacks
- Data-level attacks
- Access control attacks
- Protocol-based attacks
- Side channel attacks
- Supply chain attacks
- Social engineering attacks

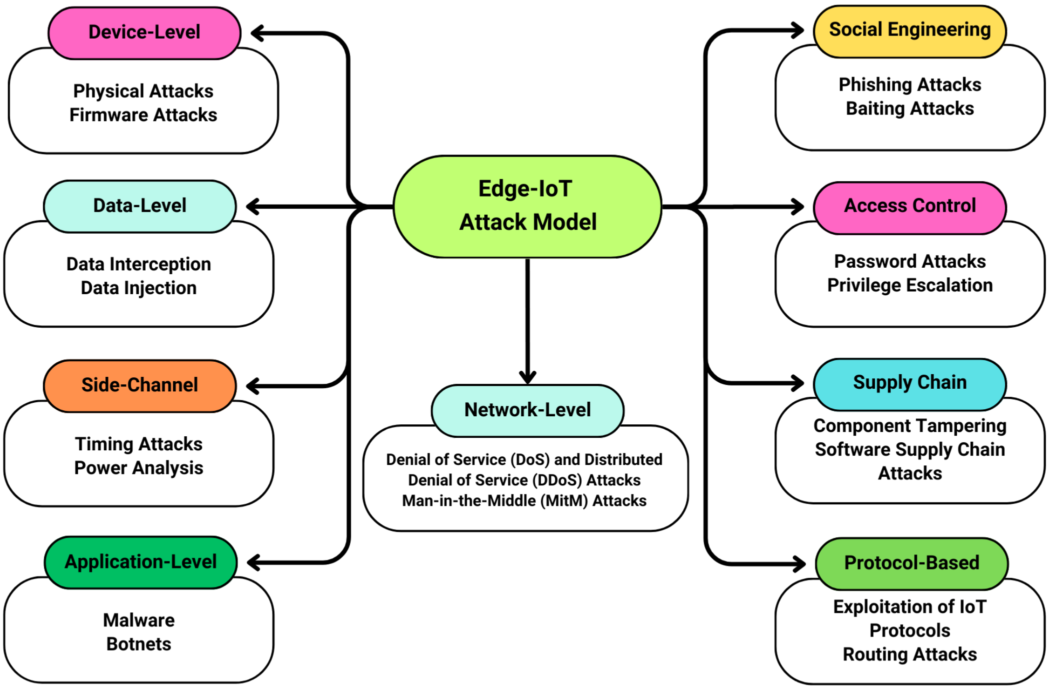

Figure 3. Edge-based IoT attack model with examples of each sub-model.

5.1. Network-Level Attacks

Distributed denial of service (DDoS) attacks and man-in-the-middle (MitM) attacks are significant network-level threats in EC-IoT environments. DDoS attacks overwhelm a network or system with traffic, rendering it inaccessible to legitimate users. In the context of EC-IoT, the decentralized nature of edge nodes can make them susceptible to DDoS attacks due to the distributed architecture [90]. These attacks can disrupt the availability of IoT services and compromise the network's reliability [91].

On the other hand, MitM attacks occur when a malicious actor intercepts and potentially alters the communication between two parties without their knowledge. In EC-IoT networks, where devices are wirelessly connected to the edge of the network, attackers can exploit the wireless nature of the communication to carry out MitM attacks [92]. These attacks can lead to unauthorized access to sensitive data transmitted between IoT devices and the edge network, posing a severe security risk [21].

Both DDoS and MitM attacks exploit vulnerabilities in the network infrastructure of EC-IoT systems. DDoS attacks target service availability by flooding the network, while MitM attacks focus on intercepting and manipulating data in transit. Understanding these attack vectors is crucial for developing robust security measures to safeguard EC-IoT environments against malicious activities.

5.2. Application-Level Attacks

At the application level, malware and botnets are significant threats in EC-IoT environments. Malware, defined as malicious software aiming to disrupt, damage, or gain unauthorized access to a computer system, can infect IoT devices at the application level, compromising their functionality and potentially spreading across the network [93]. Malware exploits vulnerabilities in IoT devices to steal sensitive data, disrupt operations, or take control of devices for malicious purposes.

Botnets are networks of compromised devices controlled by a central server, often utilized to launch coordinated attacks. In EC-IoT settings, insecure IoT devices can be manipulated by attackers to form botnets, enabling various malicious activities such as DDoS attacks, data theft, and malware dissemination [94]. Botnets utilize the computational power of multiple devices to magnify the impact of attacks, posing a potent threat in EC-IoT environments.

Both malware and botnets target the application layer in EC-IoT systems, exploiting vulnerabilities in IoT devices to compromise security and integrity. Understanding these threats is crucial for developing robust security measures to safeguard EC-IoT environments from the harmful effects of malware infections and botnet attacks.

5.3. Data-Level Attacks

Data interception and injection are two of the most prominent attacks at the data level in EC-IoT networks. Data interception involves unauthorized access to data during transmission between IoT devices and the edge network. Attackers can eavesdrop on communication channels to intercept sensitive information, jeopardizing the confidentiality and integrity of the data [95]. This attack can result in the theft of sensitive data, like personal information or proprietary business data, presenting a substantial security risk in EC-IoT systems. On the other hand, data injection attacks entail malicious actors inserting false or unauthorized data into the communication flow between IoT devices and the edge network. By injecting manipulated data packets, attackers can mislead IoT devices or the edge network into making incorrect decisions or taking malicious actions based on falsified information [96]. Data injection attacks can lead to system malfunctions, unauthorized access, or the manipulation of critical processes, undermining the reliability and trustworthiness of the entire IoT ecosystem.

5.4. Access Control Attacks

Access control attacks in EC-IoT systems, such as password attacks and privilege escalation, pose significant security risks. Password attacks involve unauthorized individuals attempting to gain access to IoT devices or edge nodes by exploiting weak or default passwords. Attackers may use brute force attacks, dictionary attacks, or password spraying to guess or crack passwords, allowing them to gain unauthorized access to sensitive data or control over IoT devices [92]. Password attacks pose a significant threat to the security and integrity of EC-IoT systems, as compromised passwords can lead to unauthorized access and potential data breaches. Privilege escalation is another security threat where attackers exploit vulnerabilities in the system to elevate their privileges beyond what is intended. In EC-IoT environments, privilege escalation can enable attackers to gain higher access levels than they are authorized, granting them control over critical functions or sensitive data [39]. By exploiting weaknesses in access control mechanisms, attackers can manipulate the system to their advantage, potentially causing significant harm to the IoT ecosystem. Both password attacks and privilege escalation underscore the importance of robust access control mechanisms in securing EC-IoT environments.

5.5. Protocol-Based Attacks

Protocol-based attacks in EC-IoT target vulnerabilities in communication protocols to compromise the security and integrity of the network. One common type of attack is the abuse of IoT communication protocols, leading to threats like AR-DDoS attacks.

These attacks exploit protocols such as constrained application protocols (CoAPs), simple service discovery protocols (SSDPs), and simple network management protocols (SNMPs) to disrupt services and compromise the availability of IoT systems [39].

Additionally, attacks can target the data transmission protocols used in IoT environments. Communication technologies like cellular networks, WiFi, ZigBee, and Bluetooth follow IoT or data transmission protocols such as the hypertext transfer protocol (HTTP) and message queuing telemetry transport (MQTT). Attackers may exploit vulnerabilities in these protocols to intercept or manipulate data, leading to unauthorized access or data breaches [35]. Also, attacks at the network layer of IoT systems can involve routing attacks, DoS attacks, and attacks on neighbor discovery protocols. In routing attacks, malicious devices redirect messages to incorrect paths, while DoS attacks flood the network with excessive data to cause congestion and resource exhaustion. Attacks on neighbor discovery protocols aim to disrupt the discovery process and compromise network integrity [42].

5.6. Side-Channel Attacks

Side-channel attacks in EC-IoT exploit unintended information leakage from the physical implementation of a system. These attacks target side-channel information such as power consumption, electromagnetic emissions, or timing variations to infer sensitive data like encryption keys or confidential information [39]. By analyzing these side-channel signals, attackers can extract valuable information without directly accessing the cryptographic algorithms or keys, compromising the system's security. Additionally, side-channel attacks can leak hardware information, such as sounds or power consumption, to extract critical data like encryption keys [39]. Attackers leverage this leaked information to gain unauthorized access to IoT devices or edge nodes, potentially leading to data breaches or unauthorized control over the system. The hidden connections between publicly available side-channel data and sensitive information make side-channel attacks a potent threat in EC-IoT environments [19].

5.7. Supply Chain Attacks

Supply chain attacks in EC-IoT systems involve malicious actors targeting vulnerabilities in the supply chain to compromise the security and integrity of the network. These attacks can occur at various supply chain stages, from the manufacturing of IoT devices to the distribution and deployment phases. Attackers may infiltrate the supply chain to introduce counterfeit components, tamper with hardware or software, or implant malware into devices before they reach end-users [42]. By exploiting weaknesses in the supply chain, attackers can compromise the confidentiality, availability, and authenticity of IoT devices, potentially leading to data breaches, service disruptions, or unauthorized access to sensitive information. Supply chain attacks pose a significant threat to the overall security of EC-IoT ecosystems, highlighting the importance of ensuring the integrity and security of every component within the supply chain [41].

5.8. Social Engineering Attacks

Social engineering attacks in EC-IoT systems involve manipulating individuals to disclose sensitive information or perform actions compromising the network's security. Attackers exploit human psychology and trust to deceive users into providing confidential data, such as login credentials or personal information. These attacks often involve impersonation, pretexting, phishing emails, or phone calls to trick individuals into disclosing valuable information [37]. Social engineering attacks can bypass traditional security measures and gain unauthorized access to IoT devices or edge nodes by exploiting human vulnerabilities rather than technical weaknesses. Attackers may use social engineering tactics to gain entry into secure areas, extract sensitive data, or manipulate individuals into executing malicious actions that could compromise the integrity of the entire IoT ecosystem [38].

6. Countermeasures in EC-IoT

Machine learning and deep learning are increasingly being utilized to enhance security measures in the internet of things (IoT) ecosystem, particularly in edge and edge-assisted IoT environments. Recent trends show a significant focus on leveraging advanced learning algorithms to strengthen security protocols in IoT systems.

Research has demonstrated a growing interest in using machine learning and deep learning techniques for IoT security [31]. These methods provide unique capabilities to address security challenges by effectively detecting anomalies and potential threats [97]. Additionally, integrating edge computing and blockchain with machine learning and deep learning has been suggested as a robust approach to ensuring reliable and efficient IoT security [98].

In the realm of IoT security, deep learning has shown promise in detecting cyberattacks and malicious devices within IoT networks [99]. Furthermore, advancements in federated learning, transfer learning, and deep learning are paving the way for more sophisticated models that are capable of autonomously identifying cyberthreats in diverse IoT-driven edge networks [100].

To enhance security in edge-assisted IoT environments, intelligent intrusion detection systems based on federated learning have been proposed [101]. Customized intrusion detection models utilizing federated transfer learning are emerging as a trending approach to designing tailored security solutions for heterogeneous IoT networks [102].

Moreover, the convergence of blockchain, machine learning, fog computing, and edge computing is being considered as a potential solution to bolster IoT security [62]. Studies have also emphasized the significance of hybrid approaches combining supervised learning and optimization algorithms for optimal detection of IoT cyberattacks [103].

6.1. Non-AI Methods

Traditional countermeasures are vital for ensuring comprehensive security in EC-IoT environments. These methods form a robust defense framework. For instance, a 2023 survey emphasized the critical role of traditional methods like firewalls, VPNs, and IDS in preventing unauthorized access and safeguarding data integrity [104]. Another study explored the effectiveness of robust encryption techniques and regular software updates in maintaining IoT security amidst evolving threats [105]. Additionally, network segmentation and multi-factor authentication significantly enhance security by isolating potential breaches and reducing unauthorized access [106].

Curated, problem-focused countermeasures are widely accepted as industry standards. Although these countermeasures are primarily developed for large, non-EC-IoT networks, they can still perform satisfactorily in EC-IoT networks. Traditional countermeasures reduce dependency on technologies such as ML or DL, ensuring that basic security measures are always in place. The authors of ref. [46] suggested employing a virtual private network (VPN) terminator system and an intrusion prevention system (IPS) with oblivious authentication to detect connected devices.

The authors of ref. [107] recommended integrating IOTA and attribute-based encryption for access control in IoT to mitigate unauthorized resource access. The research in ref. [108–110] explored blockchain-based solutions to mitigate DDoS attacks in IoT settings. The work in ref. [111] introduced privacy-preserving and security measures in SDN-based IoT, while the research in ref. [112] proposed a moving target defense (MTD) strategy for IoT cybersecurity.

6.2. AI Methods

The era of AI has also revolutionized the approach to securing EC-IoT environments. AI methods, particularly ML and DL, offer advanced solutions for detecting and preventing diverse security threats by identifying subtle patterns and anomalies that traditional methods might miss. This proactive defense is crucial, as ML has become integral to IoT security systems, helping to detect attacks, authenticate users, and categorize suspicious activities.

DL is also experiencing an exponential transition into automation applications, promising higher performance and lower complexity. However, this transition involves complex data processing, which can be time-consuming and costly. Many studies focus on supervised learning, often overlooking techniques like unsupervised and reinforcement learning and critical methodologies such as transfer, federated, and online learning [113,114]. Table 2 summarizes existing ML and DL-based techniques for detecting attacks and their advantages and disadvantages. Future research should explore unsupervised, reinforcement, and hybrid learning models and integrate new methodologies to enhance IoT security against adversarial threats.

Table 2. ML and DL-based countermeasures for different attack types in EC-IoT.

Attack Type	**AI Application**	**Advantages**	**Disadvantages**
Network-level	CNNs, RNNs (LSTMs)	High accuracy in detecting anomalies, real-time analysis	Significant computational resources required, complex model training
Application-level	Autoencoders, GANs	Effective anomaly detection, can simulate attack scenarios	Significant training time, needs large labeled datasets
Data-level	RNNs, VAEs	Good at detecting temporal anomalies, handles high-dimensional data	Potential for high false positive rates, requires continuous training
Access control	LSTMs, DBNs	Detects complex user behavior patterns, adaptive authentication	High computational cost, complex implementation
Protocol-based attacks	Autoencoders, GANs	Detects protocol-specific anomalies, improves IDS robustness	Requires extensive training data, computationally intensive
Side channel	CNNs, RNNs	Effective analysis of side channel signals, real-time detection	Significant computational power needed, difficult to implement
Supply chain	Autoencoders, GANs	Detects anomalies in supply chain data, simulates attack scenarios	High resource requirements, requires continuous updates
Social engineering	RNNs, DNNs	Analyzes communication patterns, detects phishing attempts	High false positive rate, requires large amounts of training data

6.2.1. Machine Learning

ML methods are essential in enhancing the security of EC-IoT systems by providing robust mechanisms for detecting and mitigating various attacks. For network-level attacks, support vector machines (SVMs) are used for binary classification of normal versus attack traffic, while random forests analyze various features of network traffic to classify and detect anomalies [42,115]. In application-level attacks, decision trees apply rule-based detection by identifying decision rules from training data, and naive Bayes classifiers use probabilistic classification to detect anomalies [42,115].

For data-level attacks, K-nearest neighbors (KNN) detect data points that deviate significantly from the norm, and principal component analysis (PCA) is employed for dimensionality reduction and anomaly detection [42,115]. Logistic regression is applied for binary classification of access attempts in access control attacks, while random forests analyze features of access attempts to detect anomalies [42,115].

In protocol-based attacks, SVMs classify normal and anomalous protocol usage patterns, and decision trees create rule-based models to detect deviations in protocol usage [42,115]. For side-channel attacks, PCA is used for dimensionality reduction and anomaly detection, while KNN identifies anomalous side-channel signals that deviate from normal patterns [42,115].

Supply chain attacks are countered by random forests, which classify and detect anomalies in supply chain processes, and logistic regression, which models and detects deviations in supply chain activities [42,115]. Social engineering attacks are addressed using naive Bayes classifiers for probabilistic classification of communication content to detect phishing attempts, and SVMs analyze the features of communications to classify and detect social engineering attacks [42,115].

6.2.2. Deep Learning

DL methods play a critical role in enhancing the security of EC-IoT systems by providing sophisticated mechanisms to detect and mitigate various types of attacks. Convolutional neural networks (CNNs) are used to analyze network traffic patterns, identifying anomalies indicative of network-level attacks such as SYN flooding and de-synchronization [115]. Recurrent neural networks (RNNs), including long short-term memory networks (LSTMs), are effective for time-series analyses of network traffic, enabling the detection of temporal anomalies [42]. Autoencoders, another DL method, are utilized for detecting anomalies in application-layer data by reconstructing normal patterns and identifying deviations, making them effective against application-layer attacks [42]. Generative adversarial networks (GANs) are employed to simulate attack scenarios and improve the robustness of intrusion detection systems (IDS) via training on both normal and adversarial examples [115].

For data-level attacks, RNNs and variational autoencoders (VAEs) are used to detect data anomalies over time and in high-dimensional data, respectively, helping to identify tampered or unauthorized data entries [42,115]. Access control attacks are mitigated using LSTM networks and deep belief networks (DBNs), which model complex user behavior patterns and detect deviations indicative of unauthorized access [42,115]. Protocol-based attacks are countered using autoencoders for detecting anomalies in protocol-specific data and GANs for generating synthetic attack data to improve IDS robustness [42,115].

To address side-channel attacks, CNNs analyze side-channel signals like power consumption and electromagnetic emissions to detect anomalies, while RNNs perform temporal analyses of these signals to identify patterns indicative of attacks [42,115]. For supply chain attacks, autoencoders detect anomalies in supply chain data, identifying tampered or counterfeit components, and GANs simulate supply chain attack scenarios to enhance detection capabilities [42,115]. Lastly, RNNs and deep neural networks (DNNs) are employed to analyze communication patterns and detect social engineering attacks such as phishing emails and other deceptive tactics [42,115–119].

7. Open Challenges and Future Research Opportunities

The implementation of EC-IoT security faces several critical challenges, including power constraints, memory limitations, data privacy, and ethical concerns, as well as local processing risks and training constraints. Addressing these challenges requires a proper understanding of the new and emerging technologies and the development of new, robust solutions designed to meet the specific needs of EC-IoT systems. Therefore, this section discusses some future research directions and emerging trends aimed at tackling these challenges through innovative solutions. The issues discussed in this section are summarized in Table 3. The table highlights the importance of ongoing research and development to ensure that EC-IoT systems can operate efficiently and securely. By exploring advanced methodologies and cutting-edge technologies, we aim to provide a roadmap for addressing these critical challenges, ultimately fostering a more resilient and secure EC-IoT ecosystem.

Table 3. Summary of challenges and future research directions for EC-IoT security.

Challenge	Description	Future Research Directions
Power constraints	Limited processing power in edge devices requires solutions like model pruning, on-device learning, and federated learning (FL), which can reduce data transmission but require complex implementation.	• Develop advanced pruning algorithms to maintain accuracy • Enhance model efficiency with quantization and knowledge distillation • Design energy-efficient FL algorithms • Integrate edge caching and opportunistic computing
Training constraints	Task offloading helps with intensive tasks but depends on network reliability and may introduce latency. Edge-centric training can enhance autonomy and efficiency.	• Create efficient task offloading strategies • Develop edge-centric training techniques to reduce cloud dependency
Memory limitations	Quantization reduces memory usage but can affect model precision. Mixed precision training can optimize performance and memory efficiency.	• Enhance post-training quantization methods • Develop mixed precision training techniques
Local processing risks	Hybrid processing ensures real-time processing and reduces latency but requires sophisticated architecture.	• Develop optimized hybrid architectures • Implement dynamic task allocation algorithms
Data privacy	Edge–cloud collaboration enhances data safety but can introduce latency and requires robust communication channels.	• Enhance secure multi-party computation methods • Leverage blockchain technology for secure data transactions
Ethical concerns	AI integration in EC-IoT raises ethical concerns such as potential bias, transparency, accountability, and informed consent.	• Address AI bias and ensure fairness • Ensure transparency and accountability in AI decision-making • Ensure informed consent and clear communication • Develop ethical guidelines prioritizing user well-being

Power constraints: The challenge of limited processing power in edge devices necessitates innovative solutions like model pruning, which reduces model size and complexity. However, it may lead to accuracy loss and requires careful tuning. Future research should focus on developing sophisticated pruning algorithms, such as structured and adaptive pruning, that maintain accuracy while reducing size [31,120]. Also, quantization and knowledge distillation can enhance model efficiency. On-device learning optimizes energy usage and improves device longevity but is limited by capabilities and may need frequent updates. Efficient on-device learning algorithms should be designed for low power consumption without sacrificing performance [11,20]. Federated learning (FL) reduces data transmission needs, enhancing privacy and efficiency, but requires complex implementation. Research should develop energy-efficient FL algorithms to minimize power consumption by optimizing communication protocols and reducing update frequencies [35,120]. Hierarchical FL structures can balance power consumption and computational load. Integrating edge caching and opportunistic computing can reduce energy demands while maintaining a robust performance.

Training constraints: Task offloading helps offload intensive tasks to the cloud while retaining critical processing at the edge, but it depends on network reliability and may introduce latency. Future research should focus on creating efficient task offloading strategies that minimize latency and maximize the utilization of edge and cloud resources [31,35]. Developing edge-centric training techniques that focus on maximizing the training capabilities of edge devices while minimizing dependency on cloud resources can also be beneficial. These techniques can enhance the autonomy and efficiency of edge networks, ensuring robust performance even with limited cloud interactions.

Memory limitations: Quantization is a method used to address memory limitations by lowering memory usage and enabling efficient computation on edge devices. However, this can potentially reduce model precision and affect performance. Future research could enhance post-training quantization methods to maintain a higher model accuracy while reducing memory usage [11,28]. Another promising area is mixed precision training, where lower precisions are used during less-critical training phases and higher precisions are used for essential computations. This balance can help optimize performance and memory efficiency, making deploying sophisticated models on resource-constrained edge devices feasible.

Local processing risks: Hybrid processing ensures real-time processing, reduces latency, is resource-intensive, and requires sophisticated architecture. Future research should focus on developing optimized hybrid architectures that efficiently distribute processing tasks between edge and cloud-based methods based on real-time requirements and resource availability [20,35]. Implementing dynamic task allocation algorithms that can adapt to changing network conditions and processing loads is also crucial. These algorithms can ensure optimal performance and resource utilization, providing a balanced approach to processing that leverages the strengths of edge and cloud resources.

Data privacy: Edge–cloud collaborations balance the load between the edge and cloud, enhancing data safety but potentially introducing latency issues and requiring robust communication channels. Enhancing secure multi-party computation methods can ensure data privacy during collaborative processing between edge and cloud processes [28,39]. Leveraging blockchain technology to create secure and immutable records of data transactions between edge devices and the cloud can enhance overall security. This integration can provide a decentralized and transparent approach to data management, reducing the risk of data breaches and ensuring the integrity of data exchanges.

Ethical concerns: The integration of AI in EC-IoT raises significant ethical concerns due to the quantity of data these networks handle. These concerns must be carefully assessed and addressed to ensure responsible and fair use of technology. One primary ethical issue is the potential for bias and unfairness in AI algorithms, which can perpetuate or amplify existing biases in the data, leading to discriminatory outcomes [1,2]. Guaranteeing transparency and accountability in AI-based decision-making processes is also essential; stakeholders must be able to understand and audit the decisions made by these systems to foster trust and accountability [5]. Additionally, informed consent is essential for maintaining user trust and compliance with data protection regulations, requiring clear communication to users about the data being collected and their intended use [6]. Ethical guidelines must prioritize user well-being, avoid harm, and respect user autonomy to ensure that AI technologies contribute positively to society [7]. Addressing these ethical concerns is vital for the responsible deployment of AI in EC-IoT systems, guiding future research toward developing fair, transparent, and accountable AI frameworks [8].

8. Conclusions

This paper explores the integration of EC-IoT systems with AI to address significant security and privacy challenges in IoT networks. It discusses fundamental concepts, recent advancements, and various approaches for improving EC-IoT security, emphasizing AI-based threat detection and mitigation techniques. This paper introduces the most current threats, their effects on EC-IoT systems, and a taxonomy of AI-based security models, highlighting their effectiveness in enhancing EC-IoT security. It also provides a concise discussion on implementing and optimizing AI algorithms tailored for edge-based IoT environments. Finally, it outlines open challenges and potential research directions to inspire future research and practical applications in the evolving landscape of EC-IoT security.

Author Contributions: Investigation, D.R.; writing, D.R.; writing—review and editing, N.K.; supervision, N.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The original contributions presented in the study are included in the article, further inquiries can be directed to the corresponding authors.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Fawzy, D.; Moussa, S.; Badr, N. The internet of things and architectures of big data analytics: Challenges of intersection at different domains. *IEEE Access* **2022**, *10*, 4969–4992. [CrossRef]
2. Din, I.; Guizani, M.; Hassan, S.; Kim, B.; Khan, M.; Atiquzzaman, M. The internet of things: A review of enabled technologies and future challenges. *IEEE Access* **2019**, *7*, 7606–7640. [CrossRef]
3. Chataut, R.; Phoummalayvane, A.; Akl, R. Unleashing the Power of IoT: A Comprehensive Review of IoT Applications and Future Prospects in Healthcare, Agriculture, Smart Homes, Smart Cities, and Industry 4.0. *Sensors* **2023**, *23*, 7194. [CrossRef]
4. Ye, L.; Wang, Z.; Jia, T.; Ma, Y.; Shen, L.; Zhang, Y.; Li, H.; Chen, P.; Wu, M.; Liu, Y.; et al. Research progress on low-power artificial intelligence of things (AIoT) chip design. *Sci. China Inf. Sci.* **2023**, *66*, 200407. [CrossRef]
5. Ibarra-Esquer, J.; Gonzalez-Navarro, F.; Sánchez, J.; Flores-Rios, B.; Astorga-Vargas, M.; González-Ramírez, M. Graphical framework for categorizing data capabilities and properties of objects in the internet of things. *IEEE Access* **2020**, *8*, 22366–22377. [CrossRef]
6. Jan, S.; Ahmed, S.; Shakhov, V.; Koo, I. Toward a lightweight intrusion detection system for the internet of things. *IEEE Access* **2019**, *7*, 42450–42471. [CrossRef]
7. Nain, Z.; Musaddiq, A.; Qadri, Y.; Nauman, A.; Afzal, M.; Kim, S. Riata: A reinforcement learning-based intelligent routing update scheme for future generation iot networks. *IEEE Access* **2021**, *9*, 81161–81172. [CrossRef]
8. Ahmad, I.; Abdullah, S.; Bukhsh, M.; Ahmed, A.; Arshad, H.; Khan, T. Message scheduling in blockchain based iot environment with additional fog broker layer. *IEEE Access* **2022**, *10*, 97165–97182. [CrossRef]
9. Eldrandaly, K.; Abdel-Basset, M.; Shawky, L. Internet of spatial things: A new reference model with insight analysis. *IEEE Access* **2019**, *7*, 19653–19669. [CrossRef]
10. Xu, W.; Fang, W.; Ding, Y.; Zou, M.; Xiong, N. Accelerating federated learning for iot in big data analytics with pruning, quantization and selective updating. *IEEE Access* **2021**, *9*, 38457–38466. [CrossRef]
11. Alwarafy, A.; Al-Thelaya, K.A.; Abdallah, M.; Schneider, J.; Hamdi, M. A Survey on Security and Privacy Issues in Edge-Computing-Assisted Internet of Things. *IEEE Internet Things J.* **2021**, *8*, 4004–4022. [CrossRef]

12. Salh, A.; Ngah, R.; Audah, L.; Kim, K.; Abdullah, Q.; Al-Molikie, Y.M.; Aljaloud, K.A.; Talib, H.N. Energy-efficient federated learning with resource allocation for green iot edge intelligence in b5g. *IEEE Access* **2023**, *11*, 16353–16367. [CrossRef]
13. Manokaran, J.; Vairavel, G. An empirical comparison of machine learning algorithms for attack detection in internet of things edge. *ECS Trans.* **2022**, *107*, 2403–2417. [CrossRef]
14. Boopathi, M.; Gupta, S.; Mohammed Zabeeulla, A.N.; Gupta, R.; Vekriya, V.; Pandey, A. Optimization algorithms in security and privacy-preserving data disturbance for collaborative edge computing social IoT deep learning architectures. *Res. Sq.* **2023**. [CrossRef]
15. Tawalbeh, L.; Muheidat, F.; Tawalbeh, M.; Quwaider, M. IoT privacy and security: Challenges and solutions. *Appl. Sci.* **2020**, *10*, 4102. [CrossRef]
16. Liao, H.; Zhou, Z.; Zhao, X.; Zhang, L.; Mumtaz, S.; Jolfaei, A.; Ahmed, S.H.; Bashir, A.K. Learning-based context-aware resource allocation for edge-computing-empowered industrial iot. *IEEE Internet Things J.* **2020**, *7*, 4260–4277. [CrossRef]
17. Nagarajan, G.; Simpson, S.; Venkatachalam, K.; Alrasheedi, A.; Askar, S.; Abouhawwash, M.; Parthasarathi, P. A novel edge-based trust management system for the smart city environment using eigenvector analysis. *J. Healthc. Eng.* **2022**, *2022*, 5625897 [CrossRef]
18. Wang, Y.; Tian, Z.; Fan, X.; Huang, Y.; Nowzari, C.; Zeng, K. Distributed swarm learning for internet of things at the edge: Where artificial intelligence meets biological intelligence. *arXiv* **2022**, arXiv:2210.16705. [CrossRef]
19. Fazeldehkordi, E.; Grønli, T.M. A Survey of Security Architectures for Edge Computing-Based IoT. *IoT* **2022**, *3*, 332–365. [CrossRef]
20. Zhang, S.; Cao, D.; Ning, Z. A decentralized and reliable trust measurement for edge computing enabled internet of things. *Concurr. Comput. Pract. Exp.* **2022**, *34*, e7238. [CrossRef]
21. Li, J.; Cai, J.; Khan, F.; Rehman, A.U.; Balasubramaniam, V.; Sun, J.; Venu, P. A Secured Framework for SDN-Based Edge Computing in IoT-Enabled Healthcare System. *IEEE Access* **2020**, *8*, 135479–135490. [CrossRef]
22. Dawod, A.; Georgakopoulos, D.; Jayaraman, P.; Nirmalathas, A.; Parampalli, U. IoT device integration and payment via an autonomic blockchain-based service for IoT device sharing. *Sensors* **2022**, *22*, 1344. [CrossRef]
23. Hwang, J.; Nkenyereye, L.; Sung, N.; Kim, J.; Song, J. IoT service slicing and task offloading for edge computing. *IEEE Internet Things J.* **2021**, *8*, 11526–11547. [CrossRef]
24. Waris, Z.; Jaleel, A.; Shoaib, M.; Abalo, D. A suite of design quality metrics for internet of things by modelling its ecosystem as a schema graph. *Math. Probl. Eng.* **2022**, *2022*, 3278371. [CrossRef]
25. Aziez, M.; Benharzallah, S.; Bennoui, H. A full comparison study of service discovery approaches for internet of things. *Int. J. Pervasive Comput. Commun.* **2019**, *15*, 30–56. [CrossRef]
26. Ma, Y.; Wu, Y.; Ge, J.; Li, J. An architecture for accountable anonymous access in the internet-of-things network. *IEEE Access* **2018**, *6*, 14451–14461. [CrossRef]
27. An, J.; Li, W.; Gall, F.; Kovac, E.; Kim, J.; Taleb, T. EIF: Toward an elastic IoT fog framework for AI services. *IEEE Commun. Mag.* **2019**, *57*, 28–33. [CrossRef]
28. Sha, K.; Yang, T.A.; Wei, W.; Davari, S. A Survey of Edge Computing-Based Designs for IoT Security. *Digit. Commun. Netw.* **2020**, *6*, 195–202. [CrossRef]
29. Hassija, V.; Chamola, V.; Saxena, V.; Jain, D.; Goyal, P.; Sikdar, B. A survey on IoT security: Application areas, security threats, and solution architectures. *IEEE Access* **2019**, *7*, 82721–82743. [CrossRef]
30. Ullah, A.; Azeem, M.; Ashraf, H.; Alaboudi, A.A.; Humayun, M.; Jhanjhi, N. Secure Healthcare Data Aggregation and Transmission in IoT—A Survey. *IEEE Access* **2021**, *9*, 16849–16865. [CrossRef]
31. Al-Garadi, M.A.; Mohamed, A.; Al-Ali, A.K.; Du, X.; Ali, I.; Guizani, M. A survey of machine and deep learning methods for Internet of Things (IoT) security. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 1646–1685. [CrossRef]
32. Sarker, V.K.; Queralta, J.P.; Gia, T.N.; Tenhunen, H.; Westerlund, T. A Survey on LoRa for IoT: Integrating Edge Computing. In Proceedings of the 2019 Fourth International Conference on Fog and Mobile Edge Computing (FMEC), Rome, Italy, 10–13 June 2019. [CrossRef]
33. Liu, D.; Yan, Z.; Ding, W.; Atiquzzaman, M. A Survey on Secure Data Analytics in Edge Computing. *IEEE Internet Things J.* **2019**, 6, 4946–4967. [CrossRef]
34. Uprety, A.; Rawat, D.B. Reinforcement Learning for IoT Security: A Comprehensive Survey. *IEEE Internet Things J.* **2021**, *8*, 8693–8706. [CrossRef]
35. Xu, Z.; Liu, W.; Huang, J.; Yang, C.; Lu, J.; Tan, H. Artificial Intelligence for Securing IoT Services in Edge Computing: A Survey. *Secur. Commun. Netw.* **2020**, *2020*, 8872586. [CrossRef]
36. Yue, Y.; Li, S.; Legg, P.; Li, F. Deep Learning-Based Security Behaviour Analysis in IoT Environments: A Survey. *Secur. Commun. Netw.* **2021**, *2021*, 8873195. [CrossRef]
37. Ahmad, I.; Niazy, M.S.; Ziar, R.A.; Khan, S. Survey on IoT: Security Threats and Applications. *J. Robot. Control (JRC)* **2021**, *2*, 1–5. [CrossRef]
38. Ahmad, W.; Rasool, A.; Javed, A.R.; Baker, T.; Jalil, Z. Cyber Security in IoT-Based Cloud Computing: A Comprehensive Survey. *Electronics* **2021**, *11*, 16. [CrossRef]
39. Yu, M.; Zhuge, J.; Cao, M.; Shi, Z.; Jiang, L. A Survey of Security Vulnerability Analysis, Discovery, Detection, and Mitigation on IoT Devices. *Future Internet* **2020**, *12*, 27. [CrossRef]

40. Hamdan, S.; Ayyash, M.; Almajali, S. Edge-Computing Architectures for Internet of Things Applications: A Survey. *Sensors* **2020**, *20*, 6441. [CrossRef]
41. Chegini, H.; Naha, R.K.; Mahanti, A.; Thulasiraman, P. Process Automation in an IoT–Fog–Cloud Ecosystem: A Survey and Taxonomy. *IoT* **2021**, *2*, 92–118. [CrossRef]
42. Tsiknas, K.; Taketzis, D.; Demertzis, K.; Skianis, C. Cyber Threats to Industrial IoT: A Survey on Attacks and Countermeasures. *IoT* **2021**, *2*, 163–186. [CrossRef]
43. Alsharif, M.H.; Kelechi, A.H.; Jahid, A.; Kannadasan, R.; Singla, M.K.; Gupta, J.; Geem, Z.W. A comprehensive survey of energy-efficient computing to enable sustainable massive IoT networks. *Alex. Eng. J.* **2024**, *91*, 12–29. [CrossRef]
44. Mundhe Prachi, N.; Rokade, M.D. Autonomous IoT System Security Capability: Pushing IoT Security to the Edge. *Int. J. Adv. Res. Sci. Commun. Technol. (IJARSCT)* **2022**, *2*, 378. [CrossRef]
45. Liao, Z.; Pang, X.; Zhang, J.; Xiong, B.; Wang, J. Blockchain on Security and Forensics Management in Edge Computing for IoT: A Comprehensive Survey. *IEEE Trans. Netw. Serv. Manag.* **2022**, *19*, 1159–1175. [CrossRef]
46. Canavese, D.; Mannella, L.; Regano, L.; Basile, C. Security at the Edge for Resource-Limited IoT Devices. *Sensors* **2024**, *24*, 590. [CrossRef] [PubMed]
47. Ren, J.; Hou, T.; Zheng, S.; Tang, C. Collaborative edge computing and caching with deep reinforcement learning decision agents. *IEEE Access* **2020**, *8*, 120604–120612. [CrossRef]
48. Chen, Y.; Qiu, Z. Cloud network and mathematical model calculation scheme for dynamic big data. *IEEE Access* **2020**, *8*, 137322–137329. [CrossRef]
49. Zhao, Y.; Wang, W.; Li, Y.; Colman-Meixner, C.; Tornatore, M.; Zhang, J. Edge computing and networking: A survey on infrastructures and applications. *IEEE Access* **2019**, *7*, 101213–101230. [CrossRef]
50. Wang, F.; Zhang, M.; Wang, X.; Ma, X.; Liu, J. Deep learning for edge computing applications: A state-of-the-art survey. *IEEE Access* **2020**, *8*, 58322–58336. [CrossRef]
51. Habibi, P.; Farhoudi, M.; Kazemian, S.; Khorsandi, S.; Leon-Garcia, A. Fog computing: A comprehensive architectural survey. *IEEE Access* **2020**, *8*, 69105–69133. [CrossRef]
52. Rosero-Montalvo, P.; István, Z.; Hernández, W. A survey of trusted computing solutions using fpgas. *IEEE Access* **2023**, *11*, 31583–31593. [CrossRef]
53. Bhat, S.; Sofi, I.; Chi, C. Edge computing and its convergence with blockchain in 5g and beyond: Security, challenges, and opportunities. *IEEE Access* **2020**, *8*, 205340–205373. [CrossRef]
54. Sharghivand, N.; Derakhshan, F.; Siasi, N. A comprehensive survey on auction mechanism design for cloud/edge resource management and pricing. *IEEE Access* **2021**, *9*, 126502–126529. [CrossRef]
55. Girs, S.; Sentilles, S.; Asadollah, S.; Ashjaei, M.; Mubeen, S. A systematic literature study on definition and modeling of service-level agreements for cloud services in IoT. *IEEE Access* **2020**, *8*, 134498–134513. [CrossRef]
56. Zhang, H.; Shi, J.; Deng, B.; Jia, G.; Han, G.; Shu, L. Mcte: Minimizes task completion time and execution cost to optimize scheduling performance for smart grid cloud. *IEEE Access* **2019**, *7*, 134793–134803. [CrossRef]
57. Pham, Q.; Le, L.; Chung, S.; Hwang, W. Mobile edge computing with wireless backhaul: Joint task offloading and resource allocation. *IEEE Access* **2019**, *7*, 16444–16459. [CrossRef]
58. Gao, Z.; Hao, W.; Han, Z.; Yang, S. Q-learning-based task offloading and resources optimization for a collaborative computing system. *IEEE Access* **2020**, *8*, 149011–149024. [CrossRef]
59. Abdulazeez, D.; Askar, S. Offloading mechanisms based on reinforcement learning and deep learning algorithms in the fog computing environment. *IEEE Access* **2023**, *11*, 12555–12586. [CrossRef]
60. Nezami, Z.; Zamanifar, K.; Djemame, K.; Pournaras, E. Decentralized edge-to-cloud load balancing: Service placement for the internet of things. *IEEE Access* **2021**, *9*, 64983–65000. [CrossRef]
61. Mayer, A.; Rodrigues, V.; Costa, C.; Righi, R.; Roehrs, A.; Antunes, R. Fogchain: A fog computing architecture integrating blockchain and Internet of Things for personal health records. *IEEE Access* **2021**, *9*, 122723–122737. [CrossRef]
62. Khan, N.; Awang, A.; Karim, S. Security in internet of things: A review. *IEEE Access* **2022**, *10*, 104649–104670. [CrossRef]
63. Klein, T.; Fenn, T.; Katzenbach, A.; Teigeler, H.; Lins, S.; Sunyaev, A. A threat model for vehicular fog computing. *IEEE Access* **2022**, *10*, 133256–133278. [CrossRef]
64. Khashan, O. Hybrid lightweight proxy re-encryption scheme for secure fog-to-things environment. *IEEE Access* **2020**, *8*, 66878–66887. [CrossRef]
65. Ribeiro, F.; Kamienski, C. A survey on trustworthiness for the internet of things. *IEEE Access* **2021**, *9*, 42493–42514. [CrossRef]
66. Ammad, M.; Shah, M.; Islam, S.; Maple, C.; Alaulamie, A.; Rodrigues, J. A novel fog-based multi-level energy-efficient framework for IoT-enabled smart environments. *IEEE Access* **2020**, *8*, 150010–150026. [CrossRef]
67. Verma, P.; Tiwari, R.; Hong, W.; Upadhyay, S.; Yeh, Y. Fetch: A deep learning-based fog computing and IoT integrated environment for healthcare monitoring and diagnosis. *IEEE Access* **2022**, *10*, 12548–12563. [CrossRef]
68. Hou, L.; Gregory, M.; Li, S. A survey of multi-access edge computing and vehicular networking. *IEEE Access* **2022**, *10*, 123436–123451. [CrossRef]
69. Wang, B.; Li, M.; Jin, X.; Guo, C. A Reliable IoT Edge Computing Trust Management Mechanism for Smart Cities. *IEEE Access* **2020**, *8*, 46373–46399. [CrossRef]

70. Malazi, H.; Chaudhry, S.; Kazmi, A.; Palade, A.; Cabrera, C.; White, G.; Clarke, S. Dynamic service placement in multi-access edge computing: A systematic literature review. *IEEE Access* **2022**, *10*, 32639–32688. [CrossRef]
71. Babar, M.; Khan, M.; Ali, F.; Imran, M.; Shoaib, M. Cloudlet computing: Recent advances, taxonomy, and challenges. *IEEE Access* **2021**, *9*, 29609–29622. [CrossRef]
72. Nayyer, M.; Raza, I.; Hussain, S.; Jamal, M.; Gillani, Z.; Hur, S.; Ashraf, I. LBRO: Load balancing for resource optimization in edge computing. *IEEE Access* **2022**, *10*, 97439–97449. [CrossRef]
73. Nam, S. The impact of 5g multi-access edge computing cooperation announcement on the telecom operators' firm value. *ETRI J.* **2022**, *44*, 588–598. [CrossRef]
74. Santi, N.; Mitton, N. A resource management survey for mission-critical and time-critical applications in multi-access edge computing. *ITU J. Future Evol. Technol.* **2021**, *2*, 61–80. [CrossRef]
75. Jin, H.; Gregory, M.; Li, S. A review of intelligent computation offloading in multi-access edge computing. *IEEE Access* **2022**, *10*, 71481–71495. [CrossRef]
76. Wang, X. Research on computational offloading strategies based on mobile edge computing. In Proceedings of the Second International Conference on Optics and Communication Technology (ICOCT 2022), Hefei, China, 15–17 July 2022. [CrossRef]
77. Siriwardhana, Y.; Porambage, P.; Liyanage, M.; Ylianttila, M. A survey on mobile augmented reality with 5g mobile edge computing: Architectures, applications, and technical aspects. *IEEE Commun. Surv. Tutor.* **2021**, *23*, 1160–1192. [CrossRef]
78. Jiang, F.; Wang, K.; Dong, L.; Pan, C.; Xu, W.; Yang, K. AI driven heterogeneous mec system with uav assistance for dynamic environment: Challenges and solutions. *IEEE Netw.* **2021**, *35*, 400–408. [CrossRef]
79. Goudarzi, M.; Palaniswami, M.; Buyya, R. Scheduling IoT applications in edge and fog computing environments: A taxonomy and future directions. *ACM Comput. Surv.* **2022**, *55*, 1–41. [CrossRef]
80. Lim, J. Latency-aware task scheduling for IoT applications based on artificial intelligence with partitioning in small-scale fog computing environments. *Sensors* **2022**, *22*, 7326. [CrossRef] [PubMed]
81. Xu, T.; Wang, X.; Su, T.; Wan, L.; Sun, L. Vehicle location in edge computing enabling IoTs based on bistatic FDA-MIMO radar. *IEEE Access* **2021**, *9*, 46398–46408. [CrossRef]
82. Kumhar, M.; Bhatia, J. Edge computing in SDN-enabled IoT-based healthcare frameworks. *Int. J. Reliab. Qual. E-Healthc.* **2022**, *11*, 1–15. [CrossRef]
83. An, R. Optimal design of ecological landscape spatial structure based on edge computing of internet of things. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 1–9. [CrossRef]
84. Shen, S.; Zhou, Y.; Ci, S. Security in edge-assisted internet of things: Challenges and solutions. *Sci. China Inf. Sci.* **2020**, *63*, 220302. [CrossRef]
85. Kim, Y.; Song, C.; Han, H.; Jung, H.; Kang, S. Collaborative task scheduling for IoT-assisted edge computing. *IEEE Access* **2020**, *8*, 216593–216606. [CrossRef]
86. Gao, X.; Liu, R.; Kaushik, A. A Distributed Virtual Network Function Placement Approach in Satellite Edge and Cloud Computing. *arXiv* **2021**, arXiv:2104.02421. [CrossRef]
87. Alnajim, A.M.; Habib, S.; Islam, M.; Thwin, S.M.; Alotaibi, F. A Comprehensive Survey of Cybersecurity Threats, Attacks, and Effective Countermeasures in Industrial Internet of Things. *Technologies* **2023**, *11*, 161. [CrossRef]
88. Mahadevappa, P.; Al-amri, R.; Alkawsi, G.; Alkahtani, A.A.; Alghenaim, M.F.; Alsamman, M. Analyzing Threats and Attacks in Edge Data Analytics within IoT Environments. *IoT* **2024**, *5*, 123–154. [CrossRef]
89. Khraisat, A.; Alazab, A. A critical review of intrusion detection systems in the internet of things: Techniques, deployment strategy, validation strategy, attacks, public datasets and challenges. *Cybersecurity* **2023**, *4*, 18. [CrossRef]
90. Lei, W.; Wen, H.; Hou, W.; Xu, X. New Security State Awareness Model for IoT Devices with Edge Intelligence. *IEEE Access* **2021**, *9*, 69756–69765. [CrossRef]
91. Bukhsh, M.; Abdullah, S.; Bajwa, I.S. A Decentralized Edge Computing Latency-Aware Task Management Method with High Availability for IoT Applications. *IEEE Access* **2021**, *8*, 40791–40808. [CrossRef]
92. Hsu, C.L.; Le, T.V.; Lu, C.F.; Lin, T.W.; Chuang, T.H. A Privacy-Preserved E2E Authenticated Key Exchange Protocol for Multi-Server Architecture in Edge Computing Networks. *IEEE Access* **2020**, *8*, 40791–40808. [CrossRef]
93. Chen, B.; Cheng, S.; Mwangi, M. A mobility-based epidemic model for iot malware spread. *IEEE Access* **2022**, *10*, 107929–107941. [CrossRef]
94. Alasmary, F.; Alraddadi, S.; Al-Ahmadi, S.; Al-Muhtadi, J. Shieldrnn: A distributed flow-based ddos detection solution for IoT using sequence majority voting. *IEEE Access* **2022**, *10*, 88263–88275. [CrossRef]
95. Alharbi, I.; Almalki, A.; Alyami, M.; Zou, C.; Yan, S. Profiling attack on wifi-based iot devices using an eavesdropping of an encrypted data frames. *Adv. Sci. Technol. Eng. Syst. J.* **2022**, *7*, 49–57. [CrossRef]
96. AlAmri, S.; ALAbri, F.; Sharma, T. *Artificial Intelligence Deployment to Secure IoT in Industrial Environment*; IntechOpen: London, UK, 2023. [CrossRef]
97. Banaamah, A.; Ahmad, I. Intrusion detection in iot using deep learning. *Sensors* **2022**, *22*, 8417. [CrossRef] [PubMed]
98. Ebrahim, M.; Hafid, A.; Elie, E. Blockchain as privacy and security solution for smart environments: A survey. *arXiv* **2022**, arXiv:2203.08901. [CrossRef]
99. Lingamallu, R. Securing iot networks: A fog-based framework for malicious device detection. *Matec Web Conf.* **2024**, *392*, 01103. [CrossRef]

100. Garg, S.; Kaur, K.; Kaddoum, G.; Garigipati, P.; Aujla, G. Security in iot-driven mobile edge computing: New paradigms, challenges, and opportunities. *IEEE Netw.* **2021**, *35*, 298–305. [CrossRef]
101. Man, D.; Zeng, F.; Yang, W.; Yu, M.; Lv, J.; Wang, Y. Intelligent intrusion detection based on federated learning for edge-assisted internet of things. *Secur. Commun. Netw.* **2021**, *2021*, 9361348. [CrossRef]
102. Abosata, N.; Al-Rubaye, S.; Tsourdos, A. Customised intrusion detection for an industrial iot heterogeneous network based on machine learning algorithms called ftl-cid. *Sensors* **2022**, *23*, 321. [CrossRef]
103. Sirat, M. Hybrid of supervised learning and optimization algorithm for optimal detection of iot distributed denial of service attacks. *Int. J. Innov. Comput.* **2023**, *13*, 1–12. [CrossRef]
104. Doe, J.; Smith, A. Recent advances in non-AI countermeasures for IoT security. *J. Cybersecur.* **2023**, *15*, 123–145.
105. Miller, B.; Brown, C. A survey on traditional security measures in IoT: Challenges and solutions. *Int. J. Netw. Secur.* **2023**, *20*, 234–256.
106. Wilson, R.; Taylor, L. Edge computing and IoT security: Strategies and best practices. *IEEE Internet Things J.* **2023**, *10*, 2345–2356.
107. Zhang, Y.; Nakanishi, R.; Sasabe, M.; Kasahara, S. Combining IOTA and Attribute-Based Encryption for access control in the Internet of Things. *Sensors* **2021**, *21*, 5053. [CrossRef]
108. Shah, Z.; Ullah, I.; Li, H.; Levula, A.; Khurshid, K. Blockchain based solutions to mitigate distributed denial of service (DDoS) attacks in the Internet of Things (IoT): A survey. *Sensors* **2022**, *22*, 1094. [CrossRef]
109. Setia, P. Enhancing cybersecurity defense of IoT ecosystem using blockchain. *Suranaree J. Sci. Technol.* **2023**, *30*, 010238. [CrossRef]
110. Ghribi, E.; Khoei, T.T.; Gorji, H.T.; Ranganathan, P.; Kaabouch, N. A Secure Blockchain-based Communication Approach for UAV Networks. In Proceedings of the IEEE International Conference on Electro Information Technology (EIT), Chicago, IL, USA, 31 July–1 August 2020; pp. 411–415.
111. Ahmadvand, H.; Lal, C.; Hemmati, H.; Sookhak, M.; Conti, M. Privacy-preserving and security in SDN-based IoT: A survey. *IEEE Access* **2023**, *11*, 44772–44786. [CrossRef]
112. Mercado-Velazquez, A.; Escamilla-Ambrosio, P.; Ortiz-Rodriguez, F. A moving target defense strategy for Internet of Things cybersecurity. *IEEE Access* **2021**, *9*, 118406–118418. [CrossRef]
113. Talaei Khoei, T.; Kaabouch, N. Machine Learning: Models, Challenges, and Research Directions. *Future Internet* **2023**, *15*, 332. [CrossRef]
114. Khazane, H.; Ridouani, M.; Salahdine, F.; Kaabouch, N. A Holistic Review of Machine Learning Adversarial Attacks in IoT Networks. *Future Internet* **2024**, *16*, 32. [CrossRef]
115. DeMedeiros, K.; Hendawi, A.; Alvarez, M. A Survey of AI-Based Anomaly Detection in IoT and Sensor Networks. *Sensors* **2023**, *23*, 1352. [CrossRef]
116. Aldhaheri, A.; Alwahedi, F.; Ferrag, M.A.; Battah, A. Deep learning for cyber threat detection in IoT networks: A review. *Internet Things Cyber-Phys. Syst.* **2023**, *4*, 110–128. [CrossRef]
117. Madhu, B.; Chari, M.V.G.; Vankdothu, R.; Silivery, A.K.; Aerranagula, V. Intrusion detection models for IOT networks via deep learning approaches. *Meas. Sens.* **2023**, *25*, 100641. [CrossRef]
118. Wang, Z.; Chen, H.; Yang, S.; Luo, X.; Li, D.; Wang, J. A lightweight intrusion detection method for IoT based on deep learning and dynamic quantization. *PeerJ Comput. Sci.* **2023**, *9*, e1569. [CrossRef] [PubMed]
119. Alghamdi, R.; Bellaiche, M. An ensemble deep learning based IDS for IoT using Lambda architecture. *Cybersecurity* **2023**, *6*, 5. [CrossRef]
120. Ferrag, M.A.; Shu, L.; Yang, X.; Derhab, A.; Maglaras, L.A. Deep learning for cyber threat detection in IoT networks: A review. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 1646–1685.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.